Comment: Comment-1-
Comment: Comment-2-
Comment: Comment-3-
Comment: Comment-4-

PP-Module for Session Border Controllers

Version: 1.0
2022-09-09
National Information Assurance Partnership

Revision History

Version	Date	Comment
1.0	2022-08-12	Initial Release

Contents

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:

- collaborative Protection Profile for Network Devices, Version 2.2e (NDcPP)

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.
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	A requirement for security enforcement by the TOE.

Functional Requirement (SFR)	
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 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 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 of 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.

1.4 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.

[JF] Note figure has known issues (blurry, figure title in actual image, duplicate trusted channel entry in key). Will need to re-make if editable version doesn't exist

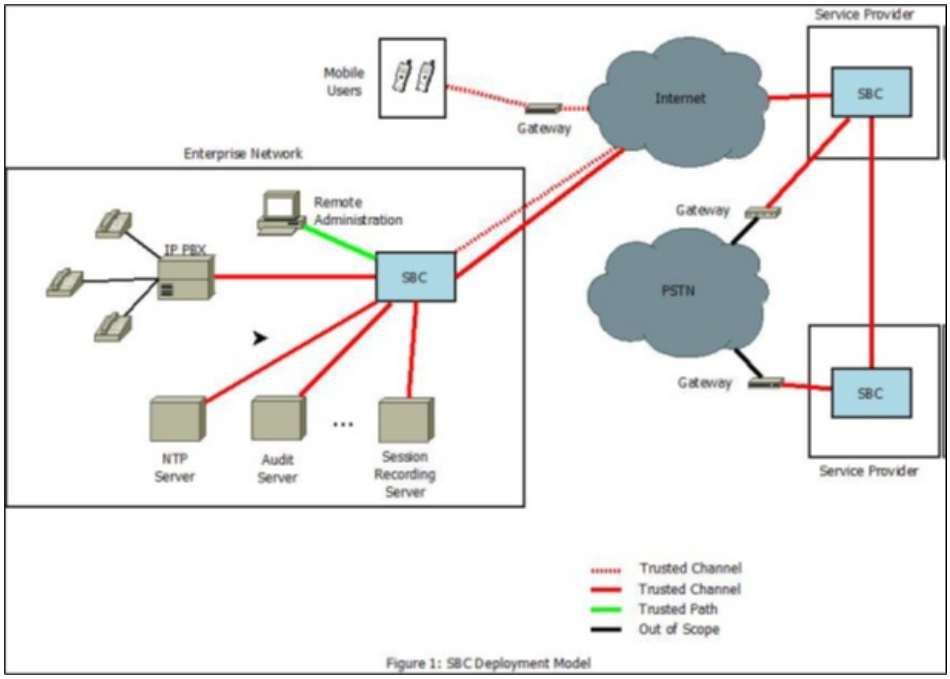


Figure 1: SBC Deployment Model

1.5 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 VVoIP 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 the SBC 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. .

2 Conformance Claims

Conformance Statement

This PP-Module inherits exact conformance as required from the specified Base-PP and as defined in the CC and CEM addenda for Exact Conformance, Selection-Based SFRs, and Optional SFRs (dated May 2017).

No PPs or PP-Modules may be specified in a PP-Configuration with this PP-Module other than the Base-PP specified in Section 1.1 Overview.

CC Conformance Claims

This PP-Module is conformant to Parts 2 (extended) and 3 (conformant) of Common Criteria Version 3.1, Release 5 [CC].

Package Claims

This PP-Module does not claim conformance to any packages.

3 Security Problem Description

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 in order 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

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. This document does not define any additional assumptions.

3.3 Organizational Security Policies

An organization deploying the TOE is expected to satisfy the organizational security policy listed below in addition to all organizational security policies defined by the claimed Base-PP.

This document does not define any additional OSPs.

4 Security Objectives

4.1 Security Objectives for the TOE

O.AUTHORIZED_ADMINISTRATION

All network devices are expected to provide services that allow the security functionality of the device to be managed. The SBC, as a specific type of network device, has a refined set of management functions to address its specialized behavior.

Addressed by: FMT_SMF.1/SBC

O.PROTECTED_COMMUNICATIONS

To mitigate the threat of data-in-transit disclosure, the SBC must ensure that remote communications are secured using appropriate means. This includes the security of VVoIP signaling and media channels and Session Initiation Protocol (SIP) trunking, in addition to any secure communications channels that are prescribed by the Base-PP such as communication with audit or authentication servers.

Addressed by: FCS_TLSC_EXT.1 (refined from Base-PP), FCS_TLSC_EXT.2 (refined from Base-PP), FCS_TLSS_EXT.1 (refined from Base-PP), FCS_TLSS_EXT.2 (refined from Base-PP), FIA_X509_EXT.1/Rev (refined from Base-PP), FIA_X509_EXT.2 (refined from Base-PP), FIA_X509_EXT.3 (refined from Base-PP), FTP_ITC.1 (refined from Base-PP), FCS_SRTP_EXT.1, FIA_SIPT_EXT.1, FTP_ITC.1/ESC, FTP_ITC.1/VVoIP, FTP_ITC.1/H323 (selection-based)

O.RESOURCE_AVAILABILITY

The SBC is not capable of performing its primary functionality if an attacker is able to prevent it from handling user data through a denial-of-service attack. Therefore, the SBC is expected to provide security functions that allow it to prioritize its resources and protect against traffic that is designed only to disrupt availability of the device.

Addressed by: FRU_PRS_EXT.1, FRU_RSA.1

O.SYSTEM_MONITORING

In order to ensure that potentially malicious activity is detected, the NDcPP requires security-relevant events to be audited. The SBC also provides security functions to support system monitoring, defines additional security-relevant events for specific SBC functions, and requires the use of a Network Time Protocol (NTP) server to provide accurate system time. The SBC is also expected to support real-time system monitoring by providing the ability to automatically generate alerts when certain types of events occur.

Addressed by: FAU_ARP_EXT.1, FAU_GEN.1/SBC, FAU_SAA.1, FAU_SEL.1

[JF] This is saying that NTP is required but that's not currently backed up by SFRs. Should it be? e.g. mandate the NTP selection in Base-PP FPT_STM_EXT.1 and mandate FCS_NTP_EXT.1

O.TOPOLOGY_HIDING

In order to ensure that there is no unauthorized disclosure of network information, the SBC is expected to hide the topology of the protected network. The SBC ensures no unauthorized disclosure by functioning as a B2BUA and by providing support for network address translation (NAT). These mechanisms ensure that the intended recipient of data being transmitted through the TOE is not revealed and that devices inside the protected network are not directly accessible.

Addressed by: FDP_IFC.1, FDP_IFF.1, FFW_NAT_EXT.1

O.TRAFFIC_FILTERING

In order to ensure that malicious traffic cannot compromise the SBC or devices on its protected network, the SBC is expected to provide rudimentary traffic filtering capabilities. This ensures that unauthorized TCP/UDP traffic is blocked and that all signaling and media traffic is first checked to be well-formed prior to performing any action on it.

Addressed by: FFW_ACL_EXT.1, FFW_ACL_EXT.2, FFW_DPI_EXT.1

O.USER_DATA_DELIVERY

When user data is transmitted between calling parties, the calling parties expect that this data is only transmitted to the intended recipients. The SBC is expected to provide this assurance through correctly functioning as a B2BUA and through correct implementation of SIP.

Addressed by: FDP_IFC.1, FDP_IFF.1, FFW_NAT_EXT.1, FIA_SIPT_EXT.1, FIA_SIPS_EXT.1 (optional)

4.2 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.

4.3 Security Objectives Rationale

This section describes how the assumptions, threats, and organizational security policies map to the security objectives.

Table 1: Security Objectives Rationale

Threat, Assumption, or OSP	Security Objectives	Rationale
T.MALICIOUS_TRAFFIC	O.SYSTEM_MONITORING	The TOE mitigates the threat of malformed traffic causing a system crash by ensuring that any such instances are logged so that their cause can be diagnosed and prevented in the future.
	O.TRAFFIC_FILTERING	The TOE mitigates the threat of malformed traffic causing a failure of the TOE by providing a mechanism to prevent the TSF from processing it.
T.NETWORK_ACCESS	O.AUTHORIZED_ADMINISTRATION	The TOE mitigates the threat of unauthorized network access by giving the administrator the ability to configure traffic filtering rules to block unauthorized traffic.
	O.PROTECTED_COMMUNICATIONS	The TOE mitigates the threat of unauthorized network access by enforcing the use of protected communications channels that prevent impersonation of legitimate subjects.
	O.SYSTEM_MONITORING	The TOE mitigates the threat of unauthorized network access by ensuring that any such instances are logged so that their cause can be diagnosed and prevented in the future.
	O.TOPOLOGY_HIDING	The TOE mitigates the threat of unauthorized network access by hiding its topology so that an attacker on an external network cannot discover or enumerate devices on the TOE's internal network.
	O.TRAFFIC_FILTERING	The TOE mitigates the threat of unauthorized network access by enforcing traffic filtering rules that prevent devices on the internal network from being accessed.
T.RESOURCE_EXHAUSTION	O.AUTHORIZED_ADMINISTRATION	The TOE mitigates the threat of resource exhaustion by giving administrators the ability to configure traffic rules so that traffic flooding attempts can be discarded.
	O.RESOURCE_AVAILABILITY	The TOE mitigates the threat of the transmission of network traffic that causes the inability of the TOE to perform its functions, by protecting against disruptive traffic.
	O.SYSTEM_MONITORING	The TOE mitigates the threat of unauthorized network access by ensuring that any such instances are logged so that their cause can be diagnosed and prevented in the future.
	O.TRAFFIC_FILTERING	The TOE mitigates the threat of resource exhaustion by providing the ability to filter network traffic that could cause a denial of service.
T.UNTRUSTED_COMMUNICATION_CHANNELS	O.PROTECTED_COMMUNICATIONS	The TOE mitigates the threat of disclosure of data in transit by enforcing the use of protected communications channels that prevent transmitted data from unauthorized disclosure.
T.USER_DATA_REUSE	O.USER_DATA_DELIVERY	The TOE mitigates the threat of inadvertently sending user data to an unintended destination by implementing measures that ensure that data is only sent to the intended recipient.

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 (including replacing an assignment with a more restrictive selection) 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 NDcPP 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 Session Border Controller 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 Cryptographic Support (FCS)

FCS_TLSC_EXT.1 TLS Client Protocol without Mutual Authentication

FCS_TLSC_EXT.1.1

This SFR is selection-based in the NDcPP but is mandated by this PP-Module because Transport Layer Security (TLS) is used for SIP trunking. An SBC implements TLS as both a client and a server.

Evaluation Activities

FCS_TLSC_EXT.1
There are no additional evaluation activities for this component beyond what the NDcPP requires.

FCS_TLSC_EXT.2 TLS Client Support for Mutual Authentication

FCS_TLSC_EXT.2.1

This SFR is optional in the NDcPP but is mandated by this PP-Module because SIP trunking requires mutually-authenticated TLS.

Evaluation Activities

FCS_TLSC_EXT.2
There are no additional evaluation activities for this component beyond what the NDcPP requires.

FCS_TLSS_EXT.1 TLS Server Protocol without Mutual Authentication

FCS_TLSS_EXT.1.1

This SFR is selection-based in the NDcPP but is mandated by this PP-Module because TLS is used for SIP trunking. An SBC implements TLS as both a client and a server.

Evaluation Activities

FCS_TLSS_EXT.1
TSS
There are no additional TSS evaluation activities for this component beyond what the NDcPP requires.

Guidance
There are no additional guidance evaluation activities for this component beyond what the NDcPP requires.

Tests
There are no additional test evaluation activities for this component beyond what the NDcPP requires.

FCS_TLSS_EXT.2 TLS Server Support for Mutual Authentication

FCS_TLSS_EXT.2.1

This SFR is optional in the NDcPP but is mandated by this PP-Module because SIP trunking requires mutually-authenticated TLS.

Evaluation Activities

FCS_TLSS_EXT.2
There are no additional evaluation activities for this component beyond what the NDcPP requires.

5.1.1.2 Identification and Authentication (FIA)

FIA_X509_EXT.1/Rev X.509 Certificate Validation

FIA_X509_EXT.1.1/Rev

This SFR is selection-based in the Base-PP but mandatory in this PP-Module because the TOE's TLS implementation requires appropriate X.509 functionality.

Evaluation Activities

FIA_X509_EXT.1/Rev
There are no additional evaluation activities for this component beyond what the NDcPP requires.

FIA_X509_EXT.2 X.509 Certificate Authentication

FIA_X509_EXT.2.1

This SFR is selection-based in the Base-PP but mandatory in this PP-Module because the TOE's TLS implementation requires appropriate X.509 functionality.

Evaluation Activities

FIA_X509_EXT.2
There are no additional evaluation activities for this component beyond what the NDcPP requires.

FIA_X509_EXT.3 X.509 Certificate Requests

FIA_X509_EXT.3.1

This SFR is selection-based in the Base-PP but mandatory in this PP-Module because the TOE's TLS implementation requires appropriate X.509 functionality.

Evaluation Activities

FIA_X509_EXT.3
There are no additional evaluation activities for this component beyond what the NDcPP requires.

5.1.1.3 from nd ftp

FTP_ITC.1 Inter-TSF Trusted Channel

FTP_ITC.1.1

The TSF shall be capable of using **TLS and** [**selection**: *IPsec*, *SSH*, *DTLS*, *HTTPS*, ***SNMPv3***, ***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]*] 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.

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*].

Application Note: TLS is mandated for SIP trunking as required by FIA_SIPT_EXT.1. SNMPv3 added as a selection to support FAU_ARP_EXT.1.

Evaluation Activities

FTP_ITC.1
The evaluator shall evaluate this SFR in the manner specified in the NDcPP except that SNMPv3 communications shall be tested (if claimed) in addition to any other selected protocols. Testing for SNMPv3 is performed through evaluation of FAU_ARP_EXT.1 if claimed there.

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 Security Audit (FAU)

FAU_ARP_EXT.1 Security Audit Automatic Response

FAU_ARP_EXT.1.1

The TSF 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.

Evaluation Activities

FAU_ARP_EXT.1
TSS
The evaluator shall verify that the TSS describes the ability of the TOE to transmit potential security violations to an alert receiver in the operational environment.

Guidance
The evaluator shall verify that the operational guidance provides instructions on how to configure the TOE so that it is able to communicate potential security violations to an alert receiver in the operational environment using the selected protocols.

Tests
The evaluator shall deploy the TOE in an environment that contains an alert receiver in the operational environment. The evaluator shall configure the TOE to communicate with an alert receiver in the manner that is specified by the operational guidance. The evaluator shall deploy a packet capture tool that is capable of sniffing the traffic between the TOE and the alert receiver. For each type of potential security violation that is defined by the ST, the evaluator shall cause that potential security violation to occur on the TOE, including configuring the TOE to detect the behavior as a potential security violation if it is necessary to do so.

Depending on what the TSF considers to be potential security violations, it may be necessary for the evaluator to set up traffic generators, heat guns, or other equipment that is used to simulate potential security violations.

After this is done, the evaluator shall observe via use of the packet capture tool and direct interaction with the alert receiver that the TSF transmitted the potential security violation and that it correctly used the selected protocols.

FAU_GEN.1/SBC Audit Data Generation (Session Border Controller)

FAU_GEN.1.1/SBC

The TSF shall be able to generate an audit record 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 adminsitrative actions;**
d. **[*Specifically defined auditable events listed in the Auditable Events table ()***

Requirement	Auditable Events	Additional Audit Record Contents		
FAU_ARP_EXT.1	None			
FAU_SAA.1	None			
FAU_SEL.1	None			
FCS_SRTP_EXT.1	None			
FDP_IFC.1	None			
FDP_IFF.1	Any modifications to the B2BUA policy	None		
FFW_ACL_EXT.1	Application of traffic filtering rules	Source and destination of observed traffic		
		FFW_ACL_EXT.2	Application of traffic filtering rules	Source and destination of observed traffic
				Rule relevant to observed traffic
Result of rule evaluation				
FFW_DPI_EXT.1	Application of deep packet inspection rules	Source and destination of observed traffic		
		Rule relevant to observed traffic		
		Result of rule evaluation		
FFW_NAT_EXT.1	None			
FIA_SIPS_EXT.1	Call Detail Record (CDR)	Calling party		
		Called party		
		Start time of the call		
		Call duration		
		Call type		
FIA_SIPT_EXT.1	All SIP trunk authentication attempts	Username and IP address of the servie provider		
FMT_SMF.1/SBC	All management actions	Identifier of initiator		

FRU_PRS_EXT.1	None	
FRU_RSA.1	None	
FTP_ITC.1/ESC	Initiation of the trusted channel	Identification of the initiator and target of the trusted channel
	Termination of the trusted channel	
	Failure of the trusted channel functions	
FTP_ITC.1/H323 (selection-based)	Initiation of the trusted channel	Identification of the initiator and target of the trusted channel
	Termination of the trusted channel	
	Failure of the trusted channel functions	
FTP_ITC.1/VVoIP	Initiation of the trusted channel	Identification of the initiator and target of the trusted channel
	Termination of the trusted channel	
	Failure of the trusted channel functions	

Table 2: Auditable 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 TSF.

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.

For SFRs labeled as optional or selection-based, the auditable event is required only if the corresponding SFR is claimed.

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 TSF shall record within each audit record at least the following information:

a. Date and time of the event, type of event, subject identity, 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-**Module**/ST, [*information specified in column three of the Auditable Events table ()*].

Evaluation Activities

FAU_GEN.1/SBC

TSS
The evaluator shall examine the TSS to determine that it identifies the TOE's auditable events. If the TOE is distributed across multiple components, the evaluator shall also ensure that the TSS identifies the component that is responsible for each type of auditable event.

Guidance
The evaluator shall check the operational guidance and ensure that it lists all of the auditable events and provides a format for audit records. Each audit record format type must be covered, along with a brief description of each field. The evaluator shall check to make sure that every audit event type mandated by the PP-Module and claimed in the ST is described and that the description of the fields contains the information required in FAU_GEN.1.2/SBC and the additional information specified in the Auditable Events table of the PP-Module.

If the TOE's default configuration does not include all required auditable events, the evaluator shall check the operational guidance to ensure that it includes instructions on how to place the TOE into its evaluated configuration by ensuring that all required auditable events are generated.

Tests
The evaluator shall test the TOE's ability to correctly generate audit records by having the TOE generate audit records in accordance with the EAs associated with the functional requirements in the PP-Module. Additionally, the evaluator shall test that each administrative action applicable in the context of the PP-Module is auditable. When verifying the test results, the evaluator shall ensure the audit records generated during testing match the format specified in the operational guidance, and that the fields in each audit record have the proper entries.

Note that the testing here can be accomplished in conjunction with the testing of the security mechanisms directly. For example, the testing that is performed to ensure that the operational guidance provided is correct will verify that AGD_OPE.1 is satisfied and should address the invocation of the administrative actions that are needed to verify the audit records are generated as expected.

FAU_SAA.1 Potential Violation Analysis

FAU_SAA.1.1

The TSF 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 TSF 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).

Evaluation Activities

FAU_SAA.1
TSS
The evaluator shall verify that the TSS describes the conditions that will be flagged by the TSF as a potential security violation and whether these conditions are administratively configurable.

Guidance
If the conditions that are flagged by the TSF as a potential security violation are configurable, the evaluator shall review the operational guidance to determine that it describes how an administrator can configure potential security violations.

Tests
Testing for this SFR is completed in conjunction with FAU_ARP_EXT.1. This SFR is tested by causing each type of potential security violation defined by the TSF and observing that they are correctly treated as such. This activity is performed as part of the EA for FAU_ARP_EXT.1 so a separate test is not required.

FAU_SEL.1 Selective Audit

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. [*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 the Auditable Events table 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.

Evaluation Activities

FAU_SEL.1
TSS
The evaluator shall examine the TSS to verify that it identifies the auditable events that can be suppressed and the filters that can be applied to suppress them. For example, if TOE has the ability to suppress the generation of events related to application of rules, the evaluator shall examine the TSS to determine whether this suppression is done globally, on a per-rule basis, etc.

Guidance
The evaluator shall examine the operational guidance to verify that it identifies the auditable events that can be suppressed and instructions for enabling/disabling the generation of these events.

Tests
For each auditable event that can be disabled, the evaluator shall configure the TOE to enable all auditable events, perform actions against the TOE that cause these events to be generated, and verify that the corresponding events are generated. The evaluator shall then disable the generation of a specific type of event, repeat the activity, and verify that a corresponding event is not generated.

For cases where multiple event types can be suppressed in this manner, or multiple mechanisms exist to selectively suppress events, the evaluator shall repeat this test as many times as necessary to ensure that each mechanism is validated. For example, if the suppression of audit records for application of traffic filtering rules can be configured globally, on a per-rule basis, and on a per-subject basis, the evaluator shall ensure that all three mechanisms of suppression are tested individually.

5.2.2 Cryptographic Support (FCS)

FCS_SRTP_EXT.1 Secure Real-Time Transport Protocol

FCS_SRTP_EXT.1.1

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

FCS_SRTP_EXT.1.2

The TSF shall implement SDES-SRTP supporting the following cipher suites: [**selection**:

- *AES_CM_128_HMAC_SHA1_80, in accordance with RFC 4568*
- *AES_CM_128_HMAC_SHA1_32, in accordance with RFC 4568*
- *AES_256_CM_HMAC_SHA1_80, in accordance with RFC 6188*
- *AES_256_CM_HMAC_SHA1_32, in accordance with RFC 6188*
- *AEAD_AES_128_GCM, in accordance with RFC 7714*
- *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 SDES dialog using one of the identified cipher suites. The ST author should select all cipher suites that are supported.

FCS_SRTP_EXT.1.3

The TSF shall ensure the SRTP NULL algorithm [**selection**: *is disabled*, *can be disabled by a [Security Administrator]*].

FCS_SRTP_EXT.1.4

The TSF shall allow the SRTP ports to be used for SRTP communications to be specified by a [*Security Administrator*].

Evaluation Activities

FCS_SRTP_EXT.1
TSS
The evaluator shall verify that the TSS describes the ability of the TOE to do the following:

1. *Support the use of SRTP and the cipher suites that are supported by the SRTP implementation.*
2. *Disable the SRTP NULL algorithm and/or provide the ability for it to be disabled by a Security Administrator.*
3. *Provide the ability for a Security Administrator to specify the SRTP ports used for SRTP communications.*

Guidance
The evaluator shall verify that the TSS describes the ability of the TOE to do the following:

1. *How to configure the cipher suites used by SRTP.*
2. *[conditional, if "can be disabled by a [Security Administrator]" is selected in FCS_SRTP_EXT.1.3] How to disable use of the SRTP NULL algorithm.*
3. *How to specify the ports used for SRTP communications.*

Tests
The evaluator shall perform the following tests:

- ***Test 1.1:***
  1. *If necessary, configure the TOE to use SRTP.*
  2. *Deploy a packet capture tool that is capable of sniffing traffic on the network interface where SRTP traffic will be transmitted.*
  3. *Establish an SRTP connection with the TOE and verify using packet captures and audit logs that SRTP communications are established and that encrypted traffic is transmitted over the SRTP channel.*
  4. *Repeat this test for each cipher suite supported for the SRTP implementation.*
- ***Test 1.2:***
  1. *Deploy a packet capture tool that is capable of sniffing traffic on the network interface where SRTP traffic will be transmitted.*
  2. *[conditional, if "can be disabled by a [Security Administrator]" is selected in FCS_SRTP_EXT.1.3] Configure the TOE to disable use of the SRTP NULL algorithm.*
  3. *Transmit SRTP NULL message to the TOE and observe that it is rejected.*
- ***Test 1.3:***
  1. *Configure the TOE to use a specified port for SRTP traffic.*
  2. *Deploy a packet capture tool that is capable of sniffing traffic on the network interface where SRTP traffic will be transmitted.*
  3. *Transmit SRTP traffic to the TOE and observe that the traffic is transmitted over the specified port.*
  4. *Configure the TOE to use a different port for SRTP traffic.*
  5. *Transmit SRTP traffic to the TOE and observe that the traffic is transmitted over the newly-specified port.*

5.2.3 User Data Protection (FDP)

FDP_IFC.1 Subset Information Flow Control

FDP_IFC.1.1

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

Evaluation Activities

FDP_IFC.1
N/A - the evaluation of this SFR is performed as part of FDP_IFF.1.

FDP_IFF.1 Simple Security Attributes

FDP_IFF.1.1

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

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 [*following configurable behavioral rules: [**selection**:*

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

]].

FDP_IFF.1.4

The TSF shall explicitly authorize an information flow based on the following rules: [*if the TSF 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 TSF shall explicitly deny an information flow based on the following rules: [*if the TSF 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*].

Evaluation Activities

FDP_IFF.1
TSS
The evaluator shall review the TSS to verify that it describes the ability of the TOE to function as a B2BUA and that it provides the ability to operate in either an allowlist or a denylist posture.

Guidance
The evaluator shall review the operational guidance to verify that it provides instructions for setting the TOE into either an allowlist or a denylist posture and for how to add or remove entries from the allowlist or denylist.

Tests
The evaluator shall perform the following tests:

- ***Test 2.1:** Configure a custom Access Control List (ACL) to deny a call originating from an IP address or subnet. Make a call from that IP address or subnet and verify the call cannot be completed. Verify calls from any other IP address or subnet will complete a call.*
- ***Test 2.2:** Configure a custom ACL to only permit a call originating from an IP address or subnet. Make a call from that IP address or subnet and verify the call can be completed.*
- ***Test 2.3:** Configure a custom ACL to deny a call destined for an IP address or subnet. Make a call to that IP address or subnet and verify the call cannot be completed. Verify calls to any other IP address or subnet will complete a call.*
- ***Test 2.4:** Configure a custom ACL to only permit a call destined an IP address or subnet. Make a call to that IP address or subnet and verify the call can be completed. Verify calls to any other IP address or subnet will not complete a call.*
- ***Test 2.5:** Configure a custom ACL to deny a call using a certain signaling (e.g. SIP) or media (e.g. RTP) protocol. Make a call using that protocol and verify the call cannot be completed. If other signaling (e.g. H.323) and/or media (e.g. SRTP) protocols are supported, verify that they can be used to complete a call while this ACL is in effect.*
- ***Test 2.6:** Configure a custom ACL to only permit a call using a certain signaling (e.g., SIP) or media (e.g., RTP) protocol. Make a call using that protocol and verify the call can be completed. If other signaling (e.g. H.323) and/or media (e.g. SRTP) protocols are supported, verify that they cannot be used to complete a call while this ACL is in effect.*
- ***Test 2.7:** On the TOE, configure an allowlist of allowed callers by calling number and all other numbers to be blocked. Verify the configuration through the audit log. Call through the TOE from each one of the allowlisted numbers. Verify that each number can complete. Attempt a call through the TOE from other non-allowlisted numbers. Verify that the calls cannot complete.*
- ***Test 2.8:** On the TOE, configure an allowlist of allowed callers by IP address and all other IP addresses to be blocked. Verify the configuration through the audit log. Call through the TOE from each one of the allowlisted IP addresses. Verify that each IP address can complete. Change the IP address of the end points; however, keep the calling number the*

same. Attempt a call through the TOE from new IP addresses. Verify that the calls cannot complete.

- ***Test 2.9:*** *On the TOE, configure a denylist of disallowed callers by calling number and all other numbers to be allowed. Verify the configuration through the audit log. Attempt to call through the TOE from each one of the denylisted numbers. Verify that each number cannot complete. Call through the TOE from other non-denylisted numbers. Verify that the calls can complete.*
- ***Test 2.10:*** *On the TOE, configure a denylist of disallowed callers by IP address and all other IP addresses to be allowed. Verify the configuration through the audit log. Attempt to call through the TOE from each one of the denylisted IP addresses. Verify that each IP address cannot complete. Change the IP address of the end-points; however, keep the calling number the same. Attempt a call through the TOE from new IP addresses. Verify that the calls can complete.*

5.2.4 Firewall

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.

FFW_ACL_EXT.1 Real-Time Communications Traffic Filtering

FFW_ACL_EXT.1.1

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

FFW_ACL_EXT.1.2

The TSF 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 vs virtual or trust zone, e.g., trusted vs 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 TSF 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 TSF shall allow the traffic filtering rules to be assigned to each distinct network interface.

FFW_ACL_EXT.1.5

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

FFW_ACL_EXT.1.7

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

Evaluation Activities

FFW_ACL_EXT.1.1

TSS

The evaluator shall verify that the TSS provides a description of the TOE's initialization/startup process, which clearly indicates where processing of network packets begins to take place, and provides a discussion that supports the assertion that packets cannot flow during this process.

The evaluator shall verify that the TSS also includes a narrative that identifies the components (e.g., an active entity such as a process or task) involved in processing the network packets and describes the safeguards that would prevent packets flowing through the TOE without applying the ruleset in the event of a component failure. This could include the failure of a component, such as a process being terminated, or a failure within a component, such as memory buffers full and cannot process packets.

Guidance

The guidance documentation associated with this element is assessed in the subsequent test EAs.

Tests

The evaluator shall perform the following tests:

- ***Test 3.1:*** *The evaluator shall attempt to get network traffic to flow through the TOE while the TOE is being initialized. A steady flow of network packets that would otherwise be denied by the ruleset should be sourced and be directed to a host. The evaluator shall verify, using a packet sniffer, that none of the generated network traffic is permitted through the firewall during initialization.*

  The evaluator shall attempt to get network traffic to flow through the TOE while the TOE is being initialized. A steady flow of network packets that would be permitted by the ruleset should be sourced and be directed at a host. The evaluator shall verify, using a packet sniffer, that none of the generated network traffic is permitted through the TOE during initialization and is only permitted once initialization is complete.

FFW_ACL_EXT.1.2

TSS

The evaluator shall verify that the TSS describes a packet filtering policy and the following attributes are identified as being configurable within traffic filtering rules for the associated protocols:

- *IPv4/IPv6*
    - *Source address (e.g., 10.0.0.1/16, 10.0.0.1, any)*
    - *Destination Address (e.g., 10.0.0.1/16, 10.0.0.1, any)*
    - *Transport Layer Protocol (e.g., TCP, UDP, TCP+UDP)*
- *TCP/UDP (for signaling channel)*
    - *Source Port*
    - *Destination Port*
- *Distinct interface (physical/virtual or trust zone, e.g., trusted/untrusted)*
- *Application (Real-Time Communications Protocol)*
    - *Signaling (whatever is claimed by the TSF; SIP, H.323, or both)*

The evaluator shall verify that each rule can identify the following actions: permit or drop with the option to log the operation. The evaluator shall verify that the TSS identifies all interface types subject to the packet filtering policy and explains how rules are associated with distinct network interfaces.

Guidance

The evaluator shall verify that the guidance documentation identifies the following attributes as

being configurable within traffic filtering rules for the associated protocols:

- *IPv4/IPv6*
  - *Source address (e.g., 10.0.0.1/16, 10.0.0.1, any)*
  - *Destination Address (e.g., 10.0.0.1/16, 10.0.0.1, any)*
  - *Transport Layer Protocol (e.g., TCP, UDP, TCP+UDP)*
- *TCP/UDP (for signaling channel)*
  - *Source Port*
  - *Destination Port*
- *Distinct interface (physical/virtual or trust zone, e.g., trusted/untrusted)*
- *Application (Real-Time Communications Protocol)*
  - *Signaling (whatever is claimed by the TSF; SIP, H.323, or both)*

The evaluator shall verify that the guidance documentation indicates that each rule can identify the following actions: permit, drop, and log.

Tests
The evaluator shall perform the following tests:

- ***Test 4.1:*** *The evaluator shall use the instructions in the guidance documentation to test that stateful packet filter firewall rules can be created that permit, drop, and log packets for each of the following attributes:*
  - *IPv4/IPv6*
    - *Source address (e.g., 10.0.0.1/16, 10.0.0.1, any)*
    - *Destination Address (e.g., 10.0.0.1/16, 10.0.0.1, any)*
    - *Transport Layer Protocol (e.g., TCP, UDP, TCP+UDP)*
  - *TCP/UDP (for signaling channel)*
    - *Source Port*
    - *Destination Port*
  - *Distinct interface (physical/virtual or trust zone, e.g., trusted/untrusted)*
  - *Application (Real-Time Communications Protocol)*
    - *Signaling (whatever is claimed by the TSF; SIP, H.323, or both)*
- ***Test 4.2:*** *Repeat Test 1 above as needed to ensure that traffic filtering rules can be defined for each distinct network interface type supported by the TOE.*

FFW_ACL_EXT.1.3
This element is evaluated through the evaluation activities for FFW_ACL_EXT.1.2.
FFW_ACL_EXT.1.4
This element is evaluated through the evaluation activities for FFW_ACL_EXT.1.2.
FFW_ACL_EXT.1.5
TSS
The evaluator shall verify that the TSS identifies the protocols that support session handling to include both TCP and UDP.

The evaluator shall verify that the TSS describes how sessions are established (including handshake processing) and maintained.

The evaluator shall verify that for TCP, the TSS identifies and describes the use of the following attributes in session determination: source and destination addresses, source and destination ports, sequence number, and individual flags.

The evaluator shall verify that for UDP, the TSS identifies and describes the following attributes in session determination: source and destination addresses and source and destination ports.

The evaluator shall verify that the TSS describes how established sessions are removed. The TSS shall describe how connections are removed for each protocol based on normal completion and/or timeout conditions. The TSS shall also indicate when session removal becomes effective (e.g., before the next packet that might match the session is processed).

Guidance
The evaluator shall verify that the guidance documentation describes session behaviors. For example, a TOE might not log packets that are permitted as part of an existing session.

Tests
The evaluator shall perform the following tests:

- ***Test 5.1:*** *The evaluator shall configure the TOE to permit and log TCP traffic. The evaluator shall initiate a TCP session. While the TCP session is being established, the evaluator shall introduce session establishment packets with incorrect flags to determine that the altered traffic is not accepted as part of the session (i.e., a log event is generated to show the ruleset was applied). After a TCP session is successfully established, the evaluator shall alter each of the session determining attributes (source and destination addresses, source and destination ports, sequence number, flags) one at a time in order to verify that the altered packets are not accepted as part of the established session.*
- ***Test 5.2:*** *The evaluator shall terminate the TCP session established per Test 1 as described*

in the TSS. The evaluator shall then immediately send a packet matching the former session definition in order to ensure it is not forwarded through the TOE without being subject to the ruleset.

- ***Test 5.3:*** *The evaluator shall expire (i.e., reach timeout) the TCP session established per Test 1 as described in the TSS. The evaluator shall then send a packet matching the former session in order to ensure it is not forwarded through the TOE without being subject to the ruleset.*
- ***Test 5.4:*** *The evaluator shall configure the TOE to permit and log UDP traffic. The evaluator shall establish a UDP session. Once a UDP session is established, the evaluator shall alter each of the session determining attributes (source and destination addresses, source and destination ports) one at a time in order to verify that the altered packets are not accepted as part of the established session.*
- ***Test 5.5:*** *The evaluator shall expire (i.e., reach timeout) the UDP session established per Test 4 as described in the TSS. The evaluator shall then send a packet matching the former session in order to ensure it is not forwarded through the TOE without being subject to the ruleset.*

FFW_ACL_EXT.1.6
TSS
The evaluator shall verify that the TSS describes the algorithm applied to incoming packets, including the processing of default rules, determination of whether a packet is part of an established session, and application of administrator defined and ordered ruleset.

Guidance
The evaluator shall verify that the guidance documentation describes how the order of traffic filtering rules is determined and provides the necessary instructions so that an administrator can configure the order of rule processing.

Tests
The evaluator shall perform the following tests:

- ***Test 6.1:*** *The evaluator shall devise two equal stateful traffic filtering rules with alternate operations – permit and drop. The rules should then be deployed in two distinct orders and in each case the evaluator shall ensure that the first rule is enforced in both cases by generating applicable packets and using packet capture and logs for confirmation.*
- ***Test 6.2:*** *The evaluator shall repeat the procedure above, except that the two rules should be devised where one is a subset of the other (e.g., a specific address vs. a network segment). Again, the evaluator should test both orders to ensure that the first is enforced regardless of the specificity of the rule.*

FFW_ACL_EXT.1.7
TSS
The evaluator shall verify that the TSS describes the process for applying traffic filtering rules and also that the behavior (either by default, or as configured by the administrator) is to deny packets when there is no rule match unless another required condition allows the network traffic (i.e., FFW_ACL_EXT.1.5).

Guidance
The evaluator shall verify that the guidance documentation describes the behavior if no rules or special conditions apply to the network traffic. If the behavior is configurable, the evaluator shall verify that the guidance documentation provides the appropriate instructions to configure the behavior to deny packets with no matching rules.

Tests
For each attribute in FFW_ACL_EXT.1.2, the evaluator shall construct a test to demonstrate that the TOE can correctly compare the attribute from the packet header to the ruleset, and shall demonstrate both the permit and deny for each case. The evaluator shall check the log in each case to confirm that the relevant rule was applied. The evaluator shall record a packet capture for each test to demonstrate the correct TOE behavior.

FFW_ACL_EXT.2 Stateful VVoIP Traffic Filtering

FFW_ACL_EXT.2.1

The TSF 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 TSF 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 VVoIP 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 VVoIP 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 VVoIP protocol traffic.

Evaluation Activities

FFW_ACL_EXT.2
TSS
The evaluator shall verify that the TSS describes the ability of the TOE to perform stateful traffic filtering of all VVoIP protocols specified in FFW_ACL_EXT.2.1. The evaluator shall also verify that the TSS identifies the default stateful traffic filtering rules that are enforced by the TSF and what actions are taken when traffic is found to be in violation of one more of these rules.

The evaluator shall verify that the TSS describes the ability of the TOE to dynamically open and close ports to handle VVoIP traffic such that the ports used to carry VVoIP traffic are not predictable and ports are not open and listening for VVoIP traffic.

Guidance
If the TOE provides the ability to configure its stateful traffic filtering rules, the evaluator shall review the guidance documentation to verify that it provides instructions on how to do so.

Tests
The evaluator shall perform the following tests:

- ***Test 7.1:*** *[conditional, “SIP” is selected in FFW_ACL_EXT.2.1 and “SIP traffic where a BYE message precedes an INVITE message” is selected in FFW_ACL_EXT.2.2] The evaluator shall connect a remote endpoint to the TOE and use it to transmit an out of sequence SIP request where a BYE message is sent before an INVITE request. The evaluator shall use packet captures and audit logs to verify that the out of sequence traffic was sent and that the call attempt was dropped and logged by the TOE.*
- ***Test 7.2:*** *[conditional, “H.323 (H.225, H.245)” is selected in FFW_ACL_EXT.2.1 and “H.225 traffic where an RFC reply precedes any other traffic” is selected in FFW_ACL_EXT.2.2] The evaluator shall connect a remote endpoint to the TOE and use it to transmit an out of sequence H.225 request where an RCF reply is sent before any other traffic. The evaluator shall use packet captures and audit logs to verify that the out of sequence traffic was sent and that the call attempt was dropped and logged by the TOE.*
- ***Test 7.3:*** *[conditional, “H.323 (H.225, H.245)” is selected in FFW_ACL_EXT.2.1 and “H.245 traffic where a ResponseMessage precedes a RequestMessage” is selected in FFW_ACL_EXT.2.2] The evaluator shall connect a remote endpoint to the TOE and use it to transmit an out of sequence H.245 request where a ResponseMessage is sent prior to a corresponding RequestMessage. The evaluator shall use packet captures and audit logs to verify that the out of sequence traffic was sent and that the call attempt was dropped and logged by the TOE.*
- ***Test 7.4:*** *[conditional, “MGCP” is selected in FFW_ACL_EXT.2.1 and “MGCP traffic where DLCX message precedes a CRCX message” is selected in FFW_ACL_EXT.2.2] The evaluator*

shall connect a remote endpoint to the TOE and use to transmit an out of sequence MGCP request where a DLCX message is sent prior to a corresponding CRCX message. The evaluator shall use packet captures and audit logs to verify that the out of sequence traffic was sent and that the call attempt was dropped and logged by the TOE.

- ***Test 7.5:*** *The evaluator shall configure a custom ACL to deny a call originating from an IP address or subnet. The evaluator shall then make a call from that IP address or subnet and verify the call cannot be completed. The evaluator shall also verify that calls from any other IP address or subnet will complete a call.*
- ***Test 7.6:*** *The evaluator shall complete a call and capture the packets. The evaluator shall examine the packet capture and take note of the ports the media channel (RTP, SRTP) is communicating over. The evaluator shall then terminate the call. Using a packet generator, the evaluator shall attempt to send traffic over the media ports that were active when the call was active. Using packet captures, the evaluator shall then verify that the traffic does not traverse the TOE on these ports.*

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 ST 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*].

Evaluation Activities

FFW_DPI_EXT.1
TSS
The evaluator shall examine the TSS to verify that it describes the ability of the TOE to perform deep packet inspection for any or all of H.323, SIP, RTP, and RTCP traffic (consistent with the ST's SFR claim) and the rules that the TSF enforces to determine whether the received traffic is well-formed. The evaluator shall also verify that the TSS describes what actions the TOE performs when malformed traffic is detected.

Guidance
If the deep packet inspection function of the TSF is configurable, the evaluator shall verify that the guidance documentation provides instructions on how to configure this function.

Tests
The evaluator shall repeat the following test for each protocol that the TOE is capable of performing deep packet inspection for: If the deep packet function is configurable, the evaluator shall configure this function to flag, log, and/or drop malformed traffic, depending on the selections chosen in FFW_DPI_EXT.1.3. The evaluator shall then transmit malformed traffic to the TOE. Using packet captures and audit logs, the evaluator shall verify that the malformed traffic was sent to the TOE, logged, and not transmitted any further. The evaluator shall repeat this test for each type of malformed traffic that can be detected by the TOE as described in FFW_DPI_EXT.1.2.

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

Evaluation Activities

FFW_NAT_EXT.1
TSS
The evaluator shall review the TSS to verify that it describes the ability of the TOE to support NAT for the protocols specified in FFW_NAT_EXT.1.2. The evaluator shall also verify that the TSS describes how the TSF uses NAT to replace the IP address header value of outbound traffic and how the TOE keeps track of the original identities of calling parties.

Guidance
If the ST author selected "a [Security Administrator]-defined value" in FFW_NAT_EXT.1.3, the evaluator shall verify that the guidance documentation provides instructions on how to define the IP address header value

Tests
The evaluator shall place a call originating from the "internal" network to the "external" network. The evaluator shall use packet captures on the "external" network to verify that the data in the packets do not disclose the "internal" network's addressing or naming structure.

If the ST author selected "a Security Administrator-defined value" in FFW_NAT_EXT.1.3, the evaluator shall specify a given IP header value and verify that the traffic replaces the original header value with the administrator-defined value. If the ST author instead selected "the IP address of the TOE," the evaluator shall verify that this header value is the IP address of the TOE's interface to the "external" network.

5.2.5 Identification and Authentication (FIA)

FIA_SIPT_EXT.1 Session Initiation Protocol Trunking

FIA_SIPT_EXT.1.1

The TSF shall provide support for SIP trunking.

FIA_SIPT_EXT.1.2

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

FIA_SIPT_EXT.1.4

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

Evaluation Activities

FIA_SIPT_EXT.1
TSS
The evaluator shall verify that the TSS describes the ability of the TOE to support authenticated and encrypted SIP trunking along with the method by which the trunk peer will authenticate to the TOE.

Guidance
The evaluator shall verify that the guidance documentation provides instructions on how to configure SIP trunking to require encryption and authentication if this function is configurable.

Tests
The evaluator shall perform the following tests:

- ***Test 8.1:*** *Configure the TOE to support an encrypted SIP trunk. Configure a trunk peer to communicate with the TOE using the SIP trunk. Present a correct username/password combination or valid X.509 certificate on the trunk peer with a SIP trunk request that originates from an expected IP address. Verify via packet capture and audit log that the session was established.*

- ***Test 8.2:*** *Repeat Test 1 but provide incorrect username/password information or invalid X.509 certificate with the trunk peer and verify via packet capture and audit log that the session was not established.*
- ***Test 8.3:*** *Repeat Test 1 but change the IP address of the trunk peer and verify via packet capture and audit log that the session was not established.*

5.2.6 Security Management (FMT)

FMT_SMF.1/SBC Specification of Management Functions (SBC)

FMT_SMF.1.1/SBC

The TSF 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.

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.

Evaluation Activities

FMT_SMF.1/SBC
TSS
The evaluator shall examine the TSS to determine that, for each administrative function listed in the SFR, the ability to execute the function and the logical interfaces used to perform the function is claimed. For each of these functions, the evaluator shall also confirm that the TSS details how the ability to manipulate the TSF data through these interfaces is disallowed for non-administrative users.

Guidance
The evaluator shall review the guidance documentation to determine that each of the functions detailed in the TSS are identified, and that configuration information is provided to ensure that only administrators have access to the functions.

Tests
For each management function specified in FMT_SMF.1.1/SBC, the evaluator shall access the TOE with appropriate authorizations, perform the required function, and demonstrate that configuration of the function results in the proper expected behavior. For behavior related to SBC functionality (as opposed to manipulation of user accounts), this may be tested in conjunction with other SFRs.

The evaluator shall also ensure that all relevant management functionality from FMT_SMF.1 in the Base-PP that relates to the SBC PP-Module are tested in conjunction with SBC functionality. For example, for SBC functions that rely on time services, the evaluator shall ensure that a

Security Administrator can either manually configure the time or specify NTP server connectivity and ensure that the SBC functions will make use of the configured time data.

The evaluator shall also demonstrate that a user who lacks privileges to execute these functions (as described in the operational guidance) are unable to execute them.

[JF] It was commented elsewhere that there was a statement that implies NTP support is required. If it does end up being required, the example listed in this test should be changed.

5.2.7 Resource Utilization (FRU)

FRU_PRS_EXT.1 Limited Priority of Service

FRU_PRS_EXT.1.1

The TSF shall assign a priority to each type of communications packet that traverses the TSF.

FRU_PRS_EXT.1.2

The TSF shall ensure that each access to network bandwidth shall be mediated on the basis of the subject's assigned priority.

Evaluation Activities

FRU_PRS_EXT.1
TSS
The evaluator shall verify that the TSS describes the ability of the TOE to prioritize traffic flows as well as the mechanism by which access to network bandwidth is granted by the TSF.

Guidance
The evaluator shall examine the guidance documentation for a description of how to configure Quality of Service (QoS) for the TOE, including how to set tags for given traffic flows.

Tests
The evaluator shall perform the following tests:

- ***Test 9.1:*** *Configure the TOE to support QoS. Set QoS tags for media and signaling traffic flows. Complete a call between calling parties that are connected to the TOE via two different external interfaces. Verify, using packet captures, that traffic between the TOE and the callee is tagged with appropriate QoS markings.*
- ***Test 9.2:*** *Configure the TOE to support QoS. Set QoS tags for media and signaling traffic flows. Configure one remote endpoint to act as a calling party that sends a continuous stream of VVoIP traffic (media and signaling) to another endpoint that is connected to the TOE via a different external interface. Using a tool of choice, create a data stream of non-VVoIP (no media and no signaling) traffic that ingresses one interface, passes through the TOE, and egresses on the TOE. These shall be the same interfaces used by the VVoIP traffic. Verify using packet captures that traffic between the TOE and the callee is tagged with appropriate QoS markings, and that VVoIP and non-VVoIP traffic packets are passed through the TOE. Change the TOE QoS configuration to rate-limit, or police, non-VVoIP traffic. Verify either using packet captures that VVoIP traffic passes through the TOE while non-VVoIP traffic is rate-limited (egress packets are less than ingress traffic) OR that Rating factor (R-Factor) and/or Mean Opinion Score (MOS) values signal mediation.*

FRU_RSA.1 Maximum Quotas

FRU_RSA.1.1

The TSF 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 SFR is for the TOE to be resistant to denial of service attacks.

Evaluation Activities

FRU_RSA.1
TSS
The evaluator shall verify that the TSS describes the internal resources that the TSF can protect from DoS attacks as well as the types of behavior that would constitute a DoS attack against each of these resources.

Guidance
If the ability to protect against DoS attacks is configurable, the evaluator shall verify that the operational guidance provides instructions on how to configure this function.

Tests
The evaluator shall perform the following tests:

- ***Test 10.1:*** *Using a tool of choice, attempt a DoS attack that creates excess CPU cycles. Place a call while this attack occurs. Verify through packet capture and audio file or screenshot that the call was successful.*
- ***Test 10.2:*** *Using a tool of choice, attempt a DoS attack that attempts to exhaust the TOE's memory. Place a call while this attack occurs. Verify through packet capture and audio file or screenshot that the call was successful.*
- ***Test 10.3:*** *Using a tool of choice, perform protocol fuzzing for each communications protocol supported by the TOE. Verify that fuzzing does not cause the TOE to be compromised or to experience degraded functionality. For each tool of choice used to perform these tests, the evaluator shall provide justification for the appropriateness of the chosen tool.*

5.2.8 Trusted Path/Channels (FTP)

FTP_ITC.1/ESC Inter-TSF Trusted Channel (ESC Communications)

FTP_ITC.1.1/ESC

The TSF shall provide a **signaling** channel between itself and **an ESC 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 end points 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 Base-PP.

FTP_ITC.1.2/ESC

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

FTP_ITC.1.3/ESC

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

Evaluation Activities

FTP_ITC.1/ESC
This SFR is an iteration of FTP_ITC.1 as defined in the NDcPP. The evaluator shall repeat the EAs defined for FTP_ITC.1 in the NDcPP for this iteration of the SFR.

FTP_ITC.1/VVoIP Inter-TSF Trusted Channel (VVoIP Communications)

FTP_ITC.1.1/VVoIP

The TSF 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 end points 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 Base-PP.

FTP_ITC.1.2/VVoIP

The TSF shall permit [*the TSF, the authorized IT entities*] to initiate communication via the trusted channel.

FTP_ITC.1.3/VVoIP

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

Evaluation Activities

FTP_ITC.1/VVoIP
This SFR is an iteration of FTP_ITC.1 as defined in the NDcPP. The evaluator shall repeat the EAs defined for FTP_ITC.1 in the NDcPP for this iteration of the SFR.

5.3 TOE Security Functional Requirements Rationale

The following rationale provides justification for each security objective for the TOE, showing that the SFRs are suitable to meet and achieve the security objectives:

Table 3: SFR Rationale

Objective	Addressed by	Rationale
O.AUTHORIZED_ADMINISTRATION	FMT_SMF.1/SBC	This SFR supports the objective by defining TSF management functions that require authorizations to use.
O.PROTECTED_COMMUNICATIONS	FCS_TLSC_EXT.1 (refined from Base-PP)	This SFR supports the objective by requiring TLS for SIP trunking and ESC signaling channel communications.
	FCS_TLSC_EXT.2 (refined from Base-PP)	This SFR supports the objective by requiring mutually-authenticated TLS for SIP trunking.
	FCS_TLSS_EXT.1 (refined from Base-PP)	This SFR supports the objective by requiring TLS for SIP trunking and ESC signaling channel communications.
	FCS_TLSS_EXT.2 (refined from Base-PP)	This SFR supports the objective by requiring mutually-authenticated TLS for SIP trunking.
	FIA_X509_EXT.1/Rev (refined from Base-PP)	This SFR supports the objective by defining requirements for the X.509 validation algorithm used by the TOE's TLS implementation.
	FIA_X509_EXT.2 (refined from Base-PP)	This SFR supports the objective by defining requirements for the X.509 validation algorithm used by the TOE's TLS implementation.
	FIA_X509_EXT.3 (refined from Base-PP)	This SFR supports the objective by defining a mechanism by which the TOE obtains the certificates it uses for TLS client and server connections.
	FTP_ITC.1 (refined from Base-PP)	This SFR supports the objective by defining external interfaces that require protected communications as well as the trusted protocols used to protect those communications.
	FCS_SRTP_EXT.1	This SFR supports the objective by defining the TOE's implementation of the SRTP protocol that is used to protect VVoIP endpoint communications.
	FIA_SIPT_EXT.1	This SFR supports the objective by defining secure behavior for SIP trunking.
	FTP_ITC.1/ESC	This SFR supports the objective by defining how communications with an external ESC are protected.
	FTP_ITC.1/VVoIP	This SFR supports the objective by defining how communications with an external VVoIP endpoint are protected.
	FTP_ITC.1/H323 (selection-based)	This SFR supports the objective by defining H.323 as a permitted method of protected communications for when a conformant TOE implements this logical interface.
O.RESOURCE_AVAILABILITY	FRU_PRS_EXT.1	This SFR supports the objective by requiring the TSF to implement priority of service to ensure that low-priority traffic cannot cause a denial of service.
	FRU_RSA.1	This SFR supports the objective by enforcing quotas for TSF resources to prevent denial of service.
O.SYSTEM_	FAU_ARP_EXT.1	This SFR supports the objective by defining the ability to

MONITORING		generate security violations that are transmitted to external entities.
	FAU_GEN.1/SBC	This SFR supports the objective by iterating a Base-PP requirement to define additional auditable events that are specific to SBC functionality.
	FAU_SAA.1	This SFR supports the objective by defining a set of rules to monitor auditable events for potential security violations.
	FAU_SEL.1	This SFR supports the objective 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.
O.TOPOLOGY_ HIDING	FDP_IFC.1	This SFR supports the objective by defining a B2BUA policy so that VVoIP endpoints are only connected to each other through the TOE as an intermediary.
	FDP_IFF.1	This SFR supports the objective by defining the specific rules that the B2BUA policy enforces.
	FFW_NAT_EXT.1	This SFR supports the objective by defining the use of NAT to obfuscate IP addresses of endpoint devices on the TOE's internal network.
O.TRAFFIC_ FILTERING	FFW_ACL_EXT.1	This SFR supports the objective by defining capabilities for traffic filtering of network packets.
	FFW_ACL_EXT.2	This SFR supports the objective by defining specific methods of stateful traffic inspection for specific protocols.
	FFW_DPI_EXT.1	This SFR supports the objective by defining the capability to perform DPI for certain network traffic.
O.USER_DATA_ DELIVERY	FDP_IFC.1	This SFR supports the objective by defining a B2BUA policy that is used by the TOE to establish connections between VVoIP endpoints.
	FDP_IFF.1	This SFR supports the objective by defining the rules that the B2BUA policy enforces.
	FFW_NAT_EXT.1	This SFR supports the objective 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_SIPT_EXT.1	This SFR supports the objective by defining the use of SIP trunking, which requires authentication of endpoints to ensure data is only transmitted to the intended endpoint.
	FIA_SIPS_EXT.1 (optional)	This SFR supports the objective by defining an optional capability to handle SIP registration in cases where the OE does not include an ESC that will provide that functionality.

5.4 TOE Security Assurance Requirements

This PP-Module does not define any SARs beyond those defined within the Base-PP to which it can claim conformance. It is important to note that a TOE that is evaluated against this PP-Module is inherently evaluated against the NDcPP as well. This PP includes a number of EAs associated with both Security Functional Requirements (SFRs) and SARs. Additionally, this PP-Module includes a number of SFR-based EAs that similarly refine the SARs of the Base-PP. The evaluation laboratory will evaluate the TOE against the chosen Base-PP and supplement that evaluation with the necessary SFRs that are taken from this PP-Module.

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

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 to/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/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 denial of service 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 to/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 Objectives

The objectives for the TOEs are consistent with the NDcPP based on the following rationale:

PP-Module TOE Objective	Consistency Rationale
O.AUTHORIZED_ADMINISTRATION	The NDcPP does not define any TOE objectives; instead, it maps SFRs directly to threats. This TOE objective is consistent with the

	NDcPP because the individual security functions needed to satisfy the objective do not contradict with the security functions required by the NDcPP.
O.PROTECTED_COMMUNICATIONS	The NDcPP does not define any TOE objectives; instead, it maps SFRs directly to threats. This TOE objective is consistent with the NDcPP because the individual security functions needed to satisfy the objective do not contradict with the security functions required by the NDcPP.
O.RESOURCE_AVAILABILITY	The NDcPP does not define any TOE objectives; instead, it maps SFRs directly to threats. This TOE objective is consistent with the NDcPP because the individual security functions needed to satisfy the objective do not contradict with the security functions required by the NDcPP.
O.SYSTEM_MONITORING	The NDcPP does not define any TOE objectives; instead, it maps SFRs directly to threats. This TOE objective is consistent with the NDcPP because the individual security functions needed to satisfy the objective do not contradict with the security functions required by the NDcPP.
O.TOPOLOGY_HIDING	The NDcPP does not define any TOE objectives; instead, it maps SFRs directly to threats. This TOE objective is consistent with the NDcPP because the individual security functions needed to satisfy the objective do not contradict with the security functions required by the NDcPP.
O.TRAFFIC_FILTERING	The NDcPP does not define any TOE objectives; instead, it maps SFRs directly to threats. This TOE objective is consistent with the NDcPP because the individual security functions needed to satisfy the objective do not contradict with the security functions required by the NDcPP.
O.USER_DATA_DELIVERY	The NDcPP does not define any TOE objectives; instead, it maps SFRs directly to threats. This TOE objective is consistent with the NDcPP because the individual security functions needed to satisfy the objective do not contradict with the security functions required by the NDcPP.

6.1.4 Consistency of Requirements

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

PP-Module Requirement	Consistency Rationale
	Modified SFRs
FCS_TLSC_EXT.1	This PP-Module mandates the inclusion of this selection-based SFR because it is required to implement the trusted communications required by the PP-Module.
FCS_TLSC_EXT.2	This PP-Module mandates the inclusion of this optional SFR because it is required to implement the trusted communications required by the PP-Module.
FCS_TLSS_EXT.1	This PP-Module mandates the inclusion of this selection-based SFR because it is required to implement the trusted communications required by the PP-Module.
FCS_TLSS_EXT.2	This PP-Module mandates the inclusion of this optional SFR because it is required to implement the trusted communications required by the PP-Module.
FIA_X509_EXT.1/Rev	This PP-Module mandates the inclusion of this selection-based SFR because it is a dependency of the TLS requirements that it also mandates.
FIA_X509_EXT.2	This PP-Module mandates the inclusion of this selection-based SFR because it is a dependency of the TLS requirements that it also mandates.
FIA_X509_EXT.3	This PP-Module mandates the inclusion of this selection-based SFR because it is a dependency of the TLS requirements that it also mandates.
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 and to optionally allow the use of a new protocol (SNMPv3) specifically for the use of the alert channel that is defined in the PP-

	Module.
Additional SFRs	
This PP-Module does not add any requirements when the NDcPP is the base.	
Mandatory SFRs	
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 iterates a Base-PP requirement to define 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.
FCS_SRTP_EXT.1	This SFR applies to the implementation of SRTP, which is a protocol that is not used for any Base-PP functionality.
FDP_IFC.1	This SFR applies to the TOE's implementation of a B2BUA policy, which applies to the TOE's through-traffic interfaces and is therefore beyond the original scope of the Base-PP.
FDP_IFF.1	This SFR applies to the TOE's implementation of a B2BUA policy, which applies to the TOE's through-traffic interfaces and is therefore beyond the original scope of the Base-PP.
FFW_ACL_EXT.1	This SFR applies to traffic filtering, which applies to the TOE's through-traffic interfaces and is therefore beyond the original scope of the Base-PP.
FFW_ACL_EXT.2	This SFR applies to traffic filtering, which applies to the TOE's through-traffic interfaces and is therefore beyond the original scope of the Base-PP.
FFW_DPI_EXT.1	This SFR applies to DPI, which applies to the TOE's through-traffic interfaces and is therefore beyond the original scope of the Base-PP.
FFW_NAT_EXT.1	This SFR applies to NAT, which applies to the TOE's through-traffic interfaces and is therefore beyond the original scope of the Base-PP.
FIA_SIPT_EXT.1	This SFR applies to SIP trunking, which is a logical interface that is beyond the original scope of the Base-PP.
FMT_SMF.1/SBC	This SFR defines management functions for SBC that are not applicable to the Base-PP and therefore appropriately defined as a separate iteration of FMT_SMF.1.
FRU_PRS_EXT.1	This SFR applies to enforcement of bandwidth priority of service, which is a mechanism that is beyond the scope of the Base-PP and does not interfere with the ability of the Base-PP to process valid network traffic securely.
FRU_RSA.1	This SFR applies to enforcement of resource quotas, which is a mechanism that is beyond the scope of the Base-PP and does not interfere with the ability of the Base-PP to process valid network traffic securely.
FTP_ITC.1/ESC	The PP-Module iterates an SFR defined in the Base-PP to define a new external interface for communications with an ESC. This does not interfere with the ability of the Base-PP to enforce its security functionality on the existing logical interfaces.
FTP_ITC.1/VVoIP	The PP-Module iterates an SFR defined in the Base-PP to define a new external interface for communications with a VVoIP endpoint. This does not interfere with the ability of the Base-PP to enforce its security functionality on the existing logical interfaces.
Optional SFRs	
This PP-Module does not define any Optional requirements.	
Selection-based SFRs	
FTP_ITC.1/H323	The 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.
Objective SFRs	

This PP-Module does not define any Objective requirements.	
Implementation-based SFRs	
FIA_SIPS_EXT.1	This SFR applies to SIP registration, which is beyond the original scope of the Base-PP.

Appendix A - Optional SFRs

A.1 Strictly Optional Requirements

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

A.2 Objective Requirements

This PP-Module does not define any Objective SFRs.

A.3 Implementation-dependent Requirements

A.3.1 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 compiles 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 VVoIP 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 8 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 TSF 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-dependent based on whether the SBC has the capability to perform its own SIP registration of devices.

Evaluation Activities

FIA_SIPS_EXT.1
TSS
The evaluator shall verify that the TSS describes the ability of the TOE to support SIP in compliance with RFC 3261, including the ability to require password authentication for SIP REGISTER function requests. The evaluator shall also verify that the TSS describes the allowed composition of SIP authentication passwords.

The evaluator shall verify that the TSS describes the ability of the TSF to modify SIP header values for SIP traffic received by the TOE prior to retransmitting it.

Guidance
The evaluator shall verify that the guidance documentation indicates that SIP REGISTER requests must be authenticated by the TOE along with the minimum password strength required for the authentication credential.

The evaluator shall also verify that the guidance documentation provides instructions for how to configure the TOE to manipulate SIP header values.

Tests

The evaluator shall perform the following tests:

- ***Test 11.1:*** *Attempt to have a SIP client issue a SIP REGISTER request without providing authentication credentials. Observe that the request is rejected and logged by the TSF.*
- ***Test 11.2:*** *Attempt to have a SIP client issue a SIP REGISTER request with authentication credentials using characters not supported by the TSF. Observe that the request is rejected and logged by the TSF.*
- ***Test 11.3:*** *Attempt to have a SIP client issue a SIP REGISTER request with valid authentication credentials using characters supported by the TSF. Observe that the request is accepted and logged by the TSF. Repeat this test as many times as necessary to ensure that passwords of the minimum and maximum supported lengths are used and that each supported character is used in at least one password.*

  Test 4: Configure the TOE to manipulate SIP header values. Place a call through the TOE. Capture traffic both before it is received by the TOE and after it exits the TOE. Verify that the SIP header values have been modified. Repeat for each supported header modification, as necessary.

Appendix B - Selection-based Requirements

B.1 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, FIA_SIPS_EXT.1.1.

FTP_ITC.1.1/H323

[JF] need syntax for when there are >3 triggers for a sel-based SFR (FFW_ACL_EXT.1, FFW_ACL_EXT.2, FFW_DPI_EXT.1, FIA_SIPS_EXT.1) The TSF shall provide an **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 end points 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 Base-PP.

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.

FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, and FCS_IPSEC_EXT.1 are defined in the Base-PP.

Evaluation Activities

FTP_ITC.1/H323
This SFR is an iteration of FTP_ITC.1 as defined in the NDcPP. The evaluator shall repeat the EAs defined for FTP_ITC.1 in the NDcPP for this iteration of the SFR.

Appendix C - Extended Component Definitions

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

C.1 Extended Components Table

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

Table 4: Extended Component Definitions

Functional Class	Functional Components
Cryptographic Support (FCS)	FCS_SRTP_EXT Secure Real-Time Transport Protocol
Firewall	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)

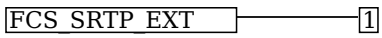
This Module defines the following extended components as part of the FCS class originally defined by CC Part 2:

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

FCS_SRTP_EXT.1.2

The TSF shall implement SDES-SRTP supporting the following cipher suites [**assignment**: *list of supported cipher suites and the standard in which they are defined*].

FCS_SRTP_EXT.1.3

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

FCS_SRTP_EXT.1.4

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

C.2.2 Firewall

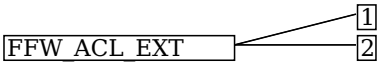
This Module defines the following extended components as part of the class originally defined by CC Part 2:

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 TSF to implement traffic filtering rules based on network protocol attributes.

FFW_ACL_EXT.2, Stateful VVoIP Traffic Filtering, requires the TSF 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 TSF shall perform traffic filtering on network packets processed by the TOE.

FFW_ACL_EXT.1.2

The TSF 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 TSF 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**.

FFW_ACL_EXT.1.4

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

FFW_ACL_EXT.1.5

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

FFW_ACL_EXT.1.7

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

FFW_ACL_EXT.2.2

The TSF 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 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.

FFW_ACL_EXT.2.4

The TSF 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

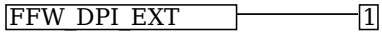
The TSF shall not define a static range of ports to remain open indefinitely for the purpose of allowing VVoIP protocol traffic.

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

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

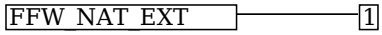
When traffic is found to be in violation of a DPI rule, the TSF shall take the following action: [**assignment**: *action taken in response to rule violation*].

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)

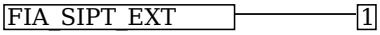
This Module defines the following extended components as part of the FIA class originally defined by CC Part 2:

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 TSF 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 TSF shall provide support for SIP trunking.

FIA_SIPT_EXT.1.2

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

FIA_SIPT_EXT.1.4

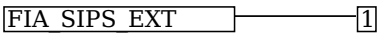
The TSF shall require a service provider to encrypt traffic using TLS in order to establish a SIP trunk.

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 TSF 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 TSF shall implement the [**selection**: *SIP that complies with RFC 3261, H.323 protocol that compiles 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 VVoIP traffic.

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**: *minimum numeric length*] characters in the set of [**assignment**: *supported character set*].

FIA_SIPS_EXT.1.4

The TSF 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)

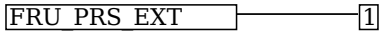
This Module defines the following extended components as part of the FRU class originally defined by CC Part 2:

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 TSF 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 TSF shall assign a priority to each type of communications packet that traverses the TSF.

FRU_PRS_EXT.1.2

The TSF 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)

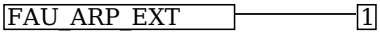
This Module defines the following extended components as part of the FAU class originally defined by CC Part 2:

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 TOE 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 Module. These requirements are not featured explicitly as SFRs and should not be included in the ST. They are not included as standalone SFRs because it would increase the time, cost, and complexity of evaluation. This approach is permitted by [CC] Part 1, 8.2 Dependencies between components.

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

Table 5: Implicitly Satisfied Requirements

Requirement	Rationale for Satisfaction
FMT_MSA.3 – Static Attribute Initialization	FDP_IFF.1 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 SFR has not been defined by this PP-Module because the enforcement of FDP_IFF.1 is not dependent on the initial state of security attributes. For example, FDP_IFF.1.2 requires the TSF 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 TSF determines “validity” in this case. 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 TSF. FDP_IFF.1.4 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 SFR whether the absence of a calling party from both the allowlist and the denylist means they are authorized or rejected by default.
FMT_SMR.1 – Security Roles	FCS_CKM.1 (which is defined in this PP-Module as FCS_CKM.1/VPN) requires FCS_CKM.4 to be claimed so that the generated keys are not disclosed through improper or nonexistent key destruction methods. Each of the supported Base-PPs except for the App PP define FCS_CKM_EXT.4 as an extended SFR, which defines key destruction functionality consistent with FCS_CKM.4, but with additional details that are specific to the respective technology types of the Base-PP. When the App PP is the Base-PP, this PP-Module defines its own instance of FCS_CKM_EXT.4 to achieve the same purpose. The dependency on FCS_CKM.4 is considered to be satisfied through the fact that a compliant TOE will always claim FCS_CKM_EXT.4, which is intended to satisfy the same purpose.

Appendix E - 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 VVoIP 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-dependent)	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 F - 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 G - Acronyms

Acronym	Meaning
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
IETF	Internet Engineering Task Force
IP-PBX	Internet Protocol Public Branch Exchange
ITU-T	ITU Telecommunication Standardization Sector
MGCP	Media Gateway Control Protocol
MOS	Mean Opinion Score
NAT	Network Address Translation
OE	Operational Environment
PP	Protection Profile
PP-Configuration	Protection Profile Configuration
PP-Module	Protection Profile Module
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RTCP	RTP Control Protocol
RTP	Real-Time Transport Protocol
SAR	Security Assurance Requirement
SDES	Security Descriptions for Media Streams
SDP	Session Description Protocol
SFR	Security Functional Requirement
SIP	Session Initiation Protocol
SRTP	Secure Real-Time Transport Protocol
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
TSS	TOE Summary Specification
VVoIP	Voice/Video Over IP

Appendix H - Bibliography

Identifier	Title
[CC]	Common Criteria for Information Technology Security Evaluation - • Part 1: Introduction and General Model, CCMB-2017-04-001, Version 3.1 Revision 5, April 2017. • Part 2: Security Functional Components, CCMB-2017-04-002, Version 3.1 Revision 5, April 2017. • Part 3: Security Assurance Components, CCMB-2017-04-003, Version 3.1 Revision 5, April 2017.
[NDcPP]	collaborative Protection Profile for Network Devices, Version 2.2e, March 23, 2020
[NDcPP SD]	Supporting Document - Evaluation Activities for Network Device cPP, Version 2.2, December 2019