Network Device Collaborative Protection Profile (NDcPP) Extended Package

Enterprise Session Controller

Version: 1.0

2016-10-25

National Information Assurance Partnership

Revision History

Version	Date	Comment
v0.1	2016-08-26	Initial draft
v0.2	2016-09-16	Updates based on TC feedback
v0.3	2016-10-24	Updates based on TC feedback
v1.0	2016-10-25	Final for publishing

Table of Contents

1 Introduction 5
1.1 Overview 5
1.2 Terms 5
1.2.1 Common Criteria Terms 5
1.2.2 Technology Terms 5
1.3 Compliant Targets of Evaluation 6
1.3.1 TOE Boundary 7
1.4 Use Cases 9
2 Conformance Claims 11
3 Security Problem Description 12
3.1 Threats 12
3.2 Assumptions 12
3.3 Organizational Security Policies 13
4 Security Objectives 14
4.1 Security Objectives for the TOE 14
4.2 Security Objectives for the Operational Environment 14
4.3 Security Objectives Rationale 14
5 Security Requirements 15
5.1 NDcPP Security Functional Requirements Direction 15
5.1.1 Security Audit (FAU) 16
5.1.2 Cryptographic Support (FCS) 17
5.1.3 Identification and Authentication (FIA) 18
5.1.4 Security Management (FMT) 18
5.1.5 Protection of the TSF (FPT) 21
5.1.6 Trusted Path/Channels (FTP) 21
5.2 TOE Security Functional Requirements 23
5.2.1 Security Audit (FAU) 23
5.2.2 User Data Protection (FDP) 28
5.2.3 Identification and Authentication (FIA) 32
5.2.4 Security Management (FMT) 34
5.2.5 Protection of the TSF (FPT) 35
5.3 TOE Security Assurance Requirements 38
5.3.1 Class AVA: Vulnerability Assessment 38
A. Optional Requirements 39
B. Selection-Based Requirements 40
C. Objective Requirements 42
D. Entropy Documentation and Assessment 43
E. References 44

F. Acronyms 45

1 Introduction

1.1 Overview

The scope of this Extended Package (EP) is to describe the security functionality of an Enterprise Session Controller in terms of [CC] and to define functional and assurance requirements for such products. This EP is not complete in itself, but rather extends collaborative Protection Profile for Network Devices (NDcPP) because an ESC is a specific type of network device. An ESC performs a critical role in a voice/video over IP (VVoIP) infrastructure so mitigating threats against its functionality is important for an organization to ensure that sensitive communications are not subject to unauthorized disclosure to unintended recipients.

1.2 Terms

The following sections provide both Common Criteria and technology terms used in this EP.

1.2.1 Common Criteria Terms

Common Criteria (CC)	Common Criteria for Information Technology Security Evaluation.
Common Evaluation Methodology (CEM)	Common Evaluation Methodology for Information Technology Security Evaluation.
Extended Package (EP)	An implementation-independent set of security requirements for a specific subset of products described by a PP.
Protection Profile (PP)	An implementation-independent set of security requirements for a category of products.
Security Assurance Requirement (SAR)	A requirement for how the TOE's proper implementation of the SFRs is verified by an evaluator.
Security Functional Requirement (SFR)	A requirement for security enforcement by the TOE.
Security Target (ST)	A set of implementation-dependent security requirements for a specific product.
Target of Evaluation (TOE)	The product under evaluation. In this case, a network device with Enterprise Session Controller capabilities.
TOE Security Functionality (TSF)	The security functionality of the product under evaluation.
TOE Summary Specification (TSS)	A description of how a TOE satisfies the SFRs in a ST.

1.2.2 Technology Terms

Term	**Meaning**
Audit Log	A persistent record of security-relevant events such as administrative access, administrative actions performed, system failures, and the establishment and termination of remote communications.
Call Detail Record	A log of call metadata that can be used to determine characteristics of a call, such as its length and involved parties, without recording any of its content.

Call Processing	The act of translating a dialed phone number into an attempt to establish a connection with the appropriate party; this is in contrast to the actual transmission of voice/video media over a call.
Enterprise Session Controller	A type of network device that is responsible for establishment, processing, and termination of Voice/Video over IP (VVoIP) calls.
Service Provider	A third-party telecommunications company that is responsible for providing commercial service and connectivity to the worldwide telephone network.
Session Border Controller	A type of network device that resides on the edge of a VVoIP network that is responsible for filtering corrupted or potentially malicious traffic and preventing it from entering or leaving the network.
System Log	A live display of system characteristics that can be viewed on demand to diagnose system performance in real time. This data is typically only stored for a short period of time if at all.
Telecommunications Device	In this EP, used to refer generally to any piece of infrastructure equipment that the ESC may connect to other than a VVoIP Endpoint, which could include equipment such as a call conferencing server or Session Border Controller.
Trunking	The concept of connecting multiple networks together; analogous to the use of a T1 line in a legacy telephone network.
VVoIP Endpoint	A VVoIP-capable phone or software application that a human user can use to make or receive a voice or video call.

1.3 Compliant Targets of Evaluation

The Target of Evaluation that is defined by the combination of the NDcPP and this EP is a network device, either a dedicated appliance with a non-modifiable operating system, or a general-purpose server running an independent commercially-available operating system that provides ESC functionality. Regardless of whether the TOE is a standalone appliance or a general-purpose server that is configured to function as an ESC, the TOE must be capable of satisfying all of the mandatory requirements of the NDcPP.

An ESC is a privately-owned telecommunication switch where its primary function is to set up, process, and terminate voice & video calls over an enterprise-wide Internet Protocol (IP) network. ESC operation is analogous to the tasks of 1930's telephone switchboard-operators, which is to patch (connect) together callers to callees. But today's ESC executes switchboard operations automatically, while providing simultaneous connectivity to hundreds of callers at lightning speed. In addition to establishing, processing, and managing thousands of connected calls, most ESCs support auxiliary services such as Voice & Video over IP (VVoIP) Conferencing, Voicemail, Chat, Telepresence, Encrypted Communications, and Protocol Translation for end-to-end connectivity of diverse endpoints.

ESCs are commonly known as Call Servers, Communications Servers, and Call-Processing Systems, and they vary in complexities and capabilities. The typical ESC can manage thousands of calls between diverse client devices such as VoIP-handsets, Softphones, Desktop Telepresence Systems, Room-size Video Telepresence Systems, and Mobile Devices. ESCs are normally installed within a SCIF or other entry-controlled environment, especially systems that can register numerous VVoIP endpoints. To protect the ESC, a Session Border Controller (SBC) is installed on the outer edge of the VVoIP network to help protect the ESC from external network attacks. Also note that a fairly robust ESC system includes many major components such as its own database, operating system (O/S), conferencing system, dialplan, network manager, call-signaling protocols (e.g. H.323, SIP, SS7), and its own ‘Operations, Administration, and Management (OA&M)’ application system.

If any one of these major components is successfully attacked, then one can expect the entire ESC system to be negatively impacted. The intention of this Extended Package (EP) is to provide a list of security requirements needed by an ESC for protection of its functionality and protection of the VVoIP communications it is responsible for facilitating.

1.3.1 TOE Boundary

An ESC is a logical component of a physical hardware appliance that is responsible for establishing connectivity between VVoIP endpoints. The ESC is an advanced version of a legacy IP-PBX system. As a specific type of network device, an ESC TOE will be evaluated against both the NDcPP and this EP. All functionality described by the SFRs are within the TOE boundary, as is the ability for the TSF to establish secure remote connections with trusted entities in the Operational Environment.

Figure 1 below shows a typical VVoIP infrastructure in which an ESC is deployed.

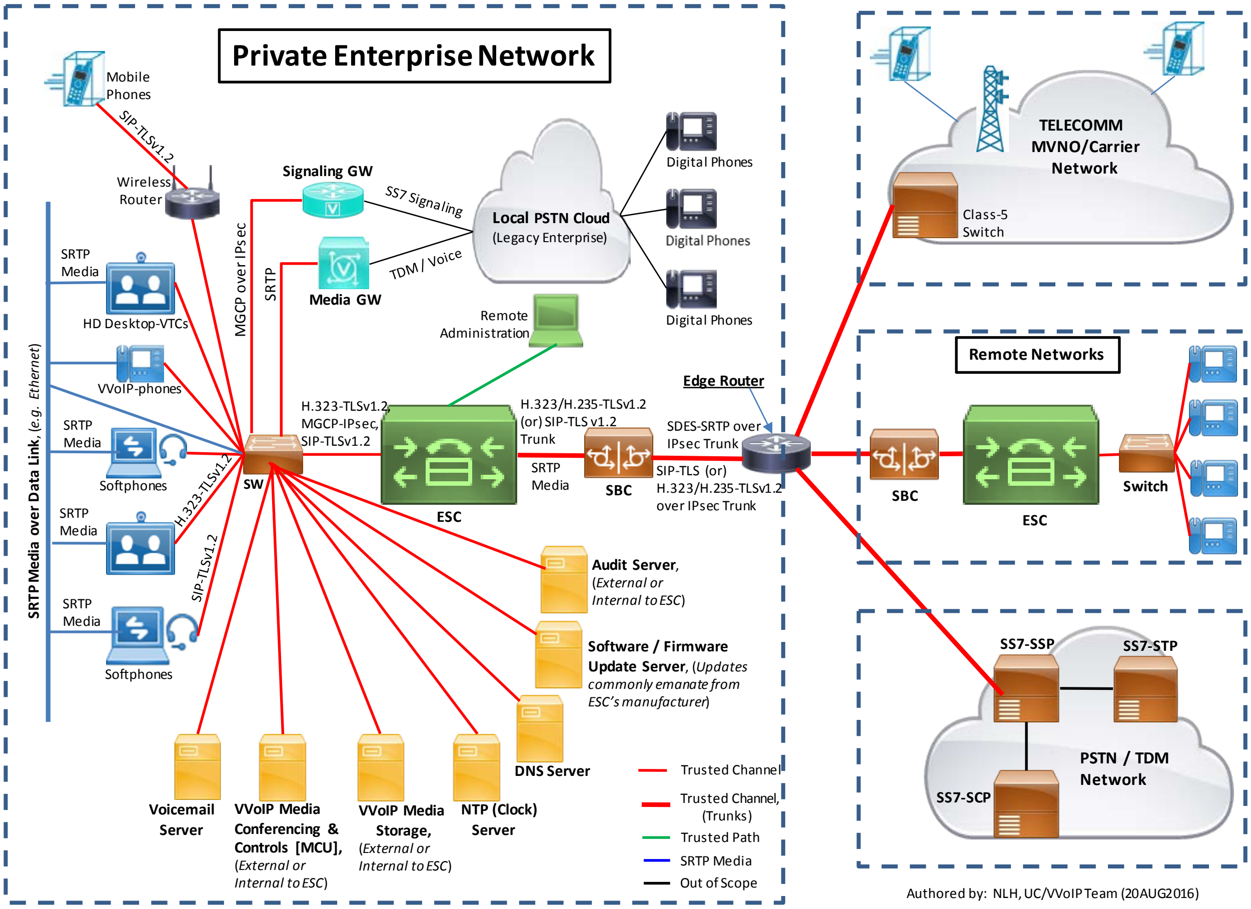

Private Enterprise Network
Mobile Phones
SIP-TLSv1.2
Wireless Router
Signaling GW
SS7 Signaling
Local PSTN Cloud (Legacy Enterprise)
Digital Phones
Digital Phones
Digital Phones
Media GW
TDM / Voice
MGCP over IPsec
SRTP
SRTP Media
HD Desktop-VTCs
Remote Administration
VVoIP-phones
SRTP Media over Data Link, (e.g. Ethernet)
SRTP Media
Softphones
H.323-TLSv1.2
SW
SRTP Media
SIP-TLSv1.2
SRTP Media
Softphones
H.323-TLSv1.2, MGCP-IPsec, SIP-TLSv1.2
ESC
H.323/H.235-TLSv1.2 (or) SIP-TLS v1.2 Trunk
SRTP Media
SBC
Edge Router
SDES-SRTP over IPsec Trunk
SIP-TLS (or) H.323/H.235-TLSv1.2 over IPsec Trunk
Audit Server, (External or Internal to ESC)
Software / Firmware Update Server, (Updates commonly emanate from ESC's manufacturer)
DNS Server
Voicemail Server
VVoIP Media Conferencing & Controls [MCU], (External or Internal to ESC)
VVoIP Media Storage, (External or Internal to ESC)
NTP (Clock) Server
Trusted Channel
Trusted Channel, (Trunks)
Trusted Path
SRTP Media
Out of Scope
TELECOMM MVNO/Carrier Network
Class-5 Switch
Remote Networks
SBC
ESC
Switch
SS7-SSP
SS7-STP
PSTN / TDM Network
SS7-SCP
Authored by: NLH, UC/VVoIP Team (20AUG2016)

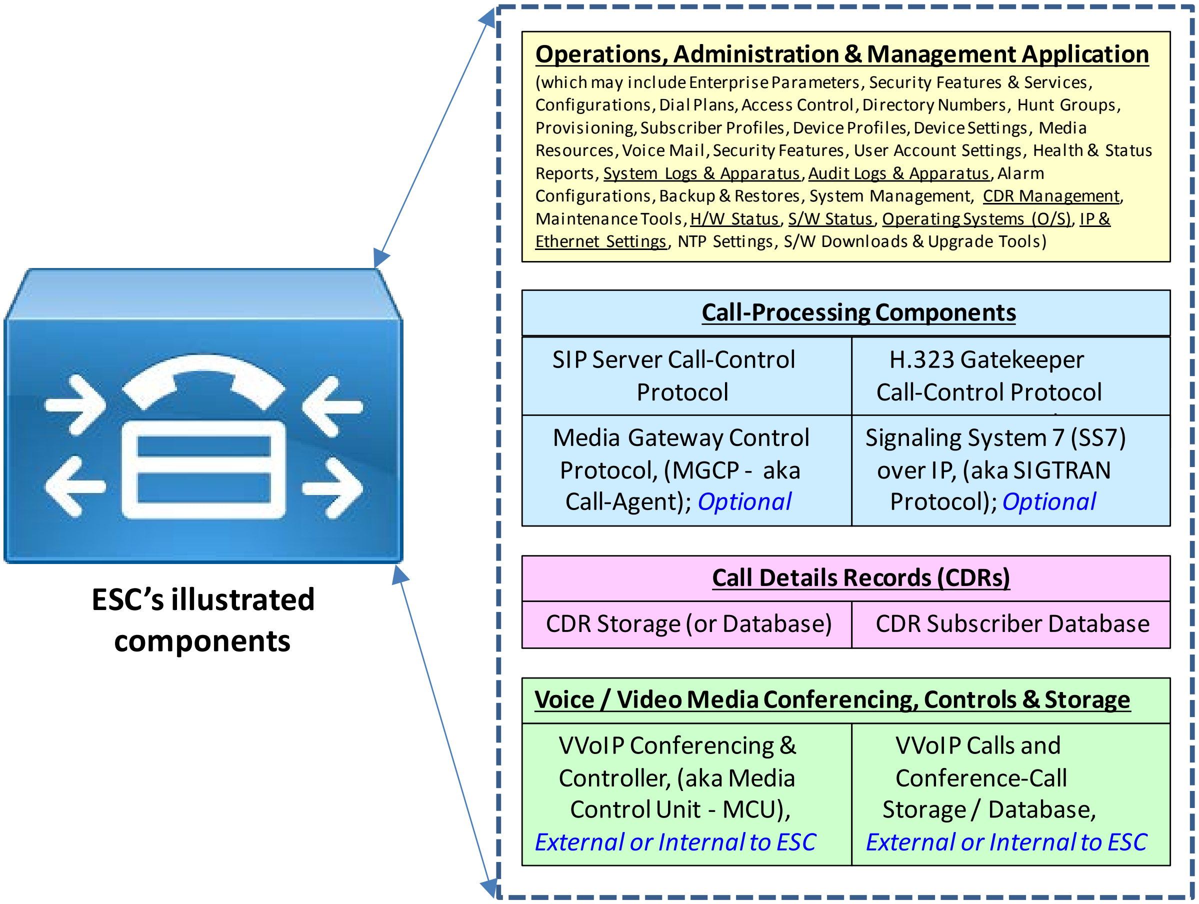
Figure 1 - Representative ESC Deployment

As can be seen from this figure, the ESC’s purpose is to provide an interface between VVoIP networks in order to connect calls. The ESC depends on or communicates with a number of services that are located within the internal network such as voicemail, conferencing, NTP, DNS, and software updates that are downloaded from VVoIP endpoint manufacturers and stored on the ESC for distribution to the clients.

Certain storage capabilities may be implemented exclusively within the TOE or within both the TOE and its operational environment (such as the TOE maintaining an internal audit log that is also written to an external audit server).

For connecting networks, the ESC relies on edge routing to handle lower-level communications between the networks and on a Session Border Controller (SBC) to filter out potentially malicious activity.

The ESC itself, which can be administered locally or remotely, consists of several different logical components, as shown in Figure 2 below.



Operations, Administration & Management Application

(which may include Enterprise Parameters, Security Features & Services, Configurations, Dial Plans, Access Control, Directory Numbers, Hunt Groups, Provisioning, Subscriber Profiles, Device Profiles, Device Settings, Media Resources, Voice Mail, Security Features, User Account Settings, Health & Status Reports, System Logs & Apparatus, Audit Logs & Apparatus, Alarm Configurations, Backup & Restores, System Management, CDR Management, Maintenance Tools, H/W Status, S/W Status, Operating Systems (O/S), IP & Ethernet Settings, NTP Settings, S/W Downloads & Upgrade Tools)

Call-Processing Components	
SIP Server Call-Control Protocol	H.323 Gatekeeper Call-Control Protocol
Media Gateway Control Protocol, (MGCP - aka Call-Agent); *Optional*	Signaling System 7 (SS7) over IP, (aka SIGTRAN Protocol); *Optional*

Call Details Records (CDRs)	
CDR Storage (or Database)	CDR Subscriber Database

Voice / Video Media Conferencing, Controls & Storage	
VVoIP Conferencing & Controller, (aka Media Control Unit - MCU), *External or Internal to ESC*	VVoIP Calls and Conference-Call Storage / Database, *External or Internal to ESC*

Authored by: NLH, UC/VVoIP Team (20AUG2016)

ESC System Components

Figure 2 - ESC Components

As can be seen from the figure above, the ESC provides the following logical capabilities:

- Operations, Administration, and Management Application (OA&M) – responsible for providing a management interface to the ESC's configuration.
- Call Processing – responsible for setting up and tearing down calls between VVoIP endpoints using one or more call control protocols.
- Call Detail Records – responsible for storage of call activity for auditing purposes.

- Voice/Video Media Conferencing, Controls, and Storage – responsible for establishing multi-way conference calls and storage of call recordings.

Different ESCs may implement these capabilities in different ways. This EP defines a minimum baseline of capabilities that all conformant ESCs must provide.

1.4 Use Cases

Requirements in this EP are designed to address the security problem in the following use cases. Use cases are not mutually exclusive; a TOE may implement more than one of these use cases. The description of these use cases provide instructions for how the TOE and its Operational Environment should be made to support the functionality required by this EP.

[USE CASE 1] Dedicated Appliance

The ESC is sold and packaged as a standalone network appliance that does not have a direct interface to the underlying platform operating system, customized application, or commercial-off-the-shelf (COTS) database.

[USE CASE 2] Call Processing (Connect VVoIP Calls Together)

The ESC serves as a call control system that employs multiple technologies for processing and managing voice/video calls between end-point devices. The ESC receives a call-request message from the source IP-phone (endpoint-A), then locate and connect call-originator to the destination device (endpoint-B). Simply stated, the privately owned ESC is used as a centralized system to process, manage, and connect calls between registered IP-phones. It should be noted that H.323 and SIP are the ESC's most commonly used call-processing (i.e. call control) protocols. Both H.323 and SIP maintain conceptually similar purposes which are to setup, process, and terminate voice/video calls between endpoints. In addition, H.323, SIP, and supplemental call control protocols such as MGCP, SIGTRAN and SS7 do not limit ESC capabilities, but instead enhances its flexibilities. In short, both H.323 and SIP provides an ESC the capabilities required for execution of all use cases (i.e. uses cases 1, 2, 3, 4). Both H.323 and SIP provide the ESC call control capabilities, both support trunking between ESC and Service Providers, both support trunking between an array of ESCs, and both can be bonded with encryptions schemes that can secure the ESC's call control function.

[USE CASE 3] Trunk Calls to/from Telecommunications Service Provider

The previous use case describes how an ESC is used to process and manage calls between IP-devices that are registered to the ESC. In such use cases the proxied calls are typically local or internal to the call-processing system, especially to small SIP Proxy Servers. But another use case for the ESC is its capability to bundle numerous calls that emanate from locally registered VVoIP-phones, onto an ESC's communication trunk for connectivity through a Telecomm Service Provider (e.g. Verizon) to remote endpoints. Basically, the ESC supports the aggregation of all registered IP devices for the purpose of passing local calls over a single trunk to an external service provider. The purpose of trunking calls is a long establish method first developed by legacy telephone companies for bundling local (e.g. campus, corporate) telephone lines into a single line for a more simplistic connection out to a telephone company's central office. This allows the central office to use a single trunk for connecting thousands of phones to a large building or campus, as oppose to connecting every possible telephone line from a specific location back to the telephone company's central office.

[USE CASE 4] Trunk Calls in/out to Remote ESCs

Similar to trunking calls to Service Providers, the ESC can trunk thousands of calls to other remote ESC's. An illustrated use case includes a meshed configuration of trunk connected ESCs that are deployed to support a metropolitan-sized enterprise-wide VVoIP call-processing network. This particular type of use case may not require any of the meshed ESCs to be connected to a service provider.

2 Conformance Claims

Conformance Statement

To be conformant to this EP, an ST must demonstrate Exact Conformance, a subset of Strict Conformance as defined in [CC] Part 1 (ASE_CCL). The ST must include all components in this PP that are:

- Unconditional (which are always required)
- Selection-based (which are required when certain selections are chosen in the unconditional requirements)

It may also include components that are:

- Optional
- Objective

Unconditional requirements are found in the main body of the document (Section 5), while appendices contain the selection-based, optional, and objective requirements. The ST may iterate any of these components but it must not introduce any additional component (e.g. from CC Part 2 or 3) that is not defined in either this EP or the NDcPP, which it extends.

CC Conformance Claims

This EP is conformant to Parts 2 (extended) and 3 (conformant) of Common Criteria Version 3.1, Revision 4 [CC].

PP Claims

This EP does not claim conformance to any Protection Profile. Note that this EP extends the NDcPP, which means that it relies on the NDcPP to provide some set of 'base' functionality which is then expanded upon by this EP. This however does not imply that the EP is conformant to the NDcPP.

Package Claims

This EP does not claim conformance to any packages.

3 Security Problem Description

The ESC is a network appliance that incorporates multiple components and protocols, and is designed with the purpose of connecting and managing calls that emanate from registered VVoIP endpoints. The ESC is also designed to provide centralized control of an enterprise-wide VVoIP communication network. As the central control system that manages and processes VVoIP calls from as many as 50,000 endpoints per node, it is critically important for the ESC to be protected because it is a single point of failure for tens of thousands of end-users.

As a centralized system the ESC is subject to attacks from the very VVoIP endpoints that are registered to the ESC. Any VVoIP endpoint could be a threat to launch a malicious attack against the ESC. Therefore the ESC shall possess the security requirements needed for mitigating such a threat type.

The security problem is described in terms of the threats that the TOE is expected to address, assumptions about its operational environment, and any organizational security policies that the TOE is expected to enforce.

Note that as an EP of the NDcPP, all threats, assumptions, and OSPs defined there will also apply to an ESC TOE unless otherwise specified.

The Security Functional Requirements (SFRs) defined in this EP will mitigate the threats that are defined in the EP but will also mitigate some NDcPP threats in more comprehensive detail due to the specific capabilities provided by an ESC.

3.1 Threats

T.MALICIOUS_TRAFFIC

A malformed packet is a protocol packet containing modified data not recognizable by the receiving device (e.g. TOE), or contains modified protocol packets intended to crash or cause the TOE to act in ways unintended. An attacker may attempt to use a VVoIP endpoint to send these malformed packets or malicious traffic towards the TOE in an attempt to control or crash the call control system and connected network devices. To mitigate VVoIP endpoint devices from being used to successfully launch malicious traffic, the TOE must provide encryption remedies to prevent modification of protocol packets. The TOE must also provide authentication mechanisms to prevent unauthorized VVoIP endpoints from improperly registering to the ESC for the purpose of launching malicious attacks.

T.NETWORK_DISCLOSURE

An attacker may attempt to “map” IP addresses of VVoIP endpoint/devices and other telecommunications equipment for the purpose of determining the organizational structure of the enterprise, providing reconnaissance for future targeted attacks.

T.UNAUTHORIZED_CLIENT

An attacker may attempt to register an unauthorized VVoIP endpoint to the TOE for the purpose of impersonating a legitimate end user device in order to gain unauthorized connectivity to other clients or active calls.

3.2 Assumptions

The assumptions defined for the ESC’s Operational Environment are identical to those defined by the NDcPP.

3.3 Organizational Security Policies

The following organizational security policy is applicable to the TOE if the TOE is deployed on an independent, commercially-available operating system:

P.SECURED_PLATFORM

Administrators in the organization ensure that general purpose computers use secure operating systems and are configured in accordance with applicable security standards.

4 Security Objectives

4.1 Security Objectives for the TOE

The NDcPP defines no security objectives for the TOE so no additional TOE security objectives are defined in this EP.

4.2 Security Objectives for the Operational Environment

The security objectives for the operational environment for this EP are the same as the security objectives for the operational environment of the base NDcPP with the following exceptions:

- OE.NO_THRU_TRAFFIC_PROTECTION is not applicable to this EP. The ESC has a responsibility to establish VVoIP calls between endpoints and as such will be responsible for securing the call set up and tear-down processes. Depending on the functionality of a given ESC, it may also have additional responsibilities such as conferencing capabilities that require it to secure through traffic for additional purposes.
- If the TOE is a software application deployed on a general-purpose server which functions as a network device, OE.NO_GENERAL_PURPOSE is not applicable to this EP because the OS exercises its general purpose functionally to allow for installation and operation of the ESC. Instead, the following objective is substituted:

OE.SECURED_PLATFORM

The operating system of the network device does not provide an interface or other capability that can be used to adversely affect the TOE or its own functionality.

4.3 Security Objectives Rationale

This section describes how the assumptions, threats, and organizational security policies map to the security objectives. Note that this section only provides mappings for the security objectives defined in this EP.

Threat, Assumption, or OSP	Security Objective	Rationale
P.SECURED_PLATFORM	OE.SECURED_PLATFORM	In order to ensure that the ESC is not subject to compromise it is important for the OS that it is installed on to be secure in terms of closing unnecessary interfaces and providing appropriate security functionality. However, it is necessary for this EP to make this an assumption in the scenario where the TOE uses a commercial third-party OS because the ESC vendor is not responsible for providing the OS and therefore has no control over its inherent functionality or administrative configuration.

5 Security Requirements

This chapter describes the security requirements which have to be fulfilled by the TOE. Those requirements comprise functional components from Part 2 and assurance components from Part 3 of [CC]. The following notations are used:

- **Refinement** operation (denoted by **bold text**): is used to add details to a requirement, and thus further restricts a requirement.
- **Selection** (denoted by *italicized text*): is used to select one or more options provided by the [CC] in stating a requirement.
- **Assignment** operation (denoted by *italicized text*): is used to assign a specific value to an unspecified parameter, such as the length of a password. Showing the value in square brackets indicates assignment.
- **Iteration** operation: are identified with a number inside parentheses (e.g. "(1)")

5.1 NDcPP Security Functional Requirements Direction

This section instructs the ST author on what selections must be made to certain SFRs contained in the NDcPP in order to mitigate the threats defined in this EP or to mitigate a threat from the NDcPP in a more specific or restrictive manner than what it specifies.

Full assurance activities are not repeated for the requirements in this section; only the additional testing needed to supplement what has already been captured in the Supporting Documents for the NDcPP is included.

5.1.1 Security Audit (FAU)

FAU_GEN.1 Audit Data Generation (Audit Log)

There are additional auditable events that serve to extend the FAU_GEN.1 SFR found in the NDcPP. The following events should be combined with those of the NDcPP in the context of a conforming Security Target.

Application Note: *The NDcPP requires that all administrative actions be audited. This requirement is extended to this EP for all activities that are specific to ESC-related functionality.*

Table 1 - Audit Log Events

SFR	Auditable Event	Additional Audit Record Contents
FIA_UAU.2/TC	Successful or failed authentication of trunk connected network component	ID of Administrator that attempts to connect trunk to external device (if available); IP-address of device where trunk request was initiated (if available); IP-address of external device where trunk is to be connected (if available).
FIA_UAU.2/VVoIP	Successful or failed registration of VVoIP endpoint/device	ID of Administrator that attempt to register VVoIP endpoint to TOE (if available); IP-address of device where registration attempt was initiated (if available); IP-address of VVoIP endpoint that attempt to register to ESC (if available).
FIA_UAU.2/VVoIP	Authentication of external VVoIP endpoint/device	**<u>NOTE</u>:** Same as above for FIA_UAU.2/VVoIP. Authentication of external VVoIP endpoints must occur before registration. In short, no successful registration of VVoIP endpoint can happen until after the successful authentication of the VVoIP endpoint.
FMT_SMF.1	TOE database query	ID of Administrator attempting to query or modify database; IP-address of device where database query was initiated; the exact SQL command/instruction that was executed.

FMT_SMF.1	Enabling/disabling VVoIP endpoint/device features	ID of Administrator attempting to enable/disable service or feature on ESC or on external registered device; IP-address of device where enabling/disabling of services or features was initiated; the feature or service that was enabled/disabled.

Assurance Activity

The evaluator shall complete the assurance activity for FAU_GEN.1 as described in the NDcPP for the auditable events defined above in addition to the applicable auditable events that are defined in the NDcPP. The evaluator shall also ensure that the administrative actions defined for this EP are appropriately audited.

FAU_STG.1 Protected Audit Trail Storage

This SFR is optional in the NDcPP but is mandated by this EP because the ESC is expected to maintain audit data internal to the TOE which must be protected from unauthorized access.

Application Note: *Both the "audit data" (FAU_GEN.1) and "system log" data (FAU_GEN.1/Log) are expected to be protected from unauthorized access. This SFR applies to all data related to the behavior of the TOE regardless of how it is categorized or where it is stored.*

Assurance Activity

No additional testing is required for this SFR beyond what is required for the NDcPP.

5.1.2 Cryptographic Support (FCS)

FCS_TLSC_EXT.2 TLS Client Protocol with Authentication

This SFR is optional in the NDcPP but is mandated by this EP because TLS is used to secure SIP and H.323 communications. Additionally, this EP mandates the use of TLS 1.2, so "TLS 1.1 (RFC 4346)" cannot be selected for FCS_TLSC_EXT.2.1 in a conformant ST.

Assurance Activity

No additional testing is required for this SFR beyond what is required for the NDcPP.

FCS_TLSS_EXT.2 TLS Server Protocol with Authentication

This SFR is optional in the NDcPP but is mandated by this EP because TLS is used to secure SIP and H.323 communications. Additionally, if DTLS is supported by the TOE (see FCS_DTLS_EXT.1), it is tested in the same manner as this SFR. Additionally, this EP mandates the use of TLS 1.2, so “TLS 1.1 (RFC 4346)” cannot be selected for FCS_TLSS_EXT.2.1 in a conformant ST.

Assurance Activity

No additional testing is required for this SFR beyond what is required for the NDcPP.

5.1.3 Identification and Authentication (FIA)

FIA_X509_EXT.2 X.509 Certificate Authentication

FIA_X509_EXT.2.1 The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [***IPsec, [selection: TLS, HTTPS, SSH, no other protocols]***], ***VVoIP endpoint registration,*** *and [selection: code signing for system software updates, code signing for integrity verification, [assignment: other uses], no additional uses*].

Application Note: *The NDcPP requires the ST author to select the protocol(s) that certificate authentication is used for. Because this EP mandates the use of X.509 certificates for IPsec, the SFR is refined to include this automatically. Additional protocols may or may not be selected depending on the other functionality provided by the TSF.*

FIA_X509_EXT.2.2 When the TSF cannot establish a connection to determine the validity of a certificate, the TSF shall [*selection: allow the administrator to choose whether to accept the certificate in these cases, accept the certificate, not accept the certificate*].

Assurance Activity

No additional assurance activities are specified for this SFR beyond what is defined in the NDcPP Supporting Documents.

5.1.4 Security Management (FMT)

FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to manage the TSF data to [*selection: Security Administrators, users, [assignment: other administrative roles]*].

Application Note: *For each role defined in FMT_SMR.2, it is expected that the ST author will describe the extent to which the role is authorized to manage or interact with the TSF.*

Assurance Activity

In addition to the assurance activities specified in the NDcPP Supporting Documents for this SFR, the evaluator shall perform the following testing:

Test

For each administrative role defined in this SFR, the evaluator shall authenticate to the TOE as a member of that role and verify that the TSF authorizes them to perform only those functions authorized for that role as defined by the ST and administrative guidance.

FMT_SMF.1 Specification of Management Functions

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 enable/disable voice and video recordings for any registered VVoIP endpoint;**
- **Ability to display the real-time connection status of all VVoIP endpoints (hardware and software) and telecommunications devices;**
- **Ability to clear all TSF data stored on disk;**
- [*selection:*
  - *Ability to configure audit behavior;*
  - *Ability to configure the list of TOE-provided services available before an entity is identified and authenticated, as specified in FIA_UIA_EXT.1;*
  - *Ability to configure the cryptographic functionality;*
  - ***Ability to configure the password policy;***
  - ***Ability to specify the set of audited events;***
  - ***Ability to configure the behavior of the TOE in response to a self-test failure;***
  - *No other capabilities*]

Application Note: *The TOE developer is encouraged, but not required, to provide a more sophisticated password strength policy than what is prescribed by FIA_PMG_EXT.1 as defined in the NDcPP. This may include the ability for an administrator to configure the metrics used to define an acceptable password. At minimum, the minimum password length must be configurable.*

Assurance Activity

In addition to the assurance activities specified in the NDcPP Supporting Documents for this SFR, the evaluator shall perform the following tests:

Test

Test 1: The evaluator shall deploy a test environment with two or more registered VVoIP endpoints. The evaluator shall choose two endpoints and configure the TOE to disable voice/video recording between them. The evaluator shall place a call between the two selected endpoints, verify that the call is successfully established, then terminate the call and observe that the TSF did not record the call. The evaluator shall then configure the TOE to enable voice/video recording between the same two endpoints, repeat the call, and verify that a recording is generated.

Test 2: The evaluator shall deploy a test environment with two or more registered VVoIP endpoints. The evaluator shall choose two endpoints and configure the TOE to disable voice/video recording between them. The evaluator shall place a call between the two selected endpoints, and verify that the call is successfully established. While the call is active, the evaluator shall use the TSF to review active connections and verify that the call is listed. The evaluator shall discontinue the call and verify that the TSF no longer shows it as active.

Test 3 (optional): If "ability to configure the password policy" is selected, the evaluator shall observe what the password strength policy is configured to by default on the TOE and shall verify that it is enforced by defining several weak administrative passwords for a given administrator account that are appropriately rejected by the TSF. The evaluator shall then modify the TOE's password policy in such a manner that at least one of these weak passwords would now be accepted by the policy. The evaluator shall repeat the attempted password changes and observe that the TSF correctly accepts or rejects the passwords based on the new policy.

FMT_SMR.2 Restrictions on Security Roles

FMT_SMR.2.1 The TSF shall maintain the roles:

- Security Administrator
- **User**
- **[*selection: [assignment: other roles], No other roles*]**

FMT_SMR.2.2 The TSF shall be able to associate users with roles.

FMT_SMR.2.3 The TSF shall ensure that the conditions

- The Security Administrator role shall be able to administer the TOE locally;
- **The User role shall be able to administer the TOE locally;**
- The Security Administrator role shall be able to administer the TOE remotely;
- **The User role shall be able to administer the TOE remotely;**
- **[*selection: [assignment: other conditions], No other conditions*]**

are satisfied.

Application Note: *This SFR has been refined from the NDcPP to mandate the inclusion of at least one additional role so that the TSF can define different levels of authorization for the extent to which different individuals can manage the TOE.*

Assurance Activity

No additional assurance activities are prescribed for this SFR. The testing for FMT_SMR.2 as defined in the NDcPP Supporting Documents and for FMT_MTD.1 in this EP are sufficient to show that this SFR has been met.

5.1.5 Protection of the TSF (FPT)

FPT_STM.1 Reliable Time Stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps **using Network Time Protocol version 4 (NTPv4) as specified in RFC 5905, configuring the optional message authentication code (MAC) for symmetric key authentication scheme and Autokey (RFC 5906)**.

Assurance Activity

TSS

The evaluator shall verify that the TSS describes the ability of the TOE to support NTP synchronization.

Guidance

The evaluator shall review the guidance documentation to confirm that it provides instructions for how to enable NTP synchronization.

Test

The evaluator shall manually set the system time to an incorrect value. The evaluator shall then follow the guidance documentation to enable NTP synchronization, synchronize with an NTP server, and observe that the system time is set to the current time.

5.1.6 Trusted Path/Channels (FTP)

FTP_ITC.1 Inter-TSF Trusted Channel

FTP_ITC.1.1 The TSF shall be capable of using **NTPv4 and** [*selection: IPsec, SSH, HTTPS, TLS,* ***SNMPv3, SRTP, DTLS***] to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: audit server, **NTP server, VVoIP endpoints (for protection of signaling protocols), VVoIP endpoints (for protection of voice/video/media content), other ESC devices (for SIP trunking),** [*selection: authentication server,* ***VVoIP conferencing system,*** *[assignment: other capabilities]*] that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.

Application Note: *The NDcPP provides the ability for the ST author to specify the protocols used to establish trusted communications. This EP mandates the inclusion of certain selections based on the required methods of securing VVoIP-related traffic and defines additional protocols for capabilities that are specific to ESC devices. As* *described in section 5.1.2, all relevant selection-based protocol requirements must be included based on the selections that are mandated by this EP.*

FTP_ITC.1.2 The TSF shall permit the TSF, or the authorized IT entities to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [*assignment: list of services for which the TSF is able to initiate communications*].

Assurance Activity

In addition to the assurance activities specified in the NDcPP Supporting Documents for this SFR, the evaluator shall perform the following tests:

Test

Test 1: The evaluator shall set up the TOE to communicate with an NTP server using NTPv4. When performing testing for FPT_STM.1 (in the NDcPP), the evaluator shall capture traffic between the TOE and NTP server to verify that it is using the correct protocol. The evaluator shall verify that the TOE is capable of supporting the optional message authentication code (MAC) for symmetric key authentication scheme and Autokey in accordance with the refinement of FPT_STM.1 defined in this EP.

Test 2: For each combination of signaling protocol (SIP, H.323), method of securing that protocol (IPsec, TLS), and method of securing transmitted media (SRTP, DTLS), the evaluator shall configure the TOE to use the selected protocols through a trunk to a remote ESC. The evaluator shall register a VVoIP endpoint to the TOE and a second VVoIP endpoint to the remote ESC. The evaluator shall place a packet sniffer on the network and capture traffic from the TOE to the local VVoIP endpoint and the remote ESC. The evaluator shall then place a call from one VVoIP endpoint to the other. The evaluator shall verify that the TOE's audit trail shows that the local VVoIP endpoint was configured as a client using the configured protocol, that the traffic between the local VVoIP endpoint and the TOE is unintelligible, and that the traffic between the TOE and the remote ESC is protected for both signaling and media communications using the configured methods of securing them.

The evaluator shall repeat this test as many times as is necessary to demonstrate that each combination of securing the signaling protocol communications, securing the media protocol communications, and securing the SIP trunk from the TOE to the remote ESC can be used as claimed. Note that in any case where this results in double encryption of the traffic (e.g. SRTP-protected media tunneled through IPsec over a SIP trunk), the evaluator shall conduct the test with the outer layer enabled and then disabled in order to verify that both methods of protection are being used.

Test 3 (conditional): If 'VVoIP conferencing system' is selected, the evaluator shall repeat test 2 (depending on the protocols the TOE claims to support) in an environment where the TOE is being used to establish a conference call between three or more registered VVoIP endpoints. In both cases, the evaluator shall verify that all SIP and SRTP traffic is encrypted.

5.2 TOE Security Functional Requirements

The Security Functional Requirements included in this section are derived from Part 2 of the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, with additional extended functional components.

5.2.1 Security Audit (FAU)

FAU_GEN.1/CDR Audit Data Generation (Call Detail Record)

FAU_GEN.1.1/CDR The TSF shall be able to generate a **call detail** record **(CDR)** for **communications between VVoIP endpoints that are established by the TOE.**

FAU_GEN.1.2/CDR The TSF shall record within each **CDR** at least the following information: **[**

- **calling party number (i.e. call originator)**
- **called party number (i.e. call receiver or terminating number)**
- **unique transaction sequence number**
- **call disposition (e.g. call connected, call terminated, call transferred)**
- **call type (e.g. voice only, voice and video, text)**
- **call start time**
- **call end time**
- **call duration**
- **unique identifier of the TOE**
- **call routing into TOE**
- **call routing out of TOE**
- **time zone**
- **call release cause, if applicable (i.e. reason for termination of call)**
- **fault condition(s), if applicable**]

Application Note: *The TOE should be uniquely identified as part of the CDR so that there is attribution of individual CDRs in environments where multiple ESCs are feeding CDRs to a centralized server.*

Assurance Activity

TSS

The evaluator shall examine the TSS to ensure it describes the format of the CDRs generated by the TOE in sufficient detail to demonstrate that the requirement is satisfied.

Guidance

The evaluator shall examine the guidance documentation to determine that it describes the format of CDRs in sufficient detail for the reader to understand their contents and any configuration actions that are required in order for the CDRs to include the data that is mandated by this EP.

Test

Note that these test activities may be performed in conjunction with other tests.

The evaluator shall deploy the TOE in an environment where it can be used to establish calls for a supported signaling protocol (i.e. SIP, H.323). The evaluator shall place a call between two VVoIP endpoints, allow it to remain connected for three minutes, and then hang up. The evaluator shall then verify that the TOE generated CDRs for this call that contain all necessary information in the format specified by the operational guidance and that this information is accurate. The evaluator shall then place a second call where the call is transferred to a third VVoIP endpoint prior to termination.

The evaluator shall repeat this testing for each type of signaling protocol supported by the TOE.

FAU_GEN.1/Log Audit Data Generation (System Log)

FAU_GEN.1.1/Log The TSF shall be able to generate a **system log** record for **current IP connections, NTP status, CPU usage, memory usage, power status, disk and file storage capacity, audit storage capacity, fan status, [*selection: power status, no other activities*].**

FAU_GEN.1.2/Log The TSF shall record within each **system log** record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure of the event); and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*event details described in Table 2*].

Table 2 – System Log Events

Event	Additional System Log Record Contents
Current IP connections	Network interface card (NIC); Status (up or down).
CPU usage	Utilization percentage of TOE CPU(s).
Memory usage	Percentage and/or amount of free memory available for use.
Disk and file storage capacity	Percentage and/or amount of available space remaining for each disk or disk partition on the TOE.
Fan status	Fan identification; Status (on or off).
Power status (conditional)	Status (on or off)

Application Note: *Unlike audit data (see FAU_GEN.1), system log data is used primarily for real-time analysis of system behavior. This data is expected to be treated as non-persistent data by the TOE.*

The ST author is expected to identify the sampling interval for the information presented in the system log so that it is clear to the evaluator how often updates to that information will be presented to an administrator.

Logging of power status is optional and is only intended for TOEs that have multiple redundant power supplies.

Assurance Activity

TSS

The evaluator shall examine the TSS to ensure that and ensure that it mentions the system log and describes how the log is presented. Each type of entry in the system log shall be listed along with a brief description of each content field and what the sampling interval for the data is. The evaluator shall also check to make sure that every log type mandated by the EP is described and that the description of the content fields contains the information required in FAU_GEN.1.2/Log.

Guidance

The evaluator shall check the guidance documentation and ensure any configuration necessary to ensure the TOE generates the required system log is included. The evaluator shall also check that each required system log item is described in the guidance documentation along with each required content field.

Test

The evaluator shall perform the following tests:

Test 1 (current IP connections): First, confirm TOE is connected via IP by pinging it from a remote device. Once IP is confirmed connected, take down IP connection either by physically disconnecting network cable from the TOE's NIC; or as TOE Administrator, issue command to logically take down IP connection. Peruse system logs to confirm IP connection is down. After confirming IP connection as down, reconnect IP or logically bring up IP connection and confirm IP status as up. Repeat for each physical network interface of the TOE.

Test 2 (CPU usage): The evaluator shall use the TOE and monitor the CPU usage status over a period of 10 minutes and observe that fluctuations in CPU usage are reported. It is not necessary to verify that this information is accurate at a low level but the evaluator is expected to justify at a high level why these fluctuations are occurring (e.g. CPU usage spikes while the TOE is establishing a call).

Test 3 (memory usage): The evaluator shall use the TOE and monitor the memory usage status over a period of 10 minutes and observe that fluctuations in memory usage are reported. It is not necessary to verify that this information is accurate at a low level but the evaluator is expected to justify at a high level why these fluctuations are occurring (e.g. memory usage spikes while the TOE is establishing a call or downloading an update).

Test 4 (disk and file storage capacity): The evaluator shall use the TOE and monitor the disk capacity status over a period of 10 minutes and observe that fluctuations in storage capacity are reported. It is not necessary to verify that this information is accurate at a low level but the evaluator is expected to justify at a high level why these changes are occurring (e.g. the evaluator transfers a file with a known file size to a disk partition and observes that the available space decreased by a corresponding amount).

Test 5 (fan status): First, confirm fan is working as designed. Once fan is confirmed functioning properly, disconnect fan to shut it down. Peruse system logs to confirm fan has been reported as down. After confirming fan as down, reconnect fan and confirm fan as up. Repeat this process for each fan that is monitored by the TSF.

Test 6 (power status):

Test 6a (conditional): If TOE employs redundant power supplies (PS), then test may be a simple matter of cycling one PS while leaving other power units untouched. Reset one PS while allowing the other(s) to remain up. Peruse system log and verify message indicating PS cycled (went down & up).

Test 6b (conditional): If TOE is supported by a single PS, than test has to be verified by waiting for system log to provide power status on periodic intervals. If system log does not report power status, then PS test failed.

FAU_SAR.1/Log Audit Review (System Log)

FAU_SAR.1.1/Log The TSF shall provide [*assignment: authorized users*] with the capability to read [*assignment: list of audit information*] from the **system log** records.

Application Note: *The expectation of this element is that the extent to which a user is able to review audit records is dependent on their assigned role as defined in FMT_SMR.2.*

FAU_SAR.1.2/Log The TSF shall provide the **system log** records in a **real-time first-in first-out scrolling method**.

Assurance Activity

Test

For each system log event described in FAU_GEN.1.1/Log, the evaluator shall review the system log to observe that they are displayed in real time. For those system log events that are periodic or persistent status messages, the evaluator shall observe that they are shown in the system log at the proper time. For those events that are triggered by a certain event, the evaluator shall cause that event to occur and ensure that it is logged. For example, the evaluator shall verify that the TOE logs data link connection status by unplugging and reconnecting the TOE's Ethernet connection and verifying that an appropriate log was generated for both. In all cases, the evaluator shall verify that the contents and formatting of the log data are consistent with what is defined in FAU_GEN.1.2/Log.

FAU_STG.1/CDR Protected Audit Trail Storage (Call Detail Record)

FAU_STG.1.1/CDR The TSF shall protect the stored **call detail records** from unauthorized **disclosure and** deletion.

FAU_STG.1.2/CDR The TSF shall be able to [*prevent*] unauthorized modifications to the stored **call detail records**.

Assurance Activity

TSS

The evaluator shall examine the TSS to ensure it describes how CDRs are protected against unauthorized modification or deletion. The evaluator shall also examine the TSS to ensure it describes any administrative access controls placed on CDR modification (e.g., Administrator Type 1 can modify/delete CDRs while Administrator Type 2 cannot modify/delete CDRs).

Guidance

The evaluator shall examine the guidance documentation to determine that it describes any configuration required for protection of the locally stored CDRs against unauthorized modification. The evaluator shall also examine the documentation to ensure that any administrative access controls and configuration of the access controls on CDR access are described.

Test

The evaluator shall log in to the TOE as an Administrator (or other role that is privileged to interact with CDRs) and verify that authorized administrators are able to view stored CDRs but have no ability to modify them. The evaluator shall then log in to the TOE with a role that lacks privilege to interact with CDRs and observe that there is no way for that user role to access the CDR data.

FAU_STG.1/VVR Protected Audit Trail Storage (Voice/Video Recording)

FAU_STG.1.1/VVR The TSF shall protect the stored **voice and video recordings** from unauthorized **disclosure and** deletion **by encrypting voice and video recording data that is stored on the TOE using an encryption method specified in FCS_COP.1**.

FAU_STG.1.2/VVR The TSF shall be able to [*prevent*] unauthorized modifications to the stored **voice and video recordings**.

Assurance Activity

TSS

The evaluator shall examine the TSS to verify that it describes the method by which locally-stored voice and video recordings are protected and that this method uses cryptographic mechanisms defined in FCS_COP.1

Guidance

If the TOE provides the ability to enable/disable encryption of locally stored voice and video recordings, the evaluator shall verify that the operational guidance provides instructions on how to enable encryption and directs the reader to ensure that this is enabled in the TOE's evaluated configuration.

Test

The evaluator shall perform the following tests:

Test 1: The evaluator shall verify that the TSF provides no interface to access voice/video recording data stored on the TOE except for legitimate access from an authorized administrator through the OA&M interface.

Test 2: Both B2B subscriber calls and voice/video conferencing calls may be stored on the TOE based on safeguards (i.e. secured or unsecured) for which they were recorded. The evaluator shall identify the location of stored voice and video records and verify that this data is stored in an encrypted format for all types of voice and video calls that can be processed by the TOE. If this functionality is configurable, the evaluator shall follow the operational guidance to enable encryption prior to generating any voice/video recordings.

5.2.2 User Data Protection (FDP)

FDP_IFC.1 Subset Information Flow Control

FDP_IFC.1.1 The TSF shall enforce the [*enterprise session controller SFP*] on [*caller-callee pairs attempting to communicate through the TOE*].

Assurance Activity

This SFR is tested in conjunction with FDP_IFF.1.

FDP_IFF.1 Information Flow Control Functions

FDP_IFF.1.1 The TSF shall enforce the [*enterprise session controller SFP*] based on the following types of subject and information security attributes: [*assignment: method by which the TSF identifies each endpoint for a call*] **using the following call control protocols: [*selection: SIP, H.323*] and [*selection: SS7, MGCP, no other call control protocols*]**.

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [*when valid communication through the TOE is attempted, the TSF will establish a connection between itself and the caller; the TSF will establish a second connection between itself and the callee; and the TSF will redirect all communications that it receives between the two endpoints out through the proper connection*].

FDP_IFF.1.3 The TSF shall enforce the [*additional information flow control SFP rules: no additional rules*].

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: [*assignment: rules, based on security attributes, that explicitly authorize information flows*].

Application Note: *The expectation of this element is that the ST author define any explicit whitelist behavior that overrides the normal information flow handling to automatically open a communications channel through the TOE. It is acceptable to complete the assignment with "no additional rules" if there are no exceptions to the behavior defined in FDP_IFF.1.2 and 1.3.*

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [*assignment: rules, based on security attributes, that explicitly deny information flows*].

Application Note: *The expectation of this element is that the ST author define any explicit blacklist behavior that overrides the normal information flow handling to automatically block a communications channel through the TOE. It is acceptable to complete the assignment with "no additional rules" if there are no exceptions to the behavior defined in FDP_IFF.1.2 and 1.3.*

Assurance Activity

TSS

The evaluator shall examine the TSS to verify that it describes the call control protocol(s) used by the TOE and the circumstances under which the TSF will transmit streaming media data. The evaluator shall verify that the TSF does not transmit any streaming media in circumstances where a VVoIP endpoint operator would not reasonably expect it to do so and whether there are any explicit overrides to the policy.

Guidance

If any aspects of the TOE's call control functionality are configurable (such as the specific call control protocol used or the circumstances in which the TSF will or will not transmit streaming media data), the evaluator shall examine the operational guidance to verify that instructions for configuring this behavior are provided.

Test

The evaluator shall perform one or more of the following tests depending on the protocols that the TOE claims to support. For each test performed, the evaluator shall conduct the test in both an IPv4 and an IPv6 environment.

If the TSF supports SIP:

The evaluator shall set up a test environment where two SIP clients are registered to the TOE and the TSF is configured to allow call signals to capture through it. The evaluator shall use a packet sniffer to capture call-signaling packets traversing the TOE. The evaluator shall place a call from one SIP client to the other and observe via packet capture that two separate SIP connections are established: one from the caller to the TOE and the other from the TOE to the callee.

If the TSF supports H.323:

The evaluator shall set up a test environment where two H.323 clients are registered to the TOE and the TSF is configured to allow call signals to capture through it. The evaluator shall use a packet sniffer to capture call-signaling packets traversing the TOE. The evaluator shall place a call from one H.323 client to the other and observe via packet capture that two separate H.323 connections are established: one from the caller to the TOE and the other from the TOE to the callee.

If the TSF supports SS7:

Unlike H.323 & SIP which are call-setup and teardown protocols primarily used to process calls between local VVoIP endpoints that are registered to the ESC, the SS7 protocol focuses on setup and teardown of calls over the legacy Public Switch Telephone Network (PSTN). Therefore, when assessing the SS7 protocol, the evaluator will need to configure the TOE to make a call from a local VVoIP endpoint through its SS7 interface to a remote endpoint.

The evaluator shall set up a test environment where a single VVoIP endpoint is registered to the TOE (through H.323 or SIP) and the TSF is configured to allow call signals through it. The evaluator shall use a packet sniffer to capture call-signaling packets traversing the TOE. The evaluator shall place a call from the locally registered VVoIP endpoint to a remote endpoint that requires the use of the TOE’s SS7 extension. The evaluator shall observe and capture SS7 signaling messages transiting through the TOE to both the local client and remote SS7-based endpoint. The evaluator shall verify that the TOE successfully sets up, processes, and tears down call between local VVoIP endpoint and external telephony device requiring SS7 signaling for connectivity. The evaluator shall also verify that the TOE transmits and receives the SS7 signaling messages IAM, ACM, and ANM to set up a call and RLC to tear down a call. The evaluator shall verify that SS7 call processing is employed by verifying that a two-way conversation can occur over the connected call.

If the TSF supports both H.323 and SIP, the evaluator shall repeat this test for the VVoIP endpoint registration method not chosen during the first iteration of the test.

If the TSF supports MGCP:

Unlike H.323 & SIP which are call-setup and teardown protocols primarily used to process calls between local VVoIP-clients that are registered to the ESC, the MGCP protocol focuses on the control of Media Gateways (MG) which set up voice calls between VVoIP networks and the PSTN. The TSF employs MGCP to control MGs that provision VVoIP calls for external connection to the PSTN and from the PSTN to the local VVoIP network. Therefore, when assessing the SS7 protocol, the evaluator will need to configure the TOE to make a call from a local VVoIP-client through its MGCP interface (i.e. MGC/Call Agent) to a remote endpoint.

The evaluator shall set up a test environment where a single VVoIP endpoint is registered to the TOE (through H.323 or SIP) and the TSF is configured to allow call signals through it. The evaluator shall use a packet sniffer to capture call-signaling packets traversing the TOE. The evaluator shall place a call from the locally registered VVoIP endpoint to a remote endpoint that requires the use of the TOE's MGCP extension for PSTN connection. The evaluator shall observe and capture MGCP signaling messages transiting the TOE to/from the local VVoIP endpoint and out to remote MGCP/PSTN endpoint. The evaluator shall verify that the TOE successfully sets up, processes, and tears down the call between the local VVoIP endpoint and external telephony device requiring MGC/PSTN signaling for connectivity. The evaluator shall also verify that the TOE transmits and receives the MGCP signaling messages NTFY, CRCX, and MDCX to set up a call and DLCX to tear down a call. The evaluator shall verify that MGCP call processing is employed by verifying that a two-way conversation can occur over the connected call.

If the TSF supports both H.323 and SIP, the evaluator shall repeat this test for the VVoIP endpoint registration method not chosen during the first iteration of the test.

FDP_RIP.1 Subset Residual Information Protection

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [*selection: allocation of the resource to, deallocation of the resource from*] the following objects: [***assignment: disk storage location(s) erased by the TSF during factory reset or other wipe operation***].

Application Note: *The TOE is expected to follow guidelines for [NIST SP 800-88], 'Disk Storage Sanitization' as the method for ensuring that residual information is cleared from both volatile and nonvolatile memory. This involves overwriting the entire disk or disk partition with zeroes, followed by all ones, followed by all zeroes. Since it is not feasible to pause the wipe operation while in progress it is sufficient for the evaluator to observe during testing that the final result is all* *zeroes; however, the vendor-provided evidence is expected to provide a justification that [NIST SP 800-88] guidelines are being followed.*

Assurance Activity

TSS

The evaluator shall examine the TSS to ensure it describes the data objects overwritten as part of the sanitation operation. This should include both the TSF data that is overwritten as well as the characteristics of the physical drive that is erased (e.g. an entire drive, one or more logical partitions of a drive). The evaluator shall also examine the TSS to ensure that the sanitation process is described. In particular, the TSS must describe how the sanitation process follow the NIST 800-88 guidelines for "Disk Storage Sanitation."

Guidance

The evaluator shall examine the guidance documentation to ensure it describes the data objects overwritten as part of the sanitation operation. The evaluation shall also ensure that the guidance documentation describes the administrative procedures necessary to trigger the sanitation operation. The evaluation shall also ensure that the TOE indication that the sanitization operation has completed is described, if applicable.

Test

The following test may require the evaluator to have access to developer tools.

The evaluator shall identify the storage locations (e.g. drives, disk partitions) that are erased when the TOE performs a wipe operation. The evaluator shall then populate each of these locations with large amounts of ‘junk’ data so that a known amount of their storage is used. The evaluator shall use the TOE to verify that the current storage levels are consistent with the amount of data that was introduced to each location.

The evaluator shall then initiate a wipe command and observe that each location that is subject to erasure is 100% free. The evaluator shall use forensic tools to examine each location that is subject to erasure and verify that the data has been overwritten by all zeroes.

5.2.3 Identification and Authentication (FIA)

FIA_UAU.2/TC User Authentication before Any Action (Telecommunications Devices)

FIA_UAU.2.1/TC The TSF shall require each **telecommunications device** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that **device**.

Assurance Activity

TSS

The evaluator shall examine the TSS and ensure that the telecommunications device authentication procedures are described including a description of how the TOE prevents TSF-mediated actions by unauthenticated devices.

Guidance

The evaluator shall examine the guidance documentation and ensure that any actions required to enable authentication of telecommunications devices is described.

Test

The following testing shall be repeated in both an IPv4 and an IPv6 environment:

The evaluator shall deploy the TOE in an environment with another ESC and configure both ESCs to support an encrypted IPsec trunk to one another. The evaluator shall also deploy a packet sniffer on the IPsec trunk channel. The evaluator shall perform the following tests:

Test 1: The evaluator shall configure the TOE to accept IPsec trunk communications from the remote ESC based on username, password, and IP address. The evaluator shall then use the remote ESC to connect to the TOE and verify that the IPsec trunk is successfully established. The evaluator shall use packet captures to verify that IPsec traffic is transmitted between the TOE and the remote ESC.

Test 2: The evaluator shall repeat test 1 but enter an invalid username/password when attempting to authenticate. The evaluator shall observe that the IPsec trunk is not successfully established due to invalid credentials.

Test 3: The evaluator shall repeat test 1 but configure the TOE to accept IPsec trunk communications from a different IP address than what is assigned to the remote ESC. The evaluator shall then attempt to connect to the TOE using the remote ESC with valid credentials and observe that the IPsec trunk is not successfully established due to invalid IP address.

FIA_UAU.2/VVoIP User Authentication before Any Action (VVoIP Endpoints)

FIA_UAU.2.1/VVoIP The TSF shall require each **VVoIP endpoint** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that **endpoint**.

Application Note: *This includes both the establishment of voice/video calls and the TOE-initiated application of an update to the VVoIP endpoint software/firmware.*

Assurance Activity

TSS

The evaluator shall examine the TSS and ensure that the VVoIP endpoint authentication procedures are described including a description of how the TOE prevents TSF-mediated actions by unauthenticated devices. In addition to establishment of voice/video calls, this includes TOE-initiated application of an update to the VVoIP endpoint software/firmware.

Guidance

The evaluator shall examine the guidance documentation and ensure that any actions required to authenticate VVoIP endpoints are described.

Test

The following testing shall be repeated in both an IPv4 and an IPv6 environment:

The evaluator shall ensure that the TSF is configured to support encrypted SIP and/or H.323 client connections and that any VVoIP endpoint devices used for this testing can use the protocol that the TSF is configured to support.

The evaluator shall perform the following tests:

Test 1: The evaluator shall connect a VVoIP endpoint device to the TOE and attempt to place a call without registering. The attempt should fail. The evaluator shall also attempt to download an update from the TOE and observe failure.

Test 2: The evaluator shall load an invalid certificate onto a VVoIP endpoint device, connect that device to the TOE, and initiate the registration process. The registration process should fail due to an invalid certificate.

Test 3: The evaluator shall load a valid certificate onto a VVoIP endpoint device, connect that device to the TOE, and initiate the registration process. When prompted for a username and password, the evaluator shall supply invalid credentials and observe that the registration process fails for that reason.

Test 4: The evaluator shall load a valid certificate onto a VVoIP endpoint device, connect that device to the TOE, and initiate the registration process. When prompted for a username and password, the evaluator shall supply valid credentials and observe that the registration process succeeds and that the registered device can be used to place calls.

5.2.4 Security Management (FMT)

FMT_CFG_EXT.1 Secure by Default Configuration

FMT_CFG_EXT.1.1 The **TSF** shall provide only enough functionality to set new **Security Administrator** credentials when configured with default credentials or no credentials.

FMT_CFG_EXT.1.2 The **TSF** shall be configured by default with ~~file~~ permissions which protect it and its data from unauthorized access.

Assurance Activity

TSS

The evaluator shall check the TSS and ensure that it identifies if the TOE is delivered with default or no Security Administrative credentials. The evaluator shall also check the TSS and ensure that the functionality available when the TOE is configured with default credentials or no credentials is identified. The evaluator shall examine the identified functionality and ensure that only enough functionality to set new Security Administrator credentials is available when the TOE is configured with default credentials or no credentials.

Guidance

The evaluator shall check the guidance documentation and ensure that the administrative functionality that is available when the TOE is configured with default credentials or no credentials is identified. The evaluator shall examine the guidance documentation and ensure the instructions for establishing new Security Administrative credentials is described.

Test

Note that this test may only be deployed the first time the TOE is run or immediately following a factory reset.

The evaluator shall perform the initial setup steps for the TOE as specified in the administrative guidance. The evaluator shall verify that if a default administrative account is used to log in to the TOE for the first time, the login event is immediately followed by a prompt to change the password for the default account. If no default account is used, the evaluator shall verify that they are prompted to define an initial administrator account and that no further security-relevant actions can be performed until the evaluator has authenticated to the TOE using that account.

5.2.5 Protection of the TSF (FPT)

FPT_FLS.1 Failure with Preservation of a Secure State

FPT_FLS.1.1 The TSF shall preserve a secure state **through the following means: [*selection: audible alarm, visual indicator, reboot of the TOE, shutdown of the TOE, [assignment: other methods*]** when the following types of failures occur: [*failure of self-tests defined in FPT_TST_EXT.1, failure of [assignment: hardware components that affect the proper functioning of the TOE]*].

Assurance Activity

TSS

The evaluator shall examine the TSS to verify that it describes the TOE failures that can occur and the TOE’s response to these failures. The evaluator shall also examine the TSS to verify that it provides sufficient detail to justify how the TOE’s responses to these failures preserves a secure state.

Guidance

The evaluator shall examine the guidance documentation and ensure that if the TOE's failure handling behavior is configurable, any instructions for doing so are provided. The evaluator shall also examine the guidance documentation to verify that it identifies the potential failures that can occur and the TOE's response to them so that the reader is aware of when the TSF has failed to a secure state.

Test

The evaluator shall perform the assurance activities for FPT_TST_EXT.1 as defined in the NDcPP Supporting Documents. For each self-test failure, the evaluator shall verify that the observed TOE behavior is consistent with the failure state defined in the TSS for this SFR. If this functionality is configurable, the evaluator shall reconfigure the TOE to each possible response to a self-test failure and re-execute the testing as many times as is necessary to demonstrate that the configured behavior is observed in each case.

FPT_TUD_EXT.1/VVoIP Trusted Update (VVoIP Endpoints)

FPT_TUD_EXT.1.1/VVoIP The TSF shall provide Security Administrators the ability to query the currently executing version of the **[*registered VVoIP endpoint*]** firmware/software as well as the most recently installed version of the [*registered VVoIP endpoint*] firmware/software.

FPT_TUD_EXT.1.2/VVoIP The TSF shall provide Security Administrators the ability to manually initiate updates to **[*registered VVoIP endpoint*]** firmware/software and [*no other update mechanism*].

FPT_TUD_EXT.1.3/VVoIP The TSF shall provide means to authenticate firmware/software updates to the **[*registered VVoIP endpoint*]** using a [*selection: digital signature mechanism, published hash*] prior to installing those updates.

Application Note: *The TOE may either validate the update prior to storing it for delivery to registered VVoIP endpoints or it may provide the means to validate the update to the VVoIP endpoint itself by preserving the manufacturer's integrity/authenticity mechanism and including that information in the update. In other words, either the TSF itself validates the update or it facilitates the ability of the VVoIP endpoint to do this by providing all information necessary to validate the update to the client.*

It is typical behavior for ESCs to push software updates to registered VVoIP endpoint devices. However, many VVoIP endpoints have the ability to receive software updates from either an ESC or third-party update server. This SFR addresses the case where it is the ESC's responsibility for delivery of software updates to registered VVoIP endpoints.

Assurance Activity

TSS

The evaluator shall examine the TSS to verify that it describes the ability of the TOE to retrieve VVoIP endpoint software/firmware updates and the process by which VVoIP endpoints can register to the TOE and acquire these updates. The evaluator shall also examine the TSS to verify that it describes by which the authenticity and integrity of VVoIP endpoint software updates are assured and what role the TSF has in ensuring that updates are genuine.

Guidance

The evaluator shall examine the operational guidance to verify that it provides instructions on how to acquire and verify a VVoIP endpoint software/firmware update from the manufacturer. The evaluator shall also verify that the guidance includes instructions on how an ESC administrator can use the TOE to apply software/firmware updates to registered VVoIP endpoints.

Test

The evaluator shall perform the following test:

Step 1: Prior to downloading software update from TOE to registered VVoIP-client, the evaluator shall check to ensure the current version of the registered client device can be appropriately obtained by means of the operation methods specified by the administrator guidance.

Step 2: The evaluator shall check to ensure that VVoIP endpoint software/firmware updates are signed and/or hashed by the manufacturer based on what is specified in the ST.

Step 3: The evaluator shall check to ensure that only administrators of the TOE are permitted to initiate an update to a registered VVoIP endpoint.

Step 4: The evaluator shall check to ensure that software updates are correctly performed by verifying that the VVoIP endpoint is running the newly-obtained software version obtaining the newly updated software version of the VVoIP-client device once update has complete.

Note: In some cases the ESC will not receive an explicit message from the VVoIP endpoint stating that the software update executed successfully. In addition, some software updates will not take effect until a reboot of the VVoIP endpoint is initiated remotely by the ESC or manually/physically at the VVoIP endpoint device itself. In either scenario, the VVoIP endpoint itself will always indicate whether verification of the update has failed. Therefore, the tester can (or may have to) verify successful software download by querying the VVoIP endpoint device for new software/firmware version. The tester can also verify whether software update failed by querying the registered VVoIP endpoint for errors.

In most cases, failed software update messages will originate from the VVoIP endpoint and not the ESC. Any failed software update reported by the registered VVoIP endpoint should have the report forwarded to the TOE. However, as mentioned earlier, the registered VVoIP endpoint may not report successful software downloads and therefore no ‘successful download’ report should be expected to be forwarded to the ESC. If the VVoIP endpoint does report a ‘software download complete’ or just ‘complete’, then the TOE should receive a message indicating that the download was completed. When the VVoIP endpoint reboots, it is expected to report the new software/firmware version to the TOE so that the new version will be displayed in the OA&M application.

Step 5: The evaluator shall check to ensure that the verification of software/firmware updates from the TOE to the VVoIP endpoint fails using unauthorized data or improperly signed updates. The evaluator shall also check those cases where hash verification mechanism and digital signature verification mechanism fail.

Note: this may require the evaluator to obtain a deliberately invalid software update from the device manufacturer or developer access to the TOE so that a stored update can be manipulated directly in a manner that will cause signature and/or hash verification to fail.

5.3 TOE Security Assurance Requirements

As an EP of the NDcPP, this EP does not define any additional assurance requirements above and beyond what is defined in the base PP. In general, application of the SARs to the TOE boundary described by both the NDcPP and this EP is sufficient to demonstrate that the claimed SFRs have been implemented correctly by the TOE. However, in some cases it may be necessary to perform additional assurance activities in order to satisfy the SARs due to unique capabilities or limitations of the TOE that is specified by this EP. Where applicable, these assurance activities are described below.

5.3.1 Class AVA: Vulnerability Assessment

An ESC TOE is often represented as a software application that is installed onto a general-purpose server which is operated as a dedicated ESC device. In order to ensure that the OE.NO_GENERAL_PURPOSE environmental objective is satisfied, the evaluator shall conduct vulnerability research and penetration testing related to privilege escalation in order to attempt to ‘break out’ of the ESC interface provided by the administrator and gain general-purpose administrative functionality over the underlying OS. If the evaluator is able to use the underlying OS to affect the behavior of the TOE (through the ability to use general-purpose CLI commands or perform functions via a GUI) or introduce an application or service that causes the network device to be listening on a TCP or UDP port, the vulnerability testing will result in failure. Note that it is acceptable for administrators to have read-only access to certain areas of the OS file system if this behavior is intended by the TOE developer; only write and execute access are prohibited.

A. Optional Requirements

As indicated in Section 2, the baseline requirements (those that must be performed by the TOE) are contained in the body of this EP. Additionally, there are three other types of requirements specified in Appendix A, Appendix B, and Appendix C. The first type (in this Appendix) are requirements that can be included in the ST, but are not required in order for a TOE to claim conformance to this EP. The second type (in Appendix B) are requirements based on selections in the body of the EP: if certain selections are made, then additional requirements in that appendix must be included. The third type (in Appendix C) are components that are not required in order to conform to this EP, but will be included in the baseline requirements in future versions of this PP, so adoption by vendors is encouraged. Note that the ST author is responsible for ensuring that requirements that may be associated with those in Appendix A, Appendix B, and Appendix C but are not listed (e.g., FMT-type requirements) are also included in the ST.

This version of the EP does not define any optional requirements.

B. Selection-Based Requirements

As indicated in the introduction to this EP, the baseline requirements (those that must be performed by the TOE) are contained in the body of the EP. There are additional requirements based on selections in the body of the EP: if certain selections are made, then additional requirements below will need to be included.

FAU_SEL.1 Selective Audit

Application Note: *This requirement shall be included in STs in which 'Ability to specify the set of audited events' is chosen in FMT_SMF.1.1.*

FAU_SEL.1.1 The TSF shall be able to select the set of events to be audited from the set of all auditable events based on the following attributes:

a) [*selection: object identity, user identity, subject identity, host identity, event type*];
b) [*assignment: list of additional attributes that audit selectivity is based upon*]

Assurance Activity

TSS

The evaluator shall examine the TSS to verify that it identifies the attributes by which the TOE can be configured to selectively enable or disable the generation of auditable events.

Guidance

The evaluator shall examine the operational guidance to verify that it provides a list of the attributes that can be used to selectively enable or disable the generation of auditable events as well as instructions for performing this operation.

Test

Note that the following testing may be done in conjunction with other assurance activities since auditable events occur as a by-product of the TOE being used to perform other security functions.

The evaluator shall perform TSF-mediated actions with all auditable events enabled and observe that these events are audited as expected. The evaluator shall then log on to the TOE as an Administrator (or other role that is sufficiently privileged to modify the set of events that the TOE audits) and disable auditable events by each attribute defined in the ST. The evaluator shall then re-execute the same set of TSF-mediated actions as before and observe that audit logs are not generated for all auditable events that are administratively disabled.

FCS_DTLS_EXT.1 DTLS Protocol

Application Note: *This requirement shall be included in STs in which 'DTLS' is chosen in FTP_ITC.1.1.*

FCS_DTLS_EXT.1.1 The TSF shall implement the DTLS protocol in accordance with DTLS 1.2 (RFC 6347).

FCS_DTLS_EXT.1.2 The TSF shall implement the requirements in FCS_TLSS_EXT.2 **as defined in [NDcPP]** for the DTLS implementation, except where variations are allowed according to RFC 6347.

Assurance Activity

The evaluator shall complete the assurance activity for FCS_TLSS_EXT.2 as described in the NDcPP.

C. Objective Requirements

This Annex includes requirements that specify security functionality which also addresses threats. The requirements are not currently mandated in the body of this EP as they describe security functionality not yet widely available in commercial technology. However, these requirements may be included in the ST such that the TOE is still conformant to this EP, and it is expected that they be included as soon as possible.

Currently, no objective requirements specific to ESC TOEs have been identified.

D. Entropy Documentation and Assessment

The TOE does not require any additional supplementary information to describe its entropy source(s) beyond the requirements outlined in the ‘Entropy Documentation and Assessment’ section of the NDcPP. As with other NDcPP requirements, the only additional requirement is that the entropy documentation also applies to the ESC capabilities of the TOE in addition to the base network device functionality.

E. References

Identifier	Title
[CC]	Common Criteria for Information Technology Security Evaluation – • Part 1: Introduction and General Model, CCMB-2012-09-001, Version 3.1 Revision 4, September 2012 • Part 2: Security Functional Components, CCMB-2012-09-002, Version 3.1 Revision 4, September 2012 • Part 3: Security Assurance Components, CCMB-2012-09-003, Version 3.1 Revision 4, September 2012
[GR-1100-CORE]	Billing Automatic Message Accounting Format (BAF) Generic Requirements, Issue 17, December 2012
[NDcPP]	collaborative Protection Profile for Network Devices, Version 1.0, February 2015
[NIST SP 800-88]	Guidelines for Media Sanitization, Revision 1, December 2014

F. Acronyms

Acronym	Meaning
AMA	Automatic Message Accounting
CDR	Call Detail Record
ESC	Enterprise Session Controller
FTP	File Transfer Protocol
IP	Internet Protocol
IP-PBX	IP Private Branch Exchange
NDcPP	Collaborative Protection Profile for Network Devices
NTP	Network Time Protocol
PP	Protection Profile
SBC	Session Border Controller
SIP	Session Initiation Protocol
SNMP	Simple Network Management Protocol
SRTP	Secure Routing Transport Protocol
ST	Security Target
TC	Telecommunications [device]
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSF	TOE Security Function
TSS	TOE Summary Specification
UDP	User Datagram Protocol
VVoIP	Voice/Video over IP