

Assurance Activity Report for Juniper vSRX3.0 with Junos OS 22.2R2

**Juniper vSRX3.0 with Junos OS 22.2R2 Security Target
Version 0.9**

**collaborative Protection Profile for Network Devices
Version 2.2e**

**PP-Module for Intrusion Prevention Systems (IPS),
Version 1.0**

**PP-Module for Stateful Traffic Filter Firewalls,
Version 1.4 + Errata 20200625**

**PP-Module for Virtual Private Network (VPN) Gateways
Version 1.2**

AAR Version 0.6, 01-19-2024

Evaluated by:



**2400 Research Blvd, Suite 395
Rockville, MD 20850**

Prepared for:



**National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme**

The Developer of the TOE:

Juniper Networks, Inc.

The Author of the Security Target:

Acumen Security, LLC

The TOE Evaluation was Sponsored by:

Juniper Networks, Inc.

Evaluation Personnel:

Yogesh Pawar

Pratheek Menon

Adarsh Pandey

Common Criteria Version

Common Criteria Version 3.1 Revision 5

Common Evaluation Methodology Version

CEM Version 3.1 Revision 5

Revision History

VERSION	DATE	CHANGES
0.1	04/11/2023	Started with addressing AAR EAs after updating with MOD_VPNGWv1.2
0.2	09/01/2023	Updated TOE version to 22.2R2 from 22.2R1
0.3	09/29/2023	Addressed QA comments and minor corrections
0.4	12/14/2023	Addressed ECR comments.
0.5	01/09/2024	Addressed as per Certificate review comments.
0.6	01/19/2024	Minor update

Contents

1	TOE Overview	11
2	Assurance Activities Identification	12
3	Test Equivalency Justification	13
3.1	Architectural Description	13
3.2	OS, Processor, and Firmware Analysis.....	16
3.3	Specification of Differences	17
3.4	Equivalency Analysis	18
3.4.1	Platform/Hardware Dependencies	18
3.4.2	Software/OS Dependencies:	18
3.4.3	Differences in Libraries Used to Provide TOE Functionality	18
3.4.4	TOE Management Interface Differences	18
3.4.5	TOE Functional Differences.....	18
3.4.6	Difference Comparison	18
3.5	Recommendations/Conclusions.....	19
4	Test Bed Descriptions	20
4.1	Test Time & Location	26
5	Detailed Test Cases (TSS and Guidance Activities)	27
5.1	TSS and Guidance Activities (Auditing).....	27
5.1.1	FAU_GEN.1.....	27
5.1.1	FAU_GEN.1/IPS	32
5.1.1	FAU_GEN.1/VPN	33
5.1.2	FAU_STG.1.....	34
5.1.3	FAU_STG_EXT.1.....	35
5.2	TSS and Guidance Activities (Cryptographic Support).....	39
5.2.1	FCS_CKM.1	39
5.2.2	FCS_CKM.1.1/IKE.....	40
5.2.3	FCS_CKM.2	44
5.2.4	FCS_CKM.4	45
5.2.5	FCS_COP.1/DataEncryption	51
5.2.6	FCS_COP.1/SigGen	53
5.2.7	FCS_COP.1/Hash	54
5.2.8	FCS_COP.1/KeyedHash	55
5.2.9	FCS_RBG_EXT.1	56
5.3	TSS and Guidance Activities (IPsec)	57
5.3.1	FCS_IPSEC_EXT.1.....	57
5.4	TSS and Guidance Activities (NTP).....	73
5.4.1	FCS_NTP_EXT.1	73

5.5	TSS and Guidance Activities (SSH)	76
5.5.1	FCS_SSHS_EXT.1	76
5.6	TSS and Guidance Activities (User Data Protection)	83
5.6.1	FDP_RIP.2	83
5.7	TSS and Guidance Activities (Firewall)	84
5.7.1	FFW_RUL_EXT.1	84
5.7.2	FFW_RUL_EXT.2	99
5.8	TSS and Guidance Activities (Identification and Authentication)	100
5.8.1	FIA_AFL.1.....	100
5.8.2	FIA_PMG_EXT.1	102
5.8.3	FIA_PSK_EXT.1	104
5.8.4	FIA_UIA_EXT.1.....	104
5.8.5	FIA_UAU.7	106
5.8.6	FIA_X509_EXT.1/Rev.....	106
5.8.7	FIA_X509_EXT.2	108
5.8.8	FIA_X509_EXT.3	110
5.9	TSS and Guidance Activities (Security Management)	110
5.9.1	FMT_MOF.1/ManualUpdate.....	110
5.9.2	FMT_FMT_MOF.1/Functions	111
5.9.3	FMT_MOF.1/Services.....	113
5.9.4	FMT_MTD.1/CoreData.....	114
5.9.5	FMT_MTD.1/CryptoKeys.....	117
5.9.6	FMT_SMF.1	118
5.9.7	FMT_SMF.1/IPS.....	121
5.9.8	FMT_SMF.1/VPN.....	123
5.9.9	FMT_SMR.2	124
5.10	TSS and Guidance Activities (Packet Filtering)	125
5.10.1	FPF_RUL_EXT.1	125
5.11	TSS and Guidance Activities (Protection of the TSF)	133
5.11.1	FPT_APW_EXT.1.....	133
5.11.2	FPT_FLS.1/SelfTest	134
5.11.3	FPT_SKP_EXT.1.....	135
5.11.4	FPT_STM_EXT.1.....	135
5.11.5	FPT_TST_EXT.1.1	137
5.11.6	FPT_TST_EXT.3	138
5.11.7	FPT_TUD_EXT.1.....	139
5.12	TSS and Guidance Activities (TOE Access)	143
5.12.1	FTA_SSL_EXT.1	143
5.12.2	FTA_SSL.3	144
5.12.3	FTA_SSL.4	145
5.12.4	FTA_TAB.1	146
5.13	TSS and Guidance Activities (Trusted Path/Channels)	147
5.13.1	FTP_ITC.1.....	147
5.13.2	FTP_ITC.1/VPN	148

5.13.3	FTP_TRP.1/Admin	150
5.14	TSS and Guidance Activities (Intrusion Prevention).....	151
5.14.1	IPS_ABD_EXT.1.....	151
5.14.2	IPS_IPB_EXT.1	153
5.14.3	IPS_NTA_EXT.1.....	154
5.14.4	IPS_SBD_EXT.1	157
6	Detailed Test Cases (Test Activities).....	164
6.1	Audit.....	164
6.1.1	FAU_GEN.1 Test #1	164
6.1.2	FAU_STG_EXT.1 Test #1	164
6.1.3	FAU_STG_EXT.1 Test #2 (b)	165
6.1.4	FCS_NTP_EXT.1.1 Test #1.....	166
6.1.5	FCS_NTP_EXT.1.2 Test #1.....	166
6.1.6	FCS_NTP_EXT.1.3 Test #1.....	169
6.1.7	FCS_NTP_EXT.1.4 Test #1.....	169
6.1.8	FCS_NTP_EXT.1.4 Test #2.....	170
6.1.9	FPT_STM_EXT.1 Test #1	171
6.1.10	FPT_STM_EXT.1 Test #2.....	171
6.1.11	FPT_STM_EXT.1 Test #3.....	172
6.1.12	FTP_ITC.1 Test #1	172
6.1.13	FTP_ITC.1 Test #2	173
6.1.14	FTP_ITC.1 Test #3	173
6.1.15	FTP_ITC.1 Test #4	173
6.2	Auth.....	174
6.2.1	FAU_STG.1 Test #1	174
6.2.2	FAU_STG.1 Test #2	175
6.2.3	FCS_CKM.1 FFC	175
6.2.4	FCS_CKM.2 RSA.....	177
6.2.5	FCS_CKM.2 DH14	177
6.2.6	FCS_CKM.2 FCC	177
6.2.7	FIA_AFL.1 Test #1	177
6.2.8	FIA_AFL.1 Test #2b.....	178
6.2.9	FIA_PMG_EXT.1 Test #1	179
6.2.10	FIA_PMG_EXT.1 Test #2.....	179
6.2.11	FIA_UIA_EXT.1 Test #1	180
6.2.12	FIA_UIA_EXT.1 Test #2.....	181
6.2.13	FIA_UIA_EXT.1 Test #3	181
6.2.14	FIA_UAU.7 Test #1	182
6.2.15	FMT_MOF.1/ManualUpdate Test #1.....	182
6.2.16	FMT_MOF.1/ManualUpdate Test #2.....	183
6.2.17	FMT_MOF.1/Functions (1) Test #1	183
6.2.18	FMT_MOF.1/Functions (1)Test #2	184
6.2.19	FMT_MOF.1/Functions (2) Test #1	184
6.2.20	FMT_MOF.1/Functions (2) Test #2	185

6.2.21	FMT_MOF.1/Services Test #1	185
6.2.22	FMT_MOF.1/Services Test #2	186
6.2.23	FMT_MTD.1/CryptoKeys Test #1	186
6.2.24	FMT_MTD.1/CryptoKeys Test #2	187
6.2.25	FMT_SMF.1 Test #1.....	187
6.2.26	FMT_SMR.2 Test #1	189
6.2.27	FTA_SSL.3 Test #1	189
6.2.28	FTA_SSL.4 Test #1	190
6.2.29	FTA_SSL.4 Test #2	190
6.2.30	FTA_SSL_EXT.1.1 Test #1	191
6.2.31	FTA_TAB.1 Test #1	191
6.2.32	FTP_TRP.1/Admin Test #1.....	192
6.2.33	FTP_TRP.1/Admin Test #2.....	192
6.3	Firewall.....	192
6.3.1	FFW_RUL_EXT.1 Test #1	192
6.3.2	FFW_RUL_EXT.1 Test #2	193
6.3.3	FFW_RUL_EXT.1.2/FFW_RUL_EXT.1.3/FFW_RUL_EXT.1.4 Test #1	194
6.3.4	FFW_RUL_EXT.1.2/FFW_RUL_EXT.1.3/FFW_RUL_EXT.1.4 Test #2	198
6.3.5	FFW_RUL_EXT.1.5 Test #1	202
6.3.6	FFW_RUL_EXT.1.5 Test #2	204
6.3.7	FFW_RUL_EXT.1.5 Test #3	204
6.3.8	FFW_RUL_EXT.1.5 Test #4	205
6.3.9	FFW_RUL_EXT.1.5 Test #5	206
6.3.10	FFW_RUL_EXT.1.5 Test #6	207
6.3.11	FFW_RUL_EXT.1.5 Test #7	209
6.3.12	FFW_RUL_EXT.1.5 Test #8	210
6.3.13	FFW_RUL_EXT.1.6 Test #1	210
6.3.14	FFW_RUL_EXT.1.6 Test #2	213
6.3.15	FFW_RUL_EXT.1.7 Test #1	214
6.3.16	FFW_RUL_EXT.1.7 Test #2	214
6.3.17	FFW_RUL_EXT.1.8 Test #1	215
6.3.18	FFW_RUL_EXT.1.8 Test #2	216
6.3.19	FFW_RUL_EXT.1.9 Test #1	218
6.3.20	FFW_RUL_EXT.1.10 Test #1	218
6.3.21	FFW_RUL_EXT.2.1 Test #1	219
6.3.22	FFW_RUL_EXT.2.1 Test #2	220
6.3.23	FFW_RUL_EXT.2.1 Test #3	221
6.4	IPsec	221
6.4.1	FCS_IPSEC_EXT.1.1 Test #1	221
6.4.2	FCS_IPSEC_EXT.1.1 Test #2	222
6.4.3	FCS_IPSEC_EXT.1.2 Test #1	224
6.4.4	FCS_IPSEC_EXT.1.3 Test #1	224

6.4.5	FCS_IPSEC_EXT.1.4 Test #1	225
6.4.6	FCS_IPSEC_EXT.1.5 Test #1	227
6.4.7	FCS_IPSEC_EXT.1.6 Test #1	228
6.4.8	FCS_IPSEC_EXT.1.7 Test #2	229
6.4.9	FCS_IPSEC_EXT.1.8 Test #1	229
6.4.10	FCS_IPSEC_EXT.1.8 Test #2	230
6.4.11	FCS_IPSEC_EXT.1.10 Test #1	230
6.4.12	FCS_IPSEC_EXT.1.11 Test #1	231
6.4.13	FCS_IPSEC_EXT.1.12 Test #1	232
6.4.14	FCS_IPSEC_EXT.1.12 Test #2	232
6.4.15	FCS_IPSEC_EXT.1.12 Test #3	233
6.4.16	FCS_IPSEC_EXT.1.12 Test #4	234
6.4.17	FCS_IPSEC_EXT.1.14 Test #2	234
6.4.18	FCS_IPSEC_EXT.1.14 Test #4	236
6.4.19	FCS_IPSEC_EXT.1.14 Test #5	236
6.4.20	FCS_IPSEC_EXT.1.14 Test #6a	237
6.4.21	FCS_IPSEC_EXT.1.14 Test #6b	237
6.5	MOD_IPS	238
6.5.1	FAU_GEN.1/IPS Test #1	238
6.5.2	FMT_SMF.1/IPS Test #1	239
6.5.3	FMT_SMF.1/IPS Test #2	239
6.5.4	FMT_SMF.1/IPS Test #3	240
6.5.5	IPS_ABD_EXT.1 Test #1	240
6.5.6	IPS_ABD_EXT.1 Test #2	242
6.5.7	IPS_IPB_EXT.1 Test #1	243
6.5.8	IPS_IPB_EXT.1 Test #2	243
6.5.9	IPS_IPB_EXT.1 Test #3	244
6.5.10	IPS_SBD_EXT.1.1 Test #1	245
6.5.11	IPS_SBD_EXT.1.1 Test #2	246
6.5.12	IPS_SBD_EXT.1.2 Test #1	246
6.5.13	IPS_SBD_EXT.1.2 Test #2	248
6.5.14	IPS_SBD_EXT.1.3 Test #1	249
6.5.15	IPS_SBD_EXT.1.4 Test #1	251
6.5.16	IPS_SBD_EXT.1.6 Test #1	252
6.6	SSHS	253
6.6.1	FCS_SSHS_EXT.1.2 Test #1	253
6.6.2	FCS_SSHS_EXT.1.2 Test #2	254
6.6.3	FCS_SSHS_EXT.1.2 Test #3	254
6.6.4	FCS_SSHS_EXT.1.2 Test #4	255
6.6.5	FCS_SSHS_EXT.1.3 Test #1	255
6.6.6	FCS_SSHS_EXT.1.4 Test #1	256
6.6.7	FCS_SSHS_EXT.1.5 Test #1	257
6.6.8	FCS_SSHS_EXT.1.5 Test #2	257
6.6.9	FCS_SSHS_EXT.1.6 Test #1	258

6.6.10	FCS_SSHS_EXT.1.6 Test #2	259
6.6.11	FCS_SSHS_EXT.1.7 Test #1	259
6.6.12	FCS_SSHS_EXT.1.7 Test #2	260
6.6.13	FCS_SSHS_EXT.1.8 Test #1t.....	261
6.6.14	FCS_SSHS_EXT.1.8 Test #1b.....	261
6.7	Update.....	262
6.7.1	FPT_TST_EXT.1 Test #1	262
6.7.2	FPT_TUD_EXT.1 Test #1	263
6.7.3	FPT_TUD_EXT.1 Test #2 (a).....	264
6.7.4	FPT_TUD_EXT.1 Test #2 (b).....	264
6.7.5	FPT_TUD_EXT.1 Test #2 (c).....	265
6.8	VPN.....	266
6.8.1	FIA_PSK_EXT.1 Test #1	266
6.8.2	FAU_GEN.1/VPN Test #1.....	266
6.8.3	FMT_SMF.1/VPN Test #1	267
6.8.4	FPF_RUL_EXT.1.1 Test #1.....	267
6.8.5	FPF_RUL_EXT.1.1 Test #2.....	268
6.8.6	FPF_RUL_EXT.1.4 Test #1.....	268
6.8.7	FPF_RUL_EXT.1.4 Test #2.....	269
6.8.8	FPF_RUL_EXT.1.5 Test #1.....	269
6.8.9	FPF_RUL_EXT.1.5 Test #2.....	270
6.8.10	FPF_RUL_EXT.1.6 Test #1.....	271
6.8.11	FPF_RUL_EXT.1.6 Test #2.....	272
6.8.12	FPF_RUL_EXT.1.6 Test #3.....	273
6.8.13	FPF_RUL_EXT.1.6 Test #4.....	274
6.8.14	FPF_RUL_EXT.1.6 Test #5.....	275
6.8.15	FPF_RUL_EXT.1.6 Test #6.....	276
6.8.16	FPF_RUL_EXT.1.6 Test #7.....	277
6.8.17	FPF_RUL_EXT.1.6 Test #8.....	278
6.8.18	FPF_RUL_EXT.1.6 Test #9.....	279
6.8.19	FPF_RUL_EXT.1.6 Test #10.....	280
6.9	X509 Rev.....	281
	FIA_X509_EXT.1.1/Rev Test #1a.....	281
	FIA_X509_EXT.1.1/Rev Test #1a(ECDsa).....	282
	FIA_X509_EXT.1.1/Rev Test #1b.....	282
	FIA_X509_EXT.1.1/Rev Test #2.....	283
	FIA_X509_EXT.1.1/Rev Test #3 CRL.....	283
	FIA_X509_EXT.1.1/Rev Test #4 CRL.....	284
	FIA_X509_EXT.1.1/Rev Test #5.....	285
	FIA_X509_EXT.1.1/Rev Test #6.....	286
	FIA_X509_EXT.1.1/Rev Test #7.....	286
	FIA_X509_EXT.1.1/Rev Test #8a.....	286
	FIA_X509_EXT.1.1/Rev Test #8b.....	287
	FIA_X509_EXT.1.1/Rev Test #8c.....	288

	FIA_X509_EXT.1.2/Rev Test #1.....	289
	FIA_X509_EXT.1.2/Rev Test #2.....	290
	FIA_X509_EXT.2 Test #1	291
	FIA_X509_EXT.3 Test #1	292
	FIA_X509_EXT.3 Test #2	292
7	Security Assurance Requirements.....	294
	7.1 ADV_FSP.1 Basic Functional Specification	294
	7.1.1 ADV_FSP.1.....	294
	7.2 AGD_OPE.1 Operational User Guidance.....	295
	7.2.1 AGD_OPE.1.....	295
	7.3 AGD_PRE.1 Preparative Procedures.....	297
	7.3.1 AGD_PRE.1	297
	7.4 ALC Assurance Activities	299
	7.4.1 ALC_CMC.1.....	299
	7.4.2 ALC_CMS.1	299
	7.5 ATE_IND.1 Independent Testing – Conformance.....	300
	7.5.1 ATE_IND.1	300
	7.6 AVA_VAN.1 Vulnerability Survey	300
	7.6.1 AVA_VAN.1.....	300
8	CAVP Mapping.....	303
9	Conclusion	306

1 TOE Overview

The TOE is the Juniper Networks, Inc. Juniper vSRX3.0 with Junos OS 22.2R2 Virtual Firewall. It is intended for deployment with service providers and large enterprises. The TOE may be operated in single mode or in cluster mode. Cluster mode is a High Availability (HA) mode in which two instances of a TOE are connected and configured to operate like a single device. This ensures high availability in the case of equipment malfunction in one of the devices.

The TOE allows definition of packet filtering policies which are enforced on all traffic traversing to, from or through it. Each packet is also subjected to stateful inspection. Further security is added by an intrusion prevention function. All traffic is monitored against signatures of known attacks and for abnormalities in traffic patterns. If potentially malicious traffic is detected, protective action is taken. Security policies are managed, and the TOE configuration controlled by Security Administrators. Management occurs via a Command Line Interface (CLI) from a local or remote management station.

The TOE is deployed as a gatekeeper between two networks so that all traffic between the two networks passes through an instance of the TOE. This ensures that all traffic between the two networks is subject to the security policies the TOE enforces. Traffic and information flows are controlled based on the rules set by TOE Administrators concerning network node addresses, protocol, type of access requested, and the service requested. The TOE implements a default deny rule, i.e. it drops any network traffic not explicitly allowed by the rules. All security relevant activities and events are audited.

Additionally, the TOE implements a multi-site Virtual Private Network (VPN) gateway functionality for tunneling traffic between itself and a VPN peer. In Cluster Mode, the link between the two instances of TOE may also be secured with IPsec. If the audit records are forwarded to an external syslog server, the connection between the TOE and the syslog server may be protected with SSH. The connection between the TOE and a remote management station is also protected by SSH.

TOE software is deployed with a hypervisor and a x86 server. The user configures the hypervisor on the selected server and installs the TOE software on the hypervisor. The software is downloaded from the Juniper web site. TOE Software is protected with a digital signature and hash values. The TOE verifies the signatures and hash values at the boot up and executes a full suite of self-tests to ensure that the TOE functions correctly and only authentic TOE software is executed.

2 Assurance Activities Identification

The Assurance Activities contained within this document include all those defined within the NDcPP 2.2e based upon the core SFRs and those implemented based on selections within the PPs/EPs.

3 Test Equivalency Justification

This analysis provides an explanation of the differences between each of the hardware models included within the TOE boundary and provides an analysis of the impact each of the differences have on the TSF functionality.

3.1 Architectural Description

The Juniper vSRX3.0 Junos OS 22.2R2 Virtual machine for HP ProLiant DL380p Gen9 & PacStar 451 TOE is a purpose-built Virtual Firewall platform. The Juniper vSRX3.0 Junos OS 22.2R2 for HP ProLiant DL380p Gen9 & PacStar 451 TOE includes two different hardware models as listed below:

- HP ProLiant DL380p Gen9 with Intel Xeon E5-2600 v4 series
- PacStar 451 with Intel Xeon E-2200M series

The TOE implements Junos Control Plane (JCP) and Packet Forwarding Engine (PFE) which constitutes the Junos data plane. JCP and PFE are executed on the virtual CPUs (vCPU) which are part of the environment of the TOE. JCP is executed on one vCPU and the PFE on at least one vCPU. The vCPU number can be increased for improved performance. The complete vSRX3.0 architecture and the TOE within it is illustrated in Figure 1.

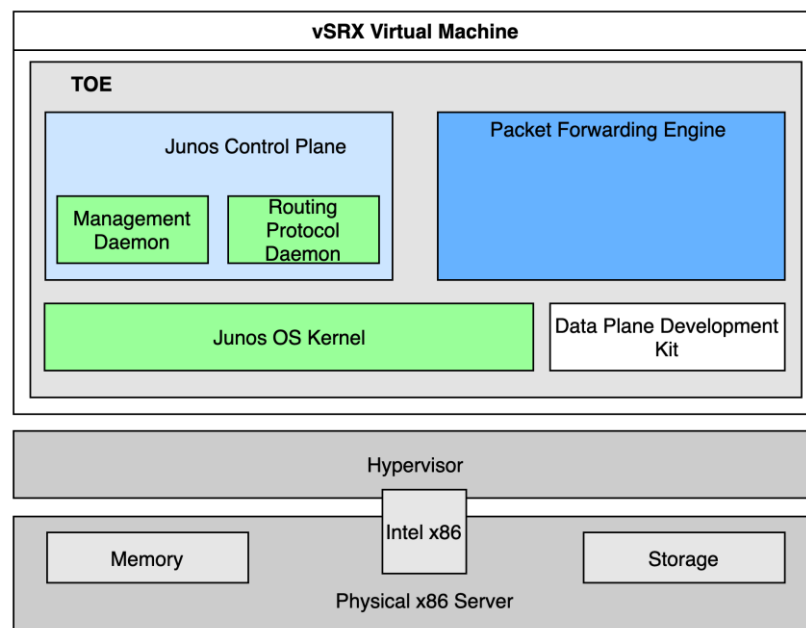


Figure 1 – vSRX3.0 Architecture

- Junos Control Plane (JCP) is the virtual Routing Engine (vRE) which implements Layer 3 routing services. It also implements all network management functions for the configuration and operation of the TOE and controls the flow of information through the TOE. Controlling the flow of information through the TOE includes Network Address Translation (NAT) and the encryption and decryption of packets for secure communication over IPsec.
- Packet Forwarding engine (PFE) implements all operations necessary for the forwarding of transit packets. That includes Flow Processing and Advanced Services.

- JCP and PFE operate independently but communicate constantly over a high-speed internal link implemented by the Junos OS. This ensures effective forwarding and routing control and the capability to run Internet-scale networks at high speeds.
- The Junos OS kernel uses the underlying hypervisor as a virtualization infrastructure to create multiple virtual machines (VMs). Only a single VM is allowed in an evaluated configuration and no additional appliances may be installed. The hypervisor is not part of the TOE and functions as a pass-through layer only.
- The TOE is configured with from three to eight virtual Network Interface Cards (vNIC). Each vNIC must be mapped to a different physical NIC. The physical server must have at least as many physical NICs as the number of vNICs configured in vSRX3.0.
- The default mode for the TOE is a single mode but it may be configured for Cluster Mode by connecting ge-0/0/1 on node 0 to ge-0/0/1 on node 1. An example of a Cluster Mode configuration is given in Figure 2. Any other configuration of the physical ports has to be removed prior to the Cluster Mode configuration. The two instances of the TOE must be in an identical configuration except for one being configured to node 0 and the other to node 1.

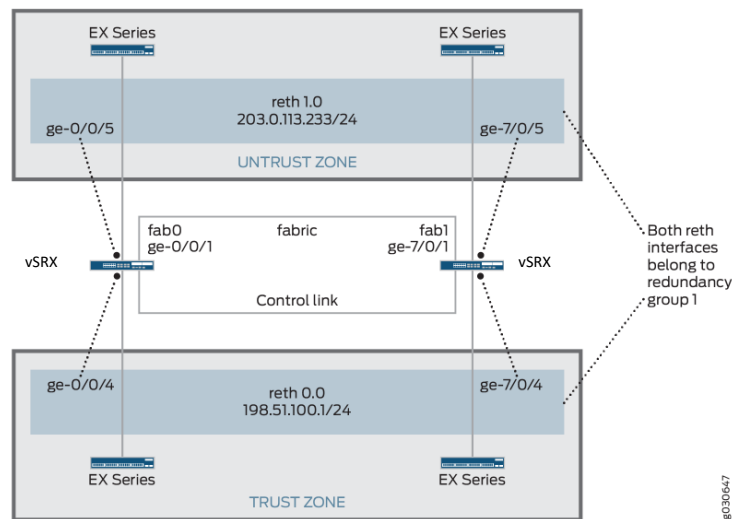


Figure 2 – Cluster Mode Configuration of the TOE

- A dedicated physical interface acts as the fxp0 interface for the HA management of the TOE. The fxp1 interface for HA control link is ge-0/0/1. Administrators may define the preferred fiber interface. Once the Administrator has defined and set up the cluster, the two devices constitute a chassis cluster have an identical cluster-id, but each has a different node ID. One of the hosts has node ID 0 and the other one node ID 1.
- Node 1 rennumbers its interfaces by adding the total number of system FPCs to the interface's original FPC number. The fabric interface remains Administrator-defined. Critical security parameters shared by the two instances of the TOE are protected by IPsec.

The appliances are physically self-contained, housing the firmware and hardware necessary to perform all switching and routing functions. The architecture components of the appliances are:

HPE ProLiant DL380 Gen9 Server

The HPE ProLiant DL380 Gen9 Server delivers the best performance and expandability in the Hewlett Packard Enterprise 2P rack portfolio. Reliability, serviceability and near continuous availability, backed by a comprehensive warranty, make it ideal for any environment. Deploy the data center standard.

SUPPORTED SOFTWARE APPLIANCES

Cybersecurity: Firewall, VPN, Network Intrusion Detection, Threat Analytics, and Network Defense

- VMware ESXi 7 Update 3 Hypervisor

Processor

- The HPE ProLiant DL380 Gen9 Server is available with Xeon processing platforms. (Intel Xeon E5-2600 v4 series)

The **Packet Forwarding Engine (PFE)** – provides all operations necessary for transit packet forwarding: HPE Embedded 1Gb Ethernet 4-port 331i Adapter, plus optional HPE FlexibleLOM or stand-up card

Power Supply

(1) HPE 500W Flex Slot Platinum Power Supply

PacStar 451

PacStar 451 is available with a wide variety of pre-loaded, pre-secured, and prequalified software applications appropriate for use in tactical communications, C4ISR/ EW, and Cyber applications. These include, but are not limited to:

- Virtualized and Software Defined Networking, Routing, Switching
- VPN, TLS Encryption, PKI
- Cybersecurity: Firewalls, IDS, Threat Analytics, SIEM, NetFlow
- Mobile Device and Wireless Network Management

The **Packet Forwarding Engine (PFE)** – provides all operations necessary for transit packet forwarding: Option for up to (5) GigE ports, (2) of which are PoE enabled

Processor

PacStar 451 is available with Xeon processing platforms.

Power Supply

- Wide range DC input (10 - 36 VDC)
- 12V DC output connector, KG-250X/XS compatible, providing ~20 watts
- Radio battery and PacStar 400-Series power snap-together Connector

SUPPORTED SOFTWARE APPLIANCES

Cybersecurity: Firewall, VPN, Network Intrusion Detection, Threat Analytics, and Network Defense

- VMware ESXi and XEN Hypervisors
- Juniper vSRX3.0 – Firewall, IDS and VPN

3.2 OS, Processor, and Firmware Analysis



The following table compares the Operating System, CPU, and firmware that runs on each of the included TOE platforms.

TOE Model	Description	Analysis
Operating System		
HP ProLiant DL380p Gen9 with Intel Xeon E5-2600 v4 series	VMWare ESXi 7 Update 3 Hypervisor	Both the TOE models includes the same VMWare ESXi 7 Update 3 Hypervisor.
PacStar 451 with Intel Xeon E-2200M series	VMWare ESXi 7 Update 3 Hypervisor	
Base CPU		
HP ProLiant DL380p Gen9 with Intel Xeon E5-2600 v4 series	Intel Xeon E5-2600 v4 series	Both the Servers are running on Xeon E series of Intel Processors but are different in architecture i.e. Intel Xeon E5-2600 v4 series is based on Broadwell architecture and Intel Xeon E-2200M series is based on Coffee Lake architecture.
PacStar 451 with Intel Xeon E-2200M series	Intel Xeon E-2200M series	

Table 1 TOE Comparison

3.3 Specification of Differences

The following tables provide a description of the physical differences between hardware models. None of the listed hardware differences have any impact of the security functionality provided by the TSF. All operate identically.

Chassis Model	Processor	Hardware Version	Network Ports	Firmware (Operating System)
HP ProLiant DL380p Gen9 	Intel Xeon E5-2600 v4 series	HP ProLiant DL380p Gen9	HPE Embedded 1Gb Ethernet 4-port 331i Adapter, plus optional HPE FlexibleLOM or stand-up card	VMWare ESXi 7 Update 3 Hypervisor
PacStar 451 	Intel Xeon E-2200M series	PacStar 451	Option for up to (5) GigE ports, (2) of which are PoE enabled	

3.4 Equivalency Analysis

The following equivalency analysis provides a per category analysis of key areas of differentiation for each hardware model to determine the minimum subset to be used in testing. The areas examined will use the areas and analysis description provided in the supporting documentation for the NDcPP. Additionally, a comparison of the data presented in section 3 is provided to identify a testing subset that will exercise each of the differences in TOE models.

3.4.1 Platform/Hardware Dependencies

The TOE boundary is inclusive of all hardware required by the TOE. The hardware platforms do not provide any of the TSF functionality. All security functionality is implemented in Platform Independent code which is line-by-line identical across hardware models. The hardware within the TOE only differs by configuration and performance, such as CPU processing speed.

Result: Both platforms are not equivalent as both have processors running on different architecture.

3.4.2 Software/OS Dependencies:

This category of differences is only applicable if the TOE is installed on an OS outside of the TOE boundary. In this case, all software including the OS is included in Junos OS and within the TOE boundary. There are no specific dependencies on the OS since the TOE will not be installed on different OSs. Furthermore, all TOE platforms include the same version of the ESXi hypervisor.

Result: All platforms are equivalent

3.4.3 Differences in Libraries Used to Provide TOE Functionality

All software binaries compiled in the TOE software are identical and have the same version numbers. There are no differences between the included libraries. Furthermore, all TOE platforms include the same version of the ESXi hypervisor.

Result: All platforms are equivalent

3.4.4 TOE Management Interface Differences

The TOE is managed via either remote CLI session or directly connected CLI. These management options are available on all hardware platforms regardless of the configuration. There is no difference in the management interface for any platform.

Result: All platforms are equivalent

3.4.5 TOE Functional Differences

Each hardware model within the TOE boundary provides identical functionality. Each device runs the same version of Junos OS software. Furthermore, all TOE platforms include the same version of the ESXi hypervisor.

Result: All platforms are equivalent

3.4.6 Difference Comparison

The following table provides a comparison of each of the categories with differences.

Model	Software	Base Processor
HP ProLiant DL380p Gen9 with Intel Xeon E5-2600 v4 series	Junos OS 22.2R2 Virtual Machine will be installed on VMWare ESXi 7 Update 3 Hypervisor.	Intel Xeon E5-2600 v4 series(Broadwell based)
PacStar 451 with Intel Xeon E-2200M series	Junos OS 22.2R2 Virtual Machine will be installed on VMWare ESXi 7 Update 3 Hypervisor.	Intel Xeon E-2200M series(Coffee Lake based)

The above table shows that the TOE hardware models are not equivalent as both are running on processors with different architecture (Broadwell | Coffee Lake).

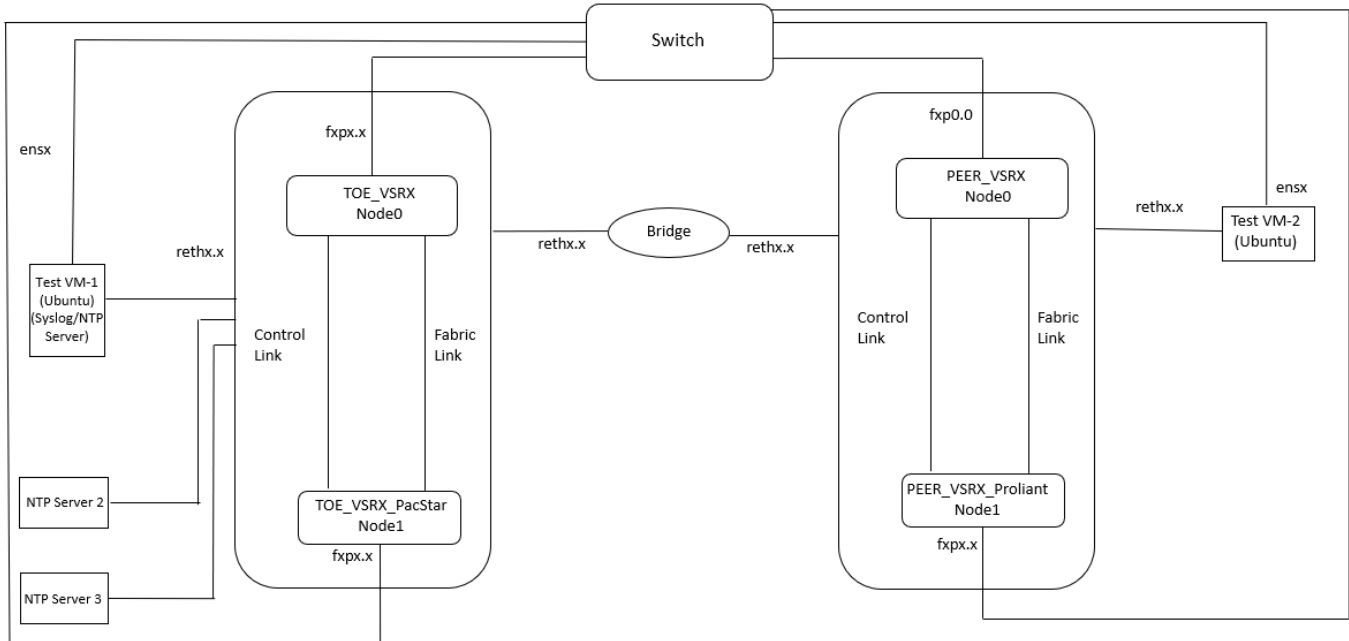
3.5 Recommendations/Conclusions

Based on the equivalency rationale listed above, testing will be performed on the following subset:

- HP ProLiant DL380p with Intel Xeon E5-2600 v4 series
- Pacstar 451 with Intel Xeon E-2200M series

4 Test Bed Descriptions

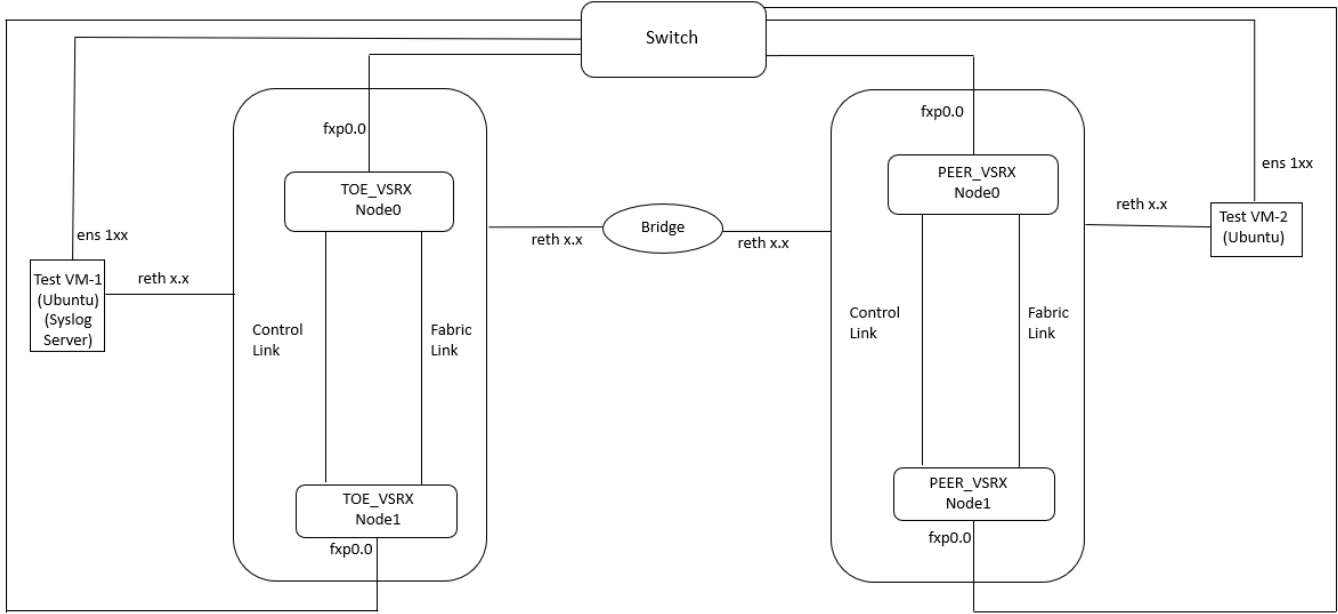
Audit



Name	OS	Version	Function	Protocols	Time	Tools (version)
TOE_VSRX	Junos	22.2R2	TOE	SSH, NTP	Manually Set and Verified	NA
Bridge (Switch)	Raspbian GNU/Linux	9	Packet Capture IPsec		Manually Set and Verified	NA
PEER_VSRX	Junos	22.2R2	PEER Device for TOE	SSH	Manually Set and Verified	NA
Audit Server\Test_VM1	Kali Linux/Ubuntu	18.04	For TOE testing and Configuration & Audit Server	SSH, NTP	Manually Set and Verified	scapy (2.3.3) tcpdump (4.9.3) OpenSSH (7.6p1) netconfd (2.10-1)

Name	OS	Version	Function	Protocols	Time	Tools (version)
Test_VM2	Kali Linux/ Ubuntu	18.04	For Peer Configuration	SSH	Manually Set and Verified	Scapy (2.3.3) Tcpdump (4.9.3) OpenSSH (7.6p1)
NTP Server 2	Ubuntu	18.04	For NTP	SSH, NTP	NTP	Scapy (2.3.3) Tcpdump (4.9.3) OpenSSH (7.6p1)
NTP Server 3	Ubuntu	18.04	For NTP	SSH, NTP	NTP	Scapy (2.3.3) Tcpdump (4.9.3) OpenSSH (7.6p1)

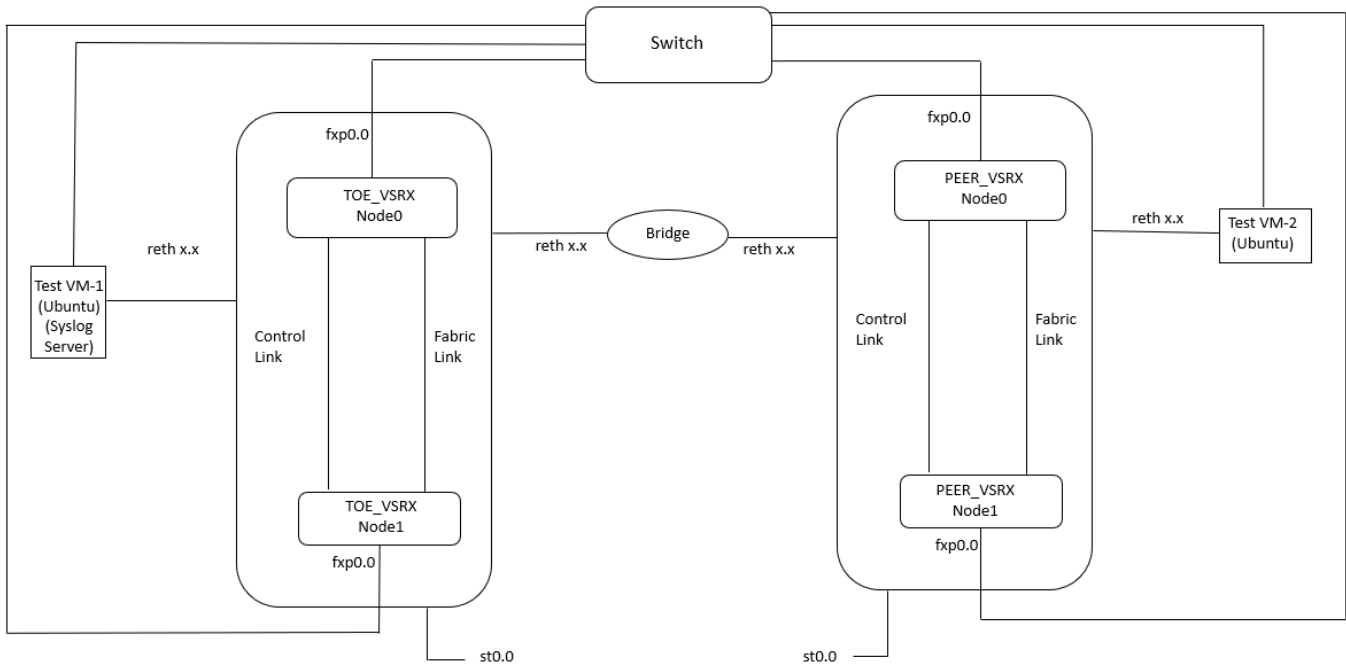
Update / SSHS / AUTH / IPS Audit



Name	OS	Version	Function	Protocols	Time	Tools (version)
TOE_VSRX	Junos	22.2R2	TOE	SSH	Manually Set and Verified	NA
Bridge	Raspbian GNU/Linux	9	To connect with TOE	SSH	Manually Set and Verified	NA
PEER_VSRX	Junos	22.2R2	PEER Device for TOE	SSH	Manually Set and Verified	NA
Test_VM1	Ubuntu	18.04 LTS	For TOE testing and Configuration & Audit Server	SSH	Manually Set and Verified	Scapy (2.4.5) Tcpdump (4.9.3) OpenSSH (7.6p1) netconfd (2.10-1) acumen-sshs

Name	OS	Version	Function	Protocols	Time	Tools (version)
Test_VM2	Ubuntu	18.04 LTS	For Peer Configuration	SSH	Manually Set and Verified	Scapy (2.4.5) Tcpdump (4.9.3) OpenSSH (7.6p1) netconfd (2.10-1) acumen-sshs

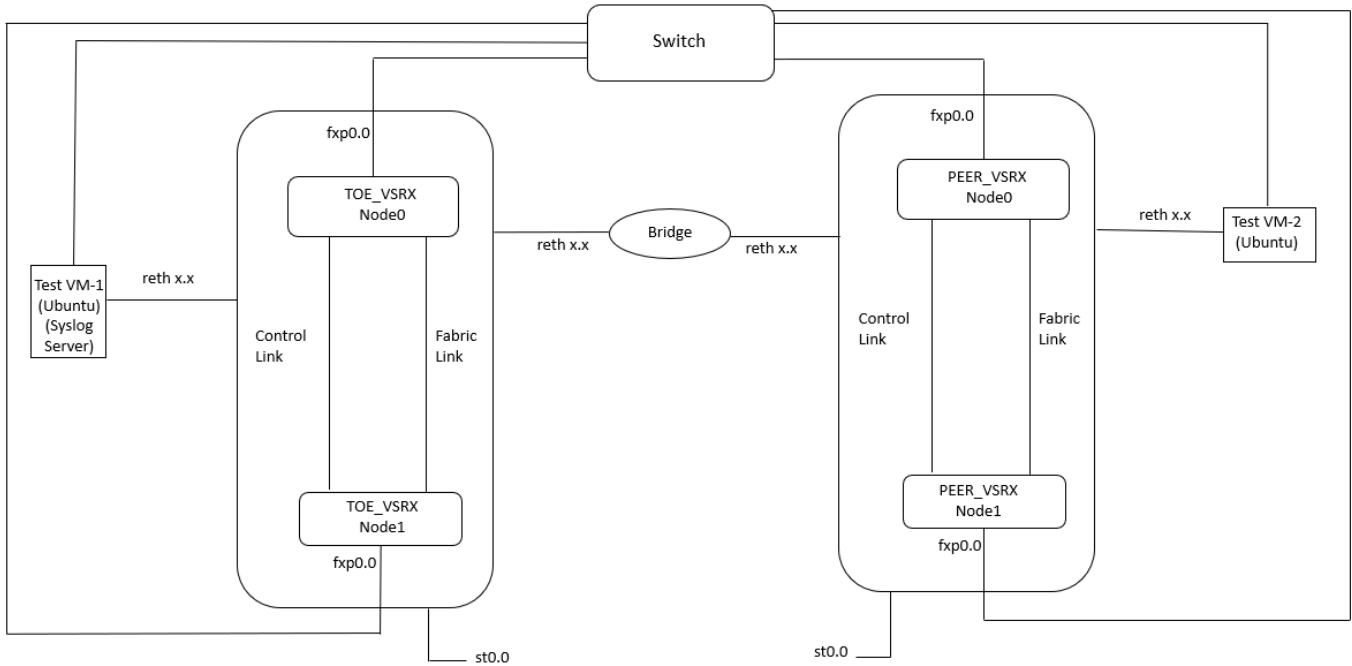
Firewall (IPV4) | IPSEC | X509 | VPN Auth



Name	OS	Version	Function	Protocols	Time	Tools (version)
TOE_VSRX	Junos	22.2R2	TOE	SSH, IPSEC	Manually Set and Verified	NA
Bridge	Raspbian GNU/Linux	11 (bullseye)	To connect with TOE	SSH	Manually Set and Verified	Tcpdump (4.99.0)

Name	OS	Version	Function	Protocols	Time	Tools (version)
PEER_VSRX	Junos	22.2R2	PEER Device for TOE	SSH, IPSEC	Manually Set and Verified	NA
Test VM-1	Ubuntu	18.04 LTS	For TOE testing and Configuration & Audit Server	SSH	Manually Set and Verified	Tcpdump (4.9.3)
Test VM-2	Ubuntu	18.04 LTS	For Peer Configuration	SSH	Manually Set and Verified	Tcpdump (4.9.3)

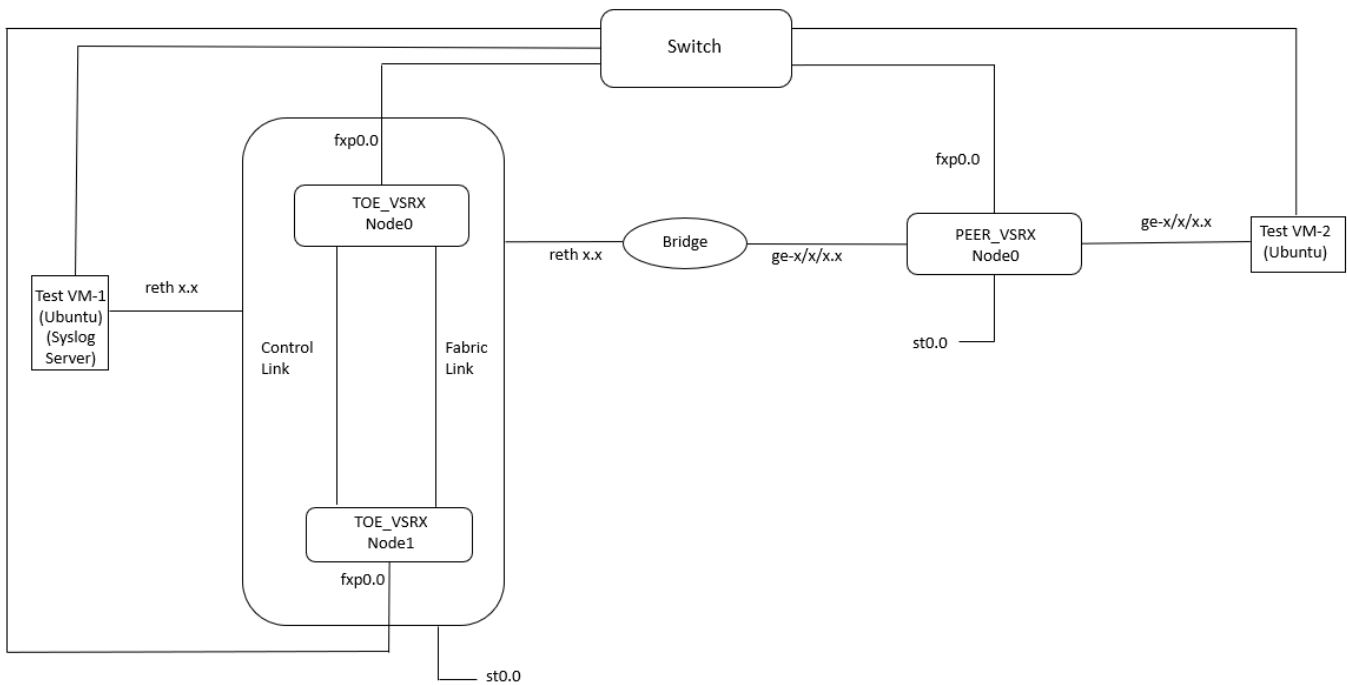
IPS Policies / Firewall(ipv6)



Name	OS	Version	Function	Protocols	Time	Tools (version)
TOE_VSRX	Junos	22.2R2	TOE	SSH	Manually Set and Verified	NA
Bridge	Raspbian GNU/Linux	9	To connect with TOE	SSH	Manually Set and Verified	NA

Name	OS	Version	Function	Protocols	Time	Tools (version)
PEER_VSRX	Junos	22.2R2	PEER Device for TOE	SSH	Manually Set and Verified	NA
Test_VM1	Ubuntu	18.04 LTS	For TOE testing and Configuration & Audit Server	SSH	Manually Set and Verified	Scapy (2.4.5) Tcpdump (4.9.3) Nmap (7.60)
Test_VM2	Ubuntu	18.04 LTS	For Peer Configuration	SSH	Manually Set and Verified	Scapy (2.4.5) Tcpdump (4.9.3)

VPN Filter



Name	OS	Version	Function	Protocols	Time	Tools (version)
TOE_VSRX	Junos	22.2R2	TOE	SSH, IPSEC	Manually Set and Verified	NA

Name	OS	Version	Function	Protocols	Time	Tools (version)
Bridge	Raspbian GNU/Linux	11 (bullseye)	To connect with TOE	SSH	Manually Set and Verified	Tcpdump (4.99.0)
PEER_VSRX	Junos	22.2R2	PEER Device for TOE	SSH, IPSEC	Manually Set and Verified	NA
Test VM-1	Ubuntu	18.04 LTS	For TOE testing and Configuration & Audit Server	SSH	Manually Set and Verified	Tcpdump (4.9.3) Scapy (2.4.5)
Test VM-2	Ubuntu	18.04 LTS	For Peer Configuration	SSH	Manually Set and Verified	Tcpdump (4.9.3) Scapy (2.4.5)

4.1 Test Time & Location

All testing was carried out at the Acumen Security offices located in 2400 Research Blvd Suite #395, Rockville, MD 20850. Testing occurred from September 2021 to September 2023.

The TOE was in a physically protected, access controlled, designated test lab with no unattended entry/exit ways. At the start of each day, the test bed was verified to ensure that it was not compromised. All evaluation documentation was always kept in a secure repository.

5 Detailed Test Cases (TSS and Guidance Activities)

5.1 TSS and Guidance Activities (Auditing)

5.1.1 FAU_GEN.1

5.1.1.1 FAU_GEN.1 TSS 1

Objective	For the administrative task of generating/import of, changing, or deleting of cryptographic keys as defined in FAU_GEN.1.1c, the TSS should identify what information is logged to identify the relevant key.
Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to determine the verdict of this assurance activity. The evaluator confirmed that within this section it identified the following information that was logged in order to identify the relevant key in relation to import/generation, changing, or deletion of cryptographic keys:</p> <ul style="list-style-type: none"> • PKID: certificate id will be recorded when generating or deleting a key pair. • IKE SPI: IP address of the initiator and responder, together with the SPI, will be recorded when generating a key pair. IP address of the initiator and responder provide the unique link to the key identifier (SPI) of the key that has been destroyed in the session termination. • SSH session keys: key reference as provided by process id. • SSH key configured for SSH public key authentication: hash of the public key used for authentication. <p>For SSH (ephemeral) session keys the PID is used as the key reference to relate the audit events on key generation and key destruction.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.1.1.2 FAU_GEN.1 Guidance 1

Objective	The evaluator shall check the guidance documentation and ensure that it provides an example of each auditable event required by FAU_GEN.1 (i.e. at least one instance of each auditable event, comprising the mandatory, optional and selection-based SFR sections as applicable, shall be provided from the actual audit record).
Evaluator Findings	<p>The evaluator examined the section titled Configuring Audit Log Options in the AGD to verify that it provides an example of each auditable event required by FAU_GEN.1. Upon investigation, the evaluator found that the AGD contains all the required information in :</p> <p>Table 6: Audit Records for all Auditable Events</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.1.1.3 FAU_GEN.1 Guidance 2

Objective	<p>The evaluator shall also make a determination of the administrative actions related to TSF data related to configuration changes. The evaluator shall examine the guidance documentation and make a determination of which administrative commands, including subcommands, scripts, and configuration files, are related to the configuration (including enabling or disabling) of the mechanisms implemented in the TOE that are necessary to enforce the requirements specified in the cPP. The evaluator shall document the methodology or approach taken while determining which actions in the administrative guide are related to TSF data related to configuration changes. The evaluator may perform this activity as part of the activities associated with ensuring that the corresponding guidance documentation satisfies the requirements related to it.</p>																										
Evaluator Findings	<p>The evaluator examined the AGD to verify that it identifies administrative commands, including subcommands, scripts, and configuration files, that are related to the configuration (including enabling or disabling) of the mechanisms implemented in the TOE that are necessary to enforce the requirements specified in the cPP. The evaluator first examined the entirety of AGD to determine what administrative commands are associated with each administrative activity. Upon investigation, the evaluator found that the following are applicable:</p> <table border="1" data-bbox="350 915 1409 1713"> <thead> <tr> <th data-bbox="350 915 571 999">Administrative Activity</th> <th data-bbox="578 915 1065 999">Method (Command/GUI Configuration)</th> <th data-bbox="1071 915 1409 999">Section</th> </tr> </thead> <tbody> <tr> <td data-bbox="350 1008 571 1083">Startup</td> <td data-bbox="578 1008 1065 1083">A series of CLI commands are provided for the configuration of audit logging</td> <td data-bbox="1071 1008 1409 1083">Configuring Audit Log Options</td> </tr> <tr> <td data-bbox="350 1092 571 1167">Shutdown</td> <td data-bbox="578 1092 1065 1167">A series of CLI commands are provided for disabling audit logging</td> <td data-bbox="1071 1092 1409 1167">Configuring Audit Log Options</td> </tr> <tr> <td data-bbox="350 1176 571 1251">Logout</td> <td data-bbox="578 1176 1065 1251">Users may terminate their sessions</td> <td data-bbox="1071 1176 1409 1251">Login and Logout Events Using SSH</td> </tr> <tr> <td data-bbox="350 1260 571 1344">Generating Keys (certificates)</td> <td data-bbox="578 1260 1065 1344">request security pki generate-key-pair certificate-id ca-ipsec</td> <td data-bbox="1071 1260 1409 1344">Configuring VPNs</td> </tr> <tr> <td data-bbox="350 1352 571 1470">Display system information</td> <td data-bbox="578 1352 1065 1470">Show version</td> <td data-bbox="1071 1352 1409 1470">How to Enable and Configure Junos OS in FIPS Mode of Operation</td> </tr> <tr> <td data-bbox="350 1478 571 1596">Creating Users</td> <td data-bbox="578 1478 1065 1596">A series of CLI commands are provided for configuring an authorized administrator</td> <td data-bbox="1071 1478 1409 1596">Configuring Administrative Credentials and Privileges</td> </tr> <tr> <td data-bbox="350 1604 571 1713">Configuring Cas</td> <td data-bbox="578 1604 1065 1713">request security pki ca-certificate load ca-profile ca-profile-ipsec filename /var/tmp/ca.cert</td> <td data-bbox="1071 1604 1409 1713">Configuring VPNs</td> </tr> </tbody> </table>			Administrative Activity	Method (Command/GUI Configuration)	Section	Startup	A series of CLI commands are provided for the configuration of audit logging	Configuring Audit Log Options	Shutdown	A series of CLI commands are provided for disabling audit logging	Configuring Audit Log Options	Logout	Users may terminate their sessions	Login and Logout Events Using SSH	Generating Keys (certificates)	request security pki generate-key-pair certificate-id ca-ipsec	Configuring VPNs	Display system information	Show version	How to Enable and Configure Junos OS in FIPS Mode of Operation	Creating Users	A series of CLI commands are provided for configuring an authorized administrator	Configuring Administrative Credentials and Privileges	Configuring Cas	request security pki ca-certificate load ca-profile ca-profile-ipsec filename /var/tmp/ca.cert	Configuring VPNs
Administrative Activity	Method (Command/GUI Configuration)	Section																									
Startup	A series of CLI commands are provided for the configuration of audit logging	Configuring Audit Log Options																									
Shutdown	A series of CLI commands are provided for disabling audit logging	Configuring Audit Log Options																									
Logout	Users may terminate their sessions	Login and Logout Events Using SSH																									
Generating Keys (certificates)	request security pki generate-key-pair certificate-id ca-ipsec	Configuring VPNs																									
Display system information	Show version	How to Enable and Configure Junos OS in FIPS Mode of Operation																									
Creating Users	A series of CLI commands are provided for configuring an authorized administrator	Configuring Administrative Credentials and Privileges																									
Configuring Cas	request security pki ca-certificate load ca-profile ca-profile-ipsec filename /var/tmp/ca.cert	Configuring VPNs																									

Configuring Revocation Servers	request security pki crl load ca-profile ca-profile-ipsec filename /var/tmp/ revoke.crl	Configuring an IPsec VPN with RSA Signature for IKE Authentication
Generating CSRs	request security pki generate-certificate-request certificate-id ms-cert subject "CN=john doe,CN=10.1.1.2,OU=sales,O=example,L=Sunnyvale,ST=CA,C=US" email user@example.net filename ms-cert-req	Configuring an IPsec VPN with RSA Signature for IKE Authentication
Performing Software Updates	system software add /<image-path>/<junos package> no-copy no-validate reboot	Installing Junos Software Packages
Setting the Time	set date YYYYMMDDHHMM.ss	Configuring the Time and Date
Configuring Admin Timeout	set system login idle-timeout minutes	Configuring the User Session Idle Timeout
Configuring the Audit Server	A series of CLI commands are provided for configuration of the Audit Server	Configuring the Remote Syslog Server
Configuring Access Banner	Set system login message login-message-banner-text	Configuring a System Login Message and Announcement
Setting Password Length	set system login password minimum-length	Configuring Administrative Credentials and Privileges
Configuring SSH	A series of CLI commands are provided for configuration for SSH	Configuring SSH on the Evaluated Configuration
Configuring IKE/IPsec	A series of CLI commands are provided for configuration for IPsec	Configuring VPN on a Device Running Junos OS
Setting firewall rules	A series of commands are provided for configuring traffic filtering rules	Configuring traffic filtering rules

Next, the evaluator examined each of the test cases and identified test cases which exercised the above referenced functionality. The audit record associated with the configuration was captured. The following table identifies the test cases in which audit records for those configurations can be found.

Administrative Activity	Method (Command/GUI Configuration)	Test Case(s)
Startup	set system login class monitor permissions trace set system login user syslog-mon class monitor authentication ssh-rsa "ssh- rsa xxxxx syslog-monitor key pair" set system services netconf ssh set system syslog file <filename> any any	FPT_STG_EXT.1 T1
Shutdown	Deleting any of the configuration items from the Startup row	FAU_STG_EXT.1 T1
Login	Via SSH or console	FTA_TAB.1 T1
Logout	exit	FTA_SSL.4 T1 and T2
Generating Keys (certificates)	Request security pki generate-key-pair	FIA_X509_EXT.1.2/Rev T1
Display system information	Show version	FPT_TUD_EXT.1 T1
Creating Users	Set system login class set system login user set system login password format sha256	FAU_STG_EXT.1 T1
Configuring CAs	request security pki ca-certificate load ca-profile ca-profile-ipsec filename /var/tmp/ca.cert	FIA_X509_EXT.1.2/Rev T1
Configuring Revocation Servers	request security pki crl load ca-profile ca-profile-ipsec filename /var/tmp/revoked.crl	FIA_X509_EXT.2 T1
Generating CSRs	request security pki generate- certificate-request certificate-id ms- cert subject "CN=john doe,CN=10.1.1.2,OU=sales,O=example, L=Sunnyvale,ST=CA,C=US" email user@example.net filename ms-cert- req	FIA_X509_EXT.3 T1
Performing Software Updates	Request system software add /<image- path/<junos package> no-copy no- validate reboot	FPT_TUD_EXT.1 T1
Setting the Time	set date YYYYMMDDHHMM.ss	FPT_STM.1 T1

	Configuring Admin Timeout	Set system login idle-timeout	FTA_SSL_EXT.1.1 T1
	Configuring the Audit Server	set system login class monitor permissions trace set system login user syslog-mon class monitor authentication ssh-rsa "ssh- rsa xxxxx syslog-monitor key pair" set system services netconf ssh set system syslog file <filename> any any	FAU_STG_EXT.1 T1
	Configuring Access Banner	Set system login message login- message-banner-text	FTA_TAB.1 T1
	Setting Password Length	Set system login password minimum length	FIA_PMG_EXT.1.1 T1
	Configuring SSH	Set system services ssh hostkey- algorithm <> set system services ssh key-exchange <> set system services ssh macs <> set system services ssh ciphers <>	FCS_SSHS_EXT.1.2 T1
	Configuring IKE/IPsec	Set security ike <> set security ipsec <> set security policies <>	FCS_IPSEC_EXT.1.1 T1
	Configuring firewall rules	A series of commands are provided for configuring traffic filtering rules	FFW_RUL_EXT.1
	Based on these findings, this assurance activity is considered satisfied.		
Verdict	Pass		

5.1.1.4 FAU_GEN.1 Guidance 3 (FWMod)

Objective	In addition to the Evaluation Activities specified in the Supporting Document for the Base-PP, the evaluator shall check the guidance documentation to ensure that it describes the audit records specified in Table 2 of the PP-Module in addition to those required by the Base-PP. If the optional SFR FFW_RUL_EXT.2 is claimed by the TOE, the evaluator shall also check the guidance documentation to ensure that it describes the relevant audit record specified in Table 3 of the PP-Module.
Evaluator Findings	The evaluator examined Table 6: Audit Records for all Auditable Events in the AGD to verify that it describes the audit records specified in Table 2 of the PP-Module in addition to those

	<p>required by the Base-PP, along with the relevant audit record specified in Table 3 of the PP-Module for the optional SFR FFW_RUL_EXT.2 .</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.1.1 FAU_GEN.1/IPS

5.1.1.1 FAU_GEN.1/IPS TSS 1

Objective	<p>The evaluator shall verify that the TSS describes how the TOE can be configured to log IPS data associated with applicable policies.</p> <p>The evaluator shall verify that the TSS describes what (similar) IPS event types the TOE will combine into a single audit record along with the conditions (e.g., thresholds and time periods) for so doing. The TSS shall also describe to what extent (if any) that may be configurable.</p> <p>For IPS_SBD_EXT.1, for each field, the evaluator shall verify that the TSS describes how the field is inspected and if logging is not applicable, any other mechanism such as counting that is deployed.</p>
Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS describes how the TOE can be configured to log IPS data associated with applicable policies. Upon investigation, the evaluator found that the TSS states that: Auditing of IPS events is different from other events given the nature of the IPS function. The following, together with the events listed in Table 10, are considered IPS auditable events:</p> <ul style="list-style-type: none"> • Start-up and shut-down of the IPS functions; • All dissimilar IPS events; • All dissimilar IPS reactions; • Totals of similar events occurring within a specified time period; and • Totals of similar reactions occurring within a specified time period. <p>For each audit log entry, the TOE stores the date and time of the event, type of event and/or reaction, and all additional data stated in Table 10.</p> <p>In addition, the evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS describes what IPS event types the TOE will combine into a single audit record along with the conditions for so doing. Upon investigation, the evaluator found that the TSS states that: IPS events often happen in bursts which generate a large volume of audit data during an attack. To manage the volume of log messages, the TOE implements log suppression. Log suppression suppresses multiple instances of the same log entry occurring from the same or similar session over a period of time. IPS log suppression is enabled by default and can</p>

	<p>be customized based on source/destination addresses, number of log occurrences after which log suppression begins, maximum number of logs that log suppression can operate on, and the time after which suppressed logs are reported.</p> <p>Suppressed logs are reported as a single log entry containing the event information and the count of occurrences.</p> <p>In addition, the evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS describes how the field is inspected and if logging is not applicable, any other mechanism such as counting that is deployed. Upon investigation, the evaluator found that the TOE logs for all applicable audit events.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.1.1.2 FAU_GEN.1/IPS Guidance

Objective	<p>The evaluator shall verify that the operational guidance describes how to configure the TOE to result in applicable IPS data logging.</p> <p>The evaluator shall verify that the operational guidance provides instructions for any configuration that may be done in regard to logging similar events (e.g., setting thresholds, defining time windows, etc.).</p>
Evaluator Findings	<p>The evaluator examined the section titled Configuring the IDP Extended Package in the AGD to verify that it describes how to configure the TOE to result in applicable IPS data logging. Upon investigation, the evaluator found that the AGD describes how to configure the TOE to result in applicable IPS data logging.</p> <p>In addition, the evaluator examined the section titled Configuring the IDP Extended Package in the AGD to verify that it provides instructions for any configuration that may be done in regard to logging similar events. Upon investigation, the evaluator found that the AGD states the Step-by-Step Procedure for logging similar events.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.1.1 FAU_GEN.1/VPN

5.1.1.1 FAU_GEN.1/VPN TSS 1

Objective	<p>The evaluator shall examine the TSS to verify that it describes the audit mechanisms that the TOE uses to generate audit records for VPN gateway behavior. If any audit mechanisms the TSF uses for this are not used to generate audit records for events defined by FAU_GEN.1 in the Base-PP, the evaluator shall ensure that any VPN gateway-specific audit mechanisms also meet the relevant functional claims from the Base-PP. For example, FAU_STG_EXT.1 requires all audit records to be transmitted to the OE over a trusted channel. This includes the audit records that are required by FAU_GEN.1/VPN. Therefore, if the TOE has an audit mechanism</p>
-----------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	that is only used for VPN gateway functionality, the evaluator shall ensure that the VPN gateway related audit records meet this requirement, even if the mechanism used to generate these audit records does not apply to any of the auditable events defined in the Base-PP.
Evaluator Findings	The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS describes the audit mechanisms that the TOE uses to generate audit records for VPN gateway behavior. Upon investigation, the evaluator found that the TSS states that: The TOE implements an audit function using syslog. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.1.2 FAU_GEN.1/VPN Guidance

Objective	The evaluator shall examine the operational guidance to verify that it identifies all security-relevant auditable events claimed in the ST and includes sample records of each event type. If the TOE uses multiple audit mechanisms to generate different sets of records, the evaluator shall verify that the operational guidance identifies the audit records that are associated with each of the mechanisms such that the source of each audit record type is clear.
Evaluator Findings	The evaluator examined Table 6: Audit Records for all Auditable Events in the AGD guidance to verify that it identifies all security-relevant auditable events claimed in the ST and includes sample records of each event type. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.2 FAU_STG.1

5.1.2.1 FAU_STG.1 TSS 1

Objective	The evaluator shall examine the TSS to ensure it describes the amount of audit data that are stored locally and how these records are protected against unauthorized modification or deletion. The evaluator shall ensure that the TSS describes the conditions that must be met for authorized deletion of audit records.
Evaluator Findings	The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS describes the amount of audit data that are stored locally, how these records are protected against unauthorized modification or deletion, and the conditions that must be met for authorized deletion of audit records. Upon investigation, the evaluator found that the TSS states that: Local audit logs are stored in /var/log/ in the TOE filesystem. Only successfully authenticated Security Administrator can read log files or delete log and archive files. Access is through the CLI interface or direct access to the filesystem.

	<p>The syslogs are automatically deleted locally according to configurable limits on storage volume. The default maximum size is 1Gb. The default maximum size can be modified using the set system syslog CLI command with the size argument.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.1.2.2 FAU_STG.1 Guidance

Objective	The evaluator shall examine the guidance documentation to determine that it describes any configuration required for protection of the locally stored audit data against unauthorized modification or deletion.
Evaluator Findings	The evaluator examined the section titled " Configuring Audit Log Options " and " Configuring Administrative Credentials and Privileges " in the AGD to verify that it describes any configuration required for protection of the locally stored audit data against unauthorized modification or deletion. Upon investigation, the evaluator found that the AGD specifies the CLI commands for configuration of audit data, and also specifies how to configure Administrator account which will be used to configure the Audit log options. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.3 FAU_STG_EXT.1

5.1.3.1 FAU_STG_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS to ensure it describes the means by which the audit data are transferred to the external audit server, and how the trusted channel is provided.
Evaluator Findings	The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS describes the means by which the audit data are transferred to the external audit server, and how the trusted channel is provided. Upon investigation, the evaluator found that the TSS states that: <p>Syslog can be configured to store the audit logs locally or to send them to one or more syslog log servers in real time via Netconf over SSH.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.1.3.2 FAU_STG_EXT.1 TSS 2

Objective	The evaluator shall examine the TSS to ensure it describes the amount of audit data that are stored locally; what happens when the local audit data store is full; and how these records are protected against unauthorized access.
Evaluator Findings	The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS describes the amount of audit data that are stored locally; what

	<p>happens when the local audit data store is full; and how these records are protected against unauthorized access. Upon investigation, the evaluator found that the TSS states that: The locally stored syslog files are automatically deleted according to configurable limits on storage volume. The default maximum size is 1Gb, but the size can be modified by the set system syslog CLI command.</p> <p>Only a Security Administrator can read, delete or archive log files through the CLI or through direct access to the filesystem.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.1.3.3 FAU_STG_EXT.1 TSS 3

Objective	<p>The evaluator shall examine the TSS to ensure it describes whether the TOE is a standalone TOE that stores audit data locally or a distributed TOE that stores audit data locally on each TOE component or a distributed TOE that contains TOE components that cannot store audit data locally on themselves but need to transfer audit data to other TOE components that can store audit data locally. The evaluator shall examine the TSS to ensure that for distributed TOEs it contains a list of TOE components that store audit data locally. The evaluator shall examine the TSS to ensure that for distributed TOEs that contain components which do not store audit data locally but transmit their generated audit data to other components it contains a mapping between the transmitting and storing TOE components.</p>
Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS describes whether the TOE is a standalone TOE that stores audit data locally or a distributed TOE that stores audit data locally on each TOE component or a distributed TOE that contains TOE components that cannot store audit data locally on themselves but need to transfer audit data to other TOE components that can store audit data locally. Upon investigation, the evaluator found that the TSS states that :</p> <p>Local audit logs are stored in /var/log/ in the TOE filesystem. The TOE is a standalone device.</p> <p>Since the TOE is not distributed, the latter parts of the TSS activity are not applicable.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.1.3.4 FAU_STG_EXT.1 TSS 4

Objective	<p>The evaluator shall examine the TSS to ensure that it details the behaviour of the TOE when the storage space for audit data is full. When the option 'overwrite previous audit record' is selected this description should include an outline of the rule for overwriting audit data. If 'other actions' are chosen such as sending the new audit data to an external IT entity, then the related behaviour of the TOE shall also be detailed in the TSS.</p>
-----------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS details the behavior of the TOE when the storage space for audit data is full. Upon investigation, the evaluator found that the TSS states that:</p> <p>The locally stored syslog files are automatically deleted according to configurable limits on storage volume. The default maximum size is 1Gb, but the size can be modified by the set system syslog CLI command.</p> <p>The TOE maintains an active log file and a number of archive files. The default number of archive files is 10 but the number is configurable to any value between 1 and 1000. When the active log file reaches its maximum size, the logging function closes the file, compresses it, and names the compressed file 'logfile.0.gz'. The TOE then opens and writes to a new active log file. When the new active log file reaches the configured maximum size, 'logfile.0.gz' is renamed 'logfile.1.gz', and the active log file is closed, compressed, and named 'logfile.0.gz'. If the maximum number of archive files is reached and the size of the active file reaches the maximum size, the oldest archive file is deleted so the current active file can be archived.</p> <p>If the administrator does not free the storage in time and the /var filesystem storage becomes exhausted a final entry is recorded in the log reporting "No space left on device" and logging is terminated. The TOE will continue to operate but audit log generation will fail.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.1.3.5 FAU_STG_EXT.1 TSS 5

Objective	<p>The evaluator shall examine the TSS to ensure that it details whether the transmission of audit information to an external IT entity can be done in realtime or periodically. In case the TOE does not perform transmission in realtime the evaluator needs to verify that the TSS provides details about what event stimulates the transmission to be made as well as the possible acceptable frequency for the transfer of audit data.</p>
Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS details whether the transmission of audit information to an external IT entity can be done in realtime or periodically. Upon investigation, the evaluator found that the TSS states that :</p> <p>Syslog can be configured to store the audit logs locally or to send them to one or more syslog log servers in real time via Netconf over SSH.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.1.3.6 FAU_STG_EXT.1 Guidance 1

Objective	The evaluator shall also examine the guidance documentation to ensure it describes how to establish the trusted channel to the audit server, as well as describe any requirements on the audit server (particular audit server protocol, version of the protocol required, etc.), as well as configuration of the TOE needed to communicate with the audit server.
Evaluator Findings	<p>The evaluator examined the section titled Configuring the Remote Syslog Server in the AGD to verify that it describes how to establish the trusted channel to the audit server, as well as describe any requirements on the audit server (particular audit server protocol, version of the protocol required, etc.), as well as configuration of the TOE needed to communicate with the audit server.</p> <p>Upon investigation, the evaluator found that to establish the trusted channel to the audit server the AGD states that:</p> <p>Configure the export of audit information to a secure, remote server by setting up an event trace monitor that sends event log messages by using NETCONF over SSH to the remote system event logging server. The following procedures show the configuration needed to send system log messages to a secure external server by using NETCONF over SSH.</p> <p>Upon further investigation, the evaluator found that for: any requirements on the audit server (particular audit server protocol, version of the protocol required, etc.), as well as configuration of the TOE needed to communicate with the audit server.</p> <p>The AGD states that:</p> <p>A secure Junos OS environment requires auditing of events and storing them in a local audit file. The recorded events are simultaneously sent to an external syslog server. A syslog server receives the syslog messages streamed from the device. The syslog server must have an SSH client with NETCONF support configured to receive the streamed syslog messages.</p> <p>the Linux-based syslog server must be configured with the IP address and gateway, and the StrongSwan IPsec client must be installed on the syslog server to initiate a VPN connection with the Junos OS device.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.1.3.7 FAU_STG_EXT.1 Guidance 2

Objective	The evaluator shall also examine the guidance documentation to determine that it describes the relationship between the local audit data and the audit data that are sent to the audit log server. For example, when an audit event is generated, is it simultaneously sent to the external server and the local store, or is the local store used as a buffer and “cleared” periodically by sending the data to the audit server.
-----------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Evaluator Findings	<p>The evaluator examined the section titled Configuring the Remote Syslog Server in the AGD to verify that it describes the relationship between the local audit data and the audit data that are sent to the audit log server. Upon investigation, the evaluator found that the AGD states that :</p> <p>A secure Junos OS environment requires auditing of events and storing them in a local audit file. The recorded events are simultaneously sent to an external syslog server. A syslog server receives the syslog messages streamed from the device.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.1.3.8 FAU_STG_EXT.1 Guidance 3

Objective	The evaluator shall also ensure that the guidance documentation describes all possible configuration options for FAU_STG_EXT.1.3 and the resulting behavior of the TOE for each possible configuration. The description of possible configuration options and resulting behavior shall correspond to those described in the TSS.
Evaluator Findings	<p>The evaluator examined the section titled Configuring Audit Log Options in the AGD to verify that it describes all possible configuration options for FAU_STG_EXT.1.3 and the resulting behavior of the TOE for each possible configuration. Upon investigation, the evaluator found that the AGD describes how to specify the number of files to be archived, the file in which to log data, the size of the files to be archived, and the system message format.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.2 TSS and Guidance Activities (Cryptographic Support)

Note that Test activities in the SD that are typically addressed by referencing CAVP certs are addressed in this section and are identified as “Test/CAVP” activities.

5.2.1 FCS_CKM.1

5.2.1.1 FCS_CKM.1 TSS 1

Objective	The evaluator shall ensure that the TSS identifies the key sizes supported by the TOE. If the ST specifies more than one scheme, the evaluator shall examine the TSS to verify that it identifies the usage for each scheme.
Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS identifies the key sizes supported by the TOE. Upon investigation, the evaluator found that the TSS states that:</p> <p>The TOE’s cryptographic module generates asymmetric keys. The asymmetric keys produced are:</p> <ul style="list-style-type: none"> • RSA 2048, 4096 bit • ECC (P-256, P-384, P-521)

	<ul style="list-style-type: none"> • DH group 14 (2048 bits) <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.2.1.2 FCS_CKM.1 Guidance 1

Objective	The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the selected key generation scheme(s) and key size(s) for all cryptographic protocols defined in the Security Target.
Evaluator Findings	<p>The evaluator examined the section titled Configuring Event Logging to a Remote Server when Initiating the Connection from the Remote Server and Configuring an IPsec VPN with an RSA Signature for IKE Authentication in the AGD to verify that it instructs the administrator how to configure the TOE to use the selected key generation scheme(s) and key size(s) for all cryptographic protocols defined in the Security Target. Upon investigation, the evaluator found that the AGD states the CLI commands for configuring the appropriate key generation scheme and key size on the TOE.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.2.1.3 FCS_CKM.1 Test/CAVP 1

Objective	The evaluator shall verify the key generation mechanisms supported by the TOE.
Evaluator Findings	<p>CAVP Certs: #A3342 covers the following key generation mechanisms:</p> <p>RSA schemes</p> <p>ECC schemes</p> <p>For the FFC schemes using “safe-prime”, a known good implementation test was performed and documented in Section 6.2.3 below.</p> <p>For additional details please refer to CAVP Mapping in Section 8 of this document.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.2.2 FCS_CKM.1.1/IKE

5.2.2.1 FCS_CKM.1.1/IKE TSS 1

Objective	<p>The evaluator shall check to ensure that the TSS describes how the key-pairs are generated. In order to show that the TSF implementation complies with FIPS PUB 186-4, the evaluator shall ensure that the TSS contains the following information:</p> <ul style="list-style-type: none"> • The TSS shall list all sections of Appendix B to which the TOE complies
-----------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	<ul style="list-style-type: none"> For each applicable section listed in the TSS, for all statements that are not "shall" (that is, "shall not," "should," and "should not"), if the TOE implements such options it shall be described in the TSS. If the included functionality is indicated as "shall not" or "should not" in the standard, the TSS shall provide a rationale for why this will not adversely affect the security policy implemented by the TOE For each applicable section of Appendix B, any omission of functionality related to "shall" or "should" statements shall be described <p>Any TOE-specific extensions, processing that is not included in the Appendices, or alternative Implementations allowed by the Appendices that may impact the security requirements the TOE is to enforce shall be described.</p>
Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS describes how the key-pairs are generated. Upon investigation, the evaluator found that the TSS states that:</p> <p>Asymmetric keys are generated in accordance with FIPS PUB 186-4 for IKE with IPsec. The TOE implements all of the "shall" and "should" requirements and none of the "shall not" or "should not" from FIPS PUB 186-4 Appendix B.3.3 and B.4.2.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.2.2.2 FCS_CKM.1.1/IKE Guidance 1

Objective	The evaluator shall check that the operational guidance describes how the key generation functionality is invoked, and describes the inputs and outputs associated with the process for each signature scheme supported. The evaluator shall also check that guidance is provided regarding the format and location of the output of the key generation process.								
Evaluator Findings	<p>The evaluator examined the section titled Configuring VPNs in the AGD to verify that it describes how the key generation functionality is invoked, and describes the inputs and outputs associated with the process for each signature scheme supported. Upon investigation, the evaluator found that the AGD states the CLI commands for invoking the key generation functionality which includes the inputs and outputs associated with the same.</p> <p>The evaluator examined the section titled Configuring Roles and Authentication Methods in the AGD to verify that it describes the format and location of the output of the key generation process. Upon investigation, the evaluator found that the Table 5 of the AGD states that :</p> <p>Table 5 – Storage and Destruction of Cryptographic Keys</p> <table border="1"> <thead> <tr> <th>Keys/CSPs</th> <th>Purpose</th> <th>Storage Location</th> <th>Method of Zeroization</th> </tr> </thead> <tbody> <tr> <td>SSH Private Host Key</td> <td>Generated with the random number generator when the SSH is first set up. Used to identify the host.</td> <td>Plaintext on the virtual disk.</td> <td>When the TOE is recommissioned, the config files (including CSP files) are removed using the Linux <code>shred</code></td> </tr> </tbody> </table>	Keys/CSPs	Purpose	Storage Location	Method of Zeroization	SSH Private Host Key	Generated with the random number generator when the SSH is first set up. Used to identify the host.	Plaintext on the virtual disk.	When the TOE is recommissioned, the config files (including CSP files) are removed using the Linux <code>shred</code>
Keys/CSPs	Purpose	Storage Location	Method of Zeroization						
SSH Private Host Key	Generated with the random number generator when the SSH is first set up. Used to identify the host.	Plaintext on the virtual disk.	When the TOE is recommissioned, the config files (including CSP files) are removed using the Linux <code>shred</code>						

		ecdsa-sha2-nistp256 (ECDSA P-256, ECDSA P-384, ECDSA P-521) and/or ssh-rsa (RSA 2048)		command to wipe the persistent storage media.
	SSH Private Host Key	Loaded into memory to complete session establishment	Plaintext in volatile memory.	The TOE calls <code>bzero()</code> at session termination. The hypervisor erases the released memory before it is placed in the free pool.
	SSH Session Key	Session keys used with SSH, AES 128, 256, hmac-sha-1, hmac-sha2-256 or hmac-sha2-512 key (160, 256 or 512), DH Private Key (2048 or elliptic curve 256/384/521-bits)	Plaintext in volatile memory	The TOE calls <code>bzero()</code> at session termination. The hypervisor erases the released memory before it is placed in the free pool.
	RNG state	Internal state and seed key of the RNG	Plaintext in volatile memory	Handled by kernel, overwritten with zeros at reboot.
	IKE Private Host Key	Private authentication key used in IKE. RSA 2048, ECDSA P-256, ECDSA P-384	Plaintext in virtual disc or in flash memory.	Erased by the Administrator issuing <code>clear security IKE security-association</code> command or zeroized at rebooting the TOE. Private keys stored in flash are not zeroized unless an explicit <code>request system zeroize</code> command is executed.
	IKE-SKEYID	IKE master secret used to derive IKE and IPsec ESP session keys	Plaintext in volatile memory	Erased by the Administrator issuing <code>clear security IKE security-association</code> command or zeroized at rebooting the TOE.
	IKE Session Key	IKE Session keys. AES, HMAC.	Plaintext in volatile memory	Erased by the Administrator issuing <code>clear security IKE security-association</code> command or zeroized at rebooting the TOE.

	ESP Session Key	ESP Session Keys. AES, HMAC.	Plaintext in volatile memory	Erased by the Administrator issuing <code>clear security ipsec security-association</code> command or zeroized at rebooting the TOE.
	IKE-DH Private Exponent	Ephemeral DH private exponent used in IKE. DH N = 224 bit, ECDH P-256, or ECDH P-384	Plaintext in volatile memory.	Erased by the Administrator issuing <code>clear security IKE security-association</code> command or zeroized at rebooting the TOE.
	IKE-PSK	Pre-shared authentication key used in IKE	Hashed in virtual disc or flash memory.	Erased by Administrator issuing a <code>clear security IKE security-association</code> command or zeroized at rebooting the TOE. Keys stored in flash are not zeroized unless an Administrator issues a <code>request system zeroize</code> command.
	ecdh private keys	Loaded into memory to complete key exchange in session establishment	Plaintext in volatile memory.	The TOE calls <code>bzero()</code> at session termination. The hypervisor erases the released memory before it is placed in the free pool.
	Based on these findings, this assurance activity is considered satisfied.			
Verdict	Pass			

5.2.2.3 FCS_CKM.1/IKE Test/CAVP 1

Objective	The evaluator shall verify the key generation mechanisms supported by the TOE.
Evaluator Findings	CAVP Certs: # A3342 For additional details please refer to CAVP Mapping in Section 8 of this document. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.3 FCS_CKM.2

5.2.3.1 FCS_CKM.2 TSS 1 [TD0580]

Objective	The evaluator shall ensure that the supported key establishment schemes correspond to the key generation schemes identified in FCS_CKM.1.1. If the ST specifies more than one scheme, the evaluator shall examine the TSS to verify that it identifies the usage for each scheme. It is sufficient to provide the scheme, SFR, and service in the TSS.
Evaluator Findings	The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS supported key establishment schemes correspond to the key generation schemes identified in FCS_CKM.1.1. Upon investigation, the evaluator found that the TSS states that: The TOE implements Diffie-Hellman group 14 key establishment using the modulus and generator specified in Section 3 of RFC3526. Asymmetric key pair are established in accordance with Section 5.6 of NIST SP 800-56A. Usage of key agreement in protocols is specified in Table 13 of ST document. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.3.2 FCS_CKM.2 Guidance 1

Objective	The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the selected key establishment scheme(s).
Evaluator Findings	The evaluator examined the section titled Configuring SSH on the Evaluated Configuration in the AGD to verify that it instructs the administrator how to configure the TOE to use the selected key establishment scheme(s). Upon investigation, the evaluator found that the AGD states the CLI commands needed to configure the appropriate key establishment scheme on the TOE. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.3.3 FCS_CKM.2 Test/CAVP 1

Objective	The evaluator shall verify the key establishment mechanisms supported by the TOE.
Evaluator Findings	CAVP Certs: # A3342 covers the following key establishment mechanisms: ECC schemes For the FFC schemes using “safe-primes”, a known good implementation test was performed and documented in Section 6.2.6 below. For additional details please refer to CAVP Mapping in Section 8 of this document. Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass
---------	------

5.2.4 FCS_CKM.4

5.2.4.1 FCS_CKM.4 TSS 1

Objective	The evaluator examines the TSS to ensure it lists all relevant keys (describing the origin and storage location of each), all relevant key destruction situations (e.g. factory reset or device wipe function, disconnection of trusted channels, key change as part of a secure channel protocol), and the destruction method used in each case. For the purpose of this Evaluation Activity the relevant keys are those keys that are relied upon to support any of the SFRs in the Security Target. The evaluator confirms that the description of keys and storage locations is consistent with the functions carried out by the TOE (e.g. that all keys for the TOE-specific secure channels and protocols, or that support FPT_APW.EXT.1 and FPT_SKP_EXT.1, are accounted for ²). In particular, if a TOE claims not to store plaintext keys in non-volatile memory then the evaluator checks that this is consistent with the operation of the TOE.																
Evaluator Findings	<p>The evaluator examined the section titled Cryptographic Key Destruction in the Security Target to verify that the TSS lists all relevant keys (describing the origin and storage location of each), all relevant key destruction situations (e.g. factory reset or device wipe function, disconnection of trusted channels, key change as part of a secure channel protocol), and the destruction method used in each case that the TSS description of keys and storage locations is consistent with the functions carried out by the TOE. Upon investigation, the evaluator found that the table 16 of the ST tabulates that:</p> <p>Table 2 – Storage and Destruction of Cryptographic Keys</p> <table border="1"> <thead> <tr> <th>Keys/CSPs</th> <th>Purpose</th> <th>Storage Location</th> <th>Method of Zeroization</th> </tr> </thead> <tbody> <tr> <td>SSH Private Host Key</td> <td>Generated with the random number generator when the SSH is first set up. Used to identify the host. ecdsa-sha2-nistp256 (ECDSA P-256, ECDSA P-384, ECDSA P-521) and/or ssh-rsa (RSA 2048)</td> <td>Plaintext on the virtual disk.</td> <td>When the TOE is recommissioned, the config files (including CSP files) are removed using the Linux <code>shred</code> command to wipe the persistent storage media.</td> </tr> <tr> <td>SSH Private Host Key</td> <td>Loaded into memory to complete session establishment</td> <td>Plaintext in volatile memory.</td> <td>The TOE calls <code>bzero()</code> at session termination. The hypervisor erases the released memory before it is placed in the free pool.</td> </tr> <tr> <td>SSH Session Key</td> <td>Session keys used with SSH, AES 128, 256, hmac-sha-1, hmac-sha2-256 or hmac-sha2-512 key (160, 256 or 512), DH Private Key</td> <td>Plaintext in volatile memory</td> <td>The TOE calls <code>bzero()</code> at session termination. The hypervisor erases the released memory before it is placed in the free pool.</td> </tr> </tbody> </table>	Keys/CSPs	Purpose	Storage Location	Method of Zeroization	SSH Private Host Key	Generated with the random number generator when the SSH is first set up. Used to identify the host. ecdsa-sha2-nistp256 (ECDSA P-256, ECDSA P-384, ECDSA P-521) and/or ssh-rsa (RSA 2048)	Plaintext on the virtual disk.	When the TOE is recommissioned, the config files (including CSP files) are removed using the Linux <code>shred</code> command to wipe the persistent storage media.	SSH Private Host Key	Loaded into memory to complete session establishment	Plaintext in volatile memory.	The TOE calls <code>bzero()</code> at session termination. The hypervisor erases the released memory before it is placed in the free pool.	SSH Session Key	Session keys used with SSH, AES 128, 256, hmac-sha-1, hmac-sha2-256 or hmac-sha2-512 key (160, 256 or 512), DH Private Key	Plaintext in volatile memory	The TOE calls <code>bzero()</code> at session termination. The hypervisor erases the released memory before it is placed in the free pool.
Keys/CSPs	Purpose	Storage Location	Method of Zeroization														
SSH Private Host Key	Generated with the random number generator when the SSH is first set up. Used to identify the host. ecdsa-sha2-nistp256 (ECDSA P-256, ECDSA P-384, ECDSA P-521) and/or ssh-rsa (RSA 2048)	Plaintext on the virtual disk.	When the TOE is recommissioned, the config files (including CSP files) are removed using the Linux <code>shred</code> command to wipe the persistent storage media.														
SSH Private Host Key	Loaded into memory to complete session establishment	Plaintext in volatile memory.	The TOE calls <code>bzero()</code> at session termination. The hypervisor erases the released memory before it is placed in the free pool.														
SSH Session Key	Session keys used with SSH, AES 128, 256, hmac-sha-1, hmac-sha2-256 or hmac-sha2-512 key (160, 256 or 512), DH Private Key	Plaintext in volatile memory	The TOE calls <code>bzero()</code> at session termination. The hypervisor erases the released memory before it is placed in the free pool.														

		(2048 or elliptic curve 256/384/521-bits)		
	RNG state	Internal state and seed key of the RNG	Plaintext in volatile memory	Handled by kernel, overwritten with zeros at reboot.
	IKE Private Host Key	Private authentication key used in IKE. RSA 2048, ECDSA P-256, ECDSA P-384	Plaintext in virtual disc or in flash memory.	Erased by the Administrator issuing <code>clear security IKE security-association</code> command or zeroized at rebooting the TOE. Private keys stored in flash are not zeroized unless an explicit request <code>system zeroize</code> command is executed.
	IKE-SKEYID	IKE master secret used to derive IKE and IPsec ESP session keys	Plaintext in volatile memory	Erased by the Administrator issuing <code>clear security IKE security-association</code> command or zeroized at rebooting the TOE.
	IKE Session Key	IKE Session keys. AES, HMAC.	Plaintext in volatile memory	Erased by the Administrator issuing <code>clear security IKE security-association</code> command or zeroized at rebooting the TOE.
	ESP Session Key	ESP Session Keys. AES, HMAC.	Plaintext in volatile memory	Erased by the Administrator issuing <code>clear security ipsec security-association</code> command or zeroized at rebooting the TOE.
	IKE-DH Private Exponent	Ephemeral DH private exponent used in IKE. DH N = 224 bit, ECDH P-256, or ECDH P-384	Plaintext in volatile memory.	Erased by the Administrator issuing <code>clear security IKE security-association</code> command or zeroized at rebooting the TOE.

	IKE-PSK	Pre-shared authentication key used in IKE	Hashed in virtual disc or flash memory.	Erased by Administrator issuing a <code>clear security IKE security-association</code> command or zeroized at rebooting the TOE. Keys stored in flash are not zeroized unless an Administrator issues a <code>request system zeroize</code> command.
	ecdh private keys	Loaded into memory to complete key exchange in session establishment	Plaintext in volatile memory.	The TOE calls <code>bzero()</code> at session termination. The hypervisor erases the released memory before it is placed in the free pool.
	Based on these findings, this assurance activity is considered satisfied.			
Verdict	Pass			

5.2.4.2 FCS_CKM.4 TSS 2

Objective	The evaluator shall check to ensure the TSS identifies how the TOE destroys keys stored as plaintext in non-volatile memory, and that the description includes identification and description of the interfaces that the TOE uses to destroy keys (e.g., file system APIs, key store APIs).
Evaluator Findings	The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS identifies how the TOE destroys keys stored as plaintext in non-volatile memory, and that the description includes identification and description of the interfaces that the TOE uses to destroy keys. Upon investigation, the evaluator found that table 16 of the ST along with the TSS states that : Cryptographic keys the TOE uses are enumerated and their methods of storage and destruction are given in Table 2. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.4.3 FCS_CKM.4 TSS 3

Objective	Where the TSS identifies keys that are stored in a non-plaintext form, the evaluator shall check that the TSS identifies the encryption method and the key-encrypting-key used, and that the key-encrypting-key is either itself stored in an encrypted form or that it is destroyed by a method included under FCS_CKM.4.
-----------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<p>Evaluator Findings</p>	<p>The evaluator examined the section titled Cryptographic Key Destruction in the Security Target to verify that the TSS identifies the encryption method and the key-encrypting-key used, and that the key-encrypting-key is either itself stored in an encrypted form or that it is destroyed by a method included under FCS_CKM.4. Upon investigation, the evaluator found that the table 16 of the ST along with TSS states that:</p> <p>The table below describes the key zeroization provided by the TOE and as referenced in FCS_CKM.4.</p> <p>Table 3 – Storage and Destruction of Cryptographic Keys</p> <table border="1" data-bbox="347 558 1471 1789"> <thead> <tr> <th data-bbox="347 558 570 611">Keys/CSPs</th> <th data-bbox="570 558 906 611">Purpose</th> <th data-bbox="906 558 1138 611">Storage Location</th> <th data-bbox="1138 558 1471 611">Method of Zeroization</th> </tr> </thead> <tbody> <tr> <td data-bbox="347 611 570 989">SSH Private Host Key</td> <td data-bbox="570 611 906 989">Generated with the random number generator when the SSH is first set up. Used to identify the host. ecdsa-sha2-nistp256 (ECDSA P-256, ECDSA P-384, ECDSA P-521) and/or ssh-rsa (RSA 2048)</td> <td data-bbox="906 611 1138 989">Plaintext on the virtual disk.</td> <td data-bbox="1138 611 1471 989">When the TOE is recommissioned, the config files (including CSP files) are removed using the Linux <code>shred</code> command to wipe the persistent storage media.</td> </tr> <tr> <td data-bbox="347 989 570 1251">SSH Private Host Key</td> <td data-bbox="570 989 906 1251">Loaded into memory to complete session establishment</td> <td data-bbox="906 989 1138 1251">Plaintext in volatile memory.</td> <td data-bbox="1138 989 1471 1251">The TOE calls <code>bzero()</code> at session termination. The hypervisor erases the released memory before it is placed in the free pool.</td> </tr> <tr> <td data-bbox="347 1251 570 1551">SSH Session Key</td> <td data-bbox="570 1251 906 1551">Session keys used with SSH, AES 128, 256, hmac-sha-1, hmac-sha2-256 or hmac-sha2-512 key (160, 256 or 512), DH Private Key (2048 or elliptic curve 256/384/521-bits)</td> <td data-bbox="906 1251 1138 1551">Plaintext in volatile memory</td> <td data-bbox="1138 1251 1471 1551">The TOE calls <code>bzero()</code> at session termination. The hypervisor erases the released memory before it is placed in the free pool.</td> </tr> <tr> <td data-bbox="347 1551 570 1675">RNG state</td> <td data-bbox="570 1551 906 1675">Internal state and seed key of the RNG</td> <td data-bbox="906 1551 1138 1675">Plaintext in volatile memory</td> <td data-bbox="1138 1551 1471 1675">Handled by kernel, overwritten with zeros at reboot.</td> </tr> <tr> <td data-bbox="347 1675 570 1789">IKE Private Host Key</td> <td data-bbox="570 1675 906 1789">Private authentication key used in IKE. RSA</td> <td data-bbox="906 1675 1138 1789">Plaintext in virtual disc or in flash memory.</td> <td data-bbox="1138 1675 1471 1789">Erased by the Administrator issuing <code>clear security</code></td> </tr> </tbody> </table>			Keys/CSPs	Purpose	Storage Location	Method of Zeroization	SSH Private Host Key	Generated with the random number generator when the SSH is first set up. Used to identify the host. ecdsa-sha2-nistp256 (ECDSA P-256, ECDSA P-384, ECDSA P-521) and/or ssh-rsa (RSA 2048)	Plaintext on the virtual disk.	When the TOE is recommissioned, the config files (including CSP files) are removed using the Linux <code>shred</code> command to wipe the persistent storage media.	SSH Private Host Key	Loaded into memory to complete session establishment	Plaintext in volatile memory.	The TOE calls <code>bzero()</code> at session termination. The hypervisor erases the released memory before it is placed in the free pool.	SSH Session Key	Session keys used with SSH, AES 128, 256, hmac-sha-1, hmac-sha2-256 or hmac-sha2-512 key (160, 256 or 512), DH Private Key (2048 or elliptic curve 256/384/521-bits)	Plaintext in volatile memory	The TOE calls <code>bzero()</code> at session termination. The hypervisor erases the released memory before it is placed in the free pool.	RNG state	Internal state and seed key of the RNG	Plaintext in volatile memory	Handled by kernel, overwritten with zeros at reboot.	IKE Private Host Key	Private authentication key used in IKE. RSA	Plaintext in virtual disc or in flash memory.	Erased by the Administrator issuing <code>clear security</code>
Keys/CSPs	Purpose	Storage Location	Method of Zeroization																								
SSH Private Host Key	Generated with the random number generator when the SSH is first set up. Used to identify the host. ecdsa-sha2-nistp256 (ECDSA P-256, ECDSA P-384, ECDSA P-521) and/or ssh-rsa (RSA 2048)	Plaintext on the virtual disk.	When the TOE is recommissioned, the config files (including CSP files) are removed using the Linux <code>shred</code> command to wipe the persistent storage media.																								
SSH Private Host Key	Loaded into memory to complete session establishment	Plaintext in volatile memory.	The TOE calls <code>bzero()</code> at session termination. The hypervisor erases the released memory before it is placed in the free pool.																								
SSH Session Key	Session keys used with SSH, AES 128, 256, hmac-sha-1, hmac-sha2-256 or hmac-sha2-512 key (160, 256 or 512), DH Private Key (2048 or elliptic curve 256/384/521-bits)	Plaintext in volatile memory	The TOE calls <code>bzero()</code> at session termination. The hypervisor erases the released memory before it is placed in the free pool.																								
RNG state	Internal state and seed key of the RNG	Plaintext in volatile memory	Handled by kernel, overwritten with zeros at reboot.																								
IKE Private Host Key	Private authentication key used in IKE. RSA	Plaintext in virtual disc or in flash memory.	Erased by the Administrator issuing <code>clear security</code>																								

		2048, ECDSA P-256, ECDSA P-384		IKE security-association command or zeroized at rebooting the TOE. Private keys stored in flash are not zeroized unless an explicit request system zeroize command is executed.
	IKE-SKEYID	IKE master secret used to derive IKE and IPsec ESP session keys	Plaintext in volatile memory	Erased by the Administrator issuing clear security IKE security-association command or zeroized at rebooting the TOE.
	IKE Session Key	IKE Session keys. AES, HMAC.	Plaintext in volatile memory	Erased by the Administrator issuing clear security IKE security-association command or zeroized at rebooting the TOE.
	ESP Session Key	ESP Session Keys. AES, HMAC.	Plaintext in volatile memory	Erased by the Administrator issuing clear security ipsec security-association command or zeroized at rebooting the TOE.
	IKE-DH Private Exponent	Ephemeral DH private exponent used in IKE. DH N = 224 bit, ECDH P-256, or ECDH P-384	Plaintext in volatile memory.	Erased by the Administrator issuing clear security IKE security-association command or zeroized at rebooting the TOE.
	IKE-PSK	Pre-shared authentication key used in IKE	Hashed in virtual disc or flash memory.	Erased by Administrator issuing a clear security IKE security-association

				command or zeroized at rebooting the TOE. Keys stored in flash are not zeroized unless an Administrator issues a <code>request system zeroize</code> command.
	ecdh private keys	Loaded into memory to complete key exchange in session establishment	Plaintext in volatile memory.	The TOE calls <code>bzero()</code> at session termination. The hypervisor erases the released memory before it is placed in the free pool.
Based on these findings, this assurance activity is considered satisfied.				
Verdict	Pass			

5.2.4.4 FCS_CKM.4 TSS 4

Objective	The evaluator shall check that the TSS identifies any configurations or circumstances that may not conform to the key destruction requirement (see further discussion in the Guidance Documentation section below). Note that reference may be made to the Guidance Documentation for description of the detail of such cases where destruction may be prevented or delayed.
Evaluator Findings	The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS identifies any configurations or circumstances that may not conform to the key destruction requirement. Upon investigation, the evaluator found that There are no configurations that do not conform to the key destruction requirement. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.4.5 FCS_CKM.4 TSS 5

Objective	Where the ST specifies the use of “a value that does not contain any CSP” to overwrite keys, the evaluator examines the TSS to ensure that it describes how that pattern is obtained and used, and that this justifies the claim that the pattern does not contain any CSPs.
Evaluator Findings	The ST does not select “a value that does not contain any CSP”. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.4.6 FCS_CKM.4 Guidance 1

Objective	A TOE may be subject to situations that could prevent or delay key destruction in some cases. The evaluator shall check that the guidance documentation identifies configurations or circumstances that may not strictly conform to the key destruction requirement, and that this description is consistent with the relevant parts of the TSS (and any other supporting information used). The evaluator shall check that the guidance documentation provides guidance on situations where key destruction may be delayed at the physical layer.
Evaluator Findings	<p>The evaluator checked the AGD and did not discover any configuration or circumstances that do not conform to the key destruction requirement. The evaluator determined that this description is consistent with the TSS.</p> <p>The evaluator also checked the AGD for guidance on situations where key destruction may be delayed at the physical layer. Upon investigation, the evaluator found that the AGD states that Zeroization can be time-consuming. Although all configurations are removed in a few seconds, the zeroization process goes on to overwrite all media, which can take considerable time depending on the size of the media.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.2.5 FCS_COP.1/DataEncryption

5.2.5.1 FCS_COP.1/DataEncryption TSS 1

Objective	The evaluator shall examine the TSS to ensure it identifies the key size(s) and mode(s) supported by the TOE for data encryption/decryption.
Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS to ensure it identifies the key size(s) and mode(s) supported by the TOE for data encryption/decryption. Upon investigation, the evaluator found that the TSS states that:</p> <p>The TOE implements the following cryptographic protocols with the stated methods of key exchange (KE) and the authentication, cipher and integrity algorithms. The details and CAVP validation certificate numbers are given in Table 15.</p> <p>IKE v1 KE: DH Group 14 (modp 2048), DH Group 19 (P-256) and DH Group 20 (P-384) Authentication: RSA 2048, ECDSA P-256, ECDSA P-384, pre-shared key Cipher: AES-CBC-128, AES-CBC-192, AES CBC-256 Integrity: HMAC-SHA-256-128, HMAC-SHA-384-192</p> <p>IKE v2 KE: DH Group 14 (modp 2048), DH Group 19 (P-256) and DH Group 20 (P-384) Authentication: RSA 2048, ECDSA P-256, ECDSA P-384, pre-shared key Cipher: AES-CBC-128, AES-CBC-192, AES CBC-256, AES-GCM-128, AES-GCM-256 Integrity: HMAC-SHA-256-128, HMAC-SHA-384-192</p>

	<p>IPSec ESP (IKE v1) KE: IKE v1 with optional DH Group 14 (modp 2048), DH Group 19 (P-256) and DH Group 20 (P-384) Authentication: IKE v1 Cipher: AES-CBC-128, AES-CBC-192, AES CBC-256 Integrity: HMAC-SHA-256-128</p> <p>IPSec ESP (IKE v2) KE: IKE v2 with optional DH Group 14 (modp 2048), DH Group 19 (P-256) and DH Group 20 (P-384) Authentication: IKE v2 Cipher: AES-CBC-128, AES-CBC-192, AES CBC-256, AES-GCM-128, AES-GCM-192, AES-GCM-256 Integrity: HMAC-SHA-256-128</p> <p>SSH v2 KE: DH Group 14 (modp 2048), ECDH-sha2-nistp256, ECDH-sha2-nistp384, ECDH-sha2-nistp521 Authentication: ECDSA P-256, ECDSA P-384, ECDSA P-521 Cipher: AES-CTR-128, AES-CTR-256, AES-CBC-128, AES-CBC-256 Integrity: HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-512</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.2.5.2 FCS_COP.1/DataEncryption Guidance 1

Objective	The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the selected mode(s) and key size(s) defined in the Security Target supported by the TOE for data encryption/decryption.
Evaluator Findings	The evaluator examined the section titled Configuring VPNs in the AGD to verify that it provides guidance instructs the administrator how to configure the TOE to use the selected mode(s) and key size(s) defined in the Security Target supported by the TOE for data encryption/decryption. Upon investigation, the evaluator found that the AGD states the CLI commands needed to configure the required encryption/decryption mode and key size. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.5.3 FCS_COP.1/DataEncryption Test/CAVP 1

Objective	The evaluator shall verify the implementation of encryption supported by the TOE.
Evaluator Findings	CAVP AES Certs: # A3335, A3339, A3342, A3343 For additional details please refer to CAVP Mapping in Section 8 of this document. Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass
---------	------

5.2.6 FCS_COP.1/SigGen

5.2.6.1 FCS_COP.1/SigGen TSS 1

Objective	The evaluator shall examine the TSS to determine that it specifies the cryptographic algorithm and key size supported by the TOE for signature services.
Evaluator Findings	The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS to ensure it specifies the cryptographic algorithm and key size supported by the TOE for signature services. Upon investigation, the evaluator found that the TSS states that : The details of the digital signature generation and verification algorithms and their CAVP validation certificate numbers are given in Table 15. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.6.2 FCS_COP.1/SigGen Guidance 1

Objective	The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the selected cryptographic algorithm and key size defined in the Security Target supported by the TOE for signature services.
Evaluator Findings	The evaluator examined the section titled Configuring VPNs in the AGD to verify that it provides guidance instructs the administrator how to configure the TOE to use the selected cryptographic algorithm and key size defined in the Security Target supported by the TOE for signature services. Upon investigation, the evaluator found that the AGD states the steps to configure the TOE to use the appropriate cryptographic algorithm and key size for signature services. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.6.3 FCS_COP.1/SigGen Test/CAVP 1

Objective	The evaluator shall verify the implementation of signature generation and verification supported by the TOE.
Evaluator Findings	CAVP RSA SigGen&SigVer (186-4) Certs: # A3342 CAVP ECDSA&SigVer SigGen (186-4) Certs: # A3342 For additional details please refer to CAVP Mapping in Section 8 of this document. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.7 FCS_COP.1/Hash

5.2.7.1 FCS_COP.1/Hash TSS 1

Objective	The evaluator shall check that the association of the hash function with other TSF cryptographic functions (for example, the digital signature verification function) is documented in the TSS.
Evaluator Findings	The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS documents the association of the hash function with other TSF cryptographic functions. Upon investigation, the evaluator found that the TSS states that : The TOE implements SHA-1, SHA-256, SHA-384 and SHA-512. They are used for constructing HMACs as stated in FCS_COP.1/KeyedHash, for verifying the digital signatures of the TOE software and software upgrades as described in FPT_FLS.1 and FPT_TUD_EXT.1, and for storing user passwords as described in FPT_APW_EXT.1. The TSF performs SHA-1, SHA-256 hashing for the NTP. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.7.2 FCS_COP.1/Hash Guidance 1

Objective	The evaluator checks the AGD documents to determine that any configuration that is required to configure the required hash sizes is present.
Evaluator Findings	The evaluator examined the section titled “Configuring SSH on the Evaluated Configuration”, “Configuring a Common Criteria Authorized Administrator”, “Configuring an IPsec VPN with a Preshared Key for IKE Authentication”, and “Unsupported Junos-FIPS Configuration Statements” in the AGD to verify that it presents any configuration that is required to configure the required hash sizes. Upon investigation, the evaluator found that the AGD states that : The root password should be reset following the change to sha256 for the password storage format. This ensures the new password is protected using a sha256 hash, rather than the default password hashing algorithm. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.7.3 FCS_COP.1/Hash Test/CAVP 1

Objective	The evaluator shall verify the implementation of hashing supported by the TOE.
Evaluator Findings	CAVP SHS Certs: # A3335, A3339, A3340, A3342, A3343 For additional details please refer to CAVP Mapping in Section 8 of this document. Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass
---------	------

5.2.8 FCS_COP.1/KeyedHash

5.2.8.1 FCS_COP.1/KeyedHash TSS 1

Objective	The evaluator shall examine the TSS to ensure that it specifies the following values used by the HMAC function: key length, hash function used, block size, and output MAC length used.
Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS specifies the following values used by the HMAC function: key length, hash function used, block size, and output MAC length used. Upon investigation, the evaluator found that the TSS states that:</p> <p>The TOE implements the following HMAC-algorithms:</p> <ul style="list-style-type: none"> • HMAC-SHA-1 with SHA-1 and key length of 160 bits, block size of 512 bits and output MAC length of 160 bits. • HMAC-SHA-256 with SHA-256 and key length of 256 bits, block size of 512 bits and output length of 256 bits. • HMAC-SHA-384 with SHA-384 and key length of 384 bits, block size of 1024 bits and output length of 384 bits. <p>HMAC-SHA-512 with SHA-512 and key length of 512 bits, block size of 1024 bits and an output length of 512 bits.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.2.8.2 FCS_COP.1/KeyedHash Guidance 1

Objective	The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the values used by the HMAC function: key length, hash function used, block size, and output MAC length used defined in the Security Target supported by the TOE for keyed hash function.
Evaluator Findings	<p>The evaluator examined the section titled “Configuring SSH on the Evaluated configuration” and “Configuring VPNs” in the AGD to verify how to configure the TOE to use the values used by the HMAC function: key length, hash function used, block size, and output MAC length used defined in the Security Target supported by the TOE for keyed hash function. Upon investigation, the evaluator found that the AGD states the CLI command used to configure to use the appropriate HMAC function and associated functions.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.2.8.3 FCS_COP.1/KeyedHash Test/CAVP 1

Objective	The evaluator shall verify the implementation of MACing supported by the TOE.
-----------	-------------------------------------------------------------------------------

Evaluator Findings	CAVP HMAC Certs: # A3335, A3339, A3340, A3342, A3343 For additional details please refer to CAVP Mapping in Section 8 of this document. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.9 FCS_RBG_EXT.1

5.2.9.1 FCS_RBG_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS to determine that it specifies the DRBG type, identifies the entropy source(s) seeding the DRBG, and state the assumed or calculated min-entropy supplied either separately by each source or the min-entropy contained in the combined seed value.
Evaluator Findings	The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS specifies the DRBG type, identifies the entropy source(s) seeding the DRBG, and state the assumed or calculated min-entropy supplied either separately by each source or the min-entropy contained in the combined seed value. Upon investigation, the evaluator found that the TSS states that : The TOE generates random bits in accordance with NIST Special Publication 800-90 using HMAC_DRBG, SHA-256. The RBG does not require any configuration and is seeded from single designated primary entropy source: Junos OS credits a single designated primary entropy source: bits 2-9 of the timestamp associated with software interrupts associated with the clock0 (RANDOM_SWI_CLOCK0). The RANDOM_SWI_CLOCK0 source produces 1-byte raw samples which are bits 2-9 of the hardware high-resolution clock, where bit 0 denotes the least significant bit (lsb), bit 1 the next least significant bit, and so on. This high-resolution clock is the lower 32 bits of the Intel CPU's TSC counter. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.9.2 FCS_RBG_EXT.1 Guidance 1

Objective	The evaluator shall confirm that the guidance documentation contains appropriate instructions for configuring the RNG functionality.
Evaluator Findings	The evaluator examined the section titled Understanding FIPS Self-Tests in the AGD to verify that it contains appropriate instructions for configuring the RNG functionality. Upon investigation, the evaluator found that the AGD states that DRBG does not require any configuration, and initialized on startup. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.9.3 FCS_RBG_EXT.1.1 Test/CAVP 1

Objective	The evaluator shall verify the implementation of SP 800-90A DRBG supported by the TOE.
Evaluator Findings	CAVP DRBG Certs: # A3335, A3342, A3343 For additional details please refer to CAVP Mapping in Section 8 of this document. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3 TSS and Guidance Activities (IPsec)

5.3.1 FCS_IPSEC_EXT.1

5.3.1.1 FCS_IPSEC_EXT.1.1 TSS 1

Objective	The evaluator shall examine the TSS and determine that it describes what takes place when a packet is processed by the TOE, e.g., the algorithm used to process the packet. The TSS describes how the SPD is implemented and the rules for processing both inbound and outbound packets in terms of the IPsec policy. The TSS describes the rules that are available and the resulting actions available after matching a rule. The TSS describes how those rules and actions form the SPD in terms of the BYPASS (e.g., no encryption), DISCARD (e.g., drop the packet), and PROTECT (e.g., encrypt the packet) actions defined in RFC 4301.
Evaluator Findings	The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS describes what takes place when a packet is processed by the TOE. Upon investigation, the evaluator found that the TSS states that : The TOE implements IPsec in accordance with RFC 4301 in tunnel mode only. A description of the implementation of packet filtering in association with IPsec is given under FPF_RUL_EXT.1. Each packet is compared to the entries in the security policy rule set in sequential order until a rule that matches the packet is found or the end of the rule set is reached. If a matching rule is found, the action stated in that rule shall be taken. If the end of the rule set is reached, the packet is discarded. When a packet is processed by the TOE, the route is checked to see if it meets a defined security policy. If the packet meets the security policy, it is processed according to the rules of that policy. When the network traffic is encrypted, the header information may not be readily available for the enforcement of the security policy rules. Additional configuration options are available to configure the packet filtering to a specific mode for IPsec VPN tunnels. The following modes may be defined: <ul style="list-style-type: none"> • Bypass mode. Directs traffic traversing the TOE through the stateful firewall inspection, but not through the IPsec VPN tunnel • Discard. Inspects and drops all packets that do not match any Permit policies.

	<ul style="list-style-type: none"> • Protect. Traffic is routed through an IPsec tunnel based on a combination of route lookup and Permit policy inspection. • Log. Logs traffic and session information for all modes. <p>Additionally, the evaluator compared the described rules to the operation of the TOE during testing and found the description of the available SPD to be consistent with the implementation of the TOE.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.3.1.2 FCS_IPSEC_EXT.1.1 TSS 2

Objective	<p>As noted in section 4.4.1 of RFC 4301, the processing of entries in the SPD is non-trivial and the evaluator shall determine that the description in the TSS is sufficient to determine which rules will be applied given the rule structure implemented by the TOE. For example, if the TOE allows specification of ranges, conditional rules, etc., the evaluator shall determine that the description of rule processing (for both inbound and outbound packets) is sufficient to determine the action that will be applied, especially in the case where two different rules may apply. This description shall cover both the initial packets (that is, no SA is established on the interface or for that particular packet) as well as packets that are part of an established SA.</p>
Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS is sufficient to determine which rules will be applied given the rule structure implemented by the TOE. Upon investigation, the evaluator found that the TSS states that:</p> <p>Each packet is compared to the entries in the security policy rule set in sequential order until a rule that matches the packet is found or the end of the rule set is reached. If a matching rule is found, the action stated in that rule shall be taken. If the end of the rule set is reached, the packet is discarded. When a packet is processed by the TOE, the route is checked to see if it meets a defined security policy. If the packet meets the security policy, it is processed according to the rules of that policy.</p> <p>For inbound traffic, the TOE looks up the SA by using the destination IP address, security protocol, and security parameter index (SPI) value. For outbound VPN traffic, the policy invokes the SA associated with the VPN tunnel. If a packet arrives and there is not an active SA for that tunnel, the packet is dropped. The TOE will then begin to establish a tunnel, so that when the packet is resent, the SA is active. After the SA is established all subsequent packets in the session will use the IPsec tunnel.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.3.1.3 FCS_IPSEC_EXT.1.1 Guidance 1

Objective	The evaluator shall examine the guidance documentation to verify it instructs the Administrator how to construct entries into the SPD that specify a rule for processing a packet. The description includes all three cases – a rule that ensures packets are encrypted/decrypted, dropped, and flow through the TOE without being encrypted. The evaluator shall determine that the description in the guidance documentation is consistent with the description in the TSS, and that the level of detail in the guidance documentation is sufficient to allow the administrator to set up the SPD in an unambiguous fashion. This includes a discussion of how ordering of rules impacts the processing of an IP packet.
Evaluator Findings	<p>The evaluator examined the section titled Configuring Security Flow Policies in the AGD to verify that it instructs the Administrator how to construct entries into the SPD that specify a rule for processing a packet. Upon investigation, the evaluator found that the AGD states the CLI commands to add entries into the SPD and to specify rules for processing a packet under three modes i.e. bypass, discard and protect. The evaluator also found that the description in the guidance documentation is consistent with the description in the TSS.</p> <p>The evaluator next compared the description of configuring SPDs found in the AGD to the one found in the TSS of the ST and found that the descriptions are consistent.</p> <p>Finally the evaluator examined the AGD to verify that the level of detail in the guidance documentation is sufficient to allow the administrator to set up the SPD in an unambiguous fashion, including a discussion of how ordering of rules impacts the processing of an IP packet. Upon investigation, the evaluator found that the AGD describes setting up the SPD in sufficient detail. The AGD section titled Configuring Traffic Filtering Rules also discusses how ordering of rules impacts the processing of an IP packet.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.3.1.4 FCS_IPSEC_EXT.1.3 TSS 1

Objective	The evaluator checks the TSS to ensure it states that the VPN can be established to operate in transport mode and/or tunnel mode (as identified in FCS_IPSEC_EXT.1.3).
Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS states that the VPN can be established to operate in transport mode and/or tunnel mode (as identified in FCS_IPSEC_EXT.1.3). Upon investigation, the evaluator found that the TSS states that :</p> <p>The TOE implements IPSec in accordance with RFC 4301 in tunnel mode only.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.3.1.5 FCS_IPSEC_EXT.1.3 Guidance 1

Objective	The evaluator shall confirm that the guidance documentation contains instructions on how to configure the connection in each mode selected.
Evaluator Findings	<p>The evaluator examined the section titled Configuring VPNs in the AGD to verify that it contains instructions on how to configure the connection in each mode selected. Upon investigation, the evaluator found that the AGD states that</p> <p>Table 8 on page 182 provides a complete list of the supported IKE protocols, tunnel modes, Phase 1 negotiation mode, authentication method or algorithm, encryption algorithm, DH groups supported for the IKE negotiation and encryption (Phase1, IKE Proposal), and for IPsec authentication and encryption (Phase2, IPsec Proposal).</p> <p>The AGD also states the CLI command for mode selection while configuring the IKE policy:</p> <p>Configuring the IKE policy.</p> <p>[edit]</p> <pre>user@host# set security ike policy ike-policy1 mode main</pre> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.3.1.6 FCS_IPSEC_EXT.1.4 TSS 1

Objective	The evaluator shall examine the TSS to verify that the selected algorithms are implemented. In addition, the evaluator ensures that the SHA-based HMAC algorithm conforms to the algorithms specified in FCS_COP.1/KeyedHash Cryptographic Operations (for keyed-hash message authentication) and if the SHA-based HMAC function truncated output is utilized it must also be described.
Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS states that the selected algorithms are implemented. Upon investigation, the evaluator found that the TSS states that:</p> <p>AES-GCM-192, AES-GCM-256, AES-CBC-128, AES-CBC-192 and AES-CBC-256 using HMAC SHA-256 are implemented for ESP protection.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.3.1.7 FCS_IPSEC_EXT.1.4 Guidance 1

Objective	The evaluator checks the guidance documentation to ensure it provides instructions on how to configure the TOE to use the algorithms selected.
Evaluator Findings	The evaluator examined the section titled Configuring VPNs in the AGD to verify that it provides instructions on how to configure the TOE to use the algorithms selected. Upon

	<p>investigation, the evaluator found that the AGD states that the CLI commands to configure the TOE to use the selected algorithms as part of the IPsec proposal.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.3.1.8 FCS_IPSEC_EXT.1.5 TSS 1

Objective	The evaluator shall examine the TSS to verify that IKEv1 and/or IKEv2 are implemented.
Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS identifies whether IKEv1 and/or IKEv2 are implemented. Upon investigation, the evaluator found that the TSS states that:</p> <p>Both IKEv1 and IKEv2 are implemented.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.3.1.9 FCS_IPSEC_EXT.1.5 TSS 2

Objective	For IKEv1 implementations, the evaluator shall examine the TSS to ensure that, in the description of the IPsec protocol, it states that aggressive mode is not used for IKEv1 Phase 1 exchanges, and that only main mode is used. It may be that this is a configurable option.
Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS states that aggressive mode is not used for IKEv1 Phase 1 exchanges, and that only main mode is used. Upon investigation, the evaluator found that the TSS states that :</p> <p>For IKEv1, only main mode is supported, while aggressive mode is not.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.3.1.10 FCS_IPSEC_EXT.1.5. Guidance 1

Objective	The evaluator shall check the guidance documentation to ensure it instructs the administrator how to configure the TOE to use IKEv1 and/or IKEv2 (as selected), and how to configure the TOE to perform NAT traversal (if selected).
Evaluator Findings	<p>The evaluator examined the section titled Configuring VPNs in the AGD to verify that it instructs the administrator how to configure the TOE to use IKEv1 and/or IKEv2 (as selected), and how to configure the TOE to perform NAT traversal (if selected). Upon investigation, the evaluator found that the AGD states the CLI command used to configure the TOE to use IKEv1/IKEv2 as part of the IKE gateway configuration. The ST does not select NAT traversal, so no configuration instructions for NAT traversal are necessary.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>

Verdict	Pass
---------	------

5.3.1.11 FCS_IPSEC_EXT.1.5. Guidance 2

Objective	If the IKEv1 Phase 1 mode requires configuration of the TOE prior to its operation, the evaluator shall check the guidance documentation to ensure that instructions for this configuration are contained within that guidance.
Evaluator Findings	The evaluator examined the section titled Configuring VPNs in the AGD to verify that it contains any necessary instructions for IKEv1 Phase 1 mode configuration. Upon investigation, the evaluator found that the AGD states the CLI commands needed for IKEv1 Phase 1 configuration. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.1.12 FCS_IPSEC_EXT.1.6 TSS 1

Objective	The evaluator shall ensure the TSS identifies the algorithms used for encrypting the IKEv1 and/or IKEv2 payload, and that the algorithms chosen in the selection of the requirement are included in the TSS discussion.
Evaluator Findings	The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS identifies the algorithms used for encrypting the IKEv1 and/or IKEv2 payload, and that the algorithms chosen in the selection of the requirement are included in the TSS discussion. Upon investigation, the evaluator found that the TSS states that The TOE implements AES-CBC-128, AES-CBC-192 and AES-CBC-256 for payload protection in IKEv1 and IKEv2, and also AES-GCM-128 and AES-GCM-256 for payload protection in IKEv2. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.1.13 FCS_IPSEC_EXT.1.6 Guidance 1

Objective	The evaluator ensures that the guidance documentation describes the configuration of all selected algorithms in the requirement.
Evaluator Findings	The evaluator examined the section titled Configuring VPNs in the AGD to verify that it describes the configuration of all selected algorithms in the requirement. Upon investigation, the evaluator found that the AGD states the CLI commands needed to configure the TOE to use the selected algorithms as part of the IKE proposal. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.1.14 FCS_IPSEC_EXT.1.7 TSS 1

Objective	The evaluator shall ensure the TSS identifies the lifetime configuration method used for limiting the IKEv1 Phase 1 SA lifetime and/or the IKEv2 SA lifetime. The evaluator shall verify that the selection made here corresponds to the selection in FCS_IPSEC_EXT.1.5.
Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS identifies the lifetime configuration method used for limiting the IKEv1 Phase 1 SA lifetime and/or the IKEv2 SA lifetime and that information corresponds to the selection in FCS_IPSEC_EXT.1.5. Upon investigation, the evaluator found that the TSS states that:</p> <p>In the evaluated configuration, the TOE permits configuration of the:</p> <ul style="list-style-type: none"> • IKEv1 Phase 1 and IKEv2 SA lifetimes in terms of length of time (180 to 86,400 seconds i.e. 0.05 to 24 hours), <p>The TOE implements the following CLI commands to configure the Phase 1 lifetime in seconds:</p> <pre>set security ike proposal <name> lifetime-seconds <seconds></pre> <p>Next, the evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the selection made here corresponds to the selection in FCS_IPSEC_EXT.1.5. Upon investigation, the evaluator found that the two were consistent with each other.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.3.1.15 FCS_IPSEC_EXT.1.7 Guidance 1 [TD0633]

Objective	The evaluator shall verify that the values for SA lifetimes can be configured and that the instructions for doing so are located in the Guidance documentation. If time-based limits are supported, configuring the limit may lead to a rekey no later than the specified limit. For some implementations, it may be necessary, though, to configure the TOE with a lower time value to ensure a rekey is performed before the maximum SA lifetime of 24 hours is exceeded (e.g. configure a time value of 23h 45min to ensure the actual rekey is performed no later than 24h). The evaluator shall verify that the Guidance documentation allows the Administrator to configure the Phase 1 SA value of 24 hours or provides sufficient instruction about the time value to configure to ensure the rekey is performed no later than the maximum SA lifetime of 24 hours. It is not permitted to configure a value of 24 hours if that leads to an actual rekey after more than 24hours. Currently there are no values mandated for the number of bytes, the evaluator just ensures that this can be configured if selected in the requirement.
-----------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<p>Evaluator Findings</p>	<p>The evaluator examined the section titled Configuring VPNs in the AGD to verify that it includes instructions for configuring values for SA lifetimes. Upon investigation, the evaluator found that the AGD states that :</p> <p>Configuring the Lifetime for an IKE SA The IKE lifetime sets the lifetime of an IKE SA. When the IKE SA expires, it is replaced by a new SA (and SPI) or is terminated. The default value IKE lifetime is 3600 seconds.</p> <p>To configure the IKE lifetime, include the lifetime-seconds statement and specify the number of seconds (180 through 86,400) at the [edit security ike proposal ike-proposal-name] hierarchy level:</p> <p>[edit security ike proposal ike-proposal-name] lifetime-seconds seconds;</p> <p>Next, the evaluator verified that the Guidance documentation provides sufficient instruction about the time value to configure to ensure the rekey is performed no later than the maximum Phase 1 SA lifetime of 24 hours. Upon investigation, the evaluator found that the mentioned maximum configurable lifetime of 86,400 seconds (24 hours) is to be configured for the same.</p> <p>Lastly, since lifetime in bytes is not selected under FCS_IPSEC_EXT.1.7, the latter TSS activity is not applicable.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
<p>Verdict</p>	<p>Pass</p>

5.3.1.16 FCS_IPSEC_EXT.1.8 TSS 1

<p>Objective</p>	<p>The evaluator shall ensure the TSS identifies the lifetime configuration method used for limiting the IKEv1 Phase 2 SA lifetime and/or the IKEv2 Child SA lifetime. The evaluator shall verify that the selection made here corresponds to the selection in FCS_IPSEC_EXT.1.5.</p>
<p>Evaluator Findings</p>	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS identifies the lifetime configuration method used for limiting the IKEv1 Phase 2 SA lifetime and/or the IKEv2 Child SA lifetime and that the information corresponds to the selection in FCS_IPSEC_EXT.1.5. Upon investigation, the evaluator found that the TSS states that :</p> <p>In the evaluated configuration, the TOE permits configuration of the:</p> <ul style="list-style-type: none"> • IKEv1 Phase 2 SA lifetimes in terms of length of time (180 to 28,800 seconds i.e. 0.05 to 8 hours), • IKEv2 Child SA lifetimes in terms of (kilo)bytes (64 to 4292967294) and length of time (180 to 28,800 seconds i.e. 0.05 to 8 hours) <p>Phase 2 lifetime can be configured in either kilobytes or seconds using the following commands:</p>

	<pre>set security ipsec proposal <name> lifetime-kilobytes <kb> set security ipsec proposal <name> lifetime-seconds <seconds></pre> <p>Next, the evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the selection made here corresponds to the selection in FCS_IPSEC_EXT.1.5. Upon investigation, the evaluator found that the two were consistent with each other.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.3.1.17 FCS_IPSEC_EXT.1.8 Guidance 1 [TD0633]

Objective	<p>The evaluator shall verify that the values for SA lifetimes can be configured and that the instructions for doing so are located in the Guidance documentation. If time-based limits are supported, configuring the limit may lead to a rekey no later than the specified limit. For some implementations, it may be necessary, though, to configure the TOE with a lower time value to ensure a rekey is performed before the maximum SA lifetime of 8 hours is exceeded (e.g. configure a time value of 7h 45min to ensure the actual rekey is performed no later than 8h). The evaluator shall verify that the Guidance documentation allows the Administrator to configure the Phase 2 SA value of 8 hours or provides sufficient instruction about the time value to configure to ensure the rekey is performed no later than the maximum SA lifetime of 8 hours. It is not permitted to configure a value of 8 hours if that leads to an actual rekey after more than 8hours. Currently there are no values mandated for the number of bytes, the evaluator just ensures that this can be configured if selected in the requirement.</p>
Evaluator Findings	<p>The evaluator examined the section titled Configuring VPNs in the AGD to verify that it includes instructions for configuring values for SA lifetimes. Upon investigation, the evaluator found that the AGD states that :</p> <p>Configuring the Lifetime for an IPsec SA The IPsec lifetime option sets the lifetime of an IPsec SA. When the IPsec SA expires, it is replaced by a new SA (and SPI) or is terminated. A new SA has new authentication and encryption keys, and SPI; however, the algorithms may remain the same if the proposal is not changed. If lifetime is not configured and a lifetime is not sent by a responder, the lifetime is 28,800 seconds.</p> <p>To configure the IPsec lifetime, include the lifetime-seconds statement and specify the number of seconds (180 through 86,400) at the [edit security ipsec proposal ipsec-proposal-name] hierarchy level:</p> <pre>[edit security ipsec proposal ipsec-proposal-name] lifetime-seconds seconds;</pre>

	<p>To configure the IPsec lifetime by number of bytes, include the lifetime-kilobytes and Specify the lifetime (in kilobytes) of an IPsec security association (SA). If this statement is not configured, the number of kilobytes used for the SA lifetime is unlimited.</p> <p>Range: 64 through 1,048,576 kilobytes at the [edit security ipsec proposal ipsec-proposal-name] hierarchy level:</p> <p>[edit security ipsec proposal ipsec-proposal-name] lifetime-kilobytes kilobytes;</p> <p>Next, the evaluator verified that the Guidance documentation provides sufficient instruction about the time value to configure to ensure the rekey is performed no later than the maximum Phase 2 SA lifetime of 8 hours. Upon investigation, the evaluator found that since a lifetime range of 180 through 86,400 seconds is supported, configuring the value at 28800 seconds (8 hours) will ensure the same.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.3.1.18 FCS_IPSEC_EXT.1.9 TSS 1

Objective	<p>The evaluator shall check to ensure that, for each DH group supported, the TSS describes the process for generating "x". The evaluator shall verify that the TSS indicates that the random number generated that meets the requirements in this PP is used, and that the length of "x" meets the stipulations in the requirement.</p>
Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS describes the process for generating "x" for each DH group supported. Upon investigation, the evaluator found that the TSS states that</p> <p>The TOE implements Diffie-Hellman Groups 14, 19, 20. In the IKEv1 phase 1 and phase 2 exchanges, the TOE and peer will agree on the best DH group both can support. When the TOE receives an IKE proposal, it will select the first DH group that matches the acceptable DH groups (one or more of DH Groups 14, 19, 20). The negotiation will fail if there is no match. Similarly, when the peer initiates the IKE protocol, the TOE will select the first match from the IKE proposal sent by the peer and the negotiation fails if no acceptable match is found.</p> <p>The TOE uses HMAC DRBG with SHA-256 for the generation of DH exponents and nonces. Nonces in the IKE key exchange protocol are of length 224 bits (for DH Group 14), 256 bits (for DH Group 19), 384 bits (for DH Group 20). The generation of random bits is described at FCS_RBG_EXT.1.</p> <p>Next, the evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS indicates that the random number generated that meets the</p>

	<p>requirements in this PP is used, and that the length of "x" meets the stipulations in the requirement. Upon investigation, the evaluator found that the TSS states that</p> <p>The generation of random bits is described at FCS_RBG_EXT.1.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.3.1.19 FCS_IPSEC_EXT.1.10 TSS 1

Objective	<p>If the first selection is chosen, the evaluator shall check to ensure that, for each DH group supported, the TSS describes the process for generating each nonce. The evaluator shall verify that the TSS indicates that the random number generated that meets the requirements in this PP is used, and that the length of the nonces meet the stipulations in the requirement.</p> <p>If the second selection is chosen, the evaluator shall check to ensure that, for each PRF hash supported, the TSS describes the process for generating each nonce. The evaluator shall verify that the TSS indicates that the random number generated that meets the requirements in this PP is used, and that the length of the nonces meet the stipulations in the requirement.</p>
Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS describes the process for generating each nonce for each DH group or PRF hash supported and indicates that the random number generated that meets the requirements in this PP is used, and indicates that the length of the nonces meet the stipulations in the requirement. Upon investigation, the evaluator found that the TSS states that</p> <p>The TOE uses HMAC DRBG with SHA-256 for the generation of DH exponents and nonces. Nonces in the IKE key exchange protocol are of length 224 bits (for DH Group 14), 256 bits (for DH Group 19), 384 bits (for DH Group 20). The generation of random bits is described at FCS_RBG_EXT.1.</p> <p>Since the second selection is not made, the latter half of the TSS activity is not applicable.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.3.1.20 FCS_IPSEC_EXT.1.11 TSS 1

Objective	<p>The evaluator shall check to ensure that the DH groups specified in the requirement are listed as being supported in the TSS. If there is more than one DH group supported, the evaluator checks to ensure the TSS describes how a particular DH group is specified/negotiated with a peer.</p>
-----------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS lists the DH groups specified in the requirement as being supported. Upon investigation, the evaluator found that the TSS states that</p> <p>The TOE implements Diffie-Hellman Groups 14, 19, 20. In the IKEv1 phase 1 and phase 2 exchanges, the TOE and peer will agree on the best DH group both can support. When the TOE receives an IKE proposal, it will select the first DH group that matches the acceptable DH groups (one or more of DH Groups 14, 19, 20). The negotiation will fail if there is no match. Similarly, when the peer initiates the IKE protocol, the TOE will select the first match from the IKE proposal sent by the peer and the negotiation fails is no acceptable match is found.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.3.1.21 FCS_IPSEC_EXT.1.11 Guidance 1

Objective	The evaluator ensures that the guidance documentation describes the configuration of all algorithms selected in the requirement.
Evaluator Findings	<p>The evaluator examined the section titled Configuring VPNs in the AGD to verify that it describes the configuration of all algorithms selected in the requirement. Upon investigation, the evaluator found that the AGD states the CLI command needed to configure the selected DH Groups.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.3.1.22 FCS_IPSEC_EXT.1.12 TSS 1

Objective	The evaluator shall check that the TSS describes the potential strengths (in terms of the number of bits in the symmetric key) of the algorithms that are allowed for the IKE and ESP exchanges. The TSS shall also describe the checks that are done when negotiating IKEv1 Phase 2 and/or IKEv2 CHILD_SA suites to ensure that the strength (in terms of the number of bits of key in the symmetric algorithm) of the negotiated algorithm is less than or equal to that of the IKE SA this is protecting the negotiation.
Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS describes the potential strengths of the algorithms that are allowed for the IKE and ESP exchanges and the checks that are done when negotiating IKEv1 Phase 2 and/or IKEv2 CHILD_SA suites. Upon investigation, the evaluator found that the TSS states that:</p> <p>The TOE checks the strengths of the configured IKE algorithms prior to committing a tunnel configuration. This ensures that the strength of the symmetric algorithm (128, 192 or 256 bits) negotiated to protect the IKEv1 Phase 1 or IKEv2 IKE_SA connection is greater than or equal to the strength of the symmetric algorithm negotiated to protect the IKEv1 Phase 2 or IKEv2 CHILD_SA connection. If the strength is not greater, an error is displayed, and the configuration fails.</p>

	Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.1.23 FCS_IPSEC_EXT.1.13 TSS 1

Objective	The evaluator ensures that the TSS identifies RSA and/or ECDSA as being used to perform peer authentication. The description must be consistent with the algorithms as specified in FCS_COP.1/SigGen Cryptographic Operations (for cryptographic signature).
Evaluator Findings	The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS identifies RSA and/or ECDSA as being used to perform peer authentication and that the algorithms are consistent with those specified in FCS_COP.1/SigGen Cryptographic Operations. Upon investigation, the evaluator found that the TSS states that: The TOE uses X.509v3 certificates with RSA and ECDSA as defined in RFC 4945. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.1.24 FCS_IPSEC_EXT.1.13 TSS 2

Objective	If pre-shared keys are chosen in the selection, the evaluator shall check to ensure that the TSS describes how pre-shared keys are established and used in authentication of IPsec connections. The description in the TSS shall also indicate how pre-shared key establishment is accomplished for TOEs that can generate a pre-shared key as well as TOEs that simply use a pre-shared key.
Evaluator Findings	The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS describes how pre-shared keys are established and used in authentication of IPsec connections. Upon investigation, the evaluator found that the TSS states that The TOE uses pre-shared keys for IPsec as described in FIA_PSK_EXT.1. The TOE supports IPSec pre-shared keys. It accepts Unicode characters to specify text-based pre-shared keys. Unicode characters are encoded as UTF-8 and treated as multiple bytes – up to 4 bytes depending on the character. The maximum length limit for text-based pre-shared keys enforced by the TOE is 255 bytes. When a pre-shared key is only composed of ASCII characters this limit is equivalent to 255 characters. The text-based pre-shared or bit-based keys may contain upper and lower case letters, numbers, and special characters (which include: “!”, “@”, “#”, “\$”, “%”, “^”, “&”, “*”, “(”, and “”). The TOE accepts pre-shared text keys and converts the text string into an authentication value as per RFC 2409 for IKEv1 or RFC 4306 for IKEv2, using the PRF that is configured as the hash algorithm for the IKE exchanges. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.1.25 FCS_IPSEC_EXT.1.13 Guidance 1

Objective	The evaluator ensures the guidance documentation describes how to set up the TOE to use certificates with RSA and/or ECDSA signatures and public keys.
Evaluator Findings	The evaluator examined the section titled Configuring an IPsec VPN with an RSA Signature for IKE Authentication and Configuring an IPsec VPN with an ECDSA Signature for IKE Authentication in the AGD to verify that it describes how to set up the TOE to use certificates with RSA and/or ECDSA signatures and public keys. Upon investigation, the evaluator found that the AGD states the CLI commands needed to configure the TOE to use certificates with RSA or ECDSA signatures and public keys. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.1.26 FCS_IPSEC_EXT.1.13 Guidance 2

Objective	The evaluator shall check that the guidance documentation describes how preshared keys are to be generated and established. The description in the guidance documentation shall also indicate how pre-shared key establishment is accomplished for TOEs that can generate a pre-shared key as well as TOEs that simply use a pre-shared key.
Evaluator Findings	The evaluator examined the section titled Configuring an IPsec VPN with a Preshared Key for IKE Authentication in the AGD to verify that it describes how pre-shared keys are to be generated and established. Upon investigation, the evaluator found that the AGD states the CLI commands to configure pre-shared key establishment. The TOE simply uses pre-shared keys but does not generate them so no configuration steps for pre-shared key generation are required. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.1.27 FCS_IPSEC_EXT.1.13 Guidance 3

Objective	The evaluator will ensure that the guidance documentation describes how to configure the TOE to connect to a trusted CA and ensure a valid certificate for that CA is loaded into the TOE and marked “trusted”.
Evaluator Findings	The evaluator examined the section titled Configuring an IPsec VPN with an RSA Signature for IKE Authentication and Configuring an IPsec VPN with an ECDSA Signature for IKE Authentication in the AGD to verify that it describes how to configure the TOE to connect to a trusted CA and ensure a valid certificate for that CA is loaded into the TOE and marked “trusted”. Upon investigation, the evaluator found that the AGD states the CLI commands needed to load CA certificates into the TOE and verify their validity. Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass
---------	------

5.3.1.28 FCS_IPSEC_EXT.1.14 TSS 1

Objective	The evaluator shall ensure that the TSS describes how the TOE compares the peer’s presented identifier to the reference identifier. This description shall include which field(s) of the certificate are used as the presented identifier (DN, Common Name, or SAN). If the TOE simultaneously supports the same identifier type in the CN and SAN, the TSS shall describe how the TOE prioritizes the comparisons (e.g. the result of comparison if CN matches but SAN does not). If the location (e.g. CN or SAN) of non-DN identifier types must explicitly be configured as part of the reference identifier, the TSS shall state this. If the ST author assigned an additional identifier type, the TSS description shall also include a description of that type and the method by which that type is compared to the peer’s presented certificate, including what field(s) are compared and which fields take precedence in the comparison.
Evaluator Findings	The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS describes how the TOE compares the peer’s presented identifier to the reference identifier. Upon investigation, the evaluator found that the TSS states that The TOE requires that the configured IKE identity of the local and remote endpoints match the contents of the X.509 certificate associated with a SA endpoint. The identity may be an email address, a fully qualified domain name or an IP address. When configuring the IKE identity of the remote endpoint the administrator must specify an email address, fully qualified domain name, or IP address that will be matched against the SAN field, or a distinguished name, in the presented certificate. If the TSF cannot establish a connection to determine the validity of a certificate, the Administrator is prompted to accept or reject the certificate. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.1.29 FCS_IPSEC_EXT.1.14 Guidance 1

Objective	The evaluator shall ensure that the operational guidance describes all supported identifiers, explicitly states whether the TOE supports the SAN extension or not and includes detailed instructions on how to configure the reference identifier(s) used to check the identity of peer(s). If the identifier scheme implemented by the TOE does not guarantee unique identifiers, the evaluator shall ensure that the operational guidance provides a set of warnings and/or CA policy recommendations that would result in secure TOE use.
Evaluator Findings	The evaluator examined the section titled Configuring VPNs in the AGD to verify that it describes all supported identifiers, explicitly states whether the TOE supports the SAN extension or not, and includes detailed instructions on how to configure the reference identifier(s) used to check the identity of peer(s). Upon investigation, the evaluator found that the AGD states that : Configuring Remote IKE IDs

	<p>By default, the IKE ID received from the peer is validated with the IP address configured for the IKE gateway. In certain network setups, the IKE ID received from the peer (the IKE ID can be an IPv4 or IPv6 address, email id, fully qualified domain name (FQDN), or a distinguished name) does not match the IKE gateway configured on the device. This can lead to a Phase 1 validation failure.</p> <p>To configure the IKE ID perform the following steps:</p> <ol style="list-style-type: none"> 1. Configure the remote-identity statement at the set security ike gateway gateway-name hierarchy level to match the IKE ID that is received from the peer. The IKE ID values can be an IPv4 address or an IPv6 address, email id, FQDN, or a distinguished name. 2. On the peer device, ensure that the IKE ID is the same as the remote-identity configured on the device. If the peer device is a Junos OS device, configure the local-identity statement at the set security ike gateway gateway-name hierarchy level. The IKE ID values can be an IPv4 address or an IPv6 address, email id, FQDN, or a distinguished name. <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.3.1.30 FCS_IPSEC_EXT.1 TSS (VPNGWMod)

Objective	All existing activities regarding "Pre-shared keys" apply to all selections including pre-shared keys. If any selection with "Pre-shared keys" is included, the evaluator shall check to ensure that the TSS describes how the selection works in conjunction with the authentication of IPsec connections.
Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to ensure that the TSS describes how the selection works in conjunction with the authentication of IPsec connections. Upon investigation, the evaluator found that the TSS states that</p> <p>The TOE supports IPSec pre-shared keys. It accepts Unicode characters to specify text-based pre-shared keys.</p> <p>The TOE accepts pre-shared text keys and converts the text string into an authentication value as per RFC 2409 for IKEv1 or RFC 4306 for IKEv2, using the PRF that is configured as the hash algorithm for the IKE exchanges.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.3.1.31 FCS_IPSEC_EXT.1.15 Guidance 1

Objective	If any selection with "Pre-shared Keys" is selected, the evaluator shall check that the operational guidance describes any configuration necessary to enable any selected authentication mechanisms.
-----------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Evaluator Findings	<p>The evaluator examined the section titled Configuring an IPsec VPN with a Preshared Key for IKE Authentication in the AGD to verify that If any selection with “Pre-shared Keys” is selected, the operational guidance describes any configuration necessary to enable any selected authentication mechanisms. Upon investigation, the evaluator found that the AGD states that In this section, configuration is given for devices running Junos OS for IPsec VPN using a preshared key as the IKE authentication method. The algorithms used in IKE or IPsec authentication or encryption is shown and the CLI commands needed to configure the TOE for setting up Pre-Shared Keys are mentioned.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.4 TSS and Guidance Activities (NTP)

5.4.1 FCS_NTP_EXT.1

5.4.1.1 FCS_NTP_EXT.1 TSS 1

Objective	<p>The evaluator shall examine the TSS to ensure it identifies the version of NTP supported, how it is implemented and what approach the TOE uses to ensure the timestamp it receives from an NTP timeserver (or NTP peer) is from an authenticated source and the integrity of the time has been maintained.</p>
Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS identifies the version of NTP supported, how it is implemented and what approach the TOE uses to ensure the timestamp it receives from an NTP timeserver (or NTP peer) is from an authenticated source and the integrity of the time has been maintained. Upon investigation, the evaluator found that the TSS states that</p> <p>The TSF supports time updates using NTPv3 and NTPv4. The TSF authentications update using an administrator-configured symmetric key and SHA-1, and SHA-256. The TOE rejects broadcast and multicast time updates. The TOE does not place a limit on the number of NTP time sources that can be configured.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.4.1.2 FCS_NTP_EXT.1 TSS 2

Objective	<p>The TOE must support at least one of the methods or may use multiple methods, as specified in the SFR element 1.2. The evaluator shall ensure that each method selected in the ST is described in the TSS, including the version of NTP supported in element 1.1, the message digest algorithms used to verify the authenticity of the timestamp and/or the protocols used to ensure integrity of the timestamp.</p>
-----------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS describes each method selected in the ST, including the version of NTP supported in element 1.1, the message digest algorithms used to verify the authenticity of the timestamp and/or the protocols used to ensure integrity of the timestamp. Upon investigation, the evaluator found that the TSS states that</p> <p>The TSF supports time updates using NTPv3 and NTPv4. The TSF authentications update using an administrator-configured symmetric key and SHA-1, and SHA-256.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.4.1.3 FCS_NTP_EXT.1.1 Guidance 1

Objective	<p>The evaluator shall examine the guidance documentation to ensure it provides the Security Administrator instructions as how to configure the version of NTP supported, how to configure multiple NTP servers for the TOE's time source and how to configure the TOE to use the method(s) that are selected in the ST.</p>
Evaluator Findings	<p>The evaluator examined the section titled Configuring Network Time Protocol in the AGD to verify that it provides the administrator instructions as how to configure the version of NTP supported, how to configure multiple NTP servers for the TOE's time source and how to configure the TOE to use the method(s) that are selected in the ST. Upon investigation, the evaluator found that the AGD states that :</p> <p>In this section, configuration is given for the device to sync with a Network Time Protocol (NTP) server. This device supports time updates using NTP version 4 and NTP version 3. The device authentications updates using an administrator configured symmetric key, SHA-1 and SHA-256. The device rejects broadcast and multicast time updates. The device does not place a limit on the number of NTP time sources that can be configured.</p> <p>To configure the device in client mode, include the server statement and other optional statements at the [edit system ntp] hierarchy level:</p> <p>[edit system ntp] server address <key key-number> <version value> <prefer>; authentication-key key-number type type value password; trusted-key[key-numbers];</p> <p>Specify the address of the system acting as the time server. Kindly specify an address, not a hostname.</p> <p>To include an authentication key in all messages sent to the time server, include the key option. The key corresponds to the key number specified in the authentication-key statement.</p>

	<p>By default, the device sends NTP version 4 packets to the time server. To set the NTP version level to 3, include the version option.</p> <p>If more than one time server is configured, one server can be marked as preferred by including the prefer option.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.4.1.4 FCS_NTP_EXT.1.2 Guidance 1

Objective	For each of the secondary selections made in the ST, the evaluator shall examine the guidance document to ensure it instructs the Security Administrator how to configure the TOE to use the algorithms that support the authenticity of the timestamp and/or how to configure the TOE to use the protocols that ensure the integrity of the timestamp.
Evaluator Findings	<p>The evaluator examined the section titled Configuring Network Time Protocol in the AGD to verify that, for each of the secondary selections made in the ST, it instructs the administrator how to configure the TOE to use the algorithms that support the authenticity of the timestamp and/or how to configure the TOE to use the protocols that ensure the integrity of the timestamp. Upon investigation, the evaluator found that the AGD states that:</p> <p>The device authentications updates using an administrator configured symmetric key, SHA-1 and SHA-256.</p> <p>The AGD also states that:</p> <p>For common criteria compliance use trusted authentication using SHA1 or SHA256 as the message digest algorithm(s) to make sure that the NTP peer is trusted. The server statement identifies the NTP server used for periodic time synchronization. The source-address statement enables administrator to specify one source address per family for each routing instance, The authentication-key statement specifies that a Sha256 scheme should be used to hash the key value for authentication, which prevents the router or switch from synchronizing with an attacker’s host posing as the time server.</p> <p>[edit]</p> <pre> system { ntp { authentication-key 12 type sha256 value " \$9\$TQFn/9t0OlcYwY4oGU9At"; ## SECRET-DATA server 10.1.4.2 key 12; source-address 10.1.4.3; trusted key 12; } } </pre> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.4.1.5 FCS_NTP_EXT.1.3 Guidance 1

Objective	The evaluator shall examine the guidance documentation to ensure it provides the Security Administrator instructions as how to configure the TOE to not accept broadcast and multicast NTP packets that would result in the timestamp being updated.
Evaluator Findings	The evaluator examined the section titled Configuring Network Time Protocol in the AGD to verify that it provides instructions as how to configure the TOE to not accept broadcast and multicast NTP packets that would result in the timestamp being updated. Upon investigation, the evaluator found that the AGD states that : The device rejects broadcast and multicast time updates. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5 TSS and Guidance Activities (SSH)

5.5.1 FCS_SSHS_EXT.1

5.5.1.1 FCS_SSHS_EXT.1.2 TSS 1 [TD0631]

Objective	The evaluator shall check to ensure that the TSS contains a list of supported public key algorithms that are accepted for client authentication and that this list is consistent with signature verification algorithms selected in FCS_COP.1/SigGen (e.g., accepting EC keys requires corresponding Elliptic Curve Digital Signature algorithm claims). The evaluator shall confirm that the TSS includes the description of how the TOE establishes a user identity when an SSH client presents a public key or X.509v3 certificate. For example, the TOE could verify that the SSH client’s presented public key matches one that is stored within the SSH server’s authorized_keys file. If password-based authentication method has been selected in the FCS_SSHS_EXT.1.2, then the evaluator shall confirm its role in the authentication process is described in the TSS.
Evaluator Findings	The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS contains a description of the public key algorithms that are acceptable for use for authentication and that this list conforms to FCS_COP.1/SigGen. Upon investigation, the evaluator found that the TSS states that The TOE implements an SSH server in accordance with the following. Below are supported Ciphers for SSH v2 KE: DH Group 14 (modp 2048), ECDH-sha2-nistp256, ECDH-sha2-nistp384, ECDH-sha2-nistp521 Authentication: ECDSA P-256, ECDSA P-384, ECDSA P-521 Cipher: AES-CTR-128, AES-CTR-256, AES-CBC-128, AES-CBC-256 Integrity: HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-512

	<p>The evaluator also examined the section titled TOE Summary Specification in the Security Target to verify that that the TSS includes the description of how the TOE establishes a user identity when an SSH client presents a public key. Upon investigation, the evaluator found that the TSS states that</p> <p>The TOE implements public key authentication for SSHv2 session authentication. Authentication succeeds if the correct private key is used. This is verified by checking that the private key corresponds to the public key stored in the authorized_keys file on the TOE filesystem. The TOE does not require multiple authentications (public key and password) for users. The TOE also supports password authentication. Expired passwords are not supported and cannot be used for authentication. The TOE does not support the configuration of host-based authentication methods.</p> <p>Finally, since password-based authentication method has been selected in the FCS_SSHS_EXT.1.2, the evaluator also examined the section titled TOE Summary Specification in the Security Target to verify that its role in the authentication process is described in the TSS. Upon investigation, the evaluator found that the TSS states that</p> <p>TOE does not require multiple authentications (public key and password) for users. The TOE also supports password authentication. Expired passwords are not supported and cannot be used for authentication.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.5.1.2 FCS_SSHS_EXT.1.3 TSS 1

Objective	The evaluator shall check that the TSS describes how “large packets” in terms of RFC 4253 are detected and handled.
Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS describes how “large packets” in terms of RFC 4253 are detected and handled. Upon investigation, the evaluator found that the TSS states that :</p> <p>The TOE reads the packet payload size in the TCP packet to determine the packet length. Packets greater than 256K bytes are dropped and the connection is terminated.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.5.1.3 FCS_SSHS_EXT.1.4 TSS 1

Objective	The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that optional characteristics are specified, and the encryption algorithms supported are specified as well. The evaluator shall check the TSS to ensure that the encryption algorithms specified are identical to those listed for this component.
-----------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<p>Evaluator Findings</p>	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS specifies the optional characteristics and the encryption algorithms supported. Upon investigation, the evaluator found that the TSS states that</p> <p>The TOE implements the following encryption methods for SSH sessions: aes128-cbc, aes256-cbc, aes128-ctr, and aes256-ctr. Negotiation of encryption algorithms in each direction is allowed. Encryption algorithm “none” is not allowed.</p> <p>The evaluator also examined the section titled TOE Summary Specification in the Security Target to verify that the encryption algorithms specified are identical to those listed for this component. Upon investigation, the evaluator found that the two were consistent with each other.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
<p>Verdict</p>	<p>Pass</p>

5.5.1.4 FCS_SSHS_EXT.1.4 Guidance 1

<p>Objective</p>	<p>The evaluator shall also check the guidance documentation to ensure that it contains instructions on configuring the TOE so that SSH conforms to the description in the TSS (for instance, the set of algorithms advertised by the TOE may have to be restricted to meet the requirements).</p>
<p>Evaluator Findings</p>	<p>The evaluator examined the section titled Configuring SSH and Console Connection in the AGD to verify that it contains instructions on configuring the TOE so that SSH conforms to the description in the TSS. Upon investigation, the evaluator found that the AGD states that AGD describes the configuration of SSH on the TOE. Specifically, the evaluator found that AGD describes the following characteristics of SSH configuration,</p> <ul style="list-style-type: none"> • System Login Message and Announcement • Limiting the Number of User Login Attempts • Specifying Host-key Algorithms • Specifying key exchange Algorithms • Specifying ciphers allowed • Specifying all the permissible message authentication code algorithms. <p>The evaluator found that AGD describes the configuration of SSH from the CLI. Finally, the evaluator compared the configuration described in AGD to the TSS of ST. The evaluator found that the configuration options in AGD are consistent with the description of SSH in the TSS.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
<p>Verdict</p>	<p>Pass</p>

5.5.1.5 FCS_SSHS_EXT.1.5 TSS 1 [TD0631]

Objective	The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that the SSH server’s host public key algorithms supported are specified and that they are identical to those listed for this component.
Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS specifies the optional characteristics and the public key algorithms supported. Upon investigation, the evaluator found that the TSS states that</p> <p>The TOE implements all mandatory algorithms and methods and may be configured to accept public-key based and/or password-based authentication. Multiple authentication mechanisms for users is not required. Port forwarding and sessions to clients are allowed. X11 forwarding is prohibited.</p> <p>The TOE does not accept the “none” cipher and implements AES-CBC-128, AES-CBC-256, AES-CTR-128, AES-CTR-256 for the protection of data over SSH and uses keys generated in accordance “ecdsa-sha2-nistp256, ecdsa-sha2-nistp384 and ecdsa-sha2-nistp521” for public-key based device authentication.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.5.1.6 FCS_SSHS_EXT.1.5 Guidance 1

Objective	The evaluator shall also check the guidance documentation to ensure that it contains instructions on configuring the TOE so that SSH conforms to the description in the TSS (for instance, the set of algorithms advertised by the TOE may have to be restricted to meet the requirements).
Evaluator Findings	<p>The evaluator examined the section titled Configuring SSH and Console Connection in the AGD to verify that it contains instructions on configuring the TOE so that SSH conforms to the description in the TSS. Upon investigation, the evaluator found that the AGD states that</p> <p>NOTE: For Common Criteria compliance use below host key algorithms :</p> <p>ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521</p> <p>AGD also describes the configuration of SSH on the TOE. Specifically, the evaluator found that AGD describes the following characteristics of SSH configuration:</p> <ul style="list-style-type: none"> • System Login Message and Announcement • Limiting the Number of User Login Attempts • Specifying Host-key Algorithms • Specifying key exchange Algorithms • Specifying ciphers allowed • Specifying all the permissible message authentication code algorithms.

	The evaluator found that AGD describes the configuration of SSH from the CLI. Finally, the evaluator compared the configuration described in AGD to the TSS of ST. The evaluator found that the configuration options in AGD are consistent with the description of SSH in the TSS. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.7 FCS_SSHS_EXT.1.6 TSS 1

Objective	The evaluator shall check the TSS to ensure that it lists the supported data integrity algorithms, and that the list corresponds to the list in this component.
Evaluator Findings	The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS lists the supported data integrity algorithms, and that that list corresponds to the list in this component. Upon investigation, the evaluator found that the TSS states that The TOE implements an SSH server in accordance with the following. Integrity: HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-512 Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.8 FCS_SSHS_EXT.1.6 Guidance 1

Objective	The evaluator shall also check the guidance documentation to ensure that it contains instructions to the Security Administrator on how to ensure that only the allowed data integrity algorithms are used in SSH connections with the TOE (specifically, that the “none” MAC algorithm is not allowed).
Evaluator Findings	The evaluator examined the section titled Configuring SSH on the Evaluated Configuration for NDcPP in the AGD to verify that it contains instructions to the administrator on how to ensure that only the allowed data integrity algorithms are used in SSH connections with the TOE. Further, it was verified that ‘none’ is not a permissible MAC algorithm. Specify all the permissible message authentication code algorithms for SSHv2 [edit] user@host#set system services ssh macs hmac-sha1 user@host#set system services ssh macs hmac-sha2-256 user@host#set system services ssh macs hmac-sha2-512 Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.9 FCS_SSHS_EXT.1.7 TSS 1

Objective	The evaluator shall check the TSS to ensure that it lists the supported key exchange algorithms, and that the list corresponds to the list in this component.
Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS lists the supported key exchange algorithms, and that that list corresponds to the list in this component. Upon investigation, the evaluator found that the TSS states that :</p> <p>Key exchange is performed only using the supported key exchange algorithms ordered as follows: ecdh-sha2-nistp256 (RFC 5656), ecdh-sha2-nistp384 (RFC 5656), ecdh-sha2-nistp521 (RFC 5656), diffie-hellman-group14-sha1 (RFC 4253).</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.5.1.10 FCS_SSHS_EXT.1.7 Guidance 1

Objective	The evaluator shall also check the guidance documentation to ensure that it contains instructions to the Security Administrator on how to ensure that only the allowed key exchange algorithms are used in SSH connections with the TOE.
Evaluator Findings	<p>The evaluator examined the section titled Configuring SSH on the Evaluated Configuration in the AGD to verify that it contains instructions to the administrator on how to ensure that only the allowed key exchange algorithms are used in SSH connections with the TOE. Upon investigation, the evaluator found that the AGD states that :</p> <p>Specify the SSH key-exchange algorithms.</p> <p>[edit system services ssh]</p> <p>user@host#set key-exchange [ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 Diffiehellman-group14-sha1]</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.5.1.11 FCS_SSHS_EXT.1.8 TSS 1

Objective	<p>The evaluator shall check that the TSS specifies the following:</p> <ul style="list-style-type: none"> a) Both thresholds are checked by the TOE. b) Rekeying is performed upon reaching the threshold that is hit first.
Evaluator Findings	The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS specifies that both thresholds are checked and that rekeying is performed upon reaching the threshold that is hit first. Upon investigation, the evaluator found that the TSS states that

	<p>For ciphers whose block size ≥ 16, the TOE rekeys every $(2^{32}-1)$ bytes. The client may request a rekeying event as a valid SSHv2 message at any time and the TOE will honor this request. Re-keying of session keys can be configured using the <code>sshd_config</code> knob. The data-limit must be set between 51200 and 1Gbyte and the time-limit must be set within 1 and 60 minutes. The TOE will rekey based on whichever limit is reached first.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.5.1.12 FCS_SSHS_EXT.1.8 Guidance 1

Objective	<p>If one or more thresholds that are checked by the TOE to fulfil the SFR are configurable, then the evaluator shall check that the guidance documentation describes how to configure those thresholds. Either the allowed values are specified in the guidance documentation and must not exceed the limits specified in the SFR (one hour of session time, one gigabyte of transmitted traffic) or the TOE must not accept values beyond the limits specified in the SFR. The evaluator shall check that the guidance documentation describes that the TOE reacts to the first threshold reached.</p>
Evaluator Findings	<p>The evaluator examined the section titled Understanding FIPS Authentication Methods in the AGD to verify that it describes how to configure any thresholds that are configurable. Upon investigation, the evaluator found that the AGD states that the AGD specifically addresses the configuration of the rekey limits for TOE SSH connections. The AGD identifies the method of configuring either time-limit or data-limit values via the CLI. The evaluator found provided instructions include the specific configurations required to ensure only approved limits are used in SSH connection with the TOE. This was confirmed by comparing the instructions in AGD to the description of rekey limits found in the TSS of ST.</p> <p>The AGD states that:</p> <p>Thresholds for SSH rekeying can be configured. The TSF ensures that within the SSH connections the same session keys are used for a threshold of no longer than one hour, and no more than one gigabyte of the transmitted data. When either of the thresholds are reached, a rekey must be performed.</p> <pre>[edit system login] user@host# set services ssh rekey time-limit number</pre> <p>Time limit before renegotiating session keys is 1 through 1440 minutes.</p> <pre>[edit system login] user@host# set services ssh rekey data-limit number</pre>

	<p>Data limit before renegotiating session keys is 51200 through 4294967295 byte.</p> <p>The evaluator also examined the section titled Understanding FIPS Authentication Methods in the AGD to verify that the guidance documentation describes that the TOE reacts to the first threshold reached. Upon investigation, the evaluator found that the AGD states that</p> <p>The TSF ensures that within the SSH connections the same session keys are used for a threshold of no longer than one hour, and no more than one gigabyte of the transmitted data. When either of the thresholds are reached, a rekey must be performed.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.6 TSS and Guidance Activities (User Data Protection)

5.6.1 FDP_RIP.2

5.6.1.1 FDP_RIP.2 TSS 1

Objective	<p>“Resources” in the context of this requirement are network packets being sent through (as opposed to “to”, as is the case when a security administrator connects to the TOE) the TOE. The concern is that once a network packet is sent, the buffer or memory area used by the packet still contains data from that packet, and that if that buffer is re-used, those data might remain and make their way into a new packet. The evaluator shall check to ensure that the TSS describes packet processing to the extent that they can determine that no data will be reused when processing network packets. The evaluator shall ensure that this description at a minimum describes how the previous data are zeroized/overwritten, and at what point in the buffer processing this occurs.</p>
Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS describes packet processing to the extent that they can determine that no data will be reused when processing network packets. Upon investigation, the evaluator found that the TSS states that</p> <p>The TOE reads incoming data from network interfaces and stores the assembled datagrams in a temporary data structure. After a datagram is processed, the content of the structure is cleared prior to the storing and processing of the next datagram.</p> <p>The evaluator examined the section titled TOE Summary Specification in the Security Target to ensure that this description at a minimum describes how the previous data are zeroized/overwritten, and at what point in the buffer processing this occurs. Upon investigation, the evaluator found that the TSS states that</p>

	<p>The TOE keeps track of the length of each datagram. When erasing the content, the data structure is padded with zeros to ensure that the entire structure is cleared prior to the accepting the next datagram.</p> <p>This ensures that no residual data of previously processed datagram may affect the inspection of the current datagram.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.7 TSS and Guidance Activities (Firewall)

5.7.1 FFW_RUL_EXT.1

5.7.1.1 FFW_RUL_EXT.1 TSS

Objective	<p>The evaluator shall verify that the TSS provides a description of the TOE's initialization/startup process, which clearly indicates where processing of network packets begins to take place, and provides a discussion that supports the assertion that packets cannot flow during this process.</p> <p>The evaluator shall verify that the TSS also include a narrative that identifies the components (e.g., active entity such as a process or task) involved in processing the network packets and describe the safeguards that would prevent packets flowing through the TOE without applying the ruleset in the event of a component failure. This could include the failure of a component, such as a process being terminated, or a failure within a component, such as memory buffers full and cannot process packets. The description shall also include a description how the TOE behaves in the situation where the traffic exceeds the amount of traffic the TOE can handle and how it is ensured that also in this condition stateful traffic filtering rules are still applied so that traffic does not pass that shouldn't pass according to the specified rules.</p>
Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS provides a description of the TOE's initialization/startup proces and provides a discussion that supports the assertion that packets cannot flow during this process. Upon investigation, the evaluator found that the TSS states that</p> <p>When the TOE boots up, it executes a suite of self-tests. Only if each self-test passes, shall the boot sequence commence. The exact boot sequence is the following:</p> <ul style="list-style-type: none"> • BIOS hardware and memory checks, • Loading and initialization of the Kernel OS, • FIPS self-tests and firmware integrity tests,

	<ul style="list-style-type: none"> • The init utility is started to mount file systems, set up network cards, and to start the processes that are run on system at startup, • Internet Service Daemon, Routing Protocol Daemon and Syslog Daemon are started, Routing and forwarding tables are initialized, • Management Daemon (or MGD) is started, and • Physical interfaces are activated. <p>The network interfaces are only activated when all functions required for processing the datagrams are verified and loaded. This ensures that the TOE is fully operational, and the rules enforced before the physical interfaces may receive any traffic.</p> <p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS includes a narrative that identifies the components involved in processing the network packets, describes the safeguards that would prevent packets flowing through the TOE without applying the ruleset in the event of a component failure and describes how the TOE behaves in the situation where the traffic exceeds the amount of traffic the TOE can handle. Upon investigation, the evaluator found that the TSS states that Packet processing is controlled by a Flow Daemon. If for any reason the Flow Daemon fails, the processing of the packets will stop, and none will be forwarded. A failure in other Daemons will not prevent the Flow Daemon from enforcing the TOE security policies. Also, any failure of the Flow Daemon will stop all processing of the packets. This ensures that packets will only be processed by a correctly functioning Flow Daemon.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.7.1.2 FFW_RUL_EXT.1.2/FFW_RUL_EXT.1.3/FFW_RUL_EXT.1.4 TSS

Objective	<p>The evaluator shall verify that the TSS describes a stateful packet filtering policy and the following attributes are identified as being configurable within stateful traffic filtering rules for the associated protocols:</p> <ul style="list-style-type: none"> • ICMPv4 <ul style="list-style-type: none"> ○ Type ○ Code • ICMPv6 <ul style="list-style-type: none"> ○ Type ○ Code • IPv4 <ul style="list-style-type: none"> ○ Source address ○ Destination Address ○ Transport Layer Protocol • IPv6
-----------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	<ul style="list-style-type: none"> ○ Source address ○ Destination Address ○ Transport Layer Protocol and where defined by the ST author, Extension Header Type, Extension Header Fields ● TCP <ul style="list-style-type: none"> ○ Source Port ○ Destination Port ● UDP <ul style="list-style-type: none"> ○ Source Port ○ Destination Port <p>The evaluator shall verify that each rule can identify the following actions: permit or drop with the option to log the operation. The evaluator shall verify that the TSS identifies all interface types subject to the stateful packet filtering policy and explains how rules are associated with distinct network interfaces.</p>
<p>Evaluator Findings</p>	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS describes a stateful packet filtering policy and the attributes listed above are identified as being configurable within stateful traffic filtering rules for the associated protocols. Upon investigation, the evaluator found that the TSS states that :</p> <p>The TOE allows Administrator to configure the stateful packet filtering rules. The rules are applied to all network traffic processed by the TOE. The TOE is configured to associate network interfaces to IP subnets. Source IP addresses are then associated with the network interface.</p> <p>The TOE performs stateful network traffic filtering on network packets using the following network traffic protocols and network fields conforming to the described RFCs:</p> <ul style="list-style-type: none"> ● RFC 792 ICMPv4: Type, Code ● RFC 4443 ICMPv6: Type, Code ● RFC 791 (IPv4): Source address, Destination Address, Transport Layer Protocol ● RFC 2460 (IPv6): Source address, Destination Address, Transport Layer Protocol ● RFC 793 (TCP): Source port, Destination port ● RFC 768 (UDP): Source port, Destination port <p>Conformance to these RFCs is demonstrated by protocol compliance testing by the product QA team.</p> <p>The evaluator also examined the section titled TOE Summary Specification in the Security Target to verify that each rule can identify the following actions: permit or drop with the option to log the operation. Upon investigation, the evaluator found that the TSS states that</p> <p>The TOE shall allow permit, deny, and log operations to be associated with rules</p>

	<p>Finally the evaluator also examined the section titled TOE Summary Specification in the Security Target to verify that the TSS identifies all interface types subject to the stateful packet filtering policy and explains how rules are associated with distinct network interfaces. Upon investigation, the evaluator found that the TSS states that</p> <p>The TOE is configured to associate network interfaces to IP subnets. Source IP addresses are then associated with the network interface.</p> <p>The TOE shall allow permit, deny, and log operations to be associated with rules and these rules can be assigned to distinct network interfaces.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.7.1.3 FFW_RUL_EXT.1.2/FFW_RUL_EXT.1.3/FFW_RUL_EXT.1.4 Guidance

Objective	<p>The evaluators shall verify that the guidance documentation identifies the following attributes as being configurable within stateful traffic filtering rules for the associated protocols:</p> <ul style="list-style-type: none"> • ICMPv4 <ul style="list-style-type: none"> ○ Type ○ Code • ICMPv6 <ul style="list-style-type: none"> ○ Type ○ Code • IPv4 <ul style="list-style-type: none"> ○ Source address ○ Destination Address ○ Transport Layer Protocol • IPv6 <ul style="list-style-type: none"> ○ Source address ○ Destination Address ○ Transport Layer Protocol and where defined by the ST author, Extension Header Type, Extension Header Fields • TCP <ul style="list-style-type: none"> ○ Source Port ○ Destination Port • UDP <ul style="list-style-type: none"> ○ Source Port ○ Destination Port <p>The evaluator shall verify that the guidance documentation indicates that each rule can identify the following actions: permit, drop, and log.</p>
-----------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	The evaluator shall verify that the guidance documentation explains how rules are associated with distinct network interfaces.
Evaluator Findings	<p>The evaluator examined the section titled Configuring Traffic Filtering Rules in the AGD to verify that it identifies the attributes listed above as being configurable within stateful traffic filtering rules for the associated protocols. Upon investigation, the evaluator found that the subsection titled Understanding Protocol Support in the AGD states that</p> <p>Here, Configuration is given for the devices running Junos OS to perform stateful network traffic filtering on network packets using network traffic protocols and network fields as described in Table 12 on page 212.</p> <p>The evaluator examined the section titled Configuring Traffic Filtering Rules in the AGD to verify that the guidance documentation indicates that each rule can identify the following actions: permit, drop, and log. Upon investigation, the evaluator found that the Subsection titled Overview in the AGD states that</p> <p>The security policy rule set is an ordered list of security policy entries enforced by the firewall rules, each of which contains the specification of a network flow and an action:</p> <ul style="list-style-type: none"> • Source IP address and network mask • Destination IP address and network mask • Protocol • Source port • Destination port • Action: permit, deny, drop silently, log <p>The evaluator examined the section titled Configuring Traffic Filtering Rules in the AGD to verify that the guidance documentation explains how rules are associated with distinct network interfaces. Upon investigation, the evaluator found that the Subsection titled Configuring Traffic Filter Rules in the AGD states that</p> <p>Traffic filter rules can be configured on a device to enforce validation against protocols attributes and direct traffic accordingly to the configured attributes. These rules are based on zones on which network interfaces are bound.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.7.1.4 FFW_RUL_EXT.1.5 TSS

Objective	<p>The evaluator shall verify that the TSS identifies the protocols that support stateful session handling. The TSS shall identify TCP, UDP, and, if selected by the ST author, ICMP.</p> <p>The evaluator shall verify that the TSS describes how stateful sessions are established (including handshake processing) and maintained.</p> <p>The evaluator shall verify that for TCP, the TSS identifies and describes the use of the following attributes in session determination: source and destination addresses, source and destination ports, sequence number, and individual flags.</p> <p>The evaluator shall verify that for UDP, the TSS identifies and describes the following attributes in session determination: source and destination addresses, source and destination ports.</p> <p>The evaluator shall verify that for ICMP (if selected), the TSS identifies and describes the following attributes in session determination: source and destination addresses, other attributes chosen in FFW_RUL_EXT.1.5.</p> <p>The evaluator shall verify that the TSS describes how established stateful sessions are removed. The TSS shall describe how connections are removed for each protocol based on normal completion and/or timeout conditions. The TSS shall also indicate when session removal becomes effective (e.g., before the next packet that might match the session is processed).</p>
Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS identifies the protocols that support stateful session handling. Upon investigation, the evaluator found that the TSS states that:</p> <p>The TOE accepts network packets if it matches an established TCP, UDP or ICMP session using:</p> <ul style="list-style-type: none"> • TCP: source and destination addresses, source and destination ports, sequence number, flags • UDP: source and destination addresses, source and destination ports • ICMP: source and destination addresses, type, code <p>The evaluator also examined the section titled TOE Summary Specification in the Security Target to verify that the TSS describes how stateful sessions are established (including handshake processing) and maintained. Upon investigation, the evaluator found that the TSS states that:</p> <p>The TOE will remove existing traffic flows due to session inactivity timeout, or completion of the session.</p> <p>The TOE supports FTP (RFC 959) to dynamically establish sessions allowing network traffic according to Administrator rules.</p>

The evaluator next examined the section titled **TOE Summary Specification** in the Security Target to verify that for TCP, the TSS identifies and describes the use of the following attributes in session determination: source and destination addresses, source and destination ports, sequence number, and individual flags. Upon investigation, the evaluator found that the TSS states that:

The TOE accepts network packets if it matches an established TCP, UDP or ICMP session using:

- **TCP: source and destination addresses, source and destination ports, sequence number, flags**

The evaluator also examined the section titled **TOE Summary Specification** in the Security Target to verify that for UDP, the TSS identifies and describes the following attributes in session determination: source and destination addresses, source and destination ports. Upon investigation, the evaluator found that the TSS states that:

The TOE accepts network packets if it matches an established TCP, UDP or ICMP session using:

- **UDP: source and destination addresses, source and destination ports**

The evaluator next examined the section titled **TOE Summary Specification** in the Security Target to verify that for ICMP, the TSS identifies and describes the following attributes in session determination: source and destination addresses, other attributes chosen in FFW_RUL_EXT.1.5. Upon investigation, the evaluator found that the TSS states that:

The TOE accepts network packets if it matches an established TCP, UDP or ICMP session using:

- **ICMP: source and destination addresses, type, code**

Finally, the evaluator examined the section titled **TOE Summary Specification** in the Security Target to verify that the TSS describes how established stateful sessions are removed, connections are removed for each protocol based on normal completion and/or timeout conditions and indicate when session removal becomes effective. Upon investigation, the evaluator found that the TSS states that:

The TOE will remove existing traffic flows due to session inactivity timeout, or completion of the session.

The TOE can be configured to drop connection attempts after a defined number of half-open TCP connections using the Junos screen 'tcp syn-flood', which provides both source and destination thresholds on the number of uncompleted TCP connections, as well as a timeout period. The source threshold option allows administrators to specify the number of SYN segments received per second from a single source IP address—regardless of the destination IP address—before Junos OS begins dropping connection requests from that source. Similarly, the destination threshold option allows administrators to specify the

	<p>number of SYN segments received per second for a single destination IP address before Junos OS begins dropping connection requests to that destination.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.7.1.5 FFW_RUL_EXT.1.5 Guidance

Objective	The evaluator shall verify that the guidance documentation describes stateful session behaviors. For example, a TOE might not log packets that are permitted as part of an existing session.
Evaluator Findings	<p>The evaluator examined the section titled Configuring Security Flow Policies in the AGD to verify that it describes stateful session behaviors. Upon investigation, the evaluator found that the AGD states:</p> <p>For more information on stateful session behavior, see Traffic Processing on SRX Series Devices https://www.juniper.net/documentation/us/en/software/junos/flow-packet-processing/topics/topic-map/security-srx-devices-processing-overview.html</p> <p>The weblink mentioned above is provided as pdf and contains below information:</p> <p>Flow-based packet processing, which is stateful, requires the creation of sessions. A session is created for the first packet of a flow for the following purposes:</p> <ul style="list-style-type: none"> • To store most of the security measures to be applied to the packets of the flow. • To cache information about the state of the flow. • For example, logging and counting information for a flow is cached in its session. (Some stateful firewall screens rely on threshold values that pertain to individual sessions or across all sessions.) • To allocate required resources for the flow for features such as NAT. • To provide a framework for features such as ALGs and firewall features. <p>Flow-based packet processing, which is stateful, requires the creation of sessions. Sessions are created based on routing and other traffic classification information to store information and allocate resources for a flow. Sessions cache information about the state of the flow, and they store most of the security measures to be applied to packets of the flow. Because of the architectural differences across devices, sessions are also managed differently by different devices.</p> <p>Regardless of these differences, conceptually the flow process is the same across all services gateways, and sessions serve the same purposes and have the same features.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.7.1.6 FFW_RUL_EXT.1.6 TSS

<p>Objective</p>	<p>The evaluator shall verify that the TSS identifies the following as packets that will be automatically dropped and are counted or logged:</p> <ul style="list-style-type: none"> a) Packets which are invalid fragments, including a description of what constitutes an invalid fragment b) Fragments that cannot be completely re-assembled c) Packets where the source address is defined as being on a broadcast network d) Packets where the source address is defined as being on a multicast network e) Packets where the source address is defined as being a loopback address f) The TSF shall reject and be capable of logging network packets where the source or destination address of the network packet is defined as being unspecified (i.e. 0.0.0.0) or an address “reserved for future use” (i.e. 240.0.0.0/4) as specified in RFC 5735 for IPv4; g) The TSF shall reject and be capable of logging network packets where the source or destination address of the network packet is defined as an “unspecified address” or an address “reserved for future definition and use” (i.e. unicast addresses not in this address range: 2000::/3) as specified in RFC 3513 for IPv6; h) Packets with the IP options: Loose Source Routing, Strict Source Routing, or Record Route specified i) Other packets defined in FFW_RUL_EXT.1.6 (if any)
<p>Evaluator Findings</p>	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS identifies the items listed above as packets that will be automatically dropped and are counted or logged. Upon investigation, the evaluator found that the TSS states that :</p> <p>The TOE enforces the following default reject rules with logging on all network traffic:</p> <ul style="list-style-type: none"> • invalid fragments; • fragmented IP packets which cannot be re-assembled completely; • where the source address is equal to the address of the network interface where the network packet was received; • where the source address does not belong to the networks associated with the network interface where the network packet was received; • where the source address is defined as being on a broadcast network; • where the source address is defined as being on a multicast network; • where the source address is defined as being a loopback address; • packets where the source or destination address is a link-local address; • where the source or destination address is defined as being an address “reserved for future use” as specified in RFC 5735 for IPv4;

	<ul style="list-style-type: none"> • where the source or destination address is defined as an “unspecified address” or an address “reserved for future definition and use” as specified in RFC 3513 for IPv6; • with the IP options: Loose Source Routing, Strict Source Routing, or Record Route specified; • packets are checked for validity. “Invalid fragments” are those that violate these rules: <ul style="list-style-type: none"> ○ No overlap ○ The total fragments in one packet should not be more than 62 pieces ○ The total length of merged fragments should not larger than 64k ○ All fragments in one packet should arrive in 2 seconds ○ The total queued fragments has limitation, depending on the platform ○ The total number of concurrent fragment processing for different packet has limitations depending on platform <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.7.1.7 FFW_RUL_EXT.1.6 Guidance

Objective	The evaluator shall verify that the guidance documentation describes packets that are discarded and potentially logged by default. If applicable protocols are identified, their descriptions need to be consistent with the TSS. If logging is configurable, the evaluator shall verify that applicable instructions are provided to configure auditing of automatically rejected packets.
Evaluator Findings	The evaluator examined the section titled Configuring Default Deny-All and Reject Rules in the AGD to verify that it describes packets that are discarded and potentially logged by default. Upon investigation, the evaluator found that the AGD states the default reject rules and the CLI commands to configure the same with logging. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.1.8 FFW_RUL_EXT.1.7 TSS

Objective	The evaluator shall verify that the TSS explains how the following traffic can be dropped and counted or logged: <ul style="list-style-type: none"> a) Packets where the source address is equal to the address of the network interface where the network packet was received b) Packets where the source or destination address of the network packet is a link-local address
-----------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	<p>c) Packets where the source address does not belong to the networks associated with the network interface where the network packet was received, including a description of how the TOE determines whether a source address belongs to a network associated with a given network interface</p>
<p>Evaluator Findings</p>	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS explains how the required traffic can be dropped and counted or logged. Upon investigation, the evaluator found that the TSS states that :</p> <p>The TOE enforces the following default reject rules with logging on all network traffic:</p> <ul style="list-style-type: none"> • invalid fragments; • fragmented IP packets which cannot be re-assembled completely; • where the source address is equal to the address of the network interface where the network packet was received; • where the source address does not belong to the networks associated with the network interface where the network packet was received; • where the source address is defined as being on a broadcast network; • where the source address is defined as being on a multicast network; • where the source address is defined as being a loopback address; • packets where the source or destination address is a link-local address; • where the source or destination address is defined as being an address “reserved for future use” as specified in RFC 5735 for IPv4; • where the source or destination address is defined as an “unspecified address” or an address “reserved for future definition and use” as specified in RFC 3513 for IPv6; • with the IP options: Loose Source Routing, Strict Source Routing, or Record Route specified; • packets are checked for validity. “Invalid fragments” are those that violate these rules: <ul style="list-style-type: none"> ○ No overlap ○ The total fragments in one packet should not be more than 62 pieces ○ The total length of merged fragments should not larger than 64k ○ All fragments in one packet should arrive in 2 seconds ○ The total queued fragments has limitation, depending on the platform ○ The total number of concurrent fragment processing for different packet has limitations depending on platform <p>The TSS also states that The TOE is configured to associate network interfaces to IP subnets. Source IP addresses are then associated with the network interface.</p>

	Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.1.9 FFW_RUL_EXT.1.7 Guidance

Objective	The evaluator shall verify that the guidance documentation describes how the TOE can be configured to implement the required rules. If logging is configurable, the evaluator shall verify that applicable instructions are provided to configure auditing of automatically rejected packets.
Evaluator Findings	The evaluator examined the section titled Configuring Traffic Filter Rules and Logging the Dropped Packets Using Default Deny-all Option in the AGD to verify that it describes how the TOE can be configured to implement the required rules and, if logging is configurable, provides instructions to configure auditing of automatically rejected packets. Upon investigation, the evaluator found that the AGD states the CLI commands needed to configure the TOE to implement required traffic filtering rules and to configure logging for automatically rejected packets. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.1.10 FFW_RUL_EXT.1.8 TSS 1

Objective	The evaluator shall verify that the TSS describes the algorithm applied to incoming packets, including the processing of default rules, determination of whether a packet is part of an established session, and application of administrator defined and ordered ruleset.
Evaluator Findings	The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS describes the algorithm applied to incoming packets, including the processing of default rules, determination of whether a packet is part of an established session, and application of administrator defined and ordered ruleset. Upon investigation, the evaluator found that the TSS states that: <ul style="list-style-type: none"> • Session Lookup module performs lookups in the session table used for all interfaces based on the information on incoming packets. The TSS also states that: <ul style="list-style-type: none"> • The Security Policy module examines traffic passing through the TOE (via Session Setup module) and determines if the traffic can pass based on administrator-configured access policies. The Security Policy module is policy enforcement engine that fulfills the security requirements of the user. The Security Policy module only allows traffic if the policy rule base contains a rule explicitly allowing the traffic. • The RPD (Routing Protocol Daemon) module provides the implementations and algorithms for the routing protocols and route calculations. Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass
---------	------

5.7.1.11 FFW_RUL_EXT.1.8 TSS 2 [TD0545]

Objective	If the TOE implements a mechanism that ensures that no conflicting rules can be configured, the TSS shall describe the underlying mechanism.
Evaluator Findings	The evaluator examined the section titled TOE Summary Specification in the Security Target and determined that the TOE does not implement a mechanism that ensures that no conflicting rules can be configured. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.1.12 FFW_RUL_EXT.1.8 Guidance

Objective	The evaluator shall verify that the guidance documentation describes how the order of stateful traffic filtering rules is determined and provides the necessary instructions so that an administrator can configure the order of rule processing.
Evaluator Findings	The evaluator examined the section titled Configuring Traffic Filtering Rules in the AGD to verify that it describes how the order of stateful traffic filtering rules is determined and provides the necessary instructions so that an administrator can configure the order of rule processing. Upon investigation, the evaluator found that the AGD states that: The security policy rule set is an ordered list of security policy entries enforced by the firewall rules, each of which contains the specification of a network flow and an action The AGD also states that : Each packet is compared against entries in the security policy rule set in sequential order until one is found that matches the specification in the policy, or until the end of the rule set is reached, in which case the implicit default policy is implemented and the packet is discarded. Traffic filter rules can be configured on a device to enforce validation against protocols attributes and direct traffic accordingly to the configured attributes. These rules are based on zones on which network interfaces are bound. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.1.13 FFW_RUL_EXT.1.9 TSS

Objective	The evaluator shall verify that the TSS describes the process for applying stateful traffic filtering rules and also that the behavior (either by default, or as configured by the administrator) is to deny packets when there is no rule match unless another required conditions allows the network traffic (i.e., FFW_RUL_EXT.1.5 or FFW_RUL_EXT.2.1).
-----------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS describes the process for applying stateful traffic filtering rules and states that the behavior is to deny packets when there is no rule match unless another required condition allows the network traffic. Upon investigation, the evaluator found that the TSS states that:</p> <p>The TOE allows Administrator to configure the stateful packet filtering rules. The rules are applied to all network traffic processed by the TOE. The TOE is configured to associate network interfaces to IP subnets. Source IP addresses are then associated with the network interface.</p> <p>The Security Policy module only allows traffic if the policy rule base contains a rule explicitly allowing the traffic.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.7.1.14 FFW_RUL_EXT.1.9 Guidance

Objective	The evaluator shall verify that the guidance documentation describes the behavior if no rules or special conditions apply to the network traffic. If the behavior is configurable, the evaluator shall verify that the guidance documentation provides the appropriate instructions to configure the behavior to deny packets with no matching rules.
Evaluator Findings	<p>The evaluator examined the section titled Configuring Default Deny-All and Reject Rules in the AGD to verify that it describes the behavior if no rules or special conditions apply to the network traffic and, if the behavior is configurable, provides the appropriate instructions to configure the behavior to deny packets with no matching rules. Upon investigation, the evaluator found that the AGD states that :</p> <p>By default, security devices running Junos OS deny traffic unless rules are explicitly created to allow it using the following command and then also states the CLI command needed to configure this behavior.</p> <p>Provided CLI command is mentioned as :</p> <p>user@host#set security policies default-policy deny-all</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.7.1.15 FFW_RUL_EXT.1.10 TSS

Objective	The evaluator shall verify that the TSS describes how the TOE tracks and maintains information relating to the number of half-open TCP connections. The TSS should identify how the TOE behaves when the administratively defined limit is reached and should describe under what circumstances stale half-open connections are removed (e.g. after a timer expires).
-----------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<p>Evaluator Findings</p>	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS describes how the TOE tracks and maintains information relating to the number of half-open TCP connections. Upon investigation, the evaluator found that the TSS states that:</p> <p>The TOE can be configured to drop connection attempts after a defined number of half-open TCP connections using the Junos screen ‘tcp syn-flood’, which provides both source and destination thresholds on the number of uncompleted TCP connections, as well as a timeout period. The source threshold option allows administrators to specify the number of SYN segments received per second from a single source IP address—regardless of the destination IP address—before Junos OS begins dropping connection requests from that source. Similarly, the destination threshold option allows administrators to specify the number of SYN segments received per second for a single destination IP address before Junos OS begins dropping connection requests to that destination.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
<p>Verdict</p>	<p>Pass</p>

5.7.1.16 FFW_RUL_EXT.1.10 Guidance 1

<p>Objective</p>	<p>The evaluator shall verify that the guidance documentation describes the behaviour of imposing TCP half-open connection limits and its default state if unconfigured. The evaluator shall verify that the guidance clearly indicates the conditions under which new connections will be dropped e.g. per-destination or per-client.</p>
<p>Evaluator Findings</p>	<p>The evaluator examined the section titled Configuring Network Attacks in the AGD to verify that it describes the behaviour of imposing TCP half-open connection limits and its default state if unconfigured. Upon investigation, the evaluator found that the AGD mentions that the device begins dropping connection requests from the configured source or destination once it hits the configured threshold.</p> <p>The evaluator examined the section titled Configuring Network Attacks in the AGD to verify that the guidance clearly indicates the conditions under which new connections will be dropped. Upon investigation, the evaluator found that the AGD mentions that the TOE supports both source and destination-based thresholds for dropping half-open TCP connections.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
<p>Verdict</p>	<p>Pass</p>

5.7.2 FFW_RUL_EXT.2

5.7.2.1 FFW_RUL_EXT.2.1 TSS

Objective	<p>The evaluator shall verify that the TSS identifies the protocols that can cause the automatic creation of dynamic packet filtering rules. In some cases rather than creating dynamic rules, the TOE might establish stateful sessions to support some identified protocol behaviors.</p> <p>The evaluator shall verify that the TSS explains the dynamic nature of session establishment and removal. The TSS also shall explain any logging ramifications.</p> <p>The evaluator shall verify that for each of the protocols selected, the TSS explains the dynamic nature of session establishment and removal specific to the protocol.</p>
Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS identifies the protocols that can cause the automatic creation of dynamic packet filtering rules. Upon investigation, the evaluator found that the TSS states that</p> <p>The TOE supports FTP (RFC 959) to dynamically establish sessions allowing network traffic according to Administrator rules.</p> <p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS explains the dynamic nature of session establishment and removal, along with logging ramifications. Upon investigation, the evaluator found that the TSS states that</p> <p>Junos implements what is referred to as an Application Layer gateway (ALG) that inspects FTP traffic to determine the port number used for data sessions. The ALG permits data traffic for the duration of the session, closing the port when the session ends.</p> <p>Session events will be logged in accordance with ‘log’ operations defined in the rules. Source and destination addresses, source and destination ports, transport layer protocol, and TOE Interface are recorded in each log record.</p> <p>FTP is the only selected protocol so the latter part of the TSS activity is not applicable.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.7.2.2 FFW_RUL_EXT.2.1 Guidance

Objective	<p>The evaluator shall verify that the guidance documentation describes dynamic session establishment capabilities.</p> <p>The evaluator shall verify that the guidance documentation describes the logging of dynamic sessions consistent with the TSS.</p>
-----------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<p>Evaluator Findings</p>	<p>The evaluator examined the section titled Configuring Traffic Filter Rules in the AGD to verify that it describes dynamic session establishment capabilities. Upon investigation, the evaluator found that the AGD states that Traffic filter rules can be configured on a device to enforce validation against protocols attributes and direct traffic accordingly to the configured attributes and states the CLI commands needed to configure traffic filter rules for FTP, which is the protocol for which dynamic definition of rules is supported by the TOE as per the ST.</p> <p>The evaluator examined the section titled Configuring Traffic Filter Rules in the AGD to verify that it describes the logging of dynamic sessions consistently with the TSS. Upon investigation, the evaluator found that the description in the AGD was consistent with the TSS section in the ST.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
<p>Verdict</p>	<p>Pass</p>

5.8 TSS and Guidance Activities (Identification and Authentication)

5.8.1 FIA_AFL.1

5.8.1.1 FIA_AFL.1 TSS 1

<p>Objective</p>	<p>The evaluator shall examine the TSS to determine that it contains a description, for each supported method for remote administrative actions, of how successive unsuccessful authentication attempts are detected and tracked. The TSS shall also describe the method by which the remote administrator is prevented from successfully logging on to the TOE, and the actions necessary to restore this ability.</p>
<p>Evaluator Findings</p>	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS contains a description, for each supported method for remote administrative actions, of how successive unsuccessful authentication attempts are detected and tracked; the method by which the remote administrator is prevented from successfully logging on to the TOE; and the actions necessary to restore this ability. Upon investigation, the evaluator found that the TSS states that</p> <p>Security Administrators may configure the retry-options to specify the rules for handling failed user authentication attempts. The retry-options are applied following the first failed login attempt and for each username separately.</p> <p>The length of delay (5-10 seconds) after each failed attempt is specified by the backoff-factor, and the increase of the delay for each subsequent failed attempt is specified by the backoff-threshold (1-3).</p> <p>The tries-before-disconnect sets the maximum number of times (1-10) the user is allowed to attempt login over SSH before the connection is disconnected. The handling of authentication failures in SSH connection establishment is stated in FCS_SSHS_EXT.1.</p> <p>Each failed attempt is tracked. When the tries-before-disconnect number is reached for any user, that user account is locked and cannot be used to authenticate remotely. The lockout-</p>

	<p>period sets the duration of account locking (1-43,200 minutes). If an account is locked, the user may login locally from the console but not remotely until the lockout period has passed.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.8.1.2 FIA_AFL.1 TSS 2

Objective	The evaluator shall examine the TSS to confirm that the TOE ensures that authentication failures by remote administrators cannot lead to a situation where no administrator access is available, either permanently or temporarily (e.g. by providing local logon which is not subject to blocking).
Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS ensures that authentication failures by remote administrators cannot lead to a situation where no administrator access is available. Upon investigation, the evaluator found that the TSS states that</p> <p>If an account is locked, the user may login locally from the console but not remotely until the lockout period has passed.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.8.1.3 FIA_AFL.1 Guidance 1

Objective	The evaluator shall examine the guidance documentation to ensure that instructions for configuring the number of successive unsuccessful authentication attempts and time period (if implemented) are provided, and that the process of allowing the remote administrator to once again successfully log on is described for each “action” specified (if that option is chosen). If different actions or mechanisms are implemented depending on the secure protocol employed (e.g., TLS vs. SSH), all must be described.
Evaluator Findings	<p>The evaluator examined the section titled Limiting the Number of User Login Attempts for SSH Sessions in the AGD to verify that it provides instructions for configuring the number of successive unsuccessful authentication attempts and time period (if implemented), and that the process of allowing the remote administrator to once again successfully log on is described for each “action” specified (if that option is chosen). Upon investigation, the evaluator found that the AGD states that :</p> <p>If the remote administrator presents a valid username and password, access to the TOE is granted. If the credentials are invalid, the TOE allows the authentication to be retried after an interval that starts after 1 second and increases exponentially. If the number of authentication attempts exceed the configured maximum, no authentication attempts are accepted for a configured time interval. When the interval expires, authentication attempts are again accepted.</p>

	Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.1.4 FIA_AFL.1 Guidance 2

Objective	The evaluator shall examine the guidance documentation to confirm that it describes, and identifies the importance of, any actions that are required in order to ensure that administrator access will always be maintained, even if remote administration is made permanently or temporarily unavailable due to blocking of accounts as a result of FIA_AFL.1.
Evaluator Findings	<p>The evaluator examined the section titled Limiting the Number of User Login Attempts for SSH Sessions in the AGD to verify that it describes, and identifies the importance of, any actions that are required in order to ensure that administrator access will always be maintained, even if remote administration is made permanently or temporarily unavailable due to blocking of accounts as a result of FIA_AFL.1. Upon investigation, the evaluator found that the AGD states that :</p> <p>By configuring ssh root-login deny , administrator can ensure the root account remains active and continues to have local administrative privileges to the TOE even if other remote users are logged off.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.8.2 FIA_PMG_EXT.1

5.8.2.1 FIA_PMG_EXT.1.1 TSS 1[TD0792]

Objective	<p>The evaluator shall check that the TSS lists the supported special character(s) for the composition of administrator passwords.</p> <p>The evaluator shall check the TSS to ensure that the minimum_password_length parameter is configurable by a Security Administrator.</p> <p>The evaluator shall check that the TSS lists the range of values supported for the minimum_password_length parameter. The listed range shall include the value of 15.</p>
Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS contains the lists of the supported special character(s) and minimum of characters supported for administrator passwords. Upon investigation, the evaluator found that the TSS states that</p> <p>The password used for user authentication is a case-sensitive, alphanumeric string. The minimum length is 10 characters and Administrator-defined maximum length of up to 20 characters. A password must contain characters from at least two different character sets (upper, lower, numeric, special). Allowed special characters are “!”, “@”, “#”, “\$”, “%”, “^”, “&”, “*”, “(”, and “)”. Any standard ASCII, extended ASCII and Unicode characters are allowed.</p>

	Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.2.2 FIA_PMG_EXT.1.1 Guidance 1

Objective	<p>The evaluator shall examine the guidance documentation to determine that it:</p> <p>a) identifies the characters that may be used in passwords and provides guidance to security administrators on the composition of strong passwords, and</p> <p>b) provides instructions on setting the minimum password length and describes the valid minimum password lengths supported.</p>
Evaluator Findings	<p>The evaluator examined the section titled Understanding the Associated Password Rules for an Authorized Administrator in the AGD to verify that it identifies the characters that may be used in passwords and provides guidance to security administrators on the composition of strong passwords, and provides instructions on setting the minimum password length and describes the valid minimum password lengths supported. Upon investigation, the evaluator found that the AGD states that :</p> <p>Use the following guidelines and configuration options for passwords and when selecting passwords for authorized administrator accounts. Passwords should be:</p> <ul style="list-style-type: none"> • Easy to remember so that users are not tempted to write it down. • Changed periodically. • Private and not shared with anyone. • Contain a minimum of 10 characters. The minimum password length is 10 characters. • Include both alphanumeric and punctuation characters, composed of any combination of upper and lowercase letters, numbers, and special characters such as, “!”, “@”, “#”, “\$”, “%”, “^”, “&”, “*”, “(”, and “)”. There should be at least a change in one case, one or more digits, and one or more punctuation marks. • Contain character sets. Valid character sets include uppercase letters, lowercase letters, numbers, punctuation, and other special characters. • Contain the minimum number of character sets or character set changes. The minimum number of character sets required in plain-text passwords in Junos FIPS is 2. <p>The AGD also states that</p> <p>Strong reusable passwords can be based on letters from a favorite phrase or word, and then concatenated with other, unrelated words, along with additional digits and punctuation.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>

Verdict	Pass
---------	------

5.8.3 FIA_PSK_EXT.1

5.8.3.1 FIA_PSK_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS to ensure that it identifies all protocols that allow pre-shared keys. For each protocol identified by the requirement, the evaluator shall confirm that the TSS states which pre-shared key selections are supported.
Evaluator Findings	The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS identifies all protocols that allow pre-shared keys. Upon investigation, the evaluator found that the TSS states that The TOE supports IPsec pre-shared keys. It accepts Unicode characters to specify generated bit-based pre-shared keys. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.3.2 FIA_PSK_EXT.1 Guidance 1

Objective	The evaluator shall examine the operational guidance to determine that it provides guidance to administrators on how to configure all selected pre-shared key options if any configuration is required.
Evaluator Findings	The evaluator examined the section titled Configuring IPsec VPN with Preshared Key as IKE Authentication on the Initiator in the AGD to verify that it provides guidance to administrators on how to configure all selected pre-shared key options if any configuration is required. Upon investigation, the evaluator found that the AGD states the CLI commands to configure the Pre-shared Keys. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.4 FIA_UIA_EXT.1

5.8.4.1 FIA_UIA_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS to determine that it describes the logon process for each logon method (local, remote (HTTPS, SSH, etc.)) supported for the product. This description shall contain information pertaining to the credentials allowed/used, any protocol transactions that take place, and what constitutes a “successful logon”.
Evaluator Findings	The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS describes the logon process for each logon method supported for the product. Upon investigation, the evaluator found that the TSS states that Security Administrators may access the TOE from console or from a remote management station over SSHv2. In both cases, the access method is the CLI. Once connected from the

	<p>console or over SSH, the user is granted a logon window displaying an access banner and requiring the user to enter username and a password.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.8.4.2 FIA_UIA_EXT.1 TSS 2

Objective	The evaluator shall examine the TSS to determine that it describes which actions are allowed before user identification and authentication. The description shall cover authentication and identification for local and remote TOE administration.
Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS describes which actions are allowed before user identification and authentication. Upon investigation, the evaluator found that the TSS states that</p> <p>None of the CLI functions shall be made available to a user until successfully authenticated. The user may only establish an SSH connection (if attempting to access the TOE remotely) and read the access banner. The TOE shall respond to an ICMP Echo but not allow any other services to the user.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.8.4.3 FIA_UIA_EXT.1 Guidance 1

Objective	The evaluator shall examine the guidance documentation to determine that any necessary preparatory steps (e.g., establishing credential material such as pre- shared keys, tunnels, certificates, etc.) to logging in are described. For each supported the login method, the evaluator shall ensure the guidance documentation provides clear instructions for successfully logging on. If configuration is necessary to ensure the services provided before login are limited, the evaluator shall determine that the guidance documentation provides sufficient instruction on limiting the allowed services.
Evaluator Findings	<p>The evaluator examined the section titled “Configuring Administrative Credentials and Privileges” and “Configuring SSH on the Evaluated Configuration” in the AGD to verify that it describes any necessary preparatory steps (e.g., establishing credential material such as pre- shared keys, tunnels, certificates, etc.) to logging in.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.8.5 FIA_UAU.7

5.8.5.1 FIA_UAU.7 Guidance 1

Objective	The evaluator shall examine the guidance documentation to determine that any necessary preparatory steps to ensure authentication data is not revealed while entering for each local login allowed.
Evaluator Findings	Upon investigation, the evaluator found that the TOE gives no visual feedback while entering authentication data for each local login allowed. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.6 FIA_X509_EXT.1/Rev

5.8.6.1 FIA_X509_EXT.1/Rev TSS 1

Objective	The evaluator shall ensure the TSS describes where the check of validity of the certificates takes place, and that the TSS identifies any of the rules for extendedKeyUsage fields (in FIA_X509_EXT.1.1) that are not supported by the TOE (i.e. where the ST is therefore claiming that they are trivially satisfied). It is expected that revocation checking is performed when a certificate is used in an authentication step and when performing trusted updates (if selected). It is not necessary to verify the revocation status of X.509 certificates during power-up self-tests (if the option for using X.509 certificates for self-testing is selected).
Evaluator Findings	The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS describes where the check of validity of the certificates takes place, and that the TSS identifies any of the rules for extendedKeyUsage fields (in FIA_X509_EXT.1.1) that are not supported by the TOE (i.e. where the ST is therefore claiming that they are trivially satisfied). Upon investigation, the evaluator found that the TSS states that The TOE checks the validity of X.509 certificates each time a certificate is presented for IPsec authentication. The validation is by the following steps. If each step passes, the certificate is considered valid. <ol style="list-style-type: none"> 1. Fields subject, issuer, subjects public key, signature, basicConstraints and validity period are extracted. Absence of any of the fields causes the validation to fail. 2. The issuer is looked up in the PKI database. Absence of the issuer or the issuer certificate not having the CA:true flag set in the basicConstraints section causes the validation to fail. 3. The TOE verifies the signature. If the signature verification fails, the validation fails. 4. The TOE confirms that the current date and time is within the validity period specified in the certificate. If not, the validation fails. 5. The TOE may be configured to perform a revocation check using CRL (specified in Sect. 6.3 of RFC 5280). If the CRL fails to download, the validation fails unless the option to skip CRL checking on download failure has been set.

	<p>6. The TOE validates a certificate path by building a chain of at least three certificates based upon issuer and subject linkage. Each certificate in the chain is validated with steps (1) through to (5) above. If any certificate in the chain fails validation, the validation fails as a whole. A self-signed certificate is not required to be at the root of the certificate chain.</p> <p>7. The TOE determines if a certificate is a CA certificate by requiring the CA:true flag to be present in the basicConstraints section.</p> <p>8. The TOE validates the extendedKeyUsage field according to the following rules:</p> <ul style="list-style-type: none"> a. Server certificates presented for TLS must have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field. b. Client certificates presented for TLS must have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field. c. Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field. <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.8.6.2 FIA_X509_EXT.1/Rev TSS 2

Objective	<p>The TSS shall describe when revocation checking is performed and on what certificates. If the revocation checking during authentication is handled differently depending on whether a full certificate chain or only a leaf certificate is being presented, any differences must be summarized in the TSS section and explained in the Guidance.</p>
Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS describes when revocation checking is performed and on what certificates. Upon investigation, the evaluator found that the TSS states that</p> <p>The TOE may be configured to perform a revocation check using CRL (specified in Sect. 6.3 of RFC 5280). If the CRL fails to download, the validation fails unless the option to skip CRL checking on download failure has been set.</p> <p>The TOE validates a certificate path by building a chain of at least three certificates based upon issuer and subject linkage. Each certificate in the chain is validated with steps (1) through to (5) above. If any certificate in the chain fails validation, the validation fails as a whole. A self-signed certificate is not required to be at the root of the certificate chain.</p> <p>The TOE determines if a certificate is a CA certificate by requiring the CA:true flag to be present in the basicConstraints section.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.8.6.3 FIA_X509_EXT.1/Rev Guidance 1

Objective	The evaluator shall also ensure that the guidance documentation describes where the check of validity of the certificates takes place, describes any of the rules for extendedKeyUsage fields (in FIA_X509_EXT.1.1) that are not supported by the TOE (i.e. where the ST is therefore claiming that they are trivially satisfied) and describes how certificate revocation checking is performed and on which certificate.
Evaluator Findings	<p>The evaluator examined the section titled Configuring VPNs in the AGD to verify that it contains describes where the check of validity of the certificates takes place, describes any of the rules for extendedKeyUsage fields (in FIA_X509_EXT.1.1) that are not supported by the TOE and describes how certificate revocation checking is performed and on which certificate. Upon investigation, the evaluator found that the AGD states that :</p> <p>The TOE checks the validity of X.509 certificates each time a certificate is presented for IPsec authentication. To validate certificates, the TOE extracts the subject, issuer, subjects public key, signature, basicConstraints and validity period fields. If any of those fields is not present, the validation fails. The issuer is looked up in the PKI database. If the issuer is not present, or if the issuer certificate does not have the CA:true flag in the basicConstraints section, the validation fails. The TOE verifies the validity of the signature. If the signature is not valid, the validation fails. It then confirms that the current date and time is within the valid time period specified in the certificate. If the TOE has been configured to perform a revocation check using CRL (as specified in RFC 5280 Section 6.3). If the CRL fails to download, the certificate is considered to have failed validation, unless the option to skip CRL checking on download failure has been enabled.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.8.7 FIA_X509_EXT.2

5.8.7.1 FIA_X509_EXT.2 TSS 1

Objective	The evaluator shall check the TSS to ensure that it describes how the TOE chooses which certificates to use, and any necessary instructions in the administrative guidance for configuring the operating environment so that the TOE can use the certificates.
Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS describes how the TOE chooses which certificates to use, and any necessary instructions in the administrative guidance for configuring the operating environment so that the TOE can use the certificates. Upon investigation, the evaluator found that the TSS states that,</p> <p>The IKE policy of the TOE must be configured by the administrator so that TOE knows which certificate to use for authentication.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>

Verdict	Pass
---------	------

5.8.7.2 FIA_X509_EXT.2 TSS 2

Objective	The evaluator shall examine the TSS to confirm that it describes the behaviour of the TOE when a connection cannot be established during the validity check of a certificate used in establishing a trusted channel. The evaluator shall verify that any distinctions between trusted channels are described. If the requirement that the administrator is able to specify the default action, then the evaluator shall ensure that the guidance documentation contains instructions on how this configuration action is performed.
Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS describes the behaviour of the TOE when a connection cannot be established during the validity check of a certificate used in establishing a trusted channel. Upon investigation, the evaluator found that the TSS states that</p> <p>If the TSF cannot establish a connection to determine the validity of a certificate, the Administrator is prompted to accept or reject the certificate.</p> <p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that any distinctions between trusted channels are described. Upon investigation, the evaluator found that the TSS states that</p> <p>When configuring the IKE identity of the remote endpoint the administrator must specify an email address, fully qualified domain name, or IP address that will be matched against the SAN field, or a distinguished name, in the presented certificate.</p> <p>Finally, since the administrator is able to specify the default action, the evaluator examined the section titled Configuring IPsec VPN with RSA Signature as IKE Authentication on the Initiator or Responder in the AGD to verify that the guidance documentation contains instructions on how this configuration action is performed. Upon investigation, the evaluator found that the set security pki ca-profile <profilename> revocation-check crl disable on-download-failure command can be used to configure the same.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.8.7.3 FIA_X509_EXT.2 Guidance 1

Objective	The evaluator shall also ensure that the guidance documentation describes the configuration required in the operating environment so the TOE can use the certificates. The guidance documentation shall also include any required configuration on the TOE to use the certificates. The guidance document shall also describe the steps for the Security Administrator to follow if the connection cannot be established during the validity check of a certificate used in establishing a trusted channel.
-----------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Evaluator Findings	<p>The evaluator examined the section titled Configuring VPNs in the AGD. Upon investigation, the evaluator found that the AGD states the necessary CLI commands to configure the TOE to use the certificates. The authentication method in the IKE proposal is to be mentioned as rsa or ecDSA signature along with the certificate name mentioned in the ike policy.</p> <p>The AGD also mentions following instructions to setup the operating environment so the TOE can use the certificates: A web server (Example Apache 2) can be used to host the CRL files on the CRL server which the device can then retrieve via HTTP.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.8.8 FIA_X509_EXT.3

5.8.8.1 FIA_X509_EXT.3 TSS 1

Objective	If the ST author selects "device-specific information", the evaluator shall verify that the TSS contains a description of the device-specific fields used in certificate requests.
Verdict	NA. no "device-specific information" selected in ST.

5.8.8.2 FIA_X509_EXT.3 Guidance 1

Objective	The evaluator shall check to ensure that the guidance documentation contains instructions on requesting certificates from a CA, including generation of a Certificate Request. If the ST author selects "Common Name", "Organization", "Organizational Unit", or "Country", the evaluator shall ensure that this guidance includes instructions for establishing these fields before creating the Certification Request.
Evaluator Findings	<p>The evaluator examined the section titled Configuring VPNs in the AGD to verify that it contains instructions on requesting certificates from a CA, including generation of a Certification Request. Upon investigation, the evaluator found that the AGD states the CLI commands needed to request certificates from a CA and to generate a certification request.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.9 TSS and Guidance Activities (Security Management)

5.9.1 FMT_MOF.1/ManualUpdate

5.9.1.1 FMT_MOF.1/ManualUpdate Guidance 1

Objective	The evaluator shall examine the guidance documentation to determine that any necessary steps to perform manual update are described. The guidance documentation shall also
-----------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	provide warnings regarding functions that may cease to operate during the update (if applicable).
Evaluator Findings	<p>The evaluator examined the section titled Configuring Roles and Authentication Methods in the AGD to verify that it describes any necessary steps to perform manual update. Upon investigation, the evaluator found that the AGD states the following CLI command to manually update the TOE:</p> <p>request system software add /<image-path>/<junos package> no-copy no-validate reboot.</p> <p>The evaluator examined the section titled Configuring Roles and Authentication Methods in the AGD to verify that it provides warnings regarding functions that may cease to operate during the update (if applicable). Upon investigation, the evaluator found that the AGD states that:</p> <p>Some functionalities might be impacted during the reboot following the software upgrade and not during the upgrade.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.9.2 FMT_FMT_MOF.1/Functions

5.9.2.1 FMT_MOF.1/Functions TSS 1

Objective	For distributed TOEs it is required to verify the TSS to ensure that it describes how every function related to security management is realized for every TOE component and shared between different TOE components. The evaluator shall confirm that all relevant aspects of each TOE component are covered by the FMT SFRs.
Verdict	NA. Neither of the two TSS activities are applicable since the TOE is a not a distributed TOE.

5.9.2.2 FMT_MOF.1/Functions TSS 2

Objective	For non-distributed TOEs, the evaluator shall ensure the TSS for each administrative function identified the TSS details how the Security Administrator determines or modifies the behaviour of (whichever is supported by the TOE) transmitting audit data to an external IT entity, handling of audit data, audit functionality when Local Audit Storage Space is full (whichever is supported by the TOE).
Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS identifies each administrative function identified the TSS details how the Security Administrator determines or modifies the behaviour of (whichever is supported by the TOE) transmitting audit data to an external IT entity, handling of audit data, audit functionality when Local Audit Storage Space is full (whichever is supported by the TOE). Upon investigation, the evaluator found that the TSS states that</p> <p>The CLI contains all functions for the configuring the handling of the audit data. The CLI, and therefore the functions, are only available to successfully authenticated Security</p>

	<p>Administrators. The functions include transmission of audit data to an external IT entity, and local handling of the audit data.</p> <p>Only a Security Administrator can read, delete or archive log files through the CLI or through direct access to the filesystem.</p> <p>The locally stored syslog files are automatically deleted according to configurable limits on storage volume. The default maximum size is 1Gb, but the size can be modified by the set system syslog CLI command.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.9.2.3 FMT_MOF.1/Functions Guidance 1

Objective	For distributed TOEs it is required to verify the Guidance Documentation to describe management of each TOE component. The evaluator shall confirm that all relevant aspects of each TOE component are covered by the FMT SFRs.
Verdict	NA. TOE is not a Distributed TOE.

5.9.2.4 FMT_MOF.1/Functions Guidance 2

Objective	For non-distributed TOEs, the evaluator shall also ensure the Guidance Documentation describes how the Security Administrator determines or modifies the behaviour of (whichever is supported by the TOE) transmitting audit data to an external IT entity, handling of audit data, audit functionality when Local Audit Storage Space is full (whichever is supported by the TOE) are performed to include required configuration settings.
Evaluator Findings	<p>The evaluator examined the section titled Configuring Roles and Authentication Methods , Creating a Secure Logging Channel, Configuring the Remote Syslog Server and Configuring Audit Log Options in the Evaluated Configuration in the AGD to verify that it describes how the Security Administrator determines or modifies the behaviour of (whichever is supported by the TOE) transmitting audit data to an external IT entity, handling of audit data, audit functionality when Local Audit Storage Space is full (whichever is supported by the TOE) are performed to include required configuration settings. Upon investigation, the evaluator found that the AGD states that</p> <p>A secure Junos OS environment requires auditing of events and storing them in a local audit file. The recorded events are simultaneously sent to an external syslog server. A syslog server receives the syslog messages streamed from the device. The syslog server must have an SSH client with NETCONF support configured to receive the streamed syslog messages.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.9.3 FMT_MOF.1/Services

5.9.3.1 FMT_MOF.1/Services TSS 1

Objective	For distributed TOEs it is required to verify the TSS to ensure that it describes how every function related to security management is realized for every TOE component and shared between different TOE components. The evaluator shall confirm that all relevant aspects of each TOE component are covered by the FMT SFRs.
Verdict	NA. TOE is not distributed TOE.

5.9.3.2 FMT_MOF.1/Services TSS 2

Objective	For non-distributed TOEs, the evaluator shall ensure the TSS lists the services the Security Administrator is able to start and stop and how that how that operation is performed.
Evaluator Findings	The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS lists the services the Security Administrator is able to start and stop and how that how that operation is performed. Upon investigation, the evaluator found that the TSS states that Most services of the TOE may not be stopped and shall automatically start at the boot up of the TOE. The Security Administrator may start and stop the forwarding of the audit files to an external syslog server, Cluster Mode operation of the TOE, and TOE Software upgrade. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.3.3 FMT_MOF.1/Services Guidance 1

Objective	For distributed TOEs it is required to verify the Guidance Documentation to describe management of each TOE component. The evaluator shall confirm that all relevant aspects of each TOE component are covered by the FMT SFRs.
Verdict	NA. TOE is not distributed TOE.

5.9.3.4 FMT_MOF.1/Services Guidance 2

Objective	For non-distributed TOEs, the evaluator shall also ensure the Guidance Documentation describes how the TSS lists the services the Security Administrator is able to start and stop and how that how that operation is performed.
Evaluator Findings	The evaluator examined the section titled Configuring Event Logging to a Remote Server and Configuring Audit Log Options in the Evaluated Configuration in the AGD to verify that it describes how the TSS lists the services the Security Administrator is able to start and stop and how that how that operation is performed. Upon investigation, the evaluator found that the AGD states the steps to start event logging to a remote server along with the steps to set audit log file options. Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass
---------	------

5.9.4 FMT_MTD.1/CoreData

5.9.4.1 FMT_MTD.1/CoreData TSS 1

Objective	The evaluator shall examine the TSS to determine that, for each administrative function identified in the guidance documentation; those that are accessible through an interface prior to administrator log-in are identified. For each of these functions, the evaluator shall also confirm that the TSS details how the ability to manipulate the TSF data through these interfaces is disallowed for non-administrative users.
Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS identifies administrative functions that are accessible through an interface prior to administrator log-in. Upon investigation, the evaluator found that the TSS states that</p> <p>The TOE only allows three services prior to the identification and authentication of the Security Administrator:</p> <ol style="list-style-type: none"> 1. Displaying of the access banner. This is a display only and does not contain any user input mechanism. Therefore, it does not allow any means for the non-authentic users to manipulate the TOE. 2. Responding to an ICMP Echo. Echo protocol is a simple IP layer protocol for querying the status of the TOE. It does not contain any session establishment and does not carry any payload. Therefore, the protocol cannot be used for modifying the TOE or TSF data. 3. Establishment of a SSHv2 connection between the TOE and a remote management station. SSH is an IP-layer connection between the TOE and a remote management station. It will make available to the remote administrator a shell in which the user may be identified and authenticated. All management of the TOE is through a CLI which shall only be made available to the remote user upon successful identification and authentication. SSHv2 itself cannot be used for issuing any management commands to the TOE. <p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS details how the ability to manipulate the TSF data through these interfaces is disallowed for non-administrative users. Upon investigation, the evaluator found that the TSS states that</p> <p>A subset of the CLI implements the functions for managing the TOEs trust store for holding the public key certificates. Access to the trust store is only through the CLI (i.e. only granted to successfully authenticated Security Administrators) or to trusted processes. This ensures that only authorized accesses are allowed.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>

Verdict	Pass
---------	------

5.9.4.2 FMT_MTD.1/CoreData TSS 2

Objective	If the TOE supports handling of X.509v3 certificates and implements a trust store, the evaluator shall examine the TSS to determine that it contains sufficient information to describe how the ability to manage the TOE’s trust store is restricted.
Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that, if the TOE supports handling of X.509v3 certificates and implements a trust store, the TSS contains sufficient information to describe how the ability to manage the TOE’s trust store is restricted. Upon investigation, the evaluator found that the TSS states that</p> <p>A subset of the CLI implements the functions for managing the TOEs trust store for holding the public key certificates. Access to the trust store is only through the CLI (i.e. only granted to successfully authenticated Security Administrators) or to trusted processes. This ensures that only authorized accesses are allowed.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.9.4.3 FMT_MTD.1/CoreData Guidance 1

Objective	The evaluator shall review the guidance documentation to determine that each of the TSF-data-manipulating functions implemented in response to the requirements of the cPP is identified, and that configuration information is provided to ensure that only administrators have access to the functions.	
Evaluator Findings	The evaluator examined the section titled Configuring Roles and Authentication Methods in the AGD to verify that it identifies each of the TSF-data-manipulating functions implemented in response to the requirements of the cPP. Upon investigation, the evaluator found that the AGD describes how administrative users can configure the TSF-data manipulating functions for the TOE. The evaluator found that the configuration of the following functionality is described within AGD,	
	Administer the TOE locally and remotely	Configuring Roles and Authentication Methods
	Configure the access banner	Configuring a System Login Message and Announcement
	Configure the session inactivity time before session termination or locking	Configuring the User Session Idle Timeout
	Update the TOE, and to verify the updates use digital signature prior to installing those updates	Installing Junos Software Packages

	Configure the authentication failure parameters	Limiting the Number of User Login Attempts for SSH Sessions
	Configure firewall rules	Configuring Traffic Filtering Rules
	Configure the cryptographic functionality	Configuring SSH on the Evaluated Configuration, Configuring VPN on a Device Running Junos OS
	Configure the lifetime for IPsec SAs	Configuring VPN on a Device Running Junos OS
	Import X.509v3 certificates	Configuring VPN on a Device Running Junos OS
	Enable, disable, determine and modify the behavior of all the security functions of the TOE identified [VPNGW_MOD] to the Administrator	Configuring VPNs
	Configure all security management functions identified in [VPNGW_MOD]	Configuring VPNs
	Ability to configure audit behavior	Configuring Audit Log Options in the Evaluated Configuration
	Ability to configure thresholds for SSH rekeying	Configuring SSH on the Evaluated Configuration
	Ability to re-enable an Administrator account	Understanding the Associated Password Rules for an Authorized Administrator
	Ability to set the time which is used for time-stamps	Configuring the time and date
	Ability to configure the reference identifier for the peer	Configuring VPN on a Device Running Junos OS
	<p>The evaluator found that this encompasses all of the TSF-data manipulating functionality required by the NDcPP.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>	
Verdict	Pass	

5.9.4.4 FMT_MTD.1/CoreData Guidance 2

Objective	<p>If the TOE supports handling of X.509v3 certificates and provides a trust store, the evaluator shall review the guidance documentation to determine that it provides sufficient information for the administrator to configure and maintain the trust store in a secure way. If the TOE supports loading of CA certificates, the evaluator shall review the guidance documentation to determine that it provides sufficient information for the administrator to securely load CA</p>
-----------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	certificates into the trust store. The evaluator shall also review the guidance documentation to determine that it explains how to designate a CA certificate a trust anchor.
Evaluator Findings	<p>The evaluator examined the section titled Configuring Roles and Authentication Methods in the AGD to verify that, if the TOE supports handling of X.509v3 certificates and provides a trust store, it provides sufficient information for the administrator to configure and maintain the trust store in a secure way. Upon investigation, the evaluator found that the AGD states that:</p> <p>Administrative users (Security Administrator) must provide unique identification and authentication data before any administrative access to the system is granted.</p> <p>The evaluator examined the section titled Configuring VPNs in the AGD to verify that, if the TOE supports loading of CA certificates, it provides sufficient information for the administrator to securely load CA certificates into the trust store and that it explains how to designate a CA certificate a trust anchor. Upon investigation, the evaluator found that the AGD states the CLI commands needed to securely load CA certificates into the TOE's trust store and to designate a CA certificate as a trust anchor.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.9.5 FMT_MTD.1/CryptoKeys

5.9.5.1 FMT_MTD.1/CryptoKeys TSS 1

Objective	For distributed TOEs it is required to verify the TSS to ensure that it describes how every function related to security management is realized for every TOE component and shared between different TOE components. The evaluator shall confirm that all relevant aspects of each TOE component are covered by the FMT SFRs.
Verdict	NA. TOE is not distributed TOE.

5.9.5.2 FMT_MTD.1/CryptoKeys TSS 2

Objective	For non-distributed TOEs, the evaluator shall ensure the TSS lists the keys the Security Administrator is able to manage to include the options available (e.g. generating keys, importing keys, modifying keys or deleting keys) and how that how those operations are performed.
Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS lists the keys the Security Administrator is able to manage to include the options available (e.g. generating keys, importing keys, modifying keys or deleting keys) and how that how those operations are performed. Upon investigation, the evaluator found that the TSS states that</p> <p>The TOE implements a rich set of cryptographic protocols and algorithms. The users are only granted limited access to the keys directly. All cryptographic protocols and algorithms the TOE</p>

	<p>implements are listed in Table 15. Cryptographic keys the TOE uses together with their storage and method of destruction are listed in Table 16.</p> <p>Management of cryptographic keys is through the CLI as part of managing and configuring SSHv2, IPSec, IKEv1 and IKEv2. All key management operations occur through the CLI commands. Additionally, some long term keys used as TOE identity keys are uploaded when the TOE is initialized for use and may be destroyed by the user decommissioning the TOE - also through CLI commands.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.9.5.3 FMT_MTD.1/CryptoKeys Guidance 1

Objective	For distributed TOEs it is required to verify the Guidance Documentation to describe management of each TOE component. The evaluator shall confirm that all relevant aspects of each TOE component are covered by the FMT SFRs.
Verdict	NA. TOE is not distributed.

5.9.5.4 FMT_MTD.1/CryptoKeys Guidance 2

Objective	For non-distributed TOEs, the evaluator shall also ensure the Guidance Documentation lists the keys the Security Administrator is able to manage to include the options available (e.g. generating keys, importing keys, modifying keys or deleting keys) and how that how those operations are performed.
Evaluator Findings	<p>The evaluator examined the section titled Configuring Roles and Authentication Methods in the AGD to verify that it lists the keys the Security Administrator is able to manage to include the options available (e.g. generating keys, importing keys, modifying keys or deleting keys) and how that how those operations are performed. Upon investigation, the evaluator found that the AGD states that the Security Administrator is Responsible for the configuration and maintenance of cryptographic elements related to the establishment of secure connections to and from the evaluated product. The SSH keys are managed by the security administrator.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.9.6 FMT_SMF.1

5.9.6.1 FMT_SMF.1 TSS 1

Objective	The evaluator shall examine the TSS, Guidance Documentation and the TOE as observed during all other testing and shall confirm that the management functions specified in FMT_SMF.1 are provided by the TOE. The evaluator shall confirm that the TSS details which security management functions are available through which interface(s) (local administration interface, remote administration interface).
-----------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<p>Evaluator Findings</p>	<p>The evaluator examined the TSS, Guidance Documentation and the TOE as observed following management functions are claimed in the TOE Summary Specification section of the ST:</p> <p>The Security Administrator has the capability to:</p> <ul style="list-style-type: none"> • Administer the TOE locally via the serial ports on the physical device or remotely over an SSH connection. • Initiate a manual update of TOE software: <ul style="list-style-type: none"> ○ Query currently executing version of TOE software (both Junos OS and underlying Wind River Linux Host OS) ○ Verify update using digital signature and published hash. • Manage Functions: <ul style="list-style-type: none"> ○ Transmission of audit data to an external IT entity, including Start/stop and modify the behaviour of the trusted communication channel to external syslog server (netconf over SSH) and the trusted path for remote Administrative sessions (SSH) ○ Handling of audit data, including setting limits of log file size and behaviour when the maximum size threshold is hit. • Manage TSF data: <ul style="list-style-type: none"> ○ Create, modify, delete administrator accounts, including configuration of authentication failure parameters ○ Reset administrator passwords • Re-enable an Administrator account • Start and stop services • Manage crypto keys: <ul style="list-style-type: none"> ○ SSH key generation (ecdsa, ssh-rsa) • Manage the trusted public keys database • Perform management functions: <ul style="list-style-type: none"> ○ Configure the access banner ○ Configure the session inactivity time before session termination or locking, including termination of session when serial console cable is disconnected ○ Manage the TOE's trust store and designate X509.v3 certificates as trust anchors; ○ Import X.509v3 certificates ○ Manage cryptographic functionality, including: <ul style="list-style-type: none"> ▪ ssh ciphers ▪ hostkey algorithm ▪ key exchange algorithm
---------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

- hashed message authentication code
- thresholds for SSH rekeying
- Set the system time
- Configure NTP
- Configure Firewall rules;
- Configure the VPN-associated cryptographic functionality;
- Definition of packet filtering rules;
- Association of packet filtering rules to network interfaces;
- Ordering of packet filtering rules by priority;
- Configure the IPsec functionality, including configuration of IKE lifetime-seconds (within range 180 to 86400 i.e. 0.05 to 25 hours , with default value of 180 seconds), IPsec lifetime-seconds (within range 180 to 28800 i.e. 0.05 to 8 hours, with default value of 28800 seconds), and Lifetime-kilobytes (within range 64 to 4294967294 kilobytes) and ability to configure the reference identifier for the peer;
- Enable, disable signatures applied to sensor interfaces, and determine the behavior of IPS functionality
- Modify these parameters that define the network traffic to be collected and analysed:
 - Source IP addresses (host address and network address);
 - Destination IP addresses (host address and network address);
 - Source port (TCP and UDP);
 - Destination port (TCP and UDP);
 - Protocol (IPv4 and IPv6)
 - ICMP type and code
- Update (import) IPS signatures;
- Create custom IPS signatures;
- Configure anomaly detection;
- Enable and disable actions to be taken when signature or anomaly matches are detected;
- Modify thresholds that trigger IPS reactions;
- Modify the duration of traffic blocking actions;
- Modify the known-good and known-bad lists (of IP addresses or address ranges);
- Configure the known-good and known-bad lists to override signature-based IPS policies.

and the evaluator found the corresponding guidance in the AGD which confirms that the

	<p>management functions specified in FMT_SMF.1 are provided by the TOE.</p> <p>The evaluator examined the section titled TOE Summary Specification in the TSS to verify that it details which security management functions are available through which interface(s). Upon investigation, the evaluator found that the AGD states that</p> <p>The TOE implements a CLI where a command exists for each management and configuration function of the TOE. The TOE may be administered locally from console or remotely from a management station. All management functions (i.e. the entire CLI) are available to all successfully authenticated Security Administrators whether accessing the TOE locally or remotely.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.9.6.2 FMT_SMF.1 Guidance 1

Objective	The evaluator shall examine the TSS and Guidance Documentation to verify they both describe the local administrative interface. The evaluator shall ensure the Guidance Documentation includes appropriate warnings for the administrator to ensure the interface is local.
Evaluator Findings	<p>The evaluator examined the section titled Understanding Management Interfaces in the AGD to verify that it describes the local administrative interface. Upon investigation, the evaluator found that the AGD states that :</p> <p>Local Management Interfaces—The RJ-45 console port on the front panel of a device is configured as RS-232 data terminal equipment (DTE). Kindly use the command-line interface (CLI) over this port to configure the device from a terminal.</p> <p>The evaluator examined the section titled Configuring SSH and Console Connection in the AGD to verify that it includes appropriate warnings for the administrator to ensure the interface is local. Upon investigation, the evaluator found that the AGD describes the steps associated with connecting to the serial port of a computer. This sufficiently ensures that the interface is a local interface. Based on these findings, this assurance activity is considered satisfied.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.9.7 FMT_SMF.1/IPS

5.9.7.1 FMT_SMF.1/IPS TSS

Objective	The evaluator shall verify that the TSS describes how the IPS data analysis and reactions can be configured. Note that this activity should have been addressed with the TSS assurance activities for IPS_ABD_EXT.1, IPS_IPB_EXT.1 and IPS_ABD_EXT.1.
-----------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Evaluator Findings	The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS describes how the IPS data analysis and reactions can be configured. Upon investigation, the evaluator found that this activity has been addressed with the TSS assurance activities for IPS_ABD_EXT.1, IPS_IPB_EXT.1 and IPS_ABD_EXT.1. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.7.2 FMT_SMF.1/IPS Guidance

Objective	The evaluator shall verify that the operational guidance describes the instructions for each function defined in the SFR, describes how to configure the IPS data analysis and reactions, including how to set any configurable defaults and how to configure each of the applicable analysis pattern matching methods and reaction modes.	
Evaluator Findings	The evaluator examined the section titled IDP Extended Package Configuration Overview in the AGD to verify that it describes the instructions for each function defined in the SFR, describes how to configure the IPS data analysis and reactions, including how to set any configurable defaults and how to configure each of the applicable analysis pattern matching methods and reaction modes. Upon investigation, the evaluator found that the AGD describes the CLI commands to configure each of the function defined in the SFR as follows:	
	Enable, disable signatures applied to sensor interfaces, and determine the behavior of IPS functionality	IDP Extended Package Configuration Overview
	Modify these parameters that define the network traffic to be collected and analyzed: <ul style="list-style-type: none"> • Source IP addresses (host address and network address) • Destination IP addresses (host address and network address) • Source port (TCP and UDP) • Destination port (TCP and UDP) • Protocol (IPv4 and IPv6) • ICMP type and code 	IDP Extended Package Configuration Overview
	Update (import) signatures	IDP Extended Package Configuration Overview
	Create custom signatures	IDP Extended Package Configuration Overview

	Configure anomaly detection	IDP Extended Package Configuration Overview
	Enable and disable actions to be taken when signature or anomaly matches are detected	IDP Extended Package Configuration Overview
	Modify thresholds that trigger IPS reactions	IDP Extended Package Configuration Overview
	Modify the duration of traffic blocking actions	IDP Extended Package Configuration Overview
	Modify the known-good and known-bad lists (of IP addresses or address ranges)	Configuring Security Flow Policies
	Configure the known-good and known-bad lists to override signature-based IPS policies]	Configuring Security Flow Policies
	Based on these findings, this assurance activity is considered satisfied.	
Verdict	Pass	

5.9.8 FMT_SMF.1/VPN

5.9.8.1 FMT_SMF.1/VPN TSS

Objective	The evaluator shall examine the TSS to confirm that all management functions specified in FMT_SMF.1/VPN are provided by the TOE. As with FMT_SMF.1 in the Base-PP, the evaluator shall ensure that the TSS identifies what logical interfaces are used to perform these functions and that this includes a description of the local administrative interface.
Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS states that all management functions specified in FMT_SMF.1/VPN are provided by the TOE. Upon investigation, the evaluator found that the TSS states that all management functions specified in FMT_SMF.1/VPN are provided by the TOE.</p> <p>Further the evaluator examined the section titled TOE Summary Specification in the Security Target to ensure that TSS identifies what logical interfaces are used to perform these functions and that this includes a description of the local administrative interface. Upon investigation, the evaluator found that the TSS states that :</p> <p>The TOE implements a CLI where a command exists for each management and configuration function of the TOE. The TOE may be administered locally from console or remotely from a management station. All management functions (i.e. the entire CLI) are available to all successfully authenticated Security Administrators whether accessing the TOE locally or remotely.</p> <p>The Security Administrator has the capability to:</p>

	<ul style="list-style-type: none"> • Administer the TOE locally via the serial ports on the physical device or remotely over an SSH connection. <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.9.8.2 FMT_SMF.1/VPN Guidance

Objective	The evaluator shall examine the operational guidance to confirm that all management functions specified in FMT_SMF.1/VPN are provided by the TOE. As with FMT_SMF.1 in the Base-PP, the evaluator shall ensure that the operational guidance identifies what logical interfaces are used to perform these functions and that this includes a description of the local administrative interface.
Evaluator Findings	<p>The evaluator examined the section titled Configuring VPN on a Device Running Junos OS in the AGD to confirm that all management functions specified in FMT_SMF.1/VPN are provided by the TOE. Upon investigation, the evaluator found that the AGD states the CLI commands needed to configure the management functions specified in the SFR.</p> <p>The guidance document also describes the local administrative interface in the section titled Understanding Management Interfaces. Upon investigation, the evaluator found that the AGD states Local Management Interfaces—The RJ-45 console port on the front panel of a device is configured as RS-232 data terminal equipment (DTE). Kindly use the command-line interface (CLI) over this port to configure the device from a terminal.</p> <p>The evaluator examined the section titled Configuring VPNs and found that the operational guidance identifies what logical interfaces are used to perform the VPN functions , Evaluator found AGD states that A secure tunnel interface (st0) is an internal interface that is used by route-based VPNs to route cleartext traffic to an IPsec VPN tunnel.</p> <p>The evaluator also found below CLI command in the AGD for VPN configuration: set security ipsec vpn vpn1 bind-interface st0.0</p> <p>NOTE: Here, vpn1 is the VPN tunnel name given by the authorized administrator.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.9.9 FMT_SMR.2

5.9.9.1 FMT_SMR.2 TSS 1

Objective	The evaluator shall examine the TSS to determine that it details the TOE supported roles and any restrictions of the roles involving administration of the TOE.
-----------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------

Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the TSS to verify that it details the TOE supported roles and any restrictions of the roles involving administration of the TOE. Upon investigation, the evaluator found that the TSS states that:</p> <p>The TOE implements a Security Administrator role ‘super-user’. It is the only role authorized to administer the TOE. Each user assigned to the Security Administrator role gains access to the full CLI.</p> <p>Each human super-user is identified and authenticated with a username and password and assigned a Security Administrator role upon successful authentication. The role assignment remains until the session is terminated.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.9.9.2 FMT_SMR.2 Guidance 1

Objective	The evaluator shall review the guidance documentation to ensure that it contains instructions for administering the TOE both locally and remotely, including any configuration that needs to be performed on the client for remote administration.
Evaluator Findings	<p>The evaluator examined the section titled Understanding Management Interfaces in the AGD to verify that it contains instructions for administering the TOE both locally and remotely, including any configuration that needs to be performed on the client for remote administration. Upon investigation, the evaluator found that the AGD states that :</p> <p>The following management interfaces can be used in the evaluated configuration:</p> <ul style="list-style-type: none"> • Local Management Interfaces—The RJ-45 console port on the front panel of a device is configured as RS-232 data terminal equipment (DTE). Kindly use the command-line interface (CLI) over this port to configure the device from a terminal. Remote Management Protocols—The device can be remotely managed over any Ethernet interface. SSHv2 is the only permitted remote management protocol that can be used in the evaluated configuration. The remote management protocols J-Web and Telnet are not available for use on the device. <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.10 TSS and Guidance Activities (Packet Filtering)

5.10.1 FPF_RUL_EXT.1

5.10.1.1 FPF_RUL_EXT.1.1 TSS 1

Objective	The evaluator shall verify that the TSS provide a description of the TOE’s initialization and startup process, which clearly indicates where processing of network packets begins to take
-----------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	<p>place, and provides a discussion that supports the assertion that packets cannot flow during this process.</p> <p>The evaluator shall verify that the TSS also includes a narrative that identifies the components (e.g., active entity such as a process or task) involved in processing the network packets and describes the safeguards that would prevent packets flowing through the TOE without applying the ruleset in the event of a component failure. This could include the failure of a component, such as a process being terminated, or a failure within a component, such as memory buffers full and cannot process packets.</p>
<p>Evaluator Findings</p>	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS provides a description of the TOE's initialization/startup process and a discussion that supports the assertion that packets cannot flow during this process. Upon investigation, the evaluator found that the TSS states that</p> <p>The boot sequence of the TOE appliances also aids in establishing the securing domain and preventing tampering or bypass of security functionality. This includes ensuring the packet filtering rules cannot be bypassed during the boot sequence of the TOE. The following steps list the boot sequence for the TOE:</p> <ul style="list-style-type: none"> • BIOS hardware and memory checks • Loading and initialization of the FreeBSD Kernel OS • FIPS self-tests and firmware integrity tests are executed • The init utility is started (mounts file systems, sets up network cards to communicate on the network, and generally starts all the processes that usually are run on a FreeBSD system at startup) • Daemon programs such as Internet Service Daemon (INETD), Routing Protocol Daemon (RPD), Syslogd are started; Routing and forwarding tables are initialized • Management Daemon (or MGD) is loaded, allowing access to management interface • Physical interfaces are active <p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS includes a narrative that identifies the components involved in processing the network packets and describes the safeguards that would prevent packets flowing through the TOE without applying the ruleset in the event of a component failure. Upon investigation, the evaluator found that the TSS states that :</p> <p>Once the interfaces are brought up, they will start to receive and send packets based on the current configuration (or not receive or send any packets if they have not been previously configured).</p> <p>Interfaces are brought up only after successful loading of kernel and Information Flow subsystems, and these interfaces cannot send or receive packets unless previously configured by an Administrator.</p>

	Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.10.1.2 FPF_RUL_EXT.1.1 Guidance 1

Objective	The operational guidance associated with this requirement is assessed in the subsequent test EAs.
Evaluator Findings	The operational guidance associated with this requirement is assessed in the subsequent test assurance activities.
Verdict	Pass

5.10.1.3 FPF_RUL_EXT.1.4 TSS 1[TD0683]

Objective	<p>The evaluator shall verify that the TSS describes a packet filtering policy that can use the following fields for each identified protocol, and that the RFCs identified for each protocol are supported:</p> <ul style="list-style-type: none"> • IPv4 (RFC 791) <ul style="list-style-type: none"> ○ source address ○ destination address ○ protocol • IPv6 (RFC 8200) <ul style="list-style-type: none"> ○ source address ○ destination address ○ next header (protocol) • TCP (RFC 793) <ul style="list-style-type: none"> ○ source port ○ destination port • UDP (RFC768) <ul style="list-style-type: none"> ○ source port ○ destination port <p>The evaluator shall verify that the TSS describes how conformance with the identified RFCs has been determined by the TOE developer (e.g., third party interoperability testing, protocol compliance testing).</p> <p>The evaluator shall verify that each rule can identify the following actions: permit, discard, and log.</p> <p>The evaluator shall verify that the TSS identifies all interface types subject to the packet filtering policy and explains how rules are associated with distinct network interfaces. Where interfaces can be grouped into a common interface type (e.g., where the same internal logical path is used, perhaps where a common device driver is used), they can be treated collectively as a distinct network interface.</p>
-----------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<p>Evaluator Findings</p>	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS describes a Packet Filtering policy that can use the above fields for each identified protocol, and that the RFCs identified for each protocol are supported. Upon investigation, the evaluator found that the TSS states that</p> <p>The security policy rule set is an ordered list of entries stating the firewall rules. Each entry contains a specification of a network flow and an action.</p> <p>The protocol fields which may be used for specifying the network flow to which the action is to be applied are the following:</p> <ul style="list-style-type: none"> • IPv4 (RFC 791) <ul style="list-style-type: none"> • source address • destination address • protocol • IPv6 (RFC 8200) <ul style="list-style-type: none"> • source address • destination address • next header (protocol) • TCP (RFC 793) <ul style="list-style-type: none"> • source port • destination port • UDP (RFC768) <ul style="list-style-type: none"> • source port • destination port <p>Next, the evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS describes how conformance with the identified RFCs has been determined by the TOE developer. Upon investigation, the evaluator found that the TSS states that</p> <p>Conformance to these RFCs is demonstrated by protocol compliance testing by the product QA team.</p> <p>The evaluator also examined the section titled TOE Summary Specification in the Security Target to verify that each rule can identify the following actions: permit, discard, and log. Upon investigation, the evaluator found that the TSS states that</p> <p>The action may be to permit, discard or log the traffic.</p> <p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS identifies all interface types subject to the packet filtering policy and explains how rules are associated with distinct network interfaces. Upon investigation, the evaluator found that the TSS states that</p> <p>Each distinct network interface may be assigned a different set of rules.</p>
---------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.10.1.4 FPF_RUL_EXT.1.4 Guidance 1

Objective	<p>The evaluators shall verify that the operational guidance identifies the following protocols as being supported and the following attributes as being configurable within packet filtering rules for the associated protocols:</p> <ul style="list-style-type: none"> • IPv4 (RFC 791) <ul style="list-style-type: none"> ○ destination address ○ protocol • IPv6 (RFC 8200) <ul style="list-style-type: none"> ○ source address ○ destination address ○ next header (protocol) • TCP (RFC 793) <ul style="list-style-type: none"> ○ source port ○ destination port • UDP (RFC768) <ul style="list-style-type: none"> ○ source port ○ destination port <p>The evaluator shall verify that the operational guidance indicates that each rule can identify the following actions: permit, discard, and log.</p> <p>The evaluator shall verify that the operational guidance explains how rules are associated with distinct network interfaces.</p> <p>The guidance may describe the other protocols contained within the ST (e.g., IPsec, IKE, potentially HTTPS, SSH, and TLS) that are processed by the TOE. The evaluator shall ensure that it is made clear what protocols were not considered as part of the TOE evaluation.</p>
Evaluator Findings	<p>The evaluator examined the section titled Understanding Protocol Support in the AGD to verify that it identifies the required protocols as being supported and the required attributes as being configurable within Packet filtering rules. Upon investigation, the evaluator found that the AGD states the network traffic protocols and network fields used to perform stateful network traffic filtering on network packets.</p> <p>The evaluator also examined the section titled section titled Understanding a Security Flow Policy on a Device Running Junos OS in the AGD to verify that it explains the possible actions taken by packet filtering. Upon investigation, the evaluator found that the AGD states that</p> <p>The following modes can be defined for a security flow policy to determine how a device directs traffic:</p>

	<ul style="list-style-type: none"> • Bypass—The <code>Permit</code> option directs the traffic traversing the device through the stateful firewall inspection, but not through the IPsec VPN tunnel. • Discard—The <code>Deny</code> option inspects and drops all packets that do not match any <code>Permit</code> policies. • Protect—The traffic is routed through an IPsec tunnel based on the combination of route lookup and <code>Permit</code> policy inspection. • Log—This option logs traffic and session information for all the modes mentioned above. <p>The evaluator next examined the section titled section titled Understanding a Security Flow Policy on a Device Running Junos OS in the AGD to verify that the operational guidance explains how rules are associated with distinct network interfaces. Upon investigation, the evaluator found that the AGD states that</p> <p>Each of these policies are associated to zones on which distinct network interfaces are bound.</p> <p>Finally, the evaluator examined the section titled Understanding Protocol Support in the AGD to verify that the guidance describes the other protocols contained within the ST, along with protocols that were not considered as part of the TOE evaluation. Upon investigation, the evaluator found that the AGD states that</p> <p>The following protocols are also supported on devices running Junos OS and are a part of this evaluation.</p> <ul style="list-style-type: none"> • IPsec • IKE • SSH <p>The following protocols are supported on devices running Junos OS but are not included in the scope of this evaluation.</p> <ul style="list-style-type: none"> • OSPF • BGP • RIP <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.10.1.5 FPF_RUL_EXT.1.5 TSS 1

Objective	The evaluator shall verify that the TSS describes the algorithm applied to incoming packets, including the processing of default rules, determination of whether a packet is part of an established session, and application of administrator defined and ordered ruleset.
Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS describes the algorithm applied to incoming packets, including the processing of default rules, determination of whether a packet is part of an established session, and application of administrator defined and ordered ruleset. Upon investigation, the evaluator found that the TSS states that</p> <p>For inbound traffic, the TOE looks up the SA by using the destination IP address, security protocol, and security parameter index (SPI) value.</p> <p>Each packet is compared to the entries in the security policy rule set in sequential order until a rule that matches the packet is found or the end of the rule set is reached. If a matching rule is found, the action stated in that rule shall be taken. If the end of the rule set is reached, the packet is discarded. When a packet is processed by the TOE, the route is checked to see if it meets a defined security policy. If the packet meets the security policy, it is processed according to the rules of that policy.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.10.1.6 FPF_RUL_EXT.1.5 Guidance 1

Objective	The evaluator shall verify that the operational guidance describes how the order of packet filtering rules is determined and provides the necessary instructions so that an administrator can configure the order of rule processing.
Evaluator Findings	<p>The evaluator examined the section titled Configuring Traffic Filtering Rules in the AGD to verify that it describes how the order of packet filtering rules is determined and provides the necessary instructions so that an administrator can configure the order of rule processing. Upon investigation, the evaluator found that the AGD states that Each packet is compared against entries in the security policy rule set in sequential order until one is found that matches the specification in the policy, or until the end of the rule set is reached, in which case the implicit default policy is implemented and the packet is discarded.</p> <p>and also provides instructions so that an administrator can configure the order of rule processing.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.10.1.7 FPF_RUL_EXT.1.6 TSS 1

Objective	<p>The evaluator shall verify that the TSS describes the process for applying packet filtering rules and also that the behavior (either by default, or as configured by the administrator) is to discard packets when there is no rule match.</p> <p>The evaluator shall verify the TSS describes when the IPv4 and IPv6 protocols supported by the TOE differ from the full list provided in the RFC Values for IPv4 and IPv6 table.</p>
Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS describes the process for applying Packet filtering rules and that the behavior is to deny packets when there is no rule match. Upon investigation, the evaluator found that the TSS states that</p> <p>The TOE implements a default policy which disallows all traffic through it. The default policy may not be changed but Security Administrators may define packet filtering rules which allow explicitly defined traffic.</p> <p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS describes when the IPv4/IPv6 protocols supported by the TOE differ from the full list provided in the RFC Values for IPv4 and IPv6 table. Upon investigation, the evaluator found that the TSS states that :</p> <p>The following protocols are not supported and will be dropped before the packet is matched to an ACL; therefore, any “permit” or “deny” entries won’t be captured in the logs.</p> <ul style="list-style-type: none"> • IPv4- none. • IPv6 - Protocols 43 (IPv6-Route), 44 (IPv6-Frag), 51 (AH), 60 (IPv6-Opts). <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.10.1.8 FPF_RUL_EXT.1.6 Guidance 1

Objective	<p>The evaluator shall verify that the operational guidance describes the behavior if no rules or special conditions apply to the network traffic. If the behavior is configurable, the evaluator shall verify that the operational guidance provides the appropriate instructions to configure the behavior to discard packets with no matching rules.</p> <p>The evaluator shall verify that the operational guidance describes the range of IPv4 and IPv6 protocols supported by the TOE.</p>
Evaluator Findings	<p>The evaluator examined the section titled Configuring Default Deny-All and Reject Rules in the AGD to verify that it describes the behavior if no rules or special conditions apply to the network traffic. Upon investigation, the evaluator found that the AGD states that By default, security devices running Junos OS deny traffic unless rules are explicitly created to allow it using the following command and then states the CLI command needed to configure this behavior.</p>

	<p>The evaluator examined the section titled Supported Protocols in the AGD to verify that it describes the range of IPv4/IPv6 protocols supported by the TOE. Upon investigation, the evaluator found that the AGD states that :</p> <p>Range of IPv4/IPv6 protocols supported by the Device:</p> <p>For IPv4 supported protocol ID range is from 1 to 100</p> <p>For IPv6 supported protocol ID range is from 1 to 142 except for protocol ID 43, 44, 51, 60.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.11 TSS and Guidance Activities (Protection of the TSF)

5.11.1 FPT_APW_EXT.1

5.11.1.1 FPT_APW_EXT.1 TSS 1

Objective	<p>The evaluator shall examine the TSS to determine that it details all authentication data that are subject to this requirement, and the method used to obscure the plaintext password data when stored. The TSS shall also detail passwords are stored in such a way that they are unable to be viewed through an interface designed specifically for that purpose, as outlined in the application note.</p>
Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS details all authentication data that are subject to this requirement and the method used to obscure the plaintext password data when stored. Upon investigation, the evaluator found that the TSS states that</p> <p>The TOE stores authentication data locally and protects it by three means:</p> <ul style="list-style-type: none"> • Passwords stored in password files are hashed with sha-256 or sha-512, • All CLI commands implement appropriate measures to not disclose passwords when entered by the user or processed by the corresponding TOE functions, and • Authentication data for public key-based authentication methods are stored in a directory owned by the user and typically shares the name with the user. This directory contains the files ‘.ssh/authorized_keys’ and ‘.ssh/authorized_keys2’ which are used for SSH public key authentication. No other users may access that directory. <p>The evaluator also examined the section titled TOE Summary Specification in the Security Target to verify that the TSS details that passwords are stored in such a way that they are unable to be viewed through an interface designed specifically for that purpose. Upon investigation, the evaluator found that the TSS states that</p>

	<p>All CLI commands implement appropriate measures to not disclose passwords when entered by the user or processed by the corresponding TOE functions</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.11.2 FPT_FLS.1/SelfTest

5.11.2.1 FPT_FLS.1/SelfTest TSS

Objective	<p>The evaluator shall ensure the TSS describes how the TOE ensures a shutdown upon a self-test failure, a failed integrity check of the TSF executable image, or a failed health test of the noise source. If there are instances when a shut-down does not occur, (e.g., a failure is deemed non-security relevant), the evaluator shall ensure that those cases are identified and a rationale is provided that supports the classification and justifies why the TOE's ability to enforce its security policies is not affected in any such instance.</p>
Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS describes how the TOE ensures a shutdown upon a self-test failure, a failed integrity check of the TSF executable image, or a failed health test of the noise source. Upon investigation, the evaluator found that the TSS states that,</p> <p>If encountering a transiently corrupt state or a failure condition, the event will be logged, and the system shall cease processing any network traffic and restart. When the TOE restarts, the boot process shall re-execute all self-tests and shall not complete without each test passing.</p> <p>Any failed self-test shall halt the TOE and transition to an error state. In an error state the TOE shall not accept any command line input or traffic to any network interface. Power cycle is required to attempt to return to operation.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.11.2.2 FPT_FLS.1/SelfTest Guidance

Objective	<p>The evaluator shall verify that the operational guidance provides information on the self-test failures that can cause the TOE to shut down and how to diagnose the specific failure that has occurred, including possible remediation steps if available.</p>
Evaluator Findings	<p>The evaluator examined the section titled Understanding FIPS Self-Tests in the AGD to verify that it provides information on the self-test failures that can cause the TOE to shut down and how to diagnose the specific failure that has occurred. Upon investigation, the evaluator found that the AGD states that:</p> <p>If the device fails a KAT, the device writes the details to a system log file, enters FIPS error state (panic), and reboots.</p>

	Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.11.3 FPT_SKP_EXT.1

5.11.3.1 FPT_SKP_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS to determine that it details how any preshared keys, symmetric keys, and private keys are stored and that they are unable to be viewed through an interface designed specifically for that purpose, as outlined in the application note. If these values are not stored in plaintext, the TSS shall describe how they are protected/obscured.
Evaluator Findings	The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS details how any pre-shared keys, symmetric keys, and private keys are stored and that they are unable to be viewed through an interface designed specifically for that purpose. Upon investigation, the evaluator found that the TSS states that The CLI does not include commands or other mechanisms for viewing the cryptographic keys. The keys are protected by kernel-level file access rights. The rights are set up to limit access to the contents of cryptographic key containers to processes with cryptographic rights and to shell users with root permission. Security Administrators do not have root permission in shell. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.11.4 FPT_STM_EXT.1

5.11.4.1 FPT_STM_EXT.1 TSS 1 [TD0632]

Objective	The evaluator shall examine the TSS to ensure that it lists each security function that makes use of time, and that it provides a description of how the time is maintained and considered reliable in the context of each of the time related functions. If “obtain time from the underlying virtualization system” is selected, the evaluator shall examine the TSS to ensure that it identifies the VS interface the TOE uses to obtain time. If there is a delay between updates to the time on the VS and updating the time on the TOE, the TSS shall identify the maximum possible delay.
Evaluator Findings	The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS lists each security function that makes use of time and provides a description of how the time is maintained and considered reliable in the context of each of the time related functions. Upon investigation, the evaluator found that the TSS states that The TOE allows the Security Administrator to set the system time. The TOE implements a real time system clock which may be used for time stamps when the date and time is required. The system clock may also be used as a source of clock cycles which may be counted to implement inactivity timers.

	<p>The time can be manually updated by a Security Administrator or automatically updated using NTP synchronization.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.11.4.2 FPT_STM_EXT.1 Guidance 1 [TD0632]

Objective	<p>The evaluator examines the guidance documentation to ensure it instructs the administrator how to set the time. If the TOE supports the use of an NTP server, the guidance documentation instructs how a communication path is established between the TOE and the NTP server, and any configuration of the NTP client on the TOE to support this communication.</p> <p>If the TOE supports obtaining time from the underlying VS, the evaluator shall verify the Guidance Documentation specifies any configuration steps necessary. If no configuration is necessary, no statement is necessary in the Guidance Documentation. If there is a delay between updates to the time on the VS and updating the time on the TOE, the evaluator shall ensure the Guidance Documentation informs the administrator of the maximum possible delay.</p>
Evaluator Findings	<p>The evaluator examined the section titled “Configuring the Time and Date” and “Configuring Network Time Protocol” in the AGD to verify that it instructs the administrator how to set the time. Upon investigation, the evaluator found that the AGD states that :</p> <p>To configure a system date and time, use the following command:</p> <p>[edit]</p> <p>user@host# set date YYY YMMDDHHMM.ss</p> <p>The evaluator examined the section titled Configuring Network Time Protocol in the AGD to verify that the guidance documentation instructs how a communication path is established between the TOE and the NTP server, and any configuration of the NTP client on the TOE to support this communication. Upon investigation, the evaluator found that the AGD states that :</p> <p>In this section, configuration is given for the device to sync with a Network Time Protocol (NTP) server. This device supports time updates using NTP version 4 and NTP version 3. The device authentications updates using an administrator configured symmetric key, SHA-1 and SHA-256. The device rejects broadcast and multicast time updates. The device does not place a limit on the number of NTP time sources that can be configured.</p> <p>To configure the device in client mode, include the server statement and other optional statements at the [edit system ntp] hierarchy level:</p> <p>[edit system ntp]</p> <p>server address <key key-number> <version value> <prefer>;</p>

	<p>authentication-key key-number type type value password;</p> <p>trusted-key[key-numbers];</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.11.5 FPT_TST_EXT.1.1

5.11.5.1 FPT_TST_EXT.1.1 TSS 1

Objective	<p>The evaluator shall examine the TSS to ensure that it details the self-tests that are run by the TSF; this description should include an outline of what the tests are actually doing (e.g., rather than saying "memory is tested", a description similar to "memory is tested by writing a value to each memory location and reading it back to ensure it is identical to what was written" shall be used). The evaluator shall ensure that the TSS makes an argument that the tests are sufficient to demonstrate that the TSF is operating correctly.</p>
Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS details the self-tests that are run by the TSF on start-up. Upon investigation, the evaluator found that the TSS states that :</p> <p>When powered on, the TOE runs the following self-tests to check the correct operation:</p> <ul style="list-style-type: none"> • Power on test to determine that the boot-device responds, and to check the memory size to confirm the amount of available memory. • File integrity test to assert the integrity of the mounted signed packages. Integrity of the firmware is verified by digital signature verification (FPT_TST_EXT.3) and regenerating the fingerprints on the executables and other immutable files and by comparing them to the SHA1 fingerprints stored in the manifest file. • Crypto integrity test to verify the integrity of CSPs, including SSH hostkeys and ike credentials (CAs, certificates, cryptographic keys). • Authentication error test to verify that verifexec is enabled and operates correctly using /opt/sbin/kats/cannot-exec.real. • Kernel, Libmd, OpenSSL, Quicksec, SSH and IPsec tests to verify correct output from known answer tests for the algorithms. • Noise source health tests to verify the correct operation of the noise source. Tests include a repetitive count test and an adaptive proportion test. <p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS makes an argument that the tests are sufficient to demonstrate that the TSF is operating correctly. Upon investigation, the evaluator found that the TSS states that</p> <p>Each Junos OS firmware image includes fingerprints of executables and other immutable files. The TOE validates each binary against a registered fingerprint prior to execution This ensures that the TOE is protected from undetected injection of unauthorized software and</p>

	<p>ensures the integrity of the TOE software. Only authorized executables are allowed to run which ensures the correct operation of the TOE.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.11.5.2 FPT_TST_EXT.1.1 Guidance 1

Objective	The evaluator shall also ensure that the guidance documentation describes the possible errors that may result from such tests, and actions the administrator should take in response; these possible errors shall correspond to those described in the TSS.
Evaluator Findings	<p>The evaluator examined the section titled Understanding FIPS Self-Tests in the AGD to verify that it describes the possible errors that may result from such tests, and actions the administrator should take in response. Upon investigation, the evaluator found that the AGD states that :</p> <p>If the device fails a KAT, the device writes the details to a system log file enters FIPS error state (panic),and reboots.</p> <p>There may be instances where the device ends up not booting correctly. It can be a result of a POST test failure, or other things. The administrators are advised to refer to this guidance document to look for solution and if the issues are not resolved, contact support team.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.11.6 FPT_TST_EXT.3

5.11.6.1 FPT_TST_EXT.3 TSS

Objective	The evaluator shall verify that the TSS describes the method used to perform self-testing on the TSF executable code, and that this method is consistent with what is described in the SFR.
Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS describes the method used to perform self-testing on the TSF executable code, and that this method is consistent with what is described in the SFR. Upon investigation, the evaluator found that the TSS states that :</p> <p>When powered on, the TOE runs the following self-tests to check the correct operation:</p> <ul style="list-style-type: none"> • Power on test to determine that the boot-device responds, and to check the memory size to confirm the amount of available memory. • File integrity test to assert the integrity of the mounted signed packages. Integrity of the firmware is verified by digital signature verification (FPT_TST_EXT.3) and regenerating the fingerprints on the executables and other immutable files and by comparing them to the SHA1 fingerprints stored in the manifest file.

	<ul style="list-style-type: none"> • Crypto integrity test to verify the integrity of CSPs, including SSH hostkeys and iked credentials (CAs, certificates, cryptographic keys). • Authentication error test to verify that verifexec is enabled and operates correctly using /opt/sbin/kats/cannot-exec.real. • Kernel, Libmd, OpenSSL, Quicksec, SSH and IPsec tests to verify correct output from known answer tests for the algorithms. • Noise source health tests to verify the correct operation of the noise source. Tests include a repetitive count test and an adaptive proportion test. <p>When the TOE boots up, it implements a File Integrity Test (see FPT_TST_EXT.1) to verify the integrity of the executable files. The integrity test uses ECDSA (P-256) digital signature function defined in FCS_COP.1/SigGen.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.11.7 FPT_TUD_EXT.1

5.11.7.1 FPT_TUD_EXT.1 TSS 1

Objective	The evaluator shall verify that the TSS describe how to query the currently active version. If a trusted update can be installed on the TOE with a delayed activation, the TSS needs to describe how and when the inactive version becomes active. The evaluator shall verify this description.
Evaluator Findings	The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS describes how to query the currently active version. Upon investigation, the evaluator found that the TSS states that Users may query the version of the TOE firmware using the CLI command show version.
Verdict	Pass

5.11.7.2 FPT_TUD_EXT.1 TSS 2

Objective	The evaluator shall verify that the TSS describes all TSF software update mechanisms for updating the system firmware and software (for simplicity the term 'software' will be used in the following although the requirements apply to firmware and software). The evaluator shall verify that the description includes a digital signature verification of the software before installation and that installation fails if the verification fails. Alternatively, an approach using a published hash can be used. In this case the TSS shall detail this mechanism instead of the digital signature verification mechanism. The evaluator shall verify that the TSS describes the method by which the digital signature or published hash is verified to include how the candidate updates are obtained, the processing associated with verifying the digital signature
-----------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	<p>or published hash of the update, and the actions that take place for both successful and unsuccessful signature verification or published hash verification.</p>
<p>Evaluator Findings</p>	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS describes all TSF software update mechanisms for updating the system. Upon investigation, the evaluator found that the TSS states that</p> <p>If a new version of the TOE firmware is available at the developer web site, Security Administrator may execute a firmware upgrade. Upgrades are downloaded and installed manually. Automated upgrade is not supported.</p> <p>Partial upgrades are supported as the ESXi hypervisor and Junos OS software may each be upgraded separately.</p> <p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS description includes a digital signature verification of the software before installation and that installation fails if the verification fails. Upon investigation, the evaluator found that the TSS states that</p> <p>Each upgrade is associated to a digitally signature which is verified prior to installation. The authenticity of the signature may be verified by validating the associated X.509 certificate. The signature of the package is verified at the beginning of the installation before the expansion of the package. If the signature verification fails, an error message is displayed, and the package is not installed. Once the upgraded package is loaded, the Administrator shall disable the loading of additional VMs. The TOE will reboot at the completion the installation.</p> <p>The Junos OS kernel maintains a set of fingerprints (SHA1 digests) for executable files and other files which should be immutable. The manifest file is signed using the Juniper package signing key and is verified by the TOE using the corresponding public key. The verification key is stored on the TOE filesystem in clear. Access to it is controlled by filesystem access rights. ECDSA (P-256) with SHA-256 is used for digital signature package verification.</p> <p>The fingerprint loader will only process a manifest for which it can successfully verify the digital signature. Without a valid digital signature an executable cannot be run. When the command is issued to install an update, the manifest file for the update is verified and stored, and each executable/immutable file is verified before being executed. If any of the fingerprints in an update are not correctly verified, the TOE uses the last known verified image.</p> <p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS describes the method by which the published hash is verified to include how the candidate updates are obtained, the processing associated with verifying the published hash of the update, and the actions that take place for both successful and unsuccessful published hash verification. Upon investigation, the evaluator found that the TSS states that</p>

	<p>When software updates are made available, an administrator can obtain, verify the integrity of the software by manually verifying the hash of the downloaded software with the hash published on the website, and install those updates.</p> <p>The updates can be downloaded from https://support.juniper.net/support/downloads/?p=vsr3. During the execution of the image, an integrity check will be performed. Only if the hash is correct, will the image be installed.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.11.7.3 FPT_TUD_EXT.1 TSS 3

Objective	If the options 'support automatic checking for updates' or 'support automatic updates' are chosen from the selection in FPT_TUD_EXT.1.2, the evaluator shall verify that the TSS explains what actions are involved in automatic checking or automatic updating by the TOE, respectively.
Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS, if the options 'support automatic checking for updates' or 'support automatic updates' are chosen, explains what actions are involved in automatic checking or automatic updating by the TOE. Upon investigation, the evaluator found that the TSS states that</p> <p>Upgrades are downloaded and installed manually. Automated upgrade is not supported.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.11.7.4 FPT_TUD_EXT.1 TSS 5

Objective	If a published hash is used to protect the trusted update mechanism, then the evaluator shall verify that the trusted update mechanism does involve an active authorization step of the Security Administrator, and that download of the published hash value, hash comparison and update is not a fully automated process involving no active authorization by the Security Administrator. In particular, authentication as Security Administration according to FMT_MOF.1/ManualUpdate needs to be part of the update process when using published hashes.
Evaluator Findings	The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS, if a published hash is used to protect the trusted update mechanism, contains a description of how the trusted update mechanism involves an active authorization step of the Security Administrator, and that download of the published hash value, hash comparison and update is not a fully automated process involving no active authorization by the Security Administrator. Upon investigation, the evaluator found that the TSS states that:

	<p>When software updates are made available, an administrator can obtain, verify the integrity of the software by manually verifying the hash of the downloaded software with the hash published on the website, and install those updates.</p> <p>The updates can be downloaded from https://support.juniper.net/support/downloads/?p=vsr3 .</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.11.7.5 FPT_TUD_EXT.1 Guidance 1

Objective	The evaluator shall verify that the guidance documentation describes how to query the currently active version. If a trusted update can be installed on the TOE with a delayed activation, the guidance documentation needs to describe how to query the loaded but inactive version.
Evaluator Findings	<p>The evaluator examined the section titled How to Enable and Configure Junos OS in FIPS Mode of Operation in the AGD to verify that it describes how to query the currently active version and, if a trusted update can be installed on the TOE with a delayed activation, the loaded but inactive version. Upon investigation, the evaluator found that the AGD states the following command as a Note :</p> <p>show version</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.11.7.6 FPT_TUD_EXT.1 Guidance 2

Objective	The evaluator shall verify that the guidance documentation describes how the verification of the authenticity of the update is performed (digital signature verification or verification of published hash). The description shall include the procedures for successful and unsuccessful verification. The description shall correspond to the description in the TSS.
Evaluator Findings	<p>The evaluator examined the section titled Installing Junos Software Packages in the AGD to verify that it describes how the verification of the authenticity of the update is performed. Upon investigation, the evaluator found that the AGD states that :</p> <p>Junos OS is delivered in signed packages that contain digital signatures to ensure the Juniper Networks software; is running. When installing the software packages, Junos OS validates the signatures and the public key certificates used to digitally sign the software packages. If the signature or certificates is found to be invalid (for example, when the certificate validity period has 24 expired or cannot be verified against the root CA stored in the Junos OS internal store), the installation process fails.</p>

	<p>The evaluator also found below statement in the AGD for verification of published hash:</p> <p>Published Hash verification:</p> <p>To obtain Published hash, go to following link:</p> <p>https://support.juniper.net/support/downloads/?p=vsrx.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.11.7.7 FPT_TUD_EXT.1 Guidance 3

Objective	If a published hash is used to protect the trusted update mechanism, the evaluator shall verify that the guidance documentation describes how the Security Administrator can obtain authentic published hash values for the updates.
Evaluator Findings	<p>The evaluator examined the section titled Configuring Roles and Authentication Methods in the AGD to verify that it describes, if a published hash is used to protect the trusted update mechanism, how the Security Administrator can obtain authentic published hash values for the updates. Upon investigation, the evaluator found that the AGD states that :</p> <p>To obtain Published hash , go to following link: https://support.juniper.net/support/downloads/?p=vsrx</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.11.7.8 FPT_TUD_EXT.1 Guidance 6

Objective	If this was information was not provided in the TSS: If the ST author indicates that a certificate-based mechanism is used for software update digital signature verification, the evaluator shall verify that the Guidance Documentation contains a description of how the certificates are contained on the device. The evaluator also ensures that the Guidance Documentation describes how the certificates are installed/updated/selected, if necessary.
Verdict	NA. Not claimed in ST.

5.12 TSS and Guidance Activities (TOE Access)

5.12.1 FTA_SSL_EXT.1

5.12.1.1 FTA_SSL_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS to determine that it details whether local administrative session locking or termination is supported and the related inactivity time period settings.
-----------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS identifies whether local administrative session locking or termination is supported and the related inactivity time period settings. Upon investigation, the evaluator found that the TSS states that :</p> <p>Security Administrators may configure the session inactivity time for session termination. The TOE maintains for each user a counter of clock cycles since last activity. The clock cycles are read from the system clock. The counter is reset on each activity on the user's session. When the counter reaches the number of clock cycles equal to the configured period of inactivity the user session is terminated. To terminate a session, the TOE exits the display device to the login prompt.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.12.1.2 FTA_SSL_EXT.1 Guidance 1

Objective	The evaluator shall confirm that the guidance documentation states whether local administrative session locking or termination is supported and instructions for configuring the inactivity time period.
Evaluator Findings	<p>The evaluator examined the section titled Configuring the User Session Idle Timeout in the AGD to verify that it states whether local administrative session locking or termination is supported and instructions for configuring the inactivity time period. Upon investigation, the evaluator found that the AGD states that :</p> <p>To configure the idle timeout for a user session, use the following command:</p> <p>[edit]</p> <p>user@host# set system login idle-timeout minutes</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.12.2 FTA_SSL.3

5.12.2.1 FTA_SSL.3 TSS 1

Objective	The evaluator shall examine the TSS to determine that it details the administrative remote session termination and the related inactivity time period.
Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS identifies administrative remote session termination and the related inactivity time period. Upon investigation, the evaluator found that the TSS states that</p> <p>Session termination, both local and remote, may be due to the user issuing an <code>exit</code> or <code>quit</code> command or by the inactivity timer triggering the termination of a session.</p>

	Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.12.2.2 FTA_SSL.3 Guidance 1

Objective	The evaluator shall confirm that the guidance documentation includes instructions for configuring the inactivity time period for remote administrative session termination.
Evaluator Findings	<p>The evaluator examined the section titled Configuring the User Session Idle Timeout in the AGD to verify that it includes instructions for configuring the inactivity time period for remote administrative session termination. Upon investigation, the evaluator found that the AGD states that :</p> <p>To configure the idle timeout for a user session, use the following command:</p> <p>[edit]</p> <p>user@host# set system login idle-timeout minutes</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.12.3 FTA_SSL.4

5.12.3.1 FTA_SSL.4 TSS 1

Objective	The evaluator shall examine the TSS to determine that it details how the local and remote administrative sessions are terminated.
Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS identifies details how the local and remote administrative sessions are terminated. Upon investigation, the evaluator found that the TSS states that</p> <p>Session termination, both local and remote, may be due to the user issuing an exit or quit command or by the inactivity timer triggering the termination of a session.</p> <p>When the user issues an exit or quit command, the TOE makes the current session inactive and all content inaccessible. Successful authentication is required for re-gaining access.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.12.3.2 FTA_SSL.4 Guidance 1

Objective	The evaluator shall confirm that the guidance documentation states how to terminate a local or remote interactive session.
Evaluator Findings	The evaluator examined the section titled Login and Logout Events Using SSH in the AGD to verify that it states how to terminate a local or remote interactive session. Upon

	<p>investigation, the evaluator found that the AGD mentions the ‘quit’ command which is used to terminate local and remote interactive sessions.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.12.4 FTA_TAB.1

5.12.4.1 FTA_TAB.1 TSS 1

Objective	<p>The evaluator shall check the TSS to ensure that it details each administrative method of access (local and remote) available to the Security Administrator (e.g., serial port, SSH, HTTPS). The evaluator shall check the TSS to ensure that all administrative methods of access available to the Security Administrator are listed and that the TSS states that the TOE is displaying an advisory notice and a consent warning message for each administrative method of access. The advisory notice and the consent warning message might be different for different administrative methods of access and might be configured during initial configuration (e.g. via configuration file).</p>
Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS details each administrative method of access available to the Security Administrator Upon investigation, the evaluator found that the TSS states that</p> <p>Security Administrators may access the TOE from console or from a remote management station over SSH. In both cases, the access method is the CLI.</p> <p>The evaluator also examined the section titled TOE Summary Specification in the Security Target to verify that the TSS lists all administrative methods of access available to the Security Administrator and that the TSS states that the TOE is displaying an advisory notice and a consent warning message for each administrative method of access. Upon investigation, the evaluator found that the TSS states that</p> <p>The TOE allows Security Administrators to configure an access banner for the authentication prompt. The banner is displayed at the login dialogue and can provide warnings against unauthorized access to the secure switch as well as any other information that the Security Administrator wishes to communicate. As the login dialogue is identical independently of whether the TOE is accessed locally or remotely, the banner shall be displayed at both methods of access.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.12.4.2 FTA_TAB.1 Guidance 1

Objective	<p>The evaluator shall check the guidance documentation to ensure that it describes how to configure the banner message.</p>
-----------	------------------------------------------------------------------------------------------------------------------------------

Evaluator Findings	<p>The evaluator examined the section titled Configuring a System Login Message and Announcement in the AGD to verify that it describes how to configure the banner message. Upon investigation, the evaluator found that the AGD states that:</p> <p>A system login message appears before the user logs in and a system login announcement appears after the user logs in. By default, no login message or announcement is displayed on the device.</p> <p>To configure a system login message, use the following command:</p> <p>[edit]</p> <p>user@host# set system login message login-message-banner-text</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.13 TSS and Guidance Activities (Trusted Path/Channels)

5.13.1 FTP_ITC.1

5.13.1.1 FTP_ITC.1 TSS 1

Objective	<p>The evaluator shall examine the TSS to determine that, for all communications with authorized IT entities identified in the requirement, each secure communication mechanism is identified in terms of the allowed protocols for that IT entity, whether the TOE acts as a server or a client, and the method of assured identification of the non-TSF endpoint. The evaluator shall also confirm that all secure communication mechanisms are described in sufficient detail to allow the evaluator to match them to the cryptographic protocol Security Functional Requirements listed in the ST.</p>
Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS, for all communications with authorized IT entities identified in the requirement, each secure communication mechanism is identified in terms of the allowed protocols for that IT entity, whether the TOE acts as a server or a client, and the method of assured identification of the non-TSF endpoint. Upon investigation, the evaluator found that the TSS states that :</p> <p>The TOE implements an SSH server to protect confidentiality and integrity of communication with a remote syslog server. The Security Administrator sets up an event trace monitor which sends event log messages by netconf over SSH to a remote syslog server. The remote audit server initiates the connection.</p> <p>The TOE also implements IPsec in tunnel mode</p> <p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS describes all secure communication mechanisms in sufficient detail to allow the evaluator to match them to the cryptographic protocol Security Functional</p>

	<p>Requirements listed in the ST. Upon investigation, the evaluator found that the TSS states that :</p> <p>The TOE provides secure communication by using IPSEC between itself and Audit server, and between itself and VPN Gateway.</p> <p>The TOE uses IPSEC protocol with X.509 certificate-based authentication. The protocols listed are consistent with those specified in the requirement.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.13.1.2 FTP_ITC.1 Guidance 1

Objective	The evaluator shall confirm that the guidance documentation contains instructions for establishing the allowed protocols with each authorized IT entity, and that it contains recovery instructions should a connection be unintentionally broken.
Evaluator Findings	<p>The evaluator examined the section titled Configuring the Remote Syslog Server in the AGD to verify that it contains instructions for establishing the allowed protocols with each authorized IT entity, and that it contains recovery instructions should a connection be unintentionally broken. Upon investigation, the evaluator found that AGD provide configuration instruction for configuring connections with each authorized IT entity. Specifically, the evaluator found that AGD provides guidance for configuring connections with a syslog server.</p> <p>Upon further investigation, the evaluator found that AGD states that :</p> <p>If the connections used by the device is unintentionally broken, the security administrator needs to restart the connection, or the device will try to re-connect with the audit server.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.13.2 FTP_ITC.1/VPN

5.13.2.1 FTP_ITC.1/VPN TSS 1

Objective	<p>The EAs specified for FTP_ITC.1 in the Supporting Document for the Base-PP shall be applied for IPsec VPN communications.</p> <p>From FTP_ITC.1:</p> <p>The evaluator shall examine the TSS to determine that, for all communications with authorized IT entities identified in the requirement, each secure communication mechanism is identified in terms of the allowed protocols for that IT entity, whether the TOE acts as a server or a client, and the method of assured identification of the non-TSF endpoint. The evaluator shall also confirm that all secure communication mechanisms are described in</p>
-----------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	sufficient detail to allow the evaluator to match them to the cryptographic protocol Security Functional Requirements listed in the ST.
Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS, for all communications with authorized IT entities identified in the requirement, each secure communication mechanism is identified in terms of the allowed protocols for that IT entity, whether the TOE acts as a server or a client, and the method of assured identification of the non-TSF endpoint. Upon investigation, the evaluator found that the TSS states that :</p> <p>The TOE also implements IPsec in tunnel mode</p> <p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS describes all secure communication mechanisms in sufficient detail to allow the evaluator to match them to the cryptographic protocol Security Functional Requirements listed in the ST. Upon investigation, the evaluator found that the TSS states that :</p> <p>The TOE also implements IPsec in tunnel mode which is used for two purposes:</p> <ol style="list-style-type: none"> 1. When the TOE is configured in a cluster mode, the communication between the two nodes may be protected with IPsec. 2. When the TOE is configured to act as a VPN gateway, the communication between the TOE and the VPN peer may be protected with IPsec tunneled over SSH. <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.13.2.2 FTP_ITC.1/VPN Guidance 1

Objective	<p>The EAs specified for FTP_ITC.1 in the Supporting Document for the Base-PP shall be applied for IPsec VPN communications.</p> <p>From FTP_ITC.1:</p> <p>The evaluator shall confirm that the guidance documentation contains instructions for establishing the allowed protocols with each authorized IT entity, and that it contains recovery instructions should a connection be unintentionally broken.</p>
Evaluator Findings	<p>The evaluator examined the section titled “Configuring the Remote Syslog Server” and “Configuring VPNs” in the AGD to verify that it contains instructions for establishing the allowed protocols with each authorized IT entity, and that it contains recovery instructions should a connection be unintentionally broken. Upon investigation, the evaluator found that the AGD provides configuration instruction for configuring connections with each authorized IT entity. Specifically, the evaluator found that AGD provides guidance for configuring connections with a syslog server.</p>

	<p>If the connections used by the device is unintentionally broken, the security administrator needs to restart the connection, or the device will try to re-connect with the audit server.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.13.3 FTP_TRP.1/Admin

5.13.3.1 FTP_TRP.1/Admin TSS 1

Objective	<p>The evaluator shall examine the TSS to determine that the methods of remote TOE administration are indicated, along with how those communications are protected. The evaluator shall also confirm that all protocols listed in the TSS in support of TOE administration are consistent with those specified in the requirement, and are included in the requirements in the ST.</p>
Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS indicates the methods of remote TOE administration and how those communications are protected. Upon investigation, the evaluator found that the TSS states that</p> <p>For remote access the remote management station is required to run an SSH client. The SSH client requests an SSHv2 connection between itself and the TOE. Upon successful SSH connection, user authentication and all subsequent administration of the TOE occurs over SSH.</p> <p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS protocols are consistent with those specified in the requirement. Upon investigation, the evaluator found that the TSS states that</p> <p>Upon successful SSH connection, user authentication and all subsequent administration of the TOE occurs over SSH.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.13.3.2 FTP_TRP.1/Admin Guidance 1

Objective	<p>The evaluator shall confirm that the guidance documentation contains instructions for establishing the remote administrative sessions for each supported method.</p>
Evaluator Findings	<p>The evaluator examined the section titled Configuring SSH and Console Connection in the AGD to verify that it contains instructions for establishing the remote administrative sessions for each supported method. Upon investigation, the evaluator found that the AGD states that</p>

	<p>SSH is an allowed remote management interface in the evaluated configuration. This topic describes how to configure SSH on the device. And then the evaluator also confirmed that the AGD provides CLI commands for configuration of SSH.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.14 TSS and Guidance Activities (Intrusion Prevention)

5.14.1 IPS_ABD_EXT.1

5.14.1.1 IPS_ABD_EXT.1.3 TSS

Objective	<p>The evaluator shall verify that the TSS describes the composition, construction, and application of baselines or anomaly-based attributes specified in IPS_ABD_EXT.1.1. The evaluator shall verify that the TSS provides a description of how baselines are defined and implemented by the TOE, or a description of how anomaly-based rules are defined and configured by the administrator.</p> <p>The evaluator shall verify that each baseline or anomaly-based rule can be associated with a reaction specified in IPS_ABD_EXT.1.3.</p> <p>The evaluator shall verify that the TSS identifies all interface types capable of applying baseline or anomaly-based rules and explains how they are associated with distinct network interfaces. Where interfaces can be grouped into a common interface type (e.g., Page 18 of 47 Activity Assurance Activity where the same internal logical path is used, perhaps where a common device driver is used) they can be treated collectively as a distinct network interface.</p>
Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS describes the composition, construction, and application of baselines or anomaly-based attributes. Upon investigation, the evaluator found that the TSS states that</p> <p>The TOE allows Administrators to define signatures for anomalous traffic in terms of throughput (bits per second), time of the day for defined source/destination address and port, frequency of traffic patterns and thresholds of traffic patterns.</p> <p>The evaluator also examined the section titled TOE Summary Specification in the Security Target to verify that the TSS provides a description of how baselines are defined and implemented by the TOE, or a description of how anomaly-based rules are defined and configured by the administrator. Upon investigation, the evaluator found that the TSS states that</p> <p>Anomaly signatures based on time of day characteristics are implemented by configuring schedulers using the CLI command <code>set schedulers</code> and attaching them to firewall policies.</p> <p>Anomaly signatures based on throughput characteristics are implemented by configuring policers with a bandwidth limit and the desired signature action (discard or forward). That</p>

	<p>is done by the CLI set <code>firewall policer</code> and attaching it to any interface with the CLI command set interfaces. Traffic exceeding the specified throughput limit is dropped when the policer is configured to discard traffic.</p> <p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS identifies all interface types capable of applying baseline or anomaly-based rules and explains how they are associated with distinct network interfaces. Upon investigation, the evaluator found that the TSS states that :</p> <p>A policer can be applied to specific inbound or outbound IP packets in a Layer 3 traffic flow at a logical interface by using a stateless firewall filter. If an input firewall filter is configured on the same logical interface as a policer, the policer is executed first. If an output firewall filter is configured on the same logical interface as a policer, the firewall filter is executed first.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.14.1.2 IPS_ABD_EXT.1.3 Guidance

Objective	<p>The evaluator shall verify that the operational guidance provides instructions to manually create baselines or anomaly-based rules according to the selections made in IPS_ABD_EXT.1.1. Note that dynamic “profiling” of a network to establish a baseline is outside the scope of this PP.</p> <p>The evaluator shall verify that the operational guidance provides instructions to associate reactions specified in IPS_ABD_EXT.1.3 with baselines or anomaly-based rules. The evaluator shall verify that the operational guidance provides instructions to associate the different policies with distinct network interfaces.</p>
Evaluator Findings	<p>The evaluator examined the section titled IDP Extended Package Configuration Overview in the AGD to verify that it provides instructions to manually create baselines or anomaly-based rules according to the selections made in IPS_ABD_EXT.1.1. Upon investigation, the evaluator found that the AGD states the CLI commands to create baseline or anomaly-based rules in accordance with the selections made in the SFR.</p> <p>The evaluator examined the section titled IDP Extended Package Configuration Overview in the AGD to verify that it provides instructions to associate reactions specified in IPS_ABD_EXT.1.3 with baselines or anomaly-based rules. Upon investigation, the evaluator found that the AGD states the CLI commands to associate reactions specified in the SFR with baselines or anomaly-based rules.</p>

	<p>The evaluator examined the section titled IDP Extended Package Configuration Overview in the AGD to verify that it provides instructions to associate the different policies with distinct network interfaces. Upon investigation, the evaluator found that the AGD states the CLI commands to associate different policies with distinct network interfaces.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.14.2 IPS_IPB_EXT.1

5.14.2.1 IPS_IPB_EXT.1.2 TSS

Objective	<p>The evaluator shall verify how good/bad lists affect the way in which traffic is analyzed with respect to processing packets. The TSS should also provide detail with the attributes that create a known good list, a known bad list, their associated rules, including how to define the source or destination IP address (e.g. a single IP address or a range of IP addresses).</p> <p>The evaluator shall also verify that the TSS identifies all the roles and level of access for each of those roles that have been specified in+ the requirement.</p>
Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS describes how good/bad lists affect the way in which traffic is analyzed with respect to processing packets and provides detail with the attributes that create a known good list, a known bad list, their associated rules, including how to define the source or destination IP address. Upon investigation, the evaluator found that the TSS states that :</p> <p>The TOE supports definition of known-good and known-bad lists of source and/or destination addresses at the firewall rule level. Address ranges are defined by creating address book entries and attaching them to firewall policies along with policy-related attributes like permit/deny etc. which will subsequently dictate how the TOE reacts to traffic matching the policy.</p> <p>The evaluator also examined the section titled TOE Summary Specification in the Security Target to verify that the TSS identifies all the roles and level of access for each of those roles that have been specified in the requirement. Upon investigation, the evaluator found that the TSS states that :</p> <p>Only authorized users assigned the Security Administrator role can access and configure the IPS policies.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.14.2.2 IPS_IPB_EXT.1.2 Guidance

Objective	The evaluator shall verify that the administrative guidance provides instructions with how each role specified in the requirement can create, modify and delete the attributes of a known good and known bad lists.
Evaluator Findings	The evaluator examined the section titled Configuring Traffic Filtering Rules in the AGD to verify that it provides instructions with how each role specified in the requirement can create, modify and delete the attributes of a known good and known bad lists. Upon investigation, the evaluator found that the AGD states the commands used to create, modify and delete the attributes of a known good and known bad lists. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.14.3 IPS_NTA_EXT.1

5.14.3.1 IPS_NTA_EXT.1.1 TSS

Objective	The evaluator shall verify that the TSS explains the TOE’s capability of analyzing IP traffic in terms of the TOE’s policy hierarchy (precedence). The TSS should identify if the TOE’s policy hierarchy order is configurable by the administrator for IPS policy elements (known-good lists, known-bad lists, signature-based rules, and anomaly-based rules). Regardless of whether the precedence is configurable, the evaluator shall verify that the TSS describes the default precedence as well as the IP analyzing functions supported by the TOE.
Evaluator Findings	The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS explains the TOE’s capability of analyzing IP traffic in terms of the TOE’s policy hierarchy, identifies if the TOE’s policy hierarchy order is configurable, and describes the default precedence. Upon investigation, the evaluator found that the TSS states that IDP policies may be associated to firewall policies. IDP can be invoked on a firewall rule by rule basis for maximum granularity. Only firewall policies marked for IDP will be processed by the IDP engine. Other rules will only be processed by the firewall. IPS Policies extend firewall policies to the matching for specific attacks by Source Zone, Destination Zone, Source IP, Destination IP, Source Port, Destination Port, and Protocol. Interface matching can be achieved through the use of zones. Attack Actions are configurable on a rule by rule basis. Rules within policies are processed in an Administrator-defined order when network traffic flows through the TOE network interfaces. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.14.3.2 IPS_NTA_EXT.1.1 Guidance

Objective	The evaluator shall verify that the guidance describes the default precedence.
-----------	--------------------------------------------------------------------------------

	If the precedence is configurable. The evaluator shall verify that the guidance explains how to configure the precedence.
Evaluator Findings	<p>The evaluator examined the section titled Configuring Traffic Filtering Rules in the AGD to verify that it describes the default precedence. Upon investigation, the evaluator found that the AGD states The firewall filter terms are evaluated in the order in which they are configured.</p> <p>Since precedence is decided by the order of configuration and isn't technically configurable, the latter part of the guidance activity is not applicable.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.14.3.3 IPS_NTA_EXT.1.2 TSS

Objective	<p>The evaluator shall verify that the TSS indicates that the following protocols are supported:</p> <ul style="list-style-type: none"> • IPv4 • IPv6 • ICMPv4 • ICMPv6 • TCP • UDP <p>The evaluator shall verify that the TSS describes how conformance with the identified protocols has been determined by the TOE developer. (e.g., third party interoperability testing, protocol compliance testing).</p>
Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS indicates that the required protocols are supported and describes how conformance with the identified protocols has been determined by the TOE developer. Upon investigation, the evaluator found that the TSS states that</p> <p>The TOE is capable of inspecting IPv4, IPv6, ICMPv4, ICMPv6, TCP and UDP traffic. Conformance to these RFCs is demonstrated by protocol compliance testing by the product QA team.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.14.3.4 IPS_NTA_EXT.1.3 TSS

Objective	The evaluator shall verify that the TSS identifies all interface types capable of being deployed in the modes of promiscuous, and or inline mode as well as the interfaces necessary to facilitate each deployment mode (at a minimum, the interfaces need to support inline mode).
-----------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	The TSS should also provide descriptions how the management interface is distinct from sensor interfaces.
Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS identifies all interface types capable of being deployed in the modes of promiscuous and or inline mode as well as the interfaces necessary to facilitate each deployment mode and describes how the management interface is distinct from sensor interfaces. Upon investigation, the evaluator found that the TSS states that</p> <p>The TOE is capable of inspecting all traffic passing through the TOE's Ethernet interfaces (inline mode). Ethernet interfaces can be assigned to Zones on which firewall and IDP policies are predicated.</p> <p>IDP management is through the CLI locally from console or remotely over an SSH connection.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.14.3.5 IPS_NTA_EXT.1.3 Guidance

Objective	<p>The evaluator shall verify that the operational guidance provides instructions on how to deploy each of the deployment methods outlined in the TSS. The evaluator shall also verify that the operational guidance provides instructions of applying IPS policies to interfaces for each deployment mode. If the management interface is configurable the evaluator shall verify operational guidance explains how to configure the interface into a management interface.</p> <p>The evaluator shall verify that the operational guidance explains how the TOE sends commands to remote traffic filtering devices.</p> <p>Note: the secure channel configurations between the TOE and the remote device would be discussed as per FTP_ITC.1 (if the ST author selects other interface types) and/or FTP_TRP.1 (for interfaces in management mode) in the base PP.</p>
Evaluator Findings	<p>The evaluator examined the section titled IDP Extended Package Configuration Overview in the AGD to verify that it provides instructions on how to deploy each of the deployment methods outlined in the TSS; applying IPS policies to interfaces for each deployment mode; and, if the management interface is configurable, explains how to configure the interface into a management interface. Upon investigation, the evaluator found that the AGD states the steps for each deployment method along with the steps for applying IPS policies to interfaces for each deployment mode and explains how to configure the interface into a management interface.</p> <p>The TOE does not support sending traffic to remote traffic filtering devices. Hence, the latter part of the guidance activity is not applicable.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>

Verdict	Pass
---------	------

5.14.4 IPS_SBD_EXT.1

5.14.4.1 IPS_SBD_EXT.1.1 TSS

Objective	<p>The evaluator shall verify that the TSS describes what is comprised within a signature rule.</p> <p>The evaluator shall verify that each signature can be associated with a reaction specified in IPS_SBD_EXT.1.5.</p> <p>The evaluator shall verify that the TSS identifies all interface types capable of applying signatures and explains how rules are associated with distinct network interfaces. Where interfaces can be grouped into a common interface type (e.g., where the same internal logical path is used, perhaps where a common device driver is used) they can be treated collectively as a distinct network interface.</p>
Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS describes what is comprised within a signature rule. Upon investigation, the evaluator found that the TSS states that</p> <p>Signatures can be defined to match any header-field value using command <code>set security idp custom-attack</code> along with the actions (allow/block), and using command <code>set security idp idp-policy</code> that defines the IDP policy the TOE enforces on matching packets. The matching criteria can be "equal", "greater-than", "less-than" or "not-equal".</p> <p>The evaluator also examined the section titled TOE Summary Specification in the Security Target to verify that each signature can be associated with a reaction specified in the SFR. Upon investigation, the evaluator found that the TSS states that</p> <p>Attack Actions are configurable on a rule by rule basis. The default action for the above is to drop the packets. To allow the packets through, the <code>alarm-without-drop</code> action can be defined using command <code>set security screen ids-option</code>.</p> <p>The evaluator also examined the section titled TOE Summary Specification in the Security Target to verify that the TSS identifies all interface types capable of applying signatures and explains how rules are associated with distinct network interfaces. Upon investigation, the evaluator found that the TSS states that</p> <p>The rules can be applied to any defined interface capable of receiving network traffic.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.14.4.2 IPS_SBD_EXT.1.1 Guidance [TD0722]

Objective	<p>The evaluator shall verify that the operational guidance provides instructions with how to create and/or configure rules using the following protocols and header inspection fields:</p> <ul style="list-style-type: none"> • IPv4: Version; Header Length; Packet Length; ID; IP Flags; Fragment Offset; Time to Live (TTL); Protocol; Header Checksum; Source Address; Destination Address; IP options; and, if selected, type of service (ToS). • IPv6: Version; payload length; next header; hop limit; source address; destination address; routing header; and, if selected, traffic class and/or flow label. • ICMP: Type; Code; Header Checksum; and, if selected, other Header fields (varies based on the ICMP type and code). • ICMPv6: Type; Code; and Header Checksum. • TCP: Source port; destination port; sequence number; acknowledgement number; offset; reserved; TCP flags; window; checksum; urgent pointer; and TCP options. • UDP: Source port; destination port; length; and UDP checksum. <p>The evaluator shall verify that the operational guidance provides instructions with how to select and/or configure reactions specified in IPS_SBD_EXT.1.5 in the signature rules.</p>
Evaluator Findings	<p>The evaluator examined the section titled IDP Extended Package Configuration Overview in the AGD to verify that it provides instructions with how to create and/or configure rules using the required protocols and header inspection fields . Upon investigation, the evaluator found that the AGD states the CLI commands used to configure rules using the mentioned protocols and header inspection fields.</p> <p>The evaluator also examined the section titled IDP Extended Package Configuration Overview in the AGD to verify that it provides instructions with how to select and/or configure reactions specified in IPS_SBD_EXT.1.5 in the signature rules. Upon investigation, the evaluator found that the AGD states the CLI commands used to select and/or configure reactions specified in IPS_SBD_EXT.1.5 in the signature rules.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.14.4.3 IPS_SBD_EXT.1.2 TSS

Objective	<p>The evaluator shall verify that the TSS describes what is comprised within a string-based detection signature.</p> <p>The evaluator shall verify that each packet payload string-based detection signature can be associated with a reaction specified in IPS_SBD_EXT.1.5.</p>
-----------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<p>Evaluator Findings</p>	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS describes what is comprised within a string-based detection signature. Upon investigation, the evaluator found that the TSS states that</p> <p>The TOE also supports string-based pattern-matching inspection of packet payload data for the supported protocols. For TCP payload inspection, the TOE implements pre-defined attack signatures to detect FTP commands, HTTP commands and content, and SMTP states. Administrators can also define custom-attack signatures for application layer protocols using the command <code>set security idp custom-attack</code>.</p> <p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that each packet payload string-based detection signature can be associated with a reaction specified in IPS_SBD_EXT.1.5. Upon investigation, the evaluator found that each packet payload string-based detection signature could be associated with a reaction specified in the SFR.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
<p>Verdict</p>	<p>Pass</p>

5.14.4.4 IPS_SBD_EXT.1.2 Guidance

<p>Objective</p>	<p>The evaluator shall verify that the operational guidance provides instructions with how to configure rules using the packet payload string-based detection fields defined in IPS_SBD_EXT.1.2. The operational guidance shall provide configuration instructions, if needed, to detect payload across multiple packets.</p> <p>The evaluator shall verify that the operational guidance provides instructions with how to configure reactions specified in IPS_SBD_EXT.1.5 for each string-based detection signature.</p> <p>The evaluator shall verify that the operational guidance provides instructions with how rules are associated with distinct network interfaces that are capable of being associated with signatures.</p>
<p>Evaluator Findings</p>	<p>The evaluator examined the section titled Configuring the IDP Extended Package in the AGD to verify that it provides instructions on how to configure rules using the packet payload string-based detection fields defined in IPS_SBD_EXT.1.2 and to detect payload across multiple packets. Upon investigation, the evaluator found that the AGD states the CLI commands for the rule configuration and that the ‘Stream’ context can be used to detect payloads across multiple packets.</p> <p>The evaluator also examined the section titled Configuring the IDP Extended Package in the AGD to verify that it provides instructions with how to configure reactions specified in IPS_SBD_EXT.1.5 for each string-based detection signature. Upon investigation, the evaluator found that the AGD states the CLI commands for configuring the specified reactions.</p>

	<p>The evaluator also examined the section titled Configuring the IDP Extended Package in the AGD to verify that it provides instructions with how rules are associated with distinct network interfaces that are capable of being associated with signatures. Upon investigation, the evaluator found that the AGD states the CLI commands for associating rules with distinct network interfaces that are capable of being associated with signatures.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.14.4.5 IPS_SBD_EXT.1.3 TSS

Objective	The evaluator shall verify that the TSS describes how the attacks defined in IPS_SBD_EXT.1.3 are processed by the TOE and what reaction is triggered when these attacks are identified.																						
Evaluator Findings	<p>The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS describes how the attacks defined in IPS_SBD_EXT.1.3 are processed by the TOE and what reaction is triggered when these attacks are identified. Upon investigation, the evaluator found that the TSS states that :</p> <p>Signatures can be defined to match any header-field value using command <code>set security idp custom-attack</code> along with the actions (allow/block), and using command <code>set security idp idp-policy</code> that defines the IDP policy the TOE enforces on matching packets. The matching criteria can be "equal", "greater-than", "less-than" or "not-equal".</p> <p>the TSS also states that :</p> <p>the TOE implements the following pre-defined attack signatures:</p> <table border="1"> <thead> <tr> <th>MOD_IPS signature name</th> <th>Junos screen name</th> </tr> </thead> <tbody> <tr> <td>IP Fragments Overlap (Teardrop attack, Bonk attack, or Boink attack)</td> <td>ip tear-drop</td> </tr> <tr> <td>IP source address equal to the IP destination (Land attack)</td> <td>tcp land</td> </tr> <tr> <td>Fragmented ICMP Traffic (e.g. Nuke attack)</td> <td>icmp fragment</td> </tr> <tr> <td>Large ICMP Traffic (Ping of Death attack)</td> <td>icmp ping-death</td> </tr> <tr> <td>TCP NULL flags</td> <td>tcp tcp-no-flag</td> </tr> <tr> <td>TCP SYN+FIN flags</td> <td>tcp syn-fin</td> </tr> <tr> <td>TCP FIN only flags</td> <td>tcp fin-no-ack</td> </tr> <tr> <td>UDP Bomb Attack</td> <td>udp length-error</td> </tr> <tr> <td>ICMP flooding (Smurf attack, and ping flood)</td> <td>icmp flood</td> </tr> <tr> <td>TCP flooding (e.g. SYN flood)</td> <td>tcp syn-flood</td> </tr> </tbody> </table>	MOD_IPS signature name	Junos screen name	IP Fragments Overlap (Teardrop attack, Bonk attack, or Boink attack)	ip tear-drop	IP source address equal to the IP destination (Land attack)	tcp land	Fragmented ICMP Traffic (e.g. Nuke attack)	icmp fragment	Large ICMP Traffic (Ping of Death attack)	icmp ping-death	TCP NULL flags	tcp tcp-no-flag	TCP SYN+FIN flags	tcp syn-fin	TCP FIN only flags	tcp fin-no-ack	UDP Bomb Attack	udp length-error	ICMP flooding (Smurf attack, and ping flood)	icmp flood	TCP flooding (e.g. SYN flood)	tcp syn-flood
MOD_IPS signature name	Junos screen name																						
IP Fragments Overlap (Teardrop attack, Bonk attack, or Boink attack)	ip tear-drop																						
IP source address equal to the IP destination (Land attack)	tcp land																						
Fragmented ICMP Traffic (e.g. Nuke attack)	icmp fragment																						
Large ICMP Traffic (Ping of Death attack)	icmp ping-death																						
TCP NULL flags	tcp tcp-no-flag																						
TCP SYN+FIN flags	tcp syn-fin																						
TCP FIN only flags	tcp fin-no-ack																						
UDP Bomb Attack	udp length-error																						
ICMP flooding (Smurf attack, and ping flood)	icmp flood																						
TCP flooding (e.g. SYN flood)	tcp syn-flood																						

	<table border="1"> <tr> <td>IP protocol scanning</td> <td>ip unknown-protocol</td> </tr> <tr> <td>TCP port scanning</td> <td>tcp port-scan</td> </tr> <tr> <td>UDP port scanning</td> <td>udp port-scan</td> </tr> <tr> <td>ICMP scanning</td> <td>icmp ip-sweep</td> </tr> </table> <p>Attack Actions are configurable on a rule by rule basis. The default action for the above is to drop the packets. To allow the packets through, the <code>alarm-without-drop</code> action can be defined using command <code>set security screen ids-option</code>.</p> <p>The rules can be applied to any defined interface capable of receiving network traffic.</p> <p>The TOE is also capable of detecting the following signatures:</p> <ul style="list-style-type: none"> • TCP SYN+RST flags, by defining a custom attack to match “protocol tcp tcp-flags rst” and “protocol tcp tcp-flags syn”, • UDP Chargen DoS attack, by configuring a firewall policy to match the predefined “junos-chargen” with the desired allow/block reaction, and • Flooding of a network (DoS attack), by the configuration of policers that allow establishing prioritization and bandwidth limits for different type of network traffic. <p>Based on these findings, this assurance activity is considered satisfied.</p>	IP protocol scanning	ip unknown-protocol	TCP port scanning	tcp port-scan	UDP port scanning	udp port-scan	ICMP scanning	icmp ip-sweep
IP protocol scanning	ip unknown-protocol								
TCP port scanning	tcp port-scan								
UDP port scanning	udp port-scan								
ICMP scanning	icmp ip-sweep								
Verdict	Pass								

5.14.4.6 IPS_SBD_EXT.1.3 Guidance

Objective	The evaluator shall verify that the operational guidance provides instructions with configuring rules to identify the attacks defined in IPS_SBD_EXT.1.3 as well as the reactions to these attacks as specified in IPS_SBD_EXT.1.5.
Evaluator Findings	The evaluator examined the section titled IDP Extended Package Configuration Overview in the AGD to verify that it provides instructions with configuring rules to identify the attacks defined in IPS_SBD_EXT.1.3 as well as the reactions to these attacks as specified in IPS_SBD_EXT.1.5. Upon investigation, the evaluator found that the AGD provides the CLI commands for configuration and reactions of these attacks.
	Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.14.4.7 IPS_SBD_EXT.1.4 TSS

Objective	The evaluator shall verify that the TSS describes how the attacks defined in IPS_SBD_EXT.1.4 are processed by the TOE and what reaction is triggered when these attacks are identified.
Evaluator Findings	The evaluator examined the section titled TOE Summary Specification in the Security Target to verify that the TSS describes how the attacks defined in IPS_SBD_EXT.1.4 are processed by

the TOE and what reaction is triggered when these attacks are identified. Upon investigation, the evaluator found that the TSS states that :

Signatures can be defined to match any header-field value using command `set security idp custom-attack` along with the actions (allow/block), and using command `set security idp idp-policy` that defines the IDP policy the TOE enforces on matching packets. The matching criteria can be "equal", "greater-than", "less-than" or "not-equal".

the TSS also states that :

the TOE implements the following pre-defined attack signatures:

MOD_IPS signature name	Junos screen name
IP Fragments Overlap (Teardrop attack, Bonk attack, or Boink attack)	ip tear-drop
IP source address equal to the IP destination (Land attack)	tcp land
Fragmented ICMP Traffic (e.g. Nuke attack)	icmp fragment
Large ICMP Traffic (Ping of Death attack)	icmp ping-death
TCP NULL flags	tcp tcp-no-flag
TCP SYN+FIN flags	tcp syn-fin
TCP FIN only flags	tcp fin-no-ack
UDP Bomb Attack	udp length-error
ICMP flooding (Smurf attack, and ping flood)	icmp flood
TCP flooding (e.g. SYN flood)	tcp syn-flood
IP protocol scanning	ip unknown-protocol
TCP port scanning	tcp port-scan
UDP port scanning	udp port-scan
ICMP scanning	icmp ip-sweep

Attack Actions are configurable on a rule by rule basis. The default action for the above is to drop the packets. To allow the packets through, the `alarm-without-drop` action can be defined using command `set security screen ids-option`.

The rules can be applied to any defined interface capable of receiving network traffic.

The TOE is also capable of detecting the following signatures:

- **TCP SYN+RST flags, by defining a custom attack to match “`protocol tcp tcp-flags rst`” and “`protocol tcp tcp-flags syn`”,**

	<ul style="list-style-type: none"> • UDP Chargen DoS attack, by configuring a firewall policy to match the predefined “junos-chargen” with the desired allow/block reaction, and • Flooding of a network (DoS attack), by the configuration of policers that allow establishing prioritization and bandwidth limits for different type of network traffic. <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

5.14.4.8 IPS_SBD_EXT.1.4 Guidance

Objective	The evaluator shall verify that the operational guidance provides instructions with configuring rules to identify the attacks defined in IPS_SBD_EXT.1.4 as well as the reactions to these attacks as specified in IPS_SBD_EXT.1.5.
Evaluator Findings	The evaluator examined the section titled Configuring Network Attacks in the AGD to verify that it provides instructions with configuring rules to identify the attacks defined in IPS_SBD_EXT.1.4 as well as the reactions to these attacks as specified in IPS_SBD_EXT.1.5. Upon investigation, the evaluator found that the AGD states the CLI commands needed to configure rules to identify attacks defined in IPS_SBD_EXT.1.4 along with the reactions to these attacks. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.14.4.9 IPS_SBD_EXT.1.6 Guidance

Objective	The evaluator shall verify that the operational guidance provides configuration instructions, if needed, to detect payload across multiple packets.
Evaluator Findings	No separate configuration is needed for detection of payloads across multiple packets since it is covered by the custom signature or custom attack. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

6 Detailed Test Cases (Test Activities)

6.1 Audit

6.1.1 FAU_GEN.1 Test #1

Item	Data
Test Assurance Activity	<p>The evaluator shall test the TOE's ability to correctly generate audit records by having the TOE generate audit records for the events listed in the table of audit events and administrative actions listed above. This should include all instances of an event: for instance, if there are several different I&A mechanisms for a system, the FIA_UIA_EXT.1 events must be generated for each mechanism. The evaluator shall test that audit records are generated for the establishment and termination of a channel for each of the cryptographic protocols contained in the ST. If HTTPS is implemented, the test demonstrating the establishment and termination of a TLS session can be combined with the test for an HTTPS session. When verifying the test results, the evaluator shall ensure the audit records generated during testing match the format specified in the guidance documentation, and that the fields in each audit record have the proper entries.</p> <p>Note that the testing here can be accomplished in conjunction with the testing of the security mechanisms directly.</p>
Test Steps	Covered by audit records in each test case.
Expected Test Results	<ul style="list-style-type: none"> • Audit records should be correctly generated for the relevant events.
Pass/Fail with Explanation	Pass, covered by audit records in each test case.

6.1.2 FAU_STG_EXT.1 Test #1

Item	Data
Test Assurance Activity	<p>Test 1: The evaluator shall establish a session between the TOE and the audit server according to the configuration guidance provided. The evaluator shall then examine the traffic that passes between the audit server and the TOE during several activities of the evaluator's choice designed to generate audit data to be transferred to the audit server. The evaluator shall observe that these data are not able to be viewed in the clear during this transfer, and that they are successfully received by the audit server. The evaluator shall record the particular software (name, version) used on the audit server during testing. The evaluator shall verify that the TOE is capable of transferring audit data to an external audit server automatically without administrator intervention.</p>
Test Steps	<ul style="list-style-type: none"> • Record the audit server name and version information. • Configure the TOE to communicate with a syslog server by generating an ECDSA public key on the remote syslog server.

	<ul style="list-style-type: none"> • On the TOE, create a class named monitor that has permission to trace events. • On the TOE, create a user named syslog-mon with the class monitor and with ECDSA public key authentication. • On the TOE, configure NETCONF with SSH. • The TOE logs that NETCONF client was used. • Verify the traffic between the TOE and syslog is not sent in plaintext.
Expected Test Results	<ul style="list-style-type: none"> • Logs obtained at audit Server verify that Audit data is transferred between itself and TOE. • Packet Capture verifies that traffic between TOE and audit server is not sent in plaintext.
Pass/Fail Explanation	The TOE is capable of transferring audit data to an external audit server automatically without administrator intervention.
Result	Pass.

6.1.3 FAU_STG_EXT.1 Test #2 (b)

Item	Data
Test Assurance Activity	<p>Test 2: The evaluator shall perform operations that generate audit data and verify that this data is stored locally. The evaluator shall perform operations that generate audit data until the local storage space is exceeded and verifies that the TOE complies with the behaviour defined in FAU_STG_EXT.1.3. Depending on the configuration this means that the evaluator has to check the content of the audit data when the audit data is just filled to the maximum and then verifies that:</p> <p>The existing audit data is overwritten with every new auditable event that should be tracked according to the specified rule (for the option 'overwrite previous audit records' in FAU_STG_EXT.1.3)</p>
Test Steps	<ul style="list-style-type: none"> • Set up syslog server on the TOE and configure syslog to log all the messages. • Generate logs. • Verify that the logs are locally stored and when the audit data is filled to the max, the existing audit data is overwritten.
Expected Test Results	<ul style="list-style-type: none"> • Log file verifies that TOE overwrites existing audit data when filled to the maximum.
Pass/Fail Explanation	When audit data is filled to the max, the existing audit data is overwritten.
Result	Pass.

6.1.4 FCS_NTP_EXT.1.1 Test #1

Item	Data
Test Assurance Activity	The version of NTP selected in element 1.1 and specified in the ST shall be verified by observing establishment of a connection to an external NTP server known to be using the specified version(s) of NTP. This may be combined with tests of other aspects of FCS_NTP_EXT.1 as described below.
Test Steps	<p>NTP Version 3:</p> <ul style="list-style-type: none"> • Verify current time on the TOE. • Verify accurate time on the NTP server. • Configure NTP Server on the TOE. • Verify that TOE syncs time from the NTP server. • Verify NTP version with packet capture. • Verify with logs. <p>NTP Version 4:</p> <ul style="list-style-type: none"> • Verify current time on the TOE. • Verify accurate time on the NTP server. • Configure NTP Server on the TOE. • Verify that TOE syncs time from the NTP server. • Verify NTP version with packet capture. • Verify with logs.
Expected Output	<ul style="list-style-type: none"> • TOE is able to successfully establish a connection with the configured NTP server using NTPv3. • Successful connection with the NTP server via NTPv3 seen in packet capture. • Successful connection with the NTP server seen in audit logs. • TOE is able to successfully establish a connection with the configured NTP server using NTPv4. • Successful connection with the NTP server via NTPv4 seen in packet capture. • Successful connection with the NTP server seen in audit logs
Pass/Fail with explanation	Pass. The TOE uses the correct NTP version as per configuration. This meets the testing requirement.

6.1.5 FCS_NTP_EXT.1.2 Test #1

Item	Data
Test Assurance Activity	[Conditional] If the message digest algorithm is claimed in element 1.2, the evaluator will change the message digest algorithm used by the NTP server in such a way that the new value does not match the configuration on the TOE and confirms that the TOE does not synchronize to this time source.

	<p>The evaluator shall use a packet sniffer to capture the network traffic between the TOE and the NTP server. The evaluator uses the captured network traffic, to verify the NTP version, to observe time change of the TOE and uses the TOE's audit log to determine that the TOE accepted the NTP server's timestamp update.</p> <p>The captured traffic is also used to verify that the appropriate message digest algorithm was used to authenticate the time source and/or the appropriate protocol was used to ensure integrity of the timestamp that was transmitted in the NTP packets.</p>
<p>Test Steps</p>	<p>Version 3 (SHA-1):</p> <ul style="list-style-type: none"> • Verify current time on the TOE. • Verify accurate time on the NTP server. • Configure NTP authentication on TOE. • Configure proper authentication on the NTP server. • Verify that NTP authentication and update is successful. • Verify the success with logs. • Verify the success with packet capture. <ul style="list-style-type: none"> • Verify current time on the TOE. • Verify accurate time on the NTP server. • Modify the message digest algorithm used by NTP server. • Verify that NTP update fails. • Verify the failure with packet capture. • Verify the failure with logs. <p>Version 4 (SHA-1):</p> <ul style="list-style-type: none"> • Verify current time on the TOE. • Verify accurate time on the NTP server. • Configure NTP authentication on TOE. • Configure proper authentication on the NTP server. • Verify that NTP authentication and update is successful. • Verify the success with logs. • Verify the success with packet capture. <ul style="list-style-type: none"> • Verify current time on the TOE. • Verify accurate time on the NTP server. • Modify the message digest algorithm used by NTP server. • Verify that NTP update fails. • Verify the failure with packet capture. • Verify the failure with logs. <p>Version 3 (SHA-256):</p> <ul style="list-style-type: none"> • Verify current time on the TOE. • Verify accurate time on the NTP server.

	<ul style="list-style-type: none"> • Configure NTP authentication on TOE. • Configure proper authentication on the NTP server. • Verify that NTP authentication and update is successful. • Verify the success with logs. • Verify the success with packet capture. • Verify current time on the TOE. • Verify accurate time on the NTP server. • Modify the message digest algorithm used by NTP server. • Verify that NTP update fails. • Verify the failure with packet capture. • Verify the failure with logs. Version 4 (SHA-256): • Verify current time on the TOE. • Verify accurate time on the NTP server. • Configure NTP authentication on TOE. • Configure proper authentication on the NTP server. • Verify that NTP authentication and update is successful. • Verify the success logs. • Verify the success with packet capture. • Verify current time on the TOE. • Verify accurate time on the NTP server. • Modify the message digest algorithm used by NTP server. • Verify that NTP update fails. • Verify the failure with packet capture. • Verify the failure with logs.
<p>Expected Output</p>	<ul style="list-style-type: none"> • NTP authentication and update for the configured NTP version and appropriate message digest algorithm is successful. • Logs show successful NTP update for the configured NTP version and appropriate message digest algorithm. • Packet capture shows successful NTP update for the configured NTP version and appropriate message digest algorithm. • NTP authentication and update fails when there is mismatch in message digest algorithm. • Logs show failed NTP authentication/update when there is mismatch in message digest algorithm.

	<ul style="list-style-type: none"> Packet capture shows failed NTP authentication/update when there is mismatch in message digest algorithm.
Pass/Fail with explanation	Pass. NTP update takes place on successful authentication using the appropriate message digest algorithm, while it fails when authentication is not successful. This meets the testing requirement.

6.1.6 FCS_NTP_EXT.1.3 Test #1

Item	Data
Test Assurance Activity	The evaluator shall configure NTP server(s) to support periodic time updates to broadcast and multicast addresses. The evaluator shall confirm the TOE is configured to not accept broadcast and multicast NTP packets that would result in the timestamp being updated. The evaluator shall check that the time stamp is not updated after receipt of the broadcast and multicast packets.
Test Steps	<p>Broadcast:</p> <ul style="list-style-type: none"> Check the current time on the TOE. Check the accurate time on the NTP server. Set NTP server to broadcast to 10.1.1.255. Verify with capture that broadcast packets are sent by NTP server. Verify that the time on the TOE is not modified. <p>Multicast:</p> <ul style="list-style-type: none"> Check the current time on the TOE. Check the accurate time on the NTP server. Set NTP server to multicast to 224.0.1.1. Verify with capture that multicast packets are sent by NTP server. Check the time on TOE and verify that it is not modified due to NTP.
Expected output	<ul style="list-style-type: none"> Broadcast packets sent by the NTP server are not able to update the timestamp on the TOE Multicast packets sent by the NTP server are not able to update the timestamp on the TOE
Pass/Fail with explanation	Pass. The TOE time stamp is not updated after receipt of the broadcast and multicast packets. This meets the testing requirement.

6.1.7 FCS_NTP_EXT.1.4 Test #1

Item	Data
------	------

Test Assurance Activity	<p>The evaluator shall confirm the TOE supports configuration of at least three (3) NTP time sources. The evaluator shall configure at least three NTP servers to support periodic time updates to the TOE. The evaluator shall confirm the TOE is configured to accept NTP packets that would result in the timestamp being updated from each of the NTP servers. The evaluator shall check that the time stamp is updated after receipt of the NTP packets. The purpose of this test is to verify that the TOE can be configured to synchronize with multiple NTP servers. It is up to the evaluator to determine that the multi-source update of the time information is appropriate and consistent with the behaviour prescribed by the RFC 1305 for NTPv3 and RFC 5905 for NTPv4.</p> <p><i>TD0528 applied</i></p>
Test Steps	<p>NTP Version 3:</p> <ul style="list-style-type: none"> • Verify the current time on the TOE. • Configure at least 3 NTP time sources on the TOE. • Verify that the TOE updates times from the configured NTP servers. • Verify successful time update from configured servers with packet capture. • Verify successful time update with the help of logs. <p>NTP Version 4:</p> <ul style="list-style-type: none"> • Verify the current time on the TOE. • Configure at least 3 NTP time sources on the TOE. • Verify that the TOE updates times from the configured NTP servers. • Verify successful time update from configured servers with packet capture. • Verify successful time update with the help of logs.
Expected Output	<ul style="list-style-type: none"> • TOE supports configuration of at least three NTP servers. • The TOE is able to successfully synchronize time with the configured NTP servers.
Pass/Fail with Explanation	<p>Pass. The TOE can be configured to synchronize time with at least three NTP servers. This meets the testing requirement.</p>

6.1.8 FCS_NTP_EXT.1.4 Test #2

Item	Data
Test Assurance Activity	<p>Test 2: (The intent of this test is to ensure that the TOE would only accept NTP updates from configured NTP Servers). The evaluator shall confirm that the TOE would not synchronize to other, not explicitly configured time sources by sending an otherwise valid but unsolicited NTP Server responses indicating different time from the TOE's current system time. This rogue time source needs to be configured in a way (e.g. degrade or disable valid and configured NTP servers) that could plausibly result in unsolicited updates becoming a preferred time source if</p>

	<p>they are not discarded by the TOE. The TOE is not mandated to respond in a detectable way or audit the occurrence of such unsolicited updates. The intent of this test is to ensure that the TOE would only accept NTP updates from configured NTP Servers. It is up to the evaluator to craft and transmit unsolicited updates in a way that would be consistent with the behaviour of a correctly functioning NTP server.</p> <p>TD0528 applied</p>
Test Steps	<ul style="list-style-type: none"> • Verify the time on the TOE. • Configure an NTP server on the TOE. • Sync the TOE with NTP server and capture those packets. • Verify with Packet Capture. • Configure a different NTP server to which the TOE syncs. • Replay the packets from the NTP server which were captured during earlier sync. • Verify the TOE does not sync with the different NTP server.
Expected Output	<ul style="list-style-type: none"> • The timestamp on the TOE isn't modified by an unconfigured or rogue NTP server.
Pass/Fail with Explanation	<p>Pass. The TOE only accepts NTP updates from configured NTP Servers. This meets the testing requirements.</p>

6.1.9 FPT_STM_EXT.1 Test #1

Item	Data
Test Assurance Activity	<p>Test 1: If the TOE supports direct setting of the time by the Security Administrator then the evaluator uses the guidance documentation to set the time. The evaluator shall then use an available interface to observe that the time was set correctly.</p>
Test Steps	<ul style="list-style-type: none"> • Confirm the current time on the TOE. • Set a new time on the TOE. • Verify the TOE logged the time change.
Expected Test Results	<ul style="list-style-type: none"> • TOE logs show that a new time was set.
Pass/Fail Explanation	<p>The TOE allows the administrative user to configure the time on the TOE.</p>
Result	<p>Pass.</p>

6.1.10 FPT_STM_EXT.1 Test #2

Item	Data
------	------

Test Assurance Activity	Test 2: If the TOE supports the use of an NTP server ; the evaluator shall use the guidance documentation to configure the NTP client on the TOE, and set up a communication path with the NTP server. The evaluator will observe that the NTP server has set the time to what is expected. If the TOE supports multiple protocols for establishing a connection with the NTP server, the evaluator shall perform this test using each supported protocol claimed in the guidance documentation.
Test Steps	<ul style="list-style-type: none"> • Confirm the current time on the TOE. • Verify the accurate time on the NTP server. • Configure NTP support on the TOE via SSH. • Verify that the new time is set. • Verify with logs and packet capture.
Expected Output	<ul style="list-style-type: none"> • The TOE is able to allow time updates from a configured NTP server. • Audit logs showing the time on the TOE is set by a NTP server. • Packet capture showing the time on the TOE is set by a NTP server.
Pass/Fail with explanation	Pass. The TOE was able to be configured to use an NTP server as a time source. This meets the testing requirements.

6.1.11 FPT_STM_EXT.1 Test #3

Item	Data
Test Assurance Activity	If the audit component of the TOE consists of several parts with independent time information , then the evaluator shall verify that the time information between the different parts are either synchronized or that it is possible for all audit information to relate the time information of the different part to one base information unambiguously.
Pass/Fail Explanation	As per ST TOE's audit component does not consist of several parts with independent time information.
Result	NA.

6.1.12 FTP_ITC.1 Test #1

Item	Data
Test Assurance Activity	The evaluators shall ensure that communications using each protocol with each authorized IT entity is tested during the course of the evaluation, setting up the connections as described in the guidance documentation and ensuring that communication is successful.
Pass/Fail Explanation	External connections from the TOE are sent via an encrypted channel. This testing is covered by the requirements in FAU_STG_EXT.1 for SSH to the syslog server and in FCS_IPSEC_EXT.1.1 for VPN communications. This meets the testing requirements.
Result	Pass.

6.1.13 FTP_ITC.1 Test #2

Item	Data
Test Assurance Activity	For each protocol that the TOE can initiate as defined in the requirement, the evaluator shall follow the guidance documentation to ensure that in fact the communication channel can be initiated from the TOE.
Pass/Fail Explanation	Each communication channel can be initiated from the TOE. This testing is covered by the requirements in FAU_STG_EXT.1 for SSH to the syslog server and in FCS_IPSEC_EXT.1.1 for VPN communications.
Result	Pass.

6.1.14 FTP_ITC.1 Test #3

Item	Data
Test Assurance Activity	The evaluator shall ensure, for each communication channel with an authorized IT entity, the channel data is not sent in plaintext.
Pass/Fail Explanation	This testing is covered by the requirements in FCS_SSHS_EXT.1 and FCS_IPSEC_EXT.1.1 Test #1.
Result	Pass.

6.1.15 FTP_ITC.1 Test #4

Item	Data
Test Assurance Activity	<p>Objective: The objective of this test is to ensure that the TOE reacts appropriately to any connection outage or interruption of the route to the external IT entities.</p> <p>The evaluator shall, for each instance where the TOE acts as a client utilizing a secure communication mechanism with a distinct IT entity, physically interrupt the connection of that IT entity for the following durations:</p> <ol style="list-style-type: none"> 1. A duration that exceeds the TOE’s application layer timeout setting, 2. A duration shorter than the application layer timeout but of sufficient length to interrupt the network link layer. <p>The evaluator shall ensure that, when the physical connectivity is restored, communications are appropriately protected and no TSF data is sent in plaintext.</p> <p>In the case where the TOE is able to detect when the cable is removed from the device, another physical network device (e.g. a core switch) shall be used to interrupt the connection between the TOE and the distinct IT entity. The interruption shall not be performed at the virtual node (e.g. virtual switch) and must be physical in nature.</p>
Test Steps	<ul style="list-style-type: none"> • Set the application layer timeout value to 10 seconds. • Initiate an SSH connection between TOE and syslog server, unplug the appropriate network cable for 5 seconds and verify that the connection is interrupted.

	<ul style="list-style-type: none"> • Reconnect the network cable and verify that the traffic is encrypted when connection gets restored. • Initiate an SSH connection between TOE and syslog server, unplug the appropriate network cable for 15 seconds and verify that the connection is interrupted. • Reconnect the network cable and verify that the traffic is encrypted when connection gets restored. • Set the application layer timeout value to 10 seconds. • Initiate an IPsec connection between TOE and Peer, unplug the appropriate network cable for 5 seconds and verify that the connection is interrupted. • Reconnect the network cable and verify that the traffic is encrypted when connection gets restored. • Initiate an IPsec connection between TOE and syslog server, unplug the appropriate network cable for 5 seconds and verify that the connection is interrupted. • Reconnect the network cable and verify that the traffic is encrypted when connection gets restored.
Expected Output	<ul style="list-style-type: none"> • TSF data is protected and not sent in plaintext once the physical connectivity is restored.
Pass/Fail with explanation	Pass. The TOE responds accordingly when a physical disconnection occurs. This meets the testing requirements.

6.2 Auth

6.2.1 FAU_STG.1 Test #1

Item	Data
Test Assurance Activity	<p>Test 1: The evaluator shall access the audit trail without authentication as Security Administrator (either by authentication as a non-administrative user, if supported, or without authentication at all) and attempt to modify and delete the audit records. The evaluator shall verify that these attempts fail.</p> <p>According to the implementation no other users than the Security Administrator might be defined and without any user authentication the user might not be able to get to the point where the attempt to access the audit trail can be executed. In that case it shall be demonstrated that access control mechanisms prevent execution up to the step that can be reached without authentication as Security Administrator.</p>
Test Steps	<ul style="list-style-type: none"> • Show the available user profiles. • Log onto the TOE with read-only profile. • Attempt to modify and delete the audit records. • The TOE did not allow an unauthenticated user to modify and delete the audit records.

Expected Test Results	<ul style="list-style-type: none"> • TOE denies access to non-administrative user to modify audit records.
Pass/Fail Explanation	The TOE does not allow an unauthenticated user to modify and delete the audit records.
Result	Pass.

6.2.2 FAU_STG.1 Test #2

Item	Data
Test Assurance Activity	The evaluator shall access the audit trail as an authorized administrator and attempt to delete the audit records. The evaluator shall verify that these attempts succeed. The evaluator shall verify that only the records authorized for deletion are deleted.
Test Steps	<ul style="list-style-type: none"> • Show the available user profiles. • Log onto the TOE with an authorized super user profile of acumensec. • Attempt to delete the audit records. • The attempt to delete the audit record was successful.
Expected Test Results	<ul style="list-style-type: none"> • TOE allows an authorized administrator to delete audit records. • TOE logs verify it allows an authorized administrator to delete audit records.
Pass/Fail Explanation	The TOE allows an authorized administrator to delete the audit records.
Result	Pass.

6.2.3 FCS_CKM.1 FFC

Item	Data
Test Assurance Activity	<p>Note: The following tests require the developer to provide access to a test platform that provides the evaluator with tools that are typically not found on factory products. Generation of long-term cryptographic keys (i.e. keys that are not ephemeral keys/session keys) might be performed automatically (e.g. during initial start-up). Testing of key generation must cover not only administrator invoked key generation but also automated key generation (if supported).</p> <p>Key Generation for Finite-Field Cryptography (FFC) The evaluator shall verify the implementation of the Parameters Generation and the Key Generation for FFC by the TOE using the Parameter Generation and Key Generation test. This test verifies the ability of the TSF to correctly produce values for the field prime p, the cryptographic prime q (dividing $p-1$), the cryptographic group generator g, and the calculation of the private key x and public key y.</p>

	<p>The Parameter generation specifies 2 ways (or methods) to generate the cryptographic prime q and the field prime p:</p> <ul style="list-style-type: none"> • Primes q and p shall both be provable primes • Primes q and field prime p shall both be probable primes <p>and two ways to generate the cryptographic group generator g:</p> <ul style="list-style-type: none"> • Generator g constructed through a verifiable process • Generator g constructed through an unverifiable process. <p>The Key generation specifies 2 ways to generate the private key x:</p> <ul style="list-style-type: none"> • $\text{len}(q)$ bit output of RBG where $1 \leq x \leq q-1$ • $\text{len}(q) + 64$ bit output of RBG, followed by a mod $q-1$ operation and a $+1$ operation, where $1 \leq x \leq q-1$. <p>The security strength of the RBG must be at least that of the security offered by the FFC parameter set.</p> <p>To test the cryptographic and field prime generation method for the provable primes method and/or the group generator g for a verifiable process, the evaluator must seed the TSF parameter generation routine with sufficient data to deterministically generate the parameter set.</p> <p>For each key length supported, the evaluator shall have the TSF generate 25 parameter sets and key pairs. The evaluator shall verify the correctness of the TSF's implementation by comparing values generated by the TSF with those generated from a known good implementation. Verification must also confirm</p> <ul style="list-style-type: none"> • $g \neq 0,1$ • q divides $p-1$ • $g^q \text{ mod } p = 1$ • $g^x \text{ mod } p = y$ <p>for each FFC parameter set and key pair.</p> <p>FFC Schemes using "safe-prime" groups Testing for FFC Schemes using safe-prime groups is done as part of testing in CKM.2.1.</p> <p>TD0580 has been applied.</p>
Pass/Fail with Explanation	This testing was performed as part of testing in CKM.2.1.
Result	Pass.

6.2.4 FCS_CKM.2 RSA

Item	Data
Test Assurance Activity	Key Establishment Schemes The evaluator shall verify the correctness of the TSF's implementation of RSAES-PKCS1-v1_5 by using a known good implementation for each protocol selected in FTP_TRP.1/Admin, FTP_TRP.1/Join, FTP_ITC.1 and FPT_ITT.1 that uses RSAES-PKCS1-v1_5.
Pass/Fail Explanation	This is not claimed in ST.
Result	NA.

6.2.5 FCS_CKM.2 DH14

This test was removed by TD0580.

6.2.6 FCS_CKM.2 FCC

Item	Data
Test Assurance Activity	FCC Schemes using "safe-prime" groups The evaluator shall verify the correctness of the TSF's implementation of safe-prime groups by using a known good implementation for each protocol selected in FTP_TRP.1/Admin, FTP_TRP.1/Join, FTP_ITC.1 and FPT_ITT.1 that uses safe-prime groups. This test must be performed for each safe-prime group that each protocol uses.
Pass/Fail Explanation	This testing was performed in conjunction with FTP_TRP.1/Admin Test #1 and FTP_ITC.1 Test #1 to demonstrate correct operation.
Result	Pass.

6.2.7 FIA_AFL.1 Test #1

Item	Data
Test Assurance Activity	The evaluator shall perform the following tests for each method by which remote administrators access the TOE (e.g., any passwords entered as part of establishing the connection protocol or the remote administrator application): Test 1: The evaluator shall use the operational guidance to configure the number of successive unsuccessful authentication attempts allowed by the TOE (and, if the time period selection in FIA_AFL.1.2 is included in the ST, then the evaluator shall also use the operational guidance to configure the time period after which access is re-enabled). The evaluator shall test that once the authentication attempts limit is reached, authentication attempts with valid credentials are no longer successful.
Test Steps	<ul style="list-style-type: none"> Set user login time out after successive unsuccessful authentication attempts.

	<ul style="list-style-type: none"> • Start a SSH session with the TOE and attempt to login with wrong password and lock the user. • Verify the user is locked out for configured time with logs. • Attempt to open another connection and attempt to login with valid password before the lockout period expires. • Verify with logs the attempt failed due to lockout account.
Expected Test Results	<ul style="list-style-type: none"> • TOE logs verify that user is lockout for configured time after set successive unsuccessful authentication attempts. • TOE logs verify that user is unable to login during the lockout period.
Pass/Fail Explanation	The TOE did not allow authentication once the authentication attempt limit has been reached.
Result	Pass.

6.2.8 FIA_AFL.1 Test #2b

Item	Data
Test Assurance Activity	<p>The evaluator shall perform the following tests for each method by which remote administrators access the TOE (e.g. any passwords entered as part of establishing the connection protocol or the remote administrator application):</p> <p>Test 2: After reaching the limit for unsuccessful authentication attempts as in Test 1 above, the evaluator shall proceed as follows:</p> <p>If the time period selection in FIA_AFL.1.2 is included in the ST, then the evaluator shall wait for just less than the time period configured in Test 1 and show that an authorisation attempt using valid credentials does not result in successful access. The evaluator shall then wait until just after the time period configured in Test 1 and show that an authorisation attempt using valid credentials results in successful access.</p>
Test Steps	<ul style="list-style-type: none"> • Set a user lockout after continuous unsuccessful authentication attempts. • Start an SSH session with the TOE and attempt to login with wrong passwords and lockout the user. • Verify with logs that the user has been locked out. • Verify that the lockout time matches the configured lockout period. • Confirm that an attempt to establish an SSH session with correct credentials just before the end of the lockout period fails. • Verify that the user gets unlocked after the end of the lockout period. • Confirm that an attempt to establish an SSH session with correct credentials succeeds now.
Expected Test Results	<ul style="list-style-type: none"> • TOE logs verify that user is lockout for configured time after set successive unsuccessful authentication attempts. • TOE logs verify that user is able to login successfully after the lockout period.

Pass/Fail Explanation	The TOE did not allow authentication until the configured lock-out time period had expired or an administrator unlocks the account.
Result	Pass.

6.2.9 FIA_PMG_EXT.1 Test #1

Item	Data
Test Assurance Activity	The evaluator shall compose passwords that meet the requirements in some way. For each password, the evaluator shall verify that the TOE supports the password. While the evaluator is not required (nor is it feasible) to test all possible compositions of passwords, the evaluator shall ensure that all characters, and a minimum length listed in the requirement are supported and justify the subset of those characters chosen for testing.
Test Steps	<ul style="list-style-type: none"> • Set the minimum password length to 10 characters. • Attempt to create 3 users (good11, good22, good33) that meet the password requirements. • Username: "good11" and Password: "Good@12345" • Username: "good22" and Password: "gOOd!@#\$\$%67890" • Username: "good33" and Password: "12345^&*()good" • Try to establish a TOE connection using all above 3 users that meet the password requirements.
Expected Test Results	<ul style="list-style-type: none"> • TOE supports configuring password according to requirements. • TOE allows successful authentication with passwords matching the requirements. • TOE logs verify successful authentication with passwords matching the requirements.
Pass/Fail Explanation	The TOE was able to create users with good passwords and reject user creation with bad passwords.
Result	Pass.

6.2.10 FIA_PMG_EXT.1 Test #2

Item	Data
Test Assurance Activity	The evaluator shall compose passwords that do not meet the requirements in some way. For each password, the evaluator shall verify that the TOE does not support the password. While the evaluator is not required (nor is it feasible) to test all possible compositions of passwords, the evaluator shall ensure that the TOE enforces the allowed characters and the minimum length listed in the requirement and justify the subset of those characters chosen for testing.
Test Steps	<ul style="list-style-type: none"> • Attempt to create 3 users (bad4, bad5, bad6) that do not meet the password requirements. The TOE did not allow the creation of these accounts as they did not meet the password length or complexity set by the TOE. • Username: "bad11" and Password: "BAD12345^&*()". • Username: "bad22" and Password: "123\$%^Bad". • Username: "bad33" and Password: "1234567890bad".

Expected Test Results	<ul style="list-style-type: none"> • TOE denies configuring password not meeting the requirements.
Pass/Fail Explanation	The TOE is able to reject users with bad passwords. This meets the requirement.
Result	Pass.

6.2.11 FIA_UIA_EXT.1 Test #1

Item	Data
Test Assurance Activity	<p>The evaluator shall perform the following tests for each method by which administrators access the TOE (local and remote), as well as for each type of credential supported by the login method:</p> <p>Test 1: The evaluator shall use the guidance documentation to configure the appropriate credential supported for the login method. For that credential/login method, the evaluator shall show that providing correct I&A information results in the ability to access the system, while providing incorrect information results in denial of access.</p>
Test Steps	<p><u>Local</u></p> <ul style="list-style-type: none"> • Attempt to log into the TOE via console with bad credentials; this should fail with TOE logs. • Attempt to log into the TOE via console with good credentials; this should succeed with TOE logs. <p><u>Remote (password-based)</u></p> <ul style="list-style-type: none"> • Log into the TOE via SSH with bad credentials; this should fail. • Log into the TOE via SSH with good credentials; this should succeed. • Verify audit logs reflect both attempts. <p><u>Remote (public key-based)</u></p> <ul style="list-style-type: none"> • Log into the TOE via SSH with bad credentials; this should fail. • Log into the TOE via SSH with good credentials; this should succeed. • Verify audit logs reflect both attempts.
Expected Test Results	<ul style="list-style-type: none"> • TOE denies user authentication using incorrect credentials. • TOE successfully authenticates user with correct credentials.
Pass/Fail Explanation	The TOE denies access when the incorrect authentication credentials are presented and allows access when the correct authentication credentials are presented.
Result	Pass.

6.2.12 FIA_UIA_EXT.1 Test #2

Item	Data
Test Assurance Activity	<p>The evaluator shall perform the following tests for each method by which administrators access the TOE (local and remote), as well as for each type of credential supported by the login method:</p> <p>Test 2: The evaluator shall configure the services allowed (if any) according to the guidance documentation, and then determine the services available to an external remote entity. The evaluator shall determine that the list of services available is limited to those specified in the requirement.</p>
Test Steps	<p><u>Password-based</u></p> <ul style="list-style-type: none"> • Show that the Ping is allowed prior to authentication. • Show that commands are not available prior to login with authentication logs reflect failure. • Verify authentication logs reflect failure. • Verify that only the login banner was displayed and observe that TOE allows the establishment of SSH session with remote management station prior to identification and authentication process. • Login into the TOE. • Show that the previously enabled commands are now available. • Verify authentication logs reflect success. <p><u>Public key-based</u></p> <ul style="list-style-type: none"> • Show that the Ping is allowed prior to authentication. • Show that commands are not available prior to login with authentication logs reflect failure. • Verify authentication logs reflect failure. • Verify that only the login banner was displayed and observe that TOE allows the establishment of SSH session with remote management station prior to identification and authentication process. • Login into the TOE. • Show that the previously enabled commands are now available. • Verify authentication logs reflect success.
Expected Test Results	<ul style="list-style-type: none"> • TOE allows only banner and ICMP echo services prior to authentication.
Pass/Fail Explanation	<p>No system services are available to an unauthenticated user connecting remotely. This meets the testing requirements.</p>
Result	<p>Pass.</p>

6.2.13 FIA_UIA_EXT.1 Test #3

Item	Data
------	------

Test Assurance Activity	The evaluator shall perform the following tests for each method by which administrators access the TOE as well as for each type of credential supported by the login method: Test 3: For local access, the evaluator shall determine what services are available to a local administrator and make sure this list is consistent with the requirement.
Test Steps	<ul style="list-style-type: none"> • Show that commands are not available prior to login. • Verify authentication logs reflect failure. • Verify that only the login banner was displayed. • Login into the TOE. • Show that the previously enabled commands are now available. • Verify authentication logs reflect success.
Expected Test Results	<ul style="list-style-type: none"> • TOE allows only banner and ICMP echo services prior to authentication.
Pass/Fail Explanation	No system services are available to an unauthenticated user connecting via locally except the banner. This testing requirements.
Result	Pass.

6.2.14 FIA_UAU.7 Test #1

Item	Data
Test Assurance Activity	The evaluator shall perform the following test for each method of local login allowed: The evaluator shall locally authenticate to the TOE. While making this attempt, the evaluator shall verify that at most obscured feedback is provided while entering the authentication information.
Test Steps	<ul style="list-style-type: none"> • Connect to the TOE via console with correct authentication credentials. • Verifying the logs reflects for local login. • Connect to the TOE via local console with incorrect authentication credentials. • Verifying the logs reflects for local login.
Expected Test Results	<ul style="list-style-type: none"> • TOE gives a obscured feedback after entering the correct credentials. • TOE gives a obscured feedback after entering the incorrect credentials.
Pass/Fail Explanation	At both the directly connected and remote login prompt, the TOE does not provide any feedback.
Result	Pass.

6.2.15 FMT_MOF.1/ManualUpdate Test #1

Item	Data
------	------

Test Assurance Activity	The evaluator shall try to perform the update using a legitimate update image without prior authentication as Security Administrator (either by authentication as a user with no administrator privileges or without user authentication at all – depending on the configuration of the TOE). The attempt to update the TOE shall fail.
Test Steps	<ul style="list-style-type: none"> • Create a read only user to attempt to perform an update. • Verify that the user “tester” fails to update the TOE, as he is not authorized to change the settings. • Verify via logs.
Expected Test Results	<ul style="list-style-type: none"> • TOE does not allow image update by a non security administrator. • TOE logs verify that image update by a non security administrator is denied.
Pass/Fail Explanation	The TOE does not allow update of image without an administrator privilege.
Result	Pass.

6.2.16 FMT_MOF.1/ManualUpdate Test #2

Item	Data
Test Assurance Activity	The evaluator shall try to perform the update with prior authentication as Security Administrator using a legitimate update image. This attempt should be successful. This test case should be covered by the tests for FPT_TUD_EXT.1 already.
Pass/Fail Explanation	Security Administrator able to perform the update with prior authentication using a legitimate image. This meets the testing requirements.
Result	Pass.

6.2.17 FMT_MOF.1/Functions (1) Test #1

Item	Data
Test Assurance Activity	Test 1 (if ‘ transmission of audit data to external IT entity ’ is selected from the second selection together with ‘ modify the behaviour of ’ in the first selection): The evaluator shall try to modify all security related parameters for configuration of the transmission protocol for transmission of audit data to an external IT entity without prior authentication as Security Administrator (by authentication as a user with no administrator privileges or without user authentication at all). Attempts to modify parameters without prior authentication should fail. According to the implementation no other users than the Security Administrator might be defined and without any user authentication the user might not be able to get to the point where the attempt to modify the security related parameters can be executed. In that case it shall be demonstrated that

	access control mechanisms prevent execution up to the step that can be reached without authentication as Security Administrator.
Test Steps	<ul style="list-style-type: none"> • Log into the TOE as a lower privileged user. • Make sure that “tester” is lower privileged user. • Attempt to modify the parameters involved with the syslog server and verify the command is rejected. • Verify the logs.
Expected Test Results	<ul style="list-style-type: none"> • TOE prevents a non security administrator to modify security related parameters.
Pass/Fail Explanation	User without prior authentication/privilege was unable to modify the audit server connection on the TOE
Result	Pass.

6.2.18 FMT_MOF.1/Functions (1)Test #2

Item	Data
Test Assurance Activity	<p>Test 2 (if 'transmission of audit data to external IT entity' is selected from the second selection together with 'modify the behaviour of' in the first selection): The evaluator shall try to modify all security related parameters for configuration of the transmission protocol for transmission of audit data to an external IT entity with prior authentication as Security Administrator. The effects of the modifications should be confirmed.</p> <p>The evaluator does not have to test all possible values of the security related parameters for configuration of the transmission protocol for transmission of audit data to an external IT entity but at least one allowed value per parameter.</p>
Pass/Fail Explanation	User with prior authentication/privilege was able to modify the audit server connection on the TOE.
Result	Pass.

6.2.19 FMT_MOF.1/Functions (2) Test #1

Item	Data
Test Assurance Activity	<p>Test 1 (if 'handling of audit data' is selected from the second selection together with 'modify the behaviour of' in the first selection): The evaluator shall try to modify all security related parameters for configuration of the handling of audit data without prior authentication as Security Administrator (by authentication as a user with no administrator privileges or without user authentication at all). Attempts to modify parameters without prior authentication should fail. According to the implementation no other users than the Security Administrator might be defined and without any user authentication the user might not be able to get to the point where the attempt can be executed. In that case it shall be demonstrated that access control mechanisms prevent execution up to the step that can be reached without authentication as Security Administrator. The term 'handling of audit data'</p>

	refers to the different options for selection and assignments in SFRs FAU_STG_EXT.1.2, FAU_STG_EXT.1.3 and FAU_STG_EXT.2/LocSpace.
Test Steps	<ul style="list-style-type: none"> • Log into the TOE as a lower privileged user. • Make sure that “tester” is lower privileged user. • Attempt to modify the parameters involved with the syslog server and verify the command is rejected. • Verify the logs.
Expected Test Results	<ul style="list-style-type: none"> • TOE prevents a non security administrator to modify security related parameters for configuration of the handling of audit data.
Pass/Fail Explanation	User without prior authentication/privilege was unable to modify parameters for configuration of the handling of audit data on the TOE.
Result	Pass.

6.2.20 FMT_MOF.1/Functions (2) Test #2

Item	Data
Test Assurance Activity	<p>Test 2 (if 'handling of audit data' is selected from the second selection together with 'modify the behaviour of' in the first selection): The evaluator shall try to modify all security related parameters for configuration of the handling of audit data with prior authentication as Security Administrator. The effects of the modifications should be confirmed. The term 'handling of audit data' refers to the different options for selection and assignments in SFRs FAU_STG_EXT.1.2, FAU_STG_EXT.1.3 and FAU_STG_EXT.2/LocSpace.</p> <p>The evaluator does not necessarily have to test all possible values of the security related parameters for configuration of the handling of audit data but at least one allowed value per parameter.</p>
Test Steps	<ul style="list-style-type: none"> • Login to the TOE as an admin. • Make sure that “acumensec” is privileged user. • Attempt to modify the parameters involved with the syslog server. • Verify the logs.
Expected Test Results	<ul style="list-style-type: none"> • TOE allows a security administrator to modify security related parameters for configuration of the handling of audit data. • TOE logs verify that it allows a security administrator to modify security related parameters for configuration of the handling of audit data.
Pass/Fail Explanation	User with prior authentication/privilege was able to modify parameters for configuration of the handling of audit data on the TOE.
Result	Pass.

6.2.21 FMT_MOF.1/Services Test #1

Item	Data
------	------

Test Assurance Activity	The evaluator shall try to enable and disable at least one of the services as defined in the Application Notes for FAU_GEN.1.1 (whichever is supported by the TOE) without prior authentication as Security Administrator (either by authenticating as a user with no administrator privileges, if possible, or without prior authentication at all). The attempt to enable/disable this service/these services should fail. According to the implementation no other users than the Security Administrator might be defined and without any user authentication the user might not be able to get to the point where the attempt to enable/disable this service/these services can be executed. In that case it shall be demonstrated that access control mechanisms prevent execution up to the step that can be reached without authentication as Security Administrator.
Test Steps	<ul style="list-style-type: none"> • Start a SSH session onto the TOE with lower privilege user. • Attempt to enable and disable the services. • Verify with audit logs.
Expected Test Results	<ul style="list-style-type: none"> • TOE does not allow a non security administrator to enable or disable services.
Pass/Fail Explanation	The TOE does not allow an unprivileged user to enable or disable the services.
Result	Pass.

6.2.22 FMT_MOF.1/Services Test #2

Item	Data
Test Assurance Activity	The evaluator shall try to enable and disable at least one of the services as defined in the Application Notes for FAU_GEN.1.1 (whichever is supported by the TOE) with prior authentication as Security Administrator. The attempt to enable/disable this service/these services should be successful.
Test Steps	<ul style="list-style-type: none"> • Start a SSH session onto the TOE with admin user. • Attempt to enable and disable the services. • Verify with audit logs.
Expected Test Results	<ul style="list-style-type: none"> • TOE allows a security administrator to enable or disable services. • TOE logs verify it allows a security administrator to enable or disable services.
Pass/Fail Explanation	The TOE allows the enabling and disabling of services when authenticated a security administrator.
Result	Pass.

6.2.23 FMT_MTD.1/CryptoKeys Test #1

Item	Data
------	------

Test Assurance Activity	The evaluator shall try to perform at least one of the related actions (modify, delete, generate/import) without prior authentication as Security Administrator (either by authentication as a non-administrative user, if supported, or without authentication at all). Attempts to perform related actions without prior authentication should fail. According to the implementation no other users than the Security Administrator might be defined and without any user authentication the user might not be able to get to the point where the attempt to manage cryptographic keys can be executed. In that case it shall be demonstrated that access control mechanisms prevent execution up to the step that can be reached without authentication as Security Administrator.
Test Steps	<ul style="list-style-type: none"> Start a SSH session onto the TOE with non-administrator user. Attempt to modify SSH ciphers by non-administrative user. This will fail.
Expected Test Results	<ul style="list-style-type: none"> TOE does not allow non-administrative user to modify cryptographic keys.
Pass/Fail Explanation	The TOE does not allow the modification of SSH ciphers via CLI for an unprivileged user.
Result	Pass.

6.2.24 FMT_MTD.1/CryptoKeys Test #2

Item	Data
Test Assurance Activity	The evaluator shall try to perform at least one of the related actions with prior authentication as Security Administrator. This attempt should be successful.
Test Steps	<ul style="list-style-type: none"> Start a SSH session onto the TOE with security administrator user. Log into the TOE, attempt to modify SSH ciphers. This will succeed. Verify via logs.
Expected Test Results	<ul style="list-style-type: none"> TOE allows security administrator user to modify cryptographic keys. TOE logs verify that it allows security administrator user to modify cryptographic keys.
Pass/Fail Explanation	The TOE allows the modification of SSH ciphers when authenticated a security administrator.
Result	Pass.

6.2.25 FMT_SMF.1 Test #1

Item	Data
Test Assurance Activity	The evaluator tests management functions as part of testing the SFRs identified in section 2.4.4. No separate testing for FMT_SMF.1 is required unless one of the management functions in FMT_SMF.1.1 has not already been exercised under any other SFR.
Test Steps	<p>The TSF shall be capable of performing the following management functions:</p> <ul style="list-style-type: none"> <i>Ability to administer the TOE locally and remotely;</i>

- Ability to configure the access banner;
- Ability to configure the session inactivity time before session termination or locking;
- Ability to update the TOE, and to verify the updates using **digital signature and [X.509 Certificate, published hash]** capability prior to installing those updates;
- Ability to configure the authentication failure parameters for FIA_AFL.1;
- Definition of packet filtering rules;
- Association of packet filtering rules to network interfaces;
- Ordering of packet filtering rules by priority;
- Ability to configure firewall rules;
- Enable, disable signatures applied to sensor interfaces, and determine the behavior of IPS functionality
- Modify these parameters that define the network traffic to be collected and analyzed:
 - Source IP addresses (host address and network address)
 - Destination IP addresses (host address and network address)
 - Source port (TCP and UDP)
 - Destination port (TCP and UDP)
 - Protocol (IPv4 and IPv6)
 - ICMP type and code
- Update (import) signatures
- Create custom signatures
- Configure anomaly detection
- Enable and disable actions to be taken when signature or anomaly matches are detected
- Modify thresholds that trigger IPS reactions
- Modify the duration of traffic blocking actions
- Modify the known-good and known-bad lists (of IP addresses or address ranges)
- Configure the known-good and known-bad lists to override signature-based IPS policies
- **Ability to manage the cryptographic keys;**
- **Ability to configure the cryptographic functionality;**
- **Ability to configure the lifetime for IPsec SAs;**
- **Ability to import X.509v3 certificates to the TOE's trust store;**
- [
 - Ability to start and stop services;
 - Ability to modify the behavior of the transmission of audit data to an external IT entity, the handling of audit data, the audit functionality when Local Audit Storage Space is full;
 - Ability to configure thresholds for SSH rekeying;
 - Ability to re-enable an Administrator account;
 - Ability to set the time which is used for time-stamps;
 - Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors;
 - No other capabilities].

Pass/Fail Explanation	All management functions identified have been tested throughout the evaluation. Thus, this requirement has been met.
Result	Pass.

6.2.26 FMT_SMR.2 Test #1

Item	Data
Test Assurance Activity	In the course of performing the testing activities for the evaluation, the evaluator shall use all supported interfaces, although it is not necessary to repeat each test involving an administrative action with each interface. The evaluator shall ensure, however, that each supported method of administering the TOE that conforms to the requirements of this cPP be tested; for instance, if the TOE can be administered through a local hardware interface; SSH; and TLS/HTTPS; then all three methods of administration must be exercised during the evaluation team's test activities.
Pass/Fail Explanation	Testing has used local console and SSH access, therefore covering all methods of administration
Result	Pass.

6.2.27 FTA_SSL.3 Test #1

Item	Data
Test Assurance Activity	The evaluator follows the guidance documentation to configure several different values for the inactivity time period referenced in the component. For each period configured, the evaluator establishes a remote interactive session with the TOE. The evaluator then observes that the session is terminated after the configured time period.
Test Steps	<ul style="list-style-type: none"> • Log into the TOE via SSH. • Configure a new idle time for one minute (60 seconds). • Log out of the TOE. • Log into the TOE via SSH. • Session will be closed in 60 seconds if there is no activity. • Verify that a log was created for the configured timeout period. • Configure a new idle timeout for two minutes (120 seconds). • Log out of the TOE. • Log into the TOE and verify session will be closed in 120 seconds if there is no activity • Verify that a log was created for the configured timeout period.
Expected Test Results	<ul style="list-style-type: none"> • TOE terminates session with user when no activity is observed for configured inactivity time period. • TOE logs verify user session is terminated.

Pass/Fail Explanation	Both the remote administrative time out periods can be set by the administrative user. The TOE enforces the configured inactivity period in each instance. This meets the testing requirements.
Result	Pass.

6.2.28 FTA_SSL.4 Test #1

Item	Data
Test Assurance Activity	The evaluator initiates an interactive local session with the TOE. The evaluator then follows the guidance documentation to exit or log off the session and observes that the session has been terminated.
Test Steps	<ul style="list-style-type: none"> • Log onto the TOE through a local administrative interface. • Log out of the TOE. • Verify the logs reflect that a session has been created and terminated.
Expected Test Results	<ul style="list-style-type: none"> • TOE can be exited from a interactive local session following the guidance documentation. • TOE logs verify that a interactive local session can be exited by following the guidance documentation.
Pass/Fail Explanation	The TOE allows user to terminate the directly connected administrative sessions. This meets the testing requirements.
Result	Pass.

6.2.29 FTA_SSL.4 Test #2

Item	Data
Test Assurance Activity	The evaluator initiates an interactive remote session with the TOE. The evaluator then follows the guidance documentation to exit or log off the session and observes that the session has been terminated.
Test Steps	<ul style="list-style-type: none"> • Log onto the TOE remotely via SSH. • Log out the TOE. • Verify the logs reflect that a session has been created and terminated.
Expected Test Results	<ul style="list-style-type: none"> • TOE can be exited from a interactive remote session following the guidance documentation. • TOE logs verify that a interactive remote session can be exited by following the guidance documentation.
Pass/Fail Explanation	TOE allows user to terminate the remote administrative sessions. This meets the testing requirements.

Result	Pass.
---------------	-------

6.2.30 FTA_SSL_EXT.1.1 Test #1

Item	Data
Test Assurance Activity	The evaluator follows the guidance documentation to configure several different values for the inactivity time period referenced in the component. For each period configured, the evaluator establishes a local interactive session with the TOE. The evaluator then observes that the session is either locked or terminated after the configured time period. If locking was selected from the component, the evaluator then ensures that reauthentication is needed when trying to unlock the session.
Test Steps	<ul style="list-style-type: none"> • Configure a time-out period for 60 seconds. • Log out of TOE. • After logging into the TOE, wait 58 seconds and perform a command. • Wait 62 seconds and attempt a command. • Verify that a log was created for the configured timeout. • Configure a new idle time (120 seconds). • Log out of TOE. • After logging into the TOE, wait 118 seconds and perform a command. • Wait 122 seconds and attempt a command. • Verify that a log was created for the configured timeout period.
Expected Test Results	<ul style="list-style-type: none"> • TOE allows configuration of inactivity period. • TOE terminates session with user when no activity is observed for configured inactivity time period. • TOE logs verify user session is terminated.
Pass/Fail Explanation	The local administrative inactivity was able to be set to multiple values. In each instance, the TOE logged the user out after the configured time. This meets the testing requirements.
Result	Pass.

6.2.31 FTA_TAB.1 Test #1

Item	Data
Test Assurance Activity	The evaluator follows the guidance documentation to configure a notice and consent warning message. The evaluator shall then, for each method of access specified in the TSS, establish a session with the TOE. The evaluator shall verify that the notice and consent warning message is displayed in each instance.
Test Steps	<ul style="list-style-type: none"> • Configure access banners on TOE. • Verify that the audit records reflected the configuration steps. • Log into the TOE via SSH. • Log into the TOE via console.

Expected Test Results	<ul style="list-style-type: none"> • TOE allows configuration of notice and consent warning message. • TOE displays the configured notice and consent warning message on access through remote SSH session. • TOE displays the configured notice and consent warning message on access local console session.
Pass/Fail Explanation	An access banner can be set for all the methods that can be used to access the device. This meets the testing requirements.
Result	Pass.

6.2.32 FTP_TRP.1/Admin Test #1

Item	Data
Test Assurance Activity	The evaluators shall ensure that communications using each specified (in the guidance documentation) remote administration method is tested during the course of the evaluation, setting up the connections as described in the guidance documentation and ensuring that communication is successful.
Test Steps	<ul style="list-style-type: none"> • Attempt to connect to the TOE via SSH. • Verify that Wireshark shows a successful connection • Verify that the TOE shows a successful connection.
Expected Test Results	<ul style="list-style-type: none"> • TOE allows remote administration using SSH
Pass/Fail Explanation	Remote administrative access to the TOE is over secure protected channels. This meets the testing requirements.
Result	Pass.

6.2.33 FTP_TRP.1/Admin Test #2

Item	Data
Test Assurance Activity	The evaluator shall ensure, for each communication channel, the channel data is not sent in plaintext.
Pass/Fail Explanation	The communication channel data is not sent in plaintext. This is covered by FTP_TRP.1/Admin_Test#1, FCS_SSH_EXT.1 and FCS_IPSEC_EXT.1 wherein the data was not sent in plaintext.
Result	Pass.

6.3 Firewall

6.3.1 FFW_RUL_EXT.1 Test #1

Item	Data
------	------

Test Assurance Activity	The evaluator shall attempt to get network traffic to flow through the TOE while the TOE is being initialized. A steady flow of network packets that would otherwise be denied by the ruleset should be sourced and be directed at a host. The evaluator shall verify using a packet sniffer that none of the generated network traffic is permitted through the firewall during initialization.
Test Steps	<p>IPv4:</p> <ul style="list-style-type: none"> • Configure a filter to drop traffic from a specific source address. • Apply the filter to the TOE's Interface. • Send continual traffic from the chosen source address and verify that it is denied. • Reboot the TOE when ping is in progress. • Verify with logs that traffic from chosen source address was denied. • Verify with Packet Capture that all traffic from chosen source address was denied during reboot. <p>IPv6:</p> <ul style="list-style-type: none"> • Configure a filter to drop traffic from a specific source address. • Apply the filter to the TOE's Interface. • Send continual traffic from the chosen source address and verify that it is denied. • Reboot the TOE when ping is in progress. • Verify with logs that traffic from chosen source address was denied. • Verify with Packet Capture that all traffic from chosen source address was denied during reboot.
Expected Test Results	<ul style="list-style-type: none"> • Packet Capture shows that denied traffic is not permitted through the TOE even during TOE initialization.
Pass/Fail with Explanation	Pass. Packets that would otherwise be denied by the ruleset are not permitted through the TOE during initialization. This meets the testing requirements.

6.3.2 FFW_RUL_EXT.1 Test #2

Item	Data
Test Assurance Activity	The evaluator shall attempt to get network traffic to flow through the TOE while the TOE is being initialized. A steady flow of network packets that would be permitted by the ruleset should be sourced and be directed at a host. The evaluator shall verify using a packet sniffer that none of the generated network traffic is permitted through the firewall during initialization and is only permitted once initialization is complete.
Test Steps	<p>IPv4:</p> <ul style="list-style-type: none"> • Configure a filter to accept traffic with a specific source address. • Apply the filter to the TOE's Interface.

	<ul style="list-style-type: none"> • Send continual traffic from the specific source address and verify it is accepted. • Reboot the TOE when ping is in progress. • Verify through the firewall log that traffic from specific source address is allowed after the reboot. • Verify through a packet capture that all traffic is denied when the TOE is performing a reboot but once the TOE is operational all traffic from the specific source address is allowed. <p>IPv6:</p> <ul style="list-style-type: none"> • Configure a filter to accept traffic with a specific source address. • Apply the filter to the TOE's Interface. • Send continual traffic from the specific source address and verify it is accepted. • Reboot the TOE when ping is in progress. • Verify through the firewall log that traffic from specific source address is allowed after the reboot • Verify through a packet capture that all traffic is denied when the TOE is performing a reboot but once the TOE is operational all traffic from the specific source address is allowed.
Expected Test Results	<ul style="list-style-type: none"> • Packet capture confirms no traffic is permitted through TOE during initialization. • Packet capture confirms packets permitted by ruleset passing through TOE after initialization
Pass/Fail with Explanation	Pass. Packets that would otherwise be allowed by the ruleset are not permitted through the firewall during initialization. This meets the testing requirements.

6.3.3 FFW_RUL_EXT.1.2/FFW_RUL_EXT.1.3/FFW_RUL_EXT.1.4 Test #1

Item	Data
Test Assurance Activity	<p>Test 1: The evaluator shall use the instructions in the guidance documentation to test that state full packet filter firewall rules can be created that permit, drop, and log packets for each of the following attributes:</p> <ul style="list-style-type: none"> • ICMPv4 <ul style="list-style-type: none"> ○ Type ○ Code • ICMPv6 <ul style="list-style-type: none"> ○ Type ○ Code • IPv4 <ul style="list-style-type: none"> ○ Source address

	<ul style="list-style-type: none"> ○ Destination Address ○ Transport Layer Protocol • IPv6 <ul style="list-style-type: none"> ○ Source address ○ Destination Address ○ Transport Layer Protocol and where defined by the ST author, ○ Extension Header Type, Extension Header Fields • TCP <ul style="list-style-type: none"> ○ Source Port ○ Destination Port • UDP <ul style="list-style-type: none"> ○ Source Port ○ Destination Port
Test Steps	<p>IPv4</p> <ul style="list-style-type: none"> ○ Source address <ul style="list-style-type: none"> • Configure a filter to drop and accept traffic with specified IPv4 source addresses. • Apply the IPv4 source address filter. • Generate and send traffic that matches the applied filter. • Verify the IPV4 packets are dropped or accepted according to the filter applied using logs. • Verify the IPV4 packets are dropped or accepted according to the filter applied using Packet Capture. ○ Destination Address <ul style="list-style-type: none"> • Configure a filter to drop and accept traffic with specified IPv4 destination addresses. • Apply the IPv4 destination address filter. • Generate and send traffic that matches the applied filter. • Verify the IPV4 packets are dropped or accepted according to the filter applied using logs. • Verify the IPV4 packets are dropped or accepted according to the filter applied using Packet Capture. ○ Transport Layer Protocol <ul style="list-style-type: none"> • Configure a filter to drop and accept traffic with a specified IPv4 transport layer protocol.

- Apply the IPv4 protocol filter.
- Generate and send traffic that matches the applied filter.
- Verify the IPV4 protocol packets are dropped or accepted according to the filter applied using logs.
- Verify the IPV4 protocol packets are dropped or accepted according to the filter applied using Packet Capture.

IPv6

○ Source address

- Configure a filter to drop and accept traffic with specified IPv6 source addresses.
- Apply the IPv6 source address filter.
- Generate and send traffic that matches the applied filter.
- Verify the IPV6 packets are dropped or accepted according to the filter applied using logs.
- Verify the IPV6 packets are dropped or accepted according to the filter applied using Packet Capture.

○ Destination Address

- Configure a filter to drop and accept traffic with specified IPv6 destination addresses.
- Apply the IPv6 destination address filter.
- Generate and send traffic that matches the applied filter.
- Verify the IPV6 packets are dropped or accepted according to the filter applied using logs.
- Verify the IPV6 packets are dropped or accepted according to the filter applied using Packet Capture.

○ Transport Layer Protocol

- Configure a filter to drop and accept traffic with a specified IPv6 transport layer protocol.
- Apply the IPv6 protocol filter.
- Generate and send traffic that matches the applied filter.
- Verify the IPV6 protocol packets are dropped or accepted according to the filter applied using logs.
- Verify the IPV6 protocol packets are dropped or accepted according to the filter applied using Packet Capture.

TCP

○ Source Port

- Configure a filter to drop and accept traffic according to specified source ports.
- Apply the source port filter.
- Generate and send traffic that matches the applied filter.
- Verify the TCP packets are dropped or accepted according to the filter applied using logs.
- Verify the traffic was sent via Wireshark packet capture.

○ Destination Port

- Configure a filter to drop and accept traffic according to specified destination ports.
- Apply the destination port filter.
- Generate and send traffic that matches the applied filter.
- Verify the TCP packets are dropped or accepted according to the filter applied using logs.
- Verify the traffic was sent via Wireshark packet capture.

UDP

○ Source Port

- Configure a filter to drop and accept traffic according to specified source ports.
- Apply the source port filter,
- Generate and send traffic that matches the applied filter.
- Verify the UDP packets are dropped or accepted according to the filter applied using logs.
- Verify the traffic was sent via Wireshark packet capture.

○ Destination Port

- Configure a filter to drop and accept traffic according to specified destination ports.
- Apply the destination port filter.
- Generate and send traffic that matches the applied filter.
- Verify the UDP packets are dropped or accepted according to the filter applied using logs.
- Verify the traffic was sent via Wireshark packet capture.

ICMPv4

• Type

- Configure a filter to accept and drop ICMPV4 packets according to its type.

	<ul style="list-style-type: none"> ○ Apply the ICMPv4 type filter ○ Generate and send traffic that matches the created filter ○ Verify through logs that the ICMPV4 packets are dropped or accepted according to the rules applied based on type. ○ Verify the traffic was sent via Wireshark packet capture ● Code <ul style="list-style-type: none"> ○ Configure a filter to accept and drop ICMPV4 packets according to its code. ○ Apply the ICMPv4 type filter ○ Generate and send traffic that matches the created filter ○ Verify through logs that the ICMPV4 packets are dropped or accepted according to the rules applied based on code. ○ Verify the traffic was sent via Wireshark packet capture <p>ICMPv6</p> <ul style="list-style-type: none"> ● Type <ul style="list-style-type: none"> ○ Configure a filter to accept and drop ICMPV4 packets according to its type. ○ Apply the ICMPv6 type filter ○ Generate and send traffic that matches the created filter ○ Verify through logs that the ICMPV6 packets are dropped or accepted according to the rules applied based on type. ○ Verify the traffic was sent via Wireshark packet capture ● Code <ul style="list-style-type: none"> ○ Configure a filter to accept and drop ICMPV4 packets according to its code. ○ Apply the ICMPv6 type filter ○ Generate and send traffic that matches the created filter ○ Verify through logs that the ICMPV6 packets are dropped or accepted according to the rules applied based on code. ○ Verify the traffic was sent via Wireshark packet capture
Expected Test Results	<ul style="list-style-type: none"> ● TOE firewall logs show traffic getting accepted or dropped according to configured filter attributes. ● Packet Capture shows traffic getting accepted or dropped according to configured filter attributes.
Pass/Fail with Explanation	Pass. This requirement pass as the TOE can implement full packet filter firewall rules that permit, drop, and log packets for each of the specified attributes.

6.3.4 FFW_RUL_EXT.1.2/FFW_RUL_EXT.1.3/FFW_RUL_EXT.1.4 Test #2

Item	Data
------	------

Test Assurance Activity	Test 2: Repeat the test assurance activity above to ensure that state full traffic filtering rules can be defined for each distinct network interface type supported by the TOE
Test Steps	<p>IPv4</p> <ul style="list-style-type: none"> ○ Source address <ul style="list-style-type: none"> • Configure a filter to drop and accept traffic with specified IPv4 source addresses. • Apply the IPv4 source address filter to VPN Interface. • Generate and send traffic that matches the applied filter. • Verify the IPV4 packets are dropped or accepted according to the filter applied using logs. • Verify the IPV4 packets are dropped or accepted according to the filter applied using Packet Capture. ○ Destination Address <ul style="list-style-type: none"> • Configure a filter to drop and accept traffic with specified IPv4 destination addresses. • Apply the IPv4 destination address filter to VPN Interface. • Generate and send traffic that matches the applied filter. • Verify the IPV4 packets are dropped or accepted according to the filter applied using logs. • Verify the IPV4 packets are dropped or accepted according to the filter applied using Packet Capture. ○ Transport Layer Protocol <ul style="list-style-type: none"> • Configure a filter to drop and accept traffic with a specified IPv4 transport layer protocol. • Apply the IPv4 protocol filter to VPN Interface. • Generate and send traffic that matches the applied filter. • Verify the IPV4 protocol packets are dropped or accepted according to the filter applied using logs. • Verify the IPV4 protocol packets are dropped or accepted according to the filter applied using Packet Capture. <p>IPv6</p> <ul style="list-style-type: none"> ○ Source address <ul style="list-style-type: none"> • Configure a filter to drop and accept traffic with specified IPv6 source addresses.

- Apply the IPv6 source address filter to VPN Interface to VPN Interface.
- Generate and send traffic that matches the applied filter.
- Verify the IPV6 packets are dropped or accepted according to the filter applied using logs.
- Verify the IPV6 packets are dropped or accepted according to the filter applied using Packet Capture.

○ **Destination Address**

- Configure a filter to drop and accept traffic with specified IPv6 destination addresses.
- Apply the IPv6 destination address filter to VPN Interface.
- Generate and send traffic that matches the applied filter.
- Verify the IPV6 packets are dropped or accepted according to the filter applied using logs.
- Verify the IPV6 packets are dropped or accepted according to the filter applied using Packet Capture.

○ **Transport Layer Protocol**

- Configure a filter to drop and accept traffic with a specified IPv6 transport layer protocol.
- Apply the IPv6 protocol filter.
- Generate and send traffic that matches the applied filter to VPN Interface.
- Verify the IPV6 protocol packets are dropped or accepted according to the filter applied using logs.
- Verify the IPV6 protocol packets are dropped or accepted according to the filter applied using Packet Capture.

TCP

○ **Source Port**

- Configure a filter to drop and accept traffic according to specified source ports.
- Apply the source port filter to VPN Interface.
- Generate and send traffic that matches the applied filter.
- Verify the TCP packets are dropped or accepted according to the filter applied using logs.
- Verify the traffic was sent via Wireshark packet capture.

○ **Destination Port**

- Configure a filter to drop and accept traffic according to specified destination ports.
- Apply the destination port filter to VPN Interface.
- Generate and send traffic that matches the applied filter.
- Verify the TCP packets are dropped or accepted according to the filter applied using logs.
- Verify the traffic was sent via Wireshark packet capture.

UDP

○ Source Port

- Configure a filter to drop and accept traffic according to specified source ports.
- Apply the source port filter to VPN Interface.
- Generate and send traffic that matches the applied filter.
- Verify the UDP packets are dropped or accepted according to the filter applied using logs.
- Verify the traffic was sent via Wireshark packet capture.

○ Destination Port

- Configure a filter to drop and accept traffic according to specified destination ports
- Apply the destination port filter to VPN Interface.
- Generate and send traffic that matches the applied filter.
- Verify the UDP packets are dropped or accepted according to the filter applied using logs
- Verify the traffic was sent via Wireshark packet capture.

ICMPv4

• Type

- Configure a filter to accept and drop ICMPV4 packets according to its type.
- Apply the ICMPv4 type filter to VPN Interface
- Generate and send traffic that matches the created filter
- Verify through logs that the ICMPV4 packets are dropped or accepted according to the rules applied based on type.
- Verify the traffic was sent via Wireshark packet capture

• Code

- Configure a filter to accept and drop ICMPV4 packets according to its code.
- Apply the ICMPv4 type filter to VPN Interface
- Generate and send traffic that matches the created filter

	<ul style="list-style-type: none"> ○ Verify through logs that the ICMPV4 packets are dropped or accepted according to the rules applied based on code. ○ Verify the traffic was sent via Wireshark packet capture <p>ICMPv6</p> <ul style="list-style-type: none"> • Type <ul style="list-style-type: none"> ○ Configure a filter to accept and drop ICMPv6 packets according to its type. ○ Apply the ICMPv6 type filter to VPN Interface ○ Generate and send traffic that matches the created filter ○ Verify through logs that the ICMPV6 packets are dropped or accepted according to the rules applied based on type. ○ Verify the traffic was sent via Wireshark packet capture • Code <ul style="list-style-type: none"> ○ Configure a filter to accept and drop ICMPv6 packets according to its code. ○ Apply the ICMPv6 type filter to VPN Interface. ○ Generate and send traffic that matches the created filter ○ Verify through logs that the ICMPV6 packets are dropped or accepted according to the rules applied based on code. ○ Verify the traffic was sent via Wireshark packet capture.
Expected Test Results	<ul style="list-style-type: none"> • TOE firewall logs show traffic getting accepted or dropped according to configured filter attributes. • Packet Capture shows traffic getting accepted or dropped according to configured filter attributes.
Pass/Fail with Explanation	Pass. TOE can implement full packet filter firewall rules that permit, drop, and log packets for each of the specified attributes on the VPN interface. This meets the testing requirements.

6.3.5 FFW_RUL_EXT.1.5 Test #1

Item	Data
Test Assurance Activity	Test 1: The evaluator shall configure the TOE to permit and log TCP traffic. The evaluator shall initiate a TCP session. While the TCP session is being established, the evaluator shall introduce session establishment packets with incorrect flags to determine that the altered traffic is not accepted as part of the session (i.e., a log event is generated to show the ruleset was applied). After a TCP session is successfully established, the evaluator shall alter each of the session determining attributes (source and destination addresses, source and destination ports, sequence number, flags) one at a time in order to verify that the altered packets are not accepted as part of the established session.
Test Steps	IPv4 <ul style="list-style-type: none"> • Configure the TOE to permit and log TCP traffic

	<ul style="list-style-type: none"> • Apply the filter to the TOE’s interface • Establish a TCP session with incorrect flag while establishment of TCP session. • Verify the session and altered packets are logged by the firewall filter • Verify through the packet capture that incorrect flag is sent while establishment of TCP session and session is not established. • Establish a TCP session and send data • Modify each of the session attributes one at a time: <ul style="list-style-type: none"> ○ Source address ○ Destination address ○ Source port ○ Destination port ○ Sequence number ○ Flags • Verify the session and altered packets are logged by the firewall filter • Verify through the packet capture that the altered packets are not accepted as part of the established session <p>IPv6</p> <ul style="list-style-type: none"> • Configure the TOE to permit and log TCP traffic with specific source and destination addresses. • Apply the filter to the TOE’s interface. • Establish a TCP session with incorrect flag while establishment of TCP session. • Verify the session and altered packets are logged by the firewall filter • Verify through the packet capture that incorrect flag is sent while establishment of TCP session and session is not established. • Establish a TCP session and send data. • Modify each of the session attributes one at a time: <ul style="list-style-type: none"> ○ Source address ○ Destination address ○ Source port ○ Destination port ○ Sequence number ○ Flags • Verify the session and altered packets are logged by the firewall filter. • Verify through the packet capture that the altered packets are not accepted as part of the established session.
Expected Test Results	<ul style="list-style-type: none"> • TOE firewall logs show traffic getting permitted according to configured filter attributes. • Packet Capture shows traffic with incorrect flag “PSH” while establishment of TCP session and TCP session is not established.

	<ul style="list-style-type: none"> • TOE firewall logs show traffic getting permitted according to configured filter attributes. • Packet Capture shows traffic getting permitted according to configured filter attributes.
Pass/Fail with Explanation	Pass. TOE does not accept altered packets (source and destination addresses, source and destination ports, sequence number, flags) after a TCP session is successfully established. This meets testing requirements.

6.3.6 FFW_RUL_EXT.1.5 Test #2

Item	Data
Test Assurance Activity	Test 2: The evaluator shall terminate the TCP session established per Test 1 as described in the TSS. The evaluator shall then immediately send a packet matching the former session definition in order to ensure it is not forwarded through the TOE without being subject to the ruleset.
Test Steps	<p>IPv4</p> <ul style="list-style-type: none"> • Configure the TOE to permit and log TCP traffic. • Apply the filter to the TOE's interface. • Establish a TCP session then terminate the session. • Send a packet that matches the former TCP session. • Verify that the Firewall logs the TCP packet similar to former session. <p>IPv6</p> <ul style="list-style-type: none"> • Configure the TOE to permit and log TCP traffic with specific source and destination addresses. • Apply the filter to the TOE's interface. • Establish a TCP session then terminate the session. • Send a packet that matches the former TCP session. • Verify that the Firewall logs the TCP packet similar to former session.
Expected Test Results	<ul style="list-style-type: none"> • TOE firewall logs show TCP traffic sent matching former TCP session getting logged. • Packet Capture verifies TCP traffic sent matches former TCP session.
Pass/Fail with Explanation	Pass. Any packet matching the TCP former session is not forwarded through the TOE without being subject to the ruleset. This meets the testing requirements.

6.3.7 FFW_RUL_EXT.1.5 Test #3

Item	Data
Test Assurance Activity	Test 3: The evaluator shall expire (i.e., reach timeout) the TCP session established per Test 1 as described in the TSS. The evaluator shall then send a packet matching the former session in order to ensure it is not forwarded through the TOE without being subject to the ruleset.

Test Steps	<p>IPv4</p> <ul style="list-style-type: none"> • Configure the TOE to permit and log TCP traffic. • Apply the filter to the TOE's interface. • Establish a TCP session and wait for the session to expire in 60 secs. • Send a packet that matches the former TCP session. • Verify that the Firewall logs the TCP packet similar to former session. <p>IPv6</p> <ul style="list-style-type: none"> • Configure the TOE to permit and log TCP traffic with specific source and destination addresses. • Apply the filter to the TOE's interface. • Establish a TCP session and wait for the session to expire in 60 secs. • Send a packet that matches the former TCP session. • Verify that the Firewall logs the TCP packet similar to former session.
Expected Test Results	<ul style="list-style-type: none"> • TOE firewall logs show TCP traffic sent matching expired TCP session getting logged and subjected to configured ruleset. • Packet Capture verifies TCP traffic sent matches expired TCP session.
Pass/Fail with Explanation	Pass. Any TCP packet matching the former expired session is not forwarded through the TOE without being subject to the ruleset. This meets the testing requirements.

6.3.8 FFW_RUL_EXT.1.5 Test #4

Item	Data
Test Assurance Activity	Test 4: The evaluator shall configure the TOE to permit and log UDP traffic. The evaluator shall establish a UDP session. Once a UDP session is established, the evaluator shall alter each of the session determining attributes (source and destination addresses, source and destination ports) one at a time in order to verify that the altered packets are not accepted as part of the established session.
Test Steps	<p>IPv4</p> <ul style="list-style-type: none"> • Configure the TOE to permit and log UDP traffic. • Apply the filter to the TOE's interface. • Establish a UDP session and send data. • Modify each of the session attributes one at a time: <ul style="list-style-type: none"> ○ Source address ○ Destination address ○ Source port ○ Destination port • Verify the session and altered packets are logged by the firewall filter.

	<ul style="list-style-type: none"> Verify through the packet capture that the altered packets are not accepted as part of the established session. <p>IPv6</p> <ul style="list-style-type: none"> Configure the TOE to permit and log UDP traffic with specific source and destination addresses. Apply the filter to the TOE's interface. Establish a UDP session and send data. Modify each of the session attributes one at a time: <ul style="list-style-type: none"> Source address Destination address Source port Destination port Verify the session and altered packets are logged by the firewall filter. Verify through the packet capture that the altered packets are not accepted as part of the established session.
Expected Test Results	<ul style="list-style-type: none"> TOE firewall logs show UDP traffic getting permitted according to configured filter attributes. Packet Capture shows UDP traffic getting permitted according to configured filter attributes.
Pass/Fail with Explanation	Pass. TOE does not accept altered packets (source and destination addresses, source and destination ports) after a UDP session is successfully established. This meets testing requirements.

6.3.9 FFW_RUL_EXT.1.5 Test #5

Item	Data
Test Assurance Activity	Test 5: The evaluator shall expire (i.e., reach timeout) the UDP session established per Test 4 as described in the TSS. The evaluator shall then send a packet matching the former session in order to ensure it is not forwarded through the TOE without being subject to the ruleset.
Test Steps	<p>IPv4</p> <ul style="list-style-type: none"> Configure the TOE to permit and log UDP traffic. Apply the filter to the TOE's interface. Establish a UDP session and wait for the session to expire in 60 secs. Send a packet that matches the former UDP session. Verify that the Firewall logs the UDP packet similar to former session. <p>IPv6</p> <ul style="list-style-type: none"> Configure the TOE to permit and log UDP traffic with specific source and destination addresses.

	<ul style="list-style-type: none"> • Apply the filter to the TOE’s interface. • Establish a UDP session and wait for the session to expire in 60 secs. • Send a packet that matches the former UDP session. • Verify that the Firewall logs the UDP packet similar to former session.
Expected Test Results	<ul style="list-style-type: none"> • TOE firewall logs show UDP traffic sent matching expired UDP session getting logged and subjected to configured ruleset. • Packet Capture verifies UDP traffic sent matches expired UDP session
Pass/Fail with Explanation	Pass. Any UDP packet matching the former expired session is not forwarded through the TOE without being subject to the ruleset. This meets the testing requirements.

6.3.10 FFW_RUL_EXT.1.5 Test #6

Item	Data
Test Assurance Activity	Test 6: If ICMP is selected , the evaluator shall configure the TOE to permit and log ICMP traffic. The evaluator shall establish a session for ICMP as defined in the TSS. Once an ICMP session is established, the evaluator shall alter each of the session determining attributes (source and destination addresses, other attributes chosen in FFW_RUL_EXT.1.5) one at a time in order to verify that the altered packets are not accepted as part of the established session.
Test Steps	<p>IPv4</p> <ul style="list-style-type: none"> • Configure the TOE to permit and log ICMP traffic. • Apply the filter to the TOE’s interface. • For each of the session attributes, verify the altered packets are not accepted as part of the session. <ul style="list-style-type: none"> ○ Source address <ul style="list-style-type: none"> ▪ Establish ICMP connection. ▪ Modify session attribute. ▪ Verify the altered packets are logged by the firewall filter. ▪ Verify the altered packets are not accepted as part of the established session. ○ Destination address <ul style="list-style-type: none"> ▪ Establish ICMP connection. ▪ Modify session attribute. ▪ Verify the altered packets are logged by the firewall filter. ▪ Verify the altered packets are not accepted as part of the established session. ○ Type <ul style="list-style-type: none"> ▪ Establish ICMP connection.

- Modify session attribute.
- Verify the altered packets are logged by the firewall filter.
- Verify the altered packets are not accepted as part of the established session.

- Code

- Establish ICMP connection.
- Modify session attribute.
- Verify the altered packets are logged by the firewall filter.
- Verify the altered packets are not accepted as part of the established session.

IPv6

- Configure the TOE to permit and log ICMP traffic with specific source and destination addresses.
- Apply the filter to the TOE's interface.
- For each of the session attributes, verify the altered packets are not accepted as part of the session.
 - Source address
 - Establish ICMP connection.
 - Modify session attribute.
 - Verify the altered packets are logged by the firewall filter.
 - Verify the altered packets are not accepted as part of the established session.
 - Destination address
 - Establish ICMP connection.
 - Modify session attribute.
 - Verify the altered packets are logged by the firewall filter.
 - Verify the altered packets are not accepted as part of the established session.
 - Type
 - Establish ICMP connection.
 - Modify session attribute.
 - Verify the altered packets are logged by the firewall filter.
 - Verify the altered packets are not accepted as part of the established session.
 - Code
 - Establish ICMP connection.
 - Modify session attribute.

	<ul style="list-style-type: none"> ▪ Verify the altered packets are logged by the firewall filter. ▪ Verify the altered packets are not accepted as part of the established session.
Expected Test Results	<ul style="list-style-type: none"> • TOE firewall logs show ICMP with modified attributes being logged. • Packet Capture shows ICMP traffic with modified attributes not accepted as part of current established session.
Pass/Fail with Explanation	Pass. TOE does not accept altered packets (source and destination addresses, type and code) after a ICMP session is successfully established. This meets testing requirements.

6.3.11 FFW_RUL_EXT.1.5 Test #7

Item	Data
Test Assurance Activity	Test 7: If applicable, the evaluator shall terminate the ICMP session established per Test 6 as described in the TSS. The evaluator shall then immediately send a packet matching the former session definition in order to ensure it is not forwarded through the TOE without being subject to the ruleset.
Test Steps	<p>IPv4</p> <ul style="list-style-type: none"> • Configure the TOE to permit and log ICMP traffic • Apply the filter to the TOE's interface • Establish a ICMP session and terminate it • Send a packet that matches the former ICMP session • Verify that the Firewall logs the ICMP packet similar to former session. <p>IPv6</p> <ul style="list-style-type: none"> • Configure the TOE to permit and log ICMP traffic with specific source and destination addresses. • Apply the filter to the TOE's interface • Establish a ICMP session and terminate it • Send a packet that matches the former ICMP session • Verify that the Firewall logs the ICMP packet similar to former session.
Expected Test Results	<ul style="list-style-type: none"> • TOE firewall logs show ICMP traffic sent matching former ICMP session getting logged and subjected to configured ruleset. • Packet Capture verifies ICMP traffic sent matches former ICMP session.
Pass/Fail with Explanation	Pass. Any packet matching the ICMP former session is not forwarded through the TOE without being subject to the ruleset. This meets the testing requirements.

6.3.12 FFW_RUL_EXT.1.5 Test #8

Item	Data
Test Assurance Activity	Test 8: The evaluator shall expire (i.e., reach timeout) the ICMP session established per Test 6 as described in the TSS. The evaluator shall then send a packet matching the former session in order to ensure it is not forwarded through the TOE without being subject to the ruleset.
Test Steps	<p>IPv4</p> <ul style="list-style-type: none"> • Configure the TOE to permit and log ICMP traffic. • Apply the filter to the TOE’s interface. • Establish a ICMP session and wait for the session to expire in 5secs. • Send a packet that matches the former ICMP session. • Verify that the Firewall logs the ICMP packet similar to former session. <p>IPv6</p> <ul style="list-style-type: none"> • Configure the TOE to permit and log ICMP traffic with specific source and destination addresses. • Apply the filter to the TOE’s interface. • Establish a ICMP session and wait for the session to expire in 5secs. • Send a packet that matches the former ICMP session. • Verify that the Firewall logs the ICMP packet similar to former session.
Expected Test Results	<ul style="list-style-type: none"> • TOE firewall logs show ICMP traffic sent matching expired ICMP session getting logged and subjected to configured ruleset. • Packet Capture verifies ICMP traffic sent matches expired ICMP session.
Pass/Fail with Explanation	Pass. Any ICMP packet matching the former expired session is not forwarded through the TOE without being subject to the ruleset. This meets the testing requirements.

6.3.13 FFW_RUL_EXT.1.6 Test #1

Item	Data
Test Assurance Activity	<p>Both IPv4 and IPv6 shall be tested for items a), b), c), d), and e) of the SFR element. Both IPv4 and IPv6 shall be tested for item i) unless the rule definition is specific to IPv4 or IPv6. Note: f), g), and h) are specific to IPv4 or IPv6 and shall be tested accordingly</p> <p>Test 1: The evaluator shall test each of the conditions for automatic packet rejection in turn. In each case, the TOE should be configured to allow all network traffic and the evaluator shall generate a packet or packet fragment that is to be rejected. The evaluator shall use packet captures to ensure that the unallowable packet or packet fragment is not passed through the TOE.</p>
Test Steps	<p>IPv4</p> <ul style="list-style-type: none"> • Packets which are invalid fragments <ul style="list-style-type: none"> ○ Create a filter to reject and log invalid fragments. ○ Send packets which are invalid fragments.

- Verify through logs that the traffic is rejected.
- Verify through Packet Capture that the traffic is rejected.
- Fragments that cannot be completely re-assembled
 - Create a filter to log fragments that cannot be re-assembled.
 - Send fragments that cannot be re-assembled.
 - Verify through logs that the traffic is rejected.
 - Verify through Packet Capture that the traffic is rejected.
- Packets where the source address is defined as being on a broadcast network.
 - Create a filter to log traffic where the source address is defined as being on a broadcast network.
 - Apply filter to the security zone associated to TOE'S interface.
 - Send traffic where the source address is defined as being on a broadcast network.
 - Verify through logs that the traffic is rejected.
 - Verify through Packet Capture that the traffic is rejected.
- Packets where the source address is defined as being on a multicast network
 - Create a filter to log traffic where the source address is defined as being on a multicast network.
 - Send traffic where the source address is defined as being on a multicast network.
 - Verify through logs that the traffic is rejected.
 - Verify through Packet Capture that the traffic is rejected.
- Packets where the source address is defined as being a loopback address
 - Create a filter to log traffic where the source address is defined as being on a loopback address.
 - Send traffic where the source address is defined as being on a loopback address.
 - Verify through logs that the traffic is rejected.
 - Verify through Packet Capture that the traffic is rejected.
- Packets where the source or destination address of the network packet is defined as being unspecified (i.e. 0.0.0.0) or an address "reserved for future use" (i.e. 240.0.0.0/4) as specified in RFC 5735 for IPv4.
 - Create a filter to log traffic where packets where the source or destination address of the network packet is defined as an "unspecified address" or an address "reserved for future definition and use"
 - Apply filter to the security zone associated to TOE'S interface.
 - Send traffic with source address matching unspecified address and reserved for further use

- Verify through logs that the traffic is rejected.
- Verify through Packet Capture that the traffic is rejected.

- Packets with the IP options: Loose Source Routing, Strict Source Routing, or Record Route specified
 - Create a filter to log traffic with packets with the IP options: Loose Source Routing, Strict Source Routing, or Record Route specified.
 - Apply filter to TOE'S interface.
 - Send traffic with IP options: Loose Source Routing, Strict Source Routing, or Record Route.
 - Verify through logs that the traffic is rejected.
 - Verify through Packet Capture that the traffic is rejected.

IPv6:

- Packets which are invalid fragments.
 - Create a filter to reject and log invalid fragments.
 - Send packets which are invalid fragments.
 - Verify through logs that the traffic is rejected.
 - Verify through Packet Capture that the traffic is rejected.

- Fragments that cannot be completely re-assembled.
 - Create a filter to log fragments that cannot be re-assembled.
 - Send fragments that cannot be re-assembled.
 - Verify through logs that the traffic is rejected.
 - Verify through Packet Capture that the traffic is rejected.

- Packets where the source address is defined as being on a broadcast network.
 - Create a filter to log traffic where the source address is defined as being on a broadcast network.
 - Send traffic where the source address is defined as being on a broadcast network.
 - Verify through logs that the traffic is rejected.
 - Verify through Packet Capture that the traffic is rejected.

- Packets where the source address is defined as being on a multicast network.
 - Create a filter to log traffic where the source address is defined as being on a multicast network.
 - Send traffic where the source address is defined as being on a multicast network.
 - Verify through logs that the traffic is rejected.
 - Verify through Packet Capture that the traffic is rejected.

	<ul style="list-style-type: none"> • Packets where the source address is defined as being a loopback address. <ul style="list-style-type: none"> ○ Create a filter to log traffic where the source address is defined as being on a loopback address. ○ Send traffic where the source address is defined as being on a loopback address. ○ Verify through logs that the traffic is rejected. ○ Verify through Packet Capture that the traffic is rejected. • Packets where the source or destination address of the network packet is defined as an “unspecified address” or an address “reserved for future definition and use” (i.e. unicast addresses not in this address range: 2000::/3) as specified in RFC 3513 for IPv6. <ul style="list-style-type: none"> ○ Create a filter to log traffic where packets where the source or destination address of the network packet is defined as an “unspecified address” or an address “reserved for future definition and use” ○ Apply filter to the security zone associated to TOE’S interface. ○ Send traffic with source address matching unspecified address and reserved for further use ○ Verify through logs that the traffic is rejected. ○ Verify through Packet Capture that the traffic is rejected.
Expected Test Results	<ul style="list-style-type: none"> • TOE Logs show that unallowed packets or packet fragments are denied by it. • Packet Capture shows unallowed packet and packet fragments not passing through TOE.
Pass/Fail with Explanation	Pass. Unallowable packet or packet fragment is rejected and logged through the TOE automatically. This meets the testing requirements.

6.3.14 FFW_RUL_EXT.1.6 Test #2

Item	Data
Test Assurance Activity	<p>Both IPv4 and IPv6 shall be tested for items a), b), c), d), and e) of the SFR element. Both IPv4 and IPv6 shall be tested for item i) unless the rule definition is specific to IPv4 or IPv6. Note: f), g), and h) are specific to IPv4 or IPv6 and shall be tested accordingly</p> <p>Test 2: For each of the cases above, the evaluator shall use any applicable guidance to enable dropped packet logging or counting. In each case above, the evaluator shall ensure that the rejected packet or packet fragment was recorded (either logged or an appropriate counter incremented).</p>
Pass/Fail with Explanation	Pass. The requirements of this test have been completed as part of testing for FFW_RUL_EXT.1.6 Test #1.

6.3.15 FFW_RUL_EXT.1.7 Test #1

Item	Data
Test Assurance Activity	<p>The following tests shall be run using IPv4 and IPv6.</p> <p>Test 1: The evaluator shall configure the TOE to drop and log network traffic where the source address of the packet matches that of the TOE network interface upon which the traffic was received. The evaluator shall generate suitable network traffic to match the configured rule and verify that the traffic is dropped, and a log message generated.</p>
Test Steps	<p>IPv4</p> <ul style="list-style-type: none"> • Configure a filter to log and drop traffic when the source address of the packet matches the address of the network interface • Apply the filter on TOE interface. • Generate and send traffic that matches the created filter. • Verify through the firewall filter that the traffic was denied. • Verify through a packet capture that the traffic was denied. <p>IPv6</p> <ul style="list-style-type: none"> • Configure a filter to log and drop traffic when the source address of the packet matches the address of the network interface. • Apply the filter on TOE interface. • Generate and send traffic that matches the created filter. • Verify through the firewall filter that the traffic was denied. • Verify through a packet capture that the traffic was denied.
Expected Test Results	<ul style="list-style-type: none"> • TOE firewall logs show traffic with source address matching TOE network interface getting dropped. • Packet Capture shows traffic with source address matching TOE network interface getting dropped.
Pass/Fail with Explanation	<p>Pass. The TOE drops and logs network traffic where the source address of the packet matches that of the TOE network interface upon which the traffic was received. This meets testing requirements</p>

6.3.16 FFW_RUL_EXT.1.7 Test #2

Item	Data
Test Assurance Activity	<p>The following tests shall be run using IPv4 and IPv6.</p> <p>Test 2: The evaluator shall configure the TOE to drop and log network traffic where the source IP address of the packet fails to match the network reachability information of the interface to which it is targeted, e.g. if the TOE believes that network 192.168.1.0/24 is reachable through interface 2, network traffic with a source address from the 192.168.1.0/24 network should be</p>

	generated and sent to an interface other than interface 2. The evaluator shall verify that the network traffic is dropped, and a log message generated.
Test Steps	<p>IPv4</p> <ul style="list-style-type: none"> • Configure a filter to drop and log network traffic when the source IP address of the packet does not match the network reachability information of the TOE interface. • Apply the filter to the TOE’s interface. • Modify traffic to send to the TOE. • Verify through the logs that the traffic is dropped. • Verify the drop of packets via packet capture. <p>IPv6</p> <ul style="list-style-type: none"> • Configure a filter to drop and log network traffic when the source IP address of the packet does not match the network reachability information of the TOE interface. • Apply the filter to the TOE’s interface. • Modify traffic to send to the TOE. • Verify through the logs that the traffic is dropped. • Verify the drop of packets via packet capture.
Expected Test Results	<ul style="list-style-type: none"> • TOE firewall logs show traffic with source address not matching the network reachability information of the interface to which it is targeted getting dropped. • Packet Capture shows traffic with source address not matching the network reachability information of the interface to which it is targeted getting dropped.
Pass/Fail with Explanation	Pass. TOE drops and logs network traffic where the source IP address of the packet fails to match the network reachability information of the interface to which it is targeted. This meets the testing requirements.

6.3.17 FFW_RUL_EXT.1.8 Test #1

Item	Data
Test Assurance Activity	<p>Test 1: If the TOE implements a mechanism that ensures that no conflicting rules can be configured, the evaluator shall try to configure two conflicting rules and verify that the TOE rejects the conflicting rule(s). It is important to verify that the mechanism is implemented in the TOE but not in the non-TOE environment.</p> <p>If the TOE does not implement a mechanism that ensures that no conflicting rules can be configured, the evaluator shall devise two equal stateful traffic filtering rules with alternate operations – permit and drop. The rules should then be deployed in two distinct orders and in each case the evaluator shall ensure that the first rule is enforced in both cases by generating applicable packets and using packet capture and logs for confirmation.</p> <p>TD0545 has been applied.</p>

Test Steps	<p>Note: TOE does not implement a mechanism that ensures that no conflicting rules can be configured.</p> <p>IPv4:</p> <ul style="list-style-type: none"> • Configure a filter to allow and drop packets with the allow rule being first. • Apply the filter to the TOE Interface. • Send traffic to configured destination address in filter. • Verify through the firewall log that traffic is allowed. • Verify allowed traffic via packet capture. <ul style="list-style-type: none"> • Configure a filter to drop and allow packets with the drop rule being first. • Apply the filter to the TOE Interface. • Send traffic to configured destination address in filter. • Verify through the firewall log that traffic is discarded. • Verify via packet capture discarded traffic. <p>IPv6</p> <ul style="list-style-type: none"> • Configure a filter to allow and drop packets with the allow rule being first. • Apply the filter to the TOE Interface. • Send traffic to configured destination address in filter. • Verify through the firewall log that traffic is allowed. • Verify allowed traffic via packet capture. <ul style="list-style-type: none"> • Configure a filter to drop and allow packets with the drop rule being first. • Apply the filter to the TOE Interface. • Send traffic to configured destination address in filter. • Verify through the firewall log that traffic is discarded. • Verify via packet capture discarded traffic.
Expected Test Results	<ul style="list-style-type: none"> • TOE logs show that traffic matching configured destination-address gets permitted when allow rule is first in the conflicting ruleset. • Packet Capture shows that traffic matching configured destination-address gets permitted when allow rule is first in the conflicting ruleset. • TOE logs show that traffic matching configured destination-address gets dropped when drop rule is first in the conflicting ruleset. • Packet Capture shows that traffic matching configured destination-address gets dropped when drop rule is first in the conflicting ruleset.
Pass/Fail with Explanation	<p>Pass. TOE enforces the first rule in the firewall filter. This meets the testing requirement.</p>

6.3.18 FFW_RUL_EXT.1.8 Test #2

Item	Data
------	------

Test Assurance Activity	Test 2: The evaluator shall repeat the procedure above, except that the two rules should be devised where one is a subset of the other (e.g., a specific address vs. a network segment). Again, the evaluator should test both orders to ensure that the first is enforced regardless of the specificity of the rule.
Test Steps	<p>IPv4:</p> <ul style="list-style-type: none"> • Configure the firewall rule order to allow packets to a specific destination-address and deny packets to its network segment. • Apply the filter to the TOE Interface. • Send traffic to configured specific destination and network segment addresses. • Verify through the firewall logs that only traffic to specific destination address are allowed and remaining addresses to network segment are discarded. • Verify the rules applied through Packet Capture. <ul style="list-style-type: none"> • Configure the firewall rule order to deny packets to a network segment and allow packets to a specific destination-address of the network segment. • Apply the filter to the TOE Interface • Send traffic to configured specific destination and network segment addresses. • Verify through the firewall logs that all traffic is dropped. • Verify the rules applied through Packet Capture. <p>IPv6:</p> <ul style="list-style-type: none"> • Configure the firewall rule order to allow packets to a specific destination-address and deny packets to its network segment. • Apply the filter to the TOE Interface. • Send traffic to configured specific destination and network segment addresses. • Verify through the firewall logs that only traffic to specific destination address are allowed and remaining addresses to network segment are discarded. • Verify the rules applied through Packet Capture. <ul style="list-style-type: none"> • Configure the firewall rule order to deny packets to a network segment and allow packets to a specific destination-address of the network segment. • Apply the filter to the TOE Interface • Send traffic to configured specific destination and network segment addresses. • Verify through the firewall logs that all traffic is dropped. • Verify the rules applied through Packet Capture.
Expected Test Results	<ul style="list-style-type: none"> • TOE firewall logs show that only traffic matching configured specific destination address is permitted when filter ruleset allows packets to a specific destination-address and denies packets to its network segment.

	<ul style="list-style-type: none"> • Packet Capture shows that only traffic matching configured specific destination address is permitted when filter ruleset allows packets to a specific destination-address and denies packets to its network segment. • TOE firewall logs show that all traffic matching configured network destination address is denied when filter ruleset denies packets to a network segment and allows packets to a specific destination-address of the network segment. • Packet Capture shows that all traffic matching configured network destination address is denied when filter ruleset denies packets to a network segment and allows packets to a specific destination-address of the network segment.
Pass/Fail with Explanation	Pass. TOE enforces the first rule in the firewall filter. This meets the testing requirement.

6.3.19 FFW_RUL_EXT.1.9 Test #1

Item	Data
Test Assurance Activity	For each attribute in FFW_RUL_EXT.1.2, the evaluator shall construct a test to demonstrate that the attribute from the packet header to the ruleset, and shall demonstrate both the permit and deny. It shall be verified that a packet is dropped if no matching rule can be identified for the packet. The evaluator shall record a packet capture for each case to confirm that the relevant rule was applied. The evaluator shall record a packet capture for each case to confirm that the relevant rule was applied. The evaluator shall record a packet capture for each case to confirm that the relevant rule was applied. The evaluator shall record a packet capture for each case to confirm that the relevant rule was applied.
Pass/Fail with Explanation	Pass. This test has been completed as part of FFW_RUL_EXT.1.2 Test#1.

6.3.20 FFW_RUL_EXT.1.10 Test #1

Item	Data
Test Assurance Activity	<p>The following tests shall be run using IPv4 and IPv6.</p> <p>Test 1: The evaluator shall define a TCP half-open connection limit on the TOE. The evaluator shall generate TCP SYN requests to pass through the TOE to the target system using a randomised source IP address and common destination IP address. The number of SYN requests should exceed the TCP half-open threshold defined on the TOE. TCP SYN-ACK messages should not be acknowledged. The evaluator shall verify through packet capture that once the defined TCP half-open threshold has been reached, subsequent TCP SYN packets are not transmitted to the target system. The evaluator shall verify that when the configured threshold is reached that, depending upon the selection, either a log entry is generated or a counter is incremented.</p>
Test Steps	<p>IPv4:</p> <ul style="list-style-type: none"> • Configure the TOE to limit the amount of half-open TCP connections. • Apply the configuration to the TOE's interface. • Send continuous traffic to the TOE. • Verify that when the configured threshold is reached a log entry is generated and a counter is incremented.

	<ul style="list-style-type: none"> • Verify with logs. • Verify with packet capture. <p>IPv6:</p> <ul style="list-style-type: none"> • Configure the TOE to limit the amount of half-open TCP connections. • Apply the configuration to the TOE's interface. • Send continuous traffic to the TOE. • Verify that when the configured threshold is reached a log entry is generated and a counter is incremented. • Verify with logs. • Verify with packet capture.
Expected Test Results	<ul style="list-style-type: none"> • TOE generates log entry and increments counter to show the half-open TCP connections after configured threshold has been reached. • Packet Capture shows TOE not responding to the half-open TCP connections after configured threshold has been reached.
Pass/Fail with Explanation	Pass. Half Open TCP SYN packets are not acknowledged by the TOE. When the configured threshold is reached, a log entry is generated by the TOE. This meets the testing requirements.

6.3.21 FFW_RUL_EXT.2.1 Test #1

Item	Data
Test Assurance Activity	Test 1: The evaluator shall define stateful traffic filtering rules to permit and log traffic for each of the supported protocols and drop and log TCP and UDP ports above 1024. Subsequently, the evaluator shall establish a connection for each of the selected protocols in order to ensure that it succeeds. The evaluator shall examine the generated logs to verify they are consistent with the guidance documentation.
Test Steps	<p>TCP</p> <ul style="list-style-type: none"> • Configure the TOE to drop and log TCP ports above 1024. • Apply the filter to the TOE's interface. • Establish a TCP connection with port 1023. • Verify through the firewall log that the connection is successful. • Verify through a packet capture that the connection is successful. • Establish a TCP connection with port 1025. • Verify through the firewall log that the connection is unsuccessful. • Verify through a packet capture that the connection is unsuccessful. <p>UDP</p> <ul style="list-style-type: none"> • Configure the TOE to drop and log UDP ports above 1024. • Apply the filter to the TOE's interface.

	<ul style="list-style-type: none"> Establish a UDP connection with port 1022. Verify through the firewall log that the connection is successful. Verify through a packet capture that the connection is established. Establish a UDP connection with port 1026. Verify through the firewall log that the connection is unsuccessful. Verify through a packet capture that the connection is not established.
Expected Test Results	<ul style="list-style-type: none"> TOE logs show traffic with supported protocols with ports below 1024 getting permitted according to configured filter. Packet Capture shows traffic with supported protocols with ports below 1024 getting permitted according to configured filter. TOE logs show traffic with supported protocols with ports above 1024 getting denied according to configured filter. Packet Capture shows traffic with supported protocols with ports above 1024 getting denied according to configured filter.
Pass/Fail with Explanation	Pass. The TOE permits and logs TCP and UDP port above 1024 and establishes a connection with the selected protocol of FTP.

6.3.22 FFW_RUL_EXT.2.1 Test #2

Item	Data
Test Assurance Activity	Test 2: Continuing from Test 1, the evaluator shall determine (e.g., using a packet sniffer) which port above 1024 opened by the control protocol, terminate the connection session, and then verify that TCP or UDP (depending on the protocol selection) packets cannot be sent through the TOE using the same source and destination addresses and ports.
Test Steps	<p>TCP</p> <ul style="list-style-type: none"> Configure the TOE to drop and log TCP ports above 1024. Apply the filter to the TOE's interface. Establish a supported TCP connection then terminate the session. Note the port opened by the Control Protocol for the former connection. Send a packet matching the former TCP session. Verify through the firewall log and packet capture that the TOE logs the packet Verify through the packet capture that the connection is rejected. <p>UDP</p> <ul style="list-style-type: none"> Configure the TOE to drop and log UDP ports above 1024. Apply the filter to the TOE's interface. Establish a supported UDP connection then terminate the session. Note the port opened by the Control Protocol for the former connection.

	<ul style="list-style-type: none"> • Send a packet matching the former UDP session. • Verify through the firewall log and packet capture that the TOE logs the packet • Verify through the packet capture that the connection is rejected.
Expected Test Results	<ul style="list-style-type: none"> • TOE logs traffic matching destination and source ports of former session with port above 1024 • Packet Capture shows traffic matching destination and source ports of former session with port above 1024 getting rejected by TOE.
Pass/Fail with Explanation	Pass. TCP or UDP packets using the same source and destination addresses and ports as former sessions are not sent through the TOE. This meets the testing requirements.

6.3.23 FFW_RUL_EXT.2.1 Test #3

Item	Data
Test Assurance Activity	Test 3: For each additionally supported protocol, the evaluator shall repeat the procedure above for the protocol. In each case the evaluator must use the applicable RFC or standard in order to determine what range of ports to block in order to ensure the dynamic rules are created and effective.
Pass/Fail with Explanation	Pass. No additional supported protocol selected. Selected FTP protocol is covered in FFW_RUL_EXT.2.1 Test #1 and FFW_RUL_EXT.2.1 Test #2

6.4 IPsec

6.4.1 FCS_IPSEC_EXT.1.1 Test #1

Item	Data
Test Assurance Activity	The evaluator shall configure the SPD such that there is a rule for dropping a packet, encrypting a packet, and allowing a packet to flow in plaintext. The selectors used in the construction of the rule shall be different such that the evaluator can generate a packet and send packets to the gateway with the appropriate fields (fields that are used by the rule - e.g., the IP addresses, TCP/UDP ports) in the packet header. The evaluator performs both positive and negative test cases for each type of rule (e.g. a packet that matches the rule and another that does not match the rule). The evaluator observes via the audit trail, and packet captures that the TOE exhibited the expected behavior: appropriate packets were dropped, allowed to flow without modification, encrypted by the IPsec implementation.
Test Flow	<ul style="list-style-type: none"> • Configure IKE/IPsec rules on the TOE for connecting to an IKE/IPsec Peer to allow (PROTECT) a specific type of traffic. • Send traffic that will trigger the rule. • Verify that the traffic is processed as required for the configured IKE/IPsec rules. • Send traffic that does not match the rule and verify that the traffic is processed accordingly. • Configure IKE/IPsec rules on the TOE for connecting to an IKE/IPsec Peer to deny (DISCARD) a specific type of traffic.

	<ul style="list-style-type: none"> • Send traffic that will trigger the rule. • Verify that the traffic is processed as required for the configured IKE/IPsec rules. • Send traffic that does not match the rule and verify that the traffic is processed accordingly. <ul style="list-style-type: none"> • Configure IKE/IPsec rules on the TOE for connecting to an IKE/IPsec Peer to send plaintext (BYPASS) a specific type of traffic. • Send traffic that will trigger the rule. • Verify that the traffic is processed as required for the configured IKE/IPsec rules. • Send traffic that does not match the rule and verify that the traffic is processed accordingly.
Expected Test Results	<ul style="list-style-type: none"> • TOE logs verify it allows specific type of traffic as configured in the policy. • Packet Capture verifies that TOE allows specific type of traffic as configured in the policy. <ul style="list-style-type: none"> • TOE logs verify it denies specific type of traffic as configured in the policy. • Packet Capture verifies that TOE denies specific type of traffic as configured in the policy. <ul style="list-style-type: none"> • TOE logs verify that it bypasses specific type of traffic as configured in the policy. • Packet Capture verifies that TOE bypasses (sends in plaintext) specific type of traffic as configured in the policy.
Pass/Fail with Explanation	Pass. The TOE implements rules for dropping a packet, encrypting a packet, and allowing a packet to flow in plaintext.

6.4.2 FCS_IPSEC_EXT.1.1 Test #2

Item	Data
Test Assurance Activity	The evaluator shall devise several tests that cover a variety of scenarios for packet processing. As with Test 1, the evaluator ensures both positive and negative test cases are constructed. These scenarios must exercise the range of possibilities for SPD entries and processing modes as outlined in the TSS and guidance documentation. Potential areas to cover include rules with overlapping ranges and conflicting entries, inbound and outbound packets, and packets that establish SAs as well as packets that belong to established SAs. The evaluator shall verify, via the audit trail and packet captures, for each scenario that the expected behavior is exhibited, and is consistent with both the TSS and the guidance documentation.
Test Flow	<ul style="list-style-type: none"> • Configure IKE/IPsec policies meeting the following: <ul style="list-style-type: none"> ○ Allow (PROTECT) a large set of traffic (e.g., TCP/IP, subnet) ○ Deny (DISCARD) a subset of the traffic (e.g., specific protocol, specific address) • Send traffic matching the policies and verify that the specific traffic is protected or discarded accordingly. • Verify via logs that the traffic is processed accordingly.

	<ul style="list-style-type: none"> • Configure IKE/IPsec policies meeting the following: <ul style="list-style-type: none"> ○ Send plaintext (BYPASS) a large set of traffic (e.g., TCP/UDP, subnet) ○ Allow (PROTECT) a subset of the traffic (e.g., specific protocol, specific address) • Send traffic matching the policies and verify that the specific traffic is protected or bypassed accordingly. • Verify via logs that the traffic is processed accordingly. • Configure IKE/IPsec policies meeting the following: <ul style="list-style-type: none"> ○ Deny (DISCARD) a small set of the traffic (e.g., specific protocol, specific address) ○ Send plaintext (BYPASS) a larger superset of traffic (e.g., TCP/UDP, subnet) • Send traffic matching the policies and verify that the specific traffic is discarded or bypassed accordingly. • Verify via logs that the traffic is processed accordingly. • Configure IKE/IPsec policies meeting the following: <ul style="list-style-type: none"> ○ Allow (PROTECT) all traffic • Send various types of traffic • Verify via logs that all traffic is encrypted • Configure IKE/IPsec policies meeting the following: <ul style="list-style-type: none"> ○ Send plaintext (BYPASS) all traffic • Send various types of traffic • Verify via logs that all traffic is sent plaintext • Configure IKE/IPsec policies meeting the following: <ul style="list-style-type: none"> ○ Deny (DISCARD) all traffic • Send various types of traffic • Verify via logs that all traffic is dropped
<p>Expected Test Results</p>	<ul style="list-style-type: none"> • TOE logs verify it protects specific type of traffic as configured in the policy. • Packet Capture verifies that TOE protects specific type of traffic as configured in the policy. • TOE logs verify it denies specific type of traffic as configured in the policy. • Packet Capture verifies that TOE denies specific type of traffic as configured in the policy. • TOE logs verify that it bypasses specific type of traffic as configured in the policy.

	<ul style="list-style-type: none"> • Packet Capture verifies that TOE bypasses (sends in plaintext) specific type of traffic as configured in the policy.
Pass/Fail with Explanation	Pass. The TOE dropped packets when configured, encrypted packets when configured, and sent packets in plaintext when configured. This meets the testing requirements.

6.4.3 FCS_IPSEC_EXT.1.2 Test #1

Item	Data
Test Assurance Activity	The evaluator shall configure the SPD such that there is a rule for dropping a packet, encrypting a packet, and allowing a packet to flow in plaintext. The evaluator may use the SPD that was created for verification of FCS_IPSEC_EXT.1.1. The evaluator shall construct a network packet that matches the rule to allow the packet to flow in plaintext and send that packet. The evaluator should observe that the network packet is passed to the proper destination interface with no modification. The evaluator shall then modify a field in the packet header; such that it no longer matches the evaluator-created entries (there may be a "TOE created" final entry that discards packets that do not match any previous entries). The evaluator sends the packet and observes that the packet was dropped.
Test Flow	<ul style="list-style-type: none"> • Configure policy on TOE to allow the packet to flow in plaintext. • Attempt a connection. • Verify via logs that the connection is successful. • Attempt a connection with modified header. • Verify via logs that the connection is unsuccessful.
Expected Test Results	<ul style="list-style-type: none"> • TOE allows traffic to flow in plaintext according to configured policy. • TOE does not respond to allowed traffic with modified header.
Pass/Fail with Explanation	Pass. When the modified packet is sent, the TOE rejects the connection.

6.4.4 FCS_IPSEC_EXT.1.3 Test #1

Item	Data
Test Assurance Activity	If tunnel mode is selected, the evaluator uses the guidance documentation to configure the TOE to operate in tunnel mode and also configures a VPN peer to operate in tunnel mode. The evaluator configures the TOE and the VPN peer to use any of the allowable cryptographic algorithms, authentication methods, etc. to ensure an allowable SA can be negotiated. The evaluator shall then initiate a connection from the TOE to connect to the VPN peer. The evaluator observes (for example, in the audit trail and the captured packets) that a successful connection was established using the tunnel mode.
Test Flow	<ul style="list-style-type: none"> • Configure an IKE/IPsec connection (ensure that tunnel mode is configured) • Initiate traffic through IPsec Tunnel. • Verify Tunnel mode was used within logs.

Expected Test Results	<ul style="list-style-type: none"> • TOE establishes successful connection with peer in tunnel mode with supported algorithms. • TOE logs verify successful connection with peer in tunnel mode with supported algorithms. • Packet Capture verifies successful connection with peer in tunnel mode with supported algorithms.
Pass/Fail with Explanation	Pass. The TOE performs a successful connection using tunnel mode.

FCS_IPSEC_EXT.1.3 Test #2

Item	Data
Test Assurance Activity	Test 2: If transport mode is selected, the evaluator uses the guidance documentation to configure the TOE to operate in transport mode and also configures a VPN peer to operate in transport mode. The evaluator configures the TOE and the VPN peer to use any of the allowed cryptographic algorithms, authentication methods, etc. to ensure an allowable SA can be negotiated. The evaluator then initiates a connection from the TOE to connect to the VPN peer. The evaluator observes (for example, in the audit trail and the captured packets) that a successful connection was established using the transport mode.
Pass/Fail with Explanation	N/A. Transport mode is not selected.

6.4.5 FCS_IPSEC_EXT.1.4 Test #1

Item	Data
Test Assurance Activity	The evaluator shall configure the TOE as indicated in the guidance documentation configuring the TOE to use each of the supported algorithms, attempt to establish a connection using ESP, and verify that the attempt succeeds.
Test Flow	<u>IKEv1</u> <ul style="list-style-type: none"> • Configure the TOE for IKEv1 AES-CBC-128 & SHA-256 configuration in ESP. • Configure the PEER for IKEv1 AES-CBC-128 & SHA-256 configuration in ESP. • Start an IPsec connection (using Ping) and verify via packet capture that the connection was established IKEv1. • Verify via logs that the connection was established using AES-CBC-128 & SHA-256. <ul style="list-style-type: none"> • Configure the TOE for IKEv1 AES-CBC-192 & sha-256 configuration in ESP. • Configure the PEER for IKEv1 AES-CBC-192 & sha-256 configuration in ESP. • Start an IPsec connection (using Ping) and verify via packet capture that the connection was established using IKEv1. • Verify via logs that the connection was established using AES-CBC-192 & SHA256 in ESP. <ul style="list-style-type: none"> • Configure the TOE for IKEv1 AES-CBC-256 & sha-256 configuration in the ESP.

- Configure the PEER for IKEv1 AES-CBC-256 & sha-256 configuration in ESP.
 - Start an IPsec connection (using Ping) and verify via packet capture that the connection was established using IKEv1.
 - Verify via logs that the connection was established using AES-CBC-256 & SHA256 in ESP.
-
- Configure the TOE for IKEv1 AES-GCM-192 in ESP.
 - Configure the PEER for IKEv1 AES-GCM-192 in ESP .
 - Start an IPsec connection (using Ping) and verify via packet capture that the connection was established using IKEv1.
 - Verify via logs that the connection was established using AES-GCM-192.
-
- Configure the TOE for IKEv1 AES-GCM-256 in ESP.
 - Configure the PEER for IKEv1 AES-GCM-256 in ESP.
 - Start an IPsec connection (using Ping) verify via packet capture that the connection was established using IKEv1.
 - Verify via logs that the connection was established using AES-GCM-256.

IKEv2

- Configure the TOE for IKEv2 AES-CBC-128 & SHA-256 configuration in ESP.
 - Configure the PEER for IKEv2 AES-CBC-128 & SHA-256 configuration in ESP.
 - Start an IPsec connection (using Ping) and verify via packet capture that the connection was established using IKEv2.
 - Verify via logs that the connection was established using AES-CBC-128 & SHA-256.
-
- Configure the TOE for IKEv2 AES-CBC-192 & sha-256 configuration in ESP.
 - Configure the PEER for IKEv2 AES-CBC-192 & sha-256 configuration in ESP.
 - Start an IPsec connection (using Ping) and verify via packet capture that the connection was established using IKEv2.
 - Verify via logs that the connection was established using AES-CBC-192 & sha-256.
-
- Configure the TOE for IKEv2 AES-CBC-256 & sha-256 configuration in the ESP.
 - Configure the PEER for IKEv2 AES-CBC-256 & sha-256 configuration in ESP.
 - Start an IPsec connection (using Ping) and verify via packet capture that the connection was established using IKEv2.
 - Verify via logs that the connection was established using AES-CBC-256 & SHA256.
-
- Configure the TOE for IKEv2 AES-GCM-192 in ESP.
 - Configure the PEER for IKEv2 AES-GCM-192 in ESP.
 - Start an IPsec connection (using Ping) and verify via packet capture that the connection was established using IKEv2.
 - Verify via logs that the connection was established using AES-GCM-192.

	<ul style="list-style-type: none"> • Configure the TOE for IKEv2 AES-GCM-256 configuration in the ESP. • Configure the PEER for IKEv2 AES-GCM-256 configuration in ESP. • Start an IPsec connection (using Ping) and verify via packet capture that the connection was established using IKEv2. • Verify via logs that the connection was established using AES-GCM-256.
Expected Test Results	<ul style="list-style-type: none"> • TOE establishes successful connection with peer with each supported algorithm. • Packet Capture verifies successful connection with peer with each supported algorithm.
Pass/Fail with Explanation	Pass. IPsec SAs can be configured with each claimed algorithm. IPsec SAs can be configured with each claimed hash algorithm. This meets the testing requirements.

6.4.6 FCS_IPSEC_EXT.1.5 Test #1

Item	Data
Test Assurance Activity	If IKEv1 is selected, the evaluator shall configure the TOE as indicated in the guidance documentation and attempt to establish a connection using an IKEv1 Phase 1 connection in aggressive mode. This attempt should fail. The evaluator should then show that main mode exchanges are supported.
Test Flow	<ul style="list-style-type: none"> • Configure the TOE to support IKEv1 using main mode only. • Configure Peer for aggressive mode. • Attempt to establish an IPsec session and verify that Aggressive mode connections are not possible via packet capture. • Verify that Aggressive mode connections are not possible via log. • Configure the Peer to support IKEv1 using main mode only • Attempt to establish an IPsec session via ping and verify that main mode is established in the ipsec connection via packet capture • Verify that main mode connection is established via log.
Expected Test Results	<ul style="list-style-type: none"> • TOE does not establish connection with peer in aggressive mode. • TOE logs verify it does not establish connection with peer in aggressive mode. • Packet Capture verifies it does not establish connection with peer in aggressive mode. • TOE establishes connection with peer in main mode. • TOE logs verify it establishes connection with peer in main mode. • Packet Capture verifies it establishes connection with peer in main mode.
Pass/Fail with Explanation	Pass. The TOE rejected a connection attempt with Aggressive mode and then accepted a connection attempt with main mode. This meets the testing requirements.

6.4.7 FCS_IPSEC_EXT.1.6 Test #1

Item	Data
Test Assurance Activity	The evaluator shall configure the TOE to use the ciphersuite under test to encrypt the IKEv1 and/or IKEv2 payload and establish a connection with a peer device, which is configured to only accept the payload encrypted using the indicated ciphersuite. The evaluator will confirm the algorithm was that used in the negotiation.
Test Flow	<ul style="list-style-type: none"> • Configure the TOE with an IKEv1 proposal using AES-CBC-128. • Configure the Peer with an IKEv1 proposal using AES-CBC-128. • Attempt a connection between the two devices. • Verify via logs that the negotiation uses AES-CBC-128 as specified in the proposal. • Configure the TOE with an IKEv1 proposal using AES-CBC-192. • Configure the Peer with an IKEv1 proposal using AES-CBC-192. • Attempt a connection between the two devices. • Verify via logs that the negotiation uses AES-CBC-192 as specified in the proposal. • Configure the TOE with an IKEv1 proposal using AES-CBC-256. • Configure the Peer with an IKEv1 proposal using AES-CBC-256. • Attempt a connection between the two devices. • Verify via logs that the negotiation uses AES-CBC-256 as specified in the proposal. • Configure the TOE with an IKEv2 proposal using AES-GCM-128. • Configure the Peer with an IKEv2 proposal using AES-GCM-128. • Attempt a connection between the two devices. • Verify via logs that the negotiation uses AES-GCM-128 as specified in the proposal. • Configure the TOE with an IKEv2 proposal using AES-GCM-256. • Configure the Peer with an IKEv2 proposal using AES-GCM-256. • Attempt a connection between the two devices. • Verify via logs that the negotiation uses AES-GCM-256 as specified in the proposal.
Expected Test Results	<ul style="list-style-type: none"> • Packet Capture verifies the IKEV1 payload is encrypted using configured ciphersuite. • Packet Capture verifies the IKEV2 payload is encrypted using configured ciphersuite.
Pass/Fail with Explanation	Pass. IKE SAs can be configured with each claimed algorithm. This meets the testing requirements.

6.4.8 FCS_IPSEC_EXT.1.7 Test #2

Item	Data
Test Assurance Activity	<p>Test 2: If 'length of time' is selected as the SA lifetime measure, the evaluator shall configure a maximum lifetime of 24 hours for the Phase 1 SA following the guidance documentation. The evaluator shall configure a test peer with a lifetime that exceeds the Phase 1 lifetime of the TOE. The evaluator shall establish a SA between the TOE and the test peer, maintain the Phase 1 SA for 24 hours, and determine that a new Phase 1 SA is negotiated on or before 24 hours has elapsed. The evaluator shall verify that the TOE initiates a Phase 1 negotiation.</p> <p>TD0800 has been applied.</p>
Test Flow	<ul style="list-style-type: none"> • Configure the TOE to support 23 hour (82800 sec) lifetime for IKEv1 Phase 1. • Configure the Peer to support 24 hour lifetime (86400 sec) for IKEv1 Phase 1. • Establish and maintain session for 24 hours. • Verify that Phase 1 renegotiates after 24 hours via log review and packet capture. <ul style="list-style-type: none"> • Configure the TOE to support 23 hour (82800 sec) lifetime for IKEv2 Phase 1. • Configure the Peer to support 24 hour lifetime (86400 sec) for IKEv2 Phase 1. • Establish and maintain session for 24 hours. • Verify that Phase 1 renegotiates after 24 hours via log review and packet capture.
Expected Test Results	<ul style="list-style-type: none"> • TOE renegotiates Phase 1 after lifetime exceeds its configured lifetime. • Packet capture verifying successful renegotiation.
Pass/Fail with Explanation	<p>Pass. The TOE renegotiates phase 1 after the lifetime exceeds the lifetime of the TOE.</p>

6.4.9 FCS_IPSEC_EXT.1.8 Test #1

Item	Data
Test Assurance Activity	<p>Test 1: If 'number of bytes' is selected as the SA lifetime measure, the evaluator shall configure a maximum lifetime in terms of the number of bytes allowed following the guidance documentation. The evaluator shall configure a test peer with a byte lifetime that exceeds the lifetime of the TOE. The evaluator shall establish a SA between the TOE and the test peer, and determine that once the allowed number of bytes through this SA is exceeded, a new SA is negotiated. The evaluator shall verify that the TOE initiates a Phase 2 negotiation.</p>
Test Flow	<ul style="list-style-type: none"> • Configure the TOE for an IKEv2 Phase 2 bytes per lifetime of 64 kB. • Configure the Peer for an IKEv2 Phase 2 bytes per lifetime of 70 kB. • Establish an IPsec session and transmit packets across the connections repeatedly. • Verify that when the bytes threshold is crossed a rekey is initiated.

Expected Test Results	<ul style="list-style-type: none"> • TOE initiates a Phase 2 renegotiation on exceeding the configured number of bytes through the SA. • Packet capture verifying Phase 2 rekeying.
Pass/Fail with Explanation	Pass. The TOE initiates a new SA when the allowed number of bytes through the existing SA is exceeded. This meets the testing requirements.

6.4.10 FCS_IPSEC_EXT.1.8 Test #2

Item	Data
Test Assurance Activity	<p>Test 2: If 'length of time' is selected as the SA lifetime measure, the evaluator shall configure a maximum lifetime of 8 hours for the Phase 2 SA following the guidance documentation. The evaluator shall configure a test peer with a Phase 2 lifetime that exceeds the Phase 2 lifetime of the TOE. The evaluator shall establish a SA between the TOE and the test peer, maintain the Phase 1 SA for 8 hours, and determine that once a new Phase 2 SA is negotiated when or before 8 hours has lapsed. The evaluator shall verify that the TOE initiates a Phase 2 negotiation.</p> <p>TD0800 has been applied.</p>
Test Flow	<ul style="list-style-type: none"> • Configure the IKEv1 Phase 2 SA Lifetime as 8 hours (28800 seconds) on the TOE. • Configure the IKEv1 Phase 2 SA lifetime for more than 8 hours (30000 seconds) on the peer. • Establish and maintain an IPsec connection between the TOE and peer for 8 hours. • Verify that a rekey was initiated before 8 hours via log review and packet capture. • Configure the IKEv2 Phase 2 SA Lifetime as 8 hours (28800 seconds) on the TOE. • Configure the IKEv2 Phase 2 SA lifetime for more than 8 hours (30000 seconds) on the peer. • Establish and maintain an IPsec connection between the TOE and peer for 8 hours. • Verify that a rekey was initiated before 8 hours via log review and packet capture.
Expected Test Results	<ul style="list-style-type: none"> • TOE renegotiates Phase 2 after lifetime exceeds its configured lifetime. • Packet capture verifying successful renegotiation.
Pass/Fail with Explanation	Pass. The TOE initiated a rekey after the configured time (8 hours in this case). This meets the testing requirements.

6.4.11 FCS_IPSEC_EXT.1.10 Test #1

Item	Data
------	------

Test Assurance Activity	Each of the following tests shall be performed for each version of IKE selected in the FCS_IPSEC_EXT.1.5 protocol selection: If the first selection is chosen, the evaluator shall check to ensure that, for each DH group supported, the TSS describes the process for generating each nonce. The evaluator shall verify that the TSS indicates that the random number generated that meets the requirements in this PP is used, and that the length of the nonces meet the stipulations in the requirement.
Pass/Fail with Explanation	Pass. Covered by FCS_IPSEC_EXT.1.10 TSS 1 Assurance Activities in the AAR.

6.4.12 FCS_IPSEC_EXT.1.11 Test #1

Item	Data
Test Assurance Activity	For each supported DH group, the evaluator shall test to ensure that all supported IKE protocols can be successfully completed using that particular DH group.
Test Flow	<p>IKEv1</p> <ul style="list-style-type: none"> • Configure DH group 14 for IKEv1 on TOE. • Configure DH group 14 for IKEv1 on PEER. • Start an IPsec connection (using Ping) and verify that Group 14 is used via capture. • Verify that DH Group 14 was used via log. <ul style="list-style-type: none"> • Configure the TOE for Group 19. • Configure the Peer for Group 19. • Generate traffic to trigger the IPsec session and verify that DH Group 19 was used via packet capture. • Verify that DH group 19 was used via log . <ul style="list-style-type: none"> • Configure the TOE for Group 20. • Configure the Peer for Group 20. • Generate traffic to trigger the IPsec session and verify that DH Group 20 was used via packet capture. • Verify that DH group 20 was used via log. <p>IKEv2</p> <ul style="list-style-type: none"> • Configure DH group 14 for IKEv2 on TOE. • Configure DH group 14 for IKEv2 on PEER. • Start an IPsec connection (using Ping) and verify that Group 14 is used via capture . • Verify that DH Group 14 was used via log. <ul style="list-style-type: none"> • Configure the TOE for Group 19. • Configure the Peer for Group 19. • Generate traffic to trigger the IPsec session and verify that DH Group 19 was used via packet capture.

	<ul style="list-style-type: none"> • Verify that DH group 19 was used via log. • Configure the TOE for Group 20. • Configure the Peer for Group 20. • Generate traffic to trigger the IPsec session and verify that DH Group 20 was used via packet capture. • Verify that DH group 20 was used via log.
Expected Test Results	<ul style="list-style-type: none"> • TOE allows IKE SA establishment using DH group 14. • TOE logs verify successful connection with DH group 14. • Packet Capture verifies successful connection with DH group 14. • TOE allows IKE SA establishment using DH group 19. • TOE logs verify successful connection with DH group 19. • Packet Capture verifies successful connection with DH group 19. • TOE allows IKE SA establishment using DH group 20. • TOE logs verify successful connection with DH group 20. • Packet Capture verifies successful connection with DH group 20.
Pass/Fail with Explanation	Pass. IKE SAs can be configured with each claimed exchange method. This meets the testing requirements.

6.4.13 FCS_IPSEC_EXT.1.12 Test #1

Item	Data
Test Assurance Activity	This test shall be performed for each version of IKE supported. The evaluator shall successfully negotiate an IPsec connection using each of the supported algorithms and hash functions identified in the requirements.
Pass/Fail with Explanation	Pass. This test has been partly completed as part of testing covered in FCS_IPSEC_EXT.1.4 Test #1 and FCS_IPSEC_EXT.1.6 Test #1.

6.4.14 FCS_IPSEC_EXT.1.12 Test #2

Item	Data
Test Assurance Activity	This test shall be performed for each version of IKE supported. The evaluator shall attempt to establish a SA for ESP that selects an encryption algorithm with more strength than that being used for the IKE SA (i.e., symmetric algorithm with a key size larger than that being used for the IKE SA). Such attempts should fail.

Test Flow	<ul style="list-style-type: none"> • Configure the TOE with AES-128-CBC (P1) and AES-256-CBC (P2) and verify commit failure. • Configure TOE to use AES-CBC-128 in P1 and AES-CBC-128 in P2 IKEv1. • Configure peer to use AES-CBC-256 in P1 and AES-CBC-256 in P2 IKEv1. • Attempt to establish a connection and verify the connection is rejected using Packet Capture. • Verify the connection is rejected using logs. • Configure TOE to use AES-CBC-128 in P1 and AES-CBC-128 in P2 IKEv2. • Configure peer to use AES-CBC-256 in P1 and AES-CBC-256 in P2 IKEv2. • Attempt to establish a connection and verify the connection is rejected using Packet Capture.. • Verify the connection is rejected using logs.
Expected Test Results	<ul style="list-style-type: none"> • When attempting to connect to a peer with the IPsec SA strength larger than the IKE SA strength, the TOE should be able to reject the connection. • Log showing the failed connection. • Packet capture showing the failed connection.
Pass/Fail with Explanation	Pass. When attempting to connect to a peer with the IPsec SA strength larger than the IKE SA strength, the TOE is able to reject the connection. This meets the testing requirements.

6.4.15 FCS_IPSEC_EXT.1.12 Test #3

Item	Data
Test Assurance Activity	This test shall be performed for each version of IKE supported. The evaluator shall attempt to establish an IKE SA using an algorithm that is not one of the supported algorithms and hash functions identified in the requirements. Such an attempt should fail.
Test Flow	<p><u>IKEv1</u></p> <ul style="list-style-type: none"> • Configure the TOE to use AES-128-CBC and SHA-256. • Configure the Peer to use AES-128-CBC and SHA-384. • Attempt a secure IPsec connection and verify that the connection is rejected via packet capture. • Verify the logs reflected on the TOE. <p><u>IKEv2</u></p> <ul style="list-style-type: none"> • Configure the TOE to use AES-128-CBC and SHA-256. • Configure the Peer to use AES-128-CBC and SHA-384. • Attempt a secure IPsec connection and verify that the connection is rejected via packet capture. • Verify the logs reflected on the TOE.

Expected Test Results	<ul style="list-style-type: none"> • TOE does not establish connection with peer when its IKE SA contains an unsupported algorithm or hash function. • TOE logs verify unsuccessful connection due to incompatible peer proposal. • Packet capture verifies unsuccessful connection due to incompatible peer proposal.
Pass/Fail with Explanation	Pass. The TOE will only support and propose the configured algorithm. If the TOE peer does not have matching algorithms this session will not be established. This meets the testing requirements.

6.4.16 FCS_IPSEC_EXT.1.12 Test #4

Item	Data
Test Assurance Activity	This test shall be performed for each version of IKE supported. The evaluator shall attempt to establish a SA for ESP (assumes the proper parameters were used to establish the IKE SA) that selects an encryption algorithm that is not identified in FCS_IPSEC_EXT.1.4. Such an attempt should fail.
Test Flow	<ul style="list-style-type: none"> • Configure the TOE to support the following algorithms: <ul style="list-style-type: none"> • IKEv1 SA (Phase 1): AES-CBC-128, SHA-256. • IPsec SA (Phase 2): AES-CBC-128, SHA-256. • Configure a peer to support the following algorithms: <ul style="list-style-type: none"> • IKEv1 SA (Phase 1): AES-CBC-128, SHA-256. • IPsec SA (Phase 2): AES-GCM-128. • Attempt to make a connection. • Verify via logs that the connection cannot be established. <ul style="list-style-type: none"> • Configure the TOE to support the following algorithms: <ul style="list-style-type: none"> • IKEv2 SA (Phase 1): AES-CBC-128, SHA-256. • IPsec SA (Phase 2): AES-CBC-128, SHA-256. • Configure a peer to support the following algorithms: <ul style="list-style-type: none"> • IKEv2 SA (Phase 1): AES-CBC-128, SHA-256. • IPsec SA (Phase 2): AES-GCM-128. • Attempt to make a connection. • Verify via logs that the connection cannot be established.
Expected Test Results	<ul style="list-style-type: none"> • TOE does not establish connection with peer when its IPsec SA contains an unsupported encryption algorithm. • TOE logs verify unsuccessful connection due to negotiation failure. • Packet capture verifies unsuccessful connection due to negotiation failure.
Pass/Fail with Explanation	Pass. Since the IPsec SA parameters did not match the IPsec SA parameters of the TOE peer, an IPsec connection could not be established. An IKE SA, however, could be established because the peer parameters matched. This meets the testing requirements.

6.4.17 FCS_IPSEC_EXT.1.14 Test #2

Item	Data
------	------

Test Assurance Activity	<p>Test 2: [conditional] For each SAN/identifier type combination selected, the evaluator shall configure the peer's reference identifier on the TOE (per the administrative guidance) to match the field in the peer's presented certificate and shall verify that the IKE authentication succeeds.</p> <p>If the TOE prioritizes SAN checking over CN (through explicit specification of the field when specifying the reference identifier or prioritization rules), the evaluator shall also configure the CN so it contains an incorrect identifier formatted to be the same type (e.g. the reference identifier on the TOE is DNS-ID; identify certificate has an identifier in SAN with correct DNS-ID, CN with incorrect DNS-ID (and not a different type of identifier)) and verify that IKE authentication succeeds.</p>
Test Flow	<ul style="list-style-type: none"> • Create and load a peer certificate with a SAN IP that matches the TOE's reference identifier. • Verify through logs and a packet capture that the connection succeeds. • Create and load a peer certificate with a FQDN in the SAN that matches the TOE's reference identifier. • Verify through logs and a packet capture that the connection succeeds. • Create and load a peer certificate with a User FQDN in the SAN that matches the TOE's reference identifier. • Verify through logs and a packet capture that the connection succeeds. • Create and load a peer certificate with a SAN IP that matches the TOE's reference identifier but with an incorrect IP in the CN field. • Verify through logs and a packet capture that the connection succeeds. • Create and load a peer certificate with a FQDN in the SAN that matches the TOE's reference identifier but with an incorrect FQDN in the CN field. • Verify through logs and a packet capture that the connection succeeds. • Create and load a peer certificate with a User FQDN in the SAN that matches the TOE's reference identifier but with an incorrect User FQDN in the CN field. • Verify through logs and a packet capture that the connection succeeds.
Expected Test Results	<ul style="list-style-type: none"> • The TOE should accept the connection when the SAN matches with the PEER. • Logs verifying successful connection. • Packet capture verifying successful connection.
Pass/Fail with Explanation	<p>Pass. The TOE accepts connections with a correct identifier in the SAN but incorrect identifier in the CN that is formatted to be the same type of identifier as the SAN. This meets the testing requirements.</p>

6.4.18 FCS_IPSEC_EXT.1.14 Test #4

Item	Data
Test Assurance Activity	<p>Test 4: [conditional] For each SAN/identifier type combination selected, the evaluator shall:</p> <p>a) Create a valid certificate with an incorrect identifier in the SAN. The evaluator shall configure a string representation of the correct identifier in the DN. If the TOE prioritizes CN checking over SAN (through explicit specification of the field when specifying the reference identifier or prioritization rules) for the same identifier type, the addition/modification shall be to any non-CN field of the DN. Otherwise, the addition/modification shall be to the CN.</p> <p>b) Configure the peer’s reference identifier on the TOE (per the administrative guidance) to match the correct identifier (expected in the SAN) and verify that IKE authentication fails.</p>
Test Flow	<ul style="list-style-type: none"> • Create and load a peer certificate with an incorrect SAN IP but a correct IP in the CN field. • Configure the correct IP on the TOE’s peer reference identifier.. • Verify through logs and a packet capture that the connection fails • Create and load a peer certificate with an incorrect FQDN in the SAN but a correct FQDN in the CN field. • Configure the correct FQDN on the TOE’s peer reference identifier. • Verify through logs and a packet capture that the connection fails. • Create and load a peer certificate with an incorrect User FQDN in the SAN but a correct User FQDN in the CN field. • Configure the correct User FQDN on the TOE’s peer reference identifier. • Verify through logs and a packet capture that the connection fails.
Expected Test Results	<ul style="list-style-type: none"> • TOE does not establish connection with local certificate having incorrect SAN and correct CN. • TOE logs verify unsuccessful connection due to local certificate authentication failure. • Packet Capture verifies unsuccessful connection due to local certificate authentication failure.
Pass/Fail with Explanation	<p>Pass. The TOE rejects connections with an incorrect identifier in the SAN but a correct identifier in the CN that is formatted to be the same type of identifier as the SAN. This meets the testing requirements.</p>

6.4.19 FCS_IPSEC_EXT.1.14 Test #5

Item	Data
------	------

Test Assurance Activity	Test 5: [conditional] If the TOE supports DN identifier types, the evaluator shall configure the peer's reference identifier on the TOE (per the administrative guidance) to match the subject DN in the peer's presented certificate and shall verify that the IKE authentication succeeds.
Test Flow	<ul style="list-style-type: none"> • Configure a peer certificate with DN identifier types commonName, organizationalName, organizationalUnitName, and countryName. • Configure the TOE's peer reference identifier to match the DN identifier fields presented in the peer certificate. • Verify that the connection succeeds.
Expected Test Results	<ul style="list-style-type: none"> • TOE establishes successful connection with peer certificate having correct DN. • TOE logs verify successful connection. • Packet Capture verifies successful connection.
Pass/Fail with Explanation	Pass. The TOE supports a connection using the DN as the peer's reference identifier. This meets the testing requirements.

6.4.20 FCS_IPSEC_EXT.1.14 Test #6a

Item	Data
Test Assurance Activity	<p>Test 6: [conditional] If the TOE supports DN identifier types, to demonstrate a bit-wise comparison of the DN, the evaluator shall create the following valid certificates and verify that the IKE authentication fails when each certificate is presented to the TOE:</p> <p>a) Duplicate the CN field, so the otherwise authorized DN contains two identical CNs.</p>
Test Flow	<ul style="list-style-type: none"> • Create a peer certificate with a single CN field. • Use the Acumen x509-mod tool to duplicate CN on the DN of the certificate. • Present this certificate to the TOE and verify that the IKE authentication fails.
Expected Test Results	<ul style="list-style-type: none"> • TOE does not establish successful connection with peer certificate having duplicate CN. • TOE logs verify unsuccessful connection. • Packet Capture verifies unsuccessful connection.
Pass/Fail with Explanation	Pass. When presented with a certificate that contains two identical CNs in the DN field, the TOE rejects the connection. This meets the testing requirements.

6.4.21 FCS_IPSEC_EXT.1.14 Test #6b

Item	Data
------	------

Test Assurance Activity	<p>Test 6: If the TOE supports DN identifier types, to demonstrate a bit-wise comparison of the DN, the evaluator shall create the following valid certificates and verify that the IKE authentication fails when each certificate is presented to the TOE:</p> <p>b) Append '\0' to a non-CN field of an otherwise authorized DN.</p>
Test Flow	<ul style="list-style-type: none"> • Create a normal peer certificate. • Use the x509-mod tool to append '\0' to a non-CN field • Configure Peer with new certificate • Initiate the traffic over the tunnel and verify that the IKE authentication fails.
Expected Test Results	<ul style="list-style-type: none"> • TOE does not establish successful connection with peer certificate has '\0' appended to a non-CN field. • TOE logs verify unsuccessful connection. • Packet Capture verifies unsuccessful connection.
Pass/Fail with Explanation	<p>Pass. When presented with a certificate that has a '\0' appended to a non-CN field of an otherwise authorized DN, the TOE rejects the connection. This meets the testing requirements.</p>

6.5 MOD_IPS

6.5.1 FAU_GEN.1/IPS Test #1

Item	Data
Test Assurance Activity	<p>The evaluator shall test that the interfaces used to configure the IPS polices yield expected IPS data in association with the IPS policies. A number of IPS policy combination and ordering scenarios need to be configured and tested by attempting to pass both allowed and anomalous network traffic matching configured IPS policies in order to trigger all required IPS events.</p> <p>Note the following:</p> <ul style="list-style-type: none"> • This activity should have been addressed with a combination of the Test EAs for the other IPS requirements. • As part of testing this activity, the evaluator shall also ensure that the audit data generated to address this SFR can be handled in the manner that FAU_STG_EXT.1 requires for all audit data
Test Steps	<p>Covered by audit records in each test case.</p>
Pass/Fail with Explanation	<p>Pass. The interfaces used to configure the IPS polices yield expected IPS data in association with the IPS policies.</p>

6.5.2 FMT_SMF.1/IPS Test #1

Item	Data
Test Assurance Activity	Test 1: The evaluator shall use the operational guidance to create a signature and enable it on an interface. The evaluator shall then generate traffic that would be successfully triggered by the signature. The evaluator should observe the TOE applying the corresponding reaction in the signature.
Test Steps	<ul style="list-style-type: none"> • Configure a custom signature filter on the TOE to deny traffic with a specific source address. • Apply the filter to the TOE’s security policy. • Send modified traffic that matches the configured filter and verify traffic was denied as per filter. • Verify through a packet capture and through logs that the traffic was appropriately denied.
Expected Test Results	<ul style="list-style-type: none"> • TOE detects and logs traffic matching the configured signature and drops the traffic according to applied policy. • Packet Capture shows that traffic matching the configured signature is dropped by TOE according to applied policy.
Pass/Fail with Explanation	Pass. Traffic matching the signature successfully triggers the TOE and applies the corresponding reaction in the signature. This meets the testing requirements.

6.5.3 FMT_SMF.1/IPS Test #2

Item	Data
Test Assurance Activity	Test 2: The evaluator shall then disable the signature and attempt to regenerate the same traffic and ensure that the TOE allows the traffic to pass with no reaction
Test Steps	<ul style="list-style-type: none"> • Disable the signature from FMT_SMF.1/IPS Test #1. • Generate the same traffic. • Verify through a packet capture and through logs that the traffic was appropriately allowed to flow.
Expected Test Results	<ul style="list-style-type: none"> • TOE permits traffic matching the configured signature when the applied IDP policy is disabled. • Packet Capture shows traffic matching the configured signature being permitted through TOE when the applied IDP policy is disabled.
Pass/Fail with Explanation	Pass. After disabling the signature, the TOE allows the same traffic to pass through it with no reaction. This meets the testing requirements.

6.5.4 FMT_SMF.1/IPS Test #3

Item	Data
Test Assurance Activity	Test 3: The evaluator shall use the operational guidance to import signatures and repeat the test conducted in Test 1.
Test Steps	<ul style="list-style-type: none"> • Select a signature among the pre-existing signatures in the TOE and configure TOE to generate alarm when traffic matching signature is encountered. • Apply the signature to the security zone upon which the TOE's interface is assigned. • Send traffic that matches the header-based signature. • Verify the attack traffic is detected by the TOE and reacts accordingly.
Expected Test Results	<ul style="list-style-type: none"> • TOE detects and logs traffic matching the configured imported signature and drops the traffic according to applied policy. • Packet Capture shows that traffic matching the configured imported signature is dropped by TOE according to applied policy.
Pass/Fail with Explanation	Pass. The TOE has imported signatures which once enabled, detect traffic matching the signature on the configured interface. This meets the testing requirements.

6.5.5 IPS_ABD_EXT.1 Test #1

Item	Data
Test Assurance Activity	Test 1: The evaluator shall use the instructions in the operational guidance to configure baselines or anomaly-based rules for each attributes specified in IPS_ABD_EXT.1.1. The evaluator shall send traffic that does not match the baseline or matches the anomaly-based rule and verify the TOE applies the configured reaction. This shall be performed for each attribute in IPS_ABD_EXT.1.1.
Test Steps	<p>Throughput:</p> <ul style="list-style-type: none"> • Create a policer to monitor the throughput. • Apply the policer to a firewall filter which specifies the IPv4 source address. • Apply the configuration to the interface. • Modify and send traffic to match the configured filter on the TOE. • Verify through logs that the TOE reacts according to configuration. • Verify via packet capture that the TOE reacts according to configuration. • To ensure that the counter has a base number of 1, the traffic is sent again without resetting the logs. • The TOE allowed and logged an additional two packets while the third was dropped and picked up by the policer. The policer counter increased by one from the previous 1 • Verify via packet capture.

- Create a policer to monitor the throughput.
- Apply the policer to a firewall filter which specifies the IPv4 destination address.
- Apply the configuration to the interface.
- Modify and send traffic to match the configured filter on the TOE.
- Verify through logs that the TOE reacts according to configuration.
- Verify via packet capture that the TOE reacts according to configuration.
- To ensure that the counter has a base number of 1, the traffic is sent again without resetting the logs.
- The TOE allowed and logged an additional two packets while the third was dropped and picked up by the policer. The policer counter increased by one from the previous 1
- Verify via packet capture.

Time of Day:

- Create a schedule, set for five minutes on a particular day of the week.
 - Apply the schedule configuration to the security policy for a particular IPV6 source address.
 - Send traffic to match the configured filter on the TOE during the scheduled time.
 - Verify through logs that while the scheduler was enabled, the appropriate traffic was denied.
 - Verify via Packet Capture.
 - After the scheduler time was complete, initiate the same traffic to the TOE.
 - Verify via logs that traffic matching configured filter after schedule time does not get logged under policy with scheduler.
 - Verify via Packet Capture.
-
- Create a schedule set for five minutes on a particular day of the week.
 - Apply the schedule configuration to the security policy for a particular IPV6 destination address.
 - Send traffic to match the configured filter on the TOE during the scheduled time.
 - Verify through logs that while the scheduler was enabled, the appropriate traffic was denied.
 - Verify via Packet Capture.
 - After the scheduler time was complete, initiate the same traffic to the TOE.
 - Verify via logs that traffic matching configured filter after schedule time does not get logged under policy with scheduler.
 - Verify via Packet Capture.

Frequency:

- Create a filter to monitor the frequency for a specific TCP source port.

	<ul style="list-style-type: none"> • Apply the configuration to the interface. • Send traffic to match the configured filter on the TOE. • Verify with logs that the frequency of traffic is logged, and that TOE applies the configured reaction. <ul style="list-style-type: none"> • Create a filter to monitor the frequency for a specific TCP destination port. • Apply the configuration to the interface. • Send traffic to match the configured filter on the TOE. • Verify with logs that the frequency of traffic is logged, and that TOE applies the configured reaction. <p>Threshold:</p> <ul style="list-style-type: none"> • Configure the TOE to send trap messages when threshold has been exceeded. • Send traffic to match configured rpm probe with specific UDP source port. • Verify through logs that the TOE sends trap messages when threshold exceeded. • Verify through Packet Capture. <ul style="list-style-type: none"> • Configure the TOE to send trap messages when threshold has been exceeded. • Send traffic to match configured rpm probe with specific UDP destination port. • Verify through logs that the TOE sends trap messages when threshold exceeded. • Verify through Packet Capture.
Expected Test Results	<ul style="list-style-type: none"> • TOE detects and logs traffic matching the baselines or anomaly-based rules for particular attribute. • Packet Capture shows that traffic matching the baselines or anomaly-based rules for particular attribute are treated according to applied policy.
Pass/Fail with Explanation	Pass. TOE applies the configured reaction for anomaly-based rules for each attribute (throughput, time of day, frequency, threshold). This meets the testing requirements.

6.5.6 IPS_ABD_EXT.1 Test #2

Item	Data
Test Assurance Activity	Test 2: Repeat the test assurance activity above to ensure that baselines or anomaly-based rules can be defined for each distinct network interface type supported by the TOE.
Pass/Fail with Explanation	Pass. All distinct network interface types supported by the TOE for attributes Throughput, Time of day, Frequency and threshold have been tested as part of IPS_ABD_EXT.1 Test #1

6.5.7 IPS_IPB_EXT.1 Test #1

Item	Data
Test Assurance Activity	Test 1: The evaluator shall use the instructions in the operational guidance to create a known-bad address list. Using a single IP address, a list of addresses or a range of addresses from that list, the evaluator shall attempt to send traffic through the TOE that would otherwise be allowed by the TOE and observe the TOE automatically drops that traffic
Test Steps	<ul style="list-style-type: none"> • Create a single entry of a known-bad address and an additional entry with a range of known-bad addresses. • Send traffic that matches the configured entries of known-bad addresses and verify connection succeeds. • Apply the entries to the security policy of TOE. • Send traffic that matches the configured entries of known-bad addresses. • Verify through a packet capture and through the TOE’s logs that traffic was appropriately denied.
Expected Test Results	<ul style="list-style-type: none"> • TOE logs confirm that before implementation of known-bad address list, traffic matching the single IP address, a list of addresses or a range of addresses in the address list are permitted by TOE. • Packet Capture shows that before implementation of known-bad address list, traffic matching the single IP address, a list of addresses or a range of addresses in the address list are permitted by TOE. • TOE logs show that traffic matching the single IP address, a list of addresses or a range of addresses in the known-bad address list are dropped by TOE. • Packet Capture shows traffic matching the single IP address, a list of addresses or a range of addresses in the known-bad address list are dropped by TOE.
Pass/Fail with Explanation	Pass. TOE drops traffic matching the configured know bad address list, which would otherwise be allowed. This meets the testing requirements.

6.5.8 IPS_IPB_EXT.1 Test #2

Item	Data
Test Assurance Activity	Test 2: The evaluator shall use the instructions in the operational guidance to create a known-good address list. Using a single IP address, a list of addresses or a range of addresses from that list, the evaluator shall attempt to send traffic that would otherwise be denied by the TOE and observe the TOE automatically allowing traffic
Test Steps	<ul style="list-style-type: none"> • Create a single entry of a known-good address and an additional entry with a range of known-good addresses. • Send traffic that matches the configured entries of known-good addresses and verify connection fails.

	<ul style="list-style-type: none"> • Apply the entries to the security policy of TOE. • Send traffic that matches the configured entries of known-good addresses. • Verify through a log that connection was created. • Verify through Wireshark Capture that Connection succeeds.
Expected Test Results	<ul style="list-style-type: none"> • TOE logs confirm that before implementation of known-good address list onto a policy, traffic matching the single IP address, a list of addresses or a range of addresses in the address list are denied by TOE by default. • Packet Capture shows that before implementation of known-good address list onto a policy, traffic matching the single IP address, a list of addresses or a range of addresses in the address list are denied by TOE by default. • TOE logs show that after implementation of known-good address list onto a policy, traffic matching the single IP address, a list of addresses or a range of addresses in the address list are permitted by TOE. • Packet Capture shows that after implementation of known-good address list onto a policy, traffic matching the single IP address, a list of addresses or a range of addresses in the address list are permitted by TOE.
Pass/Fail with Explanation	Pass. TOE allows traffic matching the configured know good address list, which would otherwise not be allowed. This meets the testing requirements.

6.5.9 IPS_IPB_EXT.1 Test #3

Item	Data
Test Assurance Activity	Test 3: The evaluator shall add conflicting IP addresses to each list and ensure that the TOE handles conflicting traffic in a manner consistent with the precedence in IPS_NTA_EXT.1.1.
Test Steps	<ul style="list-style-type: none"> • Add conflicting IP addresses to the known-bad and known-good lists. • Apply the address book entries to two security policies to deny and accept the same address entries with deny policy being applied first. • Send traffic matching the security policies applied • Verify through a packet Capture and logs that the traffic is denied. • Apply the address book entries to two security policies to deny and accept the same address entries with accept policy being applied first. • Send traffic matching the security policies applied • Verify through a packet Capture and logs that the traffic is accepted.

Expected Test Results	<ul style="list-style-type: none"> • TOE logs show that it handles conflicting traffic according to the order in which rules are applied. • Packet Capture shows that it handles conflicting traffic according to the order in which rules are applied.
Pass/Fail with Explanation	Pass. TOE handles conflicting traffic in an Administrator-defined order. This meets the testing requirements.

6.5.10 IPS_SBD_EXT.1.1 Test #1

Item	Data
Test Assurance Activity	<p>Test 1: The evaluator shall use the instructions in the operational guidance to test that packet header signatures can be created and/or configured with the selected and/or configured reactions specified in IPS_SBD_EXT.1.5 for each of the attributes listed below. Each attribute shall be individually assigned to its own unique signature:</p> <ul style="list-style-type: none"> • IPv4: Version; Header Length; Packet Length; ID; IP Flags; Fragment Offset; Time to Live (TTL); Protocol; Header Checksum; Source Address; Destination Address; and IP Options. • IPv6: Version; traffic class; flow label; payload length; next header; hop limit; source address; destination address; routing header; home address options. • ICMP: Type; Code; Header Checksum; and Rest of Header (varies based on the ICMP type and code). • ICMPv6: Type; Code; and Header Checksum; • TCP: Source port; destination port; sequence number; acknowledgement number; offset; reserved; TCP flags; window; checksum; urgent pointer; and TCP options. • UDP: Source port; destination port; length; and UDP checksum. <p>The evaluator shall generate traffic to trigger a signature and shall then use a packet sniffer to capture traffic that ensures the reactions of each rule are performed as expected.</p>
Test Steps	<p>For each of the attributes:</p> <ul style="list-style-type: none"> • IPv4: Version; Header Length; Packet Length; ID; IP Flags; Fragment Offset; Time to Live (TTL); Protocol; Header Checksum; Source Address; Destination Address; and IP Options. • IPv6: Version; traffic class; flow label; payload length; next header; hop limit; source address; destination address; routing header; home address options. • ICMP: Type; Code; Header Checksum; and Rest of Header (varies based on the ICMP type and code). • ICMPv6: Type; Code; and Header Checksum. • TCP: Source port; destination port; sequence number; acknowledgement number; offset; reserved; TCP flags; window; checksum; urgent pointer; and TCP options. • UDP: Source port; destination port; length; and UDP checksum.

	<ul style="list-style-type: none"> • Configure a filter on the TOE to drop traffic matching the attribute. • Apply the filter to the TOE's security policy. • Modify traffic to match the configured filter on the TOE. • Verify through a packet capture and through logs that the traffic was appropriately dropped.
Expected Test Results	<ul style="list-style-type: none"> • TOE logs traffic matching configured packet header signatures and verifies configured reaction of 'drop' is implemented by TOE. • Packet capture verifies the traffic matching configured packet header signatures are dropped.
Pass/Fail with Explanation	Pass. TOE is triggered with traffic matching configured signatures and reacts in the expected way by dropping the traffic. This meets the testing requirements.

6.5.11 IPS_SBD_EXT.1.1 Test #2

Item	Data
Test Assurance Activity	The evaluator shall repeat the test above to ensure that signature-based IPS policies can be defined for each distinct network interface type capable of applying signatures as supported by the TOE.
Pass/Fail with Explanation	NA. As all distinct network interface types supported by the TOE have been tested as part of IPS_SBD_EXT.1.1 Test #1.

6.5.12 IPS_SBD_EXT.1.2 Test #1

Item	Data
Test Assurance Activity	<p>Test 1: The evaluator shall use the instructions in the operational guidance to test that packet payload string-based detection rules can be assigned to the reactions specified in IPS_SBD_EXT.1.5 using the attributes specified in IPS_SBD_EXT.1.2. However, it is not required (nor is it feasible) to test all possible strings of protocol data, the evaluator shall ensure that a selection of strings in the requirement is selected to be tested. At a minimum at least one string using each of the following attributes from IPS_SBD_EXT.1.2 should be tested for each protocol. The evaluator shall generate packets that match the string in the rule and observe the corresponding reaction is as configured.</p> <ul style="list-style-type: none"> • Test at least one string of characters for ICMPv4 data: beyond the first 4 bytes of the ICMP header. • Test at least one string of characters for ICMPv6 data: beyond the first 4 bytes of the ICMP header. • TCP data (characters beyond the 20 byte TCP header):

	<ul style="list-style-type: none"> ○ Test at least one FTP (file transfer) command: help, noop, stat,syst, user, abort, acct, allo, appe, cdup, cwd, dele, list, mkd, mode, nlst, pass, pasv, port, pass, quit, rein, rest, retr, rmd, rnfr, rnto, site, smnt, stor, stou, stru, and type. ○ HTTP (web) commands and content: <ul style="list-style-type: none"> ▪ Test both GET and POST commands ▪ Test at least one administrator-defined strings to match URLs/URIs, and web page content. ○ Test at least one SMTP (email) state: start state, SMTP commands state, mail header state, mail body state, abort state. ○ Test at least one string in any additional attribute type defined within the “other types of TCP payload inspection” assignment, if any other types are specified. ● Test at least one string of UDP data: characters beyond the first 8 bytes of the UDP header; ● Test at least one string for each additional attribute type defined in the “other types of packet payload inspection” assignment, if any other types are specified.
<p>Test Steps</p>	<ul style="list-style-type: none"> ● Configure the TOE to search for the string SECURITY in an ICMPv4 packet. ● Apply the configuration to the TOE’s security policy. ● Send modified traffic that matches the IDP configuration. ● Verify through a packet capture and logs that the modified traffic was not allowed through the TOE. ● Configure the TOE to search for the string SECURITY in an ICMPv6 packet. ● Apply the configuration to the TOE’s security policy. ● Send modified traffic that matches the IDP configuration. ● Verify through a packet capture and logs that the modified traffic was not allowed through the TOE. ● Configure a filter on the TOE to block the FTP user anonymous. ● Apply the filter to the TOE’s security policy. ● Modify traffic to match the configured filter. ● Verify through a packet capture and through logs that a connection was unsuccessful. ● Configure the TOE to block HTTP GET packets. ● Apply the configuration to the TOE’s security policy. ● Send modified traffic that matches the IDP configuration. ● Verify through a packet capture and logs that the modified traffic was not allowed through the TOE. ● Configure the TOE to block HTTP POST packets. ● Apply the configuration to the TOE’s security policy. ● Send modified traffic that matches the IDP configuration.

	<ul style="list-style-type: none"> • Verify through a packet capture and logs that the modified traffic was not allowed through the TOE. • Configure the TOE to block specific string in URLs. • Apply the configuration to the TOE's security policy. • Send modified traffic that matches the IDP configuration. • Verify through a packet capture and logs that the modified traffic was not allowed through the TOE. • Configure the TOE to block webpage content. • Apply the configuration to the TOE's security policy. • Create a webpage to contain an embedded zip file and attempt to download the zip file. • Verify through a packet capture and logs that attempting to download the zip file was not permitted by the TOE. • Configure the TOE to block any SMTP packets with the mail header "MAIL FROM". • Apply the configuration to the TOE's security policy. • Send modified traffic that matches the IDP configuration. • Verify through a packet capture and logs that the modified traffic was not allowed through the TOE. • Configure the TOE to search for the string SECURITY in an UDP packet. • Apply the configuration to the TOE's security policy. • Send modified traffic that matches the IDP configuration. • Verify through a packet capture and logs that the modified traffic was not allowed through the TOE.
Expected Test Results	<ul style="list-style-type: none"> • TOE logs traffic matching payload string-based rules applied and verifies configured reaction of 'drop' is implemented by TOE. • Packet capture verifies the traffic matching payload string-based rules applied are dropped.
Pass/Fail with Explanation	Pass. The TOE detects when packets contain a specific strings of protocol data and reacts by dropping and logging the offending traffic. This meets the testing requirements.

6.5.13 IPS_SBD_EXT.1.2 Test #2

Item	Data
Test Assurance Activity	The evaluator shall repeat Test 1 above to ensure that signature-based IPS policies can be defined for each distinct network interface type capable of applying signatures as supported by the TOE.
Pass/Fail with Explanation	Pass. All distinct network interface types capable of applying signatures as supported by the TOE have been tested as part of IPS_SBD_EXT.1.2 Test #1.

6.5.14 IPS_SBD_EXT.1.3 Test #1

Item	Data
Test Assurance Activity	<p>The evaluator shall create and/or configure rules for each attack signature in IPS_SBD_EXT.1.3. For each attack, the TOE should apply its corresponding signature and enable it to each distinct network interface type capable of applying the signatures. The evaluator shall use packet captures to ensure that the attack traffic is detected by the TOE and a reaction specified in IPS_SBD_EXT.1.5 is triggered and stops the attack. Each attack should be performed one after another so as to ensure that its corresponding signature successfully identified and appropriately reacted to a particular attack.</p>
Test Steps	<p>IP Attacks</p> <ul style="list-style-type: none"> ○ IP Fragments Overlap (Teardrop attack, Bonk attack, or Boink attack) <ul style="list-style-type: none"> ○ Create a rule to detect when the IP fragments overlap. ○ Apply the signature rule to the security zone to which TOE’s interface is assigned. ○ Send traffic that matches the header-based signature. ○ Verify the attack traffic is detected by the TOE and reacts accordingly. ○ IP source address equal to the IP destination (Land attack) <ul style="list-style-type: none"> ○ Create a rule to detect when the IP source address and destination address are equal. ○ Apply the signature rule to the security zone to which TOE’s interface is assigned. ○ Send traffic that matches the header-based signature. ○ Verify the attack traffic is detected by the TOE and reacts accordingly. <p>ICMP Attacks</p> <ul style="list-style-type: none"> ○ Fragmented ICMP Traffic (e.g. Nuke attack) <ul style="list-style-type: none"> ○ Create a rule to detect ICMP fragmented packets ○ Apply the signature rule to the security zone to which TOE’s interface is assigned. ○ Send traffic that matches the header-based signature. ○ Verify the attack traffic is detected by the TOE and reacts accordingly. ○ Large ICMP Packet (e.g. Ping of Death) <ul style="list-style-type: none"> ○ Create a rule to detect Large ICMP Packets ○ Apply the signature rule to the security zone to which TOE’s interface is assigned. ○ Send traffic that matches the header-based signature. ○ Verify the attack traffic is detected by the TOE and reacts accordingly. <p>TCP Attacks</p> <ul style="list-style-type: none"> ○ TCP NULL Flag <ul style="list-style-type: none"> ○ Create a rule to detect TCP Null flags

	<ul style="list-style-type: none"> ○ Apply the signature rule to the security zone to which TOE's interface is assigned. ○ Send traffic that matches the header-based signature. ○ Verify the attack traffic is detected by the TOE and reacts accordingly. <ul style="list-style-type: none"> ○ TCP FIN+SYN Flag <ul style="list-style-type: none"> ○ Create a rule to detect TCP FIN+SYN flags ○ Apply the signature rule to the security zone to which TOE's interface is assigned. ○ Send traffic that matches the header-based signature. ○ Verify the attack traffic is detected by the TOE and reacts accordingly. <ul style="list-style-type: none"> ○ TCP FIN only Flags <ul style="list-style-type: none"> ○ Create a rule to detect TCP FIN only flags ○ Apply the signature rule to the security zone to which TOE's interface is assigned. ○ Send traffic that matches the header-based signature. ○ Verify the attack traffic is detected by the TOE and reacts accordingly. <ul style="list-style-type: none"> ○ TCP SYN+RST Flag <ul style="list-style-type: none"> ○ Create a rule to detect TCP SYN+RST flags ○ Apply the signature rule to the security zone to which TOE's interface is assigned. ○ Send traffic that matches the header-based signature. ○ Verify the attack traffic is detected by the TOE and reacts accordingly. <p>UDP Attacks</p> <ul style="list-style-type: none"> ○ UDP Bomb Attack <ul style="list-style-type: none"> ○ Create a rule to detect UDP Bomb Attack and apply the signature rule to the security zone to which TOE's interface is assigned ○ Send traffic that matches the header-based signature. ○ Verify the attack traffic is detected by the TOE and reacts accordingly. ○ UDP Chargen DoS Attack <ul style="list-style-type: none"> ○ Create a rule to detect Chargen DoS Attack and apply the signature rule to the security zone to which TOE's interface is assigned ○ Send traffic that matches the header-based signature. ○ Verify the attack traffic is detected by the TOE and reacts accordingly.
Expected Test Results	<ul style="list-style-type: none"> ● TOE logs traffic matching configured head-based signature rules and verifies configured reaction of 'drop' is implemented by TOE.

	<ul style="list-style-type: none"> • Packet capture verifies the traffic matching configured head-based signature rules are dropped.
Pass/Fail with Explanation	Pass. Each attack traffic matching configured signature is detected by the TOE and a reaction specified in IPS_SBD_EXT.1.5 is triggered and stops the attack. This meets the testing requirements.

6.5.15 IPS_SBD_EXT.1.4 Test #1

Item	Data
Test Assurance Activity	The evaluator shall configure individual signatures for each attack in IPS_SBD_EXT.1.4. For each attack, the TOE should apply its corresponding signature and enable it to each distinct network interface type capable of applying signatures. The evaluator shall use packet captures to ensure that the attack traffic is detected by the TOE and a reaction specified in IPS_SBD_EXT.1.5 is triggered and stops the attack. Each attack should be performed one after another so as to ensure that its corresponding signature successfully identified and appropriately reacted to a particular attack.
Test Steps	<p>Flooding a host (DoS Attack)</p> <ul style="list-style-type: none"> • ICMP flooding (Smurf attack, and ping flood) <ul style="list-style-type: none"> ○ Create a rule to detect ICMP Flood attack. ○ Apply the signature rule to the security zone to which TOE's interface is assigned. ○ Send traffic that matches the header-based signature. ○ Verify the attack traffic is detected by the TOE and reacts accordingly. • TCP flooding (e.g. SYN Flood) <ul style="list-style-type: none"> ○ Create a rule to detect TCP SYN Flood attack. ○ Apply the signature rule to the security zone to which TOE's interface is assigned. ○ Send traffic that matches the header-based signature. ○ Verify the attack traffic is detected by the TOE and reacts accordingly. <p>Flooding a network (DoS Attack)</p> <ul style="list-style-type: none"> • Flooding a network (DoS Attack) <ul style="list-style-type: none"> ○ Create a rule to detect Network Flood Attack. ○ Apply the signature rule to the security zone to which TOE's interface is assigned. ○ Send traffic that matches the header-based signature. ○ Verify the attack traffic is detected by the TOE and reacts accordingly. <p>Protocol and Port Scanning</p> <ul style="list-style-type: none"> • IP Protocol Scanning <ul style="list-style-type: none"> ○ Create a rule to detect IP Protocol Scanning.

	<ul style="list-style-type: none"> ○ Apply the signature rule to the security zone to which TOE's interface is assigned. ○ Send traffic that matches the header-based signature. ○ Verify the attack traffic is detected by the TOE and reacts accordingly. <ul style="list-style-type: none"> ● TCP Port Scanning <ul style="list-style-type: none"> ○ Create a rule to detect TCP Port Scanning. ○ Apply the signature rule to the security zone to which TOE's interface is assigned. ○ Send traffic that matches the header-based signature. ○ Verify the attack traffic is detected by the TOE and reacts accordingly. <ul style="list-style-type: none"> ● UDP Port Scanning <ul style="list-style-type: none"> ○ Create a rule to detect UDP Port Scanning. ○ Apply the signature rule to the security zone to which TOE's interface is assigned. ○ Send traffic that matches the header-based signature. ○ Verify the attack traffic is detected by the TOE and reacts accordingly. <ul style="list-style-type: none"> ● ICMP Scanning <ul style="list-style-type: none"> ○ Create a rule to detect ICMP Scanning. ○ Apply the signature rule to the security zone to which TOE's interface is assigned. ○ Send traffic that matches the header-based signature. ○ Verify the attack traffic is detected by the TOE and reacts accordingly.
Expected Test Results	<ul style="list-style-type: none"> ● TOE logs traffic matching configured head-based signature rules and verifies configured reaction of 'drop' is implemented by TOE. ● Packet capture verifies the traffic matching configured head-based signature rules are dropped.
Pass/Fail with Explanation	Pass. The TOE detects when there is attack traffic and reacts by dropping the offending traffic.

6.5.16 IPS_SBD_EXT.1.6 Test #1

Item	Data
Test Assurance Activity	The evaluator shall repeat one of the tests in IPS_SBD_EXT.1.2 Test 1 but generate multiple non-fragmented packets that contain the string in the rule defined. The evaluator shall verify that the malicious traffic is still detected when split across multiple non-fragmented packets.
Test Steps	<ul style="list-style-type: none"> ● Configure a filter on the TOE to search for the string 'security' split across multiple non-fragmented packets. ● Apply the filter to the TOE's security policy.

	<ul style="list-style-type: none"> • Modify SMTP traffic to match the configured filter. • Verify through a packet capture and through logs that the modified traffic was not allowed through the TOE.
Expected Test Results	<ul style="list-style-type: none"> • TOE logs multiple non-fragmented packets matching the applied string-based rule and verifies configured reaction of 'drop' is implemented by TOE. • Packet capture verifies the multiple non-fragmented packets matching the applied string-based rule are dropped.
Pass/Fail with Explanation	Pass. TOE detects malicious traffic when split across multiple non-fragmented packets.

6.6 SSHS

6.6.1 FCS_SSHS_EXT.1.2 Test #1

Item	Data / Description
Test ID	FCS_SSHS_EXT.1.2 Test#1
Objective	<p>Test 1: For each supported client public-key authentication algorithm, the evaluator shall configure a remote client to present a public key corresponding to that authentication method (e.g., 2048-bit RSA key when using ssh-rsa public key). The evaluator shall establish sufficient separate SSH connections with an appropriately configured remote non-TOE SSH client to demonstrate the use of all applicable public key algorithms. It is sufficient to observe the successful completion of the SSH Authentication Protocol to satisfy the intent of this test.</p> <p>TD0631 has been applied.</p>
Test Execution Steps	<ul style="list-style-type: none"> • Generate an ecdsa-sha2-nistp256 public key on the VM. • Copy the public key onto the TOE and verify that it is updated on the TOE. • Login to the TOE using the public key and verify that the session is established. • Verify via logs that the session was established using the configured public key. • Verify via packet capture. <ul style="list-style-type: none"> • Generate an ecdsa-sha2-nistp384 public key on the VM. • Copy the public key onto the TOE and verify that it is updated on the TOE. • Login to the TOE using the public key and verify that the session is established. • Verify via logs that the session was established using the configured public key. • Verify via packet capture. <ul style="list-style-type: none"> • Generate an ecdsa-sha2-nistp521 public key on the VM. • Copy the public key onto the TOE and verify that it is updated on the TOE. • Login to the TOE using the public key and verify that the session is established.

	<ul style="list-style-type: none"> • Verify via logs that the session was established using the configured public key. • Verify via packet capture.
Expected Results	<ul style="list-style-type: none"> • TOE logs shows successful establishment of the SSH connection.
Pass/Fail with Explanation	Pass. The remote client is able to establish a successful SSH connection using each one of the supported public key algorithms.

6.6.2 FCS_SSHS_EXT.1.2 Test #2

Item	Data / Description
Test ID	FCS_SSHS_EXT.1.2 Test#2
Objective	<p>Test 2: The evaluator shall choose one client public key authentication algorithm supported by the TOE. The evaluator shall generate a new client key pair for that supported algorithm without configuring the TOE to recognize the associated public key for authentication. The evaluator shall use an SSH client to attempt to connect to the TOE with the new key pair and demonstrate that authentication fails.</p> <p>TD0631 has been applied.</p>
Test Execution Steps	<ul style="list-style-type: none"> • Generate a new client key pair with ecdsa-sha2-nistp521 on the VM. • Verify the key configured on the TOE. • Login to the device using public key without updating the public key on the TOE and verify that the connection fails. • Verify via audit logs that the connection fails. • Verify via packet capture that the connection fails
Expected Results	<ul style="list-style-type: none"> • TOE logs verify that it denies authentication attempt from a client whose public key does not match the public key associated with it on the TOE.
Pass/Fail with Explanation	Pass. The TOE is not able to establish a connection with a remote SSH client when the TOE is not configured to recognize the associated public key for authentication. This meets the testing requirements.

6.6.3 FCS_SSHS_EXT.1.2 Test #3

Item	Data / Description
Test ID	FCS_SSHS_EXT.1.2 Test#3
Objective	<p>Test 3: [Conditional] If password-based authentication method has been selected in the FCS_SSHS_EXT.1.2, the evaluator shall configure the TOE to accept password-based authentication and demonstrate that user authentication succeeds when the correct password is provided by the connecting SSH client.</p> <p>TD0631 has been applied.</p>
Test Execution Steps	<ul style="list-style-type: none"> • Configure the TOE to ensure that the TOE supports password-based authentication. • Log into the TOE via SSH with password authentication.

	<ul style="list-style-type: none"> • Verify the Audit logs. • Verify Via Packet Capture.
Expected Results	<ul style="list-style-type: none"> • User authentication to TOE using correct password is successful. • TOE logs show successful authentication of user.
Pass/Fail with Explanation	Pass. The TOE is able to establish a connection with a remote SSH user when correct authentication credentials are presented. This meets the testing requirements.

6.6.4 FCS_SSHS_EXT.1.2 Test #4

Item	Data / Description
Test ID	FCS_SSHS_EXT.1.2 Test#4
Objective	<p>Test 4: [Conditional] If password-based authentication method has been selected in the FCS_SSHS_EXT.1.2, the evaluator shall configure the TOE to accept password-based authentication and demonstrate that user authentication fails when the incorrect password is provided by the connecting SSH client.</p> <p>TD0631 has been applied.</p>
Test Execution Steps	<ul style="list-style-type: none"> • Configure SSH on the TOE. • Attempt to Log into the TOE via SSH with password-based authentication and provide incorrect password (This will fail). • Verify authentication logs reflect failures. • Verify the Packet Capture.
Expected Results	<ul style="list-style-type: none"> • User authentication to TOE using incorrect password results in failure. • TOE logs show unsuccessful authentication attempt by user.
Pass/Fail with Explanation	Pass. The TOE is not able to establish a connection with a remote SSH user when incorrect authentication credentials are presented. This meets the testing requirements.

6.6.5 FCS_SSHS_EXT.1.3 Test #1

Item	Data
Test Assurance Activity	The evaluator shall demonstrate that if the TOE receives a packet larger than that specified in this component, that packet is dropped.
Test Steps	<ul style="list-style-type: none"> • Use the acumen-sshs to start an SSH session with the TOE and send bad length packet. • Verify packet capture. • Verify authentication logs reflect failures.
Expected Test Results	<ul style="list-style-type: none"> • TOE logs verify that packet larger than 256 KB is discarded with a 'Bad packet length' error.
Pass/Fail Explanation	The TOE drops large packets that are received within an SSH session. This meets the testing requirements.

Result	Pass.

6.6.6 FCS_SSHS_EXT.1.4 Test #1

Item	Data
Test Assurance Activity	<p>The evaluator must ensure that only claimed ciphers and cryptographic primitives are used to establish an SSH connection.</p> <p>To verify this, the evaluator shall start session establishment for an SSH connection from a remote client (referred to as 'remote endpoint' below). The evaluator shall capture the traffic exchanged between the TOE and the remote endpoint during protocol negotiation (e.g. using a packet capture tool or information provided by the endpoint, respectively). The evaluator shall verify from the captured traffic that the TOE offers all the ciphers defined in the TSS for the TOE for SSH sessions, but no additional ones compared to the definition in the TSS. The evaluator shall perform one successful negotiation of an SSH session to verify that the TOE behaves as expected. It is sufficient to observe the successful negotiation of the session to satisfy the intent of the test.</p> <p>If the evaluator detects that not all ciphers defined in the TSS for SSH are supported by the TOE and/or the TOE supports one or more additional ciphers not defined in the TSS for SSH, the test shall be regarded as failed.</p>
Test Steps	<ul style="list-style-type: none"> • Configure the TOE to support AES-128-cbc for encryption algorithm. • Connect to the TOE using AES128-cbc. • Verify successful establishment of connection via audit log. • Verify AES-128-cbc was used via packet capture. • Verify that the TOE only supports all algorithms as mentioned in the ST (aes-128-cbc, aes-256-cbc, aes-128-ctr, aes-256-ctr) via packet capture. • Configure the TOE to support AES-256-cbc for encryption algorithm. • Connect to the TOE using AES256-cbc. • Verify successful establishment of connection via audit log. • Verify AES-256-cbc was used via packet capture. • Configure the TOE to support AES-128-ctr for encryption algorithm • Connect to the TOE using AES128-ctr. • Verify that the SSH session was encrypted using AES-128-ctr via packet capture. • Verify successful establishment of connection via audit log. • Configure the TOE to support AES-256-ctr for encryption algorithm • Connect to the TOE using AES256-ctr. • Verify that the SSH session was encrypted using AES-256-ctr via packet capture. • Verify successful establishment of connection via audit log.
Expected Test Results	<ul style="list-style-type: none"> • Packet Capture shows TOE establishing successful connection with supported cipher. • Packet Capture shows TOE offering only supported ciphers as defined in the TSS.

Pass/Fail Explanation	The TOE supports successful negotiations when using the claimed cipher suites.
Result	Pass.

6.6.7 FCS_SSHS_EXT.1.5 Test #1

Item	Data / Description
Test ID	FCS_SSHS_EXT.1.5 Test#1
Objective	<p>Test 1: The evaluator shall configure (only if required by the TOE) the TOE to use each of the claimed host public key algorithms. The evaluator will then use an SSH client to confirm that the client can authenticate the TOE server public key using the claimed algorithm. It is sufficient to observe (on the wire) the successful negotiation of the algorithm to satisfy the intent of the test.</p> <p>TD0631 has been applied.</p>
Test Execution Steps	<ul style="list-style-type: none"> • Configure the TOE to use the claimed host public key algorithms. • Generate an ecdsa-sha2-nistp256 host key pair on the TOE. • Login to the TOE using the host public key and verify that the session is established. • Verify via logs that the session was established. • Verify via packet capture that the configured host key algorithm was used. • Generate an ecdsa-sha2-nistp384 host key pair on the TOE. • Login to the TOE using the host public key and verify that the session is established. • Verify via logs that the session was established. • Verify via packet capture that the configured host key algorithm was used. • Generate an ecdsa-sha2-nistp521 host key pair on the TOE. • Login to the TOE using the host public key and verify that the session is established. • Verify via logs that the session was established. • Verify via packet capture that the configured host key algorithm was used.
Expected Results	<ul style="list-style-type: none"> • TOE logs shows successful establishment of the SSH connection. • Packet capture shows session establishment with the configured host key algorithm.
Pass/Fail with Explanation	Pass. The remote client is able to establish a successful SSH connection using each one of the claimed host public key algorithms.

6.6.8 FCS_SSHS_EXT.1.5 Test #2

Item	Data / Description
Test ID	FCS_SSHS_EXT.1.5 Test#2

Objective	<p>Test 2: The evaluator shall configure a non-TOE SSH client to only allow it to authenticate an SSH server host public key algorithm that is not included in the ST selection. The evaluator shall attempt to establish an SSH connection from the non-TOE SSH client to the TOE SSH server and observe that the connection is rejected.</p> <p>TD0631 has been applied.</p>
Test Execution Steps	<ul style="list-style-type: none"> • Configure the TOE to reject SSH sessions using the unsupported ssh-rsa algorithm. • Attempt to establish an SSH session using the ssh-rsa host public key algorithm. • Verify that the connection is refused via packet capture. • Verify that the SSH session was refused using ssh-rsa via log.
Expected Results	<ul style="list-style-type: none"> • TOE logs verify connection establishment using unsupported public key algorithm(ssh-rsa) is denied by TOE. • Packet Capture verifies connection establishment using unsupported public key algorithm(ssh-rsa) is denied by TOE.
Pass/Fail with Explanation	Pass. The remote client is able to establish a successful SSH connection using each one of the claimed host public key algorithms.

6.6.9 FCS_SSHS_EXT.1.6 Test #1

Item	Data
Test Assurance Activity	<p>Test 1: [conditional, if an HMAC or AEAD_AES*_GCM algorithm is selected in the ST] The evaluator shall establish an SSH connection using each of the algorithms, except “implicit”, specified by the requirement. It is sufficient to observe (on the wire) the successful negotiation of the algorithm to satisfy the intent of the test.</p> <p>Note: To ensure the observed algorithm is used, the evaluator shall ensure a non-aes*-gcm@openssh.com encryption algorithm is negotiated while performing this test.</p>
Test Steps	<ul style="list-style-type: none"> • Configure the TOE to support HMAC-SHA1 for hashing algorithm. • Establish an SSH session with the configured supported algorithms (HMAC-SHA1). • Verify that the SSH session was encrypted using HMAC-SHA1 via capture. • Verify successful establishment of connection via log. • Configure the TOE to support HMAC-SHA2-256 for hashing algorithm. • Establish an SSH session with the configured supported algorithms (HMAC-SHA2-256). • Verify that the SSH session was encrypted using HMAC-SHA2-256 via capture. • Verify successful establishment of connection via log. • Configure the TOE to support HMAC-SHA2-512 for hashing algorithm. • Establish an SSH session with the configured supported algorithms (HMAC-SHA2-512). • Verify that the SSH session was encrypted using HMAC-SHA2-512 via capture. • Verify successful establishment of connection via log.
Expected Test Results	<ul style="list-style-type: none"> • Packet Capture Verifies that TOE supports only the MAC algorithms as mentioned in the ST.

Pass/Fail Explanation	The TOE is able to make SSH connections with each claimed data integrity algorithm. This meets the testing requirements.
Result	Pass.

6.6.10 FCS_SSHS_EXT.1.6 Test #2

Item	Data
Test Assurance Activity	<p>Test 2: [conditional, if an HMAC or AEAD_AES_*_GCM algorithm is selected in the ST] The evaluator shall configure an SSH client to only allow a MAC algorithm that is not included in the ST selection. The evaluator shall attempt to connect from the SSH client to the TOE and observe that the attempt fails.</p> <p>Note: To ensure the proposed MAC algorithm is used, the evaluator shall ensure a non-aes*-gcm@openssh.com encryption algorithm is negotiated while performing this test.</p>
Test Steps	<ul style="list-style-type: none"> Attempt to establish an SSH session using hmac-md5 mac. Verify via logs that the session fails due to unsupported mac algorithm. Verify via packet capture that the TOE does not continue negotiation.
Expected Test Results	<ul style="list-style-type: none"> TOE logs show unsuccessful negotiation with unsupported MAC algorithm(hmac-md5). Packet Capture shows unsuccessful negotiation with unsupported MAC algorithm(hmac-md5).
Pass/Fail Explanation	The TOE rejects SSH connections using the “hmac-md5” MAC for data integrity. This meets the testing requirements.
Result	Pass.

6.6.11 FCS_SSHS_EXT.1.7 Test #1

Item	Data
Test Assurance Activity	The evaluator shall configure an SSH client to only allow the diffie-hellman-group1-sha1 key exchange. The evaluator shall attempt to connect from the SSH client to the TOE and observe that the attempt fails.
Test Steps	<ul style="list-style-type: none"> Attempt to establish an SSH session using diffiehellman-group1-sha1. Verify that the SSH session was refused via logs. Verify the connection is refused via packet capture.
Expected Test Results	<ul style="list-style-type: none"> TOE logs show unsuccessful negotiation with diffiehellman-group1-sha1 key exchange. Packet Capture shows unsuccessful negotiation with diffiehellman-group1-sha1 key exchange.
Pass/Fail Explanation	The TOE rejects SSH connections using diffiehellman-group1-sha1 (a non-approved algorithm) for key exchange. This meets the testing requirements.

Result	Pass.

6.6.12 FCS_SSHS_EXT.1.7 Test #2

Item	Data
Test Assurance Activity	For each allowed key exchange method, the evaluator shall configure an SSH client to only allow that method for key exchange, attempt to connect from the client to the TOE, and observe that the attempt succeeds.
Test Steps	<ul style="list-style-type: none"> • Establish an SSH session with the configured supported key exchange algorithm (Diffie-hellman-group14-sha1). • Verify that the session is established via logs. • Verify that the SSH session was encrypted using Diffie-hellman-group14-sha1 via capture. • Establish an SSH session with the configured supported key exchange algorithm (ecdh-sha2-nistp256). • Verify that the session is established via logs. • Verify that the SSH session was encrypted using ecdh-sha2-nistp256 via capture. • Establish an SSH session with the configured supported key exchange algorithm (ecdh-sha2-nistp384). • Verify that the session is established via logs. • Verify that the SSH session was encrypted using ecdh-sha2-nistp384 via capture. • Establish an SSH session with the configured supported key exchange algorithm (ecdh-sha2-nistp521). • Verify that the session is established via logs. • Verify that the SSH session was encrypted using ecdh-sha2-nistp521 via capture.
Expected Test Results	<ul style="list-style-type: none"> • TOE logs show successful negotiation with supported (diffiehellman-group14-sha1) key exchange. • Packet Capture shows successful negotiation with supported (diffiehellman-group14-sha1) key exchange.
Pass/Fail Explanation	The TOE is able to make SSH connections with each claimed data key exchange method. This meets the testing requirements.
Result	Pass.

6.6.13 FCS_SSHS_EXT.1.8 Test #1t

Item	Data
Test Assurance Activity	<p>The evaluator needs to perform testing that rekeying is performed according to the description in the TSS. The evaluator shall test both, the time-based threshold and the traffic-based threshold.</p> <p>For testing of the time-based threshold, the evaluator shall use an SSH client to connect to the TOE and keep the session open until the threshold is reached. The evaluator shall verify that the SSH session has been active longer than the threshold value and shall verify that the TOE initiated a rekey (the method of verification shall be reported by the evaluator).</p> <p>Testing does not necessarily have to be performed with the threshold configured at the maximum allowed value of one hour of session time but the value used for testing shall not exceed one hour. The evaluator needs to ensure that the rekeying has been initiated by the TOE and not by the SSH client that is connected to the TOE.</p> <p>If one or more thresholds that are checked by the TOE to fulfil the SFR are configurable, the evaluator needs to verify that the threshold(s) can be configured as described in the guidance documentation and the evaluator needs to test that modification of the thresholds is restricted to Security Administrators (as required by FMT_MOF.1/Functions).</p>
Test Steps	<ul style="list-style-type: none"> • Login to the TOE and configure a rekey for 10 Minutes. • Send a continuous ping and verify that a rekey generates every 10 Minutes. • Verify the login time for rekey. • Verify rekey via audit logs.
Expected Test Results	<ul style="list-style-type: none"> • TOE log verifies rekeying is initiated after 10 minutes .
Pass/Fail Explanation	The TOE initiates a rekey every 10 Minutes. This meets the testing requirements.
Result	Pass.

6.6.14 FCS_SSHS_EXT.1.8 Test #1b

Item	Data
Test Assurance Activity	<p>The evaluator needs to perform testing that rekeying is performed according to the description in the TSS. The evaluator shall test both, the time-based threshold and the traffic-based threshold.</p> <p>For testing of the traffic-based threshold the evaluator shall use the TOE to connect to an SSH client and shall transmit data to and/or receive data from the TOE within the active SSH session until the threshold for data protected by either encryption key is reached. It is acceptable if the rekey occurs before the threshold is reached (e.g. because the traffic is counted according to one of the alternatives given in the Application Note for FCS_SSHS_EXT.1.8).</p>

	<p>The evaluator shall verify that more data has been transmitted within the SSH session than the threshold allows and shall verify that the TOE initiated a rekey (the method of verification shall be reported by the evaluator).</p> <p>Testing does not necessarily have to be performed with the threshold configured at the maximum allowed value of one gigabyte of transferred traffic but the value used for testing shall not exceed one gigabyte. The evaluator needs to ensure that the rekeying has been initiated by the TOE and not by the SSH client that is connected to the TOE.</p> <p>If one or more thresholds that are checked by the TOE to fulfil the SFR are configurable, the evaluator needs to verify that the threshold(s) can be configured as described in the guidance documentation and the evaluator needs to test that modification of the thresholds is restricted to Security Administrators (as required by FMT_MOF.1/Functions).</p> <p>In cases where data transfer threshold could not be reached due to hardware limitations it is acceptable to omit testing of this (SSH rekeying based on data transfer threshold) threshold if both the following conditions are met:</p> <ol style="list-style-type: none"> 1. An argument is present in the TSS section describing this hardware- based limitation and 2. All hardware components that are the basis of such argument are definitively identified in the ST. For example, if specific Ethernet Controller or WiFi radio chip is the root cause of such limitation, these chips must be identified.
Test Steps	<ul style="list-style-type: none"> • Configure the volume limit for rekeying on TOE. • Copy the file from Source to other TOE which is above 1GB in size to occur rekey. • Verify via logs that a rekey is generated in every 1GB of data.
Expected Test Results	<ul style="list-style-type: none"> • TOE log verifies rekeying is initiated after 1GB of data transfer.
Pass/Fail Explanation	The TOE initiates a rekey in every 1GB of data. This meets the testing requirements.
Result	Pass.

6.7 Update

6.7.1 FPT_TST_EXT.1 Test #1

Item	Data
Test Assurance Activity	<p>It is expected that at least the following tests are performed:</p> <ol style="list-style-type: none"> a) Verification of the integrity of the firmware and executable software of the TOE

	<p>b) Verification of the correct operation of the cryptographic functions necessary to fulfil any of the SFRs.</p> <p>The evaluator shall either verify that the self-tests described above are carried out during initial start-up or that the developer has justified any deviation from this.</p> <p>For distributed TOEs the evaluator shall perform testing of self-tests on all TOE components according to the description in the TSS about which self-test are performed by which component.</p>
Test Steps	<ul style="list-style-type: none"> • Reset or boot the TOE. • Observe boot processes for integrity testing and self-tests.
Expected Test Results	<ul style="list-style-type: none"> • TOE logs verify integrity check of executable software during reboot. • TOE logs show verification of correct operation of cryptographic functions as mentioned in SFRs during reboot.
Pass/Fail with Explanation	Pass. The TOE performs all claimed self-tests. This meets the testing requirements.

6.7.2 FPT_TUD_EXT.1 Test #1

Item	Data
Test Assurance Activity	<p>The evaluator performs the version verification activity to determine the current version of the product as well as the most recently installed version (should be the same version before updating).</p> <p>The evaluator obtains a legitimate update using procedures described in the guidance documentation and verifies that it is successfully installed on the TOE.</p> <p>(For some TOEs loading the update onto the TOE and activation of the update are separate steps ('activation' could be performed e.g. by a distinct activation step or by rebooting the device). In that case the evaluator verifies after loading the update onto the TOE but before activation of the update that the current version of the product did not change but the most recently installed version has changed to the new product version.)</p> <p>After the update, the evaluator performs the version verification activity again to verify the version correctly corresponds to that of the update and that current version of the product and most recently installed version match again.</p>
Test Steps	<ul style="list-style-type: none"> • Copy update file to the TOE. • Verify the current version of the TOE. • Compute the file hash and verify that it matches the published hash before proceeding with the update. • Attempt to install a legitimate update. • Verify the new version of the TOE.
Expected Test Results	<ul style="list-style-type: none"> • Verify that TOE gets upgraded to the new version.

Pass/Fail with Explanation	Pass. The TOE can be successfully updated.
-----------------------------------	--------------------------------------------

6.7.3 FPT_TUD_EXT.1 Test #2 (a)

Item	Data
Test Assurance Activity	<p>Test 2 [conditional]: If the TOE itself verifies a digital signature to authorize the installation of an image to update the TOE the following test shall be performed (otherwise the test shall be omitted).</p> <p>The evaluator first confirms that no updates are pending and then performs the version verification activity to determine the current version of the product, verifying that it is different from the version claimed in the update(s) to be used in this test. The evaluator obtains or produces illegitimate updates as defined below, and attempts to install them on the TOE. The evaluator verifies that the TOE rejects all of the illegitimate updates. The evaluator performs this test using all of the following forms of illegitimate updates:</p> <p>1) A modified version (e.g. using a hex editor) of a legitimately signed update</p> <p>If the TOE allows a delayed activation of updates the TOE must be able to display both the currently executing version and most recently installed version. The handling of version information of the most recently installed version might differ between different TOEs depending on the point in time when an attempted update is rejected. The evaluator shall verify that the TOE handles the most recently installed version information for that case as described in the guidance documentation. After the TOE has rejected the update the evaluator shall verify, that both, current version and most recently installed version, reflect the same version information as prior to the update attempt.</p>
Test Steps	<ul style="list-style-type: none"> • Verify the current version of the TOE. • Attempt to install a modified version of a legitimate update. • Verify the TOE rejects the update.
Expected Test Results	<ul style="list-style-type: none"> • TOE logs verify that an installation of a modified version of image is rejected by it.
Pass/Fail with Explanation	Pass. The TOE software was able to detect when an image was corrupted and rejected the image. This meets the testing requirements.

6.7.4 FPT_TUD_EXT.1 Test #2 (b)

Item	Data
Test Assurance Activity	<p>[conditional]: If the TOE itself verifies a digital signature to authorize the installation of an image to update the TOE the following test shall be performed (otherwise the test shall be omitted).</p> <p>The evaluator first confirms that no updates are pending and then performs the version verification activity to determine the current version of the product, verifying that it is different from the version claimed in the update(s) to be used in this test. The evaluator obtains or</p>

	<p>produces illegitimate updates as defined below, and attempts to install them on the TOE. The evaluator verifies that the TOE rejects all of the illegitimate updates. The evaluator performs this test using all of the following forms of illegitimate updates:</p> <p>2) An image that has not been signed</p> <p>If the TOE allows a delayed activation of updates the TOE must be able to display both the currently executing version and most recently installed version. The handling of version information of the most recently installed version might differ between different TOEs depending on the point in time when an attempted update is rejected. The evaluator shall verify that the TOE handles the most recently installed version information for that case as described in the guidance documentation. After the TOE has rejected the update the evaluator shall verify, that both, current version and most recently installed version, reflect the same version information as prior to the update attempt.</p>
Test Steps	<ul style="list-style-type: none"> • Verify the current version of the TOE. • Remove the signature from the image. • Attempt to install the update without a signature. • Verify the TOE rejects the update.
Expected Test Results	<ul style="list-style-type: none"> • TOE logs verify that an installation of a modified image without a signature is rejected by it.
Pass/Fail with Explanation	<p>Pass. The TOE software was able to detect when an image was not signed and rejected the image. This meets the testing requirements.</p>

6.7.5 FPT_TUD_EXT.1 Test #2 (c)

Item	Data
Test Assurance Activity	<p>[conditional]: If the TOE itself verifies a digital signature to authorize the installation of an image to update the TOE the following test shall be performed (otherwise the test shall be omitted).</p> <p>The evaluator first confirms that no updates are pending and then performs the version verification activity to determine the current version of the product, verifying that it is different from the version claimed in the update(s) to be used in this test. The evaluator obtains or produces illegitimate updates as defined below, and attempts to install them on the TOE. The evaluator verifies that the TOE rejects all of the illegitimate updates. The evaluator performs this test using all of the following forms of illegitimate updates:</p> <p>3) An image signed with an invalid signature (e.g. by using a different key as expected for creating the signature or by manual modification of a legitimate signature)</p> <p>If the TOE allows a delayed activation of updates the TOE must be able to display both the currently executing version and most recently installed version. The handling of version information of the most recently installed version might differ between different TOEs depending on the point in time when an attempted update is rejected. The evaluator shall verify that the TOE handles the most recently installed version information for that case as described in the guidance documentation. After the TOE has rejected the update the evaluator</p>

	shall verify, that both, current version and most recently installed version, reflect the same version information as prior to the update attempt.
Test Steps	<ul style="list-style-type: none"> • Verify the current version of the TOE. • Modify the signature of the update. • Attempt to install an update with a corrupt signature. • Verify the TOE rejects the update.
Expected Test Results	<ul style="list-style-type: none"> • TOE logs verify that an installation of a modified image with a corrupt signature is rejected by it.
Pass/Fail with Explanation	Pass. The TOE software was able to detect when an image had an invalid signature and rejected the image. This meets the testing requirements.

6.8 VPN

6.8.1 FIA_PSK_EXT.1 Test #1

Item	Data
Test Assurance Activity	For each mechanism selected in FIA_PSK_EXT.1.2 the evaluator shall attempt to establish a connection and confirm that the connection requires the selected factors in the PSK to establish the connection.
Test Steps	<ul style="list-style-type: none"> • Configure the TOE with bit-based pre-shared key. • Verify that a successful protocol negotiation can be performed with an externally generated bit-based pre-shared key. • Verify successful connection with packet capture.
Expected Test Results	<ul style="list-style-type: none"> • TOE has successful connection establishment with peer using the externally generated pre-shared key. • Packet Capture shows connection establishment with flow of ESP packets.
Pass/Fail with Explanation	Pass. The TOE can establish a connection using an externally generated bit-based pre-shared key and the same is verified using packet capture.

6.8.2 FAU_GEN.1/VPN Test #1

Item	Data
Test Assurance Activity	The evaluator shall test the audit functionality by performing actions that trigger each of the claimed audit events and verifying that the audit records are accurate and that their format is consistent with what is specified in the operational guidance. The evaluator may generate these audit events as a consequence of performing other tests that would cause these events to be generated.
Test Steps	Covered by audit records in each test case.
Pass/Fail with Explanation	Pass. Covered by audit records in test cases of VPN_Filter module and IPsec Module.

6.8.3 FMT_SMF.1/VPN Test #1

Item	Data								
Test Assurance Activity	The evaluator tests management functions as part of performing other test EAs. No separate testing for FMT_SMF.1/VPN is required unless one of the management functions in FMT_SMF.1.1/VPN has not already been exercised under any other SFR.								
Test Steps	The TSF shall be capable of performing the following management functions [<ul style="list-style-type: none"> • Definition of packet filtering rules • Association of packet filtering rules to network interfaces • Ordering of packet filtering rules by priority 								
Test Output	<p>Note: the following output is carried from FMT_SMF.1 Test#1 from Auth Module.</p> <p>This test is completed throughout the process of testing the following SFRs:</p> <table border="1" style="width: 100%;"> <thead> <tr> <th>Management Functions</th> <th>Test cases</th> </tr> </thead> <tbody> <tr> <td>Definition of packet filtering rules</td> <td>FPF_RUL_EXT.1</td> </tr> <tr> <td>Association of packet filtering rules to network interfaces</td> <td>FFW_RUL_EXT.1</td> </tr> <tr> <td>Ordering of packet filtering rules by priority</td> <td>FPF_RUL_EXT.1.6</td> </tr> </tbody> </table>	Management Functions	Test cases	Definition of packet filtering rules	FPF_RUL_EXT.1	Association of packet filtering rules to network interfaces	FFW_RUL_EXT.1	Ordering of packet filtering rules by priority	FPF_RUL_EXT.1.6
Management Functions	Test cases								
Definition of packet filtering rules	FPF_RUL_EXT.1								
Association of packet filtering rules to network interfaces	FFW_RUL_EXT.1								
Ordering of packet filtering rules by priority	FPF_RUL_EXT.1.6								
Pass/Fail with Explanation	Pass. All management functions identified have been tested throughout the evaluation. Thus, this requirement has been met.								

6.8.4 FPF_RUL_EXT.1.1 Test #1

Item	Data
Test Assurance Activity	Test 1: The evaluator shall attempt to get network traffic to flow through the TOE while the TOE is being initialized. A steady flow of network packets that would otherwise be denied by the ruleset should be sourced and directed to a host. The evaluator shall use a packet sniffer to verify none of the generated network traffic is permitted through the TOE during initialization.
Test Steps	<ul style="list-style-type: none"> • Configure a filter to drop traffic from a specific source address. • Apply the filter to the TOE’s Interface. • Send continual traffic from the chosen source address and verify that it is denied. • Reboot the TOE when ping is in progress. • Verify with logs that all traffic from chosen source address was denied. • Verify with Packet Capture that all traffic from chosen source address was denied during reboot.
Expected Test Results	Packet Capture shows that denied traffic is not permitted through the TOE even during TOE initialization.
Pass/Fail with Explanation	Pass. Packets that would otherwise be denied by the ruleset are not permitted through the TOE during initialization. This meets the testing requirements.

6.8.5 FPF_RUL_EXT.1.1 Test #2

Item	Data
Test Assurance Activity	Test 2: The evaluator shall attempt to get network traffic to flow through the TOE while the TOE is being initialized. A steady flow of network packets that would be permitted by the ruleset should be sourced and directed to a host. The evaluator shall use a packet sniffer to verify none of the generated network traffic is permitted through the TOE during initialization and is only permitted once initialization is complete.
Test Steps	<ul style="list-style-type: none"> • Configure a filter to accept traffic with a specific source address. • Apply the filter to the TOE’s Interface. • Send continual traffic from the specific source address and verify it is accepted. • Reboot the TOE when ping is in progress. • Verify through the firewall log that traffic from specific source address is allowed after the reboot. • Verify through a packet capture that all traffic is denied when the TOE is performing a reboot but once the TOE is operational all traffic from the specific source address is allowed.
Expected Test Results	<ul style="list-style-type: none"> • Packet capture confirms no traffic is permitted through TOE during initialization. • Packet capture confirms packets permitted by ruleset passing through TOE after initialization.
Pass/Fail with Explanation	Pass. Packets that would otherwise be allowed by the ruleset are not permitted through the firewall during initialization. This meets the testing requirements.

6.8.6 FPF_RUL_EXT.1.4 Test #1

Item	Data
Test Assurance Activity	<p>Test 1: The evaluator shall use the instructions in the operational guidance to test that packet filter rules can be created that permit, discard, and log packets for each of the following attributes:</p> <ul style="list-style-type: none"> ○ IPv4 <ul style="list-style-type: none"> ▪ Destination Address ▪ Protocol ○ IPv6 <ul style="list-style-type: none"> ▪ Source address ▪ Destination Address ▪ Next Header (Protocol) ○ TCP <ul style="list-style-type: none"> ▪ Source Port ▪ Destination Port ○ UDP <ul style="list-style-type: none"> ▪ Source Port

	<ul style="list-style-type: none"> ▪ Destination Port <p>Note that these test activities should be performed in conjunction with those of FPF_RUL_EXT.1.6 where the effectiveness of the rules is tested; here the evaluator is just ensuring the guidance is sufficient and the TOE supports the administrator creating a ruleset based on the above attributes. The test activities for FPF_RUL_EXT.1.6 define the combinations of protocols and attributes required to be tested. If those combinations are configured manually, that will fulfill the objective of these test activities, but if those combinations are configured otherwise (e.g., using automation), these test activities may be necessary in order to ensure the guidance is correct and the full range of configurations can be achieved by a TOE administrator.</p>
Pass/Fail with Explanation	Pass. This test has been tested in conjunction with Firewall module [FFW_RUL_EXT.1.2/FFW_RUL_EXT.1.3/ FFW_RUL_EXT.1.4 Test#1].

6.8.7 FPF_RUL_EXT.1.4 Test #2

Item	Data
Test Assurance Activity	<p>Test 2: The evaluator shall repeat Test 1 above for each distinct network interface type supported by the TOE to ensure that packet filtering rules can be defined for all supported types.</p> <p>Note that these test activities should be performed in conjunction with those of FPF_RUL_EXT.1.6 where the effectiveness of the rules is tested; here the evaluator is just ensuring the guidance is sufficient and the TOE supports the administrator creating a ruleset based on the above attributes. The test activities for FPF_RUL_EXT.1.6 define the combinations of protocols and attributes required to be tested. If those combinations are configured manually, that will fulfill the objective of these test activities, but if those combinations are configured otherwise (e.g., using automation), these test activities may be necessary in order to ensure the guidance is correct and the full range of configurations can be achieved by a TOE administrator.</p>
Pass/Fail with Explanation	Pass. This test has been tested in conjunction with Firewall module [FFW_RUL_EXT.1.2/FFW_RUL_EXT.1.3/ FFW_RUL_EXT.1.4 Test#2].

6.8.8 FPF_RUL_EXT.1.5 Test #1

Item	Data
Test Assurance Activity	Test 1: The evaluator shall devise two equal packet filtering rules with alternate operations – permit and discard. The rules should then be deployed in two distinct orders and in each case the evaluator shall ensure that the first rule is enforced in both cases by generating applicable packets and using packet capture and logs for confirmation
Test Steps	<ul style="list-style-type: none"> • Configure a filter to allow and drop packets that have the same destination-address with the allow rule being first. • Apply the filter to the TOE Interface.


	<ul style="list-style-type: none"> • Send traffic to configured destination address in filter. • Verify through the firewall log that traffic is allowed. • Verify allowed traffic via packet capture. <ul style="list-style-type: none"> • Configure a filter to drop and allow packets that have the same destination-address with the drop rule being first. • Apply the filter to the TOE Interface. • Send traffic to configured destination address in filter. • Verify through the firewall log that traffic is discarded. • Verify via packet capture discarded traffic.
Expected Test Results	<ul style="list-style-type: none"> • TOE logs show that traffic matching configured destination-address gets permitted when allow rule is first in the conflicting ruleset. • Packet Capture shows that traffic matching configured destination-address gets permitted when allow rule is first in the conflicting ruleset. • TOE logs show that traffic matching configured destination-address gets dropped when drop rule is first in the conflicting ruleset. • Packet Capture shows that traffic matching configured destination-address gets dropped when drop rule is first in the conflicting ruleset.
Pass/Fail with Explanation	Pass. TOE enforces the first rule in the firewall filter. This meets the testing requirement.

6.8.9 FPF_RUL_EXT.1.5 Test #2

Item	Data
Test Assurance Activity	Test 2: The evaluator shall repeat the procedure above, except that the two rules should be devised where one is a subset of the other (e.g. a specific address vs. a network segment). Again, the evaluator should test both orders to ensure that the first is enforced regardless of the specificity of the rule.
Test Steps	<ul style="list-style-type: none"> • Configure the firewall rule order to allow packets to a specific destination-address and deny packets to its network segment. • Apply the filter to the TOE Interface. • Send traffic to configured specific destination and network segment addresses. • Verify through the firewall logs that only traffic to specific destination address are allowed and remaining addresses to network segment are discarded. • Verify the rules applied through Packet Capture. <ul style="list-style-type: none"> • Configure the firewall rule order to deny packets to a network segment and allow packets to a specific destination-address of the network segment. • Apply the filter to the TOE Interface


	<ul style="list-style-type: none"> • Send traffic to configured specific destination and network segment addresses. • Verify through the firewall logs that all traffic is dropped. • Verify the rules applied through Packet Capture.
Expected Test Results	<ul style="list-style-type: none"> • TOE firewall logs show that only traffic matching configured specific destination address is permitted when filter ruleset allows packets to a specific destination-address and denies packets to its network segment. • Packet Capture shows that only traffic matching configured specific destination address is permitted when filter ruleset allows packets to a specific destination-address and denies packets to its network segment. • TOE firewall logs show that all traffic matching configured network destination address is denied when filter ruleset denies packets to a network segment and allows packets to a specific destination-address of the network segment. • Packet Capture shows that all traffic matching configured network destination address is denied when filter ruleset denies packets to a network segment and allows packets to a specific destination-address of the network segment.
Pass/Fail with Explanation	Pass. TOE enforces the first rule regardless of the specificity of the rule. This meets the testing requirements.

6.8.10 FPF_RUL_EXT.1.6 Test #1

Item	Data
Test Assurance Activity	<p>Test 1: The evaluator shall configure the TOE to permit and log each supported IPv4 Transport Layer Protocol (see RFC Values for IPv4 and IPv6 table for full possible list) in conjunction with a specific source address and specific destination address, specific source address and wildcard destination address, wildcard source address and specific destination address, and wildcard source address and wildcard destination address. The evaluator shall generate packets matching each supported IPv4 Transport Layer Protocol and within the configured source and destination addresses in order to ensure that the supported protocols are permitted (i.e., by capturing the packets after passing through the TOE) and logged. Any protocols not supported by the TOE must be denied.</p> <p>The following table identifies the RFC defined values for the protocol fields for IPv4 and IPv6 to be used in configuring and otherwise testing packet filtering rule definition and enforcement:</p> <div style="text-align: center;">  <p>IP Transport layer protocols.xlsx</p> </div>
Test Steps	<ul style="list-style-type: none"> • Configure TOE for all combinations of specific source address and specific destination address, specific source address and wildcard destination address, wildcard source


	<p>address and specific destination address, and wildcard source address and wildcard destination address for Allow condition.</p> <ul style="list-style-type: none"> • Configure Test Machine to send traffic with selected source and destination IPs. • Send Traffic with all combination to check traffic is allowed. • Verify with TOE logs that all combinations are allowed via TOE. • Verify with Packet capture.
Expected Test Results	<ul style="list-style-type: none"> • TOE logs show that each defined IPv4 Transport Layer Protocol matching the configured source and destination addresses are permitted through TOE. • Packet Capture shows that each defined IPv4 Transport Layer Protocol matching the configured source and destination addresses are permitted through TOE.
Pass/Fail with Explanation	<p>Pass. The TOE permits and logs packets with combinations of specific source address and specific destination address, specific source address and wildcard destination address, wildcard source address and specific destination address, and wildcard source address and wildcard destination address as configured on TOE for each defined IPV4 Transport Layer Protocol. This meets testing requirements.</p>

6.8.11 FPF_RUL_EXT.1.6 Test #2

Item	Data
Test Assurance Activity	<p>Test 2: The evaluator shall configure the TOE to permit all traffic except to discard and log each supported IPv4 Transport Layer Protocol (see RFC Values for IPv4 and IPv6 table for full possible list) in conjunction with a specific source address and specific destination address, specific source address and wildcard destination address, wildcard source address and specific destination address, and wildcard source address and wildcard destination address. The evaluator shall generate packets matching each defined IPv4 Transport Layer Protocol and within the configured source and destination addresses in order to ensure that the supported protocols are denied (i.e., by capturing no applicable packets passing through the TOE) and logged. Any protocols not supported by the TOE must also be denied but are not required to be logged.</p> <p>The following table identifies the RFC defined values for the protocol fields for IPv4 and IPv6 to be used in configuring and otherwise testing packet filtering rule definition and enforcement:</p> <p> IP Transport layer protocols.xlsx</p>
Test Steps	<ul style="list-style-type: none"> • Configure TOE for all combinations of specific source address and specific destination address, specific source address and wildcard destination address, wildcard source address and specific destination address, and wildcard source address and wildcard destination address for Deny condition.


	<ul style="list-style-type: none"> • Configure Test Machine to send traffic with selected source and destination IPs. • Send Traffic with all combination to check traffic is denied. • Verify with TOE logs that all combinations are Denied via TOE. • Verify with Packet capture.
Expected Test Results	<ul style="list-style-type: none"> • TOE logs show that each defined IPv4 Transport Layer Protocol matching the configured source and destination addresses are denied by the TOE. • Packet Capture shows that each defined IPv4 Transport Layer Protocol matching the configured source and destination addresses are denied by the TOE.
Pass/Fail with Explanation	<p>Pass. The TOE denies and logs packets with combinations of specific source address and specific destination address, specific source address and wildcard destination address, wildcard source address and specific destination address, and wildcard source address and wildcard destination address as configured on TOE for each defined IPV4 Transport Layer Protocol. This meets testing requirements.</p>

6.8.12 FPF_RUL_EXT.1.6 Test #3

Item	Data
Test Assurance Activity	<p>Test 3: The evaluator shall configure the TOE to permit and log each supported IPv4 Transport Layer Protocol (see RFC Values for IPv4 and IPv6 table for full possible list) in conjunction with a specific source address and specific destination address, specific source address and wildcard destination address, wildcard source address and specific destination address, and wildcard source address and wildcard destination address. Additionally, the evaluator shall configure the TOE to discard and log each supported IPv4 Transport Layer Protocol (see RFC Values for IPv4 and IPv6 table for full possible list) in conjunction with different (than those permitted above) combinations of a specific source address and specific destination address, specific source address and wildcard destination address, wildcard source address and specific destination address, and wildcard source address and wildcard destination address. The evaluator shall generate packets matching each supported IPv4 Transport Layer Protocol and outside the scope of all source and destination addresses configured above in order to ensure that the supported protocols are denied (i.e., by capturing no applicable packets passing through the TOE) and logged. Any protocols not supported by the TOE must be denied.</p> <p>The following table identifies the RFC defined values for the protocol fields for IPv4 and IPv6 to be used in configuring and otherwise testing packet filtering rule definition and enforcement:</p> <div style="text-align: center;">  <p>IP Transport layer protocols.xlsx</p> </div>
Test Steps	<ul style="list-style-type: none"> • Configure TOE for all combinations of specific source address and specific destination address, specific source address and wildcard destination address, wildcard source


	<p>address and specific destination address, and wildcard source address and wildcard destination address for Discard condition.</p> <ul style="list-style-type: none"> • Configure Test Machine to send traffic with selected source and destination IPs. • Send Traffic with all combination to check traffic is discarded. • Verify with TOE logs that all combinations are discarded via TOE. • Verify with Packet capture.
Expected Test Results	<ul style="list-style-type: none"> • TOE logs show that each defined IPv4 Transport Layer Protocol not matching the configured source and destination addresses are discarded by the TOE. • Packet Capture shows that each defined IPv4 Transport Layer Protocol not matching the configured source and destination addresses are discarded by the TOE.
Pass/Fail with Explanation	<p>Pass. The TOE discards and logs packets with combinations of specific source address and specific destination address, specific source address and wildcard destination address, wildcard source address and specific destination address, and wildcard source address and wildcard destination address as configured on TOE for each defined IPV4 Transport Layer Protocol. This meets testing requirements.</p>

6.8.13 FPF_RUL_EXT.1.6 Test #4

Item	Data
Test Assurance Activity	<p>Test 4: The evaluator shall configure the TOE to permit and log each supported IPv6 Transport Layer Protocol (see RFC Values for IPv4 and IPv6 table for full possible list) in conjunction with a specific source address and specific destination address, specific source address and wildcard destination address, wildcard source address and specific destination address, and wildcard source address and wildcard destination address. The evaluator shall generate packets matching each defined IPv6 Transport Layer Protocol and within the configured source and destination addresses in order to ensure that the supported protocols are permitted (i.e., by capturing the packets after passing through the TOE) and logged. Any protocols not supported by the TOE must be denied.</p> <p>The following table identifies the RFC defined values for the protocol fields for IPv4 and IPv6 to be used in configuring and otherwise testing packet filtering rule definition and enforcement:</p> <p> IP Transport layer protocols.xlsx</p>
Test Steps	<ul style="list-style-type: none"> • Configure TOE for all combinations of specific source address and specific destination address, specific source address and wildcard destination address, wildcard source address and specific destination address, and wildcard source address and wildcard destination address for Allow condition. • Configure Test Machine to send traffic with selected source and destination IPs. • Send Traffic with all combination to check traffic is allowed.


	<ul style="list-style-type: none"> • Verify with TOE logs that all combinations are allowed via TOE. • Verify with Packet capture.
Expected Test Results	<ul style="list-style-type: none"> • TOE logs show that each defined IPv6 Transport Layer Protocol matching the configured source and destination addresses are permitted through TOE. • Packet Capture shows that each defined IPv6 Transport Layer Protocol matching the configured source and destination addresses are permitted through TOE.
Pass/Fail with Explanation	Pass. The TOE permits and logs packets with combinations of specific source address and specific destination address, specific source address and wildcard destination address, wildcard source address and specific destination address, and wildcard source address and wildcard destination address as configured on TOE for each defined IPV6 Transport Layer Protocol. This meets testing requirements.

6.8.14 FPF_RUL_EXT.1.6 Test #5

Item	Data
Test Assurance Activity	<p>Test 5: The evaluator shall configure the TOE to permit all traffic except to discard and log each supported IPv6 Transport Layer Protocol (see RFC Values for IPv4 and IPv6 table for full possible list) in conjunction with a specific source address and specific destination address, specific source address and wildcard destination address, wildcard source address and specific destination address, and wildcard source address and wildcard destination address. The evaluator shall generate packets matching each defined IPv6 Transport Layer Protocol and within the configured source and destination addresses in order to ensure that the supported protocols are denied (i.e., by capturing no applicable packets passing through the TOE) and logged. Any protocols not supported by the TOE must also be denied but are not required to be logged.</p> <p>The following table identifies the RFC defined values for the protocol fields for IPv4 and IPv6 to be used in configuring and otherwise testing packet filtering rule definition and enforcement:</p> <p> IP Transport layer protocols.xlsx</p>
Test Steps	<ul style="list-style-type: none"> • Configure TOE for all combinations of specific source address and specific destination address, specific source address and wildcard destination address, wildcard source address and specific destination address, and wildcard source address and wildcard destination address for Deny condition. • Configure Test Machine to send traffic with selected source and destination IPs. • Send Traffic with all combination to check traffic is denied. • Verify with TOE logs that all combinations are Denied via TOE.

	<ul style="list-style-type: none"> • Verify with Packet capture.
Expected Test Results	<ul style="list-style-type: none"> • TOE logs show that each defined IPv6 Transport Layer Protocol matching the configured source and destination addresses are denied by the TOE. • Packet Capture shows that each defined IPv6 Transport Layer Protocol matching the configured source and destination addresses are denied by the TOE.
Pass/Fail with Explanation	<p>Pass. The TOE denies and logs packets with combinations of specific source address and specific destination address, specific source address and wildcard destination address, wildcard source address and specific destination address, and wildcard source address and wildcard destination address as configured on TOE for each defined IPV6 Transport Layer Protocol. This meets testing requirements.</p>

6.8.15 FPF_RUL_EXT.1.6 Test #6

Item	Data
Test Assurance Activity	<p>Test 6: The evaluator shall configure the TOE to permit and log each supported IPv6 Transport Layer Protocol (see RFC Values for IPv4 and IPv6 table for full possible list) in conjunction with a specific source address and specific destination address, specific source address and wildcard destination address, wildcard source address and specific destination address, and wildcard source address and wildcard destination address. Additionally, the evaluator shall configure the TOE to discard and log each supported IPv6 Transport Layer Protocol (see RFC Values for IPv4 and IPv6 table for full possible list) in conjunction with different (than those permitted above) combinations of a specific source address and specific destination address, specific source address and wildcard destination address, wildcard source address and specific destination address, and wildcard source address and wildcard destination address. The evaluator shall generate packets matching each defined IPv6 Transport Layer Protocol and outside the scope of all source and destination addresses configured above in order to ensure that the supported protocols are dropped (i.e., by capturing no applicable packets passing through the TOE) and logged. Any protocols not supported by the TOE must be denied.</p> <p>The following table identifies the RFC defined values for the protocol fields for IPv4 and IPv6 to be used in configuring and otherwise testing packet filtering rule definition and enforcement:</p> <div style="text-align: center;">  <p>IP Transport layer protocols.xlsx</p> </div>
Test Steps	<ul style="list-style-type: none"> • Configure TOE for all combinations of specific source address and specific destination address, specific source address and wildcard destination address, wildcard source

	<p>address and specific destination address, and wildcard source address and wildcard destination address for Discard condition.</p> <ul style="list-style-type: none"> • Configure Test Machine to send traffic with selected source and destination IPs. • Send Traffic with all combination to check traffic is discarded. • Verify with TOE logs that all combinations are discarded via TOE. • Verify with Packet capture.
Expected Test Results	<ul style="list-style-type: none"> • TOE logs show that each defined IPv6 Transport Layer Protocol not matching the configured source and destination addresses are discarded by the TOE. • Packet Capture shows that each defined IPv6 Transport Layer Protocol not matching the configured source and destination addresses are discarded by the TOE.
Pass/Fail with Explanation	<p>Pass. The TOE discards and logs packets with combinations of specific source address and specific destination address, specific source address and wildcard destination address, wildcard source address and specific destination address, and wildcard source address and wildcard destination address as configured on TOE for each defined IPV6 Transport Layer Protocol. This meets testing requirements.</p>

6.8.16 FPF_RUL_EXT.1.6 Test #7

Item	Data
Test Assurance Activity	<p>Test 7: The evaluator shall configure the TOE to permit and log protocol 6 (TCP) using a selected source port, a selected destination port, and a selected source and destination port combination. The evaluator shall generate packets matching the configured source and destination TCP ports in order to ensure that they are permitted (i.e., by capturing the packets after passing through the TOE) and logged.</p>
Test Steps	<ul style="list-style-type: none"> • Create a filter to configure the TOE to permit and log protocol 6 (TCP) using a selected source port. • Apply the filter the TOE's interface. • Generate traffic to match the filter applied to the TOE's interface. • Verify through firewall log the correct traffic was permitted through the interface. • Verify through Packet Capture. <ul style="list-style-type: none"> • Create a filter to configure the TOE to permit and log protocol 6 (TCP) using a selected destination port. • Apply the filter the TOE's interface. • Generate traffic to match the filters applied to the TOE's interface. • Verify through firewall log that the correct traffic was permitted through the interface. • Verify through Packet Capture.

	<ul style="list-style-type: none"> • Create a filter to configure the TOE to permit and log protocol 6 (TCP) using a selected source and destination port combination. • Apply the filter the TOE's interface. • Generate traffic to match the filters applied to the TOE's interface. • Verify through firewall log that the correct traffic was permitted through the interface. • Verify through Packet Capture.
Expected Test Results	<ul style="list-style-type: none"> • TOE logs show TCP packets with permitted source port being accepted. • Packet Capture TCP shows packets with permitted source port passing through the TOE. • TOE logs show TCP packets with permitted destination port being accepted. • Packet Capture TCP shows packets with permitted destination port passing through the TOE. • TOE logs show TCP packets with permitted source and destination port being accepted • Packet Capture TCP shows packets with permitted source and destination port passing through the TOE
Pass/Fail with Explanation	Pass. The TOE permits and logs TCP traffic with a specific source port, destination port, and a combination of both the source and destination port. This meets the testing requirement.

6.8.17 FPF_RUL_EXT.1.6 Test #8

Item	Data
Test Assurance Activity	Test 8: The evaluator shall configure the TOE to discard and log protocol 6 (TCP) using a selected source port, a selected destination port, and a selected source and destination port combination. The evaluator shall generate packets matching the configured source and destination TCP ports in order to ensure that they are denied (i.e., by capturing no applicable packets passing through the TOE) and logged.
Test Steps	<ul style="list-style-type: none"> • Create a filter to configure the TOE to deny and log protocol 6 (TCP) using a selected source port. • Apply the filter the TOE's interface. • Generate traffic to match the filter applied to the TOE's interface. • Verify through firewall log the configured traffic was denied through the interface. • Verify through Packet Capture. • Create a filter to configure the TOE to deny and log protocol 6 (TCP) using a selected destination port. • Apply the filter the TOE's interface. • Generate traffic to match the filters applied to the TOE's interface. • Verify through firewall log the configured traffic was denied through the interface.

	<ul style="list-style-type: none"> • Verify through Packet Capture. • Create a filter to configure the TOE to deny and log protocol 6 (TCP) using a selected source and destination port combination. • Apply the filter the TOE's interface. • Generate traffic to match the filters applied to the TOE's interface. • Verify through firewall log the configured traffic was denied through the interface. • Verify through Packet Capture.
Expected Test Results	<ul style="list-style-type: none"> • TOE logs show TCP packets with denied source port being dropped. • Packet Capture TCP shows packets with denied source port dropped by TOE. • TOE logs show TCP packets with denied destination port being dropped. • Packet Capture TCP shows packets with denied source port dropped by TOE. • TOE logs show TCP packets with denied source and destination port being dropped. • Packet Capture TCP shows packets with denied source port dropped by TOE.
Pass/Fail with Explanation	Pass. The TOE discards and logs TCP traffic with a specific source port, destination port, and a combination of both the source and destination port. This meets testing requirement.

6.8.18 FPF_RUL_EXT.1.6 Test #9

Item	Data
Test Assurance Activity	Test 9: The evaluator shall configure the TOE to permit and log protocol 17 (UDP) using a selected source port, a selected destination port, and a selected source and destination port combination. The evaluator shall generate packets matching the configured source and destination UDP ports in order to ensure that they are permitted (i.e., by capturing the packets after passing through the TOE) and logged. Here the evaluator ensures that the UDP port 500 (IKE) is included in the set of tests.
Test Steps	<ul style="list-style-type: none"> • Create a filter to configure the TOE to permit and log protocol 17 (UDP) using a selected source port. • Apply the filter the TOE's interface. • Generate traffic to match the filter applied to the TOE's interface. • Verify through firewall log the correct traffic was permitted through the interface. • Verify through Packet Capture. • Create a filter to configure the TOE to permit and log protocol 17 (UDP) using a selected destination port. • Apply the filter the TOE's interface. • Generate traffic to match the filters applied to the TOE's interface. • Verify through firewall log that the correct traffic was permitted through the interface.

	<ul style="list-style-type: none"> • Verify through Packet Capture. • Create a filter to configure the TOE to permit and log protocol 17 (UDP) using a selected source and destination port combination. • Apply the filter the TOE's interface. • Generate traffic to match the filters applied to the TOE's interface. • Verify through firewall log that the correct traffic was permitted through the interface. • Verify through Packet Capture.
Expected Test Results	<ul style="list-style-type: none"> • TOE logs show UDP packets with permitted source port being accepted. • Packet Capture UDP shows packets with permitted source port passing through the TOE. • TOE logs show UDP packets with permitted destination port being accepted. • Packet Capture UDP shows packets with permitted destination port passing through the TOE. • TOE logs show UDP packets with permitted source and destination port being accepted. • Packet Capture TCP shows packets with permitted source and destination port passing through the TOE.
Pass/Fail with Explanation	Pass. The TOE permits and logs UDP protocol traffic with a specific source port, destination port, and a combination of both the source and destination port.

6.8.19 FPF_RUL_EXT.1.6 Test #10

Item	Data
Test Assurance Activity	Test 10: The evaluator shall configure the TOE to discard and log protocol 17 (UDP) using a selected source port, a selected destination port, and a selected source and destination port combination. The evaluator shall generate packets matching the configured source and destination UDP ports in order to ensure that they are denied (i.e., by capturing no applicable packets passing through the TOE) and logged. Again, the evaluator ensures that UDP port 500 is included in the set of tests.
Test Steps	<ul style="list-style-type: none"> • Create a filter to configure the TOE to deny and log protocol 17 (UDP) using a selected source port. • Apply the filter the TOE's interface. • Generate traffic to match the filter applied to the TOE's interface. • Verify through firewall log the configured traffic was denied through the interface. • Verify through Packet Capture. • Create a filter to configure the TOE to deny and log protocol 17 (UDP) using a selected destination port.

	<ul style="list-style-type: none"> • Apply the filter the TOE's interface. • Generate traffic to match the filters applied to the TOE's interface. • Verify through firewall log the configured traffic was denied through the interface. • Verify through Packet Capture. <ul style="list-style-type: none"> • Create a filter to configure the TOE to deny and log protocol 17 (UDP) using a selected source and destination port combination. • Apply the filter the TOE's interface. • Generate traffic to match the filters applied to the TOE's interface. • Verify through firewall log the configured traffic was denied through the interface. • Verify through Packet Capture.
Expected Test Results	<ul style="list-style-type: none"> • TOE logs show UDP packets with denied source port being dropped. • Packet Capture TCP shows packets with denied source port dropped by TOE. <ul style="list-style-type: none"> • TOE logs show UDP packets with denied destination port being dropped. • Packet Capture UDP shows packets with denied source port dropped by TOE. <ul style="list-style-type: none"> • TOE logs show UDP packets with denied source and destination port being dropped. • Packet Capture UDP shows packets with denied source port dropped by TOE.
Pass/Fail with Explanation	Pass. The TOE discards and logs UDP traffic with a specific source port, destination port, and a combination of both the source and destination port. This meets testing requirement.

6.9 X509 Rev

FIA_X509_EXT.1.1/Rev Test #1a

Item	Data
Test Assurance Activity	Test 1a: The evaluator shall present the TOE with a valid chain of certificates (terminating in a trusted CA certificate) as needed to validate the leaf certificate to be used in the function and shall use this chain to demonstrate that the function succeeds. Test 1a shall be designed in a way that the chain can be 'broken' in Test 1b by either being able to remove the trust anchor from the TOEs trust store, or by setting up the trust store in a way that at least one intermediate CA certificate needs to be provided, together with the leaf certificate from outside the TOE, to complete the chain (e.g. by storing only the root CA certificate in the trust store).
Test Steps	<u>IPsec:</u> <ul style="list-style-type: none"> • Create a valid chain of certificates and present them to the TOE. • Verify that the connection succeeds.
Expected Test Results	<ul style="list-style-type: none"> • TOE logs verify successful connection using a valid chain of certificates.

	<ul style="list-style-type: none"> • Packet capture shows a successful connection using a valid chain of certificates.
Pass/Fail with Explanation	Pass. When a complete certificate trust chain is present, the TOE is able to make a successful connection. This meets the testing requirements.

FIA_X509_EXT.1.1/Rev Test #1a(ECDSA)

Item	Data
Test Assurance Activity	Test 1a: The evaluator shall present the TOE with a valid chain of certificates (terminating in a trusted CA certificate) as needed to validate the leaf certificate to be used in the function and shall use this chain to demonstrate that the function succeeds. Test 1a shall be designed in a way that the chain can be 'broken' in Test 1b by either being able to remove the trust anchor from the TOEs trust store, or by setting up the trust store in a way that at least one intermediate CA certificate needs to be provided, together with the leaf certificate from outside the TOE, to complete the chain (e.g. by storing only the root CA certificate in the trust store).
Test Steps	<p><u>IPsec:</u></p> <ul style="list-style-type: none"> • Create a valid chain of certificates and present them to the TOE. • Verify that the connection succeeds.
Expected Test Results	<ul style="list-style-type: none"> • TOE logs verify successful connection using a valid chain of EC certificates. • Packet capture shows a successful connection using a valid chain of EC certificates.
Pass/Fail with Explanation	Pass. When a complete certificate trust chain is present, the TOE is able to make a successful connection. This meets the testing requirements.

FIA_X509_EXT.1.1/Rev Test #1b

Item	Data
Test Assurance Activity	Test 1b: The evaluator shall then 'break' the chain used in Test 1a by either removing the trust anchor in the TOE's trust store used to terminate the chain, or by removing one of the intermediate CA certificates (provided together with the leaf certificate in Test 1a) to complete the chain. The evaluator shall show that an attempt to validate this broken chain fails.
Test Steps	<ul style="list-style-type: none"> • Delete the root CA from the TOE. • Attempt a connection. • Verify through logs and packet capture that a successful connection cannot be established.
Expected Test Results	<ul style="list-style-type: none"> • TOE logs verify that connection is unsuccessful with an incomplete chain of certificates. • Packet Capture verifies that connection negotiation is unsuccessful with an incomplete chain of certificates.

Pass/Fail with Explanation	Pass. The TOE denied the connection because a certificate in the chain was deleted. This meets the testing requirements.
-----------------------------------	--------------------------------------------------------------------------------------------------------------------------

FIA_X509_EXT.1.1/Rev Test #2

Item	Data
Test Assurance Activity	<p>The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE.</p> <p>Test 2: The evaluator shall demonstrate that validating an expired certificate results in the function failing.</p>
Test Steps	<ul style="list-style-type: none"> • Use a valid and unexpired certificate on the TOE. • Change the internal time on the TOE to a date past the expiration date of the certificate. • Attempt to verify the certificate once more. • Attempt to establish a connection with the expired certificate. • Verify through logs and packet capture that a successful connection cannot be established.
Expected Test Results	<ul style="list-style-type: none"> • TOE logs verify connection negotiation with expired certificate fails. • Packet Capture verifies unsuccessful connection negotiation with expired certificate.
Pass/Fail with Explanation	Pass. The TOE denied the connection because of the expired certificate. This meets the testing requirements.

FIA_X509_EXT.1.1/Rev Test #3 CRL

Item	Data
Test Assurance Activity	<p>The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE.</p> <p>Test 3: The evaluator shall test that the TOE can properly handle revoked certificates—conditional on whether CRL or OCSP is selected; if both are selected, then a test shall be performed for each method. The evaluator shall test revocation of the peer certificate and revocation of the peer intermediate CA certificate i.e. the intermediate CA certificate should be revoked by the root CA. The evaluator shall ensure that a valid certificate is used, and that the validation function succeeds. The evaluator then attempts the test with a certificate that has been revoked (for each method</p>

	<p>chosen in the selection) to ensure when the certificate is no longer valid that the validation function fails.</p> <p>Revocation checking is only applied to certificates that are not designated as trust anchors. Therefore, the revoked certificate(s) used for testing shall not be a trust anchor.</p>
Test Steps	<ul style="list-style-type: none"> • Create a valid certificate chain and upload them to the TOE and peer device. • Verify that the CRL downloads successfully and that there are no revoked certificates. • Attempt a connection between the TOE and the peer and verify that the connection is successful. • Revoke the peer intermediate CA certificate and update the CRL server. • Verify that the TOE successfully downloads the updated CRL. • Attempt a connection between the TOE and the peer and verify that the connection fails. • Revoke the peer end entity certificate and update the CRL server. • Verify that the TOE successfully downloads the updated CRL. • Attempt a connection between the TOE and the peer and verify that the connection fails.
Expected Test Results	<ul style="list-style-type: none"> • TOE logs verify successful connection with valid unrevoked certificates. • Packet Capture shows successful connection with valid unrevoked certificates. • TOE logs verify unsuccessful connection negotiation when intermediate CA certificate is revoked. • Packet Capture verifies unsuccessful connection negotiation when intermediate CA certificate is revoked. • TOE logs verify unsuccessful connection negotiation when end entity certificate is revoked. • Packet Capture verifies unsuccessful connection negotiation when end entity certificate is revoked.
Pass/Fail with Explanation	<p>Pass. The TOE does not connect with peers that have their certificate revoked or their intermediate CA certificate revoked. When presented non-revoked certificates, the TOE accepts the certificate. This meets the testing requirements.</p>

FIA_X509_EXT.1.1/Rev Test #4 CRL

Item	Data
------	------

Test Assurance Activity	<p>The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE.</p> <p>If OSCP is selected, the evaluator shall configure the OCSP server or use a man-in-the-middle tool to present a certificate that does not have the OCSP signing purpose and verify that validation of the OCSP response fails. If CRL is selected, the evaluator shall configure the CA to sign a CRL with a certificate that does not have the cRLsign key usage bit set and verify that validation of the CRL fails.</p>
Test Steps	<ul style="list-style-type: none"> • Configure a connection on the TOE with CRL checking enabled. • Configure the CA signing the CRL to use a signing certificate that does not have the cRLsign key usage bit set. • Load the new CA to the TOE. • Confirm that the certificate validation fails.
Expected Test Results	<ul style="list-style-type: none"> • TOE logs verify that certificate validation is unsuccessful when the CA certificate does not have cRLsign key usage enabled.
Pass/Fail with Explanation	<p>Pass. The TOE does not validate the CRL when CA signing the CRL to use a signing certificate that does not have the cRLsign key usage bit set. This meets the testing requirements.</p>

FIA_X509_EXT.1.1/Rev Test #5

Item	Data
Test Assurance Activity	<p>The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE.</p> <p>The evaluator shall modify any byte in the first eight bytes of the certificate and demonstrate that the certificate fails to validate. (The certificate will fail to parse correctly.)</p>
Test Steps	<ul style="list-style-type: none"> • Configure StrongSwan peer. • Configure the TOE to connect to a StrongSwan peer. • Run the StrongSwan Acumen tool, using it to modify the first byte of the encoding certificate, incrementing 30 to 31. • Verify that the TOE rejects the connection.
Expected Test Results	<ul style="list-style-type: none"> • TOE logs verify that connection establishment fails with a ‘failed to verify peer cert’ error when a byte of peer certificate is modified. • Packet Capture shows unsuccessful connection establishment.
Pass/Fail with Explanation	<p>Pass. The TOE rejects connections when the first 8 bytes of the certificate are modified. This meets the testing requirements.</p>

FIA_X509_EXT.1.1/Rev Test #6

Item	Data
Test Assurance Activity	<p>The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE.</p> <p>The evaluator shall modify any byte in the certificate signatureValue field (see RFC5280 Sec. 4.1.1.3), which is normally the last field in the certificate, and demonstrate that the certificate fails to validate. (The signature on the certificate will not validate.)</p>
Test Steps	<ul style="list-style-type: none"> • Run the StrongSwan Acumen tool to modify the last byte of the encoding certificate by incrementing cc to cd. • Verify that the TOE rejects the connection.
Expected Test Results	<ul style="list-style-type: none"> • TOE logs verify that connection establishment fails with a ‘failed to verify certificate signature’ error. • Packet Capture shows unsuccessful connection establishment.
Pass/Fail with Explanation	Pass. The TOE rejects connections when the last byte of the certificate is modified. This meets the testing requirements.

FIA_X509_EXT.1.1/Rev Test #7

Item	Data
Test Assurance Activity	<p>The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE.</p> <p>Test 7: The evaluator shall modify any byte in the public key of the certificate and demonstrate that the certificate fails to validate. (The hash of the certificate will not validate.)</p>
Test Steps	<ul style="list-style-type: none"> • Run the StrongSwan Acumen tool to modify any byte in public key of certificate by incrementing 82 to 83. • Verify that the TOE rejects the connection.
Expected Test Results	<ul style="list-style-type: none"> • TOE logs verify that connection establishment fails with ‘failed to verify peer cert’ and ‘pkid’ errors. • Packet Capture shows unsuccessful connection establishment.
Pass/Fail with Explanation	Pass. The TOE rejects connections when the public key of the certificate is modified. This meets the testing requirements.

FIA_X509_EXT.1.1/Rev Test #8a

Item	Data
------	------

Test Assurance Activity	<p>(Conditional on support for EC certificates as indicated in FCS_COP.1/SigGen) (Conditional on support for a minimum certificate path length of three certificates) (Conditional on TOE ability to process CA certificates presented in certificate message)</p> <p>The test shall be designed in a way such that only the EC root certificate is designated as a trust anchor, and by setting up the trust store in a way that the EC Intermediate CA certificate needs to be provided, together with the leaf certificate, from outside the TOE to complete the chain (e.g. by storing only the EC root CA certificate in the trust store). The evaluator shall present the TOE with a valid chain of EC certificates (terminating in a trusted CA certificate), where the elliptic curve parameters are specified as a named curve. The evaluator shall confirm that the TOE validates the certificate chain.</p> <p>TD0527 (12/1 Update) has been applied.</p> <p>Test 8a: (Conditional on support for EC certificates as indicated in FCS_COP.1(3)). The evaluator shall establish a valid, trusted certificate chain consisting of an EC leaf certificate, an EC Intermediate CA certificate not designated as a trust anchor, and an EC certificate designated as a trusted anchor, where the elliptic curve parameters are specified as a named curve. The evaluator shall confirm that the TOE validates the certificate chain.</p>
Test Steps	<ul style="list-style-type: none"> • Create a certificate chain with three EC certificates using named curves. • Add Root CA as trust anchor for the TOE and load the TOE ICA. • Configure the Strongswan peer with the relevant parameters. • Attempt a connection from a remote server and verify that it is successful. • Verify the successful connection with logs and packet capture.
Expected Test Results	<ul style="list-style-type: none"> • TOE validates a certificate chain with an EC root certificate designated as trust anchor and an EC Intermediate CA certificate not designated as a trust anchor.
Pass/Fail with Explanation	<p>Pass. The TOE validates the certificate chain with the EC parameters.</p>

FIA_X509_EXT.1.1/Rev Test #8b

Item	Data
Test Assurance Activity	<p>(Conditional on support for EC certificates as indicated in FCS_COP.1/SigGen) (Conditional on support for a minimum certificate path length of three certificates) (Conditional on TOE ability to process CA certificates presented in certificate message)</p> <p>The test shall be designed in a way such that only the EC root certificate is designated as a trust anchor, and by setting up the trust store in a way that the EC Intermediate CA certificate needs to be provided, together with the leaf certificate, from outside the TOE to complete the chain (e.g. by storing only the EC root CA certificate in the trust store). The evaluator shall present the TOE with a chain of EC certificates (terminating in a trusted CA certificate), where the intermediate certificate in the certificate chain uses an explicit format version of the Elliptic Curve parameters in the public key information field, and is signed by the trusted EC root CA, but having no other changes. The evaluator shall confirm the TOE treats the certificate as invalid.</p> <p>TD0527 (12/1 Update) has been applied.</p>

	Test 8b: (Conditional on support for EC certificates as indicated in FCS_COP.1(3)). The evaluator shall replace the intermediate certificate in the certificate chain for Test 8a with a modified certificate, where the modified intermediate CA has a public key information field where the EC parameters uses an explicit format version of the Elliptic Curve parameters in the public key information field of the intermediate CA certificate from Test 8a, and the modified Intermediate CA certificate is signed by the trusted EC root CA, but having no other changes. The evaluator shall confirm the TOE treats the certificate as invalid.
Test Steps	<ul style="list-style-type: none"> • Use the acumen-x509-mod tool to replace the named curve in the ICA from the previous test with an explicit curve. • Replace the ICA from the earlier test with the modified ICA certificate. • Attempt a connection from the remote server and verify that it fails. • Verify the failed connection with logs and packet capture.
Expected Test Results	<ul style="list-style-type: none"> • TOE treats the modified intermediate CA certificate as invalid.
Pass/Fail with Explanation	Pass. The TOE rejects the connection when the ICA certificate is modified to replace the named EC curve with an explicit curve.

FIA_X509_EXT.1.1/Rev Test #8c

Item	Data
Test Assurance Activity	<p>(Conditional on support for EC certificates as indicated in FCS_COP.1/SigGen) (Conditional on support for a minimum certificate path length of three certificates)</p> <p>The evaluator shall establish a subordinate CA certificate, where the elliptic curve parameters are specified as a named curve, that is signed by a trusted EC root CA. The evaluator shall attempt to load the certificate into the trust store and observe that it is accepted into the TOE's trust store. The evaluator shall then establish a subordinate CA certificate that uses an explicit format version of the elliptic curve parameters, and that is signed by a trusted EC root CA. The evaluator shall attempt to load the certificate into the trust store and observe that it is rejected, and not added to the TOE's trust store.</p> <p>TD0527 (12/1 Update) has been applied.</p> <p>Test 8c: The evaluator shall establish a subordinate CA certificate, where the elliptic curve parameters are specified as a named curve, that is signed by a trusted EC root CA. The evaluator shall attempt to load the certificate into the trust store and observe that it is accepted into the TOE's trust store. The evaluator shall then establish a subordinate CA certificate that uses an explicit format version of the elliptic curve parameters, and that is signed by a trusted EC root CA. The evaluator shall attempt to load the certificate into the trust store and observe that it is rejected, and not added to the TOE's trust store.</p>
Test Steps	<ul style="list-style-type: none"> • Add a subordinate CA certificate signed by a trusted EC root CA with the elliptic curve parameters specified as a named curve into the TOE trust store, and observe that it is accepted.

	<ul style="list-style-type: none"> • Add a subordinate CA certificate signed by a trusted EC root CA using an explicit format version of the elliptic curve parameters into a TOE's trust store and observe that it is rejected.
Expected Test Results	<ul style="list-style-type: none"> • TOE rejects the subordinate CA certificate which uses an explicit format version of the elliptic curve parameters and is signed by the EC root CA.
Pass/Fail with Explanation	Pass. The TOE rejects a subordinate CA certificate signed by a trusted EC root CA that uses an explicit format version of the elliptic curve parameters.

FIA_X509_EXT.1.2/Rev Test #1

Item	Data
Test Assurance Activity	<p>The tests described must be performed in conjunction with the other certificate services assurance activities, including the functions in FIA_X509_EXT.2.1/Rev. The tests for the extendedKeyUsage rules are performed in conjunction with the uses that require those rules. Where the TSS identifies any of the rules for extendedKeyUsage fields (in FIA_X509_EXT.1.1) that are not supported by the TOE (i.e. where the ST is therefore claiming that they are trivially satisfied) then the associated extendedKeyUsage rule testing may be omitted.</p> <p>The goal of the following tests is to verify that the TOE accepts a certificate as a CA certificate only if it has been marked as a CA certificate by using basicConstraints with the CA flag set to True (and implicitly tests that the TOE correctly parses the basicConstraints extension as part of X509v3 certificate chain validation).</p> <p>For each of the following tests the evaluator shall create a chain of at least three certificates:</p> <ul style="list-style-type: none"> - a self-signed root CA certificate, - an intermediate CA certificate and - a leaf (node) certificate. <p>The properties of the certificates in the chain are adjusted as described in each individual test below (and this modification shall be the only invalid aspect of the relevant certificate chain).</p> <p>Test 1: The evaluator shall ensure that at least one of the CAs in the chain does not contain the basicConstraints extension. The evaluator confirms that the TOE rejects such a certificate at one (or both) of the following points:</p> <ol style="list-style-type: none"> <i>as part of the validation of the leaf certificate belonging to this chain;</i> <i>when attempting to add a CA certificate without the basicConstraints extension to the TOE's trust store (i.e. when attempting to install the CA certificate as one which will be retrieved from the TOE itself when validating future certificate chains).</i>
Test Steps	<ul style="list-style-type: none"> • Create a CA certificate that does not contain the basicConstraints extension. • Sign the TOE local certificate by the CA that does not contain the basicConstraints extension. • Load the CA and local certificate onto the TOE.

	<ul style="list-style-type: none"> • Verify that the TOE identifies the signing CA certificate does not contain the basicConstraints extension and rejects the certificate signed by it. • Verify that the connection between TOE and Peer fails.
Expected Test Results	<ul style="list-style-type: none"> • TOE logs show failure in verifying the local certificate signed by a CA certificate which does not contain the basic Constraints extension.
Pass/Fail with Explanation	Pass. The TOE rejects certificates signed by a CA that does not contain the basicConstraints extension. This meets the testing requirements.

FIA_X509_EXT.1.2/Rev Test #2

Item	Data
Test Assurance Activity	<p>The tests described must be performed in conjunction with the other certificate services assurance activities, including the functions in FIA_X509_EXT.2.1/Rev. The tests for the extendedKeyUsage rules are performed in conjunction with the uses that require those rules. Where the TSS identifies any of the rules for extendedKeyUsage fields (in FIA_X509_EXT.1.1) that are not supported by the TOE (i.e. where the ST is therefore claiming that they are trivially satisfied) then the associated extendedKeyUsage rule testing may be omitted.</p> <p>The goal of the following tests is to verify that the TOE accepts only certificates that have been marked as CA certificates by using basicConstraints with the CA flag set to True (and implicitly that the TOE correctly parses the basicConstraints extension as part of X509v3 certificate chain validation).</p> <p>For each of the following tests the evaluator shall create a chain of at least three certificates:</p> <ul style="list-style-type: none"> - a self-signed root CA certificate, - an intermediate CA certificate and - a leaf (node) certificate. <p>The properties of the certificates in the chain are adjusted as described in each individual test below (and this modification shall be the only invalid aspect of the relevant certificate chain).</p> <p>Test 2: The evaluator shall ensure that at least one of the CA certificates in the chain has a basicConstraints extension in which the CA flag is set to FALSE. The evaluator confirms that the TOE rejects such a certificate at one (or both) of the following points:</p> <ol style="list-style-type: none"> 1. As part of the validation of the leaf certificate belonging to this chain; 2. When attempting to add a CA certificate with the CA flag set to FALSE to the TOE's trust store (i.e. when attempting to install the CA certificate as one which will be retrieved from the TOE itself when validating future certificate chains).
Test Steps	<p><u>IPsec:</u></p> <ul style="list-style-type: none"> • Create a CA certificate that has the CA flag in the basicConstraints extension set to FALSE. • A local certificate is signed by the CA that has the CA flag in the basicConstraints extension set to FALSE. • Load the CA and local certificate onto the TOE.

	<ul style="list-style-type: none"> • Verify that the TOE identifies the signing CA certificate has the CA flag in the basicConstraints extension set to FALSE and rejects the certificate signed by it. • Verify the connection between TOE and Peer fails.
Expected Test Results	<ul style="list-style-type: none"> • TOE logs show failure in verifying a CA certificate which has basicConstraints extension set to FALSE. • Packet Capture shows unsuccessful IPsec connection.
Pass/Fail with Explanation	Pass. The TOE rejects certificates signed by a CA that has the cA flag in the basicConstraints extension set to FALSE. This meets the testing requirements.

FIA_X509_EXT.2 Test #1

Item	Data
Test Assurance Activity	<p>The evaluator shall perform the following test for each trusted channel: The evaluator shall demonstrate that using a valid certificate that requires certificate validation checking to be performed in at least some part by communicating with a non-TOE IT entity. The evaluator shall then manipulate the environment so that the TOE is unable to verify the validity of the certificate and observe that the action selected in FIA_X509_EXT.2.2 is performed. If the selected action is administrator-configurable, then the evaluator shall follow the guidance documentation to determine that all supported administrator-configurable options behave in their documented manner.</p>
Test Steps	<ul style="list-style-type: none"> • Configure the TOE to use CRL for revocation checking. • Delete every CRL from the web server. • Verify that the TOE can no longer download a new CRL. • Verify that the TOE does not establish a connection when it cannot download a CRL. <ul style="list-style-type: none"> • Configure the TOE to allow connections to be established when CRLs can not be retrieved. • Delete every CRL from the web server. • Verify that the TOE successfully verifies the certificates despite CRL download failure. • Verify that the TOE establishes connection as configured by the administrator when validity of certificate cannot be determined.
Expected Test Results	<ul style="list-style-type: none"> • TOE logs verify that Connection is not established when revocation status of the Peer certificate is not available.

	<ul style="list-style-type: none"> • Packet Capture shows unsuccessful connection when revocation status of the Peer certificate is not available. • TOE logs verify successful connection with peer certificate without a revocation status when TOE is configured to accept certificates without checking CRL. • Packet Capture shows successful connection with peer certificate without a revocation status when TOE is configured to accept certificates without checking CRL.
Pass/Fail with Explanation	Pass. When the TOE cannot establish a connection to determine the validity of a certificate, the TOE takes the action configured by the administrator.

FIA_X509_EXT.3 Test #1

Item	Data
Test Assurance Activity	The evaluator shall use the guidance documentation to cause the TOE to generate a Certification Request. The evaluator shall capture the generated message and ensure that it conforms to the format specified. The evaluator shall confirm that the Certification Request provides the public key and other required information, including any necessary user-input information.
Test Steps	<ul style="list-style-type: none"> • From the TOE, generate a CSR • Examine the CSR contents and ensure the CSR contains the following fields <ul style="list-style-type: none"> ○ Public key ○ Device-specific information ○ Common Name ○ Organization ○ Organizational Unit ○ Country
Expected Test Results	<ul style="list-style-type: none"> • CSR generated by TOE conforms to the format specified.
Pass/Fail with Explanation	Pass. The TOE is able to generate a CSR with all of the requisite information. This meets the testing requirements.

FIA_X509_EXT.3 Test #2

Item	Data
Test Assurance Activity	The evaluator shall demonstrate that validating a response message to a Certification Request without a valid certification path results in the function failing. The evaluator shall then load a certificate or certificates as trusted CAs needed to validate the certificate response message and demonstrate that the function succeeds.
Test Steps	<ul style="list-style-type: none"> • From the TOE, generate a CSR.

	<ul style="list-style-type: none"> • Generate a signed certificate based on the generated CSR from an external CA. • Ensure that the full trust chain for the signed CA is not present on the TOE. • Load the signed certificate on the TOE. • Verify that the validation fails because the full trust chain of the CA is not present. • Add the intermediary certificate to the TOE certificate store to ensure that the signing CA now has a full certificate path. • Re-attempt to load the signed certificate on the TOE. • Verify that the validation succeeds because the path validation succeeded. • Remove the signing CA intermediary certificates from the TOE certificate store. • Verify that the TOE now identifies the signed certificate as invalid.
Expected Test Results	<ul style="list-style-type: none"> • TOE logs verify that certificate validation, and hence the authentication, fails without a valid chain of certificates. • TOE logs verify that certificate validation, and hence the authentication, is successful with a valid chain of certificates.
Pass/Fail with Explanation	Pass. The TOE does not validate certificates signed by a CA without a full trust path. The TOE does validate a certificate signed by a CA with a full trust path. This meets the testing requirements.

7 Security Assurance Requirements

7.1 ADV_FSP.1 Basic Functional Specification

7.1.1 ADV_FSP.1

7.1.1.1 ADV_FSP.1 Activity 1

Objective	The evaluator shall examine the interface documentation to ensure it describes the purpose and method of use for each TSFI that is identified as being security relevant.
Evaluator Findings	The evaluator examined the AGD (interface documentation) to verify that it describes the purpose and method of use for each TSFI that is identified as being security relevant. The evaluator examined the entire AGD. The evaluator verified the AGD describes the purpose and method of use for each security relevant TSFI by verifying the AGD satisfies all of the Guidance Evaluation Activities. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.1.1.2 ADV_FSP.1 Activity 2

Objective	The evaluator shall check the interface documentation to ensure it identifies and describes the parameters for each TSFI that is identified as being security relevant.
Evaluator Findings	The evaluator examined the AGD (interface documentation) to verify that it identifies and describes the parameters for each TSFI that is identified as being security relevant. The evaluator examined the entire AGD. The evaluator verified the AGD describes the parameters for each security relevant TSFI by verifying the AGD satisfies all of the Guidance Evaluation Activities. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.1.1.3 ADV_FSP.1 Activity 3

Objective	The evaluator shall examine the interface documentation to develop a mapping of the interfaces to SFRs.
Evaluator Findings	The evaluator examined the AGD (interface documentation) to develop a mapping of the interfaces to SFRs. The evaluator examined the entire AGD. Each Guidance Evaluation Activity is associated with a specific SFR. The Evaluation Findings for each Guidance Evaluation Activity identify the relevant interfaces, thus providing a mapping. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.2 AGD_OPE.1 Operational User Guidance

7.2.1 AGD_OPE.1

7.2.1.1 AGD_OPE.1 Activity 1

Objective	The evaluator shall ensure the Operational guidance documentation is distributed to Security Administrators and users (as appropriate) as part of the TOE, so that there is a reasonable guarantee that Security Administrators and users are aware of the existence and role of the documentation in establishing and maintaining the evaluated configuration.
Evaluator Findings	The evaluator checked the requirements below are met by the guidance documentation. Guidance documentation shall be distributed to administrators and users (as appropriate) as part of the TOE, so that there is a reasonable guarantee that administrators and users are aware of the existence and role of the documentation in establishing and maintaining the evaluated configuration. Upon investigation, the evaluator found that the CC guidance will be published with the CC certificate on www.niap-ccevs.org . Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.2.1.2 AGD_OPE.1 Activity 2

Objective	The evaluator shall ensure that the Operational guidance is provided for every Operational Environment that the product supports as claimed in the Security Target and shall adequately address all platforms claimed for the TOE in the Security Target.
Evaluator Findings	The evaluator ensured that the Operational guidance is provided for every Operational Environment that the product supports as claimed in the Security Target. The section titled Supported Platforms for vSRX Virtual Firewall of the AGD was used to determine the verdict of this assurance activity. The AGD specifies that the platforms supported are: <ul style="list-style-type: none"> • vSRX3.0 instances Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.2.1.3 AGD_OPE.1 Activity 3

Objective	The evaluator shall ensure that the Operational guidance contains instructions for configuring any cryptographic engine associated with the evaluated configuration of the TOE. It shall provide a warning to the administrator that use of other cryptographic engines was not evaluated nor tested during the CC evaluation of the TOE.
Evaluator Findings	The evaluator ensured that the Operational guidance contains instructions for configuring any cryptographic engine associated with the evaluated configuration of the TOE. While performing the Guidance Evaluation Activities for the cryptographic SFRs, the evaluator ensured guidance contained the necessary instructions for configuring the cryptographic engines.

	Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.2.1.4 AGD_OPE.1 Activity 4

Objective	The evaluator shall ensure the Operational guidance makes it clear to an administrator which security functionality and interfaces have been assessed and tested by the EAs.
Evaluator Findings	The entire AGD was used to determine the verdict of this work unit. Each confirmation command indicates tested options. Additionally, the section titled Unsupported Junos-FIPS Operational Commands specifies features that are not assessed and tested by the EAs. The evaluator ensured the Operational guidance makes it clear to an administrator which security functionality and interfaces have been assessed and tested by the EAs. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.2.1.5 AGD_OPE.1 Activity 5 [TD0536]

Objective	In addition, the evaluator shall ensure that the following requirements are also met. <ul style="list-style-type: none"> a) The guidance documentation shall contain instructions for configuring any cryptographic engine associated with the evaluated configuration of the TOE. It shall provide a warning to the administrator that use of other cryptographic engines was not evaluated nor tested during the CC evaluation of the TOE. b) The documentation must describe the process for verifying updates to the TOE for each method selected for FPT_TUD_EXT.1.3 in the Security Target. The evaluator shall verify that this process includes the following steps: <ul style="list-style-type: none"> i) Instructions for obtaining the update itself. This should include instructions for making the update accessible to the TOE (e.g., placement in a specific directory). ii) Instructions for initiating the update process, as well as discerning whether the process was successful or unsuccessful. This includes instructions that describe at least one method of validating the hash/digital signature. c) The TOE will likely contain security functionality that does not fall in the scope of evaluation under this cPP. The guidance documentation shall make it clear to an administrator which security functionality is covered by the Evaluation Activities.
Evaluator Findings	The evaluator verified the guidance documentation contains instructions for configuring any cryptographic engines in AGD_OPE.1 Activity #3. The evaluator verified the guidance documentation describes the process for verifying updates in FPT_TUD_EXT.1 Guidance 2. The evaluator verified the guidance documentation makes it clear which security functionality is covered by the Evaluation Activities in AGD_OPE.1 Activity #4. Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass
---------	------

7.3 AGD_PRE.1 Preparative Procedures

7.3.1 AGD_PRE.1

7.3.1.1 AGD_PRE.1 Activity 1

Objective	The evaluator shall examine the Preparative procedures to ensure they include a description of how the Security Administrator verifies that the operational environment can fulfil its role to support the security functionality (including the requirements of the Security Objectives for the Operational Environment specified in the Security Target).
Evaluator Findings	<p>The evaluator examined the Preparative procedures to ensure they include a description of how the administrator verifies that the operational environment can fulfil its role to support the security functionality. The evaluator reviewed the sections titled Security Administrator Role and Responsibilities of the AGD. The evaluator found that these sections describe how the Operational Environment must meet:</p> <ul style="list-style-type: none"> • OE.PHYSICAL • OE.NO_GENERAL_PURPOSE • OE.NO_THRU_TRAFFIC_PROTECTION • OE.TRUSTED_ADMN • OE.UPDATES • OE.ADMIN_CREDENTIALS_SECURE • OE.RESIDUAL_INFORMATION • OE.CONNECTIONS (IPS) • OE.CONNECTIONS (VPN) <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

7.3.1.2 AGD_PRE.1 Activity 2

Objective	The evaluator shall examine the Preparative procedures to ensure they are provided for every Operational Environment that the product supports as claimed in the Security Target and shall adequately address all platforms claimed for the TOE in the Security Target.
Evaluator Findings	<p>The evaluator checked the requirements below are met by the preparative procedures. The entire AGD was used to determine the verdict of this work unit. Upon investigation, the evaluator found that the guidance documentation describes each of the devices in the operating environment, including,</p> <ul style="list-style-type: none"> • Syslog Server • CRL Server • SSH Client • Management Console • IPsec Peer

	<ul style="list-style-type: none"> • NTP Server <p>The section titled Supported Platforms for vSRX Virtual Firewall of AGD identifies the following supported platform:</p> <ul style="list-style-type: none"> • vSRX3.0 instances <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

7.3.1.3 AGD_PRE.1 Activity 3

Objective	The evaluator shall examine the preparative procedures to ensure they include instructions to successfully install the TSF in each Operational Environment.
Evaluator Findings	<p>The evaluator checked the requirements are met by the preparative procedures. The entire AGD was used to determine the verdict of this work unit. Upon investigation, the evaluator found that AGD describes all of the functions necessary to install and configure the TOE to work in the target operating environment, including,</p> <ul style="list-style-type: none"> • Configuring Administrative Credentials and Privileges • Configuring a Common Criteria Authorized Administrator • Configuring Network Time Protocol • Configuring Roles and Authentication Methods • Configuring SSH and Console Connections • Configuring the Remote Syslog Server • Configuring Audit Log Options • Configuring Event Logging • Configuring a Secure Logging Channel • Configuring VPNs • Configuring Security Flow Policies • Configuring Traffic Filtering Rules • Configuring Network Attacks <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

7.3.1.4 AGD_PRE.1 Activity 4

Objective	The evaluator shall examine the preparative procedures to ensure they include instructions to manage the security of the TSF as a product and as a component of the larger operational environment.
Evaluator Findings	<p>The evaluator ensured the preparative procedures include instructions to manage the security of the TSF as a product and as a component of the larger operational environment. The entire AGD was used to determine the verdict of this work unit. The same commands,</p>

	<p>configurations, and interfaces used to install the TOE are also used for ongoing management, so this is satisfied by AGD_PRE.1 Activity #3.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

7.3.1.5 AGD_PRE.1 Activity 5

Objective	<p>In addition, the evaluator shall ensure that the following requirements are also met.</p> <p>The preparative procedures must</p> <p>a) include instructions to provide a protected administrative capability; and</p> <p>b) identify TOE passwords that have default values associated with them and instructions shall be provided for how these can be changed.</p>
Evaluator Findings	<p>The evaluator ensured the preparative procedures include instructions to provide a protected administrative capability and changing default passwords. The sections titled Configuring a Common Criteria Authorized Administrator and Configuring SSH and Console Connection were used to determine the verdict of this work unit. The AGD describes changing the default password associated with the root account and configuring SSH for remote administration.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

7.4 ALC Assurance Activities

7.4.1 ALC_CMC.1

7.4.1.1 ALC_CMC.1 Activity 1

Objective	<p>When evaluating that the TOE has been provided and is labelled with a unique reference, the evaluator performs the work units as presented in the CEM.</p>
Evaluator Findings	<p>The evaluator verified that the ST, TOE and Guidance are all labeled with the same hardware versions and software. The information is specific enough to procure the TOE and it includes hardware models and software versions. The evaluator checked the TOE software version and hardware identifiers during testing by examining the actual machines used for testing.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

7.4.2 ALC_CMS.1

7.4.2.1 ALC_CMS.1 Activity 1

Objective	<p>When evaluating the developer's coverage of the TOE in their CM system, the evaluator performs the work units as presented in the CEM.</p>
-----------	-----------------------------------------------------------------------------------------------------------------------------------------------

Evaluator Findings	The evaluator verified that the ST, TOE and Guidance are all labeled with the same hardware versions and software. The information is specific enough to procure the TOE and it includes hardware models and software versions. The evaluator checked the TOE software version and hardware identifiers during testing by examining the actual machines used for testing. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.5 ATE_IND.1 Independent Testing – Conformance

7.5.1 ATE_IND.1

7.5.1.1 ATE_IND.1 Activity 1

Objective	The evaluator performs the CEM work units associated with the ATE_IND.1 SAR. Specific testing requirements and EAs are captured for each SFR in Sections 2, 3 and 4. The evaluator should consult Appendix 709 when determining the appropriate strategy for testing multiple variations or models of the TOE that may be under evaluation.
Evaluator Findings	The evaluator examined the TOE to determine that the test configuration is consistent with the configuration under evaluation as specified in the ST. Upon investigation, the evaluator found that each instance of the TOE used in testing was consistent with TOE description found in the Security Target. Additionally, the evaluator found that the TOE version is consistent with what was specified in the Security Target. The evaluator examined the TOE to determine that it has been installed properly and is in a known state. The details of the installed TOE and any configuration performed with the TOE are found in the separate Test Reports. The evaluator prepared a test plan that covers all of the testing actions for ATE_IND.1 in the CEM and in the SFR-related Evaluation Activities. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.6 AVA_VAN.1 Vulnerability Survey

7.6.1 AVA_VAN.1

7.6.1.1 AVA_VAN.1 Activity 1 [TD0564, Labgram #116]

Objective	The evaluator shall document their analysis and testing of potential vulnerabilities with respect to this requirement.
Evaluator Findings	The evaluator documented their analysis and testing of potential vulnerabilities with respect to this requirement. Public searches were performed against all keywords found within the Security Target and AGD that may be applicable to specific TOE components. This included protocols, TOE software version, and TOE hardware to ensure sufficient coverage under AVA. The evaluator

	<p>searched the Internet for potential vulnerabilities in the TOE using the web sites listed below. The sources of the publicly available information are provided below.</p> <ul style="list-style-type: none"> • https://nvd.nist.gov/vuln/search • https://cve.mitre.org/cve/search_cve_list.html • https://www.cvedetails.com/vulnerability-search.php • https://www.exploit-db.com • https://www.rapid7.com/db/?type=nexpose • https://supportportal.juniper.net/s/knowledge <p>The evaluator performed the public domain vulnerability searches using the following key words. The search was performed on January 9, 2024.</p> <ul style="list-style-type: none"> • JunOS 22.2 • Juniper vSRX • Intel Xeon E5-2600 v4 • Intel Xeon E-2200M • FreeBSD 12 • Junos OS Kernel • Junos OS libmd • Junos OS libquicksec • Junos OS openssl <p>The evaluation lab examined each result provided from NVD and Exploit Search to determine if the current TOE version or component within the environment was vulnerable. Based upon the analysis, any issues found that were generated were patched in the TOE version and prior versions, mitigating the risk factor.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
Verdict	Pass

7.6.1.2 AVA_VAN.1 Activity 2

Objective	<p>The evaluator shall perform the following activities to generate type 4 flaw hypotheses:</p> <ul style="list-style-type: none"> • Fuzz testing <ul style="list-style-type: none"> ○ Examine effects of sending: <ul style="list-style-type: none"> ▪ mutated packets carrying each 'Type' and 'Code' value that is undefined in the relevant RFC for each of ICMPv4 (RFC 792) and ICMPv6 (RFC 4443) ▪ mutated packets carrying each 'Transport Layer Protocol' value that is undefined in the respective RFC for IPv4 (RFC 791) IPv6 (RFC 2460) should also be covered if it is supported and claimed by the TOE. <p>Since none of these packets will belong to an allowed session, the packets should not be processed by the TOE, and the TOE should not be adversely affected by this</p>
-----------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	<p>traffic. Any results that are unexpected (e.g., core dumps) are candidates for a flaw hypothesis.</p> <ul style="list-style-type: none"> ○ Mutation fuzz testing of the remaining fields in the required protocol headers. This testing requires sending mutations of well- formed packets that have both carefully chosen and random values inserted into each header field in turn (i.e. testing is to include both carefully chosen and random insertion test cases). The original well- formed packets would be accepted as part of a normal existing communication stream and may still be accepted as valid packets when subject to the carefully chosen mutations (the individual packet alone would be valid although its contents may not be valid in the context of preceding and/or following packets), but will often not be valid packets when random values are inserted into fields. The carefully chosen values should include semantically significant values that can be determined from the type of the data that the field represents, such as values indicating positive and negative integers, boundary conditions, invalid binary combinations (e.g. for flag sets with dependencies between bits), and missing start or end values. Randomly chosen values may not result in well-formed packets but are included nonetheless to see whether they can lead to the device entering an insecure state. Any results that are unexpected (e.g., core dumps) are candidates for a flaw hypothesis.
<p>Evaluator Findings</p>	<p>The evaluator documented the fuzz testing results with respect to this requirement.</p> <p>The evaluation lab examined each result from fuzz testing to determine if the TOE improperly processes packets. Based upon the analysis, no unexpected results occurred. Therefore, no Type 4 hypotheses were generated.</p> <p>Based on these findings, this assurance activity is considered satisfied.</p>
<p>Verdict</p>	<p>Pass</p>

8 CAVP Mapping

Each of these cryptographic algorithms have been validated as identified in the table below. Each algorithm runs on Intel® Xeon® E5-2600 v4 series, Intel® Xeon® E-2200M series CPU.

CAVP Algorithm Certificate References

SFR	Algorithm in ST	Implementation name	CAVP Alg.	CAVP Cert #
FCS_CKM.1	RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3	Junos OS 22.2R2 OpenSSL	RSA KeyGen	A3342
	ECC schemes using "NIST curves" [P-256, P-384, P-521] that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4	Junos OS 22.2R2 OpenSSL	ECDSA KeyGen	A3342
	FFC Schemes using 'safe-prime' groups that meet the following: "NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and [RFC 3526]	N/A	Tested with known good implementation.	N/A
FCS_CKM.1.1/IKE	FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3 for RSA schemes	Junos OS 22.2R2 OpenSSL	RSA KeyGen	A3342
	FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4 for ECDSA schemes and implementing "NIST curves" P-384 and [P-256]]	Junos OS 22.2R2 OpenSSL	ECDSA KeyGen	A3342
FCS_CKM.2	Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"	Junos OS 22.2R2 OpenSSL	KAS-ECC-SSC	A3342
	FFC Schemes using "safe-prime" groups that meet the following: "NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and [groups listed in RFC 3526]	N/A	Tested with known good implementation.	N/A
FCS_COP.1/ DataEncryption	AES used in [CBC, CTR, GCM] mode and cryptographic key sizes [128 bits, 192 bits, 256 bits]	Junos OS 22.2R2 Kernel	AES-CBC [128 bits, 192 bits, 256 bits]	A3335
		Junos OS 22.2R2 Dataplane	AES-CBC [128 bits, 192 bits, 256 bits]	A3339
			AES-GCM [128	

SFR	Algorithm in ST	Implementation name	CAVP Alg.	CAVP Cert #
			bits, 192 bits, 256 bits]	
		Junos OS 22.2R2 OpenSSL	AES-CBC [128 bits, 192 bits, 256 bits] AES-CTR [128 bits, 192 bits, 256 bits]	A3342
		Junos OS 22.2R2 Quicksec	AES-CBC [128 bits, 192 bits, 256 bits] AES-GCM [128 bits, 192 bits, 256 bits]	A3343
FCS_COP.1/ SigGen	RSA Digital Signature Algorithm and cryptographic key sizes (modulus) [2048 bits and 4096 bits] that meet the following: <ul style="list-style-type: none"> For RSA schemes: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3 	Junos OS 22.2R2 OpenSSL	RSA SigGen/SigVer	A3342
	Elliptic Curve Digital Signature Algorithm and cryptographic key sizes [256 bits and 384 bits] that meet the following: <ul style="list-style-type: none"> For ECDSA schemes: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 6 and Appendix D, Implementing "NIST curves" [P-256, P-384, P-521]; ISO/IEC 14888-3, Section 6.4 	Junos OS 22.2R2 OpenSSL	ECDSA SigGen/SigVer	A3342
FCS_COP.1/ Hash	cryptographic algorithm [SHA-1, SHA-256, SHA-384, SHA-512] and message digest sizes [160, 256, 384, 512] bits that meet the following: ISO/IEC 10118-3:2004.	Junos OS 22.2R2 Kernel	SHA-1, SHA2-256, SHA2-512	A3335
		Junos OS 22.2R2 Dataplane	SHA-1, SHA2-256, SHA2-384	A3339
		Junos OS 22.2R2 LibMD	SHA-1, SHA2-256, SHA2-512	A3340
		Junos OS 22.2R2 OpenSSL	SHA-1, SHA2-256, SHA2-384, SHA2-512	A3342
		Junos OS 22.2R2 Quicksec	SHA2-256, SHA2-384	A3343
FCS_COP.1/ KeyedHash	cryptographic algorithm [HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512] and cryptographic key	Junos OS 22.2R2 Kernel	HMAC-SHA-1 [160 bits]	A3335

SFR	Algorithm in ST	Implementation name	CAVP Alg.	CAVP Cert #
	sizes [160 bits, 256 bits, 384 bits and 512 bits] and message digest sizes [160, 256, 384, 512] bits that meet the following: ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”		HMAC-SHA2-256 [160 bits, 256 bits]	
		Junos OS 22.2R2 Dataplane	HMAC-SHA-1 [160 bits] HMAC-SHA2-256 [256 bits]	A3339
		Junos OS 22.2R2 LibMD	HMAC-SHA-1 [160 bits] HMAC-SHA2-256 [160 bits, 256 bits]	A3340
		Junos OS 22.2R2 OpenSSL	HMAC-SHA-1 [160 bits] HMAC-SHA2-256 [256 bits] HMAC-SHA2-512 [512 bits]	A3342
		Junos OS 22.2R2 Quicksec	HMAC-SHA2-256 [256 bits] HMAC-SHA2-384 [384 bits]	A3343
FCS_RBG_EXT.1	HMAC_DRBG (any)	Junos OS 22.2R2 Kernel	HMAC DRBG	A3335
		Junos OS 22.2R2 OpenSSL	HMAC DRBG	A3342
		Junos OS 22.2R2 Quicksec	HMAC DRBG	A3343

9 Conclusion

The testing shows that all test cases required for conformance have passed testing.

End of Document