

# PP-Module for Session Border Controllers



Version: 2.0  
2026-03-17

**National Information Assurance Partnership**

## Revision History

---

Version	Date	Comment
1.0	2022-12-05	Initial Release
2.0	2026-03-17	Apply NIAP Technical Decisions, Update to CC:2022

## Contents

---

1	Introduction
1.1	Overview
1.2	Terms
1.2.1	Common Criteria Terms
1.2.2	Technical Terms
1.3	Compliant Targets of Evaluation
1.3.1	TOE Boundary
1.4	Use Cases
1.5	Package Usage
2	Conformance Claims
3	Security Problem Definition
3.1	Threats
3.2	Assumptions
3.3	Organizational Security Policies
4	Security Objectives
4.1	Security Objectives for the Operational Environment
5	Security Requirements
5.1	Collaborative Protection Profile for Network Devices Security Functional Requirements Direction
5.1.1	Modified SFRs
5.1.1.1	Trusted Path/Channels (FTP)
5.2	TOE Security Functional Requirements
5.2.1	Auditable Events for Mandatory SFRs
5.2.2	Security Audit (FAU)
5.2.3	Cryptographic Support (FCS)
5.2.4	User Data Protection (FDP)
5.2.5	Firewall (FFW)
5.2.6	Identification and Authentication (FIA)
5.2.7	Security Management (FMT)
5.2.8	Resource Utilization (FRU)
5.2.9	Trusted Path/Channels (FTP)
5.3	TOE Security Functional Requirements Rationale
6	Consistency Rationale
6.1	Collaborative Protection Profile for Network Devices
6.1.1	Consistency of TOE Type
6.1.2	Consistency of Security Problem Definition
6.1.3	Consistency of OE Objectives
6.1.4	Consistency of Requirements
	Appendix A - Optional SFRs

- A.1 Strictly Optional Requirements
- A.2 Objective Requirements
- A.3 Implementation-dependent Requirements
  - A.3.1 Auditable Events for Implementation-Dependent SFRs
  - A.3.2 Identification and Authentication (FIA)
- Appendix B - Selection-based Requirements
  - B.1 Auditable Events for Selection-Based SFRs
  - B.2 Trusted Path/Channels (FTP)
- Appendix C - Extended Component Definitions
  - C.1 Extended Components Table
  - C.2 Extended Component Definitions
    - C.2.1 Cryptographic Support (FCS)
      - C.2.1.1 FCS\_SRTP\_EXT Secure Real-Time Transport Protocol
    - C.2.2 Firewall (FFW)
      - C.2.2.1 FFW\_ACL\_EXT Traffic Filtering
      - C.2.2.2 FFW\_DPI\_EXT Deep Packet Inspection
      - C.2.2.3 FFW\_NAT\_EXT Network Address Translation
    - C.2.3 Identification and Authentication (FIA)
      - C.2.3.1 FIA\_SIPT\_EXT Session Initiation Protocol Trunking
      - C.2.3.2 FIA\_SIPS\_EXT Session Initiation Protocol Registration
    - C.2.4 Resource Utilization (FRU)
      - C.2.4.1 FRU\_PRS\_EXT Limited Priority of Service
    - C.2.5 Security Audit (FAU)
      - C.2.5.1 FAU\_ARP\_EXT Security Audit Automatic Response
- Appendix D - Implicitly Satisfied Requirements
- Appendix E - Entropy Documentation and Assessment
- Appendix F - Allocation of Requirements in Distributed TOEs
- Appendix G - Acronyms
- Appendix H - Bibliography

# 1 Introduction

## 1.1 Overview

---

The scope of this Protection Profile Module (PP-Module) is to describe the security functionality of a Session Border Controller (SBC) in terms of [CC] and to define functional and assurance requirements for such products. This PP-Module is intended for use with the following Base-PPs:

- Network Device collaborative Protection Profile Version 4.0

This Base-PP is valid because a device that implements an SBC is a specific type of network device, and there is nothing about the implementation of an SBC that would prevent any of the security capabilities defined by the Base-PP from being satisfied.

Note that the NDcPP defines an optional architecture for a “distributed TOE” that allows for security functionality to be spread across multiple distinct components. This PP-Module does not require or prohibit the TOE from being a distributed system when the TOE conforms to the NDcPP; the TOE may be standalone or distributed in this case.

## 1.2 Terms

---

The following sections list Common Criteria and technology terms used in this document.

### 1.2.1 Common Criteria Terms

Assurance	Grounds for confidence that a TOE meets the SFRs [CC].
Base Protection Profile (Base-PP)	Protection Profile used as a basis to build a PP-Configuration.
Collaborative Protection Profile (cPP)	A Protection Profile developed by international technical communities and approved by multiple schemes.
Common Criteria (CC)	Common Criteria for Information Technology Security Evaluation (International Standard ISO/IEC 15408).
Common Criteria Testing Laboratory	Within the context of the Common Criteria Evaluation and Validation Scheme (CCEVS), an IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the NIAP Validation Body to conduct Common Criteria-based evaluations.
Common Evaluation Methodology (CEM)	Common Evaluation Methodology for Information Technology Security Evaluation.
Direct Rationale	A type of Protection Profile, PP-Module, or Security Target in which the security problem definition (SPD) elements are mapped directly to the SFRs and possibly to the security objectives for the operational environment. There are no security objectives for the TOE.

Distributed TOE	A TOE composed of multiple components operating as a logical whole.
Operational Environment (OE)	Hardware and software that are outside the TOE boundary that support the TOE functionality and security policy.
Protection Profile (PP)	An implementation-independent set of security requirements for a category of products.
Protection Profile Configuration (PP-Configuration)	A comprehensive set of security requirements for a product type that consists of at least one Base-PP and at least one PP-Module.
Protection Profile Module (PP-Module)	An implementation-independent statement of security needs for a TOE type complementary to one or more Base-PPs.
Security Assurance Requirement (SAR)	A requirement to assure the security of the TOE.
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.
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 an ST.

## 1.2.2 Technical Terms

Enterprise Session Controller (ESC)	A voice/video over IP (VVoIP) infrastructure device that is used to set up and tear down calls between VVoIP endpoints.
H.323	A communications protocol defined by the ITU Telecommunications Standardization Sector (ITU-T) that is used for creating, modifying, and terminating multimedia sessions with multiple participants.
Media Gateway Control Protocol (MGCP)	A means of communication between a media gateway and a media gateway controller.
Secure Real-Time Transport Protocol (SRTP)	A protocol that is used to provide multimedia (voice/video) streaming services with added security of encryption, message authentication and integrity, and replay protection.
Session Initiation Protocol (SIP)	A communications protocol defined by the Internet Engineering Task Force (IETF) that is used for creating, modifying, and terminating multimedia sessions with multiple participants.

## 1.3 Compliant Targets of Evaluation

---

This ~~PP-Module~~ specifically addresses SBCs that provide firewalling, interoperability, and security functions for ~~VVoIP~~ networks. The SBC also provides protected communication between trusted components of the network infrastructure.

The physical boundary of the SBC is defined by the operating system components storing or providing security functions and all software supplied by the vendor, including vendor modified components to the operating system. All the security functionality is contained and executed within the physical boundary of the device.

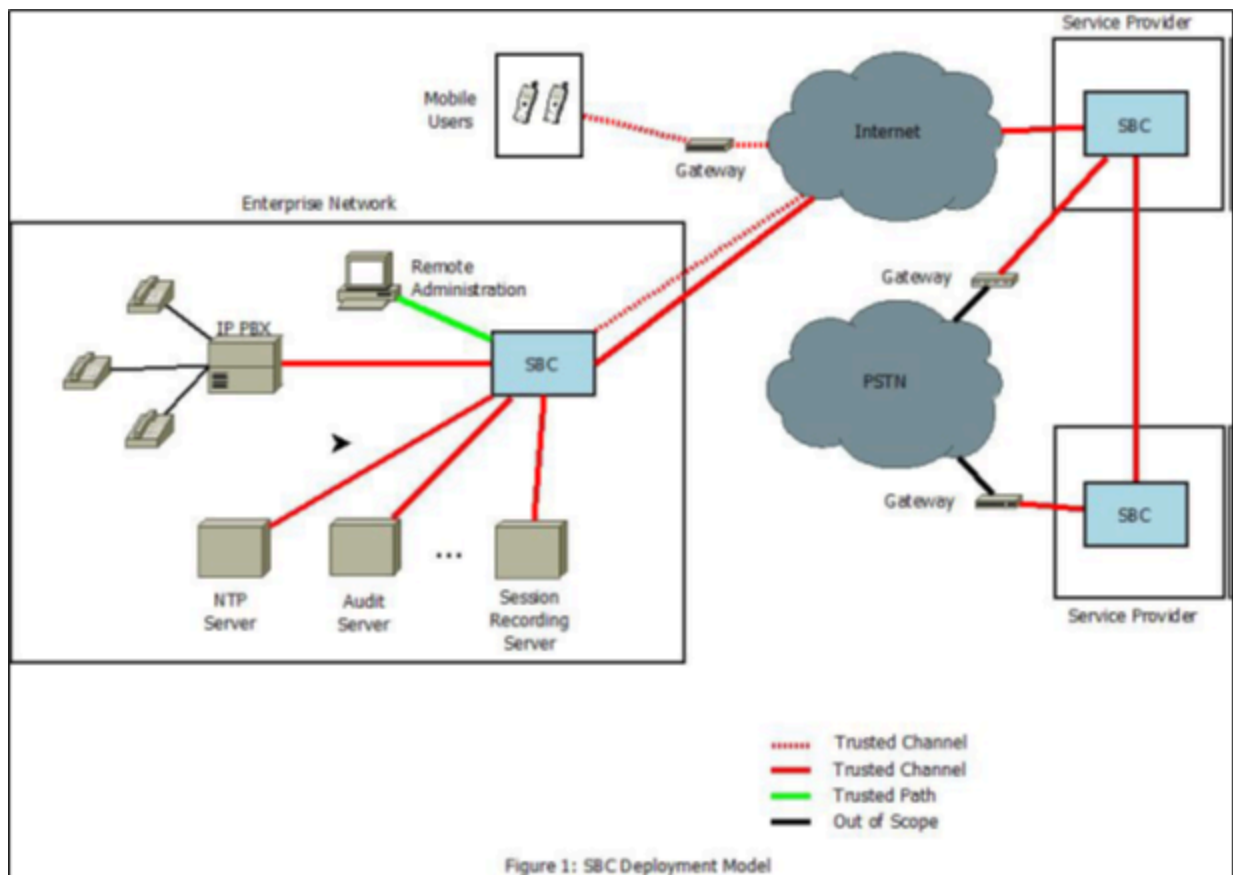
While the functionality that the ~~TOE~~ is obligated to implement in response to the described threat environment is detailed in later sections, a brief description is provided here. A compliant ~~TOE~~ will provide security functionality that addresses threats to itself. It must also protect communications between itself and an Internet Protocol Public Branch Exchange (~~IP-PBX~~) or another SBC by using a trusted channel. Some protocols required by this ~~PP-Module~~ make use of certificates; therefore, the SBC must securely store certificates and private keys.

Since this ~~PP-Module~~ builds on the NDcPP, conformant ~~TOEs~~ must implement the functionality required in the NDcPP along with the additional functionality defined in this ~~PP-Module~~ in response to the threat environment discussed later in this document.

### 1.3.1 TOE Boundary

An SBC is a security device composed of hardware and software connected to two or more distinct voice networks that provides security and interoperability functions. SBCs are deployed between peering service provider networks, service provider networks and enterprise networks, service provider networks and residential customers, or in some cases as a back-to-back user agent (~~B2BUA~~) that allows mobile users the ability to connect to their internal ~~VVoIP~~ network.

The following diagram represents a typical deployment of the ~~TOE~~ and its operational environment (~~OE~~). Note that the ~~TOE~~ boundary is limited to the physical boundary of the SBC device itself, and the trusted channels/paths that are established by the SBC.



**Figure 1: SBC Deployment Model**

## 1.4 Use Cases

This PP-Module defines a single potential use case for the SBC TOE:

### [USE CASE 1] Border Protection

The TOE is a specialized network device that provides firewall services for VoIP networks. The TOE is intended to provide protection against well-known threats that target these networks. The SBC examines headers and data values of packets and compares them to an Access Control List (ACL) to either permit or deny them to or through the SBC. The SBC is typically deployed between service providers for security, interoperability, translation, and transcoding purposes; between service providers and residential customers for security and interoperability purposes; or between service providers and enterprise networks for translation, transcoding, and security purposes. The SBC, as a border element, should also be able to establish a secure communication channel with external devices it communicates with.

## 1.5 Package Usage

This section contains selections and assignments that are required when the listed Functional Packages are claimed by this PP-Module.

Package Usage guidance defined in the TOE's relevant Base-PP applies to the usage of the packages for this module, unless explicitly stated otherwise in this section.

### Functional Package for X.509, Version 1.0

#### Certificate Verification and Assertion Required in FIA\_XCU\_EXT.1.1

Because this PP-Module mandates support for mutual authentication for ESC communications, the ST author shall select the options to both verify and assert certificate identities in FIA\_XCU\_EXT.1.1.

### **Limitations on Signature Algorithms in FIA\_X509\_EXT.1.1**

The **T.O.E** must utilize appropriate cryptographic algorithms that conform to CNSA standards. Thus, the **T.O.E** shall utilize no other algorithms outside of those specified in RFC 8603 for certificate or CRL signatures. Additionally, the **T.O.E** shall not use ECDSA with SHA-512 signatures for OCSP responses, and shall utilize no other algorithms for OCSP responses.

### **Required Extension Processing for FIA\_X509\_EXT.1.2**

The **S.T** author shall select the options to process the basicConstraints and extendedKeyUsage extensions. Other extensions may be selected as appropriate without restriction.

### **CRL or OCSP-based Revocation Required for FIA\_X509\_EXT.1.3**

The **T.O.E** must support revocation that only involves CRL or OCSP. Accordingly, the **T.O.E** shall select only from options involving CRL or OCSP in FIA\_X509\_EXT.1.3 (e.g., the selection to treat all certificates older than a given short timeframe is not an acceptable substitute or alternative for supporting CRL or OCSP).

### **Connections to CRL or OCSP Servers Required for FIA\_X509\_EXT.1.4**

Because the **T.O.E** is required to support CRL or OCSP, the **T.S.F** shall support an appropriate mechanism for obtaining revocation status information. In the case of CRL, the **S.T** author shall claim that revocation status information is obtained via network connection to a CRL distribution point. In the case of OCSP, the **S.T** author shall claim that revocation status information is obtained via network connection to an OCSP responder, via OCSP stapling, or via OCSP multi-stapling.

### **Restrictions on Acceptable Key Usage Values for FIA\_X509\_EXT.1.5**

The **T.O.E** will always support the use of extendedKeyUsage values to verify that X.509 certificates are used in accordance with their intended purpose. Accordingly, the **S.T** author shall claim that the **T.O.E** supports the processing of extendedKeyUsage fields in the leaf certificate (as opposed to application of trust store context rules or passing the certification path or other supported context information to an external function) and shall select all values that are relevant to the claimed uses of X.509 in the **S.T**. In particular, since the **P.P** does not define any functions that require the use of S/MIME, the **S.T** author shall not select this as an extendedKeyUsage value to be validated.

### **Requirements on Functions for FIA\_X509\_EXT.2.1**

The **S.T** author shall ensure that the selections and assignments in this requirement reflect the **T.O.E**'s usage of X.509 certificate validation for TLS. Other assignments and selections may be made as applicable for other **T.O.E** functions.

## **Functional Package for Transport Layer Security (TLS), Version 2.1**

### **DTLS or TLS Server and Client Functionality Required**

The **S.T** author shall select the option to utilize TLS as both a server and client. The **S.T** author shall additionally select the option to utilize DTLS as a server and client if support for DTLS is claimed in [FTP\\_ITC.1/ESC](#).

### **DTLS or TLS Mutual Authentication Required**

The **S.T** shall select the option to support mutual authentication in FCS\_TLSC\_EXT.1 and FCS\_TLSS\_EXT.1, or FCS\_DTLSC\_EXT.1 and FCS\_DTLSS\_EXT.1, according with the protocol support claimed in [FTP\\_ITC.1/ESC](#).

# 2 Conformance Claims

## Conformance Statement

An ST must claim exact conformance to this PP-Module.

The evaluation methods used for evaluating the TOE are a combination of the workunits defined in [\[CEM\]](#) as well as the Evaluation Activities for ensuring that individual SFRs and SARs have a sufficient level of supporting evidence in the Security Target and guidance documentation and have been sufficiently tested by the laboratory as part of completing ATE\_IND.1. Any functional packages this PP claims similarly contain their own Evaluation Activities that are used in this same manner.

## CC Conformance Claims

This PP-Module is conformant to Part 2 (extended) and Part 3 (conformant) of Common Criteria CC:2022, Revision 1.

## PP Claim

This PP-Module does not claim conformance to any Protection Profile.

The following PPs and PP-Modules are allowed to be specified in a PP-Configuration with this PP-Module:

- Network Device collaborative Protection Profile Version 4.0

## Package Claim

- This PP-Module is Functional Package for TLS, version 2.1 conformant.
- This PP-Module is Functional Package for X.509, version 1.0 conformant.
- This PP-Module does not conform to any assurance packages.

The functional packages to which the PP conforms may include SFRs that are not mandatory to claim for the sake of conformance. An ST that claims one or more of these functional packages may include any non-mandatory SFRs that are appropriate to claim based on the capabilities of the TSE and on any triggers for their inclusion based inherently on the SFR selections made.

# 3 Security Problem Definition

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.

## 3.1 Threats

---

The following threats that are defined in this **PP-Module** extend the threats that are defined by the **Base-PP**.

### **T.MALICIOUS\_TRAFFIC**

An attacker may attempt to send malformed packets to the SBC to cause the network stack or services listening on TCP/UDP ports on the SBC or protected network to crash.

### **T.NETWORK\_ACCESS**

An attacker may send traffic through the **.TOE** that enables them to access devices in the **.TOE**'s **OE** without authorization.

### **T.RESOURCE\_EXHAUSTION**

An attacker may transmit network traffic to the **.TOE** that causes it to be unable to perform its functions on legitimate network traffic.

### **T.UNTRUSTED\_COMMUNICATION\_CHANNELS**

An attacker may acquire sensitive **.TOE** or user data that is transmitted to or from the **.TOE** because an untrusted communication channel causes a disclosure of data in transit.

### **T.USER\_DATA\_REUSE**

User data may be inadvertently sent to a destination not intended by the original sender, causing an unauthorized disclosure of the data.

## 3.2 Assumptions

---

This **PP** defines no Assumptions beyond those defined in the claimed **Base-PP(s)**.

All assumptions for the **OE** of the **Base-PP** also apply to this **PP-Module**.

**A.NO\_THRU\_TRAFFIC\_PROTECTION** is still operative, but only for the interfaces in the **.TOE** that are defined by the **Base-PP** and not the **PP-Module**.

## 3.3 Organizational Security Policies

---

This **PP** defines no Organizational Security Policies beyond those defined in the claimed **Base-PP(s)**.

# 4 Security Objectives

## 4.1 Security Objectives for the Operational Environment

---

All objectives for the OE of the Base-PP also apply to this PP-Module. OE.NO\_THRU\_TRAFFIC\_PROTECTION is still operative, but only for the interfaces in the TOE that are defined by the Base-PP and not the PP-Module.

# 5 Security Requirements

This chapter describes the security requirements which have to be fulfilled by the product under evaluation. Those requirements comprise functional components from Part 2 and assurance components from Part 3 of [CC]. The following conventions are used for the completion of operations:

- **Refinement** operation (denoted by **bold text** or ~~strikethrough text~~): Is used to add details to a requirement or to remove part of the requirement that is made irrelevant through the completion of another operation, 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: Is indicated by appending the SFR name with a slash and unique identifier suggesting the purpose of the operation, e.g. "/EXAMPLE1."

## 5.1 Collaborative Protection Profile for Network Devices Security Functional Requirements Direction

---

In a PP-Configuration that includes the NDcPP, the TOE is expected to rely on some of the security functions implemented by the Network Device as a whole and evaluated against the NDcPP. The following sections describe any modifications that the ST author must make to the SFRs defined in the NDcPP in addition to what is mandated by [Section 5.2 TOE Security Functional Requirements](#).

### 5.1.1 Modified SFRs

The SFRs listed in this section are defined in the NDcPP and relevant to the secure operation of the TOE.

#### 5.1.1.1 Trusted Path/Channels (FTP)

##### FTP\_ITC.1: Inter-TSF Trusted Channel

This SFR has been modified to mandate the use of TLS for inter-TSF trusted channels in the TOE. Any element not mentioned in this section is unchanged from its original definition.

The text of FTP\_ITC.1.1 is replaced with:

**FTP\_ITC.1.1** The TSF shall be capable of using **TLS as defined in the Functional Package for TLS and [selection: IPsec, SSH as defined in the Functional Package for SSH, DTLS as defined in the Functional Package for TLS, HTTPS, no other protocol ]** to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: audit server, **[selection: authentication server, [assignment: other capabilities], no other capabilities]** that is logically distinct from other communication channels and provides assured identification of its endpoints and protection of the channel data from disclosure and detection of modification of the channel data.

**FTP\_ITC.1.2:** The TSF shall permit [*the TSF, the authorized IT entities*] to initiate communication via the trusted channel.

**Application Note:** TLS is mandated for SIP trunking as required by [FIA\\_SIPT\\_EXT.1](#).

## 5.2 TOE Security Functional Requirements

The following section describes the SFRs that must be satisfied by any TOE that claims conformance to this PP-Module. These SFRs must be claimed regardless of which PP-Configuration is used to define the TOE.

### 5.2.1 Auditable Events for Mandatory SFRs

**Table 1: Auditable Events for Mandatory Requirements**

Requirement	Auditable Events	Additional Audit Record Contents
FAU_ARP_EXT.1	No events specified	N/A
FAU_GEN.1/SBC	No events specified	N/A
FAU_SAA.1	No events specified	N/A
FAU_SEL.1	No events specified	N/A
FCS_SRTP_EXT.1	No events specified	N/A
FDP_IFC.1	No events specified	N/A
FDP_IFF.1	Any modifications to the B2BUA policy.	No additional information.
FFW_ACL_EXT.1	Application of traffic filtering rules.	<ul style="list-style-type: none"> <li>• Source and destination of observed traffic.</li> <li>• Rule relevant to observed traffic.</li> <li>• Result of rule evaluation.</li> </ul>
FFW_ACL_EXT.2	Application of traffic filtering rules.	<ul style="list-style-type: none"> <li>• Source and destination of observed traffic.</li> <li>• Rule relevant to observed traffic.</li> <li>• Result of rule evaluation.</li> </ul>
FFW_DPI_EXT.1	Application of deep packet inspection rules.	<ul style="list-style-type: none"> <li>• Source and destination of observed traffic.</li> <li>• Rule relevant to observed traffic.</li> <li>• Result of rule evaluation.</li> </ul>
FFW_NAT_EXT.1	No events specified	N/A
FIA_SIPT_EXT.1	All SIP trunk authentication attempts.	Username and IP address of the service provider.
FMT_SMF.1/SBC	All management actions.	Identifier of initiator.
FRU_PRS_EXT.1	No events specified	N/A
FRU_RSA.1	No events specified	N/A
FTP_ITC.1/ARP	Initiation of the trusted channel.	Identification of the initiator and target of the trusted channel.

	Termination of the trusted channel.	Identification of the initiator and target of the trusted channel.
	Failure of the trusted channel functions.	Identification of the initiator and target of the trusted channel.
FTP_ITC.1/ESC	Initiation of the trusted channel.	Identification of the initiator and target of the trusted channel.
	Termination of the trusted channel.	Identification of the initiator and target of the trusted channel.
	Failure of the trusted channel functions.	Identification of the initiator and target of the trusted channel.
FTP_ITC.1/VVoIP	Initiation of the trusted channel.	Identification of the initiator and target of the trusted channel.
	Termination of the trusted channel.	Identification of the initiator and target of the trusted channel.
	Failure of the trusted channel functions.	Identification of the initiator and target of the trusted channel.

## 5.2.2 Security Audit (FAU)

### FAU\_ARP\_EXT.1 Security Audit Automatic Response

#### FAU\_ARP\_EXT.1.1

The TSSF shall be capable of using [**selection:** *TLS, IPsec, SSH, HTTPS, SNMPv3*] to transmit potential security violations to an external IT entity in the OE upon detection.

**Application Note:** The selected protocols must be reflected in FTP\_ITC.1.

### FAU\_GEN.1/SBC Audit Data Generation (Session Border Controller)

#### FAU\_GEN.1.1/SBC

The TSSF shall be able to generate audit data of the following auditable events:

- a. Start-up and shutdown of the audit functions;
- b. All auditable events for the [*not specified*] level of audit;
- c. [*All administrative actions*];
- d. *Specifically defined auditable events listed in the Auditable Events for Mandatory SFRs table (Table 1)*
- e. [**selection:** *Auditable events listed in the Auditable Events for Implementation-Dependent SFRs table (Table 5), Auditable events listed in the Auditable Events for Selection-Based SFRs table (Table 6), no other events*]

].

**Application Note:** The auditable events defined in the Auditable Events table are for the SFRs that are explicitly defined in this PP-Module. For any SFRs that are included as part of the TOE based on the claimed Base-PP, it is expected that any

applicable auditable events defined for those SFRs in the Base-PP are also claimed as part of the TSE.

The Base-PP iteration of the SFR also requires “all administrative actions” to be audited. When the TOE includes this PP-Module, it is expected that this will also include the administrative actions that support the PP-Module defined in [FMT\\_SMF.1/SBC](#).

If the ST includes any implementation-dependent or selection-based SFRs, the selection for "Auditable events listed in the Auditable Events for Implementation-Dependent SFRs table" or "Auditable events listed in the Auditable Events for Selection-Based SFRs table" must be made, respectively. If no implementation-dependent or selection-based SFRs are included, "no other events" should be selected. The auditing of each implementation-dependent or selection-based SFR is only required if that SFR is included in the ST.

A CDR is expected to be generated at the start of a session, at the end of a session, and during a session at an interval or time period specified by the ST author.

#### FAU\_GEN.1.2/SBC

The TSE shall record within the audit data at least the following information:

- a. Date and time of the auditable event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event;
- b. For each auditable event type, based on the auditable event definitions of the functional components included in the PP, PP-Module, functional package, or ST, [*information specified in column three of the Auditable Events table in which the auditable event was defined*].

### FAU\_SAA.1 Potential Violation Analysis

#### FAU\_SAA.1.1

The TSE shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

#### FAU\_SAA.1.2

The TSE shall enforce the following rules for monitoring audited events:

- a. Accumulation or combination of [**assignment:** *subset of defined auditable events*] known to indicate a potential security violation;
- b. [**assignment:** *any other rules*].

**Application Note:** Examples of monitored audited events include authentication failures, self-test failures, or environmental failures (e.g., temperature violation).

### FAU\_SEL.1 Selective Audit

#### FAU\_SEL.1.1

The TSE 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. [*event type*]
- b. [**assignment:** *list of additional attributes that audit selectivity is based upon*]

**Application Note:** The auditable events associated with traffic filtering rules (see the [FFW\\_ACL\\_EXT.2](#) and [FFW\\_DPI\\_EXT.1](#) rows in [Table 1](#) above) may generate a significant volume of traffic that make them impractical to generate on a persistent

basis. The ~~TOE~~ must have the ability to generate these records when necessary but this ~~SFR~~ exists to allow for the generation of those events to be suppressed when the ~~TOE~~ is in its evaluated configuration.

## 5.2.3 Cryptographic Support (FCS)

### FCS\_SRTP\_EXT.1 Secure Real-Time Transport Protocol

#### FCS\_SRTP\_EXT.1.1

The ~~TSE~~ shall implement the Secure Real-Time Transport Protocol (SRTP) that complies with RFC 3711, and use Security Descriptions for Media Streams (SDS) in compliance with RFC 4568 to provide key information for the ~~SRTP~~ connection.

#### FCS\_SRTP\_EXT.1.2

The ~~TSE~~ shall implement SDS-SRTP supporting the following ciphersuites: [AEAD\_AES\_256\_GCM, in accordance with RFC 7714].

**Application Note:** This requirement specifies that the ~~SRTP~~ session that will be used to carry the ~~VoIP~~ traffic will be keyed according to an SDS dialog using one of the identified ciphersuites. The ~~ST~~ author should select all ciphersuites that are supported.

#### FCS\_SRTP\_EXT.1.3

The ~~TSE~~ shall ensure the ~~SRTP~~ NULL algorithm [**selection:** *is disabled, can be disabled by a [security administrator]*].

#### FCS\_SRTP\_EXT.1.4

The ~~TSE~~ shall allow the ~~SRTP~~ ports to be used for ~~SRTP~~ communications to be specified by a [security administrator].

## 5.2.4 User Data Protection (FDP)

### FDP\_IFC.1 Subset Information Flow Control

#### FDP\_IFC.1.1

The ~~TSE~~ shall enforce the [B2BUA policy] on [caller-callee pairs attempting to communicate through the ~~TOE~~].

### FDP\_IFF.1 Simple Security Attributes

#### FDP\_IFF.1.1

The ~~TSE~~ shall enforce the [B2BUA policy] based on the following types of subject and information security attributes: [**assignment:** *method by which the ~~TSE~~ identifies each endpoint for a call*].

#### FDP\_IFF.1.2

The ~~TSE~~ 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 ~~TSE~~ will establish a connection between itself and the caller; the ~~TSE~~ will establish a second connection between itself and the callee; and the ~~TSE~~ will redirect all communications that it receives between the two endpoints out through the proper connection].

#### FDP\_IFF.1.3

The TSE shall enforce the [following configurable behavioral rules: **[selection:**

- *Default-deny (allowlist) posture: If configured, the TSE will implicitly deny all information flows except for those explicitly authorized by the TSE.*
- *Default-allow (denylist) posture: If configured, the TSE will implicitly allow all information flows except for those explicitly denied by the TSE.*

]].

FDP\_IFF.1.4

The TSE shall explicitly authorize an information flow based on the following rules: [if the TSE is operating in an allowlist posture, any calling parties that are present on the allowlist (identifiable by calling number, source IP address, or communications protocols) are explicitly authorized].

FDP\_IFF.1.5

The TSE shall explicitly deny an information flow based on the following rules: [if the TSE is operating in a denylist posture, any calling parties that are present on the denylist (identifiable by calling number or source IP address, or communications protocols) are explicitly denied].

## 5.2.5 Firewall (FFW)

### FFW\_ACL\_EXT.1 Real-Time Communications Traffic Filtering

FFW\_ACL\_EXT.1.1

The TSE shall perform traffic filtering on network packets processed by the TOE.

FFW\_ACL\_EXT.1.2

The TSE shall allow the definition of traffic filtering for real-time communications traffic using the following network protocol fields:

- IPv4
  - source address
  - destination address
  - transport layer protocol
- IPv6
  - source address
  - destination address
  - transport layer protocol
- **TCP (for signaling channel)**
  - source port
  - destination port
- **UDP (for signaling channel)**
  - source port
  - destination port
- **Distinct Interface (physical versus virtual or trust zone, e.g., trusted versus untrusted)**
- [Application (Real-Time Communications Protocol)
  - signaling protocols: **[selection: SIP, H.323]**

**Application Note:** Real-time communications traffic can use multiple transport protocols and ports. Therefore, traffic filtering rules should be defined using the network protocol fields above, and one type of traffic may require multiple rules to

be applied. If “H.323” is selected in this requirement, the ST must include the selection-based SFR [FTP\\_ITC.1/H323](#).

#### FFW\_ACL\_EXT.1.3

The TSE shall allow the following operations to be associated with traffic filtering rules: permit or drop with the capability to log the operation **for each specific rule defined**.

**Application Note:** Whether or not logging is performed may be applied to individual rules or groups of rules on an independent basis. For example, if there are six rules defined, the TOE should allow for any subset of these rules to be logged, independent of one another.

#### FFW\_ACL\_EXT.1.4

The TSE shall allow the traffic filtering rules to be assigned to each distinct network interface.

#### FFW\_ACL\_EXT.1.5

The TSE shall:

- Accept a network packet without further processing of traffic filtering rules if it matches an allowed established session for the following protocols: TCP, UDP, based on the following network packet attributes:
  - TCP: source and destination addresses, source and destination ports, sequence number, flags
  - UDP: source and destination addresses, source and destination ports
- Remove existing traffic flows from the set of established traffic flows based on the following: [**selection:** *session inactivity timeout, completion of the expected information flow*].

#### FFW\_ACL\_EXT.1.6

The TSE shall process the applicable traffic filtering rules in an administratively defined order.

#### FFW\_ACL\_EXT.1.7

The TSE shall deny packet flow if a matching rule is not identified.

### FFW\_ACL\_EXT.2 Stateful VVoIP Traffic Filtering

#### FFW\_ACL\_EXT.2.1

The TSE shall perform stateful traffic filtering on the following VVoIP protocols: [**selection:** SIP, H.323 (H.225, H.245), MGCP].

**Application Note:** If “H.323” is selected in this requirement, the ST must include the selection-based SFR [FTP\\_ITC.1/H323](#).

#### FFW\_ACL\_EXT.2.2

The TSE shall enforce the following default stateful traffic filtering rules on all network traffic matching protocol types identified in [FFW\\_ACL\\_EXT.2.1](#):

[**selection:**

- SIP traffic where a BYE message precedes an INVITE message
- H.225 traffic where an RCF reply precedes any other traffic
- H.245 traffic where a ResponseMessage precedes a RequestMessage
- MGCP traffic where a DLCX message precedes a CRCX message

].

**Application Note:** The stateful traffic filtering rules selected in [FFW\\_ACL\\_EXT.2.2](#) must match the selections made for [VoIP](#) protocols in [FFW\\_ACL\\_EXT.2.1](#).

#### FFW\_ACL\_EXT.2.3

The [TSF](#) shall terminate any connection found to be in violation of the default stateful traffic filtering rules and provide the ability to generate an audit record of the event.

**Application Note:** Due to the potential for an SBC to receive large amounts of traffic that gets filtered by the default stateful traffic filtering rules, this [PP.Module](#) only requires that the [TSF](#) have the ability to generate audit records for all events. “Configure traffic filtering rules” in [FMT\\_SMF.1/SBC](#) provides an expectation that the administrator can determine which rules cause audit records to be generated so that the environment is not producing an excessively large volume of audit data.

#### FFW\_ACL\_EXT.2.4

The [TSF](#) shall dynamically open media ports to [VoIP](#) protocol traffic upon negotiation of a session and close these ports upon termination of a session.

#### FFW\_ACL\_EXT.2.5

The [TSF](#) shall not define a static range of ports to remain open indefinitely for the purpose of allowing [VoIP](#) protocol traffic.

### FFW\_DPI\_EXT.1 Deep Packet Inspection

#### FFW\_DPI\_EXT.1.1

The [TSF](#) shall implement [DPI](#) for the following protocols: [**selection:** [H.323](#) ([H.225](#), [H.245](#)), [SIP](#), [RTP](#), [RTCP](#)].

**Application Note:** If “H.323” is selected in this requirement, the [STI](#) must include the selection-based [SFR](#) [FTP\\_ITC.1/H323](#).

#### FFW\_DPI\_EXT.1.2

The [TSF](#) shall enforce the following rules for [DPI](#): [**assignment:** *for each protocol listed in [FFW\\_DPI\\_EXT.1.1](#), list elements of the packet data that are examined for potentially malicious content or compatibility with the protocol definition*].

#### FFW\_DPI\_EXT.1.3

When traffic is found to be in violation of a [DPI](#) rule, the [TSF](#) shall take the following action: [**selection:** *drop the traffic, generate an audit record, generate an alarm*].

### FFW\_NAT\_EXT.1 Topology Hiding/NAT Traversal

#### FFW\_NAT\_EXT.1.1

The [TSF](#) shall support [NAT](#) of signaling and media channel traffic through the [TOE](#) that is mediated by the [[B2BUA policy](#)] defined by [FDP\\_IFC.1](#).

#### FFW\_NAT\_EXT.1.2

The [TSF](#) shall support [NAT](#) for the following protocols: [**selection:** [SIP](#), [SIP-TLS](#), [H.225](#), [H.245](#)].

#### FFW\_NAT\_EXT.1.3

The [TSF](#) shall use [NAT](#) to replace the IP address header value of traffic originating from the internal network with [**selection:** *the IP address of the [TOE](#), a [security administrator]-defined value*].

#### FFW\_NAT\_EXT.1.4

The TSE shall maintain a NAT table to ensure that traffic bound for the internal network is directed to only the intended recipient.

### 5.2.6 Identification and Authentication (FIA)

#### FIA\_SIPT\_EXT.1 Session Initiation Protocol Trunking

##### FIA\_SIPT\_EXT.1.1

The TSE shall provide support for SIP trunking.

##### FIA\_SIPT\_EXT.1.2

The TSE shall require a service provider to provide valid identification in the form of a [selection: *username and password, X.509 certificate*] and IP address in order to establish a SIP trunk.

##### FIA\_SIPT\_EXT.1.3

The TSE shall require a service provider to provide a valid authentication credential in order to establish a SIP trunk.

##### FIA\_SIPT\_EXT.1.4

The TSE shall require a service provider to encrypt traffic using TLS in order to establish a SIP trunk.

### 5.2.7 Security Management (FMT)

#### FMT\_SMF.1/SBC Specification of Management Functions (SBC)

##### FMT\_SMF.1.1/SBC

The TSE shall be capable of performing the following management functions **related to SBC functionality**: [*Ability of a security administrator to:*

- *Change a user's password*
- *Require a user's password to be changed upon next login*
- *Configure the auditable events that will result in the generation of an alarm*
- *Configure the B2BUA policy*
- *Configure traffic filtering rules*
- *Configure auditable events*
- *Configure NAT*
- *Configure ports and cryptography for signaling and media communications*
- *Configure SIP communications*

].

**Application Note:** This SFR defines additional management functions for the TOE beyond what is defined in the Base-PP as FMT\_SMF.1. The TOE may have all management functionality implemented in the same logical interface; it is not necessary for “network device management” and “SBC management” to be implemented in separate interfaces.

This PP-Module may rely on management functionality defined in the Base-PP to support the implementation of its functions. For example, the SBC portion of the TOE relies on the reliable time function that must be implemented by the Base-PP portion of the TOE. If the Base-PP implements this using NTP, the “Ability to set the time which is used for time-stamps” or “Ability to configure NTP” management function defined in FMT\_SMF.1 in the Base-PP can be used to address this PP-Module’s dependency on reliable system time. Note that support for NTP is

recommended but not required.

The 'configurable auditable events' function relates to [FAU\\_SEL.1](#), specifically with respect to allowing a security administrator to determine whether a given event is auditable. As this refers to the events for the triggering of various filtering rules, it may be implicitly addressed through the 'configure traffic filtering rules' function, for example by explicitly defining a rule with a type that automatically requires it to be logged or a parameter that causes it to be logged if triggered.

## 5.2.8 Resource Utilization (FRU)

### FRU\_PRS\_EXT.1 Limited Priority of Service

#### FRU\_PRS\_EXT.1.1

The T.S.F shall assign a priority to each type of communications packet that traverses the T.S.F.

#### FRU\_PRS\_EXT.1.2

The T.S.F shall ensure that each access to network bandwidth shall be mediated on the basis of the subject's assigned priority.

### FRU\_RSA.1 Maximum Quotas

#### FRU\_RSA.1.1

The T.S.F shall enforce maximum quotas of the following resources: [CPU, memory, *assignment: other resources*], that [subjects] can use [*selection: simultaneously, over a specified period of time*].

**Application Note:** The intent of this S.F.R is for the T.O.F to be resistant to DDoS attacks.

## 5.2.9 Trusted Path/Channels (FTP)

### FTP\_ITC.1/ARP Inter-TSF Trusted Channel (Automatic Response)

#### FTP\_ITC.1.1/ARP

The T.S.F shall **be capable of using** [*selection: TLS, IPsec, SSH, DTLS, HTTPS, SNMPv3*] **to** provide a **trusted** communication channel between itself and **authorized IT entities supporting the following capabilities: security audit automatic response** that is logically distinct from other communication channels and provides assured identification of its endpoints and protection of the channel data from modification or disclosure.

#### FTP\_ITC.1.2/ARP

The T.S.F shall permit [*the T.S.F*] to initiate communication via the trusted channel.

#### FTP\_ITC.1.3/ARP

The T.S.F shall initiate communication via the trusted channel for [*transmission of potential security violations*].

**Application Note:** This S.F.R is used to specify any trusted protocols that are implemented in support of [FAU\\_ARP\\_EXT.1](#).

### FTP\_ITC.1/ESC Inter-TSF Trusted Channel (ESC Communications)

#### FTP\_ITC.1.1/ESC

The T.SF shall provide a **signaling** channel between itself and an E.SC using **TLS as specified in FCS\_TLSC\_EXT.1 and FCS\_TLSC\_EXT.2 and [selection: DTLS as specified in FCS\_DTLSC\_EXT.1 and FCS\_DTLSC\_EXT.2, no other protocol]** that is logically distinct from other communication channels and provides assured identification of its endpoints and protection of the channel data from modification or disclosure.

**Application Note:** FCS\_TLSC\_EXT.1, FCS\_TLSC\_EXT.2, FCS\_DTLSC\_EXT.1, and FCS\_DTLSC\_EXT.2 are defined in the .

FTP\_ITC.1.2/ESC

The T.SF shall permit [*the T.SF*] to initiate communication via the trusted channel.

FTP\_ITC.1.3/ESC

The T.SF shall initiate communication via the trusted channel for [*all communications with the E.SC*].

### FTP\_ITC.1/VVoIP Inter-TSF Trusted Channel (VVoIP Communications)

FTP\_ITC.1.1/VVoIP

The T.SF shall **be capable of using SRTP, [selection: SIP-TLS, IPsec, H.235, [assignment: other protocols]]** to provide a **trusted** communication channel between itself and **authorized IT entities supporting the following capabilities: VVoIP signaling and media channels** that is logically distinct from other communication channels and provides assured identification of its endpoints and protection of the channel data from modification or disclosure.

**Application Note:** FCS\_TLSC\_EXT.1, FCS\_TLSC\_EXT.2, FCS\_DTLSC\_EXT.1, and FCS\_DTLSC\_EXT.2 are defined in the .

FTP\_ITC.1.2/VVoIP

The T.SF shall permit [**selection: the T.SF, the authorized IT entities**] to initiate communication via the trusted channel.

FTP\_ITC.1.3/VVoIP

The T.SF shall initiate communication via the trusted channel for [**assignment: list of functions for which a trusted channel is required**].

## 5.3 TOE Security Functional Requirements Rationale

The following rationale provides justification for each S.F.R. for the T.O.E., showing that the S.F.R.s are suitable to address the specified threats:

**Table 2: S.F.R. Rationale**

Threat	Addressed by	Rationale
T.MALICIOUS_TRAFFIC	FAU_ARP_EXT.1	Mitigates the threat by defining the ability to generate security violations that are transmitted to external entities.
	FAU_GEN.1/SBC	Mitigates the threat by iterating a Base-PP requirement to define additional auditable events that are specific to SBC functionality.

	FAU_SAA.1	Mitigates the threat by defining a set of rules to monitor auditable events for potential security violations.
	FAU_SEL.1	Mitigates the threat by allowing for some monitoring functions to be selectively enabled and disabled as needed so that the generation of lower-priority audit records can be suppressed when it is not practical to generate those records for performance reasons.
	FTP_ITC.1/ARP	Mitigates the threat by defining the trusted channel used to securely communicate potential security violations.
T.NETWORK_ACCESS	FAU_ARP_EXT.1	Mitigates the threat by defining the ability to generate security violations that are transmitted to external entities.
	FAU_GEN.1/SBC	Mitigates the threat by iterating a Base-PP requirement to define additional auditable events that are specific to SBC functionality.
	FAU_SAA.1	Mitigates the threat by defining a set of rules to monitor auditable events for potential security violations.
	FAU_SEL.1	Mitigates the threat by allowing for some monitoring functions to be selectively enabled and disabled as needed so that the generation of lower-priority audit records can be suppressed when it is not practical to generate those records for performance reasons.
	FCS_SRTP_EXT.1	Mitigates the threat by defining the TOE's implementation of the SRTP protocol that is used to protect VoIP endpoint communications.
	FDP_IFC.1	Mitigates the threat by defining a B2BUA policy so that VoIP endpoints are only connected to each other through the TOE as an intermediary.
	FDP_IFF.1	Mitigates the threat by defining the specific rules that the B2BUA policy enforces.
	FFW_ACL_EXT.1	Mitigates the threat by defining capabilities for traffic filtering of network packets.
	FFW_ACL_EXT.2	Mitigates the threat by defining specific methods of stateful traffic inspection for specific protocols.
	FFW_DPI_EXT.1	Mitigates the threat by defining the capability to perform DPI for certain network traffic.
	FFW_NAT_EXT.1	Mitigates the threat by defining the use of NAT to obfuscate IP addresses of endpoint devices on the TOE's internal network.
	FIA_SIPT_EXT.1	Mitigates the threat by defining secure behavior for SIP trunking.

	FMT_SMF.1/SBC	Mitigates the threat by defining TSF management functions that require authorizations to use.
	FTP_ITC.1/ARP	Mitigates the threat by defining how communications of potential security violations are protected.
	FTP_ITC.1/ESC	Mitigates the threat by defining how communications with an external ESC are protected.
	FTP_ITC.1/H323 (selection-based)	Mitigates the threat by defining H.323 as a permitted method of protected communications for when a conformant TOE implements this logical interface.
	FTP_ITC.1/VVoIP	Mitigates the threat by defining how communications with an external VVoIP endpoint are protected.
T.RESOURCE_EXHAUSTION	FAU_ARP_EXT.1	Mitigates the threat by defining the ability to generate security violations that are transmitted to external entities.
	FAU_GEN.1/SBC	Mitigates the threat by iterating a Base-PP requirement to define additional auditable events that are specific to SBC functionality.
	FAU_SAA.1	Mitigates the threat by defining a set of rules to monitor auditable events for potential security violations.
	FAU_SEL.1	Mitigates the threat by allowing for some monitoring functions to be selectively enabled and disabled as needed so that the generation of lower-priority audit records can be suppressed when it is not practical to generate those records for performance reasons.
	FFW_ACL_EXT.1	Mitigates the threat by defining capabilities for traffic filtering of network packets.
	FFW_ACL_EXT.2	Mitigates the threat by defining specific methods of stateful traffic inspection for specific protocols.
	FFW_DPI_EXT.1	Mitigates the threat by defining the capability to perform DPI for certain network traffic.
	FMT_SMF.1/SBC	Mitigates the threat by defining TSF management functions that require authorizations to use.
	FRU_PRS_EXT.1	Mitigates the threat by requiring the TSF to implement priority of service to ensure that low-priority traffic cannot cause a DoS.
	FRU_RSA.1	Mitigates the threat by enforcing quotas for TSF resources to prevent DoS.
	FTP_ITC.1/ARP	Mitigates the threat by defining the trusted channel used to securely communicate potential security violations.

T.UNTRUSTED_ COMMUNICATION_ CHANNELS	FCS_SRTP_EXT.1	Mitigates the threat by defining the TOE's implementation of the SRTP protocol that is used to protect VVoIP endpoint communications.
	FIA_SIPT_EXT.1	Mitigates the threat by defining secure behavior for SIP trunking.
	FTP_ITC.1/ARP	Mitigates the threat by defining how communications of potential security violations are protected.
	FTP_ITC.1/ESC	Mitigates the threat by defining how communications with an external ESC are protected.
	FTP_ITC.1/H323 (selection-based)	Mitigates the threat by defining H.323 as a permitted method of protected communications for when a conformant TOE implements this logical interface.
	FTP_ITC.1/VVoIP	Mitigates the threat by defining how communications with an external VVoIP endpoint are protected.
T.USER_DATA_REUSE	FDP_IFC.1	Mitigates the threat by defining a B2BUA policy that is used by the TOE to establish connections between VVoIP endpoints.
	FDP_IFF.1	Mitigates the threat by defining the rules that the B2BUA policy enforces.
	FFW_NAT_EXT.1	Mitigates the threat by requiring the use of NAT to maintain a unique relationship between how external entities identify entities on the TOE's internal network and how they are actually addressed by that network.
	FIA_SIPS_EXT.1 (implementation- dependent)	Mitigates the threat by defining an optional capability to handle SIP registration in cases where the OE does not include an ESC that will provide that functionality.
	FIA_SIPT_EXT.1	Mitigates the threat by defining the use of SIP trunking, which requires authentication of endpoints to ensure data is only transmitted to the intended endpoint.

# 6 Consistency Rationale

## 6.1 Collaborative Protection Profile for Network Devices

---

### 6.1.1 Consistency of TOE Type

When this PP-Module is used to extend the NDcPP, the TOE type for the overall TOE is still a network device. The TOE boundary is simply extended to include SBC functionality that is provided by the network device.

### 6.1.2 Consistency of Security Problem Definition

Table 3: Consistency of Security Problem Definition (NDcPP base)

PP-Module Threat, Assumption, OSP	Consistency Rationale
T.MALICIOUS_TRAFFIC	The Base-PP does not define a threat for malicious traffic because all of its security-relevant external interfaces define the network device as the endpoint. This PP-Module defines interfaces where the TOE is facilitating a connection between two external entities, such that traffic between them will flow through the TOE as opposed to and from the TOE. This threat is consistent with the Base-PP because it is only applied to the interfaces defined in this PP-Module where it is relevant; it does not apply to the interfaces defined in the Base-PP.
T.NETWORK_ACCESS	The Base-PP does not define a threat for access to network resources because all of its security-relevant external interfaces define the network device as the endpoint. This PP-Module defines interfaces where the TOE is facilitating a connection between two external entities, such that traffic between them will flow through the TOE as opposed to into and out of the TOE. This threat is consistent with the Base-PP because it is only applied to the interfaces defined in this PP-Module where it is relevant; it does not apply to the interfaces defined in the Base-PP.
T.RESOURCE_EXHAUSTION	The threat of network traffic causing the TOE to be unable to perform its functions is similar to T.SECURITY_FUNCTIONALITY_FAILURE in the Base-PP because the intent of the threat is to cause the TSF to fail. The Base-PP does not define DoS protections because it does not define logical interfaces that are intended to process large volumes of network traffic. This PP-Module extends the threat by defining a specific example of it that applies to an SBC device that has this functionality.

**T.UNTRUSTED\_COMMUNICATION\_CHANNELS** The threat of disclosure of data in transit is fundamentally the same as the NDcPP threat with the same name. This PP-Module extends the threat to apply to the external interfaces that are defined specifically in support of SBC functions.

**T.USER\_DATA\_REUSE** The Base-PP does not define a threat of user data transmitted to the wrong destination because all of its security-relevant external interfaces define the network device as the endpoint. This PP-Module defines interfaces where the TOE is facilitating a connection between two external entities, such that traffic between them will flow through the TOE as opposed to and from the TOE. This threat is consistent with the Base-PP because it is only applied to the interfaces defined in this PP-Module where it is relevant; it does not apply to the interfaces defined in the Base-PP.

### 6.1.3 Consistency of OE Objectives

### 6.1.4 Consistency of Requirements

This PP-Module identifies several SFRs from the NDcPP that are needed to support Session Border Controller functionality. This is considered to be consistent because the functionality provided by the NDcPP is being used for its intended purpose. The rationale for why this does not conflict with the claims defined by the NDcPP are as follows:

**Table 4: Consistency of Requirements (NDcPP base)**

PP-Module Requirement	Consistency Rationale
<b>Modified SFRs</b>	
FTP_ITC.1	This PP-Module refines the Base-PP SFR to mandate the use of one of the trusted protocols defined by the Base-PP.
<b>Additional SFRs</b>	
This PP-Module does not add any requirements when the NDcPP is the base.	
<b>Mandatory SFRs</b>	
FAU_ARP_EXT.1	This SFR applies to the generation of alerts when a given auditable event is detected, which is beyond the original scope of the Base-PP.
FAU_GEN.1/SBC	This SFR is an iteration of a Base-PP requirement that defines additional auditable events for SBC functionality that the Base-PP could not be expected to cover.
FAU_SAA.1	This SFR applies to the detection of auditable events as potential security violations requiring the generation of alerts, which is beyond the original scope of the Base-PP.
FAU_SEL.1	This SFR applies to the behavior of the audit function with respect to the auditable events defined in this PP-Module. It does not affect the audit functions that apply to the Base-PP.

<a href="#">FCS_SRTP_EXT.1</a>	This <del>SFR</del> applies to the implementation of <del>SRTP</del> , which is a protocol that is not used for any <del>Base-PP</del> functionality.
<a href="#">FDP_IFC.1</a>	This <del>SFR</del> applies to the <del>TOE</del> 's implementation of a <del>B2BUA</del> policy, which applies to the <del>TOE</del> 's through-traffic interfaces and is therefore beyond the original scope of the <del>Base-PP</del> .
<a href="#">FDP_IFF.1</a>	This <del>SFR</del> applies to the <del>TOE</del> 's implementation of a <del>B2BUA</del> policy, which applies to the <del>TOE</del> 's through-traffic interfaces and is therefore beyond the original scope of the <del>Base-PP</del> .
<a href="#">FFW_ACL_EXT.1</a>	This <del>SFR</del> applies to traffic filtering, which applies to the <del>TOE</del> 's through-traffic interfaces and is therefore beyond the original scope of the <del>Base-PP</del> .
<a href="#">FFW_ACL_EXT.2</a>	This <del>SFR</del> applies to traffic filtering, which applies to the <del>TOE</del> 's through-traffic interfaces and is therefore beyond the original scope of the <del>Base-PP</del> .
<a href="#">FFW_DPI_EXT.1</a>	This <del>SFR</del> applies to <del>DPI</del> , which applies to the <del>TOE</del> 's through-traffic interfaces and is therefore beyond the original scope of the <del>Base-PP</del> .
<a href="#">FFW_NAT_EXT.1</a>	This <del>SFR</del> applies to <del>NAT</del> , which applies to the <del>TOE</del> 's through-traffic interfaces and is therefore beyond the original scope of the <del>Base-PP</del> .
<a href="#">FIA_SIPT_EXT.1</a>	This <del>SFR</del> applies to <del>SIP</del> trunking, which is a logical interface that is beyond the original scope of the <del>Base-PP</del> .
<a href="#">FMT_SMF.1/SBC</a>	This <del>SFR</del> is an iteration of a <del>Base-PP</del> requirement that defines additional management functions for SBC functionality that the <del>Base-PP</del> could not be expected to cover.
<a href="#">FRU_PRS_EXT.1</a>	This <del>SFR</del> applies to enforcement of bandwidth priority of service, which is a mechanism that is beyond the scope of the <del>Base-PP</del> and does not interfere with the ability of the <del>Base-PP</del> to process valid network traffic securely.
<a href="#">FRU_RSA.1</a>	This <del>SFR</del> applies to enforcement of resource quotas, which is a mechanism that is beyond the scope of the <del>Base-PP</del> and does not interfere with the ability of the <del>Base-PP</del> to process valid network traffic securely.
<a href="#">FTP_ITC.1/ARP</a>	This <del>SFR</del> is used to specify the trusted channel used for transmission of alerts as specified in <a href="#">FAU_ARP_EXT.1</a> .
<a href="#">FTP_ITC.1/ESC</a>	This <del>PP-Module</del> iterates an <del>SFR</del> defined in the <del>Base-PP</del> to define a new external interface for communications with an <del>ESC</del> . This does not interfere with the ability of the <del>Base-PP</del> to enforce its security functionality on the existing logical interfaces.
<a href="#">FTP_ITC.1/VVoIP</a>	This <del>PP-Module</del> iterates an <del>SFR</del> defined in the <del>Base-PP</del> to define a new external interface for communications with a <del>VVoIP</del> endpoint. This does not interfere with the ability of the <del>Base-PP</del> to enforce its security functionality on the existing logical interfaces.

### Optional ~~SFRs~~

This ~~PP-Module~~ does not define any Optional requirements.

### Objective ~~SFRs~~

This PP-Module does not define any Objective requirements.

### **Implementation-dependent SFRs**

[FIA\\_SIPS\\_EXT.1](#) This SFR applies to SIP registration, which is beyond the original scope of the Base-PP.

### **Selection-based SFRs**

[FTP\\_ITC.1/H323](#) This PP-Module iterates an SFR defined in the Base-PP to define a new external interface for communications using H.323. This does not interfere with the ability of the Base-PP to enforce its security functionality on the existing logical interfaces.

# Appendix A - Optional SFRs

## A.1 Strictly Optional Requirements

---

This PP-Module does not define any Strictly Optional SFRs or SARs.

## A.2 Objective Requirements

---

This PP-Module does not define any Objective SFRs.

## A.3 Implementation-dependent Requirements

---

### A.3.1 Auditable Events for Implementation-Dependent SFRs

Table 5: Auditable Events for Implementation-dependent Requirements

Requirement	Auditable Events	Additional Audit Record Contents
<a href="#">FIA_SIPS_EXT.1</a>	Call Detail Record (CDR).	<ul style="list-style-type: none"><li>• Calling party.</li><li>• Called party.</li><li>• Start time of the call.</li><li>• Call duration.</li><li>• Call type.</li></ul>

### A.3.2 Identification and Authentication (FIA)

#### FIA\_SIPS\_EXT.1 Session Initiation Protocol Registration

##### FIA\_SIPS\_EXT.1.1

The TSF shall implement the [selection: SIP that complies with RFC 3261, H.323 protocol that complies with ITU-REC H.235.0] using the Session Description Protocol (SDP) complying with RFC 4566 to describe the multimedia session that will be used to carry the VoIP traffic.

**Application Note:** If “H.323 protocol that complies with ITU-REC H.235.0” is selected in this requirement, the ST must include the selection-based SFR [FTP\\_ITC.1/H323](#).

##### FIA\_SIPS\_EXT.1.2

The TSF shall require password authentication for SIP REGISTER function requests as specified in Section 22 of RFC 3261.

##### FIA\_SIPS\_EXT.1.3

The TSF shall support ESC authentication passwords that contain at least [assignment: positive integer of eight or more] characters in the set of [upper case

characters, lower case characters, numbers, and the following special characters: "!", "@", "#", "\$", "%", "^", "&", "\*", "(", and ")", and [**assignment:** other supported special characters]].

#### FIA\_SIPS\_EXT.1.4

The TSSF shall provide the ability to modify SIP header values for SIP traffic received by the TOE prior to retransmitting the traffic.

**Application Note:** This SFR is optional because this functionality is not standard for SBCs because device registration can generally be handled by an ESC in the TOE's OE. However, in some cases, SIP registration directly to the SBC is required. If an SBC advertises this service, it is expected that this functionality be included within the TOE boundary. This SFR is therefore implementation-based on whether the SBC has the capability to perform its own SIP registration of devices.

# Appendix B - Selection-based Requirements

## B.1 Auditable Events for Selection-Based SFRs

Table 6: Auditable Events for Selection-based Requirements

Requirement	Auditable Events	Additional Audit Record Contents
FTP_ITC.1/H323	Failure of the trusted channel functions.	Identification of the initiator and target of the trusted channel.
	Initiation of the trusted channel.	Identification of the initiator and target of the trusted channel.
	Termination of the trusted channel.	Identification of the initiator and target of the trusted channel.

## B.2 Trusted Path/Channels (FTP)

### FTP\_ITC.1/H323 Inter-TSF Trusted Channel (H.323 Communications)

*The inclusion of this selection-based component depends upon selection in [FFW\\_ACL\\_EXT.1.2](#), [FFW\\_ACL\\_EXT.2.1](#), [FFW\\_DPI\\_EXT.1.1](#), [FIA\\_SIPS\\_EXT.1.1](#).*

#### FTP\_ITC.1.1/H323

The TSF shall provide a **n H.323** communication channel **in accordance with ITU-REC H.235.0** between itself and a **gatekeeper using TLS as specified in FCS\_TLSC\_EXT.1 and FCS\_TLSC\_EXT.2 and [selection: IPsec as specified in FCS\_IPSEC\_EXT.1, no other protocol]** that is logically distinct from other communication channels and provides assured identification of its endpoints and protection of the channel data from modification or disclosure.

**Application Note:** FCS\_IPSEC\_EXT.1 is defined in the Base-PP. FCS\_TLSC\_EXT.1 and FCS\_TLSC\_EXT.2 are defined in the .

#### FTP\_ITC.1.2/H323

The TSF shall permit [*the TSF*] to initiate communication via the trusted channel.

#### FTP\_ITC.1.3/H323

The TSF shall initiate communication via the trusted channel for [*all communications with the gatekeeper*].

**Application Note:** This SFR is claimed if H.323 is specified as being supported by the TOE in [FFW\\_ACL\\_EXT.1](#), [FFW\\_ACL\\_EXT.2](#), [FFW\\_DPI\\_EXT.1](#), or [FIA\\_SIPS\\_EXT.1](#).

# Appendix C - Extended Component Definitions

This appendix contains the definitions for all extended requirements specified in the PP-Module.

## C.1 Extended Components Table

---

All extended components specified in the PP-Module are listed in this table:

**Table 7: Extended Component Definitions**

Functional Class	Functional Components
Cryptographic Support (FCS)	FCS_SRTP_EXT Secure Real-Time Transport Protocol
Firewall (FFW)	FFW_ACL_EXT Traffic Filtering FFW_DPI_EXT Deep Packet Inspection FFW_NAT_EXT Network Address Translation
Identification and Authentication (FIA)	FIA_SIPS_EXT Session Initiation Protocol Registration FIA_SIPT_EXT Session Initiation Protocol Trunking
Resource Utilization (FRU)	FRU_PRS_EXT Limited Priority of Service
Security Audit (FAU)	FAU_ARP_EXT Security Audit Automatic Response

## C.2 Extended Component Definitions

---

### C.2.1 Cryptographic Support (FCS)

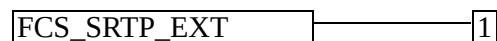
This PP-Module defines the following extended components as part of the FCS class originally defined by CC Part 2:

#### C.2.1.1 FCS\_SRTP\_EXT Secure Real-Time Transport Protocol

##### Family Behavior

This family defines requirements for the implementation of SRTP.

##### Component Leveling



[FCS\\_SRTP\\_EXT.1](#), Secure Real-Time Transport Protocol, requires the TSF to implement SRTP in accordance with specified standards, and for some of this functionality to be configurable.

**Management: FCS\_SRTP\_EXT.1**

The following actions could be considered for the management functions in FMT:

- Configuration of ports and cryptography for signaling communications.

### **Audit: FCS\_SRTP\_EXT.1**

There are no auditable events foreseen.

### **FCS\_SRTP\_EXT.1 Secure Real-Time Transport Protocol**

Hierarchical to: No other components.

Dependencies to: FMT\_SMR.1 Security Roles

FTP\_ITC.1 Inter-TSF Trusted Channel

#### **FCS\_SRTP\_EXT.1.1**

The TTSF shall implement the Secure Real-Time Transport Protocol (SRTP) that complies with RFC 3711, and use Security Descriptions for Media Streams (SDS) in compliance with RFC 4568 to provide key information for the SRTP connection.

#### **FCS\_SRTP\_EXT.1.2**

The TTSF shall implement SDS-SRTP supporting the following ciphersuites [**assignment:** *list of supported ciphersuites and the standard in which they are defined*].

#### **FCS\_SRTP\_EXT.1.3**

The TTSF shall ensure the SRTP NULL algorithm [**selection:** *is disabled, can be disabled by a [assignment: administrator role]*].

#### **FCS\_SRTP\_EXT.1.4**

The TTSF shall allow the SRTP ports to be used for SRTP communications to be specified by a [**assignment:** *administrator role*].

## **C.2.2 Firewall (FFW)**

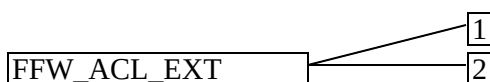
Firewall functionality involves selective processing of network traffic such that the traffic is routed or discarded based on some notion of whether the traffic is valid. Requirements in this class define capabilities for these processing functions.

### **C.2.2.1 FFW\_ACL\_EXT Traffic Filtering**

#### **Family Behavior**

This family defines requirements for controlling traffic filtering, including the use of stateful traffic filtering on protocols and ports.

#### **Component Leveling**



[FFW\\_ACL\\_EXT.1](#), Real-Time Communications Traffic Filtering, requires the TSE to implement traffic filtering rules based on network protocol attributes.

[FFW\\_ACL\\_EXT.2](#), Stateful VoIP Traffic Filtering, requires the TSE to perform stateful traffic filtering on traffic that matches certain unauthorized state conditions.

### **Management: FFW\_ACL\_EXT.1**

The following actions could be considered for the management functions in FMT:

- Configuration of traffic filtering rules.

### **Audit: FFW\_ACL\_EXT.1**

The following actions should be auditable if FAU\_GEN Security audit data generation is included in the PP/ST:

- Application of traffic filtering rules.

### **FFW\_ACL\_EXT.1 Real-Time Communications Traffic Filtering**

Hierarchical to: No other components.

Dependencies to: None

#### **FFW\_ACL\_EXT.1.1**

The TSE shall perform traffic filtering on network packets processed by the TOE.

#### **FFW\_ACL\_EXT.1.2**

The TSE shall allow the definition of traffic filtering for real-time communications traffic using the following network protocol fields:

- IPv4
  - source address
  - destination address
  - transport layer protocol
- IPv6
  - source address
  - destination address
  - transport layer protocol
- TCP
  - source port
  - destination port
- UDP
  - source port
  - destination port
- Distinct Interface
- [assignment: *other protocols or protocol types*]

#### **FFW\_ACL\_EXT.1.3**

The TSSF shall allow the following operations to be associated with traffic filtering rules: permit or drop with the capability to log the operation.

#### **FFW\_ACL\_EXT.1.4**

The TSSF shall allow the traffic filtering rules to be assigned to each distinct network interface.

#### **FFW\_ACL\_EXT.1.5**

The TSSF shall:

- Accept a network packet without further processing of traffic filtering rules if it matches an allowed established session for the following protocols: TCP, UDP, based on the following network packet attributes:
  - TCP: source and destination addresses, source and destination ports, sequence number, flags
  - UDP: source and destination addresses, source and destination ports
- Remove existing traffic flows from the set of established traffic flows based on the following: [**selection:** *session inactivity timeout, completion of the expected information flow*].

#### **FFW\_ACL\_EXT.1.6**

The TSSF shall process the applicable traffic filtering rules in an administratively defined order.

#### **FFW\_ACL\_EXT.1.7**

The TSSF shall deny packet flow if a matching rule is not identified.

#### **Management: FFW\_ACL\_EXT.2**

No specific management functions are identified.

#### **Audit: FFW\_ACL\_EXT.2**

The following actions should be auditable if FAU\_GEN Security audit data generation is included in the PP/ST:

- Application of traffic filtering rules.

#### **FFW\_ACL\_EXT.2 Stateful VVoIP Traffic Filtering**

Hierarchical to: No other components.

Dependencies to: None

#### **FFW\_ACL\_EXT.2.1**

The TSSF shall perform stateful traffic filtering on the following VVoIP protocols: [**assignment:** *VVoIP protocols*].

#### **FFW\_ACL\_EXT.2.2**

The TSSF shall enforce the following default stateful traffic filtering rules on all network traffic matching protocol types identified in [FFW\\_ACL\\_EXT.2.1](#):

- [**assignment:** *default stateful traffic filtering rules*]

#### **FFW\_ACL\_EXT.2.3**

The TSSF shall terminate any connection found to be in violation of the default stateful traffic filtering rules and provide the ability to generate an audit record of the event.

#### **FFW\_ACL\_EXT.2.4**

The TSSF shall dynamically open media ports to VVoIP protocol traffic upon negotiation of a session and close these ports upon termination of a session.

#### **FFW\_ACL\_EXT.2.5**

The TSSF shall not define a static range of ports to remain open indefinitely for the purpose of allowing VVoIP protocol traffic.

### **C.2.2.2 FFW\_DPI\_EXT Deep Packet Inspection**

#### **Family Behavior**

This family defines requirements for implementation of DPI functionality.

#### **Component Leveling**



[FFW\\_DPI\\_EXT.1](#), Deep Packet Inspection, defines traffic that the TSSF is expected to be able to perform DPI on, the specific elements of that traffic that is subject to DPI, and the action that is taken when invalid traffic is discovered by the DPI mechanism.

#### **Management: FFW\_DPI\_EXT.1**

No specific management functions are identified.

#### **Audit: FFW\_DPI\_EXT.1**

The following actions should be auditable if FAU\_GEN Security audit data generation is included in the PP/ST:

- Application of DPI rules.

#### **FFW\_DPI\_EXT.1 Deep Packet Inspection**

Hierarchical to: No other components.

Dependencies to: None

#### **FFW\_DPI\_EXT.1.1**

The TSSF shall implement DPI for the following protocols: [**assignment:** *communications protocols*].

#### **FFW\_DPI\_EXT.1.2**

The TSSF shall enforce the following rules for DPI: [**assignment:** *for each protocol listed in [FFW\\_DPI\\_EXT.1.1](#), list elements of the packet data that are examined for potentially malicious content or compatibility with the protocol definition*].

#### **FFW\_DPI\_EXT.1.3**

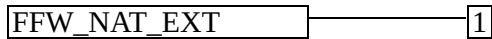
When traffic is found to be in violation of a DPI rule, the TSF shall take the following action: [**assignment:** *action taken in response to rule violation*].

### C.2.2.3 FFW\_NAT\_EXT Network Address Translation

#### Family Behavior

This family defines requirements for implementation of NAT.

#### Component Leveling



[FFW\\_NAT\\_EXT.1](#), Topology Hiding/NAT Traversal, requires the TSF to implement NAT for defined network protocols.

#### Management: FFW\_NAT\_EXT.1

The following actions could be considered for the management functions in FMT:

- Configuration of NAT.

#### Audit: FFW\_NAT\_EXT.1

There are no auditable events foreseen.

#### FFW\_NAT\_EXT.1 Topology Hiding/NAT Traversal

Hierarchical to: No other components.

Dependencies to: [FDP\\_IFC.1](#) Subset Information Flow Control  
FMT\_SMR.1 Security Roles

#### FFW\_NAT\_EXT.1.1

The TSF shall support NAT of signaling and media channel traffic through the TOE that is mediated by the [**assignment:** *information flow control policy*] defined by [FDP\\_IFC.1](#).

#### FFW\_NAT\_EXT.1.2

The TSF shall support NAT for the following protocols: [**assignment:** *list of protocols*].

#### FFW\_NAT\_EXT.1.3

The TSF shall use NAT to replace the IP address header value of traffic originating from the internal network with [**selection:** *the IP address of the TOE, a [**assignment:** *administrator role*]-defined value*].

#### FFW\_NAT\_EXT.1.4

The TSF shall maintain a NAT table to ensure that traffic bound for the internal network is directed to only the intended recipient.

### C.2.3 Identification and Authentication (FIA)

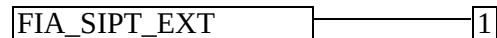
This PP-Module defines the following extended components as part of the FIA class originally defined by CC Part

### C.2.3.1 FIA\_SIPT\_EXT Session Initiation Protocol Trunking

#### Family Behavior

This family defines requirements for SIP validation, authentication, and traffic encryption.

#### Component Leveling



[FIA\\_SIPT\\_EXT.1](#), Session Initiation Protocol Trunking, requires the TSSF to implement SIP trunking using defined authentication and encryption methods.

#### Management: FIA\_SIPT\_EXT.1

The following actions could be considered for the management functions in FMT:

- Configuration of SIP communications.

#### Audit: FIA\_SIPT\_EXT.1

The following actions should be auditable if FAU\_GEN Security audit data generation is included in the PP/ST:

- All SIP trunk authentication attempts.

#### FIA\_SIPT\_EXT.1 Session Initiation Protocol Trunking

Hierarchical to: No other components.

Dependencies to: FCS\_TLSC\_EXT.1 TLS Client Protocol without Mutual Authentication  
 FCS\_TLSC\_EXT.2 TLS Client Support for Mutual Authentication  
 FCS\_TLSS\_EXT.1 TLS Server Protocol without Mutual Authentication  
 FCS\_TLSC\_EXT.2 TLS Server Support for Mutual Authentication  
 FTP\_ITC.1 Inter-TSF Trusted Channel

##### FIA\_SIPT\_EXT.1.1

The TSSF shall provide support for SIP trunking.

##### FIA\_SIPT\_EXT.1.2

The TSSF shall require a service provider to provide valid identification in the form of a [**selection:** *username and password, X.509 certificate*] and IP address in order to establish a SIP trunk.

##### FIA\_SIPT\_EXT.1.3

The TSSF shall require a service provider to provide a valid authentication credential in order to establish a SIP trunk.

##### FIA\_SIPT\_EXT.1.4

The TSE shall require a service provider to encrypt traffic using TLS in order to establish a SIP trunk.

## C.2.3.2 FIA\_SIPS\_EXT Session Initiation Protocol Registration

### Family Behavior

This family defines requirements for SIP registration.

### Component Leveling



**FIA\_SIPS\_EXT.1**, Session Initiation Protocol Registration, defines requirements for how the TSE must implement SIP registration, including protocol implementations and constraints on authentication.

### Management: FIA\_SIPS\_EXT.1

The following actions could be considered for the management functions in FMT:

- Configuration of SIP communications.

### Audit: FIA\_SIPS\_EXT.1

The following actions should be auditable if FAU\_GEN Security audit data generation is included in the PP/ST:

- Call Detail Record (CDR)

### FIA\_SIPS\_EXT.1 Session Initiation Protocol Registration

Hierarchical to: No other components.

Dependencies to: None

#### FIA\_SIPS\_EXT.1.1

The TSE shall implement the [**selection:** *SIP that complies with RFC 3261, H.323 protocol that complies with ITU-REC H.235.0*] using the Session Description Protocol (SDP) complying with RFC 4566 to describe the multimedia session that will be used to carry the VoIP traffic.

#### FIA\_SIPS\_EXT.1.2

The TSE shall require password authentication for SIP REGISTER function requests as specified in Section 22 of RFC 3261.

#### FIA\_SIPS\_EXT.1.3

The TSE shall support ESC authentication passwords that contain at least [**assignment:** *minimum numeric length*] characters in the set of [**assignment:** *supported character set*].

#### FIA\_SIPS\_EXT.1.4

The TSE shall provide the ability to modify SIP header values for SIP traffic received by the TOE prior to retransmitting the traffic.

## C.2.4 Resource Utilization (FRU)

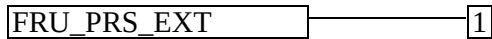
This PP-Module defines the following extended components as part of the FRU class originally defined by CC Part 2:

### C.2.4.1 FRU\_PRS\_EXT Limited Priority of Service

#### Family Behavior

This family defines requirements for prioritizing communication packets and bandwidth.

#### Component Leveling



**FRU\_PRS\_EXT.1**, Limited Priority of Service, requires the T<sub>TSF</sub> to implement mechanisms to limit the amount of network bandwidth that is available to subjects based on certain attributes.

#### Management: FRU\_PRS\_EXT.1

No specific management functions are identified.

#### Audit: FRU\_PRS\_EXT.1

There are no auditable events foreseen.

#### FRU\_PRS\_EXT.1 Limited Priority of Service

Hierarchical to: No other components.

Dependencies to: None

#### FRU\_PRS\_EXT.1.1

The T<sub>TSF</sub> shall assign a priority to each type of communications packet that traverses the T<sub>TSF</sub>.

#### FRU\_PRS\_EXT.1.2

The T<sub>TSF</sub> shall ensure that each access to network bandwidth shall be mediated on the basis of the subject's assigned priority.

### C.2.5 Security Audit (FAU)

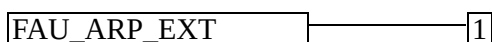
This PP-Module defines the following extended components as part of the FAU class originally defined by CC Part 2:

#### C.2.5.1 FAU\_ARP\_EXT Security Audit Automatic Response

#### Family Behavior

This family defines requirements for secure external transmission of detected security violations to the OE.

#### Component Leveling



[FAU\\_ARP\\_EXT.1](#), Security Audit Automatic Response, defines the mechanism used by the TSF to securely transmit security alerts to the OE.

**Management: FAU\_ARP\_EXT.1**

No specific management functions are identified.

**Audit: FAU\_ARP\_EXT.1**

There are no auditable events foreseen.

**FAU\_ARP\_EXT.1 Security Audit Automatic Response**

Hierarchical to: No other components.

Dependencies to: [FAU\\_SAA.1](#) Potential Violation Analysis  
FTP\_ITC.1 Inter-TSF Trusted Channel

**FAU\_ARP\_EXT.1.1**

The TSF shall be capable of using [**assignment:** *trusted channel defined in FTP\_ITC.1*] to transmit potential security violations to an external IT entity in the OE upon detection.

# Appendix D - Implicitly Satisfied Requirements

This appendix lists requirements that should be considered satisfied by products successfully evaluated against this PP-Module. These requirements are not featured explicitly as SERs and should not be included in the ST. They are not included as standalone SERs because it would increase the time, cost, and complexity of evaluation. This approach is permitted by [CC] Part 1, 8.3 Dependencies between components.

This information benefits systems engineering activities which call for inclusion of particular security controls. Evaluation against the PP-Module provides evidence that these controls are present and have been evaluated.

**Table 8: Implicitly Satisfied Requirements**

Requirement	Rationale for Satisfaction
<b>FMT_MSA.3 – Static Attribute Initialization</b>	<p data-bbox="354 747 1520 1031"><b>FDP_IFF.1</b> has a dependency on FMT_MSA.3 to define the default security posture of security attributes for the purpose of information flow control enforcement. This SER has not been defined by this PP-Module because the enforcement of <b>FDP_IFF.1</b> is not dependent on the initial state of security attributes. For example, <b>FDP_IFF.1.2</b> requires the TSE to determine if a communication attempt is valid before authorizing it. This is true regardless of whether the default value of security attributes associated with the connection attempt are permissive or restrictive; there is no difference in how the TSE determines “validity” in this case.</p> <p data-bbox="354 1056 1520 1268">The default values of security attributes do not cause the information flow control policy to behave differently for those rules that must always be enforced by the TSE. <b>FDP_IFF.1.4</b> requires that all allowlisted calling parties be authorized while all denylisted calling parties be rejected. It does not matter for the purpose of enforcing this SER whether the absence of a calling party from both the allowlist and the denylist means they are authorized or rejected by default.</p>

# Appendix E - Entropy Documentation and Assessment

The ~~TOE~~ does not require any additional supplementary information to describe its entropy sources beyond the requirements outlined in the ~~Base-PP~~.

# Appendix F - Allocation of Requirements in Distributed TOEs

For a distributed TOE, the SFRs in this PP-Module need to be met by the TOE as a whole, but not all SFRs will necessarily be implemented by all components. The following categories are defined in order to specify when each SFR must be implemented by a component:

- **All Components ("All"):** All components that comprise the distributed TOE must independently satisfy the requirement.
- **At least one Component ("One"):** This requirement must be fulfilled by at least one component within the distributed TOE.
- **Feature Dependent ("Feature Dependent"):** These requirements will only be fulfilled where the feature is implemented by the distributed TOE component (note that the requirement to meet the PP-Module as a whole requires that at least one component implements these requirements if they are claimed by the TOE).

The table below specifies how each of the SFRs in this PP-Module must be met, using the categories above.

Requirement	Description	Distributed TOE SFR Allocation
FAU_ARP_EXT.1	Security Audit Automatic Response	Feature Dependent
FAU_GEN.1/SBC	Audit Data Generation (Session Border Controller)	All
FAU_SAA.1	Potential Violation Analysis	Feature Dependent
FAU_SEL.1	Selective Audit	Feature Dependent
FCS_SRTP_EXT.1	Secure Real-Time Transport Protocol	Feature Dependent
FDP_IFC.1	Subset Information Flow Control	Feature Dependent
FDP_IFF.1	Simple Security Attributes	Feature Dependent
FFW_ACL_EXT.1	Real-Time Communications Traffic Filtering	Feature Dependent
FFW_ACL_EXT.2	Stateful VoIP Traffic Filtering	Feature Dependent
FFW_DPI_EXT.1	Deep Packet Inspection	Feature Dependent
FFW_NAT_EXT.1	Topology Hiding/NAT Traversal	Feature Dependent
FIA_SIPS_EXT.1 (implementation-based)	Session Initiation Protocol Registration	Feature Dependent
FIA_SIPT_EXT.1	Session Initiation Protocol Trunking	Feature Dependent

FMT_SMF.1/SBC	Specification of Management Functions (SBC)	Feature Dependent
FRU_PRS_EXT.1	Limited Priority of Service	Feature Dependent
FRU_RSA.1	Maximum Quotas	Feature Dependent
FTP_ITC.1/ESC	Inter-TSF Trusted Channel (ESC Communications)	Feature Dependent
FTP_ITC.1/H323 (selection-based)	Inter-TSF Trusted Channel (H.323 Communications)	Feature Dependent
FTP_ITC.1/VVoIP	Inter-TSF Trusted Channel (VVoIP Communications)	Feature Dependent

# Appendix G - Acronyms

**Table 9: Acronyms**

<b>Acronym</b>	<b>Meaning</b>
ACL	Access Control List
B2BUA	Back-To-Back User Agent
Base-PP	Base Protection Profile
CC	Common Criteria
CDR	Call Detail Record
CEM	Common Evaluation Methodology
cPP	Collaborative Protection Profile
DoS	Denial of Service
DPI	Deep Packet Inspection
ESC	Enterprise Session Controller
IP-PBX	Internet Protocol Public Branch Exchange
MGCP	Media Gateway Control Protocol
NAT	Network Address Translation
OE	Operational Environment
PP	Protection Profile
PP-Configuration	Protection Profile Configuration
PP-Module	Protection Profile Module
QoS	Quality of Service
RTCP	RTP Control Protocol
RTP	Real-Time Transport Protocol
SAR	Security Assurance Requirement
SDS	Security Descriptions for Media Streams
SDP	Session Description Protocol

<del>SFR</del>	Security Functional Requirement
<del>SIP</del>	Session Initiation Protocol
<del>SRTP</del>	Secure Real-Time Transport Protocol
<del>ST</del>	Security Target
<del>TOE</del>	Target of Evaluation
<del>TSE</del>	<del>TOE</del> Security Functionality
<del>TSEI</del>	<del>TSE</del> Interface
<del>TSS</del>	<del>TOE</del> Summary Specification
<del>VVoIP</del>	Voice/Video Over IP

# Appendix H - Bibliography

Table 10: Bibliography

Identifier	Title
[CC]	Common Criteria for Information Technology Security Evaluation - <ul style="list-style-type: none"><li>• <a href="#">Part 1: Introduction and general model</a>, CCMB-2022-11-001, CC:2022, Revision 1, November 2022.</li><li>• <a href="#">Part 2: Security functional requirements</a>, CCMB-2022-11-002, CC:2022, Revision 1, November 2022.</li><li>• <a href="#">Part 3: Security assurance requirements</a>, CCMB-2022-11-003, CC:2022, Revision 1, November 2022.</li><li>• <a href="#">Part 4: Framework for the specification of evaluation methods and activities</a>, CCMB-2022-11-004, CC:2022, Revision 1, November 2022.</li><li>• <a href="#">Part 5: Pre-defined packages of security requirements</a>, CCMB-2022-11-005, CC:2022, Revision 1, November 2022.</li></ul>
[GEM]	Common Methodology for Information Technology Security Evaluation - <ul style="list-style-type: none"><li>• <a href="#">Evaluation methodology</a>, CCMB-2022-11-006, CC:2022, Revision 1, November 2022.</li></ul>
[NDcPP]	<a href="#">collaborative Protection Profile for Network Devices, Version 4.0, December 22, 2025</a>