Comment: Comment-1-

PP-Module for MACsec Ethernet Encryptions

Version: 1.0
2022-12-16
National Information Assurance Partnership

Revision History

Version	Date	Comment
1.0	2022-12-16	Initial Release

Contents

1 Introduction
1.1 Overview
1.2 Terms
1.2.1 Common Criteria Terms
1.2.2 Technical Terms
1.3 Compliant Targets of Evaluation
1.4 TOE Boundary
1.5 Use Cases
2 Conformance Claims
3 Security Problem Description
3.1 Threats
3.2 Assumptions
3.3 Organizational Security Policies
4 Security Objectives
4.1 Security Objectives for the TOE
4.2 Security Objectives for the Operational Environment
4.3 Security Objectives Rationale
5 Security Requirements
5.0.1 Security Audit (FAU)
5.0.2 Cryptographic Support (FCS)
5.0.3 User Data Protection (FDP)
5.0.4 Firewall (FFW)
5.0.5 Identification and Authentication (FIA)
5.0.6 Security Management (FMT)
5.0.7 Resource Utilization (FRU)
5.0.8 Trusted Path/Channels (FTP)
5.0.9 Trusted Path/Channels (FTP)
5.0.10 Identification and Authentication (FIA)
Appendix A - Implicitly Satisfied Requirements
Appendix B - Allocation of Requirements in Distributed TOEs
Appendix C - Entropy Documentation and Assessment

1.0 National Information Assurance Partnership 2022-12-16 MACsec Ethernet Encryption 1.0 2022-12-16 Initial Release

1 Introduction

1.1 Overview

The scope of this PP-Module is to describe the security functionality of Media Access Control Security (MACsec) encryption 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 MACsec encryption is a specific type of network device, and there is nothing about the implementation of MACsec that would prevent any of the security capabilities defined by the Base-PP from being satisfied.

A TOE that conforms to a PP-Configuration containing this PP-Module may be a 'Distributed TOE' as defined in the NDcPP. This PP-Module does not prohibit the TOE from implementing other security functionality in a distributed manner. For example, a TOE may be deployed in such a manner that distributed nodes establish MACsec connectivity with physically separated networks while a centralized management device is used to configure the behavior of individual nodes.

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 Functional Requirement (SFR)	A requirement for security enforcement by the TOE.
Security Target (ST)	A set of implementation-dependent security requirements for a specific product.
Target of Evaluation (TOE)	The product under evaluation.
TOE Security Functionality (TSF)	The security functionality of the product under evaluation.
TOE Summary Specification (TSS)	A description of how a TOE satisfies the SFRs in an ST.

1.2.2 Technical Terms

Carrier Ethernet	MEF Carrier Ethernet standards define technology-agnostic layer-2 services. The standards include services aimed at end users (Subscriber Ethernet Services) and service providers (Operator Ethernet Services). Other related terms include Metro Ethernet Services, Provider Bridging and Provider Backbone Bridging.
Connectivity Association Key (CAK)	A symmetric key that is used as the master key for MACsec connectivity and is shared between connected MACsec endpoints.
Connectivity Association Key Name (CKN)	A unique identifier for a specific Connectivity Association Key.
Ethernet Private Line (EPL)	A service transporting customer data form one User Network Interface (UNI) to another UNI.
Ethernet Virtual Private Line (EVPL)	A Virtual Local Area Network (VLAN) based service transporting customer data. The UNI is capable of service multiplexing.
Extended Packet Numbering	A scheme that allows MACsec communications to persist using a single Secure Association Key for a larger number of frames to reduce overhead and latency associated with key agreement.
Extensible Authentication Protocol over LAN (EAPOL)	A port authentication protocol specified in IEEE 802.1X that is used to facilitate network authentication.
MAC Security Entity	An entity (e.g. computer) that is implementing MACsec.
MACsec Key Agreement (MKA)	A key agreement protocol used for distribution of MACsec keys to distributed peers.
MACsec protocol Data Unit (MPDU)	The basic MACsec frame structure that contains protcol and payload data.
Media Access Control Security (MACsec)	A standard for connectionless data confidentiality and integrity protection at the data link layer of a network connection. Formally defined in IEEE 802.1AE.
Metro Ethernet Forum (MEF)	A non-profit international industry consortium.
Packet Number (PN)	A monotonically increasing value that is guranteed to be unique for each MACsec frame transmitted using a given Secure Association Key (SAK)

SecTag	MAC Security Tag - a protocol header comprising a number of octets, beginning with an EtherType, that is prepended to the service data unit supplied by the client of the protocol and is used to provide security guarantees.
Secure Association (SA)	A mechanism that uses a Secure Assocation Key (SAK) to provide the MACsec service guarantees and security services for a sequence of transmitted frames.
Secure Association Key (SAK)	A key derived from the CAK that is used to encrypt/decrypt traffic for a given SA.
Secure Channel (SC)	A unidirectional channel (one to one or one to many) that uses symmetric key cryptography to provide a (possibly long lived) Secure Channel.
Secure Device Identifier	A device authentication credential that can be used for EAPOL and is formally defined in IEEE 802.1AR.

1.3 Compliant Targets of Evaluation

This PP-Module specifically addresses MACsec, which allows authorized systems using Ethernet Transport to maintain confidentiality of transmitted data and to take measures against frames that are transmitted or modified by unauthorized devices.

MACsec protects communication between trusted components of the network infrastructure, thus protecting the network operation. It facilitates maintenance of correct network connectivity and services as well as isolation of denial of service attacks.

The hardware, firmware, and software of the MACsec device define the physical boundary. All of the security functionality is contained and executed within the physical boundary of the device. For example, given a device with an Ethernet card, the whole device is considered to be within the boundary.

Since this PP-Module builds on the NDcPP, conformant TOEs are obligated to 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

The physical boundary for a TOE that conforms to this PP-Module is a hardware appliance that also provides generalized network device functionality, such as auditing, I&A, and cryptographic services for network communications. The TOE’s logical boundary includes all functionality required by the claimed Base-PP as well as the MACsec functionality and related capabilities that are defined in this PP-Module. Any functionality that is provided by the network device that is not relevant to the security requirements defined by this PP-Module or the Base-PP is considered to be outside the scope of the TOE.

1.5 Use Cases

A pair of MACsec devices connected by a physical medium can protect Ethernet frames switched or routed from one device to the other. The two MACsec devices are provided with a Connectivity Association Key (CAK) and utilize the MACsec Key Agreement (MKA) protocol to create a secure tunnel. MKA is used by the two MACsec devices to agree upon MACsec keys. A policy should be installed to protect traffic between the devices, with the exception of the MKA or Ethernet control traffic such as EAP over LAN (EAPOL) frames.

This PP-Module defines two potential use cases for the MACsec TOE.

[USE CASE 1] Classic Hop by Hop Deployment

MACsec can be deployed in a hop by hop manner between Ethernet devices. Two devices will protect traffic originating in protected networks traversing an untrusted link between them. The devices will first exchange MKA frames, which serve to determine the peer is an authorized peer, and agree upon a shared key and MACsec cipher suite used to set up a transmit (Tx) Secure Association (SA) and a receive (Rx) SA. Once the SAs are set up, MACsec-protected frames traverse the unprotected link.

[USE CASE 2] Over Carrier Ethernet Services

In some markets network service providers have standardized their offerings according to various versions of the Metro Ethernet Forum (MEF) specifications. One recent MEF specification is the “E-Line” (*) service type which is based on the use of point to point Ethernet Virtual Circuits (EVCs). A port based service is known as an Ethernet Private Line and a VLAN based service is known as an Ethernet Virtual Private Line (EVPL). EPL provides a point-to-point Ethernet virtual connection (EVC) between a pair of dedicated user–network interfaces (UNIs), with a high degree of transparency. EVPL provides a point-to-point or point-to-multipoint connection between UNIs. A difference between the EVPL and EPL is the degree of transparency - while EPL is highly transparent, filtering only the pause frames, EVPL is required to either peer or drop most of the Layer 2 Control Protocols. The MEF has also defined other service types such as E-LAN and E-Tree.

(*) From MEF 6.3 – Subscriber Ethernet Services Definition – November 2019 – Table 3

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).

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

- PP-Module for Stateful Traffic Filter Firewalls Version 1.4 + Errata 20200625 (MOD_FW)
- PP-Module for Virtual Private Network (VPN) Gateways Version 1.2 (MOD_VPNGW) This previously said 1.1 but that has been sunset

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.DATA_INTEGRITY

An attacker may modify data transmitted over the layer 2 link in a way that is not detected by the recipient.

Devices on a network may be exposed to attacks that attempt to corrupt or modify data in transit without authorization. If malicious devices are able to modify and replay data that is transmitted over a layer 2 link, then the data contained within the communications may be susceptible to a loss of integrity.

T.NETWORK_ACCESS

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

A MACsec device may sit on the periphery of a network, which means that it may have an externally-facing interface to a public network. Devices located in the public network may attempt to exercise services located on the internal network that are intended to be accessed only from within the internal network or externally accessible only from specifically authorized devices. If the MACsec device allows unauthorized external devices access to the internal network, these devices on the internal network may be subject to compromise. Similarly, if two MACsec devices are deployed to facilitate end-to-end encryption of traffic that is contained within a single network, an attacker could use an insecure MACsec device as a method to access devices on a specific segment of that network such as an individual LAN.

T.UNTRUSTED_MACSEC_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.

A generic network device may be threatened by the use of insecure communications channels to transmit sensitive data. The attack surface of a MACsec device also includes the MACsec trusted channels. Inability to secure communications channels, or failure to do so correctly, would expose user data that is assumed to be secure to the threat of unauthorized disclosure.

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.AUTHENTICATION_MACSEC

To further address the issues associated with unauthorized disclosure of information, a compliant TOE's authentication ability (MKA) will allow a MACsec peer to establish connectivity associations (CA) with another MACsec peer. MACsec endpoints authenticate each other to ensure they are communicating with an authorized MAC Security Entity (SecY) entity.

Addressed by: FCS_MACSEC_EXT.4, FCS_MKA_EXT.1, FIA_PSK_EXT.1, FCS_DEVID_EXT.1 (selection-based), FCS_EAP-TLS_EXT.1 (selection-based)

O.AUTHORIZED_ADMINISTRATION

All network devices are expected to provide services that allow the security functionality of the device to be managed. The MACsec device, as a specific type of network device, has a refined set of management functions to address its specialized behavior. In order to further mitigate the threat of a compromise of its security functionality, the MACsec device prescribes the ability to limit brute-force authentication attempts by enforcing lockout of accounts that experience excessive failures and by limiting access to security-relevant data that administrators do not need to view.

Addressed by: FMT_SMF.1/MACSEC, FPT_CAK_EXT.1, FIA_AFL_EXT.1 (optional), FTP_TRP.1/MACSEC (optional), FMT_SNMP_EXT.1 (selection-based)

O.CRYPTOGRAPHIC_FUNCTIONS_MACSEC

To address the issues associated with unauthorized modification and disclosure of information, compliant TOEs will implement cryptographic capabilities. These capabilities are intended to maintain confidentiality and allow for detection and modification of data that is transmitted outside of the TOE.

Addressed by: FCS_COP.1/CMAC, FCS_COP.1/MACSEC, FCS_MACSEC_EXT.2, FCS_MACSEC_EXT.3, FTP_ITC.1/MACSEC, FTP_TRP.1/MACSEC (optional), FCS_SNMP_EXT.1 (selection-based)

O.PORT_FILTERING_MACSEC

To further address the issues associated with unauthorized network access, a compliant TOE's port filtering capability will restrict the flow of network traffic through the TOE based on layer 2 frame characteristics and whether or not the traffic represents valid MACsec frames and MACsec Key Agreement Protocol Data Units (MKPDUs).

Addressed by: FCS_MACSEC_EXT.1, FIA_PSK_EXT.1, FPT_DDP_EXT.1

O.REPLAY_DETECTION

A MACsec device is expected to help mitigate the threat of MACsec data integrity violations by providing a mechanism to detect and discard replayed traffic for MACsec protocol data units (MPDUs).

Addressed by: FPT_RPL.1, FPT_RPL_EXT.1 (optional)

O.SYSTEM_MONITORING_MACSEC

To address the issues of administrators being able to monitor the operations of the MACsec device, compliant TOEs will implement the ability to log the flow of Ethernet traffic. Specifically, the TOE will provide the means for administrators to configure rules to 'log' when Ethernet traffic grants or restricts access. As a result, the 'log' will result in informative event logs whenever a match occurs. In addition, the establishment of security CAs is auditable, not only between MACsec devices, but also with MAC Security Key Agreement Entities (KaYs).

Addressed by: FAU_GEN.1/MACSEC

O.TSF_INTEGRITY

To mitigate the security risk that the MACsec device may fail during startup, it is required to fail-secure in the event that any self-test failures occur during startup. This ensures that the device will only operate when it is in a known state.

Addressed by: FPT_FLS.1

4.2 Security Objectives for the Operational Environment

All objectives for the operational environment 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.DATA_INTEGRITY	O.CRYPTOGRAPHIC_FUNCTIONS_MACSEC	The TOE mitigates the threat of data integrity violations by implementing cryptographic functionality that includes integrity protection.
	O.REPLAY_DETECTION	The TOE mitigates the threat of data integrity violations by providing a mechanism to detect and discard replayed traffic for MPDUs.
T.NETWORK_ACCESS	O.PORT_FILTERING_MACSEC	The TOE's port filtering capability reduces the threat of unauthorized access to devices in the TOE's operational environment by restricting the flow of network traffic entering through the TOE interfaces based on layer 2 frame characteristics and whether or not the traffic represents valid MACsec frames and MKPDUs.
T.UNTRUSTED_MACSEC_COMMUNICATION_CHANNELS	O.CRYPTOGRAPHIC_FUNCTIONS_MACSEC	The TOE mitigates the threat of unauthorized disclosure of information via untrusted thru traffic by providing MKA authentication functions to authorize endpoints.

5 Security Requirements

https://www.niap-ccevs.org/profile/Info.cfm?PPID=447&id=447 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 MACsec functionality that is provided by the network device. The threats defined by this PP-Module (see section 3.1) supplement those defined in the NDcPP as follows: The threat of data integrity compromise at the layer 2 level is a specific threat that can be countered by MACsec technology. The threat of a malicious entity accessing protected network resources without authorization is a specific example of the T.UNTRUSTED_COMMUNICATION_CHANNELS threat defined in the Base-PP. The threat of disclosure of data in protected communications channels is the same as the T.UNTRUSTED_COMMUNICATION_CHANNELS threat in the NDcPP. This PP-Module expands on that by introducing additional logical interfaces (MACsec, SNMP) that this threat applies to. The Base-PP does not define any TOE objectives so PP-Module objectives do not conflict with it. The Base-PP does not define any TOE objectives so PP-Module objectives do not conflict with it. The Base-PP does not define any TOE objectives so PP-Module objectives do not conflict with it. The Base-PP does not define any TOE objectives so PP-Module objectives do not conflict with it. The Base-PP does not define any TOE objectives so PP-Module objectives do not conflict with it. The Base-PP does not define any TOE objectives so PP-Module objectives do not conflict with it. The Base-PP does not define any TOE objectives so PP-Module objectives do not conflict with it.

5.0.1 Security Audit (FAU)

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 administrative actions;**
d. **[*Specifically defined auditable events listed in the Auditable Events table (Table 2)*]**

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
		Rule relevant to observed traffic
		Result of rule evaluation
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 service 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 #1: 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 (if applicable), and the outcome (success or failure) of the event; and
b. For each audit event type, based on the auditable event definitions of the functional components included in the PP-**Module**/ST, [*information specified in column three of the Auditable Events table (Table 2)*].

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.

5.0.2 Cryptographic Support (FCS)

FCS_COP.1/CMAC Cryptographic Operation (AES-CMAC Keyed Hash Algorithm)

FCS_COP.1.1/CMAC

The TSF shall perform [*keyed-hash message authentication*] in accordance with a specified cryptographic algorithm [*AES-CMAC*] and cryptographic key sizes **[selection: *128*, *256*] bits and message digest size of 128 bits** that meets the following: [*NIST SP 800-38B*].

Application Note #2: AES-CMAC is a keyed hash function that is used as part of the key derivation function (KDF) that is used for key generation.

Evaluation Activities

FCS_COP.1/CMAC
TSS
The evaluator shall examine the TSS to ensure that it specifies the following values used by the AES-CMAC function: key length, hash function used, block size, and output MAC length.

Guidance
There are no guidance EAs for this component.

Tests
The evaluator shall perform the following tests:

- *Test 1:* ***CMAC Generation Test***
  To test the generation capability of AES-CMAC, the evaluator shall provide to the TSF, for each key length-message length-CMAC length tuple (in bytes), a set of 8 arbitrary key-plaintext tuples that will result in the generation of a known MAC value when encrypted. The evaluator will then verify that the correct MAC was generated in each case.
- *Test 2:* ***CMAC Verifictaion Test***
  To test the verification capability of AES-CMAC, the evaluator shall provide to the TSF, for each key length-message length-CMAC length tuple (in bytes), a set of 20 arbitrary key-MAC tuples that will result in the generation of known messages when verified. The evaluator will then verify that the correct message was generated in each case.

  The following information should be used by the evaluator to determine the key length-message length-CMAC length tuples that should be tested:

  - *Key length: values will include the following:*
    - *16*
    - *32*

- *Message length: values will include the following:*
  - *0 (optional)*
  - *Largest value supported by the implementation (no greater than 65536)*
  - *Two values divisible by 16*
  - *Two values not divisible by 16*
- *CMAC length:*
  - *Smallest value supported by the implementation (no less than 1)*
  - *16*
  - *Any supported CMAC length between the minimum and maximum values*

FCS_COP.1/MACSEC Cryptographic Operation (MACsec AES Data Encryption/Decryption)

FCS_COP.1.1/MACSEC

The TSF shall perform [*encryption/decryption*] in accordance with a specified cryptographic algorithm [*AES used in AES Key Wrap, GCM*] and cryptographic key sizes **[selection: *128, 256*] bits** that meets the following: [*AES as specified in ISO 18033-3, AES Key Wrap as specified in NIST SP 800-38F, GCM as specified in ISO 19772*].

Evaluation Activities

FCS_COP.1/MACSEC

FCS_MACSEC_EXT.1 MACsec

FCS_MACSEC_EXT.1.1

The TSF shall implement MACsec in accordance with IEEE Standard 802.1AE-2018.

FCS_MACSEC_EXT.1.2

The TSF shall derive a Secure Channel Identifier (SCI) from a peer's MAC address and port to uniquely identify the originator of a MACsec Protocol Data Unit (MPDU).

FCS_MACSEC_EXT.1.3

The TSF shall reject any MPDUs during a given session that contain an SCI other than the one used to establish that session.

FCS_MACSEC_EXT.1.4

The TSF shall permit only EAPOL (PAE EtherType 88-8E), MACsec frames (EtherType 88-E5), control frames (EtherType 88-08) and [**assignment**: *specific VLAN tag frames*] and discard others.

Application Note #3: Depending on the Carrier Ethernet service provider a TOE might need basic VLAN tag handling abilities such as a simple add or discard to be suitable for Use Case 2.

Evaluation Activities

FCS_MACSEC_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 RTP Control Protocol (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, 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.

FCS_MACSEC_EXT.2 MACsec Integrity and Confidentiality

FCS_MACSEC_EXT.2.1

The TOE shall implement MACsec with support for integrity protection with a confidentiality offset of [**selection**: *0*, *30*, *50*].

FCS_MACSEC_EXT.2.2

The TSF shall provide assurance of the integrity of protocol data units (MPDUs) using an Integrity Check Value (ICV) derived with the Secure Association Key (SAK).

Application Note #4: The length of the ICV is dependent on the cipher suite used but will not be less than 8 octets or more than 16 octets at the end of the MPDU. The ICV protects the destination and source MAC address parameters, as well as all the fields of the MPDU.

FCS_MACSEC_EXT.2.3

The TSF shall provide the ability to derive an Integrity Check Value Key (ICK) from a CAK using a KDF.

Evaluation Activities

FCS_MACSEC_EXT.2
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 RTP Control Protocol (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, 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.

FCS_MACSEC_EXT.3 MACsec Randomness

FCS_MACSEC_EXT.3.1

The TSF shall generate unique Secure Association Keys (SAKs) using [**assignment**: *key generation or derivation method*] such that the likelihood of a repeating SAK is no less than 1 in 2 to the power of the size of the generated key.

FCS_MACSEC_EXT.3.2

The TSF shall generate unique nonce for the derivation of SAKs using the TOE's random bit generator as specified by FCS_RBG_EXT.1.

Application Note #5: FCS_RBG_EXT.1 is defined in the Base-PP so a conformant MACsec TOE will include this dependency.

Evaluation Activities

FCS_MACSEC_EXT.3
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 RTP Control Protocol (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, 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.

FCS_MACSEC_EXT.4 MACsec Key Usage

FCS_MACSEC_EXT.4.1

The TSF shall support peer authentication using pre-shared keys [**selection**: *EAP-TLS with DevIDs*, *no other method*].

Application Note #6: The definition of the peer's CAK as defined by IEEE 802.1X-2010 is synonymous with the peer authentication performed here. If EAP-TLS with DevIDs is selected, the FCS_DEVID_EXT.1 and FCS_EAPTLS_EXT.1 SFRs defined in must be claimed.

FCS_MACSEC_EXT.4.2

The TSF shall distribute SAKs between MACsec peers using AES key wrap as specified in FCS_COP.1**/MACSEC**.

Application Note #7: This requirement applies to the SAKs that are generated by the TOE. They must be wrapped by the AES Key Wrap method specified in NIST SP 800-38F.

FCS_MACSEC_EXT.4.3

The TSF shall support specifying a lifetime for CAKs.

FCS_MACSEC_EXT.4.4

The TSF shall associate Connectivity Association Key Names (CKNs) with Secure Association Key (SAK)s that are defined by the key derivation function using the CAK as input data (per IEEE 802.1X-2010, Section 9.8.1).

FCS_MACSEC_EXT.4.5

The TSF shall associate Connectivity Association Key Names (CKNs) with CAKs. The length of the CKN shall be an integer number of octets, between 1 and 32 (inclusive).

Evaluation Activities

FCS_MACSEC_EXT.4
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 RTP Control Protocol (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, 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.

5.0.3 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
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 3: Configure a custom 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 4: 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. Verify calls from another IP address or subnet cannot be completed.*
- *Test 5: 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 6: Configure a custom ACL to only permit a call destined to 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 7: 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) 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 8: 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) 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 9: 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 10: 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 endpoints; however, keep the calling number the same. Attempt a call through the TOE from new IP addresses. Verify that the calls cannot complete.*
- *Test 11: 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 12: 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 endpoints; however, keep the calling number the same. Attempt a call through the TOE from new IP addresses. Verify that the calls can complete.*

5.0.4 Firewall (FFW)

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 versus virtual or trust zone, e.g., trusted versus untrusted)**
- [*Application (Real-Time Communications Protocol)*
  - *signaling protocols: [**selection**: SIP, H.323]]*

Application Note #8: 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 #9: 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 or 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 being full to the point where they 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 test:

The evaluator shall attempt to get network traffic to flow through the TOE while the TOE is being initialized. A steady flow of network packets that would otherwise be denied by the ruleset should be sourced and directed to a host. The evaluator shall 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 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 or virtual or trust zone, e.g., trusted or 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 13: 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 14: Repeat Test 13 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 determining the validity of a session: 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 determining the validity of a session: 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 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 15: 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 attributes for determining the validity of a session (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 16: The evaluator shall terminate the TCP session established per Test 15 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 17: The evaluator shall expire (i.e., reach timeout) the TCP session established per Test 15 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 18: 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 attributes for determining the validity of a session (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 19: The evaluator shall expire (i.e., reach timeout) the UDP session established per Test 18 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 20: 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 21: 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 versus 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 #10: 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 #11: 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 #12: 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 22: [conditional, if "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 23: [conditional, if "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 24: [conditional, if "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 25: [conditional, if "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 it 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 26: 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 27: 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 #13: 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 RTP Control Protocol (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, 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.

5.0.5 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 28: 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 and 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 29: Repeat Test 28 but provide incorrect username and 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 30: Repeat Test 28 but change the IP address of the trunk peer and verify via packet capture and audit log that the session was not established.*

5.0.6 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 #14: This SFR defines additional management functions for the TOE beyond what is defined in the Base-PP as FMT_SMF.1. The TOE may have all management functionality implemented in the same logical interface; it is not necessary for “network device management” and “SBC management” to be implemented in separate interfaces. This PP-Module may rely on management functionality defined in the Base-PP to support the implementation of its functions. For example, the SBC portion of the TOE relies on the reliable time function that must be implemented by the Base-PP portion of the TOE. If the Base-PP implements this using NTP, the “Ability to set the time which is used for time-stamps” or “Ability to configure NTP” management function defined in FMT_SMF.1 in the Base-PP can be used to address this PP-Module’s dependency on reliable system time. Note that support for NTP is recommended but not required.

The 'configurable auditable events' function relates to FAU_SEL.1, specifically with respect to allowing a Security Administrator to determine whether a given event is auditable. As this refers to the events for the triggering of various filtering rules, it may be implicitly addressed through the ‘configure traffic filtering rules’ function, for example by explicitly defining a rule with a type that automatically requires it to be logged or a parameter that causes it to be logged if triggered.

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.

5.0.7 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 31: 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 32: 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) 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 #15: The intent of this SFR is for the TOE to be resistant to DoS 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 33: 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 34: 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 35: 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.*

5.0.8 Trusted Path/Channels (FTP)

FTP_ITC.1/ARP Inter-TSF Trusted Channel (Automatic Response)

FTP_ITC.1.1/ARP

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

FTP_ITC.1.2/ARP

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

FTP_ITC.1.3/ARP

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

Application Note #16: This SFR is used to specify any trusted protocols that are implemented in support of FAU_ARP_EXT.1.

Evaluation Activities

FTP_ITC.1/ARP
The evaluator shall evaluate this SFR in the manner specified for FTP_ITC.1 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.

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 #17: 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 #18: 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.

5.0.9 Trusted Path/Channels (FTP)

FTP_ITC.1/H323 Inter-TSF Trusted Channel (H.323 Communications)

The inclusion of this selection-based component depends upon selection in FFW_ACL_EXT.1.2, FFW_ACL_EXT.2.1, FFW_DPI_EXT.1.1, FIA_SIPS_EXT.1.1.

FTP_ITC.1.1/H323

The TSF shall provide 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 #19: FCS_IPSEC_EXT.1, FCS_TLSC_EXT.1, and FCS_TLSC_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 #20: 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.

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.

5.0.10 Identification and Authentication (FIA)

FIA_SIPS_EXT.1 Session Initiation Protocol Registration

FIA_SIPS_EXT.1.1

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

Application Note #21: 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 #22: This SFR is optional because this functionality is not standard for SBCs because device registration can generally be handled by an ESC in the TOE's OE. However, in some cases, SIP registration directly to the SBC is required. If an SBC advertises this service, it is expected that this functionality be included within the TOE boundary. This SFR is therefore implementation-based on whether the SBC has the capability to perform its own SIP registration of devices.

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 36: 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 37: 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 38: 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.*

  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 A - Implicitly Satisfied Requirements

This appendix lists requirements that should be considered satisfied by products successfully evaluated against this PP-Module. These requirements are not featured explicitly as 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-Module provides evidence that these controls are present and have been evaluated.

Table 3: 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.

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

Appendix C - 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. [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 [MOD_FW] PP-Module for Stateful Traffic Filter Firewalls, Version 1.4 + Errata 20200625, June 25, 2020 [MOD_VPNGW] PP-Module for VPN Gateways, Version 1.2, March 31, 2022