Assurance Activity Report for

Cisco Identity Services Engine (ISE) V3.1

Cisco Identity Services Engine (ISE) V3.1 Security Target
Version 1.4

collaborative Protection Profile for Network Devices
Version 2.2e
Network Device Collaborative Protection Profile (NDcPP) Extended Package (EP) for Authentication Servers Version 1.0

AAR Version 0.3, 8 September 2023

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:
Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134

The Author of the Security Target:
Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134

The TOE Evaluation was Sponsored by:
Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134

Evaluation Personnel:
Acumen Security

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	11/07/2023	Initial Release
0.2	18/08/2023	Updated the ECR comments
0.3	09/08/2023	Updated CAVP table and doc versions

Contents

1 TOE Overview

The TOE is an identity and access control platform that enables organizations to enforce compliance and security within the network infrastructure. The TOE includes the following options: Cisco Identity Services Engine Appliance SNS-3595, Cisco Identity Services Engine Appliance SNS-3615, Cisco Identity Services Engine Appliance SNS-3655, Cisco Identity Services Engine Appliance SNS-3695 and Cisco Identity Services Engine Virtual Machine (ISE-VM) on ESXi 6.7/7.0 running on UCSC-C220-M5SX.

1.1 TOE Product Type

The Cisco Identity Services Engine (ISE) is a network device identity, authentication, and access control policy platform that enables enterprises to enforce compliance, enhance infrastructure security, and streamline service operations. ISE allows enterprises to gather real-time contextual information from networks, users, and devices. The administrator can then use that information to make proactive governance decisions by tying identity to various network elements including access switches, wireless LAN controllers (WLCs), virtual private network (VPN) gateways, and data center switches.

1.2 Supported Non-TOE Hardware/ Software/ Firmware

The TOE supports (in some cases optionally) the following hardware, software, and firmware in its environment:

Table 1: IT Environment Components

Component	Required	Usage/Purpose Description for TOE performance
Administrative Console	Yes	This console provides the connection to the ISE appliance for administration and management. The console can connect directly to ISE or over the network via a browser or SSHv2 connection. The TOE supports the following browsers: • Mozilla Firefox version 70 and later • Google Chrome version 78 and later • Microsoft Internet Explorer 11.x
Network Access Server (NAS)	Yes	Also known as the RADIUS Authenticator, the Network Access Server is used during the 802.1X authentication exchange to relay the supplicant authentication to the Authentication Server. The 802.1X frames carry EAP authentication packets which are passed through to the RADIUS Authentication Server.
Clients	Yes	The network devices that are provided authentication services by ISE are referred to as clients
Remote Authentication Store	No	The TOE supports local authentication or authentication via a remote authentication store, including LDAP and Active Directory.
Syslog Target	Yes	The TOE must offload syslogs to an external entity, which can be another iteration of ISE or a syslog server that supports TLS-protected transfer.

1.3 TOE DESCRIPTION

This section provides an overview of the Cisco Identity Services Engine (ISE) v3.1 Target of Evaluation (TOE) and a brief description of the capabilities of the ISE product. ISE is a consolidated policy-based access control system that combines authentication, authorization, accounting (AAA) and guest management in one appliance. ISE v3.1 software runs on the Cisco Application Deployment Engine (ADE) Release 3.1 operating system (ADE-OS). ADE-OS is a Cisco-proprietary Red Hat Enterprise Linux based Operating system [RHEL v8.2]

The TOE also includes an instance of the Embedded Services Router 5921 [ESR], running IOS 15.8(3)M7. The ESR is a software-only solution for routing capabilities. The ESR provides IPsec session capabilities for ISE v3.1 to secure the channel between the TOE and NAS. that includes the cryptographic module IOS Common Cryptographic Module (IC2M), runs as a process on the RHEL bundle included in the ADE-OS.

Network access has evolved beyond just simple user name and password verifications. Additional attributes related to users and their devices are used as decision criteria in determining authorized network access. Additionally, network service provisioning can be based on data such as the type of device accessing the network, including whether it is a corporate or personal device. Cisco ISE is a scalable solution that helps network administrators meet complex network access control demands by managing the many different operations that can place heavy loads on applications and servers, including:

- Authorization and authentication requests
- Queries to identity stores such as Active Directory and LDAP databases
- Device profiling and posture checking
- Enforcement actions to remove devices from the network
- Reporting

ISE delivers secure access control across wired, wireless, and VPN connections. ISE can reach deep into the network to deliver visibility into who and what are accessing resources. Through the device profiler feed service, ISE delivers automatic updates of Cisco's validated device profiles for various IP-enabled devices from multiple vendors which simplifies the task of keeping an up-to-date library of the newest IP enabled devices.

The Cisco Secure Network Server(SNS) is based on the Cisco UCS® C220 Rack Server and is configured specifically to support the Cisco Identity Services Engine (ISE) security application. The Secure Network Server supports these applications in five versions. The Cisco Secure Network Server 3615 is designed for small deployments. The Secure Network Servers 3595, 3655, and 3695 has several redundant components such as hard disks and power supplies, making it suitable for larger deployments that require highly reliable system configurations. The Secure Network Servers 3615, 3655, and 3695 are recommended for new installations whereas the Secure Network Server 3595 is recommended for existing installations.

Apart from the SNS models described above, ISE is also available as a Vitual Machine running on ESXi 6.7/7.0 on UCSC-C220-M5SX. Cisco ISE supports the following virtual environment platforms, but only the ESXi 6.7 and 7.0 environments are a part of the evaluated configuration:

- ESXi 6.7/7.0
- Microsoft Hyper-V on Microsoft Windows Server 2012 R2 and later
- KVM on RHEL 8.2

2 Assurance Activities Identification

The Assurance Activities contained within this document include all those defined within the NDcPPv2.2e and AUTHSVR_EP_V1.0 based upon the core SFRs and those implemented based on selections within the PPs/EPs.

3 Test Equivalency Justification

Cisco ISE is a consolidated policy-based access control system that incorporates a superset of features available in existing Cisco policy platforms. Cisco ISE performs the following functions: Combines authentication, authorization, accounting (AAA), posture, and profiler into one appliance.

Cisco ISE v3.1 software runs on the Cisco Application Deployment Engine (ADE) Release 3.1 operating system (ADE-OS). ADE-OS is a Cisco-proprietary Red Hat Enterprise Linux based Operating system [RHEL v8.2]. For routing capabilities, the TOE also features an Embedded Services Router 5921 [ESR] instance running IOS 15.8(3)M7. The ESR provides IPsec session capabilities for ISE v3.1 to secure communication between the TOE and NAS.

The TOE boundary consists of the following appliances listed below. The Cisco ISE 3595, 3615, 3655, AND 3695 are physical devices while the Cisco ISE VM is a virtual machine which runs on ESXi.

All of the possible TOE platforms are listed below:

TOE Models

Model	Software	Hypervisor	Processor	System Memory
Cisco ISE Appliance 3595	ISE v3.1 running on Cisco ADE-OS	None	Intel Xeon E5-2640 v3 (Haswell)	64 GB
Cisco ISE Appliance 3615	ISE v3.1 running on Cisco ADE-OS	None	Intel Xeon Silver 4110 (Skylake)	32 GB
Cisco ISE Appliance 3655	ISE v3.1 running on Cisco ADE-OS	None	Intel Xeon Silver 4116 (Skylake)	96 GB
Cisco ISE Appliance 3695	ISE v3.1 running on Cisco ADE-OS	None	Intel Xeon Silver 4116 (Skylake)	256 GB

3.1 OS, Processor, and Firmware Analysis

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

Table 3 – Image Analysis

TOE Model	Image	Analysis
SNS-3595	ISE v3.1, running on Cisco Application Deployment Engine (ADE) Release 3.1 operating system (ADE-OS)	TOE is the Cisco ISE 3500/3600 Series appliances, and all run identical Cisco Application Deployment Engine (ADE) Release 3.1 operating system (ADE-OS).

TOE Model	Image	Analysis
SNS-3695	ISE v3.1, running on Cisco Application Deployment Engine (ADE) Release 3.1 operating system (ADE-OS)	VERDICT: The Cisco ISE 3500 and 3600 series appliances share the ADE-OS operating system version ADE Release 3.1
SNS-3615	ISE v3.1, running on Cisco Application Deployment Engine (ADE) Release 3.1 operating system (ADE-OS)	
SNS-3655	ISE v3.1, running on Cisco Application Deployment Engine (ADE) Release 3.1 operating system (ADE-OS)	
Cisco ISE VM running on ESXi 6.7/7.0 on UCSC-C220-M5SX	ISE v3.1, running on Cisco Application Deployment Engine (ADE) Release 3.1 operating system (ADE-OS)	

Table 4 – Processor Analysis

TOE	Processor	Analysis
SNS-3595	Intel Xeon E5-2640 v3 (Haswell)	SNS-3595 has processor with Haswell microarchitecture. SNS-3615, SNS-3695, and SNS-3655 has processor with Skylake microarchitecture. ISE VM running on ESXi 6.7/7.0 has processor with Skylake microarchitecture
SNS-3615	Intel Xeon Silver 4110 (Skylake)	
SNS-3695	Intel Xeon Silver 4116 (Skylake)	
SNS-3655	Intel Xeon Silver 4116 (Skylake)	
Cisco ISE VM running on ESXi 6.7/7.0 on UCSC-C220-M5SX	Intel Xeon Silver 4116 (Skylake) w/Linux 4 on ESXi 6.7 Intel Xeon Silver 4116 (Skylake) w/Linux 4 on ESXi 7.0	

3.2 Specification of Differences

The following table provides 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.

Table 5 – TOE Models and Specification

Hardware Models	Cisco Identity Services Engine Appliance 3595 (SNS-3595)	Cisco Identity Services Engine Appliance 3615 (SNS-3615)	Cisco Identity Services Engine Appliance 3655 (SNS-3655)	Cisco Identity Services Engine Appliance 3695 (SNS-3695)	Cisco Identity Services Engine – VM running on ESXi 6.7and 7.0/UCSC-C220-M5SX (ISE-VM)
Processors	Intel Xeon E5-2640 v3 (Haswell)	Intel Xeon Silver 4110 (Skylake)	Intel Xeon Silver 4116 (Skylake)	Intel Xeon Silver 4116 (Skylake)	Intel Xeon Silver 4116 (Skylake)
Memory	64 GB	32 GB	96 GB	256 GB	96 GB
Hard disk	4x600Gb disk	1x600 Gb disk	4x600Gb disk	8x600Gb disk	4x600Gb disk
RAID	Yes (RAID 0+1)	No	Yes (RAID 1+0)	Yes (RAID 1+0)	Yes (RAID 1+0)
Expansion slots	- Two PCIe slots (on a riser card)	- Two PCIe slots (on a riser card)	- Two PCIe slots (on a riser card)	- Two PCIe slots (on a riser card)	- Two PCIe slots (on a riser card)
Serial port (RJ-45 Connector)	2	2	2	2	2
USB 2.0 ports	0	0	0	0	0
USB 3.0 ports	4	4	4	4	4
1-GB Ethernet Management Port	1	1	1	1	1
Video ports	2	2	2	2	2
Hypervisor	None	None	None	None	ESXi 6.7/7.0

3.3 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 observed will use the areas

and analysis description provided in the supporting documentation for the NDcPPv2.2e and AUTHSVR_EP_v1.0. 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.

3.3.1 Platform/Hardware Dependencies

The TOE chassis includes varying form factors. Although the chassis may differ, it does not affect the functionality of the TOE. The processor is Intel Xeon E5 (Haswell) or Intel Xeon Silver (Skylake) Processor. The chassis for ISE VM is C220M5SX which has the Intel Xeon Silver (Skylake) Processor with ESXi 6.7/7.0 hypervisor running.

Result:

There are no hardware dependencies apart from the processor.

SNS-3595 has processor with Haswell microarchitecture and hence will be tested.

SNS-3615, SNS-3695, and SNS-3655 has processor with Skylake microarchitecture. Hence, they are equivalent and just one out of the three will be tested

ISE VM running on ESXi 6.7 and ISE VM running on ESXi 7.0 has processor with Skylake microarchitecture. Hence, they are equivalent and just one out of two will be tested.

3.3.2 Software/OS Dependencies

The underlying OS is installed with the application-level software on each of the devices. The ISE software runs on the Cisco Application Deployment Engine (ADE) Release 3.1 operating system (ADE-OS). The Cisco ASE-OS and the Cisco ISE software run on a dedicated Cisco ISE 3500/3600 Series appliances and on ESXi 6.7/ 7 running on Cisco UCS C220-M5SX (UCSC-C220-M5SX). All models include the same security functionality. There are no specific dependencies on the OS since the TOE will not be installed on different OS.

Result:

- There are no differences in the OS.
- All ISE Appliances are equivalent.

3.3.3 Differences in Libraries Used to Provide TOE Functionality:

All software binaries compiled in the TOE software are identical including the version of the library regardless of the platform for which the software is compiled. There are no differences between the included libraries.

Result:

- There are no differences in the included libraries.
- All ISE Appliances are equivalent.

3.3.4 TOE Management Interface Differences:

The TOE is managed via remote CLI session or remote GUI 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

3.3.5 TOE Functional Differences:

Each hardware model within the TOE boundary provides identical functionality. There is no difference in the way the user interacts with each of the devices or the services that are available to the user in for each of these devices. Each device runs the same version of ISE v3.1 software. For ISE v3.1 software, differences in the provided functionality are denoted by a different version of the software. If there had been differences in the functionality provided by the software, the actual release version would have been different for the platform.

Result: All platforms are equivalent

3.3.6 Difference Comparison:

All platforms run the same software and perform identical functionality. All platforms use identical processors. The only security relevant difference for each platform is the base CPU. Each family of platform includes a separate processor.

3.4 Recommendations/Conclusions

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

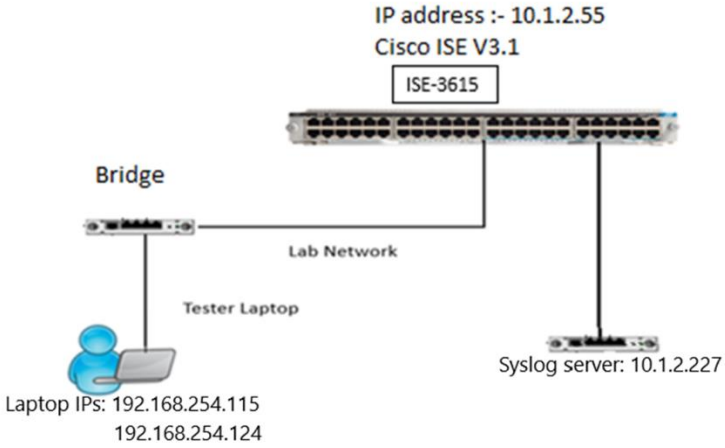
- Cisco ISE 3595, ISE 3615 and ISE VM running on ESXi 6.7 on UCSC-C220-M5SX

- Note: A full suite of testing will be performed Cisco ISE 3595, ISE 3615 and VM running on ESXi 6.7 on UCSC-C220-M5SX the running on cisco ISE software. This shall provide enough assurance that the TOE functionality executes identically regardless of the underlying platform.

4 Test Bed Descriptions

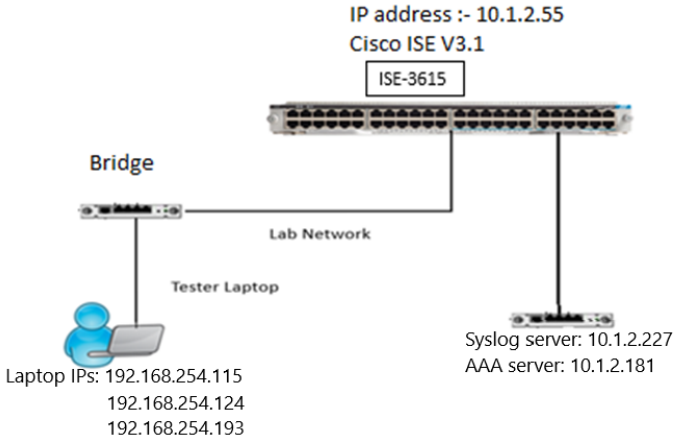
4.1 Test Bed (Cisco ISE 3615)

4.1.1 Audit



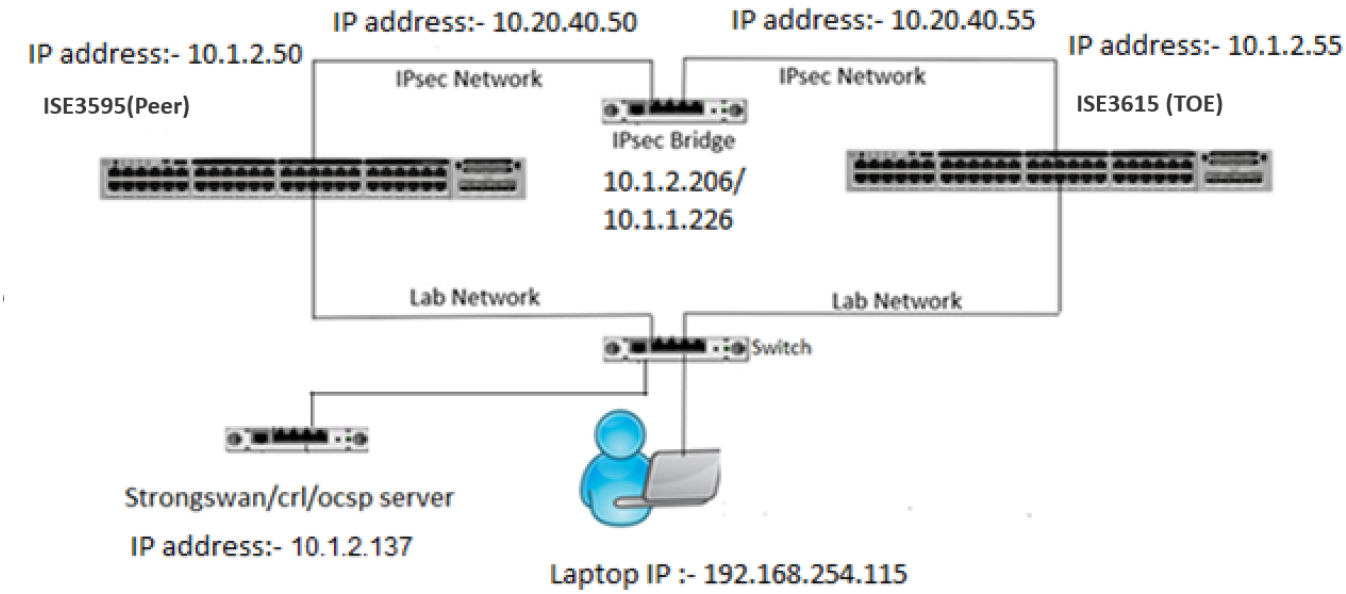
Device Name	IP Address/Hostname	Relevance to Testing
Cisco ISE3615	10.1.2.55	TOE -Physical Device
Tester Laptop	192.168.254.115 / 192.168.254.124	Test PC -Physical Device
Syslog Server	10.1.2.227	Test PC, Syslog Server- Virtual Device

4.1.2 Auth



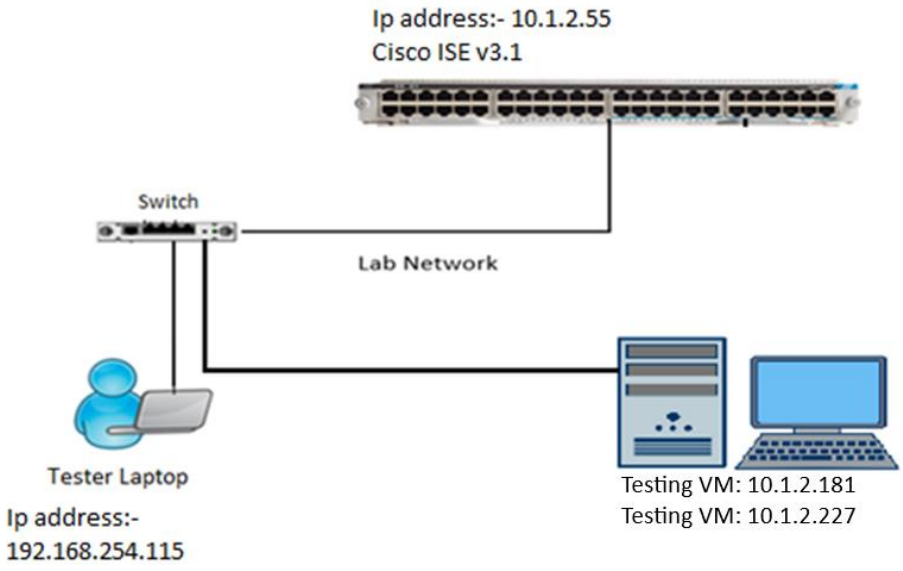
Device Name	IP Address/Hostname	Relevance to Testing
Cisco ISE3615	10.1.2.55	TOE -Physical Device
Tester Laptops	192.168.254.115 / 192.168.254.124 / 192.168.254.193	Test PC -Physical Device
Syslog /AAA server	10.1.2.227 / 10.1.2.181	Test PC, Syslog Server- Virtual Device

4.1.3 IPsec



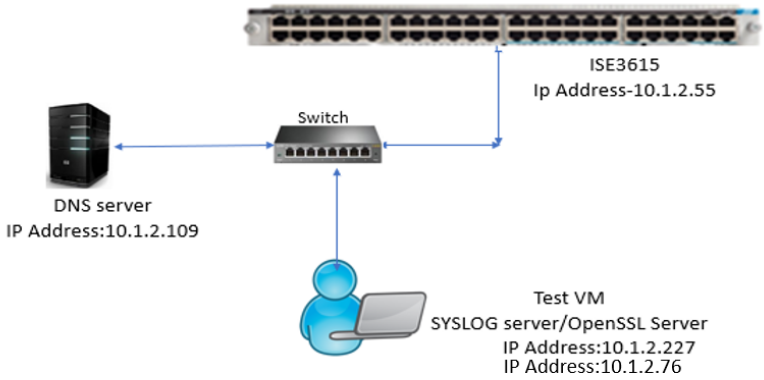
Device Name	IP Address/Hostname	Relevance to Testing
CISCO ISE 3615	10.1.2.55	TOE – Physical Device
	10.20.40.55	IPSEC IP
CISCO ISE 3595	10.1.2.50	Peer – Virtual Device
	10.20.40.50	Peer IPSEC IP
Tester Laptop	192.168.254.115	Ubuntu Server– Virtual Device
Test Server	10.1.2.137	Strongswan/CRL/OCSP server – Virtual Device
Bridge	10.1.2.206 10.1.1.226	Raspberry pi

4.1.4 SSHS



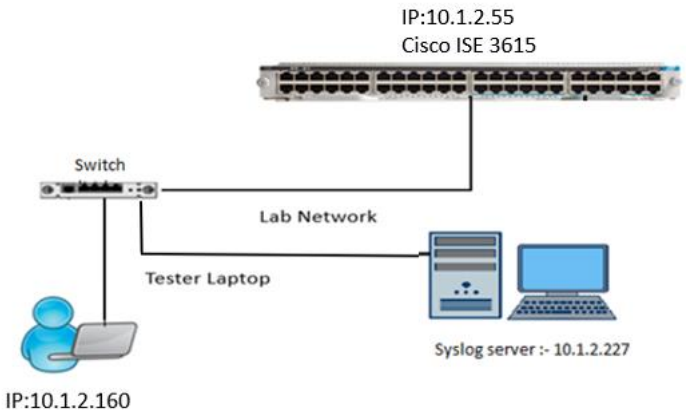
Device Name	IP Address/Hostname	Relevance to Testing
Cisco ISE 3615	10.1.2.55	TOE – Physical Device
Tester Laptop	192.168.254.115	Test PC – Physical Device
Server	10.1.2.181	Testing VM – Virtual Device
Server	10.1.2.227	Testing VM – Virtual Device

4.1.5 TLSC



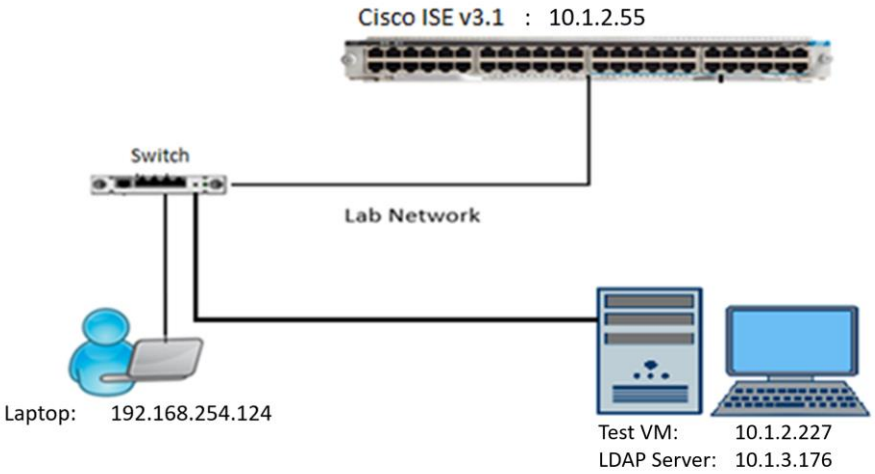
Device Name	IP Address/Hostname	Relevance to Testing
CISCO ISE3615	10.1.2.55	TOE – Physical Device
Test VM	10.1.2.227/10.1.2.76	Syslog Server – Virtual Device
DNS Server	10.1.2.109	DNS Server

4.1.6 TLSS



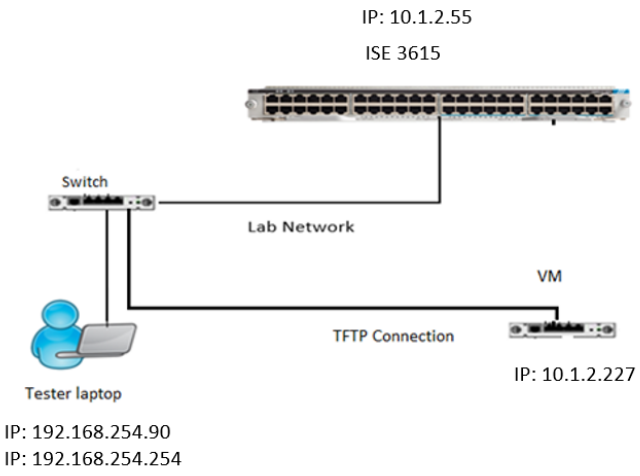
Device Name	IP Address/Hostname	Relevance to Testing
CISCO ISE 3615	10.1.2.55	TOE – Physical Device
Server	10.1.2.227	Syslog Server – Virtual Device
Tester Laptop	10.1.2.160	Test Laptop - Physical Device

4.1.7 TLSS-MA



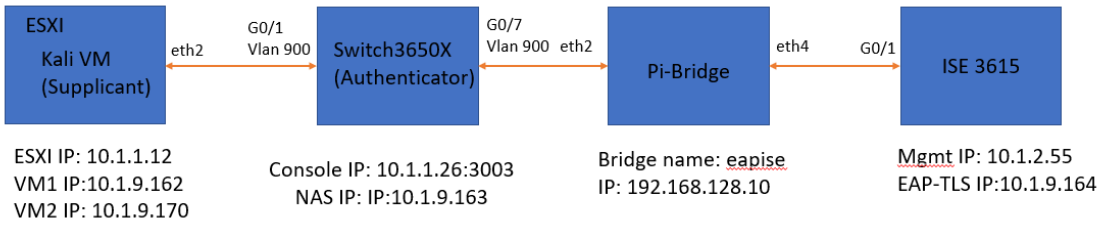
Device Name	IP Address/Hostname	Relevance to Testing
CISCO ISE 3615	10.1.2.55	TOE – Physical Device
isesyslog	10.1.2.227	Test VM – Virtual Device
Winsrv_Rodrigo	10.1.3.176	LDAP Server – Virtual Device
Tester Laptop	192.168.254.124	Test Laptop - Physical Device

4.1.8 Update



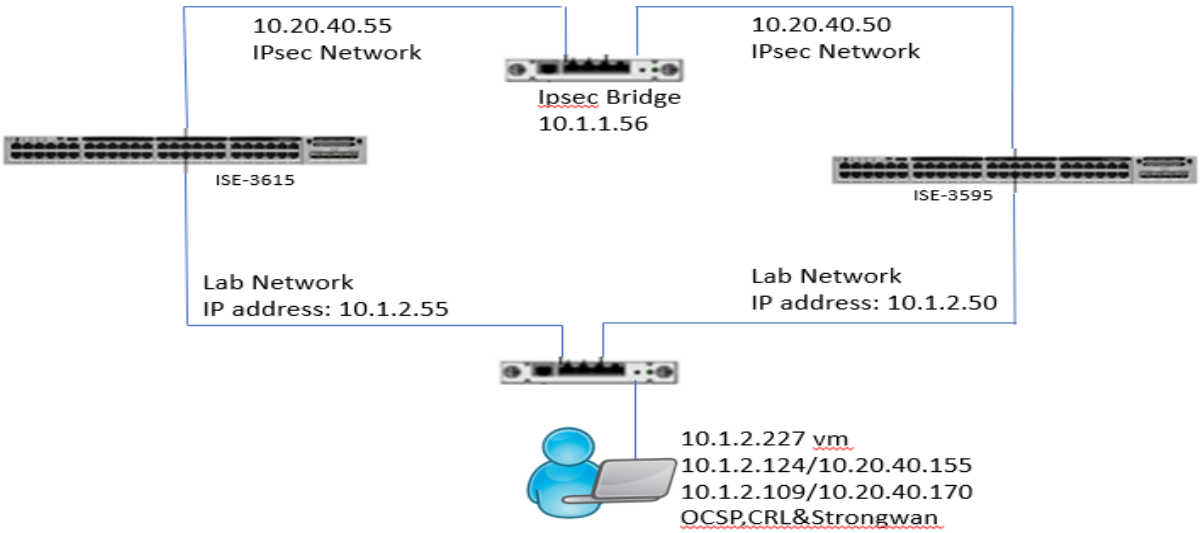
Device Name	IP Address/Hostname	Relevance to Testing
CISCO ISE3615	10.1.2.55	TOE - Physical Device
Tester Laptop	192.168.254.90	Test PC - Physical Device
VM	10.1.2.227	Test - Virtual device
Tester Laptop	192.168.254.254	Test PC - Physical Device

4.1.9 VPN Auth



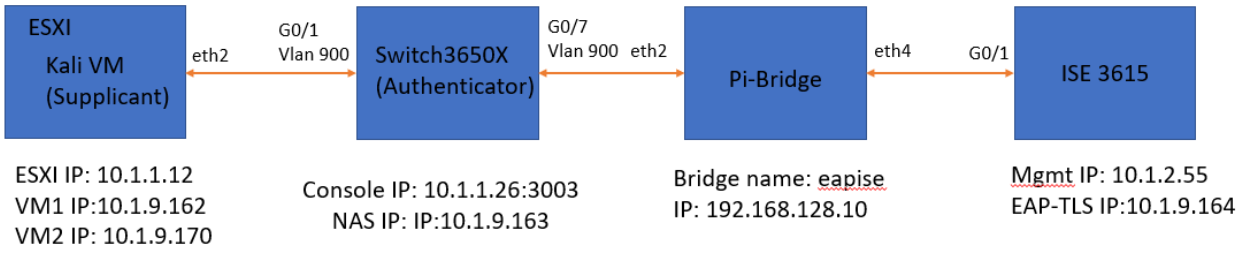
Device Name	IP Address/Hostname	Relevance to Testing
CISCO ISE3615	10.1.2.55/10.1.9.164	TOE- Physical Device
Tester Laptop	10.1.9.162/10.1.9.170	Test PC - Physical Device
Switch 3650X	10.1.1.26:3003/10.1.9.163	Switch - Physical Device
Pi-Bridge	192.168.128.10	RasberryPi – Physical Device

4.1.10 X509-Rev



Device Name	IP Address/Hostname	Relevance to Testing
CISCO ISE 3615	10.1.2.55/10.20.40.55	TOE – Physical Device
CISCO ISE 3595	10.1.2.50/10.20.40.50	Peer – Physical Device
CISCO ISE VM	10.1.2.136/10.20.40.136	Peer- Virtual Device
OCSP server/Strongwan	10.1.2.124/10.20.40.155	Ubuntu Server – Virtual Device
CRL server	10.1.2.109/10.20.40.170	Linux server-Virtual server
Syslog server	10.1.2.227	Linux server-Virtual server

4.1.11 EAP



Device Name	IP Address/Hostname	Relevance to Testing
CISCO ISE3615	10.1.2.55/10.1.9.164	TOE- Physical Device
Tester Laptop	10.1.9.162/10.1.9.170	Test PC - Physical Device
Switch 3650X	10.1.1.26:3003/10.1.9.163	Switch - Physical Device
Pi-Bridge	192.168.128.10	RasberryPi – Physical Device

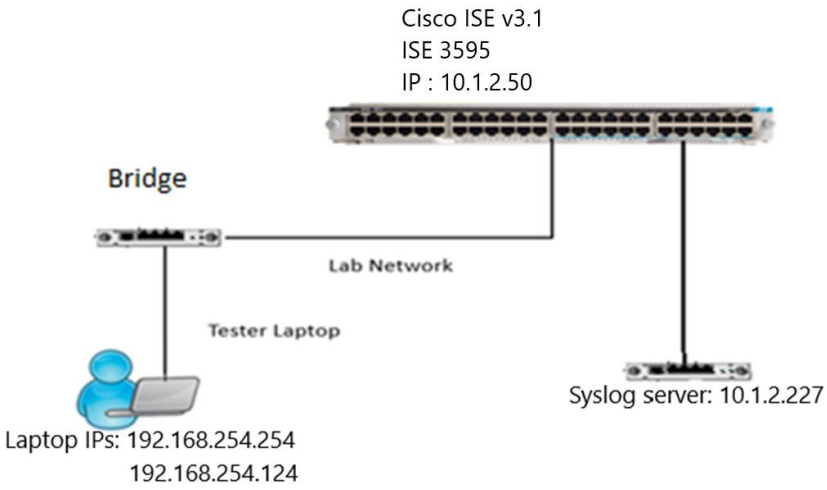
4.1.12 Test Bed Details

Name	OS	Function	Protocols	IP address	MAC Address	Time	Tools (version)
Cisco ISE 3615	ISEv3.1	TOE – Physical Device	IPsec, SSH, TFTP, OCSP, HTTPS	10.1.2.55 10.1.9.164	bia 70ea.1afb.ad0f	Manually set and verified	N/A
Server	Ubuntu 20.04.6 LTS	Testing VM – Virtual Device	IPsec, SSH, TFTP, OCSP, SCP	10.1.2.181	bia c014.fe60.b780	Manually set and verified	OpenSSL (1.1.0f), OpenSSH (8.6), Tcpdump (4.9.3) AcumenStrongswan Mod (5.6.2) Rsyslog (8.2106.0) Acumen SSHS () RADIUS Server 3.0
Server	Ubuntu 20.04.6 LTS	Testing VM – Virtual Device	IPsec, SSH, TFTP, OCSP, SCP	10.1.2.227	00:0c:29:d8:7f:39	Manually set and verified	OpenSSL (1.1.0f), OpenSSH (8.6), Tcpdump (4.9.3) AcumenStrongswan Mod (5.6.2) Rsyslog (8.2106.0) Acumen SSHS () RADIUS Server 3.0
ESXI	•	Virtualization Software.	HTTPS	10.1.1.12	N/A	N/A	N/A
Pi-Bridge	Raspbian GNU/Linux 11 (bullseye)	RasberryPi – Physical Device	IP	192.168.128.10	b8:27:eb:b9:af:a2	Manually set and verified	Tcpdump (4.9.3)
Switch 3650X	IOS v15.2	Switch - Physical Device	Ipsec, RADIUS,SSH	10.1.1.26:3003/10.1.9.163	bia d0d0.fdef.3b45	Manually set and verified	N/A
Tester Laptop	Windows 10 Pro 64 bit	Test PC – Physical Device	SSH, HTTPS, SCP,	192.168.254.115 10.1.2.160 192.168.254.90	28-7F-CF-23-A6-86	Manually set and verified	Putty (0.70), Wireshark (3.0.3), WinSCP (5.17), XCA (2.1.1) Firefox (89.0.2), Hex editor(2.5.0.0)

Name	OS	Function	Protocols	IP address	MAC Address	Time	Tools (version)
				192.168.254.254 10.1.9.162/10.1.9.170 192.168.254.108			

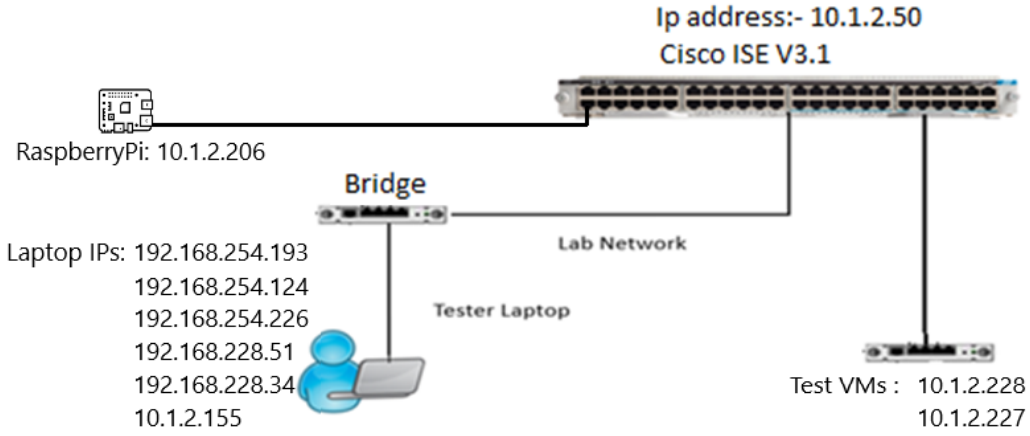
4.2 Test Bed (Cisco ISE 3595)

4.2.1 Audit



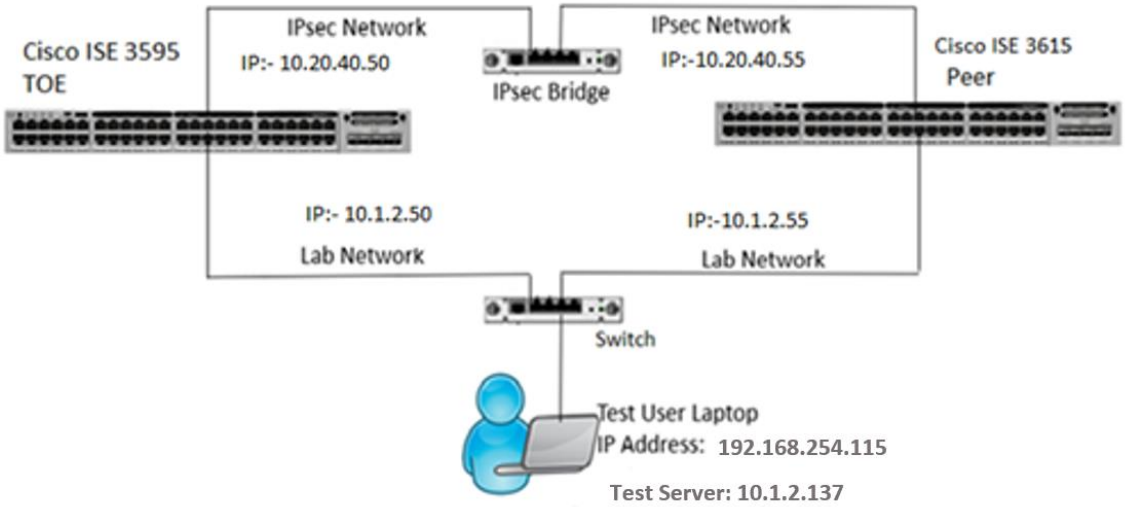
Device Name	IP Address/Hostname	Relevance to Testing
Cisco ISE3595	10.1.2.50	TOE -Physical Device
Tester Laptop	192.168.254.254 / 192.168.254.124	Test PC -Physical Device
Syslog Server	10.1.2.227	Test PC, Syslog Server- Virtual Device

4.2.2 Auth



Device Name	IP Address/Hostname	Relevance to Testing
Cisco ISE 3595	10.1.2.50	TOE – Physical Device
Tester Laptop	192.168.254.193 / 192.168.254.124 192.168.254.226 / 192.168.228.51 192.168.228.34 / 10.1.2.155	Test PC – Physical Device
Radius **Syslog**	10.1.2.228 10.1.2.227	Testing VM – Virtual Device
Raspberry Pi	10.1.2.206	Raspberry Pi – Physical device

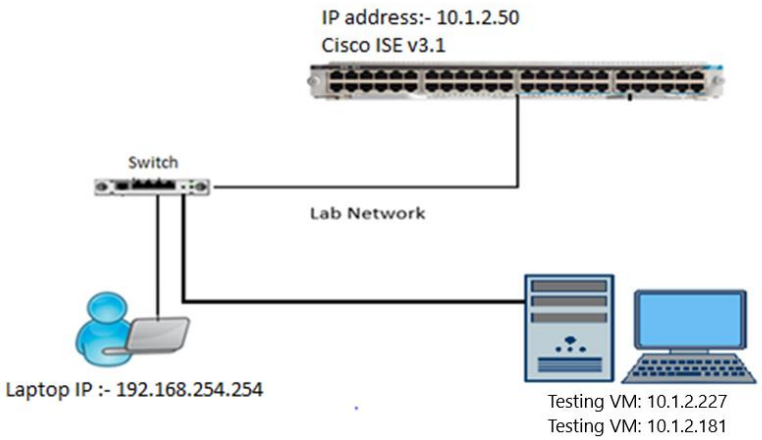
4.2.3 IPsec



Device Name	IP Address/Hostname	Relevance to Testing
CISCO ISE 3595	10.1.2.50	TOE – Physical Device
	10.20.40.50	IPSEC IP
CISCO ISE 3615	10.1.2.55	Peer – Virtual Device
	10.20.40.55	Peer IPSEC IP

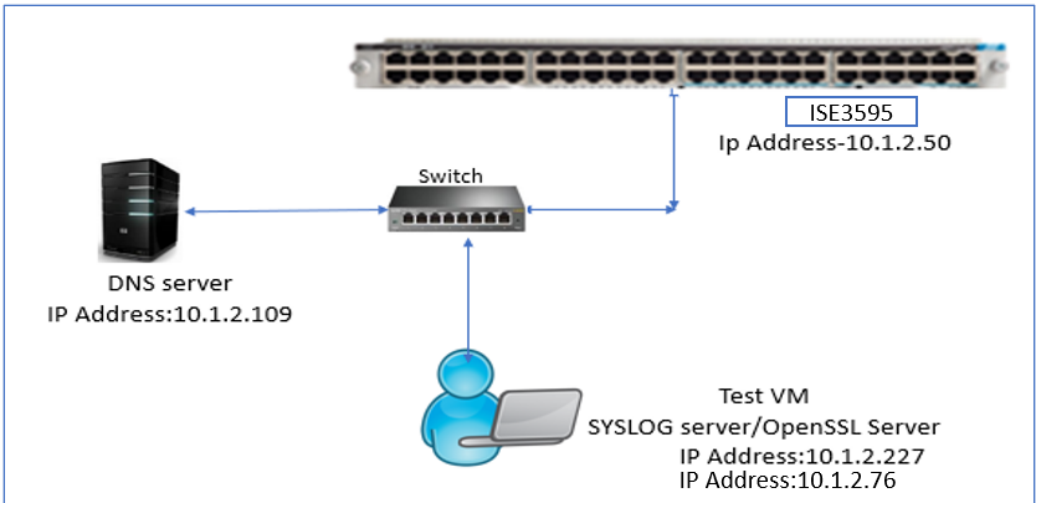
Tester Laptop	192.168.254.115	Ubuntu Server– Virtual Device
Test Server	10.1.2.137	Strongswan/CRL/OCSP server – Virtual Device

4.2.4 SSHS



Device Name	IP Address/Hostname	Relevance to Testing
Cisco ISE 3595	10.1.2.50	TOE – Physical Device
Tester Laptop	192.168.254.254	Test PC – Physical Device
Server	10.1.2.227	Testing VM – Virtual Device
Server	10.1.2.181	Testing VM – Virtual Device

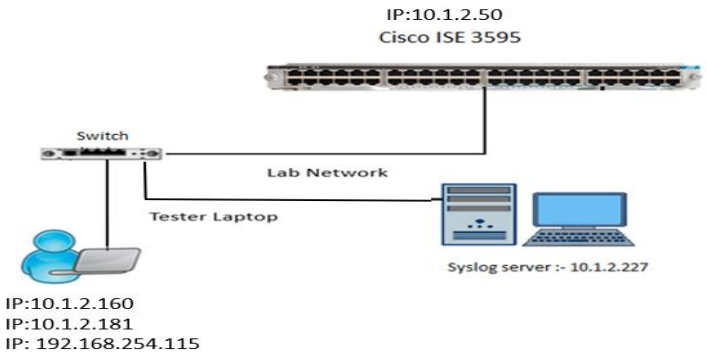
4.2.5 TLSC



Device Name	IP Address/Hostname	Relevance to Testing
CISCO ISE3615	10.1.2.50	TOE – Physical Device
Test VM	10.1.2.227/10.1.2.76	Syslog Server – Virtual Device

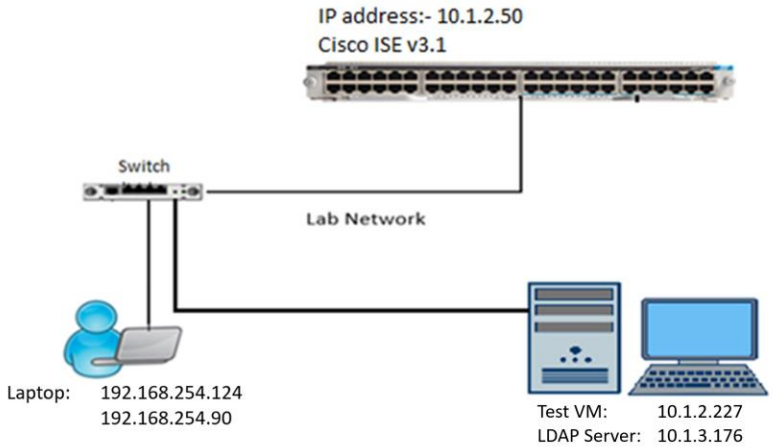
DNS Server	10.1.2.109	DNS Server

4.2.6 TLSS



Device Name	IP Address/Hostname	Relevance to Testing
CISCO ISE 3595	10.1.2.50	TOE – Physical Device
Server	10.1.2.227	Syslog Server – Virtual Device
Tester Laptop	192.168.254.115	Test Laptop - Physical Device
Tester Laptop	10.1.2.160	Test Laptop - Physical Device
Tester Laptop	10.1.2.181	Test Laptop - Physical Device

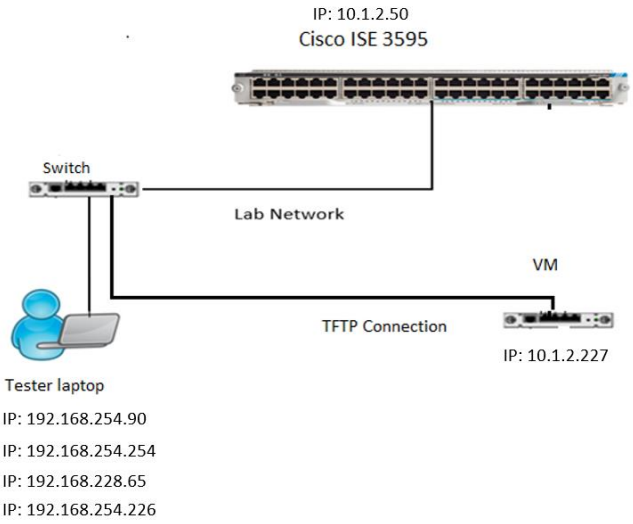
4.2.7 TLSS-MA



Device Name	IP Address/Hostname	Relevance to Testing
Cisco ISE 3595	10.1.2.50	TOE – Physical Device

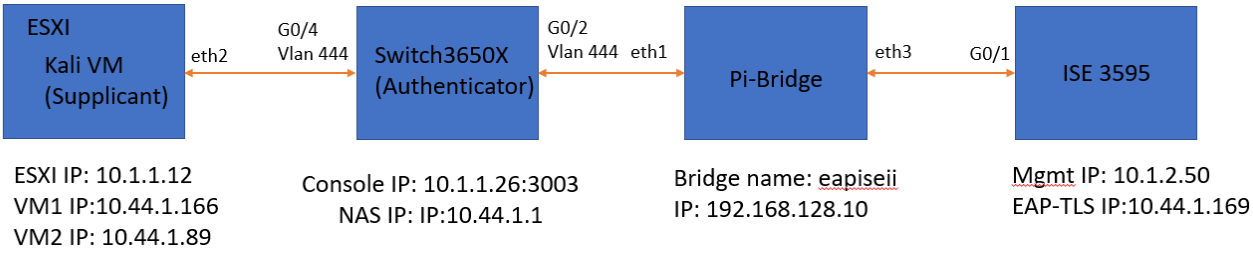
Tester Laptop	192.168.254.124 192.168.254.90	Test PC – Physical Device
Winsrv_Rodrigo	10.1.3.176	LDAP Server – Virtual Device
isesyslog	10.1.2.227	Test VM – Virtual Device

4.2.8 Update



Device Name	IP Address/Hostname	Relevance to Testing
CISCO ISE3595	10.1.2.50	TOE -Physical Device
Tester Laptop	192.168.254.90	Tester Laptop
VM	10.1.2.227	Test- Virtual device
Tester Laptop	192.168.254.254	Tester Laptop
Tester Laptop	192.168.228.65	Tester Laptop
Tester Laptop	192.168.254.226	Tester Laptop

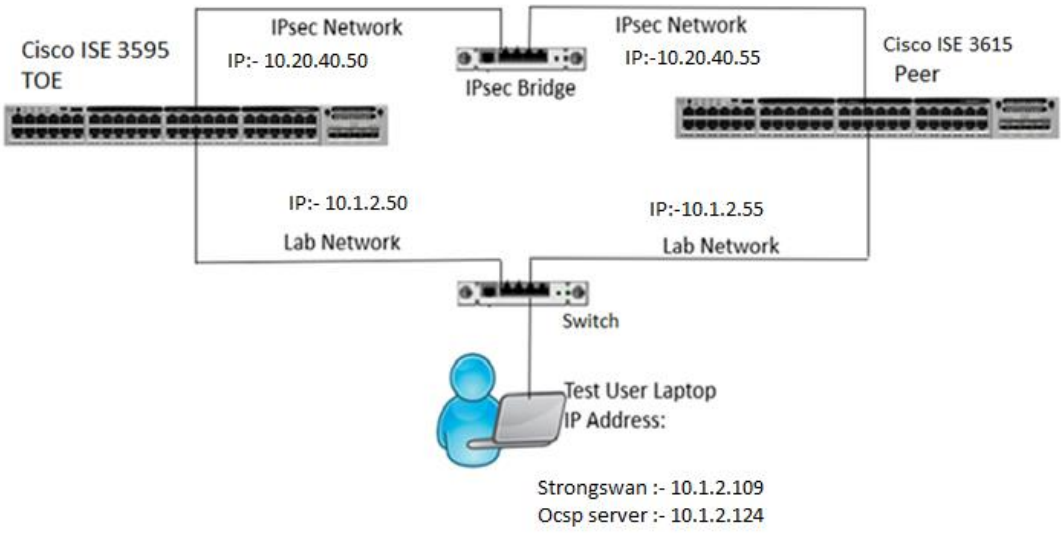
4.2.9 VPN Auth



Device Name	IP Address/Hostname	Relevance to Testing
CISCO ISE3595	10.1.2.50/10.44.1.169	TOE- Physical Device

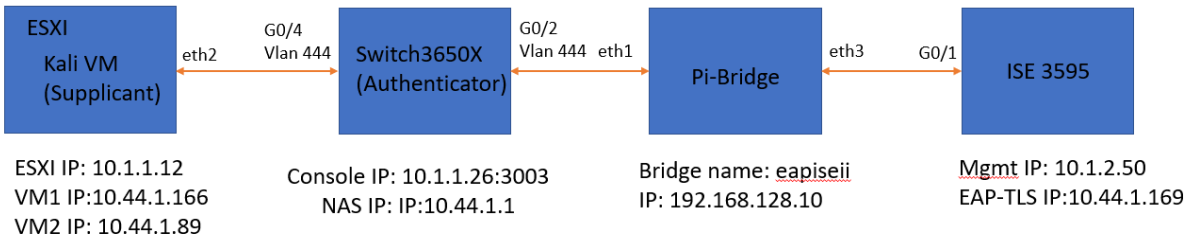
Tester Laptop	10.44.1.166/10.44.1.89	Test PC - Physical Device
Switch 3650X	10.1.1.26:3003/10.44.1.1	Switch - Physical Device
Pi-Bridge	192.168.128.10	Raspberry Pi – Physical Device

4.2.10 X509-Rev



Device Name	IP Address/Hostname	Relevance to Testing
CISCO ISE 3595	10.1.2.50/10.20.40.50	TOE – Physical Device
CISCO ISE 3615	10.1.2.55/10.20.40.55	Peer – Physical Device
OCSP server	10.1.2.124/10.20.40.155	Ubuntu Server – Virtual Device
Strong swan/CRL server	10.1.2.109/10.20.40.170	Linux server-Virtual server
Syslog server	10.1.2.227	Linux server-Virtual server

4.2.11 EAP



Device Name	IP Address/Hostname	Relevance to Testing
CISCO ISE3595	10.1.2.50/10.44.1.169	TOE- Physical Device
Tester Laptop	10.44.1.166/10.44.1.89	Test PC - Physical Device
Switch 3650X	10.1.1.26:3003/10.44.1.1	Switch - Physical Device

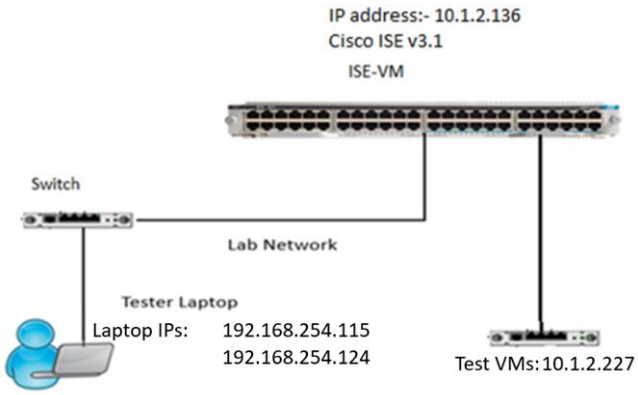
Pi-Bridge	192.168.128.10	Raspberry Pi – Physical Device

4.2.12 Test Bed Details

Name	OS	Function	Protocols	IP address	MAC Address	Time	Tools (version)
Cisco ISE 3595 TOE	ISEv3.1	TOE – Physical Device	IPsec, SSH, TFTP, OCSP, HTTPS	10.1.2.50 / 10.44.1.169	bia 0062.ec15.5167	Manually set and verified	N/A
Server	Ubuntu 20.04.6 LTS	Testing VM – Virtual Device	IPsec, SSH, TFTP, OCSP, SCP	10.1.2.227	00:0c:29:d8:7f:39	Manually set and verified	OpenSSL (1.1.0f), OpenSSH (8.6), Tcpdump (4.9.3) AcumenStrongswan Mod (5.6.2) Rsyslog (8.2106.0) Acumen SSHS () RADIUS Server 3.0
Server	Ubuntu 20.04.6 LTS	Testing VM – Virtual Device	IPsec, SSH, TFTP, OCSP, SCP	10.1.2.181	bia c014.fe60.b780	Manually set and verified	OpenSSL (1.1.0f), OpenSSH (8.6), Tcpdump (4.9.3) AcumenStrongswan Mod (5.6.2) Rsyslog (8.2106.0) Acumen SSHS () RADIUS Server 3.0
Switch 3650X	IOS v15.2	Switch - Physical Device	Ipsec, RADIUS,SSH	10.1.1.26:3003 /10.44.1.1	bia d0d0.fdef.3b45	Manually set and verified	N/A
Pi-Bridge	Raspbian GNU/Linux 11 (bullseye)	Raspberry Pi – Physical Device	IP	192.168.128.10	b8:27:eb:b9:af:a2	Manually set and verified	Tcpdump (4.9.3)
ESXI	7.0.2	Virtualization Software.	HTTPS	10.1.1.12	N/A	N/A	N/A
Tester Laptop	Windows 10 Pro 64 bit	Test PC – Physical Device	SSH, HTTPS, SCP,	192.168.254.254 192.168.254.115 10.1.2.160 10.1.2.181 192.168.228.65 192.168.254.226 192.168.254.90 10.44.1.166/ 10.44.1.89	28-7F-CF-23-A6-86	Manually set and verified	Putty (0.70), Wireshark (3.0.3), WinSCP (5.17), XCA (2.1.1) Firefox (89.0.2), Hex editor(2.5.0.0)

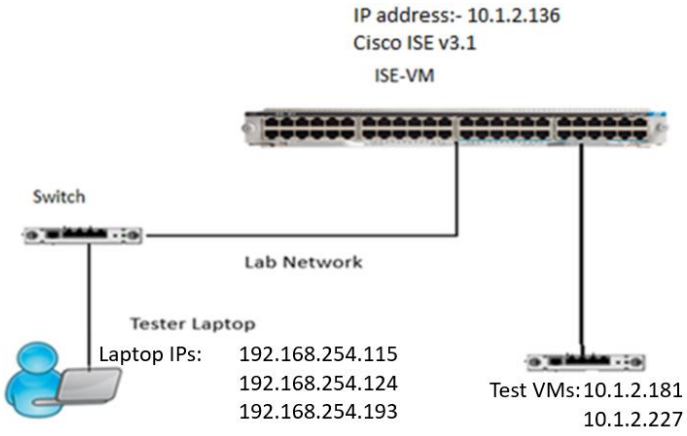
4.3 Test Bed (Cisco ISE VM)

4.3.1 Audit



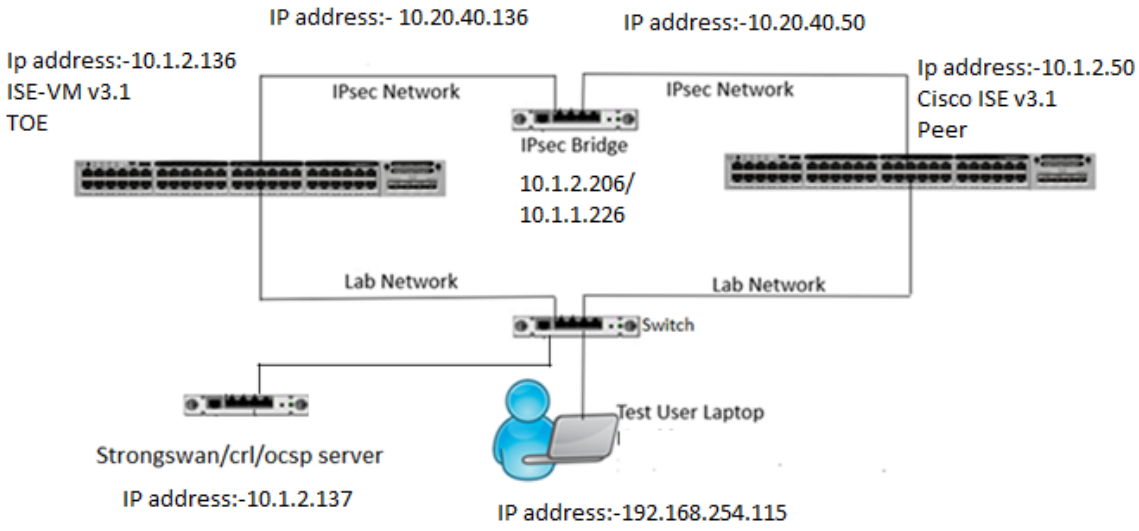
Device Name	IP Address/Hostname	Relevance to Testing
Cisco ISE-VM	10.1.2.136	TOE – Virtual Device
Tester Laptop	192.168.254.115 / 192.168.254.124	Test PC -Physical Device
Syslog Server	10.1.2.227	Test PC, Syslog Server- Virtual Device

4.3.2 Auth



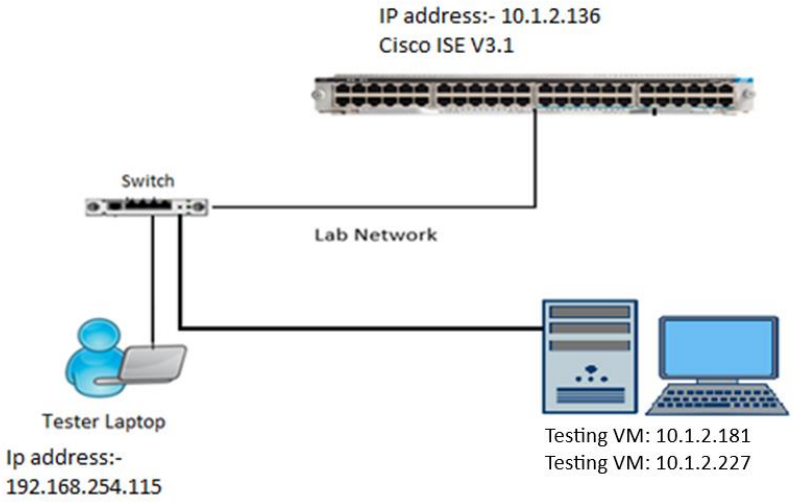
Device Name	IP Address/Hostname	Relevance to Testing
ISE-VM	10.1.2.136	TOE -Virtual Device
Tester Laptop	192.168.254.115 / 192.168.254.124 192.168.254.193	Test PC -Physical Device
Syslog, System	10.1.2.181 / 10.1.2.227	Test VM- Virtual Device

4.3.3 IPsec



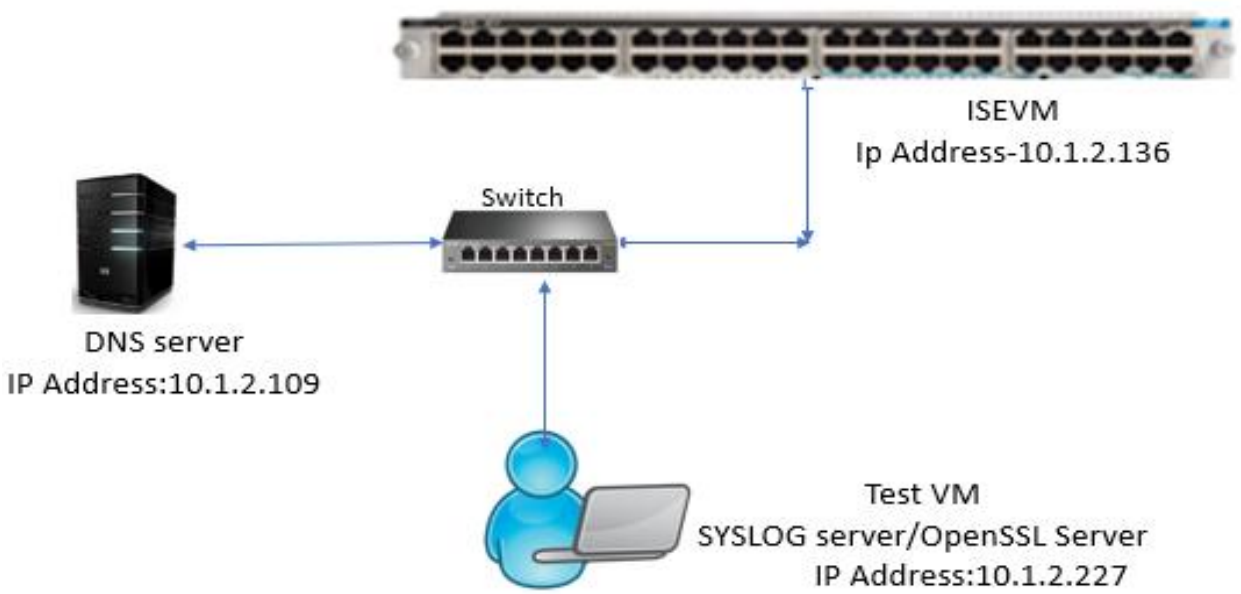
Device Name	IP Address/Hostname	Relevance to Testing
Cisco ISE-VM	10.1.2.136	TOE – Virtual Device
	10.20.40.136	IPSEC IP
CISCO ISE 3595	10.1.2.50	Peer – Virtual Device
	10.20.40.50	Peer IPSEC IP
Tester Laptop	192.168.254.115	Ubuntu Server– Virtual Device
Test Server	10.1.2.137	Strongswan/CRL/OCSP server – Virtual Device
Bridge	10.1.2.206/10.1.1.226	Raspberry pi

4.3.4 SSHS



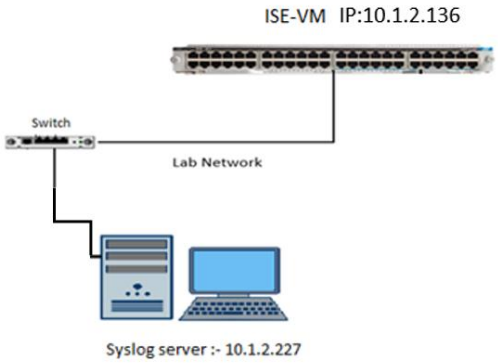
Device Name	IP Address/Hostname	Relevance to Testing
Cisco ISE-VM	10.1.2.136	TOE – Virtual Device
Tester Laptop	192.168.254.115	Test PC – Physical Device
Server	10.1.2.181	Testing VM – Virtual Device
Server	10.1.2.227	Testing VM – Virtual Device

4.3.5 TLSC



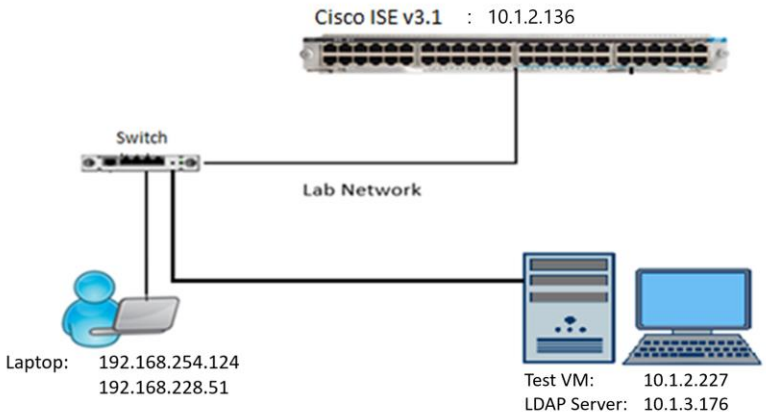
Device Name	IP Address/Hostname	Relevance to Testing
CISCO ISE -VM	10.1.2.136	TOE – Virtual Device
Test VM	10.1.2.227	Syslog Server – Virtual Device
DNS Server	10.1.2.109	DNS Server

4.3.6 TLSS



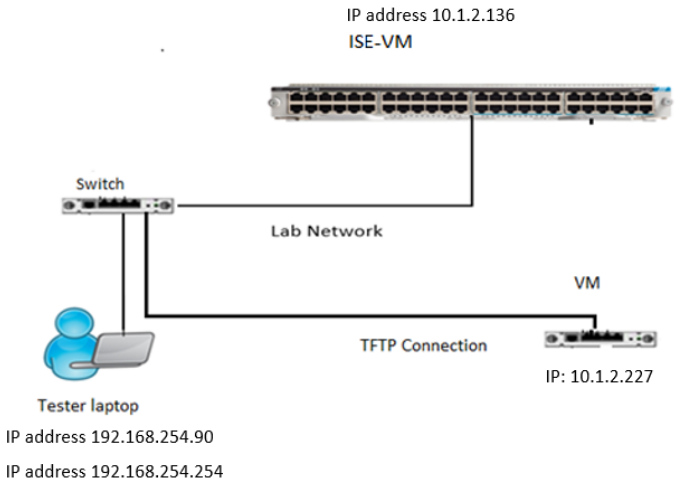
Device Name	IP Address/Hostname	Relevance to Testing
CISCO ISE -VM	10.1.2.136	TOE – Virtual Device
Server	10.1.2.227	Syslog Server – Virtual Device

4.3.7 TLSS-MA



Device Name	IP Address/Hostname	Relevance to Testing
CISCO ISE -VM	10.1.2.136	TOE – Virtual Device
isesyslog	10.1.2.227	Test VM – Virtual Device
Winsrv_Rodrigo	10.1.3.176	LDAP Server – Virtual Device
Tester Laptop	192.168.254.124 192.168.228.51	Test Laptop - Physical Device

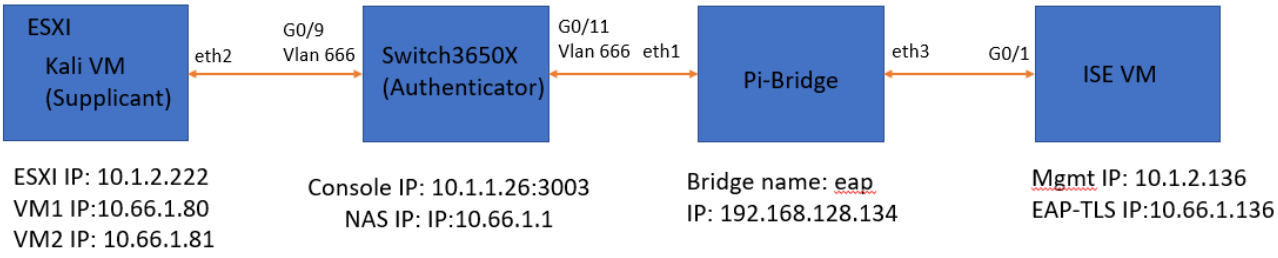
4.3.8 Update



Device Name	IP Address/Hostname	Relevance to Testing
CISCO ISE-VM	10.1.2.136	TOE -Virtual Device
Tester Laptop	192.168.254.90	Test PC-Physical Device
VM	10.1.2.227	Test- Virtual device

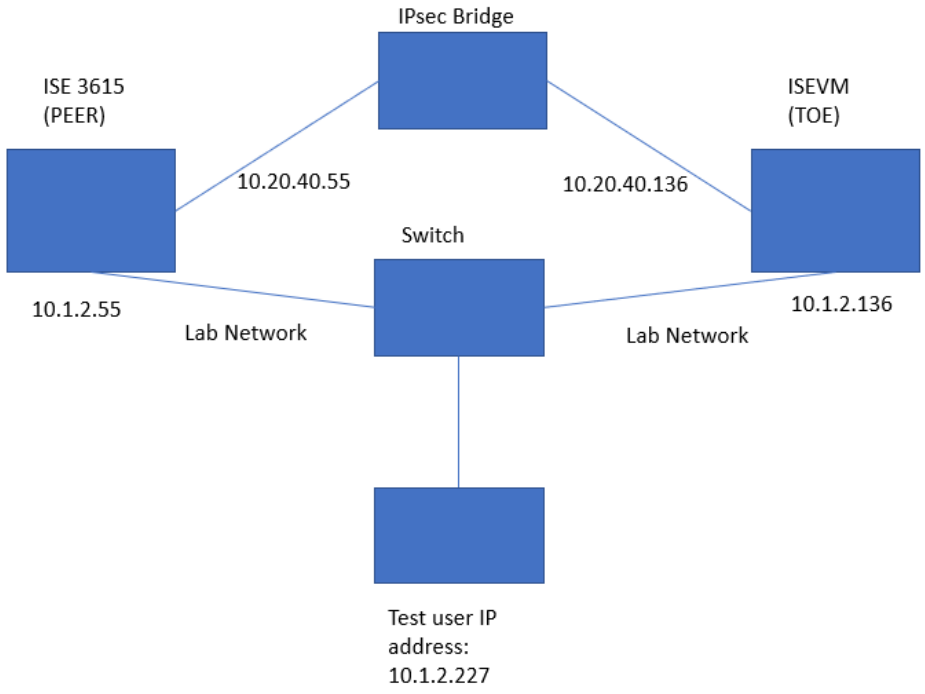
Tester Laptop	192.168.254.254	Test PC-Physical Device

4.3.9 VPN Auth



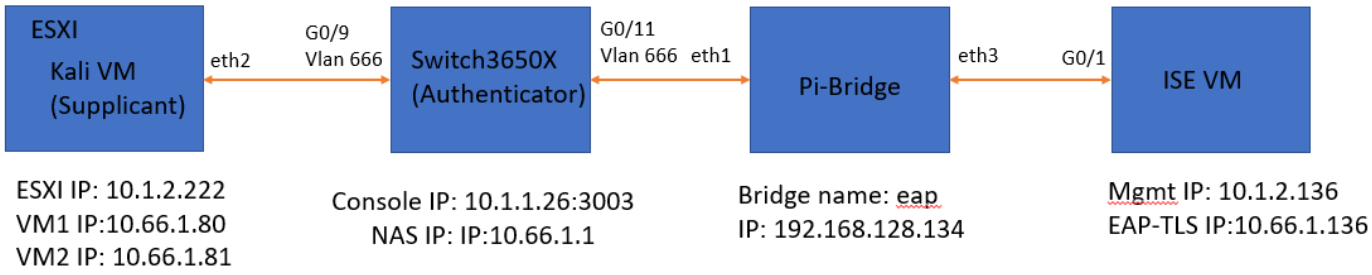
Device Name	IP Address/Hostname	Relevance to Testing
CISCO ISE3615	10.1.2.136/10.66.1.136	TOE- Virtual Device
Tester Laptop	10.66.1.80/10.66.1.81	Test PC - Physical Device
Switch 3650X	10.1.1.26:3003/10.66.1.1	Switch - Physical Device
Pi-Bridge	192.168.128.134	RasberryPi – Physical Device

4.3.10 X509-Rev



Device Name	IP Address/Hostname	Relevance to Testing
CISCO ISE -VM	10.1.2.136	TOE – Virtual Device
CISCO ISE 3615	10.1.2.55	Peer – Physical Device
CRL/OCSP Server	10.1.2.227	Ubuntu Server – Virtual Device
Tester Laptop	10.1.2.227	Ubuntu Server – Virtual Device

4.3.11 EAP



Device Name	IP Address/Hostname	Relevance to Testing
CISCO ISEVM	10.1.2.136/10.66.1.136	TOE – Virtual Device
Tester Laptop	10.66.1.80/10.66.1.81	Test PC - Physical Device
Switch 3650X	10.1.1.26:3003/10.66.1.1	Switch - Physical Device
Pi-Bridge	192.168.128.134	RasberryPi – Physical Device

4.3.12 Test Bed Details

Name	OS	Function	Protocols	IP address	MAC Address	Time	Tools (version)
CISCO ISE-VM	ISEv3.1	TOE-Physical Device	IPsec, SSH, TFTP, OCSP, HTTPS	10.1.2.136/10.66.1.136	bia 000c.29e9.2a2b	Manually set and verified	N/A
Server	Ubuntu 20.04.6 LTS	Testing VM – Virtual Device	IPsec, SSH, TFTP, OCSP, SCP	10.1.2.181	bia c014.fe60.b780	Manually set and verified	OpenSSL (1.1.0f), OpenSSH (8.6), Tcpdump (4.9.3) AcumenStrongswan Mod (5.6.2) Rsyslog (8.2106.0) Acumen SSHS () RADIUS Server 3.0
Server	Ubuntu 20.04.6 LTS	Testing VM – Virtual Device/ Syslog Server – Virtual Device	IPsec, SSH, TFTP, OCSP, SCP	10.1.2.227	00:0c:29:d8:7f:39	Manually set and verified	OpenSSL (1.1.0f), OpenSSH (8.6), Tcpdump (4.9.3) AcumenStrongswan Mod (5.6.2) Rsyslog (8.2106.0) Acumen SSHS () RADIUS Server 3.0
ESXI	7.0.2	Virtualization Software.	HTTPS	10.1.2.222	N/A	N/A	N/A
Pi-Bridge	Raspbian GNU/Linux	Rasberry Pi – Physical Device	IP	192.168.128.134	b8:27:eb:21:57:80	Manually set and verified	Tcpdump (4.9.3)
Switch 3650X	IOS v15.2	Switch - Physical Device	Ipsec, RADIUS,SSH	10.1.1.26:3003/10.66.1.1	bia d0d0.fdef.3b45	Manually set and verified	N/A
Tester Laptop	Windows 10 Pro 64 bit	Test PC - Physical Device	SSH, HTTPS, SCP,	10.66.1.80/10.66.1.81 192.168.254.115 192.168.254.90 192.168.254.254	28-7F-CF-23-A6-86	Manually set and verified	Putty (0.70), Wireshark (3.0.3), WinSCP (5.17), XCA (2.1.1) Firefox (89.0.2), Hex editor(2.5.0.0)

4.4 Test Time & Location

All testing was carried at the Acumen Security offices located in 2400 Research Blvd Suite #395, Rockville, MD 20850. Testing occurred from November 1, 2021 through May 30, 2023. The TOE was located 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 kept with the evaluator at all times.

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	The evaluator examined the FAU_GEN.1 entry in 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: The TOE generates and stores audit records locally on the TOE whenever an audited event occurs. The types of events that cause audit records to be generated include, cryptography related events, identification and authentication related events, and administrative events (the specific events and the contents of each audit record are listed in the table within the FAU_GEN.1 SFR, Table 17: Auditable Events of the Security Target. Each of the events is specified in the syslog in enough detail to identify the user for which the event is associated, when the event occurred, where the event occurred, the outcome of the event, and the type of event that occurred. Additionally, the startup and shutdown of the audit functionality is audited. Based on these findings, this assurance activity is considered satisfied.
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	The evaluator examined the section titled 'Security Relevant Events' 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 identification of each auditable event as a row within Table 9 titled 'Auditable Events'. The evaluator compared this list of events to the auditable events listed in NDcPP. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.1.3 FAU_GEN.1 Guidance 2

Objective	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

<table>
<tr><td></td><td>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.</td></tr>
<tr><td>Evaluator Findings</td><td>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:
<table>
<tr><th>Administrative Activity</th><th>Method (Command/GUI Configuration)</th><th>Section</th></tr>
<tr><td>Audit configuration</td><td>GUI/CLI Interface</td><td>Section 5.1, 5.2</td></tr>
<tr><td>Identification and Authentication configuration</td><td>GUI/CLI Interface</td><td>Section 4.5</td></tr>
<tr><td>User Creation</td><td>GUI/CLI Interface</td><td>Section 3.3.4</td></tr>
<tr><td>Clock management</td><td>GUI/CLI Interface</td><td>Section 4.4</td></tr>
<tr><td>Configuring banner</td><td>GUI/CLI Interface</td><td>Section 4.6</td></tr>
<tr><td>Creation of the Certificate Signing Request</td><td>CLI</td><td>Section 4.8.1</td></tr>
<tr><td>Authenticating the Certificate Authority</td><td>CLI</td><td>Section 4.8.3</td></tr>
<tr><td>Configuring a Revocation Mechanism</td><td>CLI</td><td>Section 4.8.6</td></tr>
<tr><td>Setting Password Length</td><td>CLI/GUI</td><td>Section 4.2</td></tr>
<tr><td>Configuring TLS</td><td>GUI</td><td>Section 3.3.2</td></tr>
</table>
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.
<table>
<tr><th>Administrative Activity</th><th>Method (Command/GUI Configuration)</th><th>Test Case(s)</th></tr>
</table></td></tr>
</table>

	Audit configuration	GUI/CLI Interface	FAU_GEN.1 T1
	Identification and Authentication configuration	GUI/CLI Interface	FIA_PMG_EXT.1 T1
	User Creation	GUI/CLI Interface	FIA_PMG_EXT.1 T1
	Clock Management	GUI/CLI Interface	FPT_STM_EXT.1 T1
	Configuring Banner	GUI/CLI Interface	FTA_TAB.1 T1
	Creation of the Certificate Signing Request	CLI	FIA_X509_EXT.3 T1
	Authenticating the Certificate Authority	CLI	FIA_X509_EXT.1.1/Rev T1
	Configuring a Revocation Mechanism	CLI	FIA_X509_EXT.3 T1
	Setting Password Length	GUI/CLI Interface	FIA_PMG_EXT.1 T1
	Configuring TLS	GUI	FCS_TLSC_EXT.1 T1 FCS_TLSS_EXT.1 T1
	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 FAU_STG.1 entry in 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. On the TOE, the local log files rotate after a certain size threshold is reached. The number of days of local log files is configurable, with the default of keeping records only up to last 7 days. From the Administration > System > Logging > Local Log Settings page an administrator is able to configure the storage period for logs in days and delete the existing log file. Only the Security Administrator may delete all of the rolled over log files by the "Delete Local Logs Now" selection in the administration application. The ISE RBAC (Role-Based Access Control) policy does not allow for any user that is not a Security Administrator to delete log files. No

	user can modify log files because there is no mechanism that allows this. After the configured storage period of time has passed for logs the events exceeding the age are deleted. Based on these findings, this assurance activity is considered satisfied.
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 'Logging Protection' 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 states that: If a Security administrator wants to back up the logs between iterations of ISE, or send events to another IT entity, then protection must be provided for the communications. This requires that the TLS remote logging target be created and that UDP syslog be removed. Next, the evaluator found that AGD provides instructions for configuring the secure connection between the TOE and the remote audit server via GUI. 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 FAU_STG_EXT.1 entry in 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. The TOE can offload events to other entities (including other ISE nodes) over TLS protected syslog. The Security Administrators can configure securing the syslog data using TCP. TCP syslog buffers events in a local file that is limited to a total of 100MB. The limit is specified as a file size, not a specific number of events. Overwriting is handled by wrapping to the beginning of the file (overwriting the oldest events). By default, upon adding the remote logging target through the GUI, the remote logging target is enabled. The audit events are not sent to the remote logging target until the administrator has configured which type of logging audit records need to be sent. ISE will transmit audit information in realtime when the ISE has an established connection to the Non-TOE External Secure Syslog Server Based on these findings, this assurance activity is considered satisfied.
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 FAU_STG_EXT.1 entry in 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 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. On the TOE, the local log files rotate after a certain size threshold is reached. The number of days of local log files is configurable, with the default of keeping records only up to last 7 days. From the Administration > System > Logging > Local Log Settings page an administrator is able to configure the storage period for logs in days and delete the existing log file. Only the Security Administrator may delete all of the rolled over log files by the "Delete Local Logs Now" selection in the administration application. The ISE RBAC (Role-Based Access Control) policy does not allow for any user that is not a Security Administrator to delete log files. No user can modify log files because there is no mechanism that allows this. After the configured storage period of time has passed for logs the events exceeding the age are deleted. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.3.3 FAU_STG_EXT.1 TSS 3

Objective	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.
Evaluator Findings	The evaluator examined the FAU_STG_EXT.1 entry in 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. The TOE is stand-alone and stores its own syslog events locally on the platform. The TOE can offload events to other entities (including other ISE nodes) over TLS protected syslog. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.3.4 FAU_STG_EXT.1 TSS 4

Objective	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.
Evaluator Findings	The evaluator examined the FAU_STG_EXT.1 entry 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. The Security Administrators can configure securing the syslog data using TCP. TCP syslog buffers events in a local file that is limited to a total of 100MB. The limit is specified as a file size, not a specific number of events. Overwriting is handled by wrapping to the beginning of the file (overwriting the oldest events). By default, upon adding the remote logging target through the GUI, the remote logging target is enabled. The audit events are not sent to the remote logging target until the administrator has configured which type of logging audit records need to be sent. ISE will transmit audit information in realtime when the ISE has an established connection to the Non-TOE External Secure Syslog Server Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.3.5 FAU_STG_EXT.1 TSS 5

Objective	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.
Evaluator Findings	The evaluator examined the FAU_STG_EXT.1 entry in 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: ISE will transmit audit information in realtime when the ISE has an established connection to the Non-TOE External Secure Syslog Server Based on these findings, this assurance activity is considered satisfied.
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	The evaluator examined the section titled 'Logging Protection' 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. Upon investigation, the evaluator found that the AGD states that: If a Security administrator wants to backup the logs between iterations of ISE, or send events to another IT entity, then protection must be provided for the communications. This requires that the TLS remote logging target be created and that UDP syslog be removed. AGD provides instructions for configuring the secure connection between the TOE and the remote audit server via GUI. Based on these findings, this assurance activity is considered satisfied.
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	The evaluator examined the section titled 'Logging Protection' 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: By default, upon adding the Remote Logging Target the Remote Logging Target is Enabled. However, syslog messages are unsent to this Remote Logging Target until the administrator has configured which type of logging audit records desired. Based on these findings, this assurance activity is considered satisfied.
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	The evaluator examined the section titled "Local Logs Storage Settings and Deletion" 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 TOE does not support the configuration of different methods of handling exhausted local audit storage. Next, the evaluator compared the exhausted local audit handling description found in the AGD to the description provided by the TSS of the ST. The descriptions of the behavior found in the AGD and ST are consistent. Based on these findings, this assurance activity is considered satisfied.
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	The evaluator examined the FCS_CKM.1 entry in 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: Asymmetric cryptographic keys are generated in accordance with the FFC schemes using cryptographic key sizes of 2048 bits or greater that meet the FIPS 186-4, Digital Signature Standard and using Diffie-Hellman group 14 that meets RFC 3256, Section 3. The TOE also uses ECC schemes using "NIST curves" P-256, P-384, P-521 that meets the FIPS PUB 186-4, "Digital Signature Standard (DSS). Based on these findings, this assurance activity is considered satisfied.
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	The evaluator examined the section titled SSL/TLS Settings 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 that: ISE will disallow importing ISE certificates with 1024-bit RSA key sizes when ISE is in FIPS mode. For Diffie-Hellman parameter size of 2048 bits, configuring ISE into FIPS mode automatically always sets the TLS server ISE Administration application to use Diffie-Hellman parameter size of 2048 bits. Based on these findings, this assurance activity is considered satisfied.
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	CAVP Certs: # A1420, A2697,A1462 Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.2 FCS_CKM.2

5.2.2.1 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 FCS_CKM.2 entry in 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 RSA key establishment schemes that is conformant to RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 3447, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1" The cryptographic key establishment is implemented in the TOE according to the RSA-based schemes that meet the NIST SP 800-56B for TLS, SSH and digital signatures and Finite-field based schemes (CAVP Cert # A1420 and Cert # A2697) that meet NIST SP 800-56A for TLS and SSH. The TOE implements Diffie-Hellman (group 14) based key establishment schemes that meets RFC 3526, Section 3 and Elliptic curve-based schemes that meet the NIST Special Publication 800-56A Revision 2., "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography". The TOE also implements and uses the prime and generator specified in RFC 3526 Section 3 when generating parameters for the key exchange. The TOE also uses Finite field -based key establishment schemes that meets the NIST SP800-56A Revision 2, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography". The TOE acts as both a sender and receiver for RSA based key establishment and Elliptic curve-based key establishment schemes. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.2.2 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 AGD to verify that it instructs the administrator how to configure the TOE to use the selected key establishment scheme(s). The entire AGD was used to determine the verdict of this Assurance Activity. Upon investigation, the evaluator found that the AGD states that: Various configuration steps are detailed throughout the AGD, and it is required and the key establishment schemes are used automatically when the appropriate cryptographic function is invoked. Upon further investigation the evaluator found that Section 3.3.1 titled 'Remote Administration Protocols' and Section 3.3.4 'SSH Public-Key Authentication' has detailed steps which instructs the administrator how to configure the TOE to use the selected key establishment scheme(s). Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.2.3 FCS_CKM.2 Test/CAVP 1

Objective	The evaluator shall verify the key establishment mechanisms supported by the TOE.

Evaluator Findings	CAVP Certs: # A1420, A2697, A1462 Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.3 FCS_CKM.4

5.2.3.1 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 for2). 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	The evaluator examined the section titled 'Key Protection and Zeroization' 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. Upon investigation, the evaluator found below information: The evaluator examined the section titled 'Key Protection and Zeroization' in the Security Target to verify that the TSS description of keys and storage locations is consistent with the functions carried out by the TOE. Upon investigation, the evaluator found below information

Name	Description	Zeroization
Diffie-Hellman Shared Secret	The value is zeroized after it has been given back to the consuming operation. The value is overwritten by 0's. This key is stored in DRAM.	Automatically after completion of DH exchange, by calling a specific API within the two crypto modules, when module is shutdown, or reinitialized. Overwritten with: 0x00
Diffie Hellman private exponent	The function returns the value to the TOE and then calls the function to perform the zeroization of the generated key pair. These values are automatically zeroized after generation and once the value has been provided back to the actual	Zeroized upon completion of DH exchange, by calling a specific API within the two crypto modules, when module is

			consumer. This key is stored in DRAM.	shutdown, or reinitialized. Overwritten with: 0x00	
		ISE server certificate	The certificate is used for TLS, HTTPS client connections, secure transport between ISE nodes, and secure connections to authentication stores. The ISE server certificate private key is stored on the local filesystem and in DRAM.	Generation of a new certificate. Overwritten with: 0x00	
		SSH Private Key	Once the function has completed the operations requiring the RSA key object, the module over writes the entire object (no matter its contents) via API call. This overwrites the key with all 0's. The SSH server host private key is stored on the local filesystem and in DRAM.	Generation of a new key Overwritten with: 0x00	
		SSH Session Key	The results zeroized by overwriting the values with 0x00. This is done when a session is ended. This key is stored in DRAM.	Automatically when the SSH session is terminated. Overwritten with: 0x00	
		RNG Seed	This seed is for the RNG. The seed is stored in DRAM.	Zeroized upon power cycle the device	
		RNG Seed Key	This is the seed key for the RNG. The seed key is stored in DRAM.	Zeroized upon power cycle the device	
		RADIUS Shared Secrets	RADIUS Shared Secrets are stored within a local database in non-volatile storage.	When shared secrets are changed. Overwritten by a new value of the key	

		IPsec Pre-shared secrets	IPsec pre-shared secrets are stored within a local database in AES-128 CBC mode encrypted format within a local database in non-volatile storage.	When shared secrets are changed. Overwritten by a new value of the key	
		IKE session encrypt key	This the key IPsec key used for encrypting the traffic in an IPsec connection. This key is stored in DRAM.	Automatically after IKE session terminated. Overwritten with: 0x00	
		IKE session authentication key	This the key IPsec key used for authenticating the traffic in an IPsec connection. This key is stored in DRAM.	Automatically after IKE session terminated. Overwritten with: 0x00	
		IPsec encryption key	This is the key used to encrypt IPsec sessions. This key is stored in DRAM.	Automatically when IPsec session terminated. Overwritten with: 0x00	
		IPsec authentication key	This is the key used to authenticate IPsec sessions. This key is stored in DRAM.	Automatically when IPsec session terminated. Overwritten with: 0x00	
		TLS Session Keys	The results zeroized by overwriting the values with 0x00. This is done when a session is ended. This key is stored in DRAM.	Automatically when the SSH session is terminated. Overwritten with: 0x00	
		CLI Passwords	command line interface (CLI) passwords are stored on the local filesystem in a SHA-256 hashed crypted format	When passwords are changed. Overwritten by a new value of the key	
		Admin UI Passwords	Administrators to administration web application are stored in AES-128 CBC mode encrypted format within a local database in non-volatile storage, when ISE has been configured to use identities in the local storage.	When passwords are changed. Overwritten by a new value of the key	

		Pairwise Master Key (PMK)	Key generated by the authentication Server after the successful authentication of the Supplicant	Automatically when the TLS session is terminated. Overwritten by zeroes
		Key Encryption Key for Encrypting critical security parameters stored in local database	The KEK used to encrypt critical security parameters in the local database is stored on the filesystem and inaccessible from any software interface.	When modified by running the CLI command 'application reset-config', the KEK is modified. Overwritten by zeroes
		Local Database passwords	The local database administrator and user passwords are automatically generated using random unique values for each ISE deployment. Security administrators may modify the passwords using the CLI commands: application reset-passwd ise internal-database-admin application reset-passwd Ise internal-database-user	When passwords are changed. Overwritten by zeroes
	Based on these findings, this assurance activity is considered satisfied.			
Verdict	Pass			

5.2.3.2 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 FCS_CKM.4 entry in 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 the TSS states that:

	The TOE meets all requirements for destruction of keys and Critical Security Parameters (CSPs) in that none of the symmetric keys, pre-shared keys, or private keys are stored in plaintext form. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.3.3 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.
Evaluator Findings	The evaluator examined the section titled 'TOE Summary Specification' 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 TSS states that: The AES key that is used to encrypt these other keys stored in the DRAM. The keys stored on the hard disk drive can be destroyed completely by overwriting the hard disk drive with zeroes and this is accomplished by the Perform System Erase utility. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.3.4 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 FCS_CKM.4 entry in 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 the TSS states that: The secret keys used for symmetric encryption, private keys, and CSPs used to generate keys, are zeroized immediately after use, or on system shutdown. Hence no circumstances were found where destruction may be prevented or delayed. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.3.5 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 evaluator verified that ST does not specify the use of "a value that does not contain any CSP" to overwrite keys. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.3.6 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	The evaluator reviewed the TSS and entire AGD and found no instance in which key destruction is delayed following the request for destruction. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.4 FCS_COP.1/DataEncryption

5.2.4.1 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	The evaluator examined the FCS_COP.1/DataEncryption entry in the section titled 'TOE Summary Specification' in the Security Target to verify that the TSS 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: The TOE provides symmetric encryption and decryption capabilities using AES (as specified in ISO 18033-3), in CBC mode (as specified in ISO 10116), CTR mode (as specified in IOS 10116) and GCM mode (as specified in ISO 19772) with key sizes of 128 bits and 256 bits. These key sizes are used for both TLS, IPsec and SSH. CTR mode is used only in SSH. The AES CAVP certificate number is listed in below table

Algorithm	Description	Mode Supported	CAVP Cert. #
AES	Used for symmetric encryption/decryption	CBC (128 and 256 bits) CTR (128 and 256 bits) GCM (128, and 256 bits)	A1420 A2697 A1462
SHS (SHA-1, SHA-256, SHA-384, and SHA-512)	Cryptographic hashing services	Byte Oriented	A1420 A2697 A1462
HMAC (HMAC-SHA-1, HMAC-SHA-256,	Keyed hashing services and software integrity test	Byte Oriented	A1420 A2697 A1462

	HMAC-SHA384, and HMAC-SHA-512)			
	DRBG	Deterministic random bit generation services in accordance with ISO/IEC 18031:2011	CTR_DRBG (AES 256)	A1420 A2697 A1462
	DSA	Signature Verification	FIPS PUB 186-4, "Digital Signature Standard (DSS)"	A1420 A2697 A1462
	RSA	Signature Verification and key transport	FIPS PUB 186-4 Key Generation (2048-bit key, 4096-bit key)	A1420 A2697 A1462
	ECDSA	Signature generation and Signature verification	FIPS PUB 186-4, "Digital Signature Standard (DSS)" (256 bits, 384 bits and 521 bits) NIST curves- P-256, P-384 and P-521	A1420 A2697 A1462
	CVL – KAS-FFC	Key Agreement	NIST Special Publication 800-56A	A1420 A2697 A1462
	CVL-KAS-ECC	Key Agreement	NIST Special Publication 800-56A	A1420 A2697 A1462
	For additional details, please refer to the CAVP Mapping in Table 2. Based on these findings, this assurance activity is considered satisfied.			
Verdict	Pass			

5.2.4.2 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 'Virtual Private Networks (VPN)' in the AGD to verify that it 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 it contains all the required information. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.4.3 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: # A1420, A2697, A1462. For additional details, please refer to the CAVP Mapping in Table 2. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.5 FCS_COP.1/SigGen

5.2.5.1 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 FCS_COP.1/SigGen entry in section titled 'TOE Summary Specification' in the Security Target to verify that the TSS 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 TOE will provide cryptographic signature services using RSA Digital Signature Algorithm with key size of 2048 bits that meets the FIPS 186-4 Digital Signature Standard. The ISE product can be configured to generate key sizes of 1024-bit, but administrative guidance for the evaluated configuration instructs administrators to only use keys with size 2048. Key sizes of 4096 bits are also supported but it was not tested. In addition, the TOE will provide cryptographic signature services using ECDSA with key size of 256 or greater as specified in FIPS PUB 186-4, "Digital Signature Standard". The TOE provides cryptographic signature services using ECDSA that meets ISO/IEC 14888-3, Section 6.4 with NIST curves P-256, P-384 and P-521. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.5.2 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 'Virtual Private Networks (VPN') 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 it contains all the required information. Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass

5.2.5.3 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: # A1420, A2697, A1462 CAVP ECDSA&SigVer SigGen (186-4) Certs: #A1420, A2697, A1462 For additional details, please refer to the CAVP Mapping in Table 2. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.6 FCS_COP.1/Hash

5.2.6.1 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 FCS_COP.1/Hash entry in 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 provides cryptographic hashing services using SHA-1, SHA-256, SHA-384 and SHA-512. SHA-256 and SHA-512 are used for generating certificate signing requests or generating self-signed certificates on the TOE. SHA-1, SHA-256, SHA-384 and SHA-512 are used for TLS, IPsec and SSH. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.6.2 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 'IKEv1 Transform Sets' 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: Both confidentiality and integrity are configured with the hash sha and encryption aes commands respectively. As a result, confidentiality-only mode is disabled. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.6.3 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: # A1420, A2697, A1462 For additional details, please refer to the CAVP Mapping in Table 2. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.7 FCS_COP.1/KeyedHash

5.2.7.1 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	The evaluator examined the FCS_COP.1/KeyedHash entry in 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: The TOE provides keyed-hashing message authentication services using HMAC-SHA-1 (key size – 160 bits, block size 512 bits), HMAC-SHA-256 (key size – 256 bits, block size 512 bits) HMAC-SHA-384 (key size – 384 bits, block size 1024 bits) and HMAC-SHA-512 (key size -512 bits, block size 1024 bits) and meets the ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2" standard. Note that HMAC-SHA-1, HMAC-SHA-256 and HMAC-SHA-512 are used for SSH connections, while HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384 and HMAC-SHA-512 are used for TLS and IPsec connections. The MAC lengths for HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384 and HMAC-SHA-512 are 160, 256, 384 and 512 bits respectively. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.7.2 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	The evaluator examined the section titled 'IPsec Transforms and Lifetimes' 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 following: Regardless of the IKE version selected, the TOE must be configured with the proper transform for IPsec ESP encryption and integrity as well as IPsec lifetimes. TOE-common-criteria(config)# crypto ipsec transform-set example esp-aes 128 esp-sha-hmac Note that this configures IPsec ESP to use HMAC-SHA-1 and AES-CBC-128. To change this to the other allowed algorithms the following options can replace 'esp-aes 128' in the command above. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.7.3 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: # A1420, A2697, A1462 For additional details, please refer to the CAVP Mapping in Table 2. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.8 FCS_RBG_EXT.1

5.2.8.1 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 FCS_RBG_EXT.1 entry in 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 implements a random bit generator (RBG) based on the AES-256 block cipher, in accordance with ISO/IEC 18031:2011. The Intel Secure Key includes the Intel DRNG random bit generator (RBG) when ISE runs on the SNS-3500 series or SNS-3600 series appliances or when ISE runs as a VMware virtual machine on ESXi 6.7/ UCSC-C220M5SX). Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.8.2 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 confirmed that the guidance documentation contains appropriate instructions for configuring the RNG functionality. Upon investigation, the evaluator found that no configuration is required for implementation of the RNG functionality. The entirety of AGD was used for this activity. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.8.3 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: # A1420, A2697, A1462 For additional details, please refer to the CAVP Mapping in Table 2.

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

5.2.9 FCS_EAP-TLS_EXT.1

5.2.9.1 FCS_EAP-TLS_EXT.1 TSS 1

Objective	The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that optional characteristics (e.g., extensions supported) are specified as well as the supported ciphersuites. The evaluator shall check the TSS to ensure that the ciphersuites specified are identical to those listed for this component.
Evaluator Findings	The evaluator examined the TSS to check the description of the implementation of this protocol in the TSS to ensure that optional characteristics (e.g., extensions supported) are specified as well as the supported ciphersuites. The TSS entry for FCS_EAP-TLS_EXT.1 in the section 'TOE Summary Specification' of ST was used to determine the verdict of this assurance activity. Upon investigation, the evaluator found that : The following ciphersuites are supported: Mandatory Ciphersuite: • TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268 Optional Ciphersuites: • TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246 • TLS_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246 • TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288 • TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256 as defined in RFC 5246 • TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246 • TLS_DHE_RSA_WITH_AES_256_GCM_ SHA384 as defined in RFC 5288 • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 • TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289 • TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 There are no optional characteristics supported. Additionally, the evaluator compared the list of ciphersuites provided by the TSF to the functions mapped in the TSS and found them to be consistent. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.9.2 FCS_EAP-TLS_EXT.1 Guidance 1

Objective	The evaluator shall check that the operational guidance contains instructions for the administrator to configure the list of Certificate Authorities that are allowed to sign certificates used by the authentication server that will be accepted by the TOE in the EAP-TLS exchange, and instructions on how to specify the algorithm suites that will be proposed and accepted by the TOE during the EAP-TLS exchange. The evaluator shall also check the operational guidance to ensure that it contains instructions on configuring the TOE so that TLS conforms to the description in the TSS (for instance, the set of ciphersuites advertised by the TOE may have to be restricted to meet the requirements).
Evaluator Findings	The evaluator examined the Guidance document to verify that it contains instructions for the administrator to configure the list of Certificate Authorities that are allowed to sign certificates used by the authentication server that will be accepted by the TOE in the EAP-TLS exchange and instructions on how to specify the algorithm suites that will be proposed and accepted by the TOE during the EAP-TLS exchange. The section 'ISE Configuration Steps – ISE EAP-TLS Server' was used for this activity. On investigation, the evaluator found that the Guidance document contains all the required instructions for the configuration of list of Certificate Authorities that are allowed to sign certificates used by the authentication server. The evaluator also verified that the Guidance document contains instructions on configuring the TOE so that TLS conforms to the description in the TSS. Configure How ISE Extracts the Identity from the EAP-TLS X.509 client certificate • The purpose of the Certificate Authentication Profile is to inform ISE which certificate field the identity (machine or user) can be found on the client certificate (end-identity certificate) presented to ISE during EAP-TLS (also during other certificate-based authentication methods). From ISE GUI, navigate to the Menu: Administration > Identity Management > External Identity Sources • In the Left-Side Navigation, click on Certificate Authentication Profile folder • Add a new Certificate Authentication Profile by clicking on the Add button • Complete the following fields: o Name o Use Identity From: selected radio button for Certificate Attribute, pull down the selection where the identity will be obtained from in the EAP-TLS Client certificate. o Optionally: Add a Description o Leave Identity Store as default value of [not applicable] o Match Client Certificate Against Certificate in Identity Store: Keep default value with selected radio button for "Never". • Click the Submit button save the Certificate Authentication Profile. • Use Identity From is used to choose the certificate attribute from which a specific field the identity can be found. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3 TSS and Guidance Activities (HTTPS)

5.3.1 FCS_HTTPS_EXT.1

5.3.1.1 FCS_HTTPS_EXT.1.1 TSS 1

Objective	The evaluator shall examine the TSS and determine that enough detail is provided to explain how the implementation complies with RFC 2818.
Evaluator Findings	The evaluator examined the FCS_HTTPS_EXT.1 entry in the section titled 'TOE Summary Specification' in the Security Target to verify that the TSS provides enough detail to explain how the implementation complies with RFC 2818. Upon investigation, the evaluator found that the TSS states that: The TOE provides HTTPS, as specified in RFC 2818, to provide a secure interactive interface for remote administrative functions, and to support secure exchange of user authentication parameters during login. HTTPS uses TLS to securely establish the encrypted remote session. The sessions are not established with invalid certificates. Note that port 80 is exposed on the product, but only as a redirect to port 443. HTTP connections are not allowed. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.1.2 FCS_HTTPS_EXT.1.1 Guidance 1

Objective	The evaluator shall examine the guidance documentation to verify it instructs the Administrator how to configure TOE for use as an HTTPS client or HTTPS server.
Evaluator Findings	The evaluator examined the section titled 'Remote Administration Protocols' in the AGD to verify that it instructs the Administrator how to configure TOE for use as an HTTPS client or HTTPS server. Upon investigation, the evaluator found that the AGD states that: HTTPS must be used for connections to the administrative GUI. Note that when connecting to the GUI, both port 80 (HTTP) and 443 (HTTPS) are listening, but port 80 by default is redirected to port 443. This setting cannot be changed. It is the administrator's responsibility to configure their HTTPS client per the SSL/TLS Settings in Section 3.3.2. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4 TSS and Guidance Activities (RADIUS)

5.4.1 FCS_RADIUS_EXT.1

5.4.1.1 FCS_RADIUS_EXT.1.1 TSS 1

Objective	The evaluator shall examine the TSS to ensure that RADIUS is specified as the protocol by which all communication between the TOE and the NAS is conducted. The evaluator shall examine the TSS to ensure that EAP is specified as the authentication protocol to be used between the TOE and the NAS, that TLS is the means of mutual authentication to be carried out over EAP, and that other authentication frameworks are disallowed. The evaluator shall check the

	description of the implementation of this protocol to ensure that RADIUS encapsulated EAP Message Authenticators conform to RFC 3579.
Evaluator Findings	The evaluator examined the TSS to ensure that RADIUS is specified as the protocol by which all communication between the TOE and the NAS is conducted. The TSS entry for FCS_RADIUS_EXT.1 in the section titled 'TOE Summary Specification' of ST was used to determine the verdict of this assurance activity. Upon investigation, the evaluator found that "The RADIUS protocol is implemented by the TOE for communication with the NAS (Authenticator) per RFC 2865. RADIUS encapsulated EAP and use of EAP-TLS for authentication is implemented according to RFC 3579 and 5216 respectively. Other authentication frameworks are disallowed." Based on these findings, this assurance activity is considered satisfied.
Verdict	Pas

5.4.1.2 FCS_RADIUS_EXT.1.1 Guidance 1

Objective	The evaluator shall verify that the guidance contains all necessary instructions to configure RADIUS and encapsulated EAP-TLS on the TOE, in accordance with RFCs 2865, 2869, 3579, and 5216.
Evaluator Findings	The evaluator examined the guidance documentation to determine if it describes how to configure RADIUS and encapsulated EAP-TLS on the TOE. Section 'Configuring Radius' and 'Configuring EAP-TLS' of AGD was used to determine the verdict of this assurance activity. Upon investigation, the evaluator found that AGD describes the steps to configure RADIUS and EAP-TLS using GUI. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5 TSS and Guidance Activities (IPsec)

5.5.1 FCS_IPSEC_EXT.1

5.5.1.1 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 FCS_IPSEC_EXT.1 entry in 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 to provide authentication and encryption services to prevent unauthorized viewing or modification of data as it travels over the external network.

	A crypto map (the Security Policy Definition) set can contain multiple entries, each with a different access list. The crypto map entries are searched in a sequence - the router attempts to match the packet to the access list (acl) specified in that entry. When a packet matches a permit entry in a particular access list, the method of security in the corresponding crypto map is applied. If the crypto map entry is tagged as ipsecisakmp, IPsec is triggered. The traffic matching the permit acls would then flow through the IPSec tunnel and be classified as "PROTECTED". Traffic that does not match a permit acl in the crypto map, but that is not disallowed by other acls on the interface is allowed to BYPASS the tunnel. Traffic that does not match a permit acl and is also blocked by other non-crypto acls on the interface would be DISCARDED. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.2 FCS_IPSEC_EXT.1.1 TSS 2

Objective	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.
Evaluator Findings	The evaluator examined the FCS_IPSEC_EXT.1 entry in 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: A crypto map (the Security Policy Definition) set can contain multiple entries, each with a different access list. The crypto map entries are searched in a sequence - the router attempts to match the packet to the access list (acl) specified in that entry. When a packet matches a permit entry in a particular access list, the method of security in the corresponding crypto map is applied. If the crypto map entry is tagged as ipsecisakmp, IPsec is triggered. The traffic matching the permit acls would then flow through the IPSec tunnel and be classified as "PROTECTED". Traffic that does not match a permit acl in the crypto map, but that is not disallowed by other acls on the interface is allowed to BYPASS the tunnel. Traffic that does not match a permit acl and is also blocked by other non-crypto acls on the interface would be DISCARDED. If there is no SA that the IPsec can use to protect this traffic to the peer, IPsec uses IKE to negotiate with the remote peer to set up the necessary IPsec SAs on behalf of the data flow. The negotiation uses information specified in the crypto map entry as well as the data flow information from the specific access list entry. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.3 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	The evaluator examined the section titled 'IPsec Overview' 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 that: A crypto map set can contain multiple entries, each with a different access list. The crypto map entries are searched in a sequence--the router attempts to match the packet to the access list specified in that entry. When a packet matches a permit entry in a particular access list, and the corresponding crypto map entry is tagged as cisco, connections are established, if necessary. If the crypto map entry is tagged as ipsec-isakmp, IPsec is triggered. If there is no SA that the IPsec can use to protect this traffic to the peer, IPsec uses IKE to negotiate with the remote peer to set up the necessary IPsec SAs on behalf of the data flow. The negotiation uses information specified in the crypto map entry as well as the data flow information from the specific access list entry. Once established, the set of SAs (outbound to the peer) is then applied to the triggering packet and to subsequent applicable packets as those packets exit the router. "Applicable" packets are packets that match the same access list criteria that the original packet matched. For example, all applicable packets could be encrypted before being forwarded to the remote peer. The corresponding inbound SAs are used when processing the incoming traffic from that peer. Access lists associated with IPsec crypto map entries also represent the traffic that the router needs protected by IPsec. Inbound traffic is processed against crypto map entries--if an unprotected packet matches a permit entry in a particular access list associated with an IPsec crypto map entry, that packet is dropped because it was not sent as an IPsec-protected packet. The evaluator found that the description of the configuration of SPDs found in AGD is consistent with the options described in the TSS of ST. The descriptions in AGD do not introduce any rule configurations not described in the TSS of ST and the configuration of each option described in the TSS of ST is addressed in AGD. Finally, the evaluator compared the operations available during testing to both the descriptions of configuration in AGD and the available options described in the TSS of ST and found that all available configuration options are described. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.4 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	The evaluator examined the FCS_IPSEC_EXT.1 entry in 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: In addition to tunnel mode, which is the default IPsec mode, the TOE also supports transport mode, allowing for only the payload of the packet to be encrypted. If tunnel mode is explicitly specified, the router will request tunnel mode and will accept only tunnel mode Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.5 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	The evaluator examined the section titled IPsec Transforms and Lifetimes 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 the following: TOE-common-criteria(config-crypto)#mode tunnel This configures tunnel mode for IPsec. Tunnel is the default, but by explicitly specifying tunnel mode, the router will request tunnel mode and will accept only tunnel mode. TOE-common-criteria(config-crypto)#mode transport This configures transport mode for IPsec. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.6 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	The evaluator examined the FCS_IPSEC_EXT.1 entry in 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: The TOE implementation of the IPsec standard (in accordance with the RFCs noted in the SFR) uses the Encapsulating Security Payload (ESP) protocol to provide authentication, encryption and anti-replay services. The IPsec protocol ESP is implemented using the cryptographic algorithms AES-CBC-128 and AES-CBC-256 together with HMAC-SHA-1, HMAC-SHA-256 and HMAC-SHA-512. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.7 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.

<table>
<tr><td>Evaluator Findings</td><td>The evaluator examined the section titled IPsec Transforms and Lifetimes in the AGD to verify that it provides instructions on how to configure the TOE to use the algorithms selected. Upon investigation, the evaluator found that the AGD states that:

Regardless of the IKE version selected, the TOE must be configured with the proper transform for IPsec ESP encryption and integrity as well as IPsec lifetimes.

TOE-common-criteria(config)# crypto ipsec transform-set example esp-aes 128 esp-sha-hmac

Note that this configures IPsec ESP to use HMAC-SHA-1 and AES-CBC-128. To change this to the other allowed algorithms the following options can replace ‘esp-aes 128’ in the command above:

<table><tr><td>Encryption Algorithm</td><td>Command</td></tr><tr><td>AES-CBC-256</td><td>esp-aes 256</td></tr><tr><td>AES-GCM-128</td><td>esp-gcm 128</td></tr><tr><td>AES-GCM-256</td><td>esp-gcm 256</td></tr></table>
Based on these findings, this assurance activity is considered satisfied.</td></tr>
<tr><td>Verdict</td><td>Pass</td></tr>
</table>

5.5.1.8 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	The evaluator examined the FCS_IPSEC_EXT.1 entry in 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. The TOE supports both IKEv1 and IKEv2 session establishment. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.9 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	The evaluator examined the FCS_IPSEC_EXT.1 entry in 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: The TOE supports both IKEv1 and IKEv2 session establishment. As part of this support, the TOE can be configured to not support aggressive mode for IKEv1 exchanges and to only use main mode using the ‘crypto ISAKMP aggressive-mode disable’ command. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.10 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	The evaluator examined the section titled IKEv1 Transform Sets, IKEv2 Transform Sets and NAT Traversal 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 that. The following settings must be set in configuring the IPsec with IKEv1 functionality for the TOE: TOE-common-criteria # conf t TOE-common-criteria (config)#crypto isakmp policy 1 TOE-common-criteria (config-isakmp)# hash sha TOE-common-criteria (config-isakmp)# encryption aes This configures IPsec IKEv1 to use AES-CBC-128 for payload encryption. AES-CBC-256 can be selected with 'encryption aes 256'. *Note: the authorized administrator must ensure that the keysize for this setting is greater than or equal to the keysize selected for ESP in Section 4.6.2 below. If AES 128 is selected here, then the highest keysize that can be selected on the TOE for ESP is AES 128 (either CBC or GCM).* *Note: Both confidentiality and integrity are configured with the hash sha and encryption aes commands respectively. As a result, confidentiality-only mode is disabled.* The following settings must be set in configuring the IPsec with IKEv2 functionality for the TOE: TOE-common-criteria # conf t TOE-common-criteria (config)#crypto ikev2 proposal sample TOE-common-criteria (config-ikev2-proposal)# integrity sha1 TOE-common-criteria (config-ikev2-proposal)# encryption aes-cbc-128 This configures IPsec IKEv2 to use AES-CBC-128 for payload encryption. AES-CBC-256 can be selected with 'encryption aes-cbc-256'. AES-GCM-128 and AES-GCM-256 can also be selected similarly. *Note: the authorized administrator must ensure that the keysize for this setting is greater than or equal to the keysize selected for ESP in Section 4.6.2 below. If AES 128 is selected here, then the highest keysize that can be selected on the TOE for ESP is AES 128 (either CBC or GCM).* *Note: Both confidentiality and integrity are configured with the hash sha and encryption aes commands respectively. As a result, confidentiality-only mode is disabled.* For successful NAT traversal over an IOS-XE NAT device for an IPsec connection between two IOS-XE peers, the following configuration needs to be used - <u>On an IOS NAT device (router between the IPsec endpoints):</u> config terminal ip nat service list <ACL-number> ESP spi-match access-list <ACL-number> permit <protocol> <local-range> <remote-range> end

	On each IOS peer (IPsec router endpoints): config terminal crypto ipsec nat-transparency spi-matching end Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.11 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 'IKEv1 Transform Sets' 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 following: TOE-common-criteria (config-isakmp)# crypto isakmp aggressive-mode disable Main mode is the default mode and the crypto isakmp aggressive-mode disable ensures all IKEv1 Phase 1 exchanges will be handled in the default main mode. TOE-common-criteria(config-isakmp)#exit Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.12 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 FCS_IPSEC_EXT.1 entry in 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 provides AES-CBC-128 and AES-CBC-256 for encrypting the IKEv1 Phase 1, and AES-CBC-128 and AES-CBC-256 for IKEv1 Phase 2 and IKEv2 payloads. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.13 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 'IKEv1 Transform Sets' and 'IKEv2 Transform Sets' 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 following: TOE-common-criteria (config-isakmp)# hash sha

	TOE-common-criteria (config-isakmp)# encryption aes This configures IPsec IKEv1 to use AES-CBC-128 for payload encryption. AES-CBC-256 can be selected with 'encryption aes 256'. Note: the authorized administrator must ensure that the keysize for this setting is greater than or equal to the keysize selected for ESP in Section 4.6.2 below. If AES 128 is selected here, then the highest keysize that can be selected on the TOE for ESP is AES 128 (either CBC or GCM). Note: Both confidentiality and integrity are configured with the hash sha and encryption aes commands respectively. As a result, confidentiality-only mode is disabled. TOE-common-criteria (config-ikev2-proposal)# integrity sha1 TOE-common-criteria (config-ikev2-proposal)# encryption aes-cbc-128 This configures IPsec IKEv2 to use AES-CBC-128 for payload encryption. AES-CBC-256 can be selected with 'encryption aes-cbc-256'. AES-GCM-128 and AES-GCM-256 can also be selected similarly. Note: the authorized administrator must ensure that the keysize for this setting is greater than or equal to the keysize selected for ESP in Section 4.6.2 below. If AES 128 is selected here, then the highest keysize that can be selected on the TOE for ESP is AES 128 (either CBC or GCM). Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.14 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	The evaluator examined the FCS_IPSEC_EXT.1 entry in 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: The TOE supports configuration lifetimes of both Phase 1 SAs and Phase 2 SAs using the following command, lifetime. The time values for Phase 1 SAs can be limited up to 24 hours and for Phase 2 SAs up to 8 hours, but it is configurable to 8 hours. The Phase 2 SA lifetimes can also be configured by an Administrator based on number of packets. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.15 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.
Evaluator Findings	The evaluator examined the section titled 'IKEv1 Transform Sets' in the AGD to verify that it includes instructions for configuring values for SA lifetimes. Upon investigation, the evaluator found that the AGD states the following: TOE-common-criteria (config-isakmp)# lifetime 86400 The default time value for Phase 1 SAs is 24 hours (86400 seconds), but this setting can be changed using the command above with different values. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.16 FCS_IPSEC_EXT.1.8 TSS 1

Objective	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.
Evaluator Findings	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: The TOE supports configuration lifetimes of both Phase 1 SAs and Phase 2 SAs using the following command, lifetime. The time values for Phase 1 SAs can be limited up to 24 hours and for Phase 2 SAs up to 8 hours, but it is configurable to 8 hours. The Phase 2 SA lifetimes can also be configured by an Administrator based on number of packets. The TOE supports configuring the maximum amount of traffic that is allowed to flow for a given IPsec SA (IKEv1 Phase 2 SA and IKEv2 Child SA only) using the following command, 'crypto ipsec security-association lifetime'. The default amount is 2560KB, which is the minimum configurable value. The maximum configurable value is 4GB. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.17 FCS_IPSEC_EXT.1.8 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 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.
Evaluator Findings	The evaluator examined the section titled 'IPsec Transforms and Lifetimes' in the AGD to verify that it includes instructions for configuring values for SA lifetimes. Upon investigation, the evaluator found that the AGD states the following: TOE-common-criteria (config)#crypto ipsec security-association lifetime seconds 28800 The default time value for Phase 2 SAs is 1 hour. There is no configuration required for this setting since the default is acceptable, however to change the setting to 8 hours as claimed in the Security Target the crypto ipsec security-association lifetime command can be used as specified above. TOE-common-criteria (config)#crypto ipsec security-association lifetime kilobytes 100000 This configures a lifetime of 100 MB of traffic for Phase 2 SAs. The default amount for this setting is 2560KB, which is the minimum configurable value for this command. The maximum configurable value for this command is 4GB. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.18 FCS_IPSEC_EXT.1.9 TSS 1

Objective	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.
Evaluator Findings	The evaluator examined the FCS_IPSEC_EXT.1 entry in 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 The TOE supports Diffie-Hellman Group 14 (2048-bit keys), 19 (256-bit Random ECP), 24 (2048-bit MODP with 256-bit POS), and 20 (384-bit Random ECP) in support of IKE Key Establishment. These keys are generated using the AES-CTR Deterministic Random Bit Generator (DRBG), as specified in SP 800-90, and the following corresponding key sizes (in bits) are used: 320 (for DH Group 14), 256 (for DH Group 19), 256 (for DH Group 24), and 384 (for DH Group 20). The secret value 'x' used in the IKE Diffie-Hellman key exchange ("x" in gx mod p) is generated using a NIST-approved AES-CTR Deterministic Random Bit Generator (DRBG). Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.19 FCS_IPSEC_EXT.1.10 TSS 1

Objective	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. 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.
Evaluator Findings	The evaluator examined the FCS_IPSEC_EXT.1 entry in 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. The TOE supports Diffie-Hellman Group 14, 19, 24, and 20. Group 14 (2048-bit keys) can be set by using the "group 14" command in the config mode. The nonces used in IKE exchanges are generated in a manner such that the probability that a specific nonce value will be repeated during the life a specific IPsec SA is less than 1 in 2^[128]. The secret value 'x' used in the IKE Diffie-Hellman key exchange ("x" in gx mod p) is generated using a NIST-approved AES-CTR Deterministic Random Bit Generator (DRBG). Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.20 FCS_IPSEC_EXT.1.11 TSS 1

Objective	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.
Evaluator Findings	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: The TOE supports Diffie-Hellman Group 14 (2048-bit keys), 19 (256-bit Random ECP), 24 (2048-bit MODP with 256-bit POS), and 20 (384-bit Random ECP) in support of IKE Key Establishment. These keys are generated using the AES-CTR Deterministic Random Bit Generator (DRBG), as specified in SP 800-90, and the following corresponding key sizes (in bits) are used: 320 (for DH Group 14), 256 (for DH Group 19), 256 (for DH Group 24), and 384 (for DH Group 20). Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.21 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	The evaluator examined the section titled 'IKEv1 Transform Sets' and 'IKEv2 Transform Sets' 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 following:

	TOE-common-criteria (config-isakmp)# group 14 This selects DH Group 14 (2048-bit MODP) for IKE, but 19 (256-bit Random ECP), 24 (2048-bit MODP with 256-bit POS), 20 (384-bit Random ECP), 15 (3072-bit MODP), and 16 (4096-bit MODP) are also allowed and supported. TOE-common-criteria (config-ikev2-proposal)# group 14 This selects DH Group 14 (2048-bit MODP) for IKE, but 19 (256-bit Random ECP), 24 (2048-bit MODP with 256-bit POS), 20 (384-bit Random ECP), 15 (3072-bit MODP), and 16 (4096-bit MODP) are also allowed and supported. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.22 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	The evaluator examined the FCS_IPSEC_EXT.1 entry in 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. The strength of the symmetric algorithm negotiated to protect the IKEv1 Phase 1 and 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. IKE separates negotiation into two phases: phase 1 and phase 2. Phase 1 creates the first tunnel, which protects later ISAKMP negotiation messages. The key negotiated in phase 1 enables IKE peers to communicate securely in phase 2. During Phase 2 IKE establishes the IPsec SA. IKE maintains a trusted channel, referred to as a Security Association (SA), between IPsec peers that is also used to manage IPsec connections, including: • The negotiation of mutually acceptable IPsec options between peers (including peer authentication parameters, either signature based or pre-shared key based), • The establishment of additional Security Associations to protect packets flows using Encapsulating Security Payload (ESP), and • The agreement of secure bulk data encryption AES keys for use with ESP. After the two peers agree upon a policy, the security parameters of the policy are identified by an SA established at each peer, and these IKE SAs apply to all subsequent IKE traffic during the negotiation. The TOE provides AES-CBC-128 and AES-CBC-256 for encrypting the IKEv1 Phase 1, and AES-CBC-128 and AES-CBC-256 for IKEv1 Phase 2 and IKEv2 payloads. The administrator is instructed in the AGD to ensure that the size of key used for ESP must be greater than or equal to the key size used to protect the IKE payload.

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

5.5.1.23 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 FCS_IPSEC_EXT.1 entry in 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 IKE protocols implement Peer Authentication using RSA and ECDSA with X.509v3 certificates, or pre-shared keys. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.24 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 FCS_IPSEC_EXT.1 entry in 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: Preshared keys can be configured using the 'crypto isakmp key' key command and may be proposed by each of the peers negotiating the IKE establishment. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.25 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 'X.509 Certificates' and 'Setting X.509 for use with IKE' 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 that. The TOE may be configured by the privileged administrators to use X.509v3 certificates to authenticate IPsec peers. RSA certificates are supported. Once X.509v3 keys are installed on the TOE, they can be set for use with IKEv1 with the commands:

	TOE-common-criteria (config)#crypto isakmp policy 1 TOE-common-criteria (config-isakmp)# authentication rsa-sig And for IKEv2 with the commands: TOE-common-criteria (config)#crypto ikev2 profile sample TOE-common-criteria(config-ikev2-profile)#authentication [remote | local] rsa-sig If an invalid certificate is loaded, authentication will not succeed. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.26 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 'IKEv1 Transform Sets' and 'IKEv2 Transform Sets' 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 following configuration: <u>IKEv1</u> TOE-common-criteria (config-isakmp)# authentication pre-share This configures IPsec to use pre-shared keys. X.509 v3 certificates are also supported for authentication of IPsec peers. See Section 4.6.3 below for additional information. TOE-common-criteria(config-isakmp)# exit TOE-common-criteria(config)# Crypto isakmp key cisco123!cisco123!CISC address 11.1.1.4 Note: Pre-shared keys on the TOE must be at least 22 characters in length and can be composed of any combination of upper and lower case letters, numbers, and special characters (that include: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")"). The TOE supports pre-shared keys up to 128 bytes in length. While longer keys increase the difficulty of brute-force attacks, longer keys increase processing time. IKEv2 TOE-common-criteria (config-ikev2-keyring-peer)# pre-shared-key cisco123!cisco123!CISC This section creates a keyring to hold the pre-shared keys referenced in the steps above. In IKEv2 these pre-shared keys are specific to the peer. Note: Pre-shared keys on the TOE must be at least 22 characters in length and can be composed of any combination of upper and lower case letters, numbers, and special characters (that include: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")"). The TOE supports pre-shared keys up to 128 bytes in length. While longer keys increase the difficulty of brute-force attacks, longer keys increase processing time. Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass

5.5.1.27 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 ‘Authenticating the Certificate Authority’ 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 that: The TOE must authenticate the CA by acknowledging its attributes match the publicly posted fingerprint. The TOE administrator must verify that the output of the command below matches the fingerprint of the CA on its public site. Authenticate the CA: crypto ca authenticate trustpoint-name Device (config)#crypto ca authenticate ciscotest Certificate has the following attributes: Fingerprint MD5: 8DE88FE5 78FF27DF 97BA7CCA 57DC1217 Fingerprint SHA1: 271E80EC 30304CC1 624EEE32 99F43AF8 DB9D0280 % Do you accept this certificate? [yes/no]: yes Trustpoint CA certificate accepted. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.28 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 FCS_IPSEC_EXT.1 entry in 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 supports the following presented identifier types: a) subjectAltName entry of type dNSName (DNS-ID in RFC 6125) b) CN-ID as defined in RFC 6125, c) subjectAltName entry of type iPAddress; and d) Wildcards in DNS domain names.

	If the DN or SAN within the client certificate does not match the expected identifier on the TOE, the connection will be rejected. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.29 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 IPsec Overview 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 The TOE supports reference identifiers as configured by the Administrator to be either FQDN or IP address and compares it to the Subject Alternative Name (SAN) or the Common Name (CN) fields in the certificate of the peer. The order of comparison is SAN followed by CN. If the TOE successfully matches the reference identifier to the presented identifier, IKE authentication will succeed. The identifier scheme implemented by the TOE guarantees unique identifiers. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6 TSS and Guidance Activities (SSH)

5.6.1 FCS_SSHS_EXT.1

5.6.1.1 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 FCS_SSHS_EXT.1 entry in 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, that this list conforms to FCS_SSHS_EXT.1.5, and that if password-based authentication methods have been selected in the ST then these are also described. Upon investigation, the evaluator found that the TSS states that: The TOE implementation of SSHv2 supports the following public key algorithm for authentication - RSA Signature Verification. The TOE supports RSA public-keys (rsa-sha2-256, rsa-sha2-512) and password-based authentication for administrators accessing the TOE through SSHv2. The TOE implementation of SSHv2 supports the following encryption algorithms - AES-128-CTR, AES-256-CTR to ensure confidentiality of the session Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.1.2 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	The evaluator examined the FCS_SSHS_EXT.1 entry in 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: SSH connections will be dropped if the TOE receives a packet larger than 35,000 bytes. Large packets are detected by the SSH implementation and dropped internal to the SSH process. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.1.3 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.
Evaluator Findings	The evaluator examined the FCS_SSHS_EXT.1 entry in 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: The TOE implementation of SSHv2 supports the following encryption algorithms - AES-128-CTR, AES-256-CTR to ensure confidentiality of the session. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.1.4 FCS_SSHS_EXT.1.4 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	The evaluator examined the section titled 'Remote Administration Protocols' 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: To enforce the required AES-CBC 128-bit or AES-CBC 256-bit cipher requirement and SHA macs when connecting to the TOE, the SSH client must request these algorithms. On Linux-based systems this is done with the following SSH syntax: ssh -2 –c [aes128-cbc or aes256-cbc] –m [sha macs] Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.1.5 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	The evaluator examined the FCS_SSHS_EXT.1 entry in 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: The TOE supports RSA public-keys (ssh-rsa, rsa-sha2-256, rsa-sha2-512) and password-based authentication for administrators accessing the TOE through SSHv2. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.1.6 FCS_SSHS_EXT.1.5 TSS 2

Objective	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.
Evaluator Findings	The evaluator examined the FCS_SSHS_EXT.1 entry in section titled 'TOE Summary Specification' in the Security Target to verify that the TSS describes how the TOE establishes a user identity when an SSH client presents a public key or X.509v3 certificate. Upon investigation, the evaluator found that the TSS states that: The TOE ensures and verifies that the SSH client's presented public key matches one that is stored within the TOE's SSH server's authorized keys file. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.1.7 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	The evaluator examined the section titled SSH Public-Key Authentication 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 . SSH host key algorithms - The SSH host key algorithms on the TOE are configured by default when the TOE is operating in the CC mode. No additional configuration steps are required. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.1.8 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 FCS_SSHS_EXT.1 entry in 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 following integrity algorithms are supported: hmac-sha1, hmac-sha2-256, hmac-sha2-512 Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.1.9 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 'Remote Administration Protocols' 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. Upon investigation, the evaluator found that the AGD states that: To enforce the required AES-CBC 128-bit or AES-CBC 256-bit cipher requirement and SHA macs when connecting to the TOE, the SSH client must request these algorithms. On Linux-based systems this is done with the following SSH syntax: ssh -2 –c [aes128-cbc or aes256-cbc] –m [sha macs] Note: The hashing method 'none' is NOT to be used in the evaluated configuration. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.1.10 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	The evaluator examined the FCS_SSHS_EXT.1 entry in 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: The diffie-hellman-group14-sha1 or ecdh-sha2-nistp521, ecdh-sha2-nistp384, and/or ecdh-sha2-nistp256 are the only allowed key exchange method used. Optional characteristics are not supported. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.1.11 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	The evaluator examined the section titled 'Remote Administration Protocols' 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: To enforce the required Diffie-Hellman-Group14-SHA1 SSH key exchanges, the CLI admin must enter the following commands from the Cisco ISE Command-Line Interface (CLI) Configuration Mode: service sshd key-exchange-algorithm diffie-hellman-group14-sha1 Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.1.12 FCS_SSHS_EXT.1.8 TSS 1

Objective	The evaluator shall check that the TSS specifies the following: 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 FCS_SSHS_EXT.1 entry in 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: SSH connections are rekeyed before 1 hour or 1GB has been transmitted using key. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.1.13 FCS_SSHS_EXT.1.8 Guidance 1

Objective	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.
Evaluator Findings	The evaluator examined the section titled SSH Public-Key Authentication 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 SSH connections are rekeyed before 1 hour or 1GB has been transmitted using that key. These rekey settings are the same for all ISE installations regardless of whether ISE is operating in FIPS 140 mode. SSH rekey thresholds are default and cannot be configured by users. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7 TSS and Guidance Activities (TLS)

5.7.1 FCS_TLSC_EXT.1

5.7.1.1 FCS_TLSC_EXT.1.1 TSS 1

Objective	The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that the ciphersuites supported are specified. The evaluator shall check the TSS to ensure that the ciphersuites specified include those listed for this component.
Evaluator Findings	The evaluator examined the FCS_TLSC_EXT.1 entry in section titled 'TOE Summary Specification' in the Security Target to verify that the TSS specifies the ciphersuites supported and that the ciphersuites specified include those listed for this component. Upon investigation, the evaluator found that the TSS states that. As a TLS client, the TOE supports – • TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246 • TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246 • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 • TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289 • TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.1.2 FCS_TLSC_EXT.1.1 Guidance 1

Objective	The evaluator shall check the guidance documentation to ensure that it contains instructions on configuring the TOE so that TLS conforms to the description in the TSS.

Evaluator Findings	The evaluator examined the section titled SSL /TLS Settings in the AGD to verify that it contains instructions on configuring the TOE so that TLS conforms to the description in the TSS. Upon investigation, the evaluator found that the AGD states that. The evaluated configuration requires that when connecting to the TOE over TLS1.2, it must be used with one of the following algorithms- a) TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246 b) TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246 c) TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289 d) TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 e) TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 f) TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 g) TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289 h) TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 i) TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 j) TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 The SSL/TLS client must be configured for one or more of the above algorithms. The AGD also lists the exact steps required for enabling the above algorithms. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.1.3 FCS_TLSC_EXT.1.2 TSS 1

Objective	The evaluator shall ensure that the TSS describes the client's method of establishing all reference identifiers from the administrator/application configured reference identifier, including which types of reference identifiers are supported (e.g. application-specific Subject Alternative Names) and whether IP addresses and wildcards are supported.
Evaluator Findings	The evaluator examined the FCS_TLSC_EXT.1 entry in section titled 'TOE Summary Specification' in the Security Target to verify that the TSS describes the client's method of establishing all reference identifiers from the administrator/application-configured reference identifier, including which types of reference identifiers are supported; whether IP addresses and wildcards are supported. Upon investigation, the evaluator found that the TSS states that. The TOE supports the following presented identifier types: a) subjectAltName entry of type dNSName (DNS-ID in RFC 6125) b) CN-ID as defined in RFC 6125, c) subjectAltName entry of type iPAddress; and d) Wildcards in DNS domain names. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.1.4 FCS_TLSC_EXT.1.2 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 includes support for IP addresses, 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 'SSL/TLS Settings' in the AGD to verify that it describes all supported identifiers, explicitly states whether the TOE supports the SAN extension or not, includes detailed instructions on how to configure the reference identifier(s) used to check the identity of peer(s), and provides a set of warnings and/or CA policy recommendations that would result in secure TOE use. Upon investigation, the evaluator found that the AGD states the following related to TLS configuration: **Instructions for Setting the Reference Identifier for Certificate Validation in TLS**: • When the TOE acts as a TLS client to LDAPS servers, it obtains the reference identifiers from the administrator configured value in the LDAP Identity Source Hostname/IP field. (Administration application. Menu: Administration > Identity Management > External Identity Sources. Left-Navigation: LDAP. "Connection" tab. Hostname/IP field) • When the TOE acts as a TLS client to TLS Secure Syslog servers, it obtains the reference identifiers from the administrator configured value in the Remote Logging Targets IP/Host Address field. (Administration application. Menu: Administration > System > Logging. Left-Navigation: Remote Logging Targets. IP/Host Address field) • The TOE supports the following presented identifier types: 1. subjectAltName entry of type dNSName (DNS-ID in RFC 6125) 2. CN-ID as defined in RFC 6125 exact case-sensitive match only (i.e., no wildcards supported in CN-ID) 3. subjectAltName entry of type iPAddress; and 4. Wildcards in left-most label subjectAltName entry of type dNSName. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.1.5 FCS_TLSC_EXT.1.4 TSS 1

Objective	The evaluator shall verify that TSS describes the Supported Elliptic Curves/Supported Groups Extension and whether the required behaviour is performed by default or may be configured.
Evaluator Findings	The evaluator examined the FCS_TLSC_EXT.1 entry in section titled 'TOE Summary Specification' in the Security Target to verify that the TSS describes the Supported Elliptic Curves Extension and whether the required behaviour is performed by default or may be configured. Upon investigation, the evaluator found that the TSS states that: The TOE also uses ECC schemes using "NIST curves" P-256, P-384, P-521 and presents the elliptic curve extension in the Client Hello message. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.1.6 FCS_TLSC_EXT.1.4 Guidance 1

Objective	If the TSS indicates that the Supported Elliptic Curves/Supported Groups Extension must be configured to meet the requirement, the evaluator shall verify that AGD guidance includes configuration of the Supported Elliptic Curves/Supported Groups Extension.
Evaluator Findings	The evaluator examined the section titled SSL/TLS Settings in the AGD to verify that, if the TSS indicates that the Supported Elliptic Curves Extension must be configured to meet the requirement, it includes configuration of the Supported Elliptic Curves Extension. Upon investigation, the evaluator found that the AGD states that Enabling FIPS mode in the TOE is the first step to limiting the TLS versions supported to 1.2 and also limits the allowed ciphersuites to the list claimed in the FCS_TLSS_EXT.1.2 SFR of the ST. The next step is to uncheck the “Enable Allow TLS 1.0 only for legacy clients” and “Allow TLS 1.1” checkboxes and check the ‘AllowEnable SHA-1 ciphers” and only for legacy clients“Allow ECDHE-RSA” ” checkboxciphers. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.2 FCS_TLSC_EXT.2

5.7.2.1 FCS_TLSC_EXT.2.1 TSS 1

Objective	The evaluator shall ensure that the TSS description required per FIA_X509_EXT.2.1 includes the use of client-side certificates for TLS mutual authentication.
Evaluator Findings	The evaluator examined the FCS_TLSC_EXT.2 entry in section titled ‘TOE Summary Specification’ in the Security Target to verify that the TSS description required per FIA_X509_EXT.2.1 includes the use of client-side certificates for TLS mutual authentication. Upon investigation, the evaluator found that the TSS states that: The TOE as a client is capable of presenting a certificate to a TLS server for TLS mutual authentication. The TOE supports mutual authentication using X.509 certificates conforming to RFC 5280. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.2.2 FCS_TLSC_EXT.2.1 Guidance 1

Objective	If the TSS indicates that mutual authentication using X.509v3 certificates is used, the evaluator shall verify that the AGD guidance includes instructions for configuring the client-side certificates for TLS mutual authentication.
Evaluator Findings	The evaluator examined the section titled ‘SSL/TLS Settings’ in the AGD to verify that it includes instructions for configuring the client-side certificates for TLS mutual authentication and the TSS indicates that mutual authentication using X.509v3 certificates is used. Upon investigation, the evaluator found that the AGD states that: <u>Steps for Configuring the Client-side Certificates for TLS Authentication:</u> The following two steps are required to configure the client-side certificates for TLS authentication - 1. The TLS server Certificate Authority certificates for the TOE Administration application, the LDAPS Server and the Secure Syslog Audit Server must be imported

	into the “Trusted Certificates” data store. When importing the Trusted Certificate Authority certificate(s), all the following must be configured: a) The checkbox “Validate Certificate Extensions” must be checked. b) The “Trusted For:” fields must be configured as follows: Check the checkbox “Trust for client authentication and Syslog” when the TOE acts as a Secure Syslog client to a Secure Syslog Server and the Trusted Certificate Authority certificate is for the Secure Syslog Server. When the HTTPS client’s certificate authority certificate is being used to authenticate to the TOE using client-certificate authentication, the Certificate Authority Certificate must have the “Trusted for client authentication and Syslog” checkbox checked. c) Check the checkbox “Trust for authentication within ISE” when the Certificate Authority certificate is for the non-TOE LDAPS Server. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.3 FCS_TLSS_EXT.1

5.7.3.1 FCS_TLSS_EXT.1.1 TSS 1

Objective	The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that the ciphersuites supported are specified. The evaluator shall check the TSS to ensure that the ciphersuites specified are identical to those listed for this component.
Evaluator Findings	The evaluator examined the FCS_TLSS_EXT.1 entry in section titled ‘TOE Summary Specification’ in the Security Target to verify that the TSS specifies the ciphersuites supported and that the ciphersuites specified are identical to those listed for this component. Upon investigation, the evaluator found that the TSS states that: The TOE implements TLS 1.2, conformant to RFC 5246 and supports the following ciphersuites as a TLS server – • TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268 • TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246 • TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256 as defined in RFC 5246 • TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246 • TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289 • TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.3.2 FCS_TLSS_EXT.1.1 Guidance 1

Objective	The evaluator shall check the guidance documentation to ensure that it contains instructions on configuring the TOE so that TLS conforms to the description in the TSS (for instance, the set of ciphersuites advertised by the TOE may have to be restricted to meet the requirements).

Evaluator Findings	The evaluator examined the section titled 'SSL/TLS Settings' in the AGD to verify that it contains instructions on configuring the TOE so that TLS conforms to the description in the TSS. Upon investigation, the evaluator found that the AGD contains instructions on configuring the TOE so that TLS conforms to the description in the TSS. Upon investigation, the evaluator found that the AGD states that: In order to only enable the mandatory ciphersuites the other non-standard ciphersuites must be disabled in the browser. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.3.3 FCS_TLSS_EXT.1.2 TSS 1

Objective	The evaluator shall verify that the TSS contains a description of how the TOE technically prevents the use of old SSL and TLS versions.
Evaluator Findings	The evaluator examined the FCS_TLSS_EXT.1 entry in section titled 'TOE Summary Specification' in the Security Target to verify that the TSS contains a description of the denial of old SSL and TLS versions. Upon investigation, the evaluator found that the TSS states that: All connections from clients requesting SSL2.0, SSL3.0, TLS1.0 and TLS1.1 are denied. The TOE only supports standard extensions, methods, and characteristics. TLS is used for HTTPS/TLS for management purposes and to establish encrypted sessions with other instances of the TOE and IT entities to send/receive audit data. The trusted channel is established only when the peer certificate is valid. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.3.4 FCS_TLSS_EXT.1.2 Guidance 1

Objective	The evaluator shall verify that any configuration necessary to meet the requirement must be contained in the AGD guidance.
Evaluator Findings	The evaluator examined the section titled SSL/TLS Settings in the AGD to verify that it contains any configuration necessary to meet the requirement must be contained in the AGD guidance. Upon investigation, the evaluator found that the AGD states that: The SSL/TLS client must be configured for one or more of the above algorithms. See the documentation for your browser for the specific configuration settings. Enabling FIPS mode in the TOE is the first step to limiting the TLS versions supported to 1.2 and also limits the allowed ciphersuites to the list claimed in the FCS_TLSS_EXT.1.2 SFR of the ST. The next step is to uncheck the "Allow TLS 1.0" and "Allow TLS 1.1" checkboxes and check the 'Allow SHA-1 ciphers" and "Allow ECDHE-RSA" ciphers. This will allow ISE as TLS client to LDAPS servers to only support TLS v1.2. Menu: Administration > System > Settings Left-side navigation: Protocols > Security Settings: • Firefox Example Configuration For Firefox, you should open Firefox > Preferences > and select Use TLS 1.2. Next type "about:config" in the address bar. A warning will come up about changing these settings.

	Do a search on security and you will see the algorithms listed as: security.ssl3.rsa_aes_128_sha. In order to only enable the mandatory ciphersuites the other non-standard ciphersuites must be disabled in the browser. Double click on each ciphersuite that must be disabled and the Value will turn to false. See Table 7 below for details. • Internet Explorer Example Configuration To verify TLS is configured Open Internet Explorer > Tools > Internet Options > Advanced – Scroll Down to Security – select TLS 1.2. In order to prioritize the ciphersuites that internet explorer uses > Start > Run 'gpedit.msc' The Local Group Policy Editor will open, then click on > Local Computer Policy > Computer Configuration > Administrative Templates > Network > SSL Configuration Settings – Double click on the SSL Cipher Suite Order > Click Edit Policy Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.3.5 FCS_TLSS_EXT.1.3 TSS 1 **[TD0635]**

Objective	If using ECDHE and/or DHE ciphers, the evaluator shall verify that the TSS lists all EC Diffie-Hellman curves and/or Diffie-Hellman groups used in the key establishment by the TOE when acting as a TLS Server. For example, if the TOE supports TLS_DHE_RSA_WITH_AES_128_CBC_SHA cipher and Diffie-Hellman parameters with size 2048 bits, then list Diffie-Hellman Group 14.
Evaluator Findings	The evaluator examined the FCS_TLSS_EXT.1 entry in section titled 'TOE Summary Specification' in the Security Target to verify that, if using ECDHE or DHE ciphers, the TSS describes the key agreement parameters of the server Key Exchange message. Upon investigation, the evaluator found that the TSS states that: The keys establishment parameters are generated using RSA with key sizes 2048 bits and 4096 bits and DH with 2048 bits. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.3.6 FCS_TLSS_EXT.1.3 Guidance 1

Objective	The evaluator shall verify that any configuration necessary to meet the requirement must be contained in the AGD guidance.
Evaluator Findings	The evaluator examined the section titled 'SSL/TLS' setting in the AGD to verify that it contains any configuration necessary to meet the requirement. Upon investigation, the evaluator found that the AGD states that ISE will disallow importing ISE certificates with 1024 bit RSA key sizes when ISE is in FIPS mode. For Diffie-Hellman parameter size of 2048 bits, configuring ISE into FIPS mode automatically always sets the TLS server ISE Administration application to use Diffie-Hellman parameter size of 2048 bits. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.3.7 FCS_TLSS_EXT.1.4 TSS 1

Objective	The evaluator shall verify that the TSS describes if session resumption based on session IDs is supported (RFC 4346 and/or RFC 5246) and/or if session resumption based on session tickets is supported (RFC 5077).
Evaluator Findings	The evaluator examined the FCS_TLSS_EXT.1 entry of section titled TOE Security Functional Requirement Measures in the Security Target. Upon investigation, the evaluator found that the TSS states that. TLS session resumption is supported by the TOE based on session IDs according to RFC 5246 (TLS1.2). The TOE keeps track of the negotiated sessions using sessions IDs that allows the TOE to resume a TLS session. When a client attempts to reconnect to a TLS server with a session ID, the TLS server can resume the encrypted communication by looking up the session keys. Session IDs are the only context for session resumption. When the TLS server cannot look up the session keys corresponding to the session ID, a new TLS session needs to negotiate via a full TLS handshake. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.3.8 FCS_TLSS_EXT.1.4 TSS 2

Objective	If session tickets are supported, the evaluator shall verify that the TSS describes that the session tickets are encrypted using symmetric algorithms consistent with FCS_COP.1/DataEncryption. The evaluator shall verify that the TSS identifies the key lengths and algorithms used to protect session tickets.
Evaluator Findings	The evaluator examined the section titled 'TOE Summary Specifications' in the Security Target. Upon investigation, the evaluator found that the TSS states that the TOE supports session resumption. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.3.9 FCS_TLSS_EXT.1.4 TSS 3

Objective	If session tickets are supported, the evaluator shall verify that the TSS describes that session tickets adhere to the structural format provided in Section 4 of RFC 5077 and if not, a justification shall be given of the actual session ticket format.
Evaluator Findings	The evaluator examined the section titled 'TOE Summary Specifications' in the Security Target. Upon investigation, the evaluator found that the TSS states that the TOE supports session resumption. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.3.10 FCS_TLSS_EXT.1.4 TSS 4 **[TD0569]**

Objective	If the TOE claims a (D)TLS server capable of session resumption (as a single context, or across multiple contexts), the evaluator verifies that the TSS describes how session resumption operates (i.e. what would trigger a full handshake, e.g. checking session status, checking Session ID, etc.). If multiple contexts are used the TSS describes how session resumption is coordinated across those contexts. In case session establishment and session resumption are

	always using a separate context, the TSS shall describe how the contexts interact with respect to session resumption (in particular regarding the session ID). It is acceptable for sessions established in one context to be resumable in another context.
Evaluator Findings	The evaluator examined the section titled 'TOE Summary Specifications' in the Security Target and determined that the TOE does not claim a (D)TLS server capable of session resumption. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.3.11 FCS_TLSS_EXT.1.4 Guidance 1 [**TD0569]**

Objective	The evaluator shall verify that any configuration necessary to meet the requirement must be contained in the AGD guidance.
Evaluator Findings	The evaluator examined the section titled 'SSL/TLS Settings, Configuring EAP-TLS ' in the AGD to verify that it contains any configuration necessary to meet the requirement. Upon investigation, the evaluator found that the AGD states that: Session Resumption – Session resumption is enabled by default for the TLS server connections and cannot be disabled. Section 4.11 describes the configuration of the EAP -TLS Server session resumption capabilities. For EAP-TLS server by default session resumption is disabled. In the TOE Administration User Interface, the EAP-TLS server session resumption can be enabled by navigation to the menu: Administration > System > Settings Navigate on Left-Side: Protocols > EAP-TLS. Check the "Enable EAP TLS Session Resume" checkbox Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.4 FCS_TLSS_EXT.2

5.7.4.1 FCS_TLSS_EXT.2.1 and FCS_TLSS_EXT.2.2 TSS 1

Objective	The evaluator shall ensure that the TSS description required per FIA_X509_EXT.2.1 includes the use of client-side certificates for TLS mutual authentication.
Evaluator Findings	The evaluator examined the section titled 'TOE summary specification' in the Security Target to verify that the TSS description required per FIA_X509_EXT.2.1 includes the use of client-side certificates for TLS mutual authentication. Upon investigation, the evaluator found that the TSS states that The TOE also uses ECC schemes using "NIST curves" P-256, P-384, P-521 and presents the elliptic curve extension in the Client Hello message. The TOE as a client is capable of presenting a certificate to a TLS server for TLS mutual authentication. The TOE supports mutual authentication using X.509 certificates conforming to RFC 5280. . Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.4.2 FCS_TLSS_EXT.2.1 and FCS_TLSS_EXT.2.2 TSS 2

Objective	The evaluator shall verify the TSS describes how the TSF uses certificates to authenticate the TLS client. The evaluator shall verify the TSS describes if the TSF supports any fallback

	authentication functions (e.g. username/password, challenge response) the TSF uses to authenticate TLS clients that do not present a certificate. If fallback authentication functions are supported, the evaluator shall verify the TSS describes whether the fallback authentication functions can be disabled.
Evaluator Findings	The evaluator examined the section titled 'TOE summary specification' in the Security Target to verify that the TSS describes how the TSF uses certificates to authenticate the TLS client. The evaluator verifies the TSS describes if the TSF supports any fallback authentication functions (e.g. username/password, challenge response) the TSF uses to authenticate TLS clients that do not present a certificate. If fallback authentication functions are supported and verify the TSS describes whether the fallback authentication functions can be disabled. Upon investigation, the evaluator found that the TSS states that the TOE only supports standard extensions, methods, and characteristics. TLS is used for HTTPS/TLS for management purposes and to establish encrypted sessions with other instances of the TOE and IT entities to send/receive audit data. The trusted channel is established only when the peer certificate is valid. LDAPS has support for additional extensions to support communication with external authentication stores. The TOE verifies that the presented identifier matches the reference identifier according to RFC 6125. When the TOE acts as a TLS client to LDAPS servers, it obtains the RFC 6125 reference identifiers from the administrator configured value in the LDAP Identity Source Hostname/IP field. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.4.3 FCS_TLSS_EXT.2.1 and FCS_TLSS_EXT.2.2 Guidance 1

Objective	If the TSS indicates that mutual authentication using X.509v3 certificates is used, the evaluator shall verify that the AGD guidance includes instructions for configuring the client-side certificates for TLS mutual authentication.
Evaluator Findings	The evaluator examined the section titled SSL/TLS setting in the AGD to verify that, if the TSS indicates that mutual authentication using X.509v3 certificates is used, it includes instructions for configuring the client-side certificates for TLS mutual authentication. Upon investigation, the evaluator found that the AGD provides instructions for configuring client-side certificates. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.4.4 FCS_TLSS_EXT.2.1 and FCS_TLSS_EXT.2.2 Guidance 2

Objective	The evaluator shall verify the guidance describes how to configure the TLS client certificate authentication function. If the TSF supports fallback authentication functions, the evaluator shall verify the guidance provides instructions for configuring the fallback authentication functions. If fallback authentication functions can be disabled, the evaluator shall verify the guidance provides instructions for disabling the fallback authentication functions.
Evaluator Findings	The evaluator examined the section titled 'Authentication Stores 'in the AGD. The TOE doesn't support fallback authentication functions Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

5.7.4.5 FCS_TLSS_EXT.2.3 TSS 1

Objective	The evaluator shall verify that the TSS describes which types of identifiers are supported during client authentication (e.g. Fully Qualified Domain Name (FQDN)). If FQDNs are supported, the evaluator shall verify that the TSS describes that corresponding identifiers are matched according to RFC6125. For all other types of identifiers, the evaluator shall verify that the TSS describes how these identifiers are parsed from the certificate, what the expected identifiers are and how the parsed identifiers from the certificate are matched against the expected identifiers.
Evaluator Findings	The evaluator examined the section titled 'TOE summary specification' in the Security Target. Upon investigation, the evaluator found that the TSS states that the TOE supports reference identifiers as configured by the Administrator to be either FQDN or IP address and compares it to the Subject Alternative Name (SAN) or the Common Name (CN) fields in the certificate of the peer. The order of comparison is SAN followed by CN. If the TOE successfully matches the reference identifier to the presented identifier, IKE authentication will succeed. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.4.6 FCS_TLSS_EXT.2.3 Guidance 1

Objective	The evaluator shall ensure that the AGD guidance describes the configuration of expected identifier(s) for X.509 certificate-based authentication of TLS clients. The evaluator ensures this description includes all types of identifiers described in the TSS and, if claimed, configuration of the TOE to use a directory server.
Evaluator Findings	The evaluator examined the section titled 'SSL/TLS Settings' in the AGD to verify that it contains any configuration necessary to meet the requirement. Upon investigation, the evaluator found that the AGD states that • When the TOE acts as a TLS client to TLS Secure Syslog servers, it obtains the reference identifiers from the administrator configured value in the Remote Logging Targets IP/Host Address field. (Administration application. Menu: Administration > System > Logging. Left-Navigation: Remote Logging Targets. IP/Host Address field) The following two steps are required to configure the client-side certificates for TLS authentication - • The TLS server Certificate Authority certificates for the TOE Administration application, the LDAPS Server and the Secure Syslog Audit Server must be imported into the "Trusted Certificates" data store. When importing the Trusted Certificate Authority certificate(s), all of the following must be configured: • The checkbox "Validate Certificate Extensions" must be checked. • The "Trusted For:" fields must be configured as follows: Check the checkbox "Trust for client authentication and Syslog" when the TOE acts as a Secure Syslog client to a Secure Syslog Server and the Trusted Certificate Authority certificate is for the Secure Syslog Server. When the HTTPS client's certificate authority certificate is being used to authenticate to the TOE using client-certificate authentication, the Certificate Authority Certificate must have the "Trusted for client authentication and Syslog" checkbox checked. • Check the checkbox "Trust for authentication within ISE" when the Certificate Authority certificate is for the non-TOE LDAPS Server.

	• The configured TOE Server certificate for usage “EAP Authentication” must contain one of the supported RFC 6125 reference identifiers as configured on the LDAPS Server(s) and Secure Syslog Audit Server(s). • When the TOE acts as a TLS client to LDAPS servers, it obtains the RFC 6125 reference identifiers from the administrator configured value in the LDAP Identity Source Hostname/IP field. (Administration application. Menu: Administration > Identity Management > External Identity Sources. Left-Navigation: LDAP. “Connection” tab. Hostname/IP field) • When the TOE acts as a TLS client to TLS Secure Syslog servers, it obtains the reference identifiers from the administrator configured value in the Remote Logging Targets IP/Host Address field. (Administration application. Menu: Administration > System > Logging. Left-Navigation: Remote Logging Targets. IP/Host Address field). • The TOE supports the following presented identifier types: • subjectAltName entry of type dNSName (DNS-ID in RFC 6125) • CN-ID as defined in RFC 6125, • subjectAltName entry of type iPAddress; and • Wildcards in DNS domain names. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8 TSS and Guidance Activities (Identification and Authentication)

5.8.1 FIA_AFL.1

5.8.1.1 FIA_AFL.1 TSS 1

Objective	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.
Evaluator Findings	The evaluator examined the FIA_AFL.1 entry in 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: The TOE provides the privileged administrator the ability to specify the maximum number of unsuccessful authentication attempts before privileged administrator or non-privileged administrator is locked out through the administrative CLI using a privileged CLI command or the GUI. When a privileged administrator or non-privileged administrator attempting to log into the administrative CLI or GUI exceeds the administratively set maximum number of failed authentication attempts, the user will not be granted access to the administrative

	functionality of the TOE until a privileged administrator resets the user's number of failed login attempts through the administrative CLI or GUI. Based on these findings, this assurance activity is considered satisfied.
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	The evaluator examined the FIA_AFL.1 entry in 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: To ensure the Administrator account does not get locked out by the number of failed attempts, the Emergency account must be enabled. This requires the use of an enabled local administrator account that has read-write access and web access. The purpose of this account is a work around to ensure administrator access to the TOE is available when remote authentication is not available. Access to this account should be limited and only used when no other option is available to gain access to the TOE, such as another Authorized Administrator. Based on these findings, this assurance activity is considered satisfied.
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	The evaluator examined the section titled 'User Lockout' 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 provides commands and additional guidance on authentication command for SSH sessions regarding failed attempts or unlocking an account. 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	The evaluator examined the section titled 'User Lockout' 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: To ensure the Administrator account does not get locked out by the number of failed attempts, the Emergency account must be enabled. This requires the use of an enabled local administrator account that has read-write access and web access. The purpose of this account is a work around to ensure administrator access to the TOE is available when remote authentication is not available. Access to this account should be limited and only used in when no other option is available to gain access to the TOE, such as another Authorized Administrator. Based on these findings, this assurance activity is considered satisfied.

5.8.2 FIA_PMG_EXT.1

5.8.2.1 FIA_PMG_EXT.1.1 TSS 1

Objective	The evaluator shall examine the TSS to determine that it contains the lists of the supported special character(s) and minimum and maximum number of charters supported for administrator passwords.
Evaluator Findings	The evaluator examined the FIA_PMG_EXT.1 entry in 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 and maximum number of charters supported for administrator passwords. Upon investigation, the evaluator found that the TSS states that: The TOE supports the local definition of users with corresponding passwords. The passwords can be composed of any combination of upper and lower case letters, numbers, and special characters (that include: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")"). Minimum password length is settable by the Security Administrator, with a default of six characters and can be configured for minimum password lengths of 15 characters or greater. It is configured via the Administration menu in the web-based UI, on the Admin Actions tab, under Password Policy Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.2.2 FIA_PMG_EXT.1.1 Guidance 1

Objective	The evaluator shall examine the guidance documentation to determine that it: a) identifies the characters that may be used in passwords and provides guidance to security administrators on the composition of strong passwords, and b) provides instructions on setting the minimum password length and describes the valid minimum password lengths supported.
Evaluator Findings	The evaluator examined the section titled 'Initial Setup' 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: 1. Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”]; 2. Minimum password length shall be settable by the Security Administrator, and support passwords of 15 characters or greater. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.3 FIA_PSK_EXT.1

5.8.3.1 FIA_PSK_EXT.1.1 TSS 1

Objective	The evaluator shall examine the TSS to ensure that it identifies all protocols that allow text-based pre-shared keys and states that text-based pre-shared keys of 22 characters are supported. For each protocol identified by the requirement. The evaluator shall also verify that the selection of IPsec or RadSec matches the selection in FTP_ITC.1.
Evaluator Findings	The evaluator reviewed the FIA_PSK_EXT.1.1 entry in the section ‘TOE Summary Specification’ for determining this requirement. Within this section, the evaluator found the following text : The TOE supports use of IKEv1 (ISAKMP) and IKEv2 pre-shared keys for authentication of IPsec tunnels. Preshared keys can be entered as ASCII character strings, or HEX values. The TOE supports keys that are from 22 characters in length up to 127 characters in length. The data that is input is conditioned prior to use via SHA-1. Use for pre-shared keys is also supported by the TOE for RADIUS protocol. The evaluator verified that the selection of IPsec matches the selection in FTP_ITC.1. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

1.1.1.1 FIA_PSK_EXT.1.1 Guidance 1

Objective	The evaluator shall examine the operational guidance to determine that it provides guidance to administrators on the composition of strong text-based pre-shared keys and (if the selection indicates keys of various lengths can be entered) that it provides information on the range of lengths supported. The guidance must specify the allowable characters for pre-shared keys and that list must be a super-set of the list contained in FIA_PSK_EXT.1.2.
Evaluator Findings	The evaluator examined the Guidance document and determined that it provides guidance to administrators on the composition of strong pre-shared keys in section ‘IKEv1 Transform Sets’ and ‘IKEv2 Transform Sets’. The evaluator found that the AGD states the following: TOE-common-criteria(config)# Crypto isakmp key cisco123!cisco123!CISC address 11.1.1.4 Note: Pre-shared keys on the TOE must be at least 22 characters in length and can be composed of any combination of upper and lower case letters, numbers, and special characters (that include: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, and “)”). The TOE supports pre-shared keys up to 128 bytes in length. While longer keys increase the difficulty of brute-force attacks, longer keys increase processing time.

	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 FIA_UIA_EXT.1 entry in 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: The TOE requires all users to be successfully identified and authenticated before allowing any services and/or TSF mediated actions to be performed (other than the display of the warning banner) per the authentication policy. A pre-authentication banner is also displayed at both the CLI and GUI. Access to the web-based interface (via HTTPS), the CLI (SSH), and the console, all require at a minimum username and password be provided and successfully verified prior to access being granted. A successful login requires a correct username and password pair be confirmed, as existing in the local user database or a remote authentication store. The SSH interface supports authentication using SSH keys which are provided during the SSH connection request. Based on these findings, this assurance activity is considered satisfied.
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	The evaluator examined the FIA_UIA_EXT.1 entry in 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: The TOE requires all users to be successfully identified and authenticated before allowing any services and/or TSF mediated actions to be performed (other than the display of the warning banner) per the authentication policy. Based on these findings, this assurance activity is considered satisfied.
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 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	The evaluator examined the section titled Secure Management 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. Upon investigation, the evaluator found that the AGD provides instructions for configuring user authentication on the TOE. Configuration of Identification and Authentication settings is restricted to the CLI administrator and Identity Admin, Super Admin, and System Admin group roles on the GUI. Based on these findings, this assurance activity is considered satisfied.
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	The evaluator examined the section titled Identification and Authentication in the AGD to verify that it describes any necessary preparatory steps to ensure authentication data is not revealed while entering for each local login allowed. Upon investigation, the evaluator found that the AGD states that: Configuration of Identification and Authentication settings is restricted to the CLI administrator and Identity Admin, Super Admin, and System Admin group roles on the GUI. The ISE 3.1 can be configured to use the following authentication methods: • Local authentication o administrative password - Requires user to provide correct username and password combination to authenticate o public-key based - Requires user to provide correct username and private key combination to authenticate During each login attempt, authentication data is not revealed when credentials are entered, and this is implemented by default. No additional preparatory steps are required for the same 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 FIA_X509_EXT.1 entry in 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 uses X.509v3 certificates as defined by RFC 5280 to support authentication for IPsec connections and to support authentication for TLS connections to the audit server and the authentication server. When a certificate is imported/added into the TOE, the purpose for which the certificate is to be used needs to be specified - Admin: Authenticating the Admin portal EAP: For TLS-based EAP authentication Portal: For communicating with all Cisco ISE end-user portals Different certificates from each node for communicating with the Admin portal (Admin) and for TLS-based EAP authentication (EAP) can be associated. However, only one certificate from each node for each of these purposes can be associated. The certificate path is validated by ensuring that all the CA certificates have the basicConstraints extension and the CA flag is set to TRUE and the certificate path must terminate with a trusted CA certificate. The extendedKeyUsage field is validated according to the rules listed below. • The TSF shall validate the extendedKeyUsage field according to the following rules: ○ *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.* ○ *Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.* ○ *Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.* ○ *OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.* Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.6.2 FIA_X509_EXT.1/Rev TSS 2

Objective	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.
Evaluator Findings	The evaluator examined the FIA_X509_EXT.1 entry in 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:

	OCSP and CRL revocation checking is performed when authenticating a certificate provided by the remote server during TLS establishment. Both OCSP and CRL may be used to validate the revocation status of the certificates when ISE acts as a Secure LDAP (LDAPS) client to LDAPS servers. For all other cases, it's only CRL that is supported to validate the certificate revocation status. Checking is also done for the basicConstraints extension and the CA flag to determine whether they are present and set to TRUE. If they are not, the certificate is not accepted. An automatic process for loading CRLs is provided by the TOE. Based on these findings, this assurance activity is considered satisfied.
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	The evaluator examined the section titled X.509 Certificates 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 all the information about validity of the certificates and revocation. Based on these findings, this assurance activity is considered satisfied.
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.
Evaluator Findings	The evaluator examined the FIA_X509_EXT.2 entry in section titled 'TOE Summary Specification' in the Security Target to verify that the TSS describes how the TOE chooses which certificates to use. Upon investigation, the evaluator found that the TSS states that: When a certificate is imported/added into the TOE, the purpose for which the certificate is to be used needs to be specified - Admin: Authenticating the Admin portal EAP: For TLS-based EAP authentication Portal: For communicating with all Cisco ISE end-user portals Different certificates from each node for communicating with the Admin portal (Admin) and for TLS-based EAP authentication (EAP) can be associated. However, only one certificate from each node for each of these purposes can be associated. Based on these findings, this assurance activity is considered satisfied.
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	The evaluator examined the FIA_X509_EXT.2 entry in 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: The TOE performs validation when communication is received from a peer during establishment of a session. When the connection to determine the validity of the certificate cannot be established, the TOE allows the administrator to either accept/not accept the certificate based on the following conditions - a. accept the certificate when: 1. the CRL revocation HTTP download fails with the ISE configuration setting 'Bypass CRL Verification if CRL is not Received' is checked. (e.g., the CRL Distribution HTTP URL server host is unreachable. CRL download receives an HTTP 500 error) 2. OCSP revocation checks on LDAPS client connections fail and the ISE configuration contains the two checkboxes unchecked: Reject the request if OCSP returns UNKNOWN status; and Reject the request if OCSP Responder is unreachable b. not accept the certificate when: 1. the CRL revocation HTTP download fails with the ISE configuration setting 'Bypass CRL Verification if CRL is not Received' is unchecked. 2. OCSP revocation checks on LDAPS client connections fail and the ISE configuration contains the two checkboxes checked: Reject the request if OCSP returns UNKNOWN status; and Reject the request if OCSP Responder is unreachable. If the connection to determine the certificate validity cannot be established, the administrator is able to choose whether or not to accept the certificate. The evaluator verified that the required configuration commands are present in the AGD. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.7.3 FIA_X509_EXT.2 Guidance 1

Objective	The evaluator shall check the administrative guidance to ensure that it includes any necessary instructions for configuring the operating environment so that the TOE can use the certificates.
Evaluator Findings	The evaluator examined the section titled 'X.509 Certificates' in the AGD to ensure that it includes any necessary instructions for configuring the operating environment so that the TOE can use the certificates. Upon investigation, the evaluator found that the AGD states that:

	The TOE may be configured by the privileged administrators to use X.509v3 certificates to authenticate IPsec peers. RSA certificates are supported. Creation of these certificates and loading them on the TOE is covered in the section – "Configuring Certificate Enrollment for a PKI" in [8], and a portion of the TOE configuration for use of these certificates follows below. The evaluator observed the subsequent steps and found that the AGD included all the steps for configuring the operating environment. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.7.4 FIA_X509_EXT.2 Guidance 2

Objective	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	The evaluator examined the section titled 'Steps for Configuring X.509 Certificate Revocation Configuring a Revocation Mechanism for PKI Certificate Status Checking and Checking Validity' in the AGD to verify that, if the requirement that the administrator is able to specify the default action, the guidance documentation contains instructions on how this configuration action is performed. Upon investigation, the evaluator found that the AGD contains information about configuration. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.7.5 FIA_X509_EXT.2 Guidance 3

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	The evaluator examined the section titled Configuring Certificate Chain Validation in the AGD. Upon investigation, the evaluator found that the AGD states that: A trustpoint associated with the root CA cannot be configured to be validated to the next level. The chain-validation command is configured with the continue keyword for the trust point associated with the root CA, an error message will be displayed, and the chain validation will revert to the default chain-validation command setting. Based on these findings, this assurance activity is considered satisfied.
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.

Evaluator Findings	The evaluator examined the FIA_X509_EXT.3 entry in section titled 'TOE Summary Specification' in the Security Target to verify that the TSS contains a description of the device-specific fields used in certificate requests. Upon investigation, the evaluator found that the TSS states that: The device-specific information used is 'Node, city and state.' Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

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	The evaluator examined the section titled 'X.509' Certificates 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 AGD provides instructions for generating CSRs. The evaluator found that these instructions include the complete set of steps necessary to configure a fully formed CSR containing each of the fields described in FIA_X509_EXT.3. Finally, the evaluator found that AGD provides instructions for generating CSRs from the CLI. Based on these findings, this assurance activity is considered satisfied.
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	The evaluator examined the guidance documentation to determine if any necessary steps to perform manual update are described. The evaluator also verified that the guidance documentation provides warnings regarding functions that may cease to operate during the update. Upon investigation, the evaluator found that Section 'Secure Acceptance of the TOE' of AGD states the following: Step 7 Approved methods for obtaining a Common Criteria evaluated software images: • Download the Common Criteria evaluated software image file from Cisco.com onto a trusted computer system. Software images are available from Cisco.com at the following: http://www.cisco.com/cisco/software/navigator.html. • The TOE ships with the correct software images installed.

	Step 8 Digital Signature mechanism is used to verify software/firmware update files (to ensure they have not been modified from the originals distributed by Cisco) before they are used to actually update the applicable TOE components. The updates can be downloaded from the software.Cisco.com. The TOE image files are digitally signed so their integrity can be verified during the boot process, and an image that fails an integrity check will not be loaded. The digital certificates used by the update verification mechanism are contained on the TOE. If the digital signature fails, contact Cisco Technical Assistance Center (TAC) https://tools.cisco.com/ServiceRequestTool/create/launch.do. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.2 FMT_FMT_MOF.1/Functions

5.9.2.1 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	The evaluator examined the FMT_MOF.1/Functions entry in 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: On the TOE, the local log files rotate after a certain size threshold is reached. The number of days of local log files is configurable, with the default of keeping records only up to last 7 days. From the Administration > System > Logging > Local Log Settings page an administrator is able to configure the storage period for logs in days and delete the existing log file. Only the Security Administrator may delete all of the rolled over log files by the "Delete Local Logs Now" selection in the administration application. The ISE RBAC (Role-Based Access Control) policy does not allow for any user that is not a Security Administrator to delete log files. No user can modify log files because there is no mechanism that allows this. After the configured storage period of time has passed for logs the events exceeding the age are deleted. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.2.2 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	The evaluator examined the section titled 'Security Relevant Events' 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: ISE 3.1 can maintain logs in multiple locations: local storage of the generated audit records, and when configured for a syslog backup will simultaneously offload those events to a peer instantiation of ISE or a different log server. ISE 3.1 administrators should review logs at both locations. Instructions for viewing logs are found in AGD Section 5.1 Audit events are simultaneously sent to the external server and the local store upon creation. If the external server is not available the TOE will buffer events until they can be sent. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.3 FMT_MOF.1/Services

5.9.3.1 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 FMT_MOF.1/Services entry in 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: From the Administration > System > Logging > Local Log Settings page an administrator is able to configure the storage period for logs in days and delete the existing log file. Only the Security Administrator may delete all of the rolled over log files by the "Delete Local Logs Now" selection in the administration application. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.3.2 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 Deleting Audit Records 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 that: From the Administration > System > Logging > Local Log Settings page a System admin or a Super admin is able to configure the storage period for logs in days and delete the existing log file. The administrator may delete all of the rolled over log files by the "Delete Local Logs Now" selection in the administration application. After the configured storage period of time has passed for logs the events exceeding the age are automatically deleted.

	TCP syslog buffers events in a local file that is limited to a total of 100MB. The limit is specified as a file size, not a specific number of events. Overwriting is handled by wrapping to the beginning of the file (overwriting the oldest events). The value of 100MB is configurable and the lowest value for the configuration is 10 MB and the allowed increments need to be whole numbers 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	The evaluator examined the FMT_MTD.1/CoreData entry in 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: None of the administrative functions of the product are available prior to administrator log-in. The evaluator examined the FMT_MTD.1/CoreData entry in 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: The TOE restricts the ability to enable the functions to perform manual update to the Security Administrator. The TOE restricts access to the management functions to the Security Administrator. Based on these findings, this assurance activity is considered satisfied.
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	The evaluator examined the FMT_MTD.1/CoreData entry in 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: The TOE restricts the ability to enable the functions to perform manual update to the Security Administrator. The TOE restricts access to the management functions to the Security Administrator. The TOE supports two levels of administrators, the CLI-admin (local console or SSHv2 accessible) and the web-based admin user. The same functionality is available on the

	TOE via the web-based interface and CLI, with the exception that only the CLI-admin can start and stop the ISE application and reload (update) or shutdown the ISE appliance via the CLI. None of the administrative functions of the product are available prior to administrator log-in. Based on these findings, this assurance activity is considered satisfied.
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 following sections in each 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 each AGD includes configuration of the following in the respective sections:
	• Audit Configuration
	  ○ *Sections titled 'Logging Configuration', 'Logging Protection', and 'Security Relevant Events'*
	• Identification/Authentication
	  ○ *Sections titled 'User Roles', 'Passwords', 'Identification and Authentication', 'User Lockout'*
	• SSH configuration
	  ○ *Section titled 'Remote Administration Protocols*
	• IPsec configuration
	  ○ *Section titled 'IPsec Overview'*
	• Time stamps
	  ○ *Section titled 'Clock Management'*
	• Session time-out
	  ○ *Section titled 'Session Termination'*
	• TOE Banner
	  ○ *Section titled 'Login Banners'*
	• TOE updates
	  ○ *Section titled 'Secure Acceptance of the TOE'*
	• X.509 Certificates
	  ○ *Section titled 'X.509 Certificates'*
	The evaluator found that this encompasses all the TSF-data manipulating functionality required by the NDcPP.
	Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass

5.9.4.4 FMT_MTD.1/CoreData Guidance 2

Objective	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

	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	The evaluator examined the section titled 'Storing Certificates to a Local Storage Location' 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: Certificates are stored to NVRAM by default; however, some routers do not have the required amount of NVRAM to successfully store certificates. All Cisco platforms support NVRAM and flash local storage. Depending on the platform, an authorized administrator may have other supported local storage options including bootflash, slot, disk, USB flash, or USB token. During run time, an authorized administrator can specify what active local storage device will be used to store certificates. The evaluator examined the section titled 'Storing Certificates to a Local Storage Location' 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 following: The summary steps for storing certificates locally to the TOE are as follows: 1. Enter configure terminal mode: Device # configure terminal 2. Specify the local storage location for certificates: crypto pki certificate storage location-name Device(config)# crypto pki certificate storage flash:/certs 3. Exit: Device(config)# exit 4. Save the changes made: Device# copy system:running-config nvram:startup-config 5. Display the current setting for the PKI certificate storage location: Device# show crypto pki certificates storage Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.5 FMT_MTD.1/CryptoKeys

5.9.5.1 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	The evaluator examined the FMT_MTD.1/ CryptoKeys entry in 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:

	The Security administrator have the ability to generate, delete and import/export cryptographic keys. - Ability to configure the RADIUS shared secret - Ability to define an authorized NAS - Ability to enable, disable, and determine and modify the behavior of all the security functions of the TOE identified in this EP to the administrator - [Ability to configure the IPsec functionality] Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.5.2 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	The evaluator examined the section titled 'SSH Public-Key Authentication' 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 the following: 1. Authorize the use of the public key for the user created in step 1. • Login to the ISE Command Line Interface (CLI) as the user created in step 1 using the password authentication method. • Add the SFTP server host key Run the EXEC command 'crypto host_key add host <FQDN or IPv4 address>' hostname/userid# crypto host_key add host <FQDN or IPv4 address> where <FQDN or IPv4 address> MUST match the value configured under the SFTP Repository 'Server Name' field value. • Verify that the SSH RSA public key file is accessible from the ISE SFTP client. hostname/userid# show repository sftp | include foobar foobar_ise-administration-node.key.pub The foobar_ise-administration-node.key.pub filename output after the command indicates that the public key file in the example is present at the SFTP server and the ISE SFTP client is able to perform a file listing for the file. • Authorize the public key for user Run the 'crypto key import <public key filename> repository <repository name>' command to authorize use of the SSH RSA public key in the <public key filename> for the currently logged in CLI user. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.6 FMT_SMF.1

5.9.6.1 FMT_SMF.1 TSS 1

Objective	The evaluator shall confirm that the TSS details which security management functions are available through which interface(s) (local administration interface, remote administration interface). The evaluator shall examine the TSS and Guidance Documentation to verify they both describe the local administrative interface.
Evaluator Findings	The evaluator examined the entry for FMT_SMF.1 in the section 'TOE Summary Specification' to verify that it details which security management functions are available through which interface(s). Upon investigation, the evaluator found that the TSS states that: The TOE provides all the capabilities necessary to securely manage the TOE, the services provided by the TOE. The management functionality of the TOE is provided through the TOE CLI or HTTPS web-based interface. The specific management capabilities available from the TOE are identified in the text of the SFR - FMT_SMF.1. The Security administrator have the ability to generate, delete and import/export cryptographic keys. Based on these findings, this assurance activity is considered satisfied.
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	The evaluator examined the section titled 'Operational Environment Components and Secure Installation and Configuration' in the AGD to verify that it describes the local administrative interface. Upon investigation, the evaluator found that the AGD states that console provides the connection to the ISE appliance for administration and management Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.7 FMT_SMR.2

5.9.7.1 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	The evaluator examined the section titled 'TOE Summary Specification' to verify that the TOE supported roles and any restrictions of the roles involving administration of the TOE. Upon investigation, the evaluator found that the AGD states that. Cisco ISE provides role-based access control (RBAC) policies that ensure security by restricting administrative privileges. RBAC policies are associated with default admin groups to define roles and permissions. A standard set of permissions (for menu as well as data access) is paired with each of the predefined admin groups, and is thereby aligned with the associated role and job function.

	RBAC restricts system access to authorized users through the use of roles that are then associated with admin groups. Each admin group has the ability to perform certain tasks with permissions that are defined by an RBAC policy. Policies restrict or allow a person to perform tasks that are based on the admin group (or groups) to which that person is assigned. A user can be assigned to multiple roles, which provides them with privileges for each role to which they are assigned. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.7.2 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	The evaluator examined the section titled Remote Administration Protocols 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 that ISE provides two ways to manage the TOE remotely and that it includes all the required configuration that needs to be performed on the client for remote administration. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.10 TSS and Guidance Activities (Protection of the TSF)

5.10.1 FPT_APW_EXT.1

5.10.1.1 FPT_APW_EXT.1 TSS 1

Objective	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.
Evaluator Findings	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. The evaluator also examined the FPT_APW_EXT.1 entry in 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: The TOE by default secures all locally defined user passwords using SHA256 hashing for CLI passwords, and AES encryption for GUI credentials. In this manner, the TOE ensures that plaintext user passwords will not be disclosed even to administrators. The TOE stores all private keys in a secure directory that is not accessible to administrators. There is no way an administrator can access/view the private keys in the secure directory

	where they are stored. All pre-shared and symmetric keys are stored in encrypted (AES) form to prevent access. TOE is designed specifically to not disclose any keys stored in the TOE. All pre-shared and symmetric keys are stored in encrypted form using AES encryption to additionally obscure access. The AES key used for this encryption is stored on the filesystem and in DRAM. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.10.2 FPT_SKP_EXT.1

5.10.2.1 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 FPT_SKP_EXT.1 entry in 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 TOE stores all private keys in a secure directory that is not accessible to administrators. There is no way an administrator can access/view the private keys in the secure directory where they are stored. All pre-shared and symmetric keys are stored in encrypted (AES) form to prevent access. TOE is designed specifically to not disclose any keys stored in the TOE. All pre-shared and symmetric keys are stored in encrypted form using AES encryption to additionally obscure access. The AES key used for this encryption is stored on the filesystem and in DRAM. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.10.3 FPT_STM_EXT.1

5.10.3.1 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 FPT_STM_EXT.1 entry in 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 provides a source of date and time information, used in audit timestamps. This function can be configured from the Administration > System > Settings > System Time page by a Super Admin or System Admin role only. The clock function is reliant on the system clock provided by the underlying hardware. This date and time is used as the time stamp that is applied to TOE generated audit records and used to track inactivity of administrative sessions. The time information is also used to set system time, determining AAA timeout, administrative session timeout and checking for expiry of certificates. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.10.3.2 FPT_STM_EXT.1 Guidance 1

Objective	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. 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.
Evaluator Findings	The evaluator examined the section titled 'Clock Management' 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: Configuration of clock settings is limited to the CLI administrator and Super Admin and System Admin group roles on the GUI and This version of TOE cannot provide secure NTP channel. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.10.4 FPT_TST_EXT.1.1

5.10.4.1 FPT_TST_EXT.1.1 TSS 1

Objective	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.
Evaluator Findings	The evaluator examined the FPT_TST_EXT.1 entry in 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: The self-tests include:

	AES Known Answer Test - With a known input and output, the AES algorithm implementation is tested by comparing the result with the expected result. This is done separately for both encryption and decryption. AES-GCM Known Answer Test - With a known input and output, the AES algorithm implementation in GCM mode is tested by comparing the result with the expected result. This is done separately for both encryption and decryption. FIPS 186-4 ECDSA Sign/Verify Test – The ECDSA signature and verification implementation is tested. ECC CDH Know Answer Test – This tests the SP800-56A Section 5.7.1.2 Elliptic Curve Cryptography Cofactor Diffie-Hellman (ECC CDH) Primitive. RSA Known Answer Test – With a known input and output, the RSA signature service algorithm is tested by comparing the result with the expected result. This is done separately for both signing and verification. DRBG Known Answer Test - (CTR_DRBG KAT) – With known input and output, the DRBG computation is tested by comparing an expected pre-computed and stored result against the result computed at runtime. HMAC Known Answer Test - This includes the HMAC-SHA1 KAT, HMAC-SHA256KAT, HMAC-SHA384KAT and HMAC-SHA512 KAT. With a known input and output, the keyed-hash message authentication using each of the HMAC-SHA1, HMAC-SHA256 and HMACSHA512 algorithms is tested by comparing the result with the expected result. SHA-1/256/384/512 Known Answer Test - With a known input and output, the cryptographic hashing service implementation using each of the SHA1, SHA256 and SHA512 algorithms is tested by comparing the result with the expected result. Software Integrity Test (HMAC-SHA1) - The HMAC-SHA1 value of the module is computed and compared to the correct already-computed HMAC-SHA1 value for verification. The evaluator examined the FPT_TST_EXT.1 entry in 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: These tests are sufficient to verify that the correct version of the TOE software is running as well as that the cryptographic operations are all performing as expected Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.10.4.2 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	The evaluator examined the section titled 'Modes of Operation' 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 the following: ISE uses a cryptographic module, that runs a suite of self-tests during the TOE initial start-up to verify its correct operation. These tests check the integrity of the code, and the correct operation of each cryptographic algorithm and method used (i.e. AES-CBC, SHA-1, etc.) If any of the tests fail, the administrative web-based UI will not be accessible, and the security administrator will for a limited time window be able to login to the CLI on the KVM (keyboard, video, mouse) console to run the CLI command – "*show application status ise*" to determine that services have been disabled because "FIPS INTEGRITY CHECK HAS FAILED". Eventually the administrator will be unable to login to the CLI even on the KVM as all services are shutdown including the ability to login to the CLI. After authenticating, a fatal error is displayed, and the user is only allowed to press <Enter> to logout and no other actions can be performed. The error message is: "ERROR: ISE SERVICES HAVE BEEN DISABLED BECAUSE FIPS INTEGRITY CHECK HAS FAILED! EITHER REIMAGE FROM ISE INSTALLATION MEDIA, OR CONTACT CISCO TECHNICAL SUPPORT CENTER FOR INSTRUCTIONS ON DIAGNOSING THE FAILURE. Press <Enter> to logout". Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.10.5 FPT_TUD_EXT.1

5.10.5.1 FPT_TUD_EXT.1 TSS 1

Objective	The evaluator shall verify that the TSS describes 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 FPT_TUD_EXT.1 entry in 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: The TOE has specific versions that can be queried by an administrator from the CLI using the "show version" command, or from the administration GUI, lower left "Help" > About Identity Services Engine. When updates are made available by Cisco, an administrator (specifically the Super Admin or System Admin) can manually obtain the updates from the Cisco website and install them. Digital Signatures and published hash mechanisms are used to verify software/firmware update files (to ensure they have not been modified from the originals distributed by Cisco) before they are used to actually update the applicable TOE components. The updates can be downloaded from the software.Cisco.com The evaluator examined the FPT_TUD_EXT.1 section titled 'TOE Summary Specification' in the Security Target to verify that the TSS, if a trusted update can be installed on the TOE with a delayed activation, describes how and when the inactive version becomes active. Upon investigation, the evaluator found that the TSS states that: The TOE does not support delayed activation. Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass

5.10.5.2 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 or published hash of the update, and the actions that take place for both successful and unsuccessful signature verification or published hash verification.
Evaluator Findings	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 software, 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: Digital Signatures and published hash mechanisms are used to verify software/firmware update files (to ensure they have not been modified from the originals distributed by Cisco) before they are used to actually update the applicable TOE components. The updates can be downloaded from the software.Cisco.com. The evaluator examined the FPT_TUD_EXT.1 entry in section titled 'TOE Summary Specification' in the Security Target to 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 or published hash of the update, and the actions that take place for both successful and unsuccessful signature verification or published hash verification. Upon investigation, the evaluator found that the TSS states that: The TOE image files are digitally signed so their integrity can be verified during the boot process, and an image that fails an integrity check will not be loaded. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.10.5.3 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	The evaluator examined the FPT_TUD_EXT.1 entry in 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. The evaluator examined the Security Target and found that the options 'support automatic checking for updates' or 'support automatic updates' are not chosen from the selection in FPT_TUD_EXT.1.2.

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

5.10.5.4 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 FPT_TUD_EXT.1 entry in the section titled TOE Security Functional Requirement Measures 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 The Security administrator can also use a published hash to verify the integrity of the downloaded image. This is not an automated process, and the Security Administrator needs to compare the hash value of the downloaded image with the published hash to confirm integrity. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.10.5.5 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	The evaluator examined the section titled 'Verifying Software Version' 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 that: The administrator must run command "show version" and "show application version ise" to query the currently active version. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.10.5.6 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	The evaluator examined the section titled 'Secure Acceptance of the TOE' 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 describes the software update procedures for the TOE. These procedures include a description of the determination of a successful or unsuccessful verification. Finally, the evaluator compared the description in AGD to the description found in the TSS of ST. The evaluator found that the descriptions were consistent. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.10.5.7 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	The evaluator examined the section titled 'Secure Acceptance of the TOE' 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 Step 10 of the Section 'Secure Acceptance of the TOE' mentions the published hash values for the updates in Table 6. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.11 TSS and Guidance Activities (TOE Access)

5.11.1 FTA_SSL_EXT.1

5.11.1.1 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	The evaluator examined the FTA_SSL_EXT.1 entry in 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: An administrator can configure maximum inactivity times for both local and remote administrative sessions. When a session is inactive (i.e., no session input) for the configured period of time the TOE will terminate the session, requiring the administrator to log in again to establish a new session when needed. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.11.1.2 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	The evaluator examined the section titled 'Session Termination' 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 the following: Inactivity settings must trigger termination of the administrator session. These settings are configurable by setting the Administration > System > Admin Access > Settings-> Session Timeout setting in the GUI, which defines a session idle timeout period in minutes. After this period elapses, the session times out and access is no longer possible during this session. The administrator may re-initiate the login process to continue work. For the CLI, this timeout is configured using the command: terminal session-timeout *minutes* After this period elapses at the CLI, the session times out and access is no longer possible during this session. The administrator may re-initiate the login process to continue work. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.11.2 FTA_SSL.3

5.11.2.1 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	The evaluator examined the FTA_SSL.3 entry in 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: An administrator can configure maximum inactivity times for both local and remote administrative sessions. When a session is inactive (i.e., no session input) for the configured period of time the TOE will terminate the session, requiring the administrator to log in again to establish a new session when needed. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.11.2.2 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	The evaluator examined the section titled 'Session Termination' 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 the following: Inactivity settings must trigger termination of the administrator session. These settings are configurable by setting the Administration > System > Admin Access > Settings-> Session Timeout setting in the GUI, which defines a session idle timeout period in minutes. After this period elapses, the session times out and access is no longer possible during this session. The administrator may re-initiate the login process to continue work. For the CLI, this timeout is configured using the command:

	terminal session-timeout *minutes* After this period elapses at the CLI, the session times out and access is no longer possible during this session. The administrator may re-initiate the login process to continue work. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.11.3 FTA_SSL.4

5.11.3.1 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	The evaluator examined the FTA_SSL.4 entry in 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: Each administrator logged onto the TOE can manually terminate her session using the "LogOut" link in the web-based or the "exit" or "forceout <username>" commands at the CLI. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.11.3.2 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 'Session Termination' in the AGD to verify that it states how to terminate a local or remote interactive session. Upon investigation, the evaluator found that the AGD states the following : Each administrator logged onto the TOE can manually terminate his/her session using the "Log Out" link in the web-based GUI or the "exit" or "forceout <username>" commands at the CLI. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.11.4 FTA_TAB.1

5.11.4.1 FTA_TAB.1 TSS 1

Objective	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).

Evaluator Findings	The evaluator examined the FTA_TAB.1 entry in 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 and states that the TOE is displaying an advisory notice and consent warning message for each administrative method of access. Upon investigation, the evaluator found that the TSS states that: The TOE displays a privileged Administrator specified banner on the CLI management interface prior to allowing any administrative access to the TOE. The TOE also displays a banner at the web-based interface that is accessed via HTTPS. The local console access to the TOE takes the administrator to the CLI, where the administrative banner is displayed. The banner available at the local console and remote CLI are the same. The banners for the CLI and the GUI are separately configurable. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.11.4.2 FTA_TAB.1 Guidance 1

Objective	The evaluator shall check the guidance documentation to ensure that it describes how to configure the banner message.
Evaluator Findings	The evaluator examined the section titled **Login Banners** in the AGD to verify that it describes how to configure the banner message. Upon investigation, the evaluator found that the AGD describes the required commands for setting the login banner for CLI and GUI. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.11.5 FTA_TSE.1

5.11.5.1 FTA_TSE.1 TSS 1

Objective	The evaluator shall examine the TSS to determine that all of the attributes on which a user session can be denied are specifically defined.
Evaluator Findings	The evaluator examined the FTA_TSE.1 in the section 'TOE Summary Specification' to determine if all the attributes are defined on which a user session can be denied. The TSS states that: The TOE rejects authentication requests based on invalid credentials but can also impose authorization policies to deny requests based on the following criteria – • Administrator defined Time and Date Ranges • Administrator defined Maximum Number of Concurrent User Sessions, Maximum Number of Concurrent Sessions Per User Identity Group and/or Maximum Number of Concurrent Sessions per User within a User Identity Group. • Administrator defined list of Endpoint IPv4 addresses and/or subnets, IPv6 addresses and/or subnets, and/or MAC Addresses. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.11.5.2 FTA_TSE.1 Guidance 1

Objective	The evaluator shall examine the operational guidance to determine that it contains guidance for configuring each of the attributes identified in the TSS.

Evaluator Findings	The evaluator verified that the Guidance document describes how to configure each of the attributes identified in the TSS for denying a user session. Section 'User Session Establishment-Denial Attributes' was used to determine the verdict of this activity. Upon investigation, the evaluator found that the Guidance document contains all the necessary steps for configuring each of the attributes identified in the TSS: Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.12 TSS and Guidance Activities (Trusted Path/Channels)

5.12.1 FTP_ITC.1

5.12.1.1 FTP_ITC.1 TSS 1

Objective	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.
Evaluator Findings	The evaluator examined the FTP_ITC.1 entry in 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: The TOE protects communications with devices to which it sends syslogs, including other iterations of ISE, using TLS. This protects the data from disclosure by encryption and by checksums that verify that data has not been modified. The communication channel between the TOE and the NAS is secured via IPsec and the communication via the trusted channel can be initiated by either of the two communicating parties. The evaluator examined the FTP_ITC.1 entry in 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: The TOE also protects communications with external authentication stores in the following manner:

External Authentication Store	Protection Mechanism
LDAP Server(s)	TLS
Active Directory Services (acting as the Secure LDAP server)	TLS

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

5.12.1.2 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	The evaluator examined the Guidance document to determine if it contains instructions for establishing allowed protocols with each authorized IT entity. The section titled Logging Protection of AGD was used to determine the verdict of this assurance activity. Upon investigation, the evaluator found that AGD provides configuration instructions for configuring connections with each authorized IT entity. Specifically, the evaluator found that AGD provides guidance for configuring connections with the following authorized IT entities, • Remote Logging servers • Authentication Servers Next, the evaluator reviewed AGD and found for each connection a description of how to recover from unintentional disconnections. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.12.2 FTP_ITC.1 (AUTHSVR)

5.12.2.1 FTP_ITC.1 TSS 1 (AUTHSVR)

Objective	The evaluator shall examine the TSS to determine that, for all communications with authorized IT entities identified in the requirement, each communications mechanism is identified in terms of the allowed protocols for that IT entity. The evaluator shall also confirm that all protocols listed in the TSS are specified and included in the requirements in the ST.
Evaluator Findings	The evaluator examined the TSS to determine if communications mechanisms are identified for all communications with authorized IT entities. The TSS entry for FTP_ITC.1 in the section titled TOE Summary Specification of ST was used to determine the verdict of this assurance activity. Upon investigation, the evaluator found that the TSS identifies connections with the following authorized IT entities • Authentication server Next, the evaluator verified that for each communication identified in the TSS a description of the secure communication mechanism is provided. Specifically, the evaluator found that "The TOE also protects communications with external authentication stores in the following manner: External Authentication Store / Protection Mechanism LDAP Server(s) / TLS Active Directory Directory Services (acting as the Secure LDAP server) / TLS Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.12.2.2 FTP_ITC.1 Guidance 1 (AUTHSVR)

Objective	The evaluator shall confirm that the guidance documentation contains instructions for establishing and re-establishing the allowed protocols with each authorized IT entity.
Evaluator Findings	The evaluator examined the Guidance document to determine if it contains instructions for establishing allowed protocols with each authorized IT entity. The section titled "SSL/TLS Settings" of AGD was used to determine the verdict of this assurance activity. Upon investigation, the evaluator found that AGD provides instruction for configuring connections with each authorized IT entity. Specifically, the evaluator found that AGD provides guidance for configuring connections with the following authorized IT entities, • LDAP Server Next, the evaluator reviewed AGD and found that for each connection a description of how to recover from unintentional disconnections. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.12.3 FTP_TRP.1/Admin

5.12.3.1 FTP_TRP.1/Admin TSS 1

Objective	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.
Evaluator Findings	The evaluator examined the FTP_TRP.1/Admin entry in 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: All remote administrative communications take place over a secure encrypted SSHv2 (CLI) session or HTTPS/TLS (web-based GUI) session. The evaluator examined the FTP_TRP.1/Admin entry in 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: Both SSHv2 and HTTPS sessions are protected using AES encryption. The remote users are able to initiate both TLS and SSHv2 communications with the TOE. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.12.3.2 FTP_TRP.1/Admin Guidance 1

Objective	The evaluator shall confirm that the guidance documentation contains instructions for establishing the remote administrative sessions for each supported method.
Evaluator Findings	The evaluator examined the section titled 'Remote Administration Protocols' 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 provides

	instructions for configuring the remote administration of the TOE. AGD provides instructions for configuring the following protocols, • SSHV2 • HTTPS/TLS Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.13 TSS and Guidance Activities (Communications)

5.13.1 FCO_NRO.1.1

5.13.1.1 FCO_NRO.1.1 TSS 1

Objective	The evaluator shall check the description of the implementation of this protocol to ensure that RADIUS encapsulated EAP Message Authenticators conform to RFC 3579.
Evaluator Findings	The evaluator examined the TSS to ensure that it describes the implementation of this protocol to ensure that RADIUS encapsulated EAP Message Authenticators conform to RFC 3579. The FCO_NRO.1 in the section titled 'TOE Summary Specification' of ST was used to determine the verdict of this assurance activity. The evaluator found that the TSS states "The TOE has the ability to validate the authenticity of the NAS (as defined by RFC 3579) and prevent this component from being spoofed. The TOE receives the transmitted Access-Request and has the ability to identify that it was transmitted from the Authenticator. This is done specifically by verifying the Message Authenticator that is computed in part using a shared secret known to both the NAS and the TOE". Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.13.1.2 FCO_NRO.1.1 Guidance 1

Objective	The evaluator shall verify that the guidance contains all necessary instructions to configure RADIUS and encapsulated EAP on the TOE, in order to ensure that evidence of origin for all incoming RADIUS Access-Request packets is collected and preserved.
Evaluator Findings	The evaluator examined the Guidance document to determine if it describes all necessary instructions to configure RADIUS and encapsulated EAP on the TOE. Sections 'Configuring Radius' and 'Configuring EAP-TLS' of AGD was used to determine the verdict of this assurance activity. Upon investigation, the evaluator found that AGD contains the steps to configure Radius and EAP on the TOE via GUI. The AGD also mentions that "All Access-Requests sent to the TOE are logged". Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.13.2 FCO_NRR.1.1

5.13.2.1 FCO_NRR.1.1 TSS 1

Objective	The evaluator shall check the description of the implementation of this protocol to ensure that RADIUS Response Authenticators conform to RFC 2865.

Evaluator Findings	The evaluator examined the TSS to ensure that it describes the implementation of this protocol to ensure that RADIUS Response Authenticators conform to RFC 2865. The TSS entry for FCO_NRR.1 in the section titled 'TOE Summary Specification' of ST was used to determine the verdict of this assurance activity. The evaluator found that the TSS states: The TOE has the ability to return a valid response to the NAS upon receipt of an Access-Request as defined RFC 2865". Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.13.2.2 FCO_NRR.1.1 Guidance 1

Objective	The evaluator shall verify that the guidance contains all necessary instructions to configure RADIUS and encapsulated EAP on the TOE, in order to ensure that evidence of receipt of all incoming RADIUS Access- Request packets is generated and transmitted correctly.
Evaluator Findings	The evaluator examined the Guidance document to determine if it describes all necessary instructions to configure RADIUS and encapsulated EAP on the TOE. Section 'Configuring Radius' and 'Configuring EAP-TLS' of AGD was used to determine the verdict of this assurance activity. Upon investigation, the evaluator found that AGD contains the steps to configure Radius and EAP on the TOE via GUI. 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	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. Note that the testing here can be accomplished in conjunction with the testing of the security mechanisms directly.
Test Steps	Trigger each auditable event on the TOE Verify that each audit record is generated and contains the required information
Expected Test Results	Each required audit record generated by the TOE.
Pass/Fail with Explanation	Pass, The audit records associated with each test case are recorded with each test case. A comparison of required audit records to the presented audit records was additionally performed. This analysis shows that each required audit record is generated by the TOE, meeting the test requirements.

6.1.2 FAU_STG_EXT.1 Test #1

Item	Data
Test Assurance Activity	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.
Test Steps	• Check with the name and version of the audit server • Log into the TOE and configure the syslog server connection • Configure the syslog server • Verify with logs • Verify with packet capture

Expected Test Results	*Evidences will show that when logs will be sent from the TOE to the syslog server and the connection will be configured and encrypted.*
Pass/Fail with Explanation	Pass, As we configured syslog server in the end result when syslogs are sent from the TOE to the syslog server the syslogs are encrypted hence it meets the requirement.

6.1.3 FAU_STG_EXT.1 Test #2

Item	Data
Test Assurance Activity	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: 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)
Test Steps	• Show the local log setting configuration • Check downloadable logs showing that the new logs are written over the oldest log
Expected Test Results	*The TOE overwrites the oldest log when the log buffer reaches its set limit*
Pass/Fail with Explanation	Pass. After performing once, the limit is reached, the oldest audit record is overwritten. This meets the testing requirements.

6.1.4 FPT_STM.EXT.1 Test #1

Item	Data
Test Assurance Activity	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.

Test Steps	• Confirm current time.
	  ○ show clock
	• Set new time
	  ○ clock set 21:21:21 21 Dec 2021
	• Verify the time on the TOE was updated.
	  ○ show clock
	Verify logs were generated for time change

Expected Test Results	• *Evidence will show the change in Time.* • *Check in the logs captured.*
Pass/Fail with Explanation	Pass. After configuring the desired time, it will reflect likewise in result. This meets the testing requirements.

6.1.5 FTP_ITC.1 Test #1

Item	Data

Test Assurance Activity	Test 1: 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.
Test Steps	• Check with the name and version of the audit server • Log into the TOE and configure the syslog server connection • Configure the syslog server • Verify with logs • Verify with packet capture
Expected Test Results	*Evidences will show that External connections from the TOE will be send via an encrypted channel that will meet the testing requirements.*
Pass/Fail with Explanation	Pass, External connections from the TOE are sent via an encrypted channel. This meets the testing requirements

6.1.6 FTP_ITC.1 Test #2

Item	Data
Test Assurance Activity	Test 2: 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.
Expected Test Results	*Evidences will show that External connections from the TOE will be send via an encrypted channel that will meet the testing requirements.*
Pass/Fail with Explanation	Pass. This test is covered by FTP_ITC.1 Test #1.

6.1.7 FTP_ITC.1 Test #3

Item	Data
Test Assurance Activity	Test 3: The evaluator shall ensure, for each communication channel with an authorized IT entity, the channel data is not sent in plaintext.
Expected Test Results	*Evidences will show that External connections from the TOE will be send via an encrypted channel that will meets the testing requirements.*
Pass/Fail with Explanation	Pass. This test is covered by FTP_ITC.1 Test #1.

6.1.8 FTP_ITC.1 Test #4

Item	Data
Test Assurance Activity	Test 4: 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.
Test Steps	• Configure an TLS connection from TOE to syslog server • Verify that secure connection is established via packet capture • Verify the connection is successful via logs • Interrupt the connection between the devices for a duration shorter than the application layer timeout but of sufficient length to interrupt the Network link layer (less than 1 minute) • Verify the connection failure via packet capture • Verify the connection failure via logs

	• Verify secure connection is re-established via packet capture • Verify the connection is successful via logs • Interrupt the connection between the devices for a duration that exceeds the TOE's application layer timeout setting (more than 1 minute) • Verify the connection failure via packet capture • Verify the connection failure via logs • Verify secure connection is re-established via packet capture Verify the connection is successful via logs
Expected Test Results	*The TOE will react appropriately to any connection outage or interruption of the route to the external IT entities.*
Pass/Fail with Explanation	Pass. The TOE re-establishes secure connection when disconnected from the log server. This meets the testing requirements.

6.2 Auth

6.2.1 FAU_STG.1 Test #1

Item	Data
Test Assurance Activity	Test 1: The evaluator shall access the audit trail without authentication as Security Administrator (either by authentication as a nonadministrative 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. 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.
Test Steps	• Create Read only user profile. • Login to TOE as read-only user profile and try deleting the logs. The module fails as expected • Read-only User profile will won't be able to make any changes
Expected Test Results	*The TOE should not allow a non administrative user to modify and delete the audit records.*
Pass/Fail with Explanation	Pass. Access denied to TOE. Not able to access audit logs from no administrative user.

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	• Login to TOE as admin profile. • Try to delete the logs. • Verify that these attempts succeed.
Expected Test Results	Evidence will show that an authorized administrator will attempt and be able to delete audit records.
Pass/Fail with Explanation	Pass. The TOE allows the authorized user to delete logs hence it meets the testing requirements.

6.2.3 FCS_HTTPS_EXT.1 Test #1

Item	Data
Test Assurance Activity	Test 1: The evaluator shall attempt to establish each trusted path or channel that utilizes HTTPS, observe the traffic with a packet analyser, verify that the connection succeeds, and verify that the traffic is identified as TLS or HTTPS.
Test Steps	• From a remote workstation, establish an administrative session with the TOE over HTTPS • Verify that the packets are encrypted via packet capture • Verify with logs
Expected Test Result	*Evidence will show the connection will establish and encryption will be done.*
Pass/Fail with Explanation	Pass. The TOE and client encryption are done using TLS and meets the testing requirements.

6.2.4 FCS_HTTPS_EXT.1 Test#2

Item	Data
Test Assurance Activity	If the TOE is an HTTPS client or an HTTPS server utilizing X.509 client authentication, then the certificate validity shall be tested in accordance with testing performed for FIA_X509_EXT.1, and the evaluator shall perform the following test: Test 1: The evaluator shall demonstrate that using a certificate without a valid certification path results in an application notification. Using the administrative guidance, the evaluator shall then load a valid certificate and certification path, and demonstrate that the function succeeds. The evaluator then shall delete one of the certificates, and show that the selection listed in the ST occurs.
Expected Test Result	*The TOE will;* *authenticate when a valid certificate with a valid certification path is presented,* *not establish a connection when a certificate without a valid certification path is presented.*
Pass/Fail with Explanation	This test will be covered by FIA_X509_EXT.1.1, or by TLS specific tests.

6.2.5 FCS_CKM.2 Test #1

Item	Data
Test Assurance Activity	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 **TD0580 has been applied**
Expected Test Result	*Evidence will show that TOE has a correct operation of RSAES-PKCS1-v1_5 with a known good implementation.*
Pass/Fail with Explanation	This testing was performed in conjunction with FCS_TLSC_EXT.2.1 Test 1 and FCS_TLSS_EXT.2.1 Test 1 to demonstrate correct operation. This testing was performed in conjunction with FCS_SSHS_EXT.1 to demonstrate correct operation

6.2.6 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	GUI: • Confirm settings for account lockout. • Login to the GUI with incorrect user credentials 3 times. • Verify the authentication failures through logs. • Verify that the account is now locked by attempting to use correct credentials. • Verify through logs that the account is now locked. CLI: • Confirm settings for account lockout. • Login to the CLI with incorrect user credentials 3 times. • Verify that the account is now locked by attempting to use correct credentials. • Verify both sets of authentication failures through logs.
Expected Test Results	*Evidence will show that once the authentication attempts limit is reached, authentication attempts with valid credentials are no longer successful.*
Pass/Fail with Explanation	Pass, The unauthorized access using GUI & CLI user account is locked, Hence it meets the Testing requirement.

6.2.7 FIA_AFL.1 Test #2a

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 2: After reaching the limit for unsuccessful authentication attempts as in Test 1 above, the evaluator shall proceed as follows:

	If the **administrator action** selection in FIA_AFL.1.2 is included in the ST, then the evaluator shall confirm by testing that following the operational guidance and performing each action specified in the ST to re-enable the remote administrator's access results in successful access (when using valid credentials for that administrator).
Test Steps	GUI: • Confirm settings for account lockout. • Login to the GUI with incorrect user credentials 3 times. • Verify the authentication failures through logs. • Verify that the account is now locked by attempting to use correct credentials. • Verify through logs that the account is now locked. • Use an administrator account to unlock the locked user account. • Verify through logs that user account was unlocked. • Verify that the account is now unlocked and can be accessed. • Verify through logs that the user account was accessed successfully. CLI: • Confirm settings for account lockout. • Login to the CLI with incorrect user credentials 3 times. • Verify that the account is now locked by attempting to use correct credentials. • Verify both sets of authentication failures through logs. • Use an administrator account to unlock the locked user account. • Verify that the account is now unlocked and can be accessed. • Verify through logs that the account was accessed successfully.
Expected Test Results	*Evidence will show that after reaching the limit for unsuccessful authentication attempts as in Test 1 above, the evaluator will be able to verify successful access with valid administrator credentials after performing the associated administrative action.*
Pass/Fail with Explanation	Pass, After completing locked duration try to login with authorized user credentials the login is successful hence it meets the requirement.

6.2.8 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	• Configure TOE for strong password practices according to the NDCpp compliance in the ST. GUI: • Create username: Good1 password: R5yX9##lk8sxawr • Verify with logs that user 'good1' is created. • Create username: good2 password: +ccdoP%sdR67NEY(with Uppercase ,Lowercase ,special character) • Verify with logs that user 'good2' is created. • Create username: good3 password: 1029384756%%+Rt • Verify with logs that user 'good3' is created.

	• Create username: good4 password: pfJ4]+tUs9RZ#3_&,/V`sK~H}W4>mFs]T#mYH5QJ9^(N&7X7{)eD(nJc;a>)> • (?q:YE5S(j!WX4vmL}UqR5st&ECWRu9LdL+KSZnqfMC"~ • M,=5&&%3G$g{"$t-xt/k4 (127 character which is maximum supported) • Verify with logs that user 'good4' is created. Note: - We have only tested a subset on good passwords which satisfy the NDCPP compliance according to ST which should include passwords to be of length between 15 and 127 and must have at least 1 lower case, 1 upper case, 1 number and 1 special character(s). • Verify that each attempt was either accepted or rejected. (based on the password creation, attempts with "good" in the username can be created other cannot) • Verify that an audit record was generated with each attempt
Expected Test Results	*Evidence will show that prescribed password policy if matches then it will accept it as good password.*
Pass/Fail with Explanation	Pass. TOE is able to create users with good passwords hence it meets the testing requirements.

6.2.9 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	• Set password policy as below:- Min Length 16 instead of 15 Character At least 1 upper case At least 1 numeric At least 1 special character Max length 127 character (Default) ○ username: bad1 password: a ○ username: bad2 password: password ○ username: bad3 password: A#1 ○ username: bad4 password: pfJ4]+tUs9RZ#3_&,/V`sK~H}W4>mFs]T#mYH5QJ9^(N&7X7{)eD(nJc;a>)>(?q:YE5S(j!WX4vmL}UqR5st&ECWRu9LdL+KSZnqfMC "~M,=5&&%3G$g{"$t-xt/k49 (use 128 character password Max 127 character supported) • Verify that each attempt was either accepted or rejected. (based on the password creation, attempts with "good" in the username can be created other cannot) • Verify that an audit record was generated with each attempt

Expected Test Results	*The TOE only accepts valid password combinations on GUI. Audit logs show that addition of users with bad password combinations result in failure due to Invalid Password.*
Pass/Fail with Explanation	Pass, TOE reject the bad password creation hence it meets the requirement.

6.2.10 FIA_UIA_EXT.1 Test #1

Item	Data
Test Assurance Activity	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: 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.
Test Steps	• Log onto the TOE console CLI connection with incorrect credentials • Log onto the TOE console CLI with correct credentials • Log onto the TOE remote SSH CLI connection with incorrect credentials • Log onto the TOE remote SSH CLI with correct credentials • Log onto the TOE remote GUI connection with incorrect credentials • Log onto the TOE remote GUI with correct credentials • Verify all with logs
Expected Test Results	*Evidence will show that providing correct I&A information results in the ability to access the system, while providing incorrect information results in denial of access.*
Pass/Fail with Explanation	Pass, Presenting incorrect authentication credentials results in denied access to the TOE. Presenting correct authentication credentials results in access being allowed to the TOE. This meets the testing requirements.

6.2.11 FIA_UIA_EXT.1 Test #2

Item	Data
Test Assurance Activity	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: 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.
Test Steps	CLI • Show that commands are not available prior to login. • Verify authentication logs reflect failure • Login into the TOE • Show that the previously enabled commands are now available • Verify authentication logs reflect success GUI

	• Show that commands are not available prior to login. • Verify authentication logs reflect failure • Login into the TOE • Show that the previously enabled commands are now available • Verify authentication logs reflect success
Expected Test Results	*No services is available to a remote administrator attempting to login to the TOE via SSH or GUI.*
Pass/Fail with Explanation	Pass, No system services are available to an unauthenticated user connecting remotely. This meets the testing requirements.

6.2.12 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 (local and remote), 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 prior to logging in, and make sure this list is consistent with the requirement.
Test Steps	• Show that commands are not available prior to login. • Verify authentication logs reflect failure • Login into the TOE • Show that the previously enabled commands are now available • Verify authentication logs reflect success
Expected Test Results	*Evidence will show No system services are available to an unauthenticated user via the directly connected console.*
Pass/Fail with Explanation	Pass. No system service is available to an unauthenticated user connecting locally. This meets the testing requirements.

6.2.13 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	• At the directly connected login prompt, enter incorrect authentication credentials. Verify that at most obscured feedback is provided. • Verify in logs • At the directly connected login prompt, enter correct authentication credentials. Verify that at most obscured feedback is provided. • Verify in logs
Expected Test Results	*Evidence should show that no obscured feedback is flashed.*
Pass/Fail with Explanation	Pass. During local login, the TOE does not provide anything more than obscured feedback. This meets the testing requirements.

6.2.14 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	• Create a user with user privilege • Login to the TOE via SSH with user privilege • Attempt to access configuration mode without the proper privilege and verify user is unable to • Attempt to perform an update command and verify the command is rejected • Verify via logs

Expected Test Results	*When a unprivileged account tries to update a legitimate image, it should result in failure as the user doesn't have the administrator privilege. Audit logs verify that the user does not have administrator privileges.*
Pass/Fail with Explanation	Pass. The TOE did not let an unprivileged user to perform a software upgrade.

6.2.15 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.
Test Steps	• Login to the TOE via SSH with admin privilege • Attempt to access configuration mode and verify user is able to do so • Attempt to perform an update command and verify the command is available • Verify via logs
Expected Test Results	*When a privileged account tries to update a legitimate image, it should result in success as the admin user have the administrator privilege. Audit logs verify that the user have administrator privileges.*
Pass/Fail with Explanation	Pass, Authenticated user can configure trusted update. This meets the testing requirements

6.2.16 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	CLI • Start a SSH session onto the TOE with unprivileged user • Attempt to execute a configuration command to configure audit and verify the command is rejected GUI • Start a web session onto the TOE with unprivileged user • Attempt to execute a configuration command to configure audit and verify the command is rejected
Expected Test Results	*When an attempt to modify the audit data is made using an unprivileged user, it should result in failure as it is not the Security Administrator.*
Pass/Fail with Explanation	Pass. User without prior authentication/privilege was not able to perform actions on the TOE.

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

Item	Data
Test Assurance Activity	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. 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.
Test Steps	CLI • Start a SSH session onto the TOE and login as privileged user • Attempt to execute a configuration command to configure audit and verify the command is accepted. GUI • Start a web session with the TOE and login as privileged user • Attempt to make an audit configuration and verify the configuration attempt is successful.

Expected Test Results	*Evidence will show that User with prior authentication/privilege will be able to perform actions.*
Pass/Fail with Explanation	Pass. User with prior authentication/privilege was able to perform audit configuration on the TOE.

6.2.18 FMT_MOF.1/Functions Test #3

Item	Data
Test Assurance Activity	(if in the first selection **'determine the behaviour of'** has been chosen together with for any of the options in the second selection): The evaluator shall try to determine the behaviour of all options chosen from the second selection without prior authentication as Security Administrator (by authentication as a user with no administrator privileges or without user authentication at all). This can be done in one test or in separate tests. The attempt(s) to determine the behaviour of the selected functions without administrator authentication shall 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.
Test Steps	CLI • Start a SSH session onto the TOE with unprivileged user • Attempt to execute a configuration command to configure audit and verify the command is rejected GUI • Start a web session with the TOE with unprivileged user • Attempt to make a configuration command to configure audit and verify the attempt is rejected
Expected Test Results	*Evidence will show that User without prior authentication/privilege was unable to perform actions* .
Pass/Fail with Explanation	Pass. User without prior authentication/privilege was unable to perform actions on the TOE.

6.2.19 FMT_MOF.1/Functions Test #4

Item	Data
Test Assurance Activity	(if in the first selection **'determine the behaviour of'** has been chosen together with for any of the options in the second selection): The evaluator shall try to determine the behaviour of all options chosen from the second selection with prior authentication as Security Administrator. This can be done in one test or in separate tests. The attempt(s) to determine the behaviour of the selected functions with Security Administrator authentication shall be successful.
Test Steps	CLI • Start a SSH session onto the TOE and login as privileged user • Attempt to execute a configuration command to configure audit and verify the command is accepted GUI • Start a web session with the TOE and login as privileged user

	• Perform a configuration command to configure audit and verify the command is accepted
Expected Test Results	*Evidence will show that User with prior authentication will be able to perform actions.*
Pass/Fail with Explanation	Pass. User with prior authentication/privilege was able to perform actions on the TOE.

6.2.20 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	CLI • Start a SSH session onto the TOE and login as unprivileged user • Attempt to perform a configuration command to enable/disable the services and verify the command is rejected GUI • Start a web session with the TOE and login as unprivileged user • Perform a configuration command to enable/disable the services and verify the command is rejected
Expected Test Results	*Screenshot will show that User without prior privilege access will be unable to perform actions.*
Pass/Fail with Explanation	Pass. User without prior authentication/privilege was unable to perform actions on the TOE.

6.2.21 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	CLI • Start a SSH session onto the TOE and login as privileged user • Attempt to perform a configuration command to enable/disable the services and verify the command is accepted GUI • Start a web session with the TOE and login as privileged user • Perform a configuration command to enable/disable the services and verify the command is accepted

Expected Test Results	*Evidence will show that User with prior privilege access will be able to perform actions*
Pass/Fail with Explanation	Pass. User with prior authentication/privilege was able to perform actions on the TOE. This meets the testing requirement.

6.2.22 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	• Connect to the TOE as unprivileged user • Attempt to enter conf mode and verify it is rejected • Attempt to perform a configuration command to modify ciphers and verify the command is rejected
Expected Test Results	*Unprivileged user cannot perform security related configurations on the TOE.*
Pass/Fail with Explanation	Pass, Unauthenticated user cannot perform security related configurations on the TOE. This meets the testing requirements.

6.2.23 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	• Connect to the TOE as privileged user • Attempt to enter conf mode and verify it is accepted • Attempt to perform a configuration command to modify ciphers and verify the command is accepted • Verify with the log
Expected Test Results	*Authenticated user cannot perform security related configurations on the TOE.*
Pass/Fail with Explanation	Pass, Authorized user can perform security related configurations on the TOE. This meet the test requirement.

6.2.24 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	**FMT_SMF.1.1** The TSF shall be capable of performing the following management functions:

	• Ability to administer the TOE locally and remotely;
	• 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] capability prior to installing those updates;
	• Ability to configure the authentication failure parameters for FIA_AFL.1;
	  ○ [Ability to start and stop services;
	  ○ Ability to configure the cryptographic functionality;
	  ○ Ability to re-enable an Administrator account;
	  ○ Ability to set the time which is used for time-stamps;
	  ○ Ability to configure the reference identifier for the peer;
	  ○ Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors;
	  ○ Ability to import X.509v3 certificates to the TOE's trust store;]
	• Ability to configure the RADIUS shared secret
	• Ability to define an authorized NAS
	• Ability to enable, disable, and determine and modify the behavior of all the security functions of the TOE identified in this EP to the administrator
	• [Ability to configure the IPsec functionality]

Expected Test Results	*All management functions identified in section 2.4.4 have been tested throughout the evaluation. Thus, this requirement has been met.*
Pass/Fail with Explanation	Pass. Throughout the various security functionality testing of the TOE, FMT_SMF.1 Specification of Management Functions requirements have been met.

6.2.25 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 with Explanation	Pass. There are three interfaces where these can be tested (console/Remote CLI/Remote GUI) and all test cases use these interfaces. The evaluator has met this requirement through execution of the entirety of this test report by performing actions via all three interfaces

6.2.26 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	Remote CLI: • Configure a remote CLI time out period of 1 minute on administrative sessions • Connect to the TOE from the remote CLI • Let the remote CLI connection be idle for 1 minute. Verify that the session is terminated. • Verify that the session is terminated with logs. • Configure a remote CLI out period of 2 minutes on administrative sessions. • Connect to the TOE from the remote CLI. • Let the remote CLI connection be idle for 2 minutes. Verify that the session is terminated. • Verify that the session is terminated with logs. Remote GUI: • Configure a remote GUI time out period of 6 minute on administrative sessions. • Connect to the TOE from the remote GUI. • Let the remote GUI connection be idle for 6 minute. • Verify with logs. • Configure a remote GUI out period of 11 minutes on administrative sessions. • Connect to the TOE from the remote GUI. • Let the remote GUI connection be idle for 11 minutes. • Verify with logs.
Expected Test Results	*Evidence will show that remote administrative time out periods can be set by the administrative user and TOE will perform the configured inactive period in each instance.*
Pass/Fail with Explanation	Pass. 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.

6.2.27 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	• Log onto the TOE through a local administrative interface (console) • Perform some administrative activities (the actual activities are unimportant) and show clock • Using the instructions provided by the user guide log off • Verify the logs reflect the log off
Expected Test Results	*Evidence will show that after termination of the local session logs will be reflected.*
Pass/Fail with Explanation	Pass. After termination of the local session logs are reflected by the TOE hence it meets the testing requirement.

6.2.28 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	CLI • Log onto the TOE through a Remote administrative interface. • Perform some administrative activities • Logoff from the TOE. • Verify with logs GUI: • Log onto the TOE through a remote GUI interface. • Perform some administrative activities (the actual activities are unimportant). • Using the instructions provided by the user guide log off. • Verify the logs reflect the log out.
Expected Test Results	*The TOE should allow users to terminate the remote sessions. Audit logs show the successful login and logout of user from TOE.*
Pass/Fail with Explanation	Pass. The TOE allows user to terminate the remote administrative sessions. This meets the testing requirements.

6.2.29 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	• Log into the TOE via local console • Configure new session timeout (1 minute) • Verify time • Wait for 1 minute to observe inactivity logout • Verify with logs • Log into the TOE via local console • Configure new session timeout (3 minutes) • Verify time • Wait for 3 minute to observe inactivity logout • Verify with logs
Expected Test Results	*Evidence will show TOE local interactive session is terminated after the configured time period.*
Pass/Fail with Explanation	Pass. TOE local interactive session is terminated after the configured time period.

6.2.30 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	• Create a repository for banner from Remote Interface and try to configure banner • The Error showing that Banner can be replicated from Web GUI • Configure GUI pre-login Banner • Login to the TOE • Verify that Login banner displays
Expected Test Results	*Evidence will show that access banner can be set for all the methods which will be used to access the device.*
Pass/Fail with Explanation	Pass. An access banner can be set for all the methods that can be used to access the device. This meets the testing requirements.

6.2.31 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	SSH • Connect to the TOE using SSH. • Verify that the SSH session was established via capture • Verify the logs HTTP • Login to TOE with HTTPS connection • Verify the Successful login to TOE • Verify with the PCAP • Verify with the log
Expected Test Results	*Evidence should show that successful CLI and GUI connection will be made.*
Pass/Fail with Explanation	Pass. The successful communication is made via CLI and GUI, hence it meets the requirement.

6.2.32 1.32.FTP_TRP.1/Admin Test #1

Item	Data
Test Assurance Activity	The evaluator shall ensure, for each communication channel, the channel data is not sent in plaintext.
Expected Test Results	*Evidence will show that data in each communication channel is not in plaintext*
Pass/Fail with Explanation	Pass. This test is covered by FTP_TRP.1/Admin Test #1

6.3 SSH

6.3.1 FCS_SSHS_EXT.1.2 Test #1

Item	Data
Test Assurance Activity	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. **TD0631 has been applied**
Test Steps	• Ensure that a user with public-key authentication is configured • Initiate a SSH connection with the TOE from an SSH client • Verify the connection is established via packet capture • Verify the connection is established via logs
Expected Test Results	*TOE shall accept public-key authentication from a remote SSH client.*
Pass/Fail with Explanation	Pass. TOE accepts public-key authentication from a remote SSH client.

6.3.2 FCS_SSHS_EXT.1.2 Test #2

Item	Data
Test Assurance Activity	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. **TD0631 has been applied**
Test Steps	• Ensure that a user with public-key authentication is not configured on TOE • Initiate a SSH connection with the TOE from an SSH client • Verify the failure via packet capture • Verify the failure via the TOE Logs.
Expected Test Results	*Evidences will show that TOE does not accept public-key authentication from a remote SSH client if not configured previously.*
Pass/Fail with Explanation	Pass. TOE does not accept public-key authentication from a remote SSH client if not configured previously.

6.3.3 FCS_SSHS_EXT.1.2 Test #3

Item	Data

Test Assurance Activity	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. **TD0631 has been applied**
Test Steps	• Ensure that a user with password authentication is configured • Initiate a SSH connection with the TOE from an SSH client • Provide the username/password combination of the SSH user to log into the TOE • Show SSH connection details on the command line • Verify the connection is established via packet capture • Verify the connection is established via logs
Expected Test Results	*Evidence will show that TOE is able to accept password authentication from a remote SSH client.*
Pass/Fail with Explanation	Pass. TOE accepts password authentication from a remote SSH client; hence this meets the testing requirements.

6.3.4 FCS_SSHS_EXT.1.2 Test #4

Item	Data
Test Assurance Activity	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. **TD0631 has been applied**
Test Steps	• Initiate a SSH connection with the TOE from an SSH client • Provide the username & incorrect password combination of the SSH user to log into the TOE • Verify the connection is established via logs
Expected Test Results	*The result will show that TOE will not establish a connection with a remote SSH user when incorrect authentication credentials are presented.*
Pass/Fail with Explanation	Pass, TOE does not establish a connection with a remote SSH user when incorrect authentication credentials are entered Hence this meets the testing requirements.

6.3.5 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	• Establish an SSH connection to the TOE via the Acumen SSH tool • Verify the dropped connection via packet capture. • Verify the dropped connection via the TOE Logs

Expected Test Results	*Evidences will show that the TOE will drop large packets that will be received within an SSH session.*
Pass/Fail with Explanation	Pass. The TOE is receiving packets larger than specified is drop ,hence it meets the requirement.

6.3.6 FCS_SSHS_EXT.1.4 Test #1

Item	Data
Test Assurance Activity	The evaluator must ensure that only claimed ciphers and cryptographic primitives are used to establish a SSH connection. To verify this, the evaluator shall start session establishment for a 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. 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.
Note	Please Refer test bed SSHS
Test Steps	• Configure the claimed ciphers on the TOE • Connect to the TOE using AES-128-CTR • Verify that the SSH session was encrypted using AES-128-CTR via capture • Verify that the SSH session was encrypted using AES-128-CTR via log • Establish an SSH session with the configured supported algorithms (AES256-CTR) • Verify that the SSH session was encrypted using AES-256-CTR via capture • Verify that the SSH session was encrypted using AES-256-CTR via log • Establish an SSH session with the configured unsupported algorithms (AES-128-cbc) • Verify via packet capture • Verify via logs
Expected Test Result	• *Evidences will show that TOE will be able to use each of the claimed algorithms for SSH connections.* • *Logs will shows that SSH session was encrypted using AES-256-CTR as it is supported* • *Logs will shows that SSH session was encrypted using AES-128-CBC as it is not supported*
Pass/Fail with Explanation	Pass. TOE establishes a connection with a remote SSH user with only claimed ciphers and cryptographic primitives when correct authentication credentials are entered. Hence this meets the testing requirements.

6.3.7 FCS_SSHS_EXT.1.5 Test #1

Item	Data
Test Assurance Activity	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. **TD0631 has been applied**
Test Steps	• Connect to the TOE SSH with RSA-SHA2-256 based host public key authentication • Verify authentication via packet capture • Verify authentication logs • Connect to the TOE SSH with RSA-SHA2-512 based host public key authentication • Verify authentication via packet capture • Verify authentication logs
Expected Test Results	*The result will show that the TOE accepts connection with the claimed public key algorithms.*
Pass/Fail with Explanation	Pass. TOE accepts connection with the claimed public key algorithms.

6.3.8 FCS_SSHS_EXT.1.5 Test #2

Item	Data
Test Assurance Activity	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. **TD0631 has been applied**
Test Steps	• Connect to the TOE SSH with SSH-RSA (not supported) based host public key authentication • Verify authentication failure via packet capture • Verify with logs
Expected Test Results	*Evidences will show the TOE does not allow connection when the SSH client selects SSH server host public key algorithm that is not included in the ST selection.*
Pass/Fail with Explanation	Pass. The TOE does not allow connection when the SSH client selects SSH server host public key algorithm that is not included in the ST selection.

6.3.9 FCS_SSHS_EXT.1.6 Test #1

Item	Data
Test Assurance Activity	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.

	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.
Test Steps	• Establish an SSH session with the configured supported algorithms (HMAC-SHA1). • Verify that the SSH session was encrypted using HMAC-SHA1 via capture • Verify that the message integrity algorithm used was as configured via log. • 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 that the message integrity algorithm used was as configured via log. • 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 that the message integrity algorithm used was as configured via log.
Expected Test Results	*Evidences will show that the TOE is able to make SSH connections with each claimed data integrity algorithm.*
Pass/Fail with Explanation	Pass, TOE is able to make SSH connections with each claimed data integrity algorithm hence it meets the testing requirement.

6.3.10 FCS_SSHS_EXT.1.6 Test #2

Item	Data
Test Assurance Activity	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. 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.
Test Steps	• Attempt to establish an SSH session using hmac-sha1-96. • Verify wire shark does not continue negotiation • Verify TOE logs of invalid traffic
Expected Test Results	*Evidences will show that TOE rejects SSH connections using the "hmac-sha1-96" MAC for data integrity.*
Pass/Fail with Explanation	Pass. The TOE rejects SSH connections using the "hmac-sha1-96" MAC for data integrity. This meets the testing requirement.

6.3.11 FCS_SSHS_EXT.1.7 Test #1

Item	Data
Test Assurance Activity	Test 1: 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	• Attempt to establish a connection with the switch from an SSH client using diffiehellman-group1-sha1 as the key exchange method. ssh -o KexAlgorithms=diffie-hellman-group1-sha1 user1@10.1.2.50 • Capture the traffic between the devices • Verify that session was not established.

Expected Test Results	*Evidences will show that the TOE rejects SSH connections using diffiehellman-group1-sha1 (a non-approved algorithm) for key exchange.*
Pass/Fail with Explanation	Pass. TOE rejects the connection of non approved algorithm. This meets the testing requirement.

6.3.12 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	• Establish an SSH session using *diffie-hellman-group14-sha1* . • Verify that the SSH session was established via capture • Verify that the message integrity algorithm used was as configured via log. • Establish an SSH session using *ecdh-sha2-nistp256* . • Verify that the SSH session was established via capture • Verify that the message integrity algorithm used was as configured via log. • Establish an SSH session using *ecdh-sha2-nistp384* . • Verify that the SSH session was established via capture • Verify that the message integrity algorithm used was as configured via log. • Establish an SSH session using *ecdh-sha2-nistp521* . • Verify that the SSH session was established via capture • Verify that the message integrity algorithm used was as configured via log.
Expected Test Results	• *Evidences will show that the TOE is able to make SSH connections with each claimed data key exchange method* • *Logs will show that they are captured with ecdh-sha2-nistp256 . claimed data key exchange method* • *Logs will show that they are captured with ecdh-sha2-nistp384 . claimed data key exchange method* • *Logs will show that they are captured with ecdh-sha2-nistp521 . claimed data key exchange method*
Pass/Fail with Explanation	Pass. The TOE is able to make SSH connections with each claimed data key exchange method. This meets the testing requirements.

6.3.13 FCS_SSHS_EXT.1.8 Test #1

Item	Data
Test Assurance Activity	The evaluator needs to perform testing that rekeying is performed according to the description in the TSS. The evaluator shall test the **traffic-based** threshold. 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).

	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). 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. 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). 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: a. An argument is present in the TSS section describing this hardware- based limitation and b. 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	• Establish an SSH connection to the TOE via the Acumen SSH tool which tests traffic-based threshold. • Verify new key and rekey operations with the TOE logs.
Expected Test Results	*Evidences will show that the TOE is able to perform Rekey for the SSH connections with large packets.*
Pass/Fail with Explanation	Pass. The TOE is able to perform Rekey for the SSH connections according to the traffic-based threshold. This meets the testing requirements

6.3.14 FCS_SSHS_EXT.1.8 Test #2

Item	Data
Test Assurance Activity	The evaluator needs to perform testing that rekeying is performed according to the description in the TSS. The evaluator shall test the **time-based** threshold. 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). 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. 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). 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: a. An argument is present in the TSS section describing this hardware- based limitation and b. 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	• Establish an SSH connection to the TOE via the Acumen SSH tool which tests time-based threshold. • Verify new key and rekey operations with the TOE logs.
Expected Test Results	*Evidences will show that the TOE will be able to perform Rekey for the SSH connections with long term.*
Pass/Fail with Explanation	Pass. The TOE is able to perform Rekey for the SSH connections according to the time-based threshold. This meets the testing requirements

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 steps	• Configure three IKE/IPsec rules on TOE for connecting to an IKE/IPsec Peer ➢ Allow (PROTECT) a specific type of traffic • Configure the required ACL • Configure the required crypto maps • Establish an IPsec connection to the TOE peer • Verify that the traffic is processed as required for the configured IKE/IPsec rules • Verify established connection with logs • Verify with Packet Capture

	➢ Deny (DISCARD) a specific type of traffic • Configure the required ACL • Configure the required crypto maps • Establish an IPsec connection to the TOE peer • Verify that the traffic is processed as required for the configured IKE/IPsec rules • Verify that each filter was logged • Verify with Packet Capture ➢ Send plaintext (BYPASS) a specific type of traffic • Configure the required ACL • Configure the required crypto maps • Establish an IPsec connection to the TOE peer • Verify that the traffic is processed as required for the configured IKE/IPsec rules • Verify that each filter was logged • Verify with Packet Capture
Expected Test Results	*Evidence (screenshot or CLI output) of configuring the SPD.* *Packet capture and logs will show the results are allowed* *Packet capture and logs will show the results are Denied* *Packet capture and logs will show the results are Bypassed*
Pass/Fail with Explanation	Pass. The TOE dropped packets when configured, encrypted packets when configured, and sent packets in plaintext when configured. Hence it meets the testing requirements.

6.4.2 FCS_IPSEC_EXT.1.1 Test #2

Item	Data
Test Assurance Activity	The evaluator shall device 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 steps	• Create an access list • Apply the ACL on crypto map to the TOE interface • Send traffic that deny the VPN connection • Verify via packet capture • Configure IKE/IPsec policies meeting the following:- Send plaintext (BYPASS) • Send traffic that bypass the VPN connection • Verify via packet capture
Expected Test Results	*Evidences will show that access list rule will work .* *Logs will also show that the overlapping rule will not be applied.*

Pass/Fail with Explanation	Pass. The Test shows that the TOE dropped packets when configured, encrypted packets when configured, and sent packets in plaintext when configured hence it meets the testing requirements.

6.4.3 FCS_IPSEC_EXT.1.2 Test #1

Item	Data
Test Assurance Activity	The evaluator shall device 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 steps	○ Send plaintext (BYPASS) a specific type of traffic • Configure the required ACL • Configure the required crypto maps • Establish an IPsec connection to the TOE peer • Show the crypto map • Verify the connection with logs • Verify with Packet Capture • Ping the device with modified header containing an IP that is outside of the access lists . • Verify via packet capture
Expected Test Results	*Evidences will show that access list rule will work .*
Pass/Fail with Explanation	Pass The test shows that When the modified packet is sent, TOE rejects the connection hence it meets the requirement.

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 Steps	• Configure the TOE for an IPsec connection in Tunnel Mode. • Configure the PEER for an IPsec connection in Tunnel Mode • Create traffic that will trigger the IPsec Tunnel from the IPsec TOE. • Verify that an IKE session was established

	• Verify that tunnel mode was used via log • Verify that tunnel mode was used via packet capture
Expected Test Results	• *Evidence (screenshot or CLI output) of configuring the IPsec session.* • *Log showing that the IPsec session was in tunnel mode* *Packet capture showing session was in tunnel mode*
Pass/Fail with Explanation	Pass. The test shows that when configured, the TOE can establish an IPsec connection in tunnel mode hence it meets the testing requirement.

6.4.5 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.
Test steps	• Configure the TOE for an IPsec connection in Transport Mode. • Configure the PEER for an IPsec connection in Transport Mode • Create traffic that will trigger the IPsec Tunnel from the IPsec TOE. • Verify that an IKE session was established • Verify that Transport Mode was used via log • Verify that Transport Mode was used via packet capture
Expected Test Results	• *Evidence (screenshot or CLI output) of configuring the IPsec session.* • *Log showing that the IPsec session was in transport mode* *Packet capture showing session was in transport mode*
Pass/Fail with Explanation	Pass. The test shows that when configured, the TOE can establish an IPsec connection in transport mode.

6.4.6 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.
Expected Test Results	• *Evidence (screenshot or CLI output) of IPsec session configuration.* • *Logs of IPsec session configuration.* • *Packet capture showing the session establishment.* • *Logs showing the session establishment.* • *Repeat evidence for each supported DH group.* • *Repeat for each supported IKE version.*
Pass/Fail with Explanation	Pass, This test shows that IKE SAs can be configured with each claimed algorithm hence it meets the testing requirements

6.4.7 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 steps	• Configure the TOE to support IKEv1 using main mode only • Configure peer for aggressive mode • Peer configuration has the TOE configured for aggressive mode • Attempt to establish an IPsec session via Ping this will fail • 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 • Configure the TOE to support IKEv1 using main mode only • Attempt to establish an IPsec session via ping this will pass • Verify that main mode is established in the ipsec connection via log • Verify that main mode is established in the ipsec connection via packet capture
Expected Test Results	• *Evidence (screenshot or CLI output) of IKE configuration.* • *Log showing configuration.* • *Log showing the unsuccessful session attempt.* *Packet capture of the successful session.*
Pass/Fail with Explanation	Pass. The Test shows that the TOE rejects a connection attempt with Aggressive mode and then accepts a connection attempt with main mode hence it meets the testing requirements.

6.4.8 FCS_IPSEC_EXT.1.5 Test #2

Item	Data
Test Assurance Activity	If **NAT traversal** is selected within the IKEv2 selection, the evaluator shall configure the TOE so that it will perform NAT traversal processing as described in the TSS and RFC 5996, section 2.23. The evaluator shall initiate an IPsec connection and determine that the NAT is successfully traversed.
Test Flow	• Configure the TOE and peer to support NAT Traversal • Generate traffic from the endpoint IPs through the tunnel • Verify that the NAT statistics increases the counter and NAT traversal is successful • Verify with the logs.
Expected Test Results	*Evidences will show that the peer configured for NAT traversal attempts to initiate an IPsec session with the TOE the NAT is traversed*
Pass/Fail with Explanation	Pass. This test case shows that when a peer configured for NAT traversal attempts to initiate an IPsec session with the TOE the NAT is traversed

6.4.9 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	**Ikev1/Ikev2:-** **AES-128_HMAC-SHA1 :-** • Configure the TOE/Peer to use AES-CBC-128 for P1 and P2 using SHA1. • Attempt to establish the connection. • Verify traffic sent is secured using the specified algorithms via ISAKMP & IPSEC SA • Verify with logs that the connection established • Verify the packet capture **AES-256_HMAC-SHA1 :-** • Configure the TOE/Peer to use AES-CBC-256 for P1 and P2 using SHA1. • Attempt to establish the connection • Verify traffic sent is secured using the specified algorithms via ISAKMP & IPSEC SA • Verify with logs that the connection established • Verify the packet capture **AES-128_HMAC-SHA256** • Configure the TOE/Peer to use AES-CBC-128 for P1 and P2 using HMAC-SHA256 • Attempt to establish the connection • Verify traffic sent is secured using the specified algorithms via ISAKMP & IPSEC SA • Verify with logs that the connection established • Verify the packet capture **AES-256-HMAC-SHA512:-** • Configure the TOE/Peer to use AES-CBC-128 for P1 and P2 using HMAC-SHA256 • Attempt to establish the connection • Verify with logs that the connection established • Verify traffic sent is secured using the specified algorithms via ISAKMP & IPSEC SA • Verify the packet capture
Expected Test Results	This test requirement is covered by FCS_IPSEC_EXT.1.12 Test #1(IKEv1) and FCS_IPSEC_EXT.1.12 Test #1(IKEv2).
Pass/Fail with Explanation	Pass ,This test shows that IKE SAs can be configured with each claimed algorithm hence it meets the testing requirements.

6.4.10 FCS_IPSEC_EXT.1.7 Test #1

Item	Data
Test Assurance Activity	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 1 negotiation.

Expected Test Results	This test is not applicable as the number of bytes are not mentioned .
Pass/Fail with Explanation	This test is not applicable as the number of bytes are not mentioned.

6.4.11 FCS_IPSEC_EXT.1.7 Test #2(Ikev1)

Item	Data
Test Assurance Activity	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 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.
Test Steps	• Configure the IKEv1 SA Lifetime as 23 hours (82800 seconds) on the TOE • Configure the IKEv1 SA as 24 hours (86400)on the peer • Establish and IPsec connection between the TOE and peer • Maintain the connection for 24 hours • Verify that a rekey was initiated before 24 hours via log review and packet capture
Expected Test Results	• *Evidence (screenshot or CLI output) showing configuration of IKE lifetime.* • *Packet capture/session statistics are threshold is met.* • *Packet capture/logs showing session rekey.*
Pass/Fail with Explanation	Pass, This test shows that after few minutes, a new session is established between the TOE and peer, Hence it meets the testing requirement.

6.4.12 FCS_IPSEC_EXT.1.7 Test #2(Ikev2)

Item	Data
Test Assurance Activity	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 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.
Test Steps	• Configure the IKEv SA Lifetime as 23 hours (82800 seconds) on the TOE • Configure the IKEv2 SA as 24 hours (86400)on the peer • Establish and IPsec connection between the TOE and peer • Maintain the connection for 24 hours • Verify with the logs. • Verify with the packet capture.
Expected Test Results	• *Evidence (screenshot or CLI output) showing configuration of IKE lifetime.* • *Packet capture/session statistics are threshold is met.* • *Packet capture/logs showing session rekey.*
Pass/Fail with Explanation	Pass, This test shows that after few minutes, a new session is established between the TOE and peer, Hence it meets the testing requirement.

6.4.13 FCS_IPSEC_EXT.1.8 Test #1 (Ikev1)

Item	Data
Test Assurance Activity	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.
Test Steps	• Configure the TOE for kilobyte limit • Configure the Peer for kilobyte limit • Send enough data to trigger the limit • Verify that the rekey occurred via log • Verify that the rekey occurred via packet capture
Expected Test Results	*Evidences will show that TOE will start new connection negotiation after the overflow of traffic volume configured.*
Pass/Fail with Explanation	Pass. This test case shows that when configured for rekey after configured byte interval exceeds the TOE will rekey as shown in packet capture (Quick Mode) .hence it meets the requirement.

6.4.14 FCS_IPSEC_EXT.1.8 Test #1(Ikev2)

Item	Data
Test Assurance Activity	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.
Test Steps	• Configure the TOE for kilobyte limit • Configure the Peer for kilobyte limit • Send enough data to trigger the limit • Verify that the rekey occurred via log • Verify that the rekey occurred via packet capture
Expected Test Results	*Evidences will show that TOE will start new connection negotiation after the overflow of traffic volume configured.*
Pass/Fail with Explanation	Pass. This test case shows that when configured for rekey the TOE will rekey at the configured byte interval is exceeded.

6.4.15 FCS_IPSEC_EXT.1.8 Test #2 (Ikev1)

Item	Data
Test Assurance Activity	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 lifetime that exceeds the 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.
Test Steps	• Configure the IKE Phase 2 IPsec lifetime for 8 hours. • Establish an IPsec session. • Transmit packets across the connections repeatedly (to keep the session active). • Verify that when the time threshold is crossed a rekey is initiated.
Expected Test Results	
Pass/Fail with Explanation	Pass, This test case shows that when configured for rekey the TOE will rekey at the configured time interval of 8Hours-28800 sec).

6.4.16 FCS_IPSEC_EXT.1.8 Test #2 (Ikev2)

Item	Data
Test Assurance Activity	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 lifetime that exceeds the 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.
Test Steps	• Configure ipsec on the Toe to have lifetime seconds of 8 hours • Configure ipsec on the PEER to have lifetime seconds of 8.5 hours • Establish an IPsec session. • Transmit packets across the connections repeatedly (to keep the session active). • Verify that when the time threshold is crossed a rekey is initiated.
Expected Test Results	
Pass/Fail with Explanation	Pass. This test shows that when configured for rekey the TOE will rekey at the configured time interval (in this case 180 Sec).

6.4.17 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	Covered by TSS Assurance Activities in the AAR.

6.4.18 FCS_IPSEC_EXT.1.10 Test #2

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 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.
Pass/Fail with Explanation	Covered by TSS Assurance Activities in the AAR.

6.4.19 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 Steps	IKEv1 • Configure DH group 14 for IKEv1 on TOE • Configure DH group 14 for IKEv1 on PEER • Start an IPsec connection (using Ping) • Verify that DH Group 14 was used via log • Verify that Group 14 is used via capture • Configure the TOE for Group 19 • Configure the Peer for Group 19 • Generate traffic to trigger the IPsec session • Verify that DH group 19 was used via log • Verify that DH Group 19 was used via packet capture • Configure the TOE for Group 20 • Configure the Peer for Group 20 • Generate traffic to trigger the IPsec session • Verify that DH group 20 was used via log • Verify that DH Group 20 was used via packet capture • Configure the TOE for Group 24 • Configure the Peer for Group 24 • Generate traffic to trigger the IPsec session • Verify that DH group 24 was used via log • Verify that DH Group 24 was used via packet capture Ikev2 • Configure DH group 14 for IKEv1 on TOE. • Configure DH group 14 for IKEv1 on PEER. • Generate traffic to trigger the IPsec session. • Verify that DH Group 14 was used via log.

	• Verify that Group 14 was used via packet capture. • Configure the TOE for Group 19. • Configure the Peer for Group 19. • Generate traffic to trigger the IPsec session. • Verify that DH group 19 was used via log. • Verify that DH Group 19 was used via packet capture. • Configure the TOE for Group 20. • Configure the Peer for Group 20. • Generate traffic to trigger the IPsec session. • Verify that DH group 20 was used via log. • Verify that DH Group 20 was used via packet capture. • Configure the TOE for Group 24. • Configure the Peer for Group 24. • Generate traffic to trigger the IPsec session. • Verify that DH group 24 was used via log. • Verify that DH Group 24 was used via packet capture.
Expected Test Results	• Evidence (screenshot or CLI output) of IPsec session configuration. • Logs of IPsec session configuration. • Packet capture showing the session establishment. • Logs showing the session establishment. • Repeat evidence for each supported DH group. Repeat for each supported IKE version.
Pass/Fail with Explanation	Pass. The test performed for DH Group used in IPsec connections can be configured hence it meets the testing requirements.

6.4.20 FCS_IPSEC_EXT.1.12 Test #1(Ikev1)

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.
Test Steps	**AES-128_HMAC-SHA1 :-** • Configure the TOE/Peer to use AES-CBC-128 for P1 and P2 using SHA1. • Attempt to establish the connection. • Verify traffic sent is secured using the specified algorithms via ISAKMP & IPSEC SA • Verify with logs that the connection established • Verify the packet capture **AES-256_HMAC-SHA1 :-** • Configure the TOE/Peer to use AES-CBC-256 for P1 and P2 using SHA1. • Attempt to establish the connection

	• Verify traffic sent is secured using the specified algorithms via ISAKMP & IPSEC SA • Verify with logs that the connection established • Verify the packet capture **AES-128_HMAC-SHA256** • Configure the TOE/Peer to use AES-CBC-128 for P1 and P2 using HMAC-SHA256 • Attempt to establish the connection • Verify traffic sent is secured using the specified algorithms via ISAKMP & IPSEC SA • Verify with logs that the connection established • Verify the packet capture **AES-256-HMAC-SHA512:-** • Configure the TOE/Peer to use AES-CBC-128 for P1 and P2 using HMAC-SHA256 • Attempt to establish the connection • Verify with logs that the connection established • Verify traffic sent is secured using the specified algorithms via ISAKMP & IPSEC SA • Verify the packet capture
Expected Test Results	• *Evidence (screenshot or CLI output) of IPsec session configuration.* • *Logs of IPsec session configuration.* • *Packet capture showing the session establishment.* • *Logs showing the session establishment.* • *Repeat evidence for each supported DH group.* • *Repeat for each supported IKE version.*
Pass/Fail with Explanation	Pass, This test shows that IKE SAs can be configured with each claimed algorithm hence it meets the testing requirements.

6.4.21 FCS_IPSEC_EXT.1.12 Test #1(Ikev2)

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.
Test Flow	**AES-128_HMAC-SHA1 :-** • Configure the TOE/Peer to use AES-CBC-128 for P1 and P2 using SHA1. • Attempt to establish the connection. • Verify traffic sent is secured using the specified algorithms via IPSEC SA • Verify with logs that the connection established • Verify the packet capture **AES-256_HMAC-SHA1 :-** • Configure the TOE/Peer to use AES-CBC-256 for P1 and P2 using SHA1. • Attempt to establish the connection • Verify traffic sent is secured using the specified algorithms via IPSEC SA

	• Verify with logs that the connection established • Verify the packet capture **AES-128_HMAC-SHA256** • Configure the TOE/Peer to use AES-CBC-128 for P1 and P2 using HMAC-SHA256 • Attempt to establish the connection • Verify traffic sent is secured using the specified algorithms via IPSEC SA • Verify with logs that the connection established • Verify the packet capture **AES-256-HMAC-SHA512:-** • Configure the TOE/Peer to use AES-CBC-128 for P1 and P2 using HMAC-SHA256 • Attempt to establish the connection • Verify with logs that the connection established • Verify traffic sent is secured using the specified algorithms via IPSEC SA • Verify the packet capture
Expected Test Results	
Pass/Fail with Explanation	Pass ,This test shows that IKE SAs can be configured with each claimed algorithm hence it meets the testing requirements.

6.4.22 FCS_IPSEC_EXT.1.12 Test #2(IKEv1)

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 Steps	• Configure the TOE to support the following algorithms:
	  • IKE SA (Phase 1): AES-CBC-128
	  • IPsec SA (Phase 2): AES-CBC-128
	• Configure a peer to support the following algorithms:
	  • IKE SA (Phase 1): AES-CBC-128
	  • IPsec SA (Phase 2): esp-3des
	• Attempt to make a connection should fail.
	• Show connection details
	• Verify the connection in logs.
	• Verify via packet capture

Expected Test Results	• *Evidence (screenshot or CLI output) of IPsec session configuration.* • *Logs of IPsec session configuration.* • *Logs showing the session failure.*
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.

6.4.23 FCS_IPSEC_EXT.1.12 Test #2(IKEv2)

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 steps	• Configure the TOE to support the following algorithms:
	  • IKE SA (Phase 1): AES-CBC-128
	  • IPsec SA (Phase 2): AES-CBC-128
	• Configure a peer to support the following algorithms:
	  • IKE SA (Phase 1): AES-CBC-128
	  • IPsec SA (Phase 2): esp-3des
	• Attempt to make a connection should fail.
	• Show connection details
	• Verify via logs
	• Verify via packet capture.
	• Verify that the connection cannot be established

Expected Test Results	• *Evidence (screenshot or CLI output) of IPsec session configuration.* • *Logs of IPsec session configuration.* *Logs showing the session failure.*
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.

6.4.24 FCS_IPSEC_EXT.1.12 Test #3(IKEv1)

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 Steps	• Configure the TOE to support the following algorithms:
	  • IKE SA (Phase 1): AES-CBC-128, SHA-1
	  • IPsec SA (Phase 2): AES-CBC-128, SHA-1
	• Configure a peer to support the following algorithms:
	  • IKE SA (Phase 1): 3-DES,SHA-1
	  • IPsec SA (Phase 2): AES-CBC-128, SHA-1
	• Attempt to make a connection which cannot be established
	• Verify via logs
	• Verify via packet capture.

Expected Test Results	*Evidences will show that non-matching algorithm will always fails.*
Pass/Fail with Explanation	Pass, The test shows that if the TOE peer does not have matching algorithms this session will not be established hence it meets the testing requirements.

6.4.25 FCS_IPSEC_EXT.1.12 Test #3(IKev2)

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 steps	• Configure the TOE to support the following algorithms:
	  • IKE SA (Phase 1): AES-CBC-128, SHA-1
	  • IPsec SA (Phase 2): AES-CBC-128, SHA-1
	• Configure a peer to support the following algorithms:
	  • IKE SA (Phase 1): 3-DES,SHA-1
	  • IPsec SA (Phase 2): AES-CBC-128, SHA-1
	• Attempt to make a connection which cannot be established
	• Capture the logs via packet capture.

Expected Test Results	*Evidences will show that non-matching algorithm will always fails.*
Pass/Fail with Explanation	Pass, The test shows that if the TOE peer does not have matching algorithms this session will not be established hence it meets the testing requirements.

6.4.26 FCS_IPSEC_EXT.1.12 Test #4(Ikev1)

Item	Data
Test Assurance Activity	This test shall be performed for each version of IKE supported. The evaluator shall attempt to establish an SA for ESP (assumes the proper parameters where 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.
Note	Please refer Test Bed IPSEC

Test Steps	• Configure the TOE to support the following algorithms:
	  • IKE SA (Phase 1): AES-CBC-128, SHA-1
	  • IPsec SA (Phase 2): AES-CBC-128, SHA-1
	• Configure a peer to support the following algorithms:
	  • IKE SA (Phase 1): AES-CBC-128, SHA-1
	  • IPsec SA (Phase 2): 3DES, SHA-1
	• Attempt to make a connection which cannot be established
	• Capture the traffic via packet capture

Pass/Fail with Explanation	Pass. This test shows that if we configure nonmatching encryption algorithm the connection fails hence it meets the testing requirement.

6.4.27 FCS_IPSEC_EXT.1.12 Test #4(IKev2)

Item	**Data**
Test Assurance Activity	This test shall be performed for each version of IKE supported. The evaluator shall attempt to establish an SA for ESP (assumes the proper parameters where 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	Please refer Test Bed IPSEC

Expected Test Results	• Configure the TOE to support the following algorithms:
	  • IKE SA (Phase 1): AES-CBC-128, SHA-1
	  • IPsec SA (Phase 2): AES-CBC-128, SHA-1
	• Configure a peer to support the following algorithms:
	  • IKE SA (Phase 1): AES-CBC-128, SHA-1
	  • IPsec SA (Phase 2): 3DES, SHA-1

	• Attempt to make a connection which cannot be established • Verify through logs:- • Capture the traffic via packet capture
Pass/Fail with Explanation	Pass . This test shows that if we configure non matching encryption algorithm the connection fails hence it meets the testing requirement.

6.4.28 FCS_IPSEC_EXT.1.13 Test #1

Item	**Data**
Test Assurance Activity	The evaluator shall configure the TOE to use a private key and associated certificate signed by a trusted CA and shall establish an IPsec connection with the peer.
Note	Please refer Test Bed IPSEC
Test Steps	RSA:- • Configure the TOE to support the IKE/IPsec communications with digital certificates • Configure a peer to support the IKE/IPsec communications with digital certificates • Attempt to make a connection • Verify connection with IKE SA . • Verify the established connection with logs • Verify the established connection with packets capture ECDSA:- • Configure the IPsec Tunnel on the TOE • Configure the TOE to support the IKE/IPsec communications with digital certificates • Configure the IPsec Tunnel on the PEER • Configure a peer to support the IKE/IPsec communications with digital certificates • Attempt to make a connection • Capture the traffic • Verify that the connection can be established
Pass/Fail with Explanation	Pass. This test shows that TOE was able to complete a successful connection with a peer using digital certificates. Hence it meets the testing requirements.

6.4.29 FCS_IPSEC_EXT.1.13 Test #2

Item	**Data**
Test Assurance Activity	Test 2: If pre-shared keys are selected, the evaluator shall generate a pre-shared key off-TOE and use it, as indicated in the guidance documentation, to establish an IPsec connection with the peer.
Note	Please refer Test Bed IPSEC
Test Steps	• Configure the TOE to support the IKE/IPsec communications with pre-shared keys • Configure a peer to support the IKE/IPsec communications with pre-shared keys • Attempt to make a connection • Capture the traffic • Verify that the connection can be established.
Pass/Fail with Explanation	Pass, This test shows that TOE was able to complete a successful connection with a peer using pre-shared keys. Hence it meets the testing requirements.

6.4.30 FCS_IPSEC_EXT.1.14 Test #1

Item	Data
Test Assurance Activity	Test 1: [conditional] For each CN/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. If the TOE prioritizes CN checking over SAN (through explicit configuration of the field when specifying the reference identifier or prioritization rules), the evaluator shall also configure the SAN so it contains an incorrect identifier of the correct type (e.g. the reference identifier on the TOE is example.com, the CN=example.com, and the SAN:FQDN=otherdomain.com) and verify that IKE authentication succeeds.
Test Flow	CN: - IP Address • Root CA certificate authentication. • Intermediate CA certification authentication. • End Entity TOE certificate authentication. • Configure Peer's identifier in TOE's certificate map. • Configure TOE's identifier in Peer's certificate map. • Configure pki trustpoint on TOE. • Check connectivity using ping. • Log verifies tunnel is established due to the certificate. • Verify via packet capture that the tunnel is established. CN: - FQDN • Root CA certificate authentication. • Intermediate CA certification authentication. • End Entity TOE certificate authentication. • Configure Peer's identifier in TOE's certificate map. • Configure TOE's identifier in Peer's certificate map. • Configure pki trustpoint on TOE. • Check connectivity using ping. • Log verifies tunnel is established due to the certificate. • Verify via packet capture that the tunnel is established. CN: - User FQDN • Root CA certificae authentication. • Intermediate CA certification authentication. • End Entity TOE certificate authentication. • Configure Peer's identifier in TOE's certificate map. • Configure TOE's identifier in Peer's certificate map. • Configure pki trustpoint on TOE. • Check connectivity using ping. • Log verifies tunnel is established due to the certificate. Verify via packet capture that the tunnel is established.
Expected Test Results	• *Evidence (screenshot or CLI output) of IPsec session configuration.* • *Logs of IPsec session configuration.* • *Packet capture showing the session establishment.*
Pass/Fail with Explanation	Pass. This test shows that Toe validate the certificate with all type of CN – FQDN, Name FQDN. Hence it meets the requirement.

6.4.31 FCS_IPSEC_EXT.1.14 Test #2

Item	Data
Test Assurance Activity	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. 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.
Test Flow	SAN: - IP Address • Configure the TOE with SAN as IP: 10.20.40.50. • Configure the certificate with SAN as IP: 10.20.40.55. • Configure Peer's identifier in TOE's certificate map. • Configure TOE's identifier in Peer's certificate map. • Configure pki trustpoint on TOE. • Make the IKE/IPsec connection between the TOE and peer. • Verify through logs that the connection is established. • Verify through packet capture that the connection is established. SAN: - FQDN • Configure the TOE with SAN as FQDN: ISE3595.acumensec.local. • Configure the certificate with SAN as FQDN: ISE3615.acumensec.local • Configure Peer's identifier in TOE's certificate map. • Configure TOE's identifier in Peer's certificate map. • Configure pki trustpoint on TOE. • Make the IKE/IPsec connection between the TOE and peer. • Verify through logs that the connection is established. • Verify through packet capture that the connection is established. SAN: - User FQDN • Configure the TOE with SAN as User FQDN: ISE3595@acumensec.local. • Configure the peer certificate with SAN as User FQDN: ISE3615@acumensec.local. • Configure Peer's identifier in TOE's certificate map. • Configure TOE's identifier in Peer's certificate map. • Configure pki trustpoint on TOE. • Make the IKE/IPsec connection between the TOE and peer. • Verify through logs that the connection is established. • Verify through packet capture that the connection is established.
Expected Test Results	• *Evidence (screenshot or CLI output) of IPsec session configuration.* • *Logs of IPsec session configuration.* • *Logs showing the session establishment.* • *Packet capture of the session establishment.*

Pass/Fail with Explanation	Pass, The TOE accepts the connections with the correct identities. The TOE prioritize SAN checking over CN and it succeeds. This meets the testing requirements.

6.4.32 FCS_IPSEC_EXT.1.14 Test #3

Item	Data
Test Assurance Activity	Test 3: [conditional] For each CN/identifier type combination selected, the evaluator shall: a) Create a valid certificate with the CN so it contains the valid identifier followed by '\0'. 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 evaluator shall configure the SAN so it matches the reference identifier. b) Configure the peer's reference identifier on the TOE (per the administrative guidance) to match the CN without the '\0' and verify that IKE authentication fails.
Test Flow	Continue using the configuration of Trust point and IPsec from FCS_IPSEC_EXT.1.14 Test #1 • Configure the Peer's certificate with CN as IP address followed by '\0' and load on the TOE • Verify that the modified peer certificate is uploaded on the TOE • Verify the CN is not equal to the one above • Attempt to establish a connection between TOE and peer • Verify that connection fails • Verify with packet capture • Configure the Peer's certificate with CN as FQDN followed '\0' and load on the TOE • Verify that the modified peer certificate is uploaded on the TOE • Verify the CN is not equal to the one above • Attempt to establish a connection between TOE and peer • Verify that connection fails • Verify with packet capture
Expected Test Results	• *Evidence (screenshot or CLI output) of IPsec session configuration.* • *Logs of IPsec session configuration.* • *Packet capture showing the session failure.*
Pass/Fail with Explanation	Pass, The test shows that TOE rejects connections with CN mismatches. Hence it meets the testing requirements

6.4.33 FCS_IPSEC_EXT.1.14 Test #4

Item	Data
Test Assurance Activity	Test 4: [conditional] For each SAN/identifier type combination selected, the evaluator shall: 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. 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.
Test Flow	SAN as IP address • Create certificate with SAN as incorrect IP Address • Authenticate to the CA • Repeat the above steps to authenticate the peer • Attempt to establish a connection between the TOE and Peer and Verify that the connection is fails SAN as FQDN • Create Trustpoints having CN as incorrect FQDN • Create certificate with CN as FQDN • Authenticate to the CA • Repeat the above steps to authenticate the peer • Configure the TOE with the CN as IP address • Configure the Peer correct SAN to be similar to the TOE • Attempt to establish a connection between the TOE and Peer • Verify that the connection is fail • Verify packet captures SAN: - User FQDN • Configure the TOE with SAN as User FQDN: toe@acumensec.local. • Configure the peer with SAN as User FQDN: peer@acumensec.local. • Configure Peer's identifier in TOE's certificate map. • Configure TOE's identifier in Peer's certificate map. • Configure pki trustpoint on TOE. • Make the IKE/IPsec connection between the TOE and peer. • Verify through logs that the connection is established. • Verify through packet capture that the connection is established.
Expected Test Results	• *Evidence (screenshot or CLI output) of IPsec session configuration.* • *Logs of IPsec session configuration.* • *Packet capture showing the session failure.*
Pass/Fail with Explanation	Pass, This test shows that TOE rejects the connections with SAN mismatches. Hence it meets the testing requirement

6.5 TLSS

6.5.1 FCS_TLSS_EXT.1.1 Test #1

Item	Data
Test Assurance Activity	Test 1: The evaluator shall establish a TLS connection using each of the ciphersuites specified by the requirement. This connection may be established as part of the establishment of a higher-level protocol, e.g., as part of an HTTPS session. It is sufficient to observe the successful negotiation of a ciphersuite to satisfy the intent of the test; it is not necessary to examine the characteristics of the encrypted traffic to discern the ciphersuite

	being used (for example, that the cryptographic algorithm is 128-bit AES and not 256-bit AES).
Test Steps	• Establish a connection with the TOE over TLS with a particular cipher suite • Capture the traffic between the browser and the TOE • Verify that the session was established with the chosen cipher suite • Repeat for each supported cipher suite TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268 • Establish a connection with the TOE over TLS with a particular cipher suite • Capture the traffic between the browser and the TOE to verify that the session was established with the chosen cipher suite. TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246 • Establish a connection with the TOE over TLS with a particular cipher suite • Capture the traffic between the browser and the TOE to verify that the session was established with the chosen cipher suite. TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246 • Establish a connection with the TOE over TLS with a particular cipher suite • Capture the traffic between the browser and the TOE to verify that the session was established with the chosen cipher suite. TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246 • Establish a connection with the TOE over TLS with a particular cipher suite • Capture the traffic between the browser and the TOE to verify that the session was established with the chosen cipher suite. TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289 • Establish a connection with the TOE over TLS with a particular cipher suite • Capture the traffic between the browser and the TOE to verify that the session was established with the chosen cipher suite. TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 • Establish a connection with the TOE over TLS with a particular cipher suite • Capture the traffic between the browser and the TOE to verify that the session was established with the chosen cipher suite. TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 • Establish a connection with the TOE over TLS with a particular cipher suite • Capture the traffic between the browser and the TOE to verify that the session was established with the chosen cipher suite. TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 • Establish a connection with the TOE over TLS with a particular cipher suite • Capture the traffic between the browser and the TOE to verify that the session was established with the chosen cipher suite.

	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 • Establish a connection with the TOE over TLS with a particular cipher suite • Capture the traffic between the browser and the TOE to verify that the session was established with the chosen cipher suite. TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 • Establish a connection with the TOE over TLS with a particular cipher suite • Capture the traffic between the browser and the TOE to verify that the session was established with the chosen cipher suite.
Expected Test Results	*Evidence will show that TOE is able to make each connection using the supported ciphersuite, rest is failed.*
Pass/Fail with Explanation	Pass. TOE is able to make connection using each supported ciphersuite, and the rest fails.

6.5.2 FCS_TLSS_EXT.1.1 Test #2

Item	Data
Test Assurance Activity	Test 2: The evaluator shall send a Client Hello to the server with a list of ciphersuites that does not contain any of the ciphersuites in the server's ST and verify that the server denies the connection. Additionally, the evaluator shall send a Client Hello to the server containing only the TLS_NULL_WITH_NULL_NULL ciphersuite and verify that the server denies the connection.
Test Steps	• Established connection with TLS_NULL_WITH_NULL_NULL ciphersuite using acumen-tlss tool TLS_NULL_WITH_NULL_NULL • Packet capture showing related connections • Verify via logs. TLS_NULL_WITH_NULL_MD5 • Packet capture showing related connections • Verify via logs.
Expected Test Results	*Evidence will show that the TOE will reject TLS connections with the NULL cipher.*
Pass/Fail with Explanation	Pass, TOE reject TLS connections with the NULL cipher.

6.5.3 FCS_TLSS_EXT.1.1 Test #3a

Item	Data
Test Assurance Activity	Test 3: The evaluator shall perform the following modifications to the traffic: Modify a byte in the Client Finished handshake message and verify that the server rejects the connection and does not send any application data.
Test Steps	• Configure connection with a tool which allows modification of Client Finished handshake message. • Verify the TOE rejects connection.

Expected Test Results	*The TOE should not allow a connection to proceed when a byte in the Client Finished handshake message has been modified.*
Pass/Fail with Explanation	Pass ,The TOE rejects a connection to proceed when a byte in the Client Finished handshake message has been modified.

6.5.4 FCS_TLSS_EXT.1.1 Test #3b

Item	Data
Test Assurance Activity	Test 3: The evaluator shall perform the following modifications to the traffic: (Test Intent: The intent of this test is to ensure that the server's TLS implementation immediately makes use of the key exchange and authentication algorithms to: a) Correctly encrypt (D)TLS Finished message and b) Encrypt every (D)TLS message after session keys are negotiated.) The evaluator shall use one of the claimed ciphersuites to complete a successful handshake and observe transmission of properly encrypted application data. The evaluator shall verify that no Alert with alert level Fatal (2) messages were sent. The evaluator shall verify that the Finished message (Content type hexadecimal 16 and handshake message type hexadecimal 14) is sent immediately after the server's ChangeCipherSpec (Content type hexadecimal 14) message. The evaluator shall examine the Finished message (encrypted example in hexadecimal of a TLS record containing a Finished message, 16 03 03 00 40 11 22 33 44 55...) and confirm that it does not contain unencrypted data (unencrypted example in hexadecimal of a TLS record containing a Finished message, 16 03 03 00 40 14 00 00 0c...), by verifying that the first byte of the encrypted Finished message does not equal hexadecimal 14 for at least one of three test messages. There is a chance that an encrypted Finished message contains a hexadecimal value of '14' at the position where a plaintext Finished message would contain the message type code '14'. If the observed Finished message contains a hexadecimal value of '14' at the position where the plaintext Finished message would contain the message type code, the test shall be repeated three times in total. In case the value of '14' can be observed in all three tests it can be assumed that the Finished message has indeed been sent in plaintext and the test has to be regarded as 'failed'. Otherwise, it has to be assumed that the observation of the value '14' has been due to chance and that the Finished message has indeed been sent encrypted. In that latter case the test shall be regarded as 'passed'.
Test Steps	• Configure connection that use one of the claimed ciphersuites to complete a successful handshake and transmit encrypted application data. • Verify that the Finished message (Content type decimal 22) is sent immediately after the server's ChangeCipherSpec (Content type decimal 20) message, and the first byte is not hexadecimal 14.
Expected Test Results	*TOE shall perform successful handshake and transmission of properly encrypted application data.*
Pass/Fail with Explanation	Pass. TOE performs successful handshake and transmission of properly encrypted application data.

6.5.5 FCS_TLSS_EXT.1.2 Test #1

Item	Data

Test Assurance Activity	The evaluator shall send a Client Hello requesting a connection for all mandatory and selected protocol versions in the SFR (e.g. by enumeration of protocol versions in a test client) and verify that the server denies the connection for each attempt.
Test Steps	• Configure connections that use SSL 2.0, SSL 3.0, TLS 1.0, and TLS 1.1. • Verify the denied connections via logs. SSLv2.0 • Verify that TOE denies the SSLv2.0 connection via packet capture. • Verify that the connection was denied via logs. SSLv3.0 • Verify that TOE denies the SSLv3.0 connection via packet capture. • Verify that the connection was denied via logs. TLSv1.0 • Verify that TOE denies the TLSv1.0 connection via packet capture. • Verify that the connection was denied via logs. TLS 1.1 • Verify that TOE denies the TLSv1.1 connection via packet capture. • Verify that the connection was denied via logs.
Expected Test Results	*TOE shall deny SSL 2.0, SSL 3.0, TLS 1.0, and TLS 1.1 connections.*
Pass/Fail with Explanation	Pass. TOE denies SSL 2.0, SSL 3.0, TLS 1.0, and TLS 1.1 connections.

6.5.6 FCS_TLSS_EXT.1.3 Test #1a

Item	Data
Test Assurance Activity	Test 1: If **ECDHE ciphersuites** are supported: The evaluator shall repeat this test for each supported elliptic curve. The evaluator shall attempt a connection using a supported ECDHE ciphersuite and a single supported elliptic curve specified in the Elliptic Curves Extension. The Evaluator shall verify (though a packet capture or instrumented client) that the TOE selects the same curve in the Server Key Exchange message and successfully establishes the connection.
Test Steps	• Configure connection with each of the supported elliptic curve. • Verify that the TOE selects the same curve in the Server Key Exchange message and successfully establishes the connection.
Expected Test Results	*TOE shall establish connection using the supported elliptic curves.*
Pass/Fail with Explanation	Pass. TOE establishes connection using secp256r1 elliptic curve which is the only supported curve claimed in ST.

6.5.7 FCS_TLSS_EXT.1.3 Test #1b

Item	Data

Test Assurance Activity	Test 1: If **ECDHE ciphersuites** are supported: The evaluator shall attempt a connection using a supported ECDHE ciphersuite and a single unsupported elliptic curve (e.g. secp192r1 (0x13)) specified in RFC4492, chap. 5.1.1. The evaluator shall verify that the TOE does not send a Server Hello message and the connection is not successfully established.
Test Steps	• Configure connection attempt which uses a supported ECDHE ciphersuite and a single unsupported elliptic curve. • Verify that TOE does not send a Server Hello message and the connection is denied.
Expected Test Results	*TOE shall deny connection when an unsupported elliptic curve is selected.*
Pass/Fail with Explanation	Pass.TOE denies connection when an unsupported elliptic curve is selected.

6.5.8 FCS_TLSS_EXT.1.3 Test #2

Item	Data
Test Assurance Activity	Test 2: [conditional] If DHE ciphersuites are supported, the evaluator shall repeat the following test for each supported parameter size. If any configuration is necessary, the evaluator shall configure the TOE to use a supported Diffie-Hellman parameter size. The evaluator shall attempt a connection using a supported DHE ciphersuite. The evaluator shall verify (through a packet capture or instrumented client) that the TOE sends a Server Key Exchange Message where p Length is consistent with the message are the ones configured Diffie-Hellman parameter size(s).
Pass/Fail with Explanation	NA. DHE curves are not supported.

6.5.9 FCS_TLSS_EXT.1.3 Test #3

Item	Data
Test Assurance Activity	Test 3 : If **RSA key establishment ciphersuites** are supported, the evaluator shall repeat this test for each RSA key establishment key size. If any configuration is necessary, the evaluator shall configure the TOE to perform RSA key establishment using a supported key size (e.g. by loading a certificate with the appropriate key size). The evaluator shall attempt a connection using a supported RSA key establishment ciphersuite. The evaluator shall verify (through a packet capture or instrumented client) that the TOE sends a certificate whose modulus is consistent with the configured RSA key size.
Test Steps	• Configure connection with RSA key establishment ciphersuite while the TOE has a RSA certificate of 4096 bit key size. • Verify that the TOE sends a certificate whose modulus is consistent with the configured RSA key size • Configure connection with RSA key establishment ciphersuite while the TOE has a RSA certificate of 2048 bit key size. • Verify that the TOE sends a certificate whose modulus is consistent with the configured RSA key size
Expected Test Results	*TOE shall perform RSA key establishment using a supported key sizes.*
Pass/Fail with Explanation	Pass. TOE performs RSA key establishment using supported key sizes.

6.5.10 FCS_TLSS_EXT.1.4 Test #2a

Item	Data
Test Assurance Activity	Test 2: If the TOE supports session resumption using session IDs according to RFC4346 (TLS1.1) or RFC5246 (TLS1.2), the evaluator shall carry out the following steps (note that for each of these tests, it is not necessary to perform the test case for each supported version of TLS): The evaluator shall conduct a successful handshake and capture the TOE-generated session ID in the Server Hello message. The evaluator shall then initiate a new TLS connection and send the previously captured session ID to show that the TOE resumed the previous session by responding with ServerHello containing the same SessionID immediately followed by ChangeCipherSpec and Finished messages (as shown in Figure 2 of RFC 4346 or RFC 5246).
Test Steps	• Configure connection in which previously captured session ID is send and TOE resumed the previous session by responding with Server Hello containing the same Session ID. • Verify that there is successful handshake between the connection.
Expected Test Results	*TOE shall allow connections using previous session ID .*
Pass/Fail with Explanation	Pass. The TOE accepts previous session IDs and responds with ServerHello containing the same SessionID.

6.5.11 FCS_TLSS_EXT.1.4 Test #2b

Item	Data
Test Assurance Activity	Test 2: If the TOE supports session resumption using session IDs according to RFC4346 (TLS1.1) or RFC5246 (TLS1.2), the evaluator shall carry out the following steps (note that for each of these tests, it is not necessary to perform the test case for each supported version of TLS): The evaluator shall initiate a handshake and capture the TOE-generated session ID in the Server Hello message. The evaluator shall then, within the same handshake, generate or force an unencrypted fatal Alert message immediately before the client would otherwise send its Change Cipher Spec message thereby disrupting the handshake. The evaluator shall then initiate a new Client Hello using the previously captured session ID, and verify that the server (1) implicitly rejects the session ID by sending a Server Hello containing a different Session ID and performing a full handshake (as shown in figure 1 of RFC 4346 or RFC 5246), or (2) terminates the connection in some way that prevents the flow of application data
Test Steps	• Configure connection in which a session ID is exchanged with the TOE but handshake is interrupted with Alert before sending ChangeCipherSpec. Then attempt to reuse the previous session by sending the session ID in the ClientHello. • Verify that the TOE rejects the previous session ID by sending a ServerHello containing a different SessionID.

	• Verify with logs
Expected Test Results	*TOE deny the connection.*
Pass/Fail with Explanation	Pass. The TOE denies connections that reuse terminated session IDs.

6.6 Update

6.6.1 FPT_TST_EXT.1.1 Test #1

Item	Data
Test Assurance Activity	It is expected that at least the following tests are performed: a) Verification of the integrity of the firmware and executable software of the TOE b) Verification of the correct operation of the cryptographic functions necessary to fulfil any of the SFRs. 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. 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.
Note	Please Refer test bed UPDATE
Test Steps	• Access the CLI and enter the command to reload the TOE • Review audit records to ensure reboot occurred and verify no failed tests are reported to the console • Verify that all the process are running.
Expected Test Results	*Evidences will show that the claim self test will be performed by TOE.*
Pass/Fail with Explanation	Pass. The TOE performs all claimed self-tests.

6.6.2 FPT_TUD_EXT.1 Test #1

Item	Data
Test Assurance Activity	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). The evaluator obtains a legitimate update using procedures described in the guidance documentation and verifies that it is successfully installed on the TOE. (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.)

	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.
Note	Please Refer test bed UPDATE
Test Steps	• Verify the current version of the TOE • Manually verify the published hash of the image before uploading on the TOE • Perform the image update • Verify that the patch installed on the TOE • Verify with the Log
Expected Test Result	*Evidences will show that TOE software will be able to update the image that passes the integrity test.*
Pass/Fail with Explanation	Pass. TOE is able to update successfully with an image that passes the integrity test. This meets the testing requirements

6.6.3 FPT_TUD_EXT.1 Test #2 (a)

Item	Data
Test Assurance Activity	Test 2 (if digital signatures are used): 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: 1)A modified version (e.g. using a hex editor) of a legitimately signed update
Note	Please Refer test bed UPDATE
Test Steps	• Using a Hex editor modify an otherwise good firmware image. • Verify the current firmware version on the TOE. • Upload the modified image on the TOE. • Attempt to install the modified update image and verify that it fails. • Verify the failure with logs. • Verify that the TOE firmware version has not changed.
Expected Test Result	The TOE rejects the modified image and the logs validate the fact that the image wasn't installed as the TOE was not able to verify the signature.
Pass/Fail with Explanation	Pass. The TOE rejects a firmware update image that has been modified. This meets the testing requirement.

6.6.4 FPT_TUD_EXT.1 Test #2 (b)

Item	Data
Test Assurance Activity	Test 2 (if digital signatures are used): 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: 2) An image that has not been signed

Test Steps	• Verify the current firmware version on the TOE. • Attempt to install the update image and verify that it fails. • Verify the failure with logs. • Verify that the TOE firmware version has not changed.
Expected Test Result	The TOE doesn't install the modified image and refuses to update the current image. The logs depict that image was not installed as the TOE was not able to verify it due to absence of signature.
Pass/Fail with Explanation	Pass. The TOE rejects a firmware update that has not been signed. This meets the testing requirement.

6.6.5 FPT_TUD_EXT.1 Test #2 (c)

Item	Data
Test Assurance Activity	Test 2 (if digital signatures are used): 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: 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)
Test Steps	• Using a Hex editor modify an otherwise good firmware image. • Verify the current firmware version on the TOE. • Attempt to install the modified update image and verify that it fails. • Verify the failure with logs. • Verify that the TOE firmware version has not changed.
Expected Test Result	The TOE should not install the modified image and the firmware version should remain the same. The logs accurately describe the reason as to why the image wasn't installed is because the signature has been modified.
Pass/Fail with Explanation	Pass. The TOE rejects a firmware update with a bad signature. This meets the testing requirement.

6.6.6 FPT_TUD_EXT.1 Test #3 (a)

Item	Data
Test Assurance Activity	Test 3 (if published hash is verified on the TOE): If the published hash is provided to the TOE by the Security Administrator and the verification of the hash value over the update file(s) against the published hash is performed by the TOE, then the evaluator shall perform the following tests. The evaluator first confirms that no update is 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 an illegitimate update such that the hash of the update does not match the published hash. The evaluator provides the published hash value to the TOE and calculates the hash of the update either on the TOE itself (if that functionality is provided by the TOE), or else outside the TOE. The evaluator confirms that the hash values are different, and attempts to install the update on the TOE, verifying that this fails because of the difference in hash values (and that the failure is logged). Depending on the

	implementation of the TOE, the TOE might not allow the user to even attempt updating the TOE after the verification of the hash value fails. In that case the verification that the hash comparison fails is regarded as sufficient verification of the correct behaviour of the TOE
Pass/Fail with Explanation	N/A. Published hash is not verified on the TOE but instead verified manually by the Administrator prior to install or upgrade.

6.6.7 FPT_TUD_EXT.1 Test #3 (b)

Item	Data
Test Assurance Activity	Test 3 (if published hash is verified on the TOE): If the published hash is provided to the TOE by the Security Administrator and the verification of the hash value over the update file(s) against the published hash is performed by the TOE, then the evaluator shall perform the following tests. The evaluator first confirms that no update is 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 uses a legitimate update and tries to perform verification of the hash value without storing the published hash value on the TOE. The evaluator confirms that this attempt fails. Depending on the implementation of the TOE it might not be possible to attempt the verification of the hash value without providing a hash value to the TOE, e.g. if the hash value needs to be handed over to the TOE as a parameter in a command line message and the syntax check of the command prevents the execution of the command without providing a hash value. In that case the mechanism that prevents the execution of this check shall be tested accordingly, e.g. that the syntax check rejects the command without providing a hash value, and the rejection of the attempt is regarded as sufficient verification of the correct behaviour of the TOE in failing to verify the hash. The evaluator then attempts to install the update on the TOE (in spite of the unsuccessful hash verification) and confirms that this fails. Depending on the implementation of the TOE, the TOE might not allow to even attempt updating the TOE after the verification of the hash value fails. In that case the verification that the hash comparison fails is regarded as sufficient verification of the correct behaviour of the TOE
Test Output	**N/A**
Pass/Fail with Explanation	N/A. Published hash is not verified on the TOE but instead verified manually by the Administrator prior to install or upgrade.

6.7 VPN-Auth

6.7.1 FIA_PSK_EXT.1 Test #1

Item	Data
Test Assurance Activity	Test 1: The evaluator shall compose a pre-shared key of 22 characters that contains a combination of the allowed characters in accordance with the operational guidance, and demonstrates that a successful protocol negotiation can be performed with the key.
Note	Please Refer test bed VPN_AUTH
Test Steps	IPsec

	• Configure the TOE to support authentication with a 22-character PSK • Configure the Switch (NAS) to support authentication with a 22-character PSK • Attempt a connection to the TOE • Verify the connection is successful • Verify the connection is established via packet capture • Verify the connection is established via logs <u>Radius</u> • Configure the TOE to support authentication with a 22-character PSK • Configure the Switch (NAS) to support authentication with a 22-character PSK • Attempt a connection to the TOE • Verify the connection is successful • Verify the connection is established via packet capture • Verify the connection is established via logs
Expected Test Result	• *Evidence (screenshot or CLI output) showing configuration of PSK.* • *Log showing each successful authentication.*
Pass/Fail with Explanation	Pass. The TOE allows a successful protocol negotiation with a pre-shared key of 22 characters. This meets the testing requirement.

6.7.2 FIA_PSK_EXT.1 Test #2

Item	Data
Test Assurance Activity	Test 2 [conditional]: If the TOE supports pre-shared keys of multiple lengths, the evaluator shall repeat Test 1 using the minimum length; the maximum length; and an invalid length. The minimum and maximum length tests should be successful, and the invalid length must be rejected by the TOE.
Note	Please Refer test bed VPN_AUTH
Test Steps	<u>IPsec</u> • Minimum length of 22 • Configure the TOE to support authentication with a 22 character PSK • Configure the Switch (NAS) to support authentication with a 22 character PSK • Attempt a connection to the TOE • Verify the connection is successful • Verify the connection is established via packet capture • Verify the connection is established via logs • Maximum length of 127 • Configure the TOE to support authentication with a 127-character PSK • Configure the Switch (NAS) to support authentication with a 127-character PSK • Attempt a connection to the TOE • Verify the connection is successful • Verify the connection is established via packet capture • Verify the connection is established via logs

	• Invalid length of 128 • Configure the TOE to support authentication with a 128-character PSK and verify it gets rejected <u>Radius</u> • Minimum length of 22 • Configure the TOE to support authentication with a 22 character PSK • Configure the Switch (NAS) to support authentication with a 22 character PSK • Attempt a connection to the TOE • Verify the connection is successful • Verify the connection is established via packet capture • Verify the connection is established via logs • Maximum length of 127 • Configure the TOE to support authentication with a 127-character PSK • Configure the Switch (NAS) to support authentication with a 127-character PSK • Attempt a connection to the TOE • Verify the connection is successful • Verify the connection is established via packet capture • Verify the connection is established via logs • Invalid length of 128 • Configure the TOE to support authentication with a 128-character PSK and verify it rejects
Expected Test Result	• *Evidence (screenshot or CLI output) showing configuration of PSK.* *Log showing each successful authentication.*
Pass/Fail with Explanation	Pass. The TOE accepts keys of lengths within the minimum and maximum length. This meets the testing requirement.

6.7.3 FTA_TSE.1 Test #1

Item	Data
Test Assurance Activity	Test 1: The evaluator shall successfully establish a user session. The evaluator shall follow the operational guidance to configure the system so that that user's access is denied based on a specific value of an attribute. The evaluator shall then attempt to establish a session in contravention to the attribute setting while still providing valid authentication data. The evaluator shall observe that the access attempt fails. The evaluator shall repeat this test for each attribute indicated by the ST author.
Note	Please Refer test bed VPN_AUTH
Test Steps	• Configure a valid user account • Authenticate with the user to the TOE

	• Verify the connection is successful • Verify the connection is established via packet capture • Verify the connection is established via logs • Connect to the TOE with another Administrator account • Enforce a policy that will deny the account based on MAC of the created user • Apply the created policy to the Authorization policy set • Verify the policy is enforced on the TOE via logs • Attempt to login using the denied MAC address user • Verify the connection is denied • Verify the connection is denied via packet capture • Verify the connection is denied via logs • Enforce a policy that will deny the account based on date and time • Apply the created policy to the Authorization policy set • Verify the policy is enforced on the TOE via logs • Attempt to login using the user • Verify the connection is denied • Verify the connection is denied via packet capture • Verify the connection is denied via logs • Enforce a policy that will deny the account based on concurrent user sessions via GUI • Verify the connection is denied after the maximum session is reached via GUI • Verify the connection is denied via logs via GUI
Expected Test Result	• *Evidence (screenshot or CLI output) showing configuration of Denial Attributes.* • *Log showing each failure authentication*
Pass/Fail with Explanation	Pass. The user session will be denied based on the configured attributes. This meets the testing requirements

6.7.4 FTP_ITC.1(2) Test #1

Item	Data
Test Assurance Activity	Test 1: The evaluators shall ensure that communications using each protocol with each NAS 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	Continue the configuration of TOE for EAP-TLS from FCS_EAP-TLS_EXT.1.1 Test#1 • Configure the TOE for Radius over IPsec • Configure the NAS for Radius over IPsec • Generate traffic by authenticating to the TOE • Verify the connection is successful • Verify that the tunnel is up • Verify the connection is established via packet capture • Verify the connection is established via logs
Expected Test Results	• *Audit Records* • *Packet Capture showing ESP traffic between TOE and NAS* • *Status commands (showing active IPsec tunnel)*
Pass/Fail with Explanation	Pass. The TOE can be configured to successfully communicate with the external authentication server(NAS) via IPsec. This meets the testing requirements.

6.7.5 FTP_ITC.1(2) Test #2

Item	Data
Test Assurance Activity	Test 2: 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 with Explanation	Pass. This test is covered by FTP_ITC.1(2) Test#1. TOE initiates the session to the external entity. This meets the testing requirements.

6.7.6 FTP_ITC.1(2) Test #3

Item	Data
Test Assurance Activity	Test 3: The evaluator shall ensure, for each communication channel with a NAS, the channel data uses the appropriate identified protocols.
Pass/Fail with Explanation	Pass. This test is covered by FTP_ITC.1(2) Test#1. The channel data uses the appropriate identified protocols i.e., IPsec for communication with the NAS. This meets the testing requirements.

6.7.7 FTP_ITC.1 (2) Test #4

Item	Data
Test Assurance Activity	Test 4: The evaluators shall, for each protocol associated with each NAS tested during test 1, physically interrupt an established connection. The evaluator shall ensure that when physical connectivity is restored, communications are appropriately protected.
Test Steps	Continue the configuration of TOE from FTP_ITC.1(2) Test #1 • Generate traffic by authenticating to the TOE • Verify the connection is successful • Verify that the tunnel is up • Verify the connection is established via packet capture • Verify the connection is established via logs • Continue communication of traffic and physically interrupt the connection between the client/Peer and TOE for a period less than 60 seconds

	• Verify the connection failure via logs • Verify the connection failure via packet capture • Re-connect the client/Peer and TOE after a period less than 60 seconds (to trigger the application layer interruption). Verify communication return. • Verify the connection is restored via packet capture • Verify the connection is restored via logs • Now again physically interrupt the connection between the client/Peer and TOE a period greater than 60 seconds • Verify the connection failure via logs • Verify the connection failure via packet capture • Re-connect the client/Peer and TOE after a period greater than 60 seconds (to trigger the MAC layer interruption). Verify communication return. • Verify the connection restored via packet capture • Verify the connection restored via logs
Expected Test Results	• *Evidence (screenshot or CLI output) of IPsec session configuration.* • *Logs of IPsec session configuration.* • *Packet capture.*
Pass/Fail with Explanation	Pass. The TOE does not send plaintext traffic when disconnected from the external entity. This meets the testing requirements.

6.8 TLSS-MA

6.8.1 FCS_TLSS_EXT.2.1 & 2.2 Test #1a

Item	Data
Test Assurance Activity	Test 1a [conditional]: If the TOE requires or can be configured to require a client certificate, the evaluator shall configure the TOE to require a client certificate and send a Certificate Request to the client. The evaluator shall attempt a connection while sending a certificate_list structure with a length of zero in the Client Certificate message. The evaluator shall verify that the handshake is not finished successfully and no application data flows.
Note	Please refer to Test Bed TLSS-MA
Test Steps	• Connect using acumen TLSS tool by sending the empty certificate and show the connection fails • Verify the failure logs on the device • Verify the packet capture
Expected Test Result	*Evidence will show that it will rejects an attempt to open a mutually authenticated TLS connection where the client does not send a certificate.*
Pass/Fail with Explanation	Pass. The TOE rejects the connection when the client tries to connect with the empty certificate. This meets the testing requirements.

6.8.2 FCS_TLSS_EXT.2.1 & 2.2 Test #1b

Item	Data
Test Assurance Activity	Test 1b [conditional]: If the TOE supports fallback authentication functions and these functions cannot be disabled. The evaluator shall configure the fallback authentication

	functions on the TOE and configure the TOE to send a Certificate Request to the client. The evaluator shall attempt a connection while sending a certificate_list structure with a length of zero in the Client Certificate message. The evaluator shall verify the TOE authenticates the connection using the fallback authentication functions as described in the TSS. Note: Testing the validity of the client certificate is performed as part of X.509 testing.
Note	N/A – TOE Supports fallback authentication, but it can be disabled
Test Steps	N/A – TOE Supports fallback authentication, but it can be disabled
Expected Test Result	*Evidence will show that it will rejects an attempt to open a mutually authenticated TLS connection where the client does not send a certificate.*
Pass/Fail with Explanation	N/A – TOE Supports fallback authentication, but it can be disabled

6.8.3 FCS_TLSS_EXT.2.1 & 2.2 Test #2

Item	Data
Test Assurance Activity	Test 2 [conditional]: If TLS 1.2 is claimed for the TOE, the evaluator shall configure the server to send a certificate request to the client without the supported_signature_algorithm used by the client's certificate. The evaluator shall attempt a connection using the client certificate and verify that the connection is denied **TD0395 has been applied**
Note	Please refer to Test Bed TLSS-MA
Test Steps	• Client Certificate without the supported_signature_algorithm by the server • The evaluator shall attempt a connection using the client certificate and show the connection being unsuccessful • Verify the failure logs on the device • Verify the failure with packet capture
Expected Test Result	*Evidence will show that it will rejects mutually authenticated TLS connection attempts from a client whose certificate contains an unsupported signature algorithm.*
Pass/Fail with Explanation	Pass. TOE rejects mutually authenticated TLS connection attempts from a client whose certificate contains an unsupported signature algorithm.

6.8.4 FCS_TLSS_EXT.2.1 & 2.2 Test #3

Item	Data
Test Assurance Activity	Test 3: The aim of this test is to check the response of the server when it receives a client identity certificate that is signed by an impostor CA (either Root CA or intermediate CA). To carry out this test the evaluator shall configure the client to send a client identity certificate with an issuer field that identifies a CA recognised by the TOE as a trusted CA, but where the key used for the signature on the client certificate does not correspond to the CA certificate trusted by the TOE (meaning that the client certificate is invalid because its certification path does not terminate in the claimed CA certificate). The evaluator shall verify that the attempted connection is denied.

Note	Please refer to Test Bed TLSS-MA
Test Steps	• Verify the TOE CA details • Create a CA certificate whose CN matches with the CA certificate on the TOE but with different key. Then sign the client certificate with this CA with the different key. • Attempt to connect to the TOE with the new client certificate and show the connection fails • Verify the failure logs on the device • Verify the failure with packet capture
Expected Test Result	*Evidence will show that TOE rejects mutually authenticated TLS connection attempts from a client whose certificate is invalid since the signature does not correspond to the trusted CA.*
Pass/Fail with Explanation	Pass. TOE rejects mutually authenticated TLS connection attempts from a client whose certificate is invalid since the signature does not correspond to the trusted CA.

6.8.5 FCS_TLSS_EXT.2.1 & 2.2 Test #4

Item	Data
Test Assurance Activity	Test 4: The evaluator shall configure the client to send a certificate with the Client Authentication purpose in the extendedKeyUsage field and verify that the server accepts the attempted connection. The evaluator shall repeat this test without the Client Authentication purpose and shall verify that the server denies the connection. Ideally, the two certificates should be identical except for the Client Authentication purpose.
Note	Please refer to Test Bed TLSS-MA
Test Steps	Valid Certificate: • Load the client certificate containing the Client Authentication purpose • Initiate a connection with the TOE over TLS and show the connection being successful • Verify the packet capture showing the Client Authentication purpose enable Invalid Certificate: • Load the client certificate lacking the Client Authentication purpose • Initiate a connection with the TOE over TLS and show the connection being unsuccessful • Verify the failure logs on the device • Verify the packet capture lacking the Client Authentication purpose
Expected Test Result	*Evidence will show that the TOE denies a TLS connection when a certificate without the Client Authentication purpose is presented from a client.*
Pass/Fail with Explanation	Pass. TOE denies a TLS connection when a certificate without the Client Authentication purpose is presented from a client.

6.8.6 FCS_TLSS_EXT.2.1 & 2.2 Test #5 (a)

Item	Data
Test Assurance Activity	Test 5: The evaluator shall perform the following modifications to the traffic: a) Configure the server to require mutual authentication and then connect to the server with a client configured to send a client certificate that is signed by a Certificate Authority trusted by the TOE. The evaluator shall verify that the server accepts the connection.

Note	Please refer to Test Bed TLSS-MA
Test Steps	• Initiate a connection with the TOE over TLS and show the connection being successful • Verify the packet capture
Expected Test Result	*Evidence will show that the TOE accepts mutual authentication connections when client uses a trusted certificate*
Pass/Fail with Explanation	Pass. TOE accepts mutual authentication connections when client uses a trusted certificate.

6.8.7 FCS_TLSS_EXT.2.1& 2.2 Test #5 (b)

Item	Data
Test Assurance Activity	Configure the server to require mutual authentication and then modify a byte in the signature block of the client's Certificate Verify handshake message (see RFC5246 Sec 7.4.8). The evaluator shall verify that the server rejects the connection.
Note	Please refer to Test Bed TLSS-MA
Test Steps	• Use the Acumen TLS modification tool to modify a byte in the client's Certificate Verify handshake message • Verify the failure logs on the device • Verify the packet capture
Expected Test Result	E*vidence will show that the TOE rejects connections when the last byte of the client's Certificate Verify handshake message is modified.*
Pass/Fail with Explanation	Pass. TOE rejects connections when the last byte of the client's Certificate Verify handshake message is modified.

6.8.8 FCS_TLSS_EXT.2.1 & 2.2 Test #6

Item	Data
Test Assurance Activity	Using the administrative guidance, the evaluator shall load a CA certificate or certificates needed to validate the presented certificate used to authenticate an external entity and demonstrate that the function succeeds, and a trusted channel can be established.
Note	Please refer to Test Bed TLSS-MA
Test Steps	• Upload a complete certificate validation chain to the TOE • Initiate a connection with the TOE over TLS and show the connection being successful • Verify the packet capture
Expected Test Result	*Evidence will show that the TOE accepts mutual authentication connections when client uses a valid certificate and trusted path.*
Pass/Fail with Explanation	Pass. TOE accepts mutual authentication connections when client uses a valid certificate and trusted path.

6.8.9 FCS_TLSS_EXT.2.1 & 2.2 Test #7

Item	Data

Test Assurance Activity	Test 7: The evaluator shall then change the presented certificate(s) so that validation fails and show that the certificate is not automatically accepted. The evaluator shall repeat this test to cover the selected types of failure defined in the SFR (i.e. the selected ones from failed matching of the reference identifier, failed validation of the certificate path, failed validation of the expiration date, failed determination of the revocation status). The evaluator performs the action indicated in the SFR selection observing the TSF resulting in the expected state for the trusted channel (e.g. trusted channel was established) covering the types of failure for which an override mechanism is defined.
Note	Please refer to Test Bed TLSS-MA
Test Steps	Failed matching reference Identifier: • The requirements of this test case are exercised in FCS_TLSS_EXT.2.3 Test #1 Failed Certificate Path: • Remove the CA from the TOE • Attempt the connection from the TOE to the TLS server and show the connection being unsuccessful • Verify the failure logs on the device • Verify with packet capture Expired Certificate: • Create a server certificate which is expired • Attempt the connection from the TOE to the TLS server and show the connection being unsuccessful • Verify the failure logs on the device • Verify with packet capture Revocation Status: • Revoke the End Entity certificate • Attempt a connection using the revoked end entity certificate • Verify the logs on the device Verify with packet capture
Expected Test Result	*Evidence will show that the TOE rejects connections when a client certificate is invalid or does not have a trusted path.*
Pass/Fail with Explanation	Pass. TOE rejects connections when a client certificate is invalid or does not have a trusted path.

6.8.10 FCS_TLSS_EXT.2.1 & 2.2 Test #8

Item	Data
Test Assurance Activity	Test 8 [conditional]: The purpose of this test is to verify that only selected certificate validation failures could be administratively overridden. If any override mechanism is defined for failed certificate validation, the evaluator shall configure a new presented certificate that does not contain a valid entry in one of the mandatory fields or parameters (e.g. inappropriate value in extendedKeyUsage field) but is otherwise valid and signed by a trusted CA. The evaluator shall confirm that the certificate validation fails (i.e. certificate is rejected), and there is no administrative override available to accept such certificate
Note	N/A – TOE do not implement any administrative override mechanism

Test Steps	N/A – TOE do not implement any administrative override mechanism
Expected Test Result	N/A – TOE do not implement any administrative override mechanism
Pass/Fail with Explanation	N/A – TOE do not implement any administrative override mechanism

6.8.11 FCS_TLSS_EXT.2.3 Test #1

Item	Data
Test Assurance Activity	The evaluator shall send a client certificate with an identifier that does not match an expected identifier and verify that the server denies the connection.
Note	Please refer to Test Bed TLSS-MA
Test Steps	• Configure a client certificate with an identifier that does not match an expected identifier. • Initiate the connection to TOE using the client certificate and show that the connection is unsuccessful. • Verify the logs on the device • Verify with packet capture
Expected Test Result	*Evidence will show that the TOE will reject connection when a client certificate has an identifier that does not match an expected identifier*
Pass/Fail with Explanation	Pass. The TOE rejects connection when a client certificate has an identifier that does not match an expected identifier.

6.9 TLSC-MA

6.9.1 FCS_TLSC_EXT.1.1 Test #1

Item	Data
Test Assurance Activity	The evaluator shall establish a TLS connection using each of the cipher suites specified by the requirement. This connection may be established as part of the establishment of a higher-level protocol, e.g., as part of an HTTPS session. It is sufficient to observe the successful negotiation of a cipher suite to satisfy the intent of the test; it is not necessary to examine the characteristics of the encrypted traffic in an attempt to discern the cipher suite being used (for example, that the cryptographic algorithm is 128-bit AES and not 256-bit AES).
Test Steps	• CONNECT WITH DHE_RSA_WITH_AES_128_CBC_SHA256 (In open SSL AES128-SHA256 is used) • Verify with packet capture • CONNECT WITH TLS_RSA_WITH_AES_256_CBC_SHA256 • Verify with packet capture • CONNECT WITH TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 • Verify with packet capture • CONNECT WITH TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • Verify with packet capture • CONNECT WITH TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

	• Verify with packet capture • CONNECT WITH TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • Verify with packet capture • CONNECT WITH TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 • Verify with packet capture • CONNECT WITH TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 • Verify with packet capture • CONNECT WITH TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 • Verify with packet capture • CONNECT WITH TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 • Verify with packet capture
Expected Test Results	• Evidence will only approved ciphers are included in the TOE's Server Hello message; • Each cipher should be accepted when offered back to the TOE by a server.
Pass/Fail with Explanation	Pass. The TOE connects to a remote TLS server using the claimed cipher suites, This meets the testing requirement.

6.9.2 FCS_TLSC_EXT.1.1 Test #2

Item	Data
Test Assurance Activity	The evaluator shall attempt to establish the connection using a server with a server certificate that contains the Server Authentication purpose in the extended Key Usage field and verify that a connection is established. The evaluator will then verify that the client rejects an otherwise valid server certificate that lacks the Server Authentication purpose in the extended Key Usage field, and a connection is not established. Ideally, the two certificates should be identical except for the extended Key Usage field.
Test Steps	• Create a server certificate with the Server Authentication EKU. • Attempt a connection from the TOE to a TLS server using the certificate that contains the Server Authentication EKU. • Verify that the TOE accepts the connection in packet capture. • Create a server certificate that lacks the Server Authentication EKU. • Attempt a connection from the TOE to a TLS server using the invalid certificate missing the Server Authentication EKU. • Verify that the TOE rejects the connection in packet capture. • Verify with logs.
Expected Test Results	Evidence will show that the TOE will not make the connection because the evaluation of the extended key usage field fails.
Pass/Fail with Explanation	Pass, The TOE does not make the connection because the evaluation of the extendedkeyusage field fails. This meets the testing requirements.

6.9.3 FCS_TLSC_EXT.1.1 Test #3

Item	Data

Test Assurance Activity	The evaluator shall send a server certificate in the TLS connection that the does not match the server-selected cipher suite (for example, send a ECDSA certificate while using the TLS_RSA_WITH_AES_128_CBC_SHA cipher suite). The evaluator shall verify that the TOE disconnects after receiving the server's Certificate handshake message.
Test Steps	• Initiate a TLS connection using the acumen-tlsc tool such that the server certificate presented doesn't match the server-selected cipher suite. • Verify that the connection is not established through packet capture. • Verify that a log is a generated indicating that connection was rejected.
Expected Test Results	Evidence will show that TOE will rejects a connection attempt where the selected cipher suite will not match the certificate cipher suite.
Pass/Fail with Explanation	Pass, The TOE rejects a connection attempt where the selected ciphersuite does not match the certificate ciphersuite

6.9.4 FCS_TLSC_EXT.1.1 Test #4a

Item	Data
Test Assurance Activity	The evaluator shall configure the server to select the TLS_NULL_WITH_NULL_NULL cipher suite and verify that the client denies the connection.
Test Steps	• Attempt a connection to a server using the TLS_NULL_WITH_NULL_NULL ciphersuite using acumen-tlsc tool. • Verify that the TOE denies the connection. • Verify with logs.
Expected Test Results	Evidence will show it will reject a connection attempt with the TLS_NULL_WITH_NULL_NULL cipher suite.
Pass/Fail with Explanation	Pass, The TOE rejects a connection attempt with the TLS_NULL_WITH_NULL_NULL ciphersuite.

6.9.5 FCS_TLSC_EXT.1.1 Test #4b

Item	Data
Test Assurance Activity	Modify the server's selected cipher suite in the Server Hello handshake message to be a cipher suite not presented in the Client Hello handshake message. The evaluator shall verify that the client rejects the connection after receiving the Server Hello.
Test Steps	• Attempt a connection from the TOE to a remote TLS server using acumen-tlsc tool that would allow the server's ciphersuite to be modified. Verify that the connection fails. • Verify with packet capture. • Verify with logs.
Expected Test Results	Evidence will show that it will deny the connection due to the TLS version incompatible.
Pass/Fail with Explanation	Pass. The modified TLS connection was rejected. This meets the testing requirement.

6.9.6 FCS_TLSC_EXT.1.1 Test #4c

Item	Data
Test Assurance Activity	[conditional]: If the TOE presents the Supported Elliptic Curves/Supported Groups Extension the evaluator shall configure the server to perform an ECDHE or DHE key exchange in the TLS connection using a non-supported curve/group (for example P-192) and shall verify that the TOE disconnects after receiving the server's Key Exchange handshake message.
Test Steps	• Attempt a connection from the TOE with acumen-tlsc tool using non-supported curve. • Verify that the TOE disconnects after receiving the server's key exchange handshake message. • Verify with logs.
Expected Output	The acumen-tlsc tool is used to establish a TLS server connection with the TOE using an unsupported curve and the TOE should drop the connection. The packet capture shows the supported curves and then the unsupported curve used to establish the connection. The logs describe effectively describe that the connection was dropped.
Pass/Fail with Explanation	Pass. The TOE rejected a connection when an unsupported curve was used. This meets testing requirements.

6.9.7 FCS_TLSC_EXT.1.1 Test #5a

Item	Data
Test Assurance Activity	Change the TLS version selected by the server in the Server Hello to a non-supported TLS version and verify that the client rejects the connection.
Test Steps	• Using acumen-tlsc tool, attempt a connection to a remote TLS server using a non-supported TLS version and verify that the TOE rejects the connection. • Verify the connection fails with packet capture. • Verify with logs.
Expected Test Results	The acumen-tlsc tool is used to establish a TLS server connection with the TOE using an unsupported TLS version. The TOE rejects the connection when it detects that the TLS version used is unsupported. The packet capture shows the tls version used to establish the connection and then dropping the connection. The logs confirm that the connection has been terminated.
Pass/Fail with Explanation	Pass, The TOE denies the connection due to the TLS version incompatible.

6.9.8 FCS_TLSC_EXT.1.1 Test #5b

Item	Data
Test Assurance Activity	[conditional]: If **using DHE or ECDH**, modify the signature block in the Server's Key Exchange handshake message, and verify that the handshake does not finished successfully, and no application data flows. This test does not apply to cipher suites using RSA key exchange. If a TOE only supports RSA key exchange in conjunction with TLS, then this test shall be omitted.
Test Steps	• Attempt a connection from the TOE to a remote TLS server using acumen-tlsc tool that would allow the server's signature block to be modified. Verify that the connection fails. • Verify the connection with packet capture. • Verify the connection fails with logs.

Expected Test Results	The acumen-tlsc tool is used to modify the signature block in the Server's Key Exchange handshake message, in packet capture it should show that the TOE will reject the connection when the signature block is modified.
Pass/Fail with Explanation	Pass. The TOE rejects the connection when the signature block is modified. This meets testing requirements.

6.9.9 FCS_TLSC_EXT.1.1 Test #6a

Item	Data
Test Assurance Activity	Modify a byte in the Server Finished handshake message and verify that the handshake does not finish successfully and no application data flows.
Test Steps	• Attempt a connection to a modified TLS Server with acumen-tlsc tool. • Verify with packet capture. • Verify with logs.
Expected Test Results	The acumen-tlsc tool is used to establish a TLS server connection with the TOE. The tool is used to modify a byte in the Server Finished handshake message. When the TOE detects that the message has been modified, it rejects the connection. The packet should show that the connection has been dropped after a modified Server finished message is sent. The logs confirm that the connection has been terminated.
Pass/Fail with Explanation	Pass. The modified TLS connection was rejected. This meets the testing requirements.

6.9.10 FCS_TLSC_EXT.1.1 Test #6b

Item	Data
Test Assurance Activity	Send a garbled message from the server after the server has issued the ChangeCipherSpec message and verify that the handshake does not finish successfully and no application data flows.
Test Steps	• Attempt a connection to a modified TLS server using acumen-tlsc that would allow sending a garbled message from the server before the server issues the Change CipherSpec message and verify that the TOE rejects the connection. • Verify with packet capture. • Verify with logs.
Expected Test Results	The acumen-tlsc tool is used to establish a TLS server connection. The tool is used to send a garbled message after the server has issued Change CipherSpec message. When the TOE receives the garbled message, it drops the connection by sending an 'Encrypted Alert'. The packet capture should show that the connection has been concluded and the logs should confirm that the connection has been disconnected.
Pass/Fail with Explanation	Pass. The modified TLS connection was rejected. This meets the testing requirements.

6.9.11 FCS_TLSC_EXT.1.1 Test #6c

Item	Data
Test Assurance Activity	Modify at least one byte in the server's nonce in the Server Hello handshake message and verify that the client rejects the Server Key Exchange handshake message (if using a DHE or ECDHE ciphersuite) or that the server denies the client's Finished handshake message.

Test Steps	• Attempt a connection from the TOE to a remote TLS modified server that would allow the modification of the Server nonce. • Verify with packet capture that the connection attempt was rejected. • Verify with logs.
Expected Test Results	The 'acumen-tlsc' tool is used to establish a TLS server connection with the TOE. The tool modifes any byte in the Server Hello Handshake message and this results in the TOE dropping the connection. The packet capture depicts that the connection is terminated when the TOE realizes that the Server Hello Handshake has been modified. The logs confirm that the connection has been dropped.
Pass/Fail with Explanation	Pass. The modified TLS connection was rejected. This meets the testing requirement.

6.9.12 FCS_TLSC_EXT.1.2 Test #1

Item	Data
Test Assurance Activity	This test is applicable if **TLS-based communications with RFC 6125 is selected for FTP_ITC.1, FTP_TRP, or FPT_ITT.** The evaluator shall present a server certificate that contains a CN that does not match the reference identifier and does not contain the SAN extension. The evaluator shall verify that the connection fails. The evaluator shall repeat this test for each identifier type (e.g. IPv4, IPv6, FQDN) supported in the CN. When testing IPv4 or IPv6 addresses, the evaluator shall modify a single decimal or hexadecimal digit in the CN. Remark: Some systems might require the presence of the SAN extension. In this case the connection would still fail but for the reason of the missing SAN extension instead of the mismatch of CN and reference identifier. Both reasons are acceptable to pass Test 1.
Test Steps	CN: FQDN • Configure the correct reference identifier in the TOE. • Create a server certificate with invalid CN and no SAN. • Connect to the TLS Server using the mismatched CN and verify that it fails. • Verify with packet capture. • Verify with logs.
Expected Test Results	When the CN configured on server certificate doesn't match the reference identifier configured on the TOE, the TOE should reject the connection. It issues an alert of ' Bad Certificate' .The packet capture should confirm that the connection is rejected by the TOE and the logs should validate that the connection has been rejected.
Pass/Fail with Explanation	Pass, The TOE rejects the connection when there is no CN that matched the reference identifier and there is no SAN extension. This meets testing requirementsc

6.9.13 FCS_TLSC_EXT.1.2 Test #2

Item	Data

Test Assurance Activity	This test is applicable if **TLS-based communications with RFC 6125 is selected for FTP_ITC.1, FTP_TRP, or FPT_ITT.** The evaluator shall present a server certificate that contains a CN that matches the reference identifier, contains the SAN extension, but does not contain an identifier in the SAN that matches the reference identifier. The evaluator shall verify that the connection fails. The evaluator shall repeat this test for each supported SAN type (e.g. IPv4, IPv6, FQDN, URI). When testing IPv4 or IPv6 addresses, the evaluator shall modify a single decimal or hexadecimal digit in the SAN.
Test Steps	**CN/SAN: FQDN** • Configure the correct reference identifier in the TOE. • Create a server certificate with valid CN but it contains an identifier in the SAN that does not match the reference identifier. • Attempt a connection to the TLS server and verify that it fails. • Verify with packet capture. • Verify with logs. **CN:FQDN/SAN:IPv4 address** • Configure the correct reference identifier in the TOE. • Create a server certificate with valid CN but it contains an identifier in the SAN that does not match the reference identifier. • Attempt a connection to the TLS server and verify that it fails. • Verify with packet capture. • Verify with logs.
Expected Test Results	When a server certificate contains a CN that matches the reference identifier configured on TOE, but the SAN configured on the server certificate doesn't match the reference identifier, then the TOE should reject the connection. It should issue an alert of ' bad certificate'. The packet capture shows that connection is rejected, and the logs confirm that the connection is rejected.
Pass/Fail with Explanation	Pass, The TOE denies a connection when the certificate does not contain an identifier in the SAN that matches the reference identifier. This meets testing requirements.

6.9.14 FCS_TLSC_EXT.1.2 Test #3

Item	Data
Test Assurance Activity	This test is applicable if **TLS-based communications with RFC 6125 is selected for FTP_ITC.1, FTP_TRP, or FPT_ITT.** If the TOE does not mandate the presence of the SAN extension, the evaluator shall present a server certificate that contains a CN that matches the reference identifier and does not contain the SAN extension. The evaluator shall verify that the connection succeeds. The evaluator shall repeat this test for each identifier type (e.g. IPv4, IPv6, FQDN) supported in the CN. If the TOE does mandate the presence of the SAN extension, this Test shall be omitted.
Test Steps	CN: FQDN • Configure the correct reference identifier in the TOE. • Create a server certificate with valid CN but no SAN. • Connect to the TLS Server and verify that the connection is established. • Verify with packet capture.

Expected Test Results	The TOE establishes a successful TLS server connection when there is no SAN but correct FQDN CN is configured in the server certificate which matches the reference identifier configured on TOE. The packet capture confirms the successful connection.
Pass/Fail with Explanation	Pass. A connection was established when TOE is presented with a server certificate which contains a CN that matches the reference identifier and does not contain the SAN extension. This meets the testing requirements.

6.9.15 FCS_TLSC_EXT.1.2 Test #4

Item	Data
Test Assurance Activity	This test is applicable if **TLS-based communications with RFC 6125 is selected for FTP_ITC.1, FTP_TRP, or FPT_ITT.** The evaluator shall present a server certificate that contains a CN that does not match the reference identifier but does contain an identifier in the SAN that matches. The evaluator shall verify that the connection succeeds. The evaluator shall repeat this test for each supported SAN type (e.g. IPv4, IPv6, FQDN, SRV).
Test Steps	CN: FQDN • Configure the correct reference identifier in the TOE. • server certificate that contains a CN that does not match the reference identifier and contain SAN that match the reference identifier. • Connect to the TLS Server and verify that the connection is established. • Verify with packet capture that connection is successful. CN:FQDN/SAN:IPv4 address • Configure the correct reference identifier in the TOE. • server certificate that contains a CN that does not match the reference identifier and contain SAN that match the reference identifier. • Connect to the TLS Server and verify that the connection is established. • Verify with packet capture that connection is successful.
Expected Test Results	The TOE establishes successful TLS server connection when Incorrect CN is configured but correct SAN has been configured the server certificate that matches the reference identifier configured on TOE. The packet capture confirms the same and shows that a successful connection has been established
Pass/Fail with Explanation	Pass. A connection was established when TOE is presented with a server certificate that contains a CN that does not match the reference identifier but does contain an identifier in the SAN that matches. This meets the testing requirements

6.9.16 FCS_TLSC_EXT.1.2 Test #5 (1)

Item	Data
Test Assurance Activity	This test is applicable if **TLS-based communications with RFC 6125 is selected for FTP_ITC.1, FTP_TRP, or FPT_ITT.** Test 5: The evaluator shall perform the following wildcard tests with each supported type of reference identifier that includes a DNS name (i.e. CN-ID with DNS, DNS-ID, SRV-ID, URI-ID): The evaluator shall present a server certificate containing a wildcard that is not in the left-most label of the presented identifier (e.g. foo.*.example.com) and verify that the connection fails.
Test Steps	CN:FQDN

	• Configure the correct reference identifier in the TOE. • Create a server certificate containing a wildcard that is not in the left-most label of CN. • Verify that the connection fails. • Verify with packet capture. • Verify with logs. SAN:FQDN • Create a server certificate containing a wildcard that is not in the left-most label of CN. • Verify that the connection fails. • Verify with packet capture. • Verify with logs
Expected Test Results	The TOE should reject the TLS server connection as the wildcard does not match with the reference identifier configured on TOE. When the TOE rejects the connection, it issues an alert of 'Bad Certificate'. The packet capture confirms the same and logs depict that the connection was dropped as the TOE wasn't able to verify the certificate.
Pass/Fail with Explanation	Pass. The connection fails when TOE is presented with a server certificate containing a wildcard that is not in the left most label of the CN or SAN. This meets the testing requirements.

6.9.17 FCS_TLSC_EXT.1.2 Test #5 (2)(a)

Item	Data
Test Assurance Activity	This test is applicable if **TLS-based communications with RFC 6125 is selected for FTP_ITC.1, FTP_TRP, or FPT_ITT.** Test 5: The evaluator shall perform the following wildcard tests with each supported type of reference identifier that includes a DNS name (i.e. CN-ID with DNS, DNS-ID, SRV-ID, URI-ID): The evaluator shall present a server certificate containing a wildcard in the left-most label (e.g. *.example.com). The evaluator shall configure the reference identifier with a single left-most label (e.g. foo.example.com) and verify that the connection succeeds, if wildcards are supported, or fails if wildcards are not supported. (Remark: Support for wildcards was always intended to be optional. It is sufficient to state that the TOE does not support wildcards and observe rejected connection attempts to satisfy corresponding assurance activities.)
Test Steps	CN: • Configure the correct reference identifier on the TOE. • Create a server certificate with left-most label in the CN. • Attempt to connect to the TOE and verify that the connection is successful. • Verify with packet capture. SAN: • Create a server certificate with left-most label in the CN. • Attempt to connect to the TOE and verify that the connection is successful. • Verify with packet capture.
Expected Test Results	The TOE establishes a successful TLS Server connection as the reference identifier matches with the wildcard that has been configured in the server certificate. The packet capture helps to

	confirm that the reference identifier matches with the wildcard configured in the server certificate.
Pass/Fail with Explanation	Pass. The TOE established a connection with a server having a wildcard configured in the single leftmost label of the CN or the SAN. This meets the testing requirement.

6.9.18 FCS_TLSC_EXT.1.2 Test #5 (2)(b)

Item	Data
Test Assurance Activity	This test is applicable if **TLS-based communications with RFC 6125 is selected for FTP_ITC.1, FTP_TRP, or FPT_ITT.** Test 5: The evaluator shall perform the following wildcard tests with each supported type of reference identifier that includes a DNS name (i.e. CN-ID with DNS, DNS-ID, SRV-ID, URI-ID): The evaluator shall present a server certificate containing a wildcard in the left-most label (e.g. *.example.com). The evaluator shall configure the reference identifier without a left-most label as in the certificate (e.g. example.com) and verify that the connection fails. (Remark: Support for wildcards was always intended to be optional. It is sufficient to state that the TOE does not support wildcards and observe rejected connection attempts to satisfy corresponding assurance activities.)
Test Steps	CN: • Configure the correct reference identifier on the TOE. • Create a server certificate without a wildcard in the leftmost label of CN. • Attempt to connect to the TOE and verify that the connection fails. • Verify with packet capture. • Verify with logs. SAN: • Create a server certificate without a wildcard in the leftmost label of SAN. • Attempt to connect to the TOE and verify that the connection fails. • Verify with packet capture. • Verify with logs.
Expected Test Results	When the reference identifier configured on the TOE doesn't match the wildcard configured on the certificate, the TOE should drop the TLS server connection by issuing an alert of 'Bad Certificate'. The packet capture shows that connection could not be established, and the logs depict that the connection has been rejected.
Pass/Fail with Explanation	Pass. The TOE rejects a connection with a server when the reference identifier is without the left most label in the CN and SAN. This meets the testing requirements.

6.9.19 FCS_TLSC_EXT.1.2 Test #5 (2)(c)

Item	Data
Test Assurance Activity	This test is applicable if **TLS-based communications with RFC 6125 is selected for FTP_ITC.1, FTP_TRP, or FPT_ITT.** Test 5: The evaluator shall perform the following wildcard tests with each supported type of reference identifier that includes a DNS name (i.e. CN-ID with DNS, DNS-ID, SRV-ID, URI-ID):

	The evaluator shall present a server certificate containing a wildcard in the left-most label (e.g. *.example.com). The evaluator shall configure the reference identifier with two left-most labels (e.g. bar.foo.example.com) and verify that the connection fails. (Remark: Support for wildcards was always intended to be optional. It is sufficient to state that the TOE does not support wildcards and observe rejected connection attempts to satisfy corresponding assurance activities.)
Test Steps	CN: • Configure the correct reference identifier on the TOE. • Create a server certificate with a wildcard in the left-most label in the CN. • Attempt to connect to the TOE and verify that the connection fail. • Verify with packet capture. • Verify the logs SAN: • Create a server certificate with a wildcard in the left-most label in the CN. • Attempt to connect to the TOE and verify that the connection fail. • Verify with packet capture. • Verify the logs
Expected Test Results	When the reference identifier configured on TOE don't match the wildcards used, the TOE should issue an alert of ' Bad Certificate' and fail to establish a TLS server connection. The packet capture should show that the connection is dropped, and the logs confirm that the connection has been terminated.
Pass/Fail with Explanation	Pass. The TOE rejects a connection when the server certificate has a wildcard in two leftmost labels in the CN or SAN. This meets the testing requirement.

6.9.20 FCS_TLSC_EXT.1.3 Test #1

Item	Data
Test Assurance Activity	Using the administrative guidance, the evaluator shall load a CA certificate or certificates needed to validate the presented certificate used to authenticate an external entity and demonstrate that the function succeeds, and a trusted channel can be established.
Test Steps	• Connect to the TOE with a full chain • Verify it succeeds • Delete an intermediary certificate off the TOE • Re-attempt to connect • Verify that this attempt fails
Pass/Fail with Explanation	Pass, when a complete certificate trust chain is present, the TOE is able to make a successful connection. When an incomplete certificate trust chain is present, the TOE is not able to make a successful connection. This meets the testing requirements.

6.9.21 FCS_TLSC_EXT.1.3 Test #2

Item	Data
Test Assurance Activity	The evaluator shall then change the presented certificate(s) so that validation fails and show that the certificate is not automatically accepted. The evaluator shall repeat this test to cover the selected types of failure defined in the SFR (i.e. the selected ones from failed matching of the reference identifier, failed validation of

	the certificate path, failed validation of the expiration date, failed determination of the revocation status). The evaluator performs the action indicated in the SFR selection observing the TSF resulting in the expected state for the trusted channel (e.g. trusted channel was established) covering the types of failure for which an override mechanism is defined.
Pass/Fail with Explanation	Pass. A connection was failed when presented a server certificate that contains a CN that matches the reference identifier, contains the SAN extension, but does not contain an identifier in the SAN that matches the reference identifier. The requirements of this test case are exercised in in FCS_TLSC_EXT.1.2 Test #1 and Test #2, FIA_X509_EXT.1.1 Test #2, and FIA_X509_EXT.1.1 Test #3.

6.9.22 FCS_TLSC_EXT.1.3 Test #3

Item	Data
Test Assurance Activity	The purpose of this test to verify that only selected certificate validation failures could be administratively overridden. **If any override mechanism is defined for failed certificate validation**, the evaluator shall configure a new presented certificate that does not contain a valid entry in one of the mandatory fields or parameters (e.g. inappropriate value in extendedKeyUsage field) but is otherwise valid and signed by a trusted CA. The evaluator shall confirm that the certificate validation fails (i.e. certificate is rejected), and there is no administrative override available to accept such certificate.
Pass/Fail with Explanation	NA. No override options are available for failed certificate validation

6.9.23 FCS_TLSC_EXT.1.4 Test #1

Item	Data
Test Assurance Activity	If the TOE presents the **Supported Elliptic Curves/Supported Groups Extension**, the evaluator shall configure the server to perform ECDHE or DHE (as applicable) key exchange using each of the TOE's supported curves and/or groups. The evaluator shall verify that the TOE successfully connects to the server.
Test Steps	• Start a connection with the server using ECDHE cipher and secp256r1 curve. • Verify with packet capture that connection is established. • Start a connection with the server using ECDHE cipher and secp384r1 curve. • Verify with packet capture. • Start a connection with the server using ECDHE cipher and secp521r1 curve. • Verify with packet capture.
Expected Test Results	The TOE establishes a successful TLS server connection with the supported elliptic curves. The packet capture should shows the supported curve and successful connection.
Pass/Fail with Explanation	Pass. The TOE is able to establish a connection with the supported curves. This meets the testing requirement.

6.10 X509-Rev

6.10.1 FIA_X509_EXT.1.1/Rev Test #1a

Item	Data

Test Assurance Activity	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. 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 certificate to be used in the function, and shall use this chain to demonstrate that the function succeeds.
Note	Please Refer to Test Bed X509-Rev
Test Steps	TLS • Create a full chain of certificates to connect to the TOE. • Upload a complete certificate validation chain to the TOE. • Attempt to connect to the TOE with the complete certificate chain. • Verify the connection succeeds with packet capture. IPSEC • Create a full chain of certificates to connect to the TOE. • Upload a complete certificate validation chain to the TOE. • Attempt to connect to the TOE with the complete certificate chain. • Verify in Logs • Verify the connection succeeds with packet capture.
Expected Test Result	*Evidences will show following results :-* • *When a complete certificate trust chain is present, the TOE will make a successful connection.*
Pass/Fail with Explanation	Pass. This test shows when complete certificate trust chain is present, the TOE is able to make a successful connection .Hence it meets the testing requirements

6.10.2 FIA_X509_EXT.1.1/Rev Test #1b

Item	Data
Test Assurance Activity	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. Test 1b: The evaluator shall then delete one of the certificates in the presented chain (i.e. the root CA certificate or other intermediate certificate, but not the end-entity certificate), and show that an attempt to validate an incomplete chain fails.
Note	Please Refer to Test Bed X509-Rev
Test Steps	TLS • Delete an ICA certificate validation chain to the TOE.

	• Attempt to connect to the TOE with a server certificate with an incomplete chain and verify that it fails. • Verify with packet capture that server certificate chain is incomplete. • Verify with logs. IPSEC • Delete a certificate chain and connect to the TOE. • Upload a incomplete certificate validation chain to the TOE. • Attempt to connect to the TOE with the complete certificate chain. Verify in Logs Verify the connection failed with packet capture.
Expected Test Result	*Evidences will show following results :-* • *When an incomplete certificate trust chain is present, the TOE is not able to make a successful connection*
Pass/Fail with Explanation	Pass. This Test shows that When an incomplete certificate trust chain is present, the TOE is not able to make a successful connection. Hence it meets the testing requirements.

6.10.3 FIA_X509_EXT.1.1/Rev Test #2

Item	Data
Test Assurance Activity	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. The evaluator shall demonstrate that validating an expired certificate results in the function failing.
Note	Please Refer to Test Bed X509-Rev
Test Steps	TLS • A certificate is generated whose validity is expired • Import the CA, ICA certificates onto the TOE. • Configure TOE to connect to Syslog server. • Connect the Syslog server to the TOE. • Verify via Logs on TOE • Verify via pcap IPSEC • Create a certificate valid till 06 April 2024 • Verify the current time • Shift the clock to 06 April 2025 such that the certificate is expired • Attempt to establish a connection between the TOE and PEER • Verify via logs that the certificate is expired Verify via packet capture that the connection failed
Expected Test Result	*Evidences will show that without valid certificate connection cannot be done using digital certificate .*

Pass/Fail with Explanation	Pass, The test shows that TOE had rejected the connection due to expired certificate. Hence it meets the testing requirements.

6.10.4 FIA_X509_EXT.1.1/Rev Test #3

Item	Data
Test Assurance Activity	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. 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 chosen in the selection) to ensure when the certificate is no longer valid that the validation function fails.
Note	Please Refer to Test Bed X509-Rev
Test Steps	CRL-TLS • Configure syslog on the TOE Using the certificate • Verify that the certificate is valid • Run Command to test the connectivity • Pcap packet for a successful connection; application data is transmitted. **OCSP-IPSEC** • Authenticate with CA Certificate • Authenticate with Intermediate Certificate • Attempt to make a connection via ping (Connection will pass) • Output Of OCSP Responder • Output of Index.txt file • Verify with SA established • Verify the established connection with logs • Verify the established in packet capture • Revoke the intermediate certificate. • Verify that the database shows that certificate is revoked. • Attempt a connection with the TOE and verify that it fails. • Verify with OCSP responder that certificate is revoked. • Verify with packet capture. • Verify via logs. • Revoke the end entity certificate • Output of Index.txt file • Try To establish the connection using PING • Verify with Ocsp Responder’s output • Verify the connection failed with help of logs Verify via packet capture. **OCSP-TLS**

	• Create an OCSP profile • Configure the syslog using TLS • Import the CA certificate and validate the OCSP server • Import the CA certificate and validate the OCSP server • Generate the CSR and import the END ENTITY certificate • Verify that all the certificates are valid • Start the TLS server session and verify that it is established • Configure the OCSP server • Verify via packet capture that the session is established • Verify via logs • Revoke the end entity certificate of the PEER • Verify that the certificate is revoked • Establish the TLS server connection and verify that it fails • Start the OCSP responder and verify that the certificate is revoked • Verify via logs that the session failed • Verify via packet capture that the session failed • Revoke the intermediate certificate • Verify that the certificate is revoked • Establish a TLS server connection and verify that it fails • Start the OCSP responder • Verify via logs that the session failed • Verify via packet capture that the session failed
Expected Test Result	*Evidences will show that TOE will not communicate with peers that either have a revoked certificate or one of their intermediate CA certificates are revoked.*
Pass/Fail with Explanation	Pass. The revoked certificates are getting rejected.

6.10.5 FIA_X509_EXT.1.1/Rev Test #4

Item	Data
Test Assurance Activity	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. Test 4: If OCSP 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.
Note	Please Refer to Test Bed X509-Rev
Test Steps	CRL-TLS • Create a certificate without CRL signing Key usage • Import certificate and try to connect to the server • Verify with the PCAP

	TLS-OCSP: • Configure the CA signing the OCSP to use a signing certificate that does not have the OCSP sign key usage bit set • Create an OCSP profile • Import the CA certificate and validate the OCSP server • Import the CA certificate and validate the OCSP server • Generate a CSR and import it • Establish a TLS server session and verify that it fails • Start an OCSP responder • Verify via packet capture that the session failed IPSEC-OCSP • OCSP Responder for Intermediate cert without OCSP signing on TOE • Authenticate and IMPORT certificate • END Entity certificate without OCSP signing • Output of OCSP responder • Try To establish the connection using ping • Verify the connection fail with Logs
Expected Test Result	• *The Evidences will show that TOE rejects the CRL/OCSP request when the OCSP signing purpose which is an OID that is specified in the extended Key Usage extension was not set.* • *The TOE rejected the CRL when CA signing the CRL to use a signing certificate that does not have the CRLsign key usage bit set.*
Pass/Fail with Explanation	Pass, This test shows that the TOE rejected the OCSP request when the OCSP signing purpose which is an OID that is specified in the extendedKeyUsage extension was not set . The TOE rejected the CRL when CA signing the CRL to use a signing certificate that does not have the cRLsign key usage bit set. Hence it meets the testing requirements.

6.10.6 FIA_X509_EXT.1.1/Rev Test #5

Item	Data
Test Assurance Activity	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. Test 5: 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.)
Note	Please Refer to Test Bed X509-Rev
Test Steps	TLS:- • Initiate a connection modifying a byte in the first 8 bytes of the certificate. • Verify the TOE does not established any connection, pcap sequence number 8 shows the changed bytes in certificate • Verify in logs

	IPSEC:- • Configure the CA trustpoints on the TOE • Sign the CSR and create the certificate chain • Import the signed certificate into the TOE • Configure the TOE to connect to strongswanacumen • Initiate an IPsec connection modifying a byte in the first 8 bytes of the certificate. The connection state stays in "CONNECTING" • TOE Status shows that no SA were established • TOE Logs show the negotiation failing due to a certificate decoding error
Expected Test Result	*Evidences will show that it will rejects connections when the first byte of the certificate was modified.*
Pass/Fail with Explanation	Pass, This test shows that the TOE rejects connections when the first byte of the certificate was modified. Hence it meets the testing requirements.

6.10.7 FIA_X509_EXT.1.1/Rev Test #6

Item	Data
Test Assurance Activity	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. Test 6: The evaluator shall modify any byte in the last byte of the certificate and demonstrate that the certificate fails to validate. (The signature on the certificate will not validate.)
Note	Please Refer to Test Bed X509-Rev
Test Steps	TLS • Initiate a connection modifying a byte in the last bytes of the certificate. • Verify the TOE does not established any connection, pcap sequence number 12 shows the changed bytes in certificate • Verify Failure Logs IPSEC • Configure the CA trustpoints on the TOE • Sign the CSR and create the certificate chain • Import the signed certificate into the TOE • Configure the TOE to connect to strongswanacumen • Initiate an IPsec connection modifying a byte in the last bytes of the certificate. • TOE Status shows that no SA were established • TOE Logs show the negotiation failing due to a certificate decoding error
	Evidences will show that it will reject connections when the last byte of the certificate is modified.
Pass/Fail with Explanation	Pass, This test shows that the TOE rejects connections when the last byte of the certificate is modified. Hence it meets the testing requirements .

6.10.8 FIA_X509_EXT.1.1/Rev Test #7

Item	Data
Test Assurance Activity	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. 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.)
Note	Please Refer to Test Bed X509-Rev
Test Steps	TLS • Initiate a connection modifying the public key of the certificate. • Verify the TOE rejects the connection, because the certificate fails to validate. • Verify the TOE rejects the connection via logs IPSEC • Configure the CA trustpoints on the TOE • Sign the CSR and create the certificate chain • Import the signed certificate into the TOE • Configure the TOE to connect to strongswanacumen • Initiate an IPsec connection modifying a byte in the last bytes of the certificate. • TOE Status shows that no SA were established • TOE Logs show the negotiation failing due to a certificate decoding error
Expected Test Result	*Evidences will show that it will rejects connections when the public key of the certificate is modified.*
Pass/Fail with Explanation	Pass, This test shows the TOE rejects connections when the public key of the certificate is modified. Hence it meets the testing requirements.

6.10.9 FIA_X509_EXT.1.2/Rev Test #1

Item	Data
Test Assurance Activity	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 extended Key Usage rules are performed in conjunction with the uses that require those rules. Where the TSS identifies any of the rules for extended Key Usage 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 extended Key Usage rule testing may be omitted. The goal of the following tests it to verify that the TOE accepts only certificates that have been marked as CA certificates by using basic Constraints with the CA flag set to True (and implicitly that the TOE correctly parses the basic Constraints extension as part of X509v3 certificate chain validation). For each of the following tests the evaluator shall create a chain of at least three certificates: - *a self-signed root CA certificate,* - *an intermediate CA certificate and*

	- *a leaf (node) certificate.* 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). Test 1: The evaluator shall ensure that at least one of the CAs in the chain does not contain the basic Constraints extension. The evaluator confirms that the TOE rejects such a certificate at one (or both) of the following points: *(i) as part of the validation of the leaf certificate belonging to this chain;* *(ii) when attempting to add a CA certificate without the basic Constraints 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).* ***TD228 has been applied.***
Note	Please Refer to Test Bed X509-Rev
Test Steps	**TLS-IPSEC:-** TLS • Below is the CA certificate used. Note the lack of basic Constraint's extension • The certificate is loaded onto the TOE • Configure the TOE to support digital certificates • Configure the certificate used by the TOE such that, • The certificate of the CA issuing the TOE's certificate does not contain the basic Constraints extension • Verify that the TOE identifies that the signing CA certificate does not contain the basic Constraints extension • Ensure the TOE rejects the certificate
Expected Test Result	*Evidences will show that TOE will rejects connections when the CA use to sign a certificate does not have the basic Constraints extensions*
Pass/Fail with Explanation	Pass. This shows the TOE rejects a connection with a server as the Basic Constraints extension are missing as part of the chain cert. Hence it meets the requirement.

6.10.10 FIA_X509_EXT.1.2/Rev Test #2

Item	Data
Test Assurance Activity	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. The goal of the following tests it 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). For each of the following tests the evaluator shall create a chain of at least three certificates: - *a self-signed root CA certificate,* - *an intermediate CA certificate and* - *a leaf (node) certificate.* 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). 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: *(i) as part of the validation of the leaf certificate belonging to this chain;* *(ii) (ii) 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).*
Note	Please Refer to Test Bed X509-Rev
Test Steps	• Configure the TOE to support digital certificates • Configure the certificate used by the TOE such that • The certificate of the CA issuing the TOE's certificate has the cA flag in the basicConstraints extension set to FALSE • Verify that the signing CA certificate has the cA flag in the basicConstraints extension set to FALSE • Attempt to load the certificate; this will pass • Ensure the TOE rejects the TLS connection formed using the certificate.
Expected Test Result	*Evidences will show that TOE rejects connections when the False CA use to sign a certificate ,*
Pass/Fail with Explanation	Root CA cert with Basic Constraints=False is getting accepted by the TOE, but connection using the same certificate gets rejected.

6.10.11 FIA_X509_EXT.2 Test #1

Item	Data
Test Assurance Activity	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.
Note	Please Refer to Test Bed X509-Rev
Test Steps	CRL-TLS • Configure the syslog using TLS • Verify that the certificates are valid • Start the TLS server session and verify that it is established

	• Verify via packet capture that the session is established • Delete crl from http server • Run openssl to connect TOE • Verify in packet capture The connection fails with a fatal alert • Verify via logs TLS-OCSP • Create an OCSP profile • Configure the syslog using TLS • Verify that all the certificates are valid • Configure the OCSP server • Verify via packet capture that the session is established • Verify via logs • Keep the OCSP responder OFF thus the TOE will not be able to communicate with the server • Establish a TLS server session and verify that it fails • Verify via logs • Verify via packet capture that the session failed IPSEC-OCSP • Authenticate with CA Certificate • Authenticate with Intermediate Certificate • Attempt to make a connection via ping (Connection will pass) • Output Of OCSP Responder • Output of Index.txt file • Verify with SA established • Verify the established connection with logs • Keep the OCSP responder OFF thus the TOE will not be able to communicate with the server • Try To establish the connection using ping • Verify via log
Expected Test Result	***Evidences will show that*** *TOE will close the connection when it is unable to verify the certificate & The TOE session will fail when the OCSP server is kept OFF*
Pass/Fail with Explanation	Pass, The TOE closes the connection when it is unable to verify the certificate & The TOE session fails when the OCSP server is kept OFF This meets the testing requirements.

6.10.12 FIA_X509_EXT.3 Test #1

Item	Data
Test Assurance Activity	Test 1: The evaluator shall use the guidance documentation to cause the TOE to generate a Certification Request. The evaluator shall capture the generated request 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.
Note	Please Refer to Test Bed X509-Rev
Test Steps	TLS:- •

	• From the TOE, generate a CSR
	• Examine the CSR contents
	• Ensure the CSR contains the following fields
	  ○ Public Key
	  ○ CN
	  ○ Org
	  ○ OU
	  ○ Country
	Ipsec:-
	Repeat the same for IPSEC

Expected Test Result	*Evidences will show that TOE will be able to generate a CSR with all of the requisite information.*
Pass/Fail with Explanation	Pass. This shows that the TOE is able to generate a CSR with all of the requisite information. Hence it meets the testing requirements

6.10.13 FIA_X509_EXT.3 Test #2

Item	Data
Test Assurance Activity	"Test 2: 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 response message, and demonstrate that the function succeeds."
Note	Please Refer to Test Bed X509-Rev
Test Steps	TLS • From the TOE, generate a CSR request • **T**he CSR was then signed using a certificate authority called ROOT-CA that the TOE did not have a CA certificate for. • The evaluator then attempted to import the signed CSR into the TOE. • Next the evaluator imported the CA certificate (ROOT-CA) into the TOE. • After this the evaluator made another attempt to import the signed CSR. • This time certificate is accepted by the TOE IPSEC • From the TOE, generate a CSR request • The evaluator generated a new CSR using the procedure shown in the previous test. The CSR was then signed using a certificate authority chat the TOE did not have a CA certificate for. The evaluator then attempted to import the signed CSR into the TOE • Verify the full CA chain is not Installed • Next the evaluator imported the CA certificate(CA-ROOT) into the TOE. • Below logs was generated • After this the evaluator made another attempt to import the signed CSR. • This time certificate is accepted by the TOE
Expected Test Result	The evidences will show that the TOE will properly responds to request type identified within the Test Objective, whether by accepting, rejecting, or dropping the message without responding.

Pass/Fail with Explanation	Pass, This shows that TOE does not accept the certificate which does not have valid certificate path, and also it accepts the certificate if it contains the certificate path hence it meets the requirement.

6.11 EAP

6.11.1 FCO_NRO.1.1 Test#1

Item	Data
Test Assurance Activity	Test 1: The evaluator shall send a RADIUS Access-Request, from a NAS with which the TOE does not share a RADIUS secret, with NAS identification attributes correctly indicating the originating NAS, containing an encapsulated EAP-response message and a valid message-authenticator attribute. The evaluator shall verify that the TOE discards the request without responding.
Test Steps	• Configure the NAS for RADIUS • Configure the NAS on the TOE for RADIUS without the shared secret • Attempt a connection to the TOE using the NAS without the shared secret • Verify that the TOE discards the request without responding • Verify the connection is failed via packet capture • Verify the connection is failed via logs
Expected Test Result	*Evidences will show that it will reject Access-Request from the NAS when the RADIUS shared secret is missing .*
Pass/Fail with Explanation	Pass, The TOE rejects the Access-Request from the NAS when the RADIUS shared secret is missing. This meets the testing requirement.

6.11.2 FCO_NRO.1.1 Test#2

Item	Data
Test Assurance Activity	Test 2: The evaluator shall send a RADIUS Access-Request, from a NAS with which the TOE does not share a RADIUS secret, with NAS identification attributes falsely indicating a NAS with which the TOE does share a RADIUS secret, containing an encapsulated EAP-response message and a valid message-authenticator attribute. The evaluator shall verify that the TOE discards the request without responding.
Test Steps	• Configure the NAS for RADIUS • Configure the NAS on the TOE for RADIUS with an invalid shared secret • Attempt a connection to the TOE using the NAS with an invalid shared secret • Verify that the TOE discards the request without responding • Verify the connection is failed via packet capture • Verify the connection is failed via logs
Expected Test Results	*Evidences will show that it will reject Access-Request from the NAS when the RADIUS shared secret is invalid .*
Pass/Fail with Explanation	Pass, The TOE rejects the Access-Request from the NAS when the RADIUS shared secret is invalid. This meets the testing requirement.

6.11.3 FCO_NRR.1.1 Test#1

Item	Data
Test Assurance Activity	Test 1: The evaluator shall send a RADIUS Access-Request containing an encapsulated EAP-response message of type Identity, specifying a valid user account, a service for which the user is authorized, and containing all information required to authenticate the user. The evaluator shall verify that the TOE returns an Access-Challenge, and that the MD5 hash of the concatenated Code + ID + Length + Request Authenticator of the Access-Request + Attributes + Secret matches the response authenticator.
Test Steps	• Configure the TOE for RADIUS Access-Requests • Attempt a connection to the TOE • Verify the connection is successful • Verify that the MD5 hash of the concatenated Code + ID + Length + Request Authenticator of the Access-Request + Attributes + Secret matches the response authenticator • Verify the connection is established via logs
Expected Test Result	*Evidences will show that it will be able to establish a session using each permitted cipher suite.*
Pass/Fail with Explanation	Pass. The TOE accepts Access-Request containing an encapsulated EAP-response message from the NAS. This meets the testing requirement.

6.11.4 FCS_EAP-TLS_EXT.1.1 Test#1

Item	Data
Test Assurance Activity	Test 1: The evaluator shall establish a TLS connection using each of the cipher suites specified by the requirement. This connection may be established as part of the establishment of a higher-level protocol, e.g., as part of an EAP session. It is sufficient to observe (on the wire) the successful negotiation of a cipher suite to satisfy the intent of the test; it is not necessary to examine the characteristics of the encrypted traffic in an attempt to discern the cipher suite being used (for example, that the cryptographic algorithm is 128-bit AES and not 256-bit AES).
Test Steps	TLS_RSA_WITH_AES_128_CBC_SHA • Configure the TOE for EAP-TLS connection • Configure the Peer for EAP-TLS connection • Attempt a connection to the TOE using the supported ciphersuite • Verify the connection was successful on the client • Verify the connection was successful on the Switch • Verify the connection is established via packet capture • Verify the connection is established via logs

	TLS_RSA_WITH_AES_128_CBC_SHA256 • Configure the TOE for EAP-TLS connection • Configure the Peer for EAP-TLS connection • Attempt a connection to the TOE using the supported ciphersuite • Verify the connection was successful on the client • Verify the connection was successful on the Switch • Verify the connection is established via packet capture • Verify the connection is established via logs TLS_RSA_WITH_AES_256_CBC_SHA256 • Configure the TOE for EAP-TLS connection • Configure the Peer for EAP-TLS connection • Attempt a connection to the TOE using the supported ciphersuite • Verify the connection was successful on the client • Verify the connection was successful on the Switch • Verify the connection is established via packet capture • Verify the connection is established via logs TLS_RSA_WITH_AES_256_GCM_SHA384 • Configure the TOE for EAP-TLS connection • Configure the Peer for EAP-TLS connection • Attempt a connection to the TOE using the supported ciphersuite • Verify the connection is successful on the client • Verify the connection is successful on the Switch • Verify the connection is established via packet capture • Verify the connection is established via logs

	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 • Configure the TOE for EAP-TLS connection • Configure the Peer for EAP-TLS connection • Attempt a connection to the TOE using the supported ciphersuite • Verify the connection is successful on the client • Verify the connection is successful on the Switch • Verify the connection is established via packet capture • Verify the connection is established via logs TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 • Configure the TOE for EAP-TLS connection • Configure the Peer for EAP-TLS connection • Attempt a connection to the TOE using the supported ciphersuite • Verify the connection is successful on the client • Verify the connection is successful on the Switch • Verify the connection is established via packet capture • Verify the connection is established via logs TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 • Configure the TOE for EAP-TLS connection • Configure the Peer for EAP-TLS connection • Attempt a connection to the TOE using the supported ciphersuite • Verify the connection is successful on the client • Verify the connection is successful on the Switch • Verify the connection is established via packet capture • Verify the connection is established via logs

	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 • Configure the TOE for EAP-TLS connection • Configure the Peer for EAP-TLS connection • Attempt a connection to the TOE using the supported ciphersuite • Verify the connection is successful on the client • Verify the connection is successful on the Switch • Verify the connection is established via packet capture • Verify the connection is established via logs TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • Configure the TOE for EAP-TLS connection • Configure the Peer for EAP-TLS connection • Attempt a connection to the TOE using the supported ciphersuite • Verify the connection is successful on the client • Verify the connection is successful on the Switch • Verify the connection is established via packet capture • Verify the connection is established via logs TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • Configure the TOE for EAP-TLS connection • Configure the Peer for EAP-TLS connection • Attempt a connection to the TOE using the supported ciphersuite • Verify the connection is successful on the client

	• Verify the connection is successful on the Switch • Verify the connection is established via packet capture • Verify the connection is established via logs TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 • Configure the TOE for EAP-TLS connection • Configure the Peer for EAP-TLS connection • Attempt a connection to the TOE using the supported ciphersuite • Verify the connection is successful on the client • Verify the connection is successful on the Switch • Verify the connection is established via packet capture • Verify the connection is established via logs TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 • Configure the TOE for EAP-TLS connection • Configure the Peer for EAP-TLS connection • Attempt a connection to the TOE using the supported ciphersuite • Verify the connection is successful on the client • Verify the connection is successful on the Switch • Verify the connection is established via packet capture • Verify the connection is established via logs TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 • Configure the TOE for EAP-TLS connection • Configure the Peer for EAP-TLS connection • Attempt a connection to the TOE using the supported ciphersuite

	• Verify the connection is successful on the client • Verify the connection is successful on the Switch • Verify the connection is established via packet capture • Verify the connection is established via logs TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 • Configure the TOE for EAP-TLS connection • Configure the Peer for EAP-TLS connection • Attempt a connection to the TOE using the supported ciphersuite • Verify the connection is successful on the client • Verify the connection is successful on the Switch • Verify the connection is established via packet capture • Verify the connection is established via logs
Expected Test Result	• *Evidences will show that it will be able to establish a session using each permitted cipher suite .* • *Logs will show not permitted Cipher suite cannot be access.*
Pass/Fail with Explanation	Pass, The TOE is able to establish the connection using each supported ciphersuite. This meets the testing requirement.

6.11.5 FCS_EAP-TLS_EXT.1.1 Test#2

Item	Data
Test Assurance Activity	Test 2: The following test is repeated for each supported certificate signing algorithm supported. The evaluator shall attempt to establish the connection such that the client certificate contains the Client Authentication purpose in the extended Key Usage field and the Key Agreement bit is set in the Key Usage field and verify that a connection is established. The evaluator will then verify that connection is not established with an otherwise valid client certificate that lacks the Client Authentication purpose in the extended KeyUsage field
Test Steps	• Create a client certificate with the Client Authentication in the extendedKeyUsage field and the Key Agreement bit is set in the Key Usage field • Attempt a connection to the TOE using the supported ciphersuite • Verify the connection was successful on the client • Verify the connection was successful on the Switch • Verify the connection is established via packet capture • Verify the connection is established via logs

	• Create a client certificate without the Client Authentication in the extendedKeyUsage field and the Key Agreement bit is not set in the Key Usage field • Attempt a connection to the TOE using the supported ciphersuite • Verify the connection was un-successful on the client • Verify the connection was un-successful on the Switch • Verify the connection is not established via packet capture • Verify the connection is not established via logs
Expected Test Result	*Evidences will show two results:-* • *It will accept connections if client certificate includes Client Authentication purpose in the extended KeyUsage field.* • *It will reject connection if client certificate doe not contain Client Authentication purpose in the extended KeyUsage field*
Pass/Fail with Explanation	Pass. The TOE does not make the connection because the evaluation of the extended keyusage field fails. This meets the test requirements.

6.11.6 FCS_EAP-TLS_EXT.1.1 Test#3

Item	Data
Test Assurance Activity	Test 3: The evaluator shall follow the administrative guidance to configure the list of cipher suites to be proposed during EAP-TLS negotiations that is limited to only those specified by the first element of this component. The evaluator shall have the EAP-TLS client propose a set of cipher suites and show that the TOE will only negotiate the configured ciphers and ignore any others when proposed by a client. If the initial list is not a subset of the total set of cipher suites proposed by the client, the evaluator shall repeat the test specifying a proper subset of the cipher suites used in the initial test. **TD0171 has been applied.**
Test Steps	TLS_DHE_RSA_WITH_AES_128_CBC_SHA • Configure the TOE for EAP-TLS connection for supported ciphersuite • Configure the Peer for EAP-TLS connection the unsupported ciphersuite • Attempt a connection to the TOE using the unsupported ciphersuite • Verify the connection failure on the client • Verify the connection failure on the Switch • Verify the connection is failed via packet capture • Verify the connection is failed via logs

	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 • Configure the TOE for EAP-TLS connection for supported ciphersuite • Configure the Peer for EAP-TLS connection the unsupported ciphersuite • Attempt a connection to the TOE using the unsupported ciphersuite • Verify the connection failure on the client • Verify the connection failure on the Switch • Verify the connection is failed via packet capture • Verify the connection is failed via logs
Expected Test Result	*Evidences will show that it will reject the connection when using the un-supported cipher suites defined within the SFR.*
Pass/Fail with Explanation	Failed. The TOE is able to establish the connection using unsupported ciphersuites.

6.11.7 FCS_RADIUS_EXT.1.1 Test#1

Item	Data

Test Assurance Activity	Test 1: The evaluator shall send RADIUS access-requests with encapsulated EAP-response messages to the TOE, from a NAS with which the TOE shares a RADIUS pre-shared key, and verify that the TOE responds appropriately according to RFCs 2865 and 3579:
	• The evaluator shall verify that the TOE returns either an access-reject or an access-reject with an encapsulated EAP-response with type NAK.
	• Access-requests containing encapsulated EAP-response messages and each of the following attributes: User-password, CHAP-password, CHAP-challenge, ARAP-password, password-retry, reply-message, error-cause. The evaluator shall verify that in each case, the TOE discards the request without responding.
	• An access-request containing an encapsulated EAP-response message, but no message-authenticator attribute. The evaluator shall verify that the TOE discards the request without responding.
	• An access-request containing an encapsulated EAP-response message of type MD5-challenge. The evaluator shall verify that the TOE responds with an access-challenge message of type Nak or expanded Nak.
	• An access-request containing an encapsulated EAP-response message of type Identity, specifying a valid user account, a service for which the user is authorized, and containing all information required to authenticate the user.
	  ○ The evaluator shall verify that the TOE returns an access-challenge with an encapsulated EAP-TLS start packet; i.e. an EAP-request with EAP-type set to EAP-TLS, the start bit set, and no data.
	  ○ The evaluator shall go on to complete the TLS handshake, presenting valid, untrusted, expired, and revoked client certificates to the TOE, and verify that

	the handshake completes successfully only for valid certificates, and unsuccessfully otherwise, ○ The evaluator shall verify that the TOE indicates a successful TLS handshake with an access-accept with encapsulated EAP-success packet. The evaluator shall verify that the TOE indicates an unsuccessful TLS handshake with an access-reject with encapsulated EAP-failure packet. ○ During an otherwise successful handshake, the evaluator shall send an access-request with encapsulated EAP-response with EAP-type set to anything but EAP-TLS, and verify that the TOE returns an access-challenge with encapsulated EAP-request of type EAP-TLS, indicating error-cause: invalid EAP type error (ignored). The evaluator shall verify that subsequent handshake steps complete normally. ○ During an otherwise successful handshake, the evaluator shall send five or less invalid EAP packets, and verify that the TOE returns an access-reject with encapsulated EAP-failure packet after receiving an invalid packet. If the number of packets are configurable, the evaluator must follow the instructions in the operational guidance to verify the ability to set this value to 5 or less. • An access-request containing an encapsulated EAP-response message of type Identity, specifying a valid user account, and a service for which the user is not authorized. The evaluator shall verify that the TOE returns an access-reject. • An access-request containing an encapsulated EAP-response message of type Identity, specifying an invalid user account. The evaluator shall verify that the TOE returns an access-reject. • An Access-Request whose length field is incorrect. The evaluator shall verify that the TOE discards the request without responding. • An Access-Request whose code field is invalid. The evaluator shall verify that the TOE discards the request without responding. • An Access-Request containing an encapsulated EAP-response message and a message-authenticator attribute that does not match the request. The evaluator shall verify that the TOE discards the request without responding. **TD0171 has been applied.**
Test Steps	EAP-response with MD5 challenge • Configure Supplicant to send MD5-Challenge • Attempt a connection to the TOE using MD5 • Verify the connection failure on the client • Verify the connection is failed via packet capture showing an access-reject with an encapsulated EAP-response with type NAK. • Verify the connection is failed via logs EAP-response with MSCHAP-Password • Configure Supplicant to send MSCHAP-Password • Attempt a connection to the TOE using MSCHAP-Password • Verify the connection failure on the client

	• Verify the connection is failed via packet capture showing an access-reject with an encapsulated EAP-response with type NAK • Verify the connection is failed via logs EAP-response with Username-Password • Configure Supplicant to send Username-Password • Attempt a connection to the TOE using Username-Password • Verify the connection failure on the client • Verify the connection is failed via packet capture showing an access-reject with an encapsulated EAP-response with type NAK • Verify the connection is failed via logs EAP-response with Password-Retry • Configure Supplicant to send Password-Retry • Attempt a connection to the TOE using Password-Retry • Verify the connection failure on the client • Verify the connection is failed via packet capture showing an access-reject with an encapsulated EAP-response with type NAK • Verify the connection is failed via logs EAP-response for Valid Certificate • Configure Supplicant to use valid certificate • Attempt to connect to the TOE with the full chain of proper certificates • Verify the connection is successful on the client • Verify the connection is established via packet capture • Verify the connection is successful via logs EAP-response for Expired Certificate • Create an expired certificate • Configure Supplicant to use the expired certificate • Attempt a connection to the TOE using the expired certificate • Verify the connection failure on the client • Verify the connection is failed via packet capture • Verify the connection is failed via logs EAP-response for Untrusted CA Certificate • Create an invalid CA certificate • Configure Supplicant to use the invalid CA certificate • Attempt a connection to the TOE using the invalid CA certificate

	• Verify the connection failure on the client • Verify the connection is failed via packet capture • Verify the connection is failed via logs EAP-response for Invalid EAP-type • Configure Supplicant to use the protocol PEAP • Attempt a connection to the TOE using the PEAP protocol • Verify the connection failure on the client • Verify the connection is failed via packet capture • Verify the connection is failed via logs EAP-response for Invalid EAP-type • Configure Supplicant to use the protocol PEAP • Configure the TOE to send 5 invalid EAP packets • Attempt a connection to the TOE using the PEAP protocol • Verify the connection failure on the client • Verify the connection is failed via packet capture • Verify the connection is failed via logs EAP-response for Access-Deny (Service) • Configure Supplicant to send valid credentials • Configure the TOE to deny the access • Attempt a connection to the TOE using the valid credentials • Verify the connection failure on the client • Verify the connection is failed via packet capture • Verify the connection is failed via logs EAP-response for Unauthorized User • Configure Supplicant to send invalid credentials • Configure the TOE to allow only authorized user • Attempt a connection to the TOE using the invalid credentials • Verify the connection failure on the client • Verify the connection is failed via packet capture • Verify the connection is failed via logs EAP-response with invalid code field • Configure Supplicant to send valid credentials • Delete Existing bridge on the raspberry Pi module: • Modify the attribute using MITM tool • Attempt a connection to the TOE using the valid radius attribute • Verify the proper bit (code field) is modified by the MITM tool (01) • Verify the connection failure on the client

	• Packet capture before modification. • Packet capture after modification • Verify the connection is failed via logs EAP-response with invalid Message Authenticator Attribute • Configure Supplicant to send valid credentials • Delete Existing bridge on the raspberry Pi module: • Modify the attribute using MITM tool • Attempt a connection to the TOE using the valid radius attribute • Verify that the proper bit has been modified • Verify the connection failure on the client • Show the packet before being modified. • Show the packet after being modified. • Verify the connection is failed via logs EAP-response with invalid length field • Configure Supplicant to send valid credentials • Delete Existing bridge on the raspberry Pi module • Modify the length field using MITM tool • Attempt a connection to the TOE using the valid radius attribute • Verify the proper byte (length field) is modified by the MITM tool (01 of 01:1D) • Verify the connection failure on the client • Show the packet before being modified. • Show the packet after being modified. • Verify the connection is failed via logs
Expected Test Result	• *Evidences will show that TOE will properly responds to request type identified within the Test Objective, whether by accepting,* • *Logs will also show that it will be rejecting the message without responding .* • *Logs will also show that it will be dropping the message without responding*
Pass/Fail with Explanation	Pass, The TOE properly responds to request type identified within the test, by accepting, rejecting, or dropping the message without responding.

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 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 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

7.1.1.3 ADV_FSP.1 Activity 3

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

7.2 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 'Operational Environment' of the AGD was used to determine the verdict of this assurance activity. The AGD specifies that: The TOE supports (in some cases optionally) the following hardware, software, and firmware in its environment: **Table 1: Operational Environment Components**

Component	Required	Usage/Purpose Description for TOE performance
Administrative Console	Yes	This console provides the connection to the ISE appliance for administration and management. The console can connect directly to ISE or over the network via a browser or SSHv2 connection. The TOE supports the following browsers: • Mozilla Firefox version 70 and later • Google Chrome version 78 and later • Microsoft Edge
Remote Authentication Store	No	The TOE supports local authentication or authentication via a remote authentication store, including LDAP and Active Directory.
Syslog Target	Yes	The TOE must offload syslog to an external entity, which can be another iteration of ISE or a syslog server that supports TLS-protected transfer.
RADIUS Authenticator	Yes	Used during the 802.1X authentication exchange to relay the supplicant authentication to the Authentication Server. The 802.1X frames carry EAP authentication packets which are passed through to the RADIUS Authentication Server.

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 'Excluded Functionality' 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. 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: 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 Test #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 Test #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

<table>
<tr><td>Objective</td><td>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).</td></tr>
<tr><td>Evaluator Findings</td><td>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 section titled ‘Operational Environment’ of the AGD. The evaluator found that Table 3 describes how the Operational Environment must meet:

Table 3: Operational Environment Components
<table>
<tr><th>Component</th><th>Required</th><th>Usage/Purpose Description for TOE performance</th></tr>
<tr><td>Administrative Console</td><td>Yes</td><td>This console provides the connection to the ISE appliance for administration and management. The console can connect directly to ISE or over the network via a browser or SSHv2 connection.
The TOE supports the following browsers:
Mozilla Firefox version 70 and later
Google Chrome version 78 and later
Microsoft Edge</td></tr>
<tr><td>Remote Authentication Store</td><td>No</td><td>The TOE supports local authentication or authentication via a remote authentication store, including LDAP and Active Directory.</td></tr>
<tr><td>Syslog Target</td><td>Yes</td><td>The TOE must offload syslog to an external entity, which can be another iteration of ISE or a syslog server that supports TLS-protected transfer.</td></tr>
<tr><td>RADIUS Authenticator</td><td>Yes</td><td>Used during the 802.1X authentication exchange to relay the supplicant authentication to the Authentication Server. The 802.1X frames carry EAP authentication packets which are passed through to the RADIUS Authentication Server.</td></tr>
</table>
Based on these findings, this assurance activity is considered satisfied.</td></tr>
<tr><td>Verdict</td><td>Pass</td></tr>
</table>

7.3.1.2 AGD_PRE.1 Activity 2

<table>
<tr><td>Objective</td><td>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.</td></tr>
<tr><td>Evaluator Findings</td><td>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,
<table>
<tr><th>Component</th><th>Required</th><th>Usage/Purpose Description for TOE performance</th></tr>
<tr><td>Administrative Console</td><td>Yes</td><td>This console provides the connection to the ISE appliance for administration and management. The console can connect directly to ISE or over the network via a browser or SSHv2 connection.
The TOE supports the following browsers:
• Mozilla Firefox version 70 and later
• Google Chrome version 78 and later
• Microsoft Edge</td></tr>
<tr><td>Remote Authentication Store</td><td>No</td><td>The TOE supports local authentication or authentication via a remote authentication store, including LDAP and Active Directory.</td></tr>
<tr><td>Syslog Target</td><td>Yes</td><td>The TOE must offload syslog to an external entity, which can be another iteration of ISE or a syslog server that supports TLS-protected transfer.</td></tr>
<tr><td>RADIUS Authenticator</td><td>Yes</td><td>Used during the 802.1X authentication exchange to relay the supplicant authentication to the Authentication Server. The 802.1X frames carry EAP authentication packets which are passed through to the RADIUS Authentication Server.</td></tr>
</table>
• Based on these findings, this assurance activity is considered satisfied.</td></tr>
<tr><td>Verdict</td><td>Pass</td></tr>
</table>

7.3.1.3 AGD_PRE.1 Activity 3

<table>
<tr><td>Objective</td><td>The evaluator shall examine the preparative procedures to ensure they include instructions to successfully install the TSF in each Operational Environment.</td></tr>
<tr><td>Evaluator Findings</td><td>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,
• Configuring Administrative Accounts and Passwords
○ Section ‘Secure Installation and Configuration’
• Configuring SSH and Console Connections
○ Section ‘Remote Administration Protocols’</td></tr>
</table>

	• Configuring the Remote Syslog Server
	  ○ Section 'Logging Protection'
	• Configuring Audit Log Options
	  ○ Section 'Logging Configuration'
	• Configuring VPNs (IPsec)
	  ○ Section 'Virtual Private Networks (VPN)'
	Based on these findings, this assurance activity is considered satisfied.

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

7.3.1.5 AGD_PRE.1 Activity 5

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

7.4 ALC Assurance Activities

7.4.1 ALC_CMC.1

7.4.1.1 ALC_CMC.1 Activity 1

Objective	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.

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

7.4.2 ALC_CMS.1

7.4.2.1 ALC_CMS.1 Activity 1

Objective	When evaluating the developer's coverage of the TOE in their CM system, the evaluator performs the work units as presented in the CEM.
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 perform 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 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. • http://nvd.nist.gov/ • http://www.us-cert.gov • http://www.securityfocus.com/ • https://www.cvedetails.com/ • www.exploitsearch.net • www.securiteam.com • http://nessus.org/plugins/index.php?view=search • http://www.zerodayinitiative.com/advisories • https://www.exploit-db.com • https://www.rapid7.com/db/vulnerabilities The evaluator performed the public domain vulnerability searches using the following key words. The search was performed on 17 August 2023 • Cisco ISE 3600 • Cisco ISE 3500 • Cisco ISE-VM • SNS-3595 • SNS-3615 • SNS-3655 • SNS-3695 • Cisco Identity Services Engine V3.1 • Cisco Identity Services Engine • Cisco ISE SNS-3595 • Cisco ISE SNS-3615 • Cisco ISE SNS-3655 • Cisco ISE SNS-3695 • ESXi 6.7 • ESXi 7.0 • Cisco UCS C220-M5SX • TLS • Authentication server • TCP • UDP • ipsec • Intel Xeon E5-2640 • Intel Xeon Silver 4110

	• Intel Xeon Silver 4116 • Network Accesss Server 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. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.6.1.2 AVA_VAN.1 Activity 2

Objective	The evaluator shall perform the following activities to generate type 4 flaw hypotheses: • Fuzz testing o Examine effects of sending: ▪ 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. 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 traffic. Any results that are unexpected (e.g., core dumps) are candidates for a flaw hypothesis. o 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.
Evaluator Findings	The evaluator documented the fuzz testing results with respect to this requirement.

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

8 Conclusion

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

A. Appendix: CAVP Mapping

Table 2 - CAVP Mapping

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	CiscoSSL FIPS Object Module (FOM)	RSA FIPS PUB 186-4 Key Generation (2048-bit key, 4096-bit key)	A1420 A2697
		IOS Common Cryptographic Module (IC2M) Rel5a	RSA FIPS PUB 186-4 Key Generation (2048-bit key, 4096-bit key)	A1462
	ECC schemes using "NIST curves" [selection: P-256, P-384, P-521] that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4	CiscoSSL FIPS Object Module (FOM)	ECDSA Key Generation FIPS PUB 186-4, "Digital Signature Standard (DSS)" (256 bits, 384 bits and 521 bits) NIST curves- P-256, P-384 and P-521	A1420 A2697
		IOS Common Cryptographic Module (IC2M) Rel5a	ECDSA Key Generation FIPS PUB 186-4, "Digital Signature Standard (DSS)" (256 bits, 384 bits and 521 bits) NIST curves- P-256, P-384 and P-521	A1462
	FFC schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.1	CiscoSSL FIPS Object Module (FOM)	DSA Key Generation FIPS PUB 186-4, "Digital Signature Standard (DSS)"	A1420 A2697
	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	N/A	Vendor Affirmed
FCS_CKM.2	RSA-based key establishment schemes that meet the following: RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 8017, "Public-	N/A	N/A	Vendor Affirmed

SFR	Algorithm in ST	Implementation name	CAVP Alg.	CAVP Cert #
	Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1"			
	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"	CiscoSSL FIPS Object Module (FOM)	CVL-KAS-ECC	A1420 A2697
		IOS Common Cryptographic Module (IC2M) Rel5a	CVL-KAS-ECC	A1462
	Finite field-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 2, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"	CiscoSSL FIPS Object Module (FOM)	CVL-KAS-FFC	A1420 A2697
		IOS Common Cryptographic Module (IC2M) Rel5a	CVL-KAS-FFC	A1462
	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	N/A	Vendor Affirmed
FCS_COP.1/ DataEncryption	AES used in [CBC, CTR, GCM] mode and cryptographic key sizes [128 bits, 256 bits]	CiscoSSL FIPS Object Module (FOM)	AES CBC (128 and 256 bits) CTR (128 and 256 bits) GCM (128, and 256 bits)	A1420 A2697
		IOS Common Cryptographic Module (IC2M) Rel5a	AES CBC (128 and 256 bits)	A1462
FCS_COP.1/ SigGen	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	CiscoSSL FIPS Object Module (FOM)	RSA FIPS PUB 186-4 Signature Generation & Verification (2048-bit key, 4096-bit key)	A1420 A2697
		IOS Common Cryptographic Module (IC2M) Rel5a	RSA FIPS PUB 186-4 Signature Generation & Verification (2048-bit key, 4096-bit key)	A1462
	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	CiscoSSL FIPS Object Module (FOM)	ECDSA FIPS PUB 186-4, "Digital Signature	A1420 A2697

SFR	Algorithm in ST	Implementation name	CAVP Alg.	CAVP Cert #
			Standard (DSS)" (256 bits, 384 bits and 521 bits) NIST curves- P-256, P-384 and P-521	
		IOS Common Cryptographic Module (IC2M) Rel5a	ECDSA FIPS PUB 186-4, "Digital Signature Standard (DSS)" (256 bits, 384 bits and 521 bits) NIST curves- P-256, P-384 and P-521	A1462
FCS_COP.1/ Hash	[SHA-1, SHA-256, SHA-384, SHA-512] and message digest sizes [160, 256, 384, 512] bits	CiscoSSL FIPS Object Module (FOM)	SHS (SHA-1, SHA-256, SHA-384, and SHA-512)	A1420 A2697
		IOS Common Cryptographic Module (IC2M) Rel5a	SHS (SHA-1, SHA-256, SHA-384, and SHA-512)	A1462
FCS_COP.1/ KeyedHash	[HMAC-SHA-1, HMAC-SHA- 256, HMAC-SHA-384, HMAC-SHA-512] and cryptographic key sizes [key size (in bits) used in HMAC] and message digest sizes [160, 256, 384, 512] bits	CiscoSSL FIPS Object Module (FOM)	HMAC (HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA384, and HMAC-SHA-512)	A1420 A2697
		IOS Common Cryptographic Module (IC2M) Rel5a	HMAC (HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA384, and HMAC-SHA-512)	A1462
FCS_RBG_EXT.1	CTR_DRBG (AES)	CiscoSSL FIPS Object Module (FOM)	DRBG CTR_DRBG (AES 256)	A1420 A2697
		IOS Common Cryptographic Module (IC2M) Rel5a	DRBG CTR_DRBG (AES 256)	A1462

End of Document