Supporting Document
Mandatory Technical Document

PP-Module for Session Border Controllers
Version: 1.0
2022-09-09
National Information Assurance Partnership

Foreword

This is a Supporting Document (SD), intended to complement the Common Criteria version 3 and the associated Common Evaluation Methodology for Information Technology Security Evaluation.

SDs may be “Guidance Documents”, that highlight specific approaches and application of the standard to areas where no mutual recognition of its application is required, and as such, are not of normative nature, or “Mandatory Technical Documents”, whose application is mandatory for evaluations whose scope is covered by that of the SD. The usage of the latter class is not only mandatory, but certificates issued as a result of their application are recognized under the CCRA.

Technical Editor:
National Information Assurance Partnership (NIAP)

Document history:

Version	Date	Comment
1.0	2022-08-12	Initial Release

General Purpose:
The purpose of this SD is to define evaluation methods for the functional behavior of Session Border Controller products.

Acknowledgments:
This SD was developed with support from NIAP Session Border Controllers Technical Community members, with representatives from industry, government agencies, Common Criteria Test Laboratories, and members of academia.

Table of Contents

1 Introduction

1.1 Technology Area and Scope of Supporting Document

The scope of the PP-Module for Session Border Controllers is to describe the security functionality of Session Border Controllers products in terms of [CC] and to define functional and assurance requirements for them. The PP-Module is intended for use with the following Base-PP:

- Network Device, version 2.2e

This SD is mandatory for evaluations of TOEs that claim conformance to a PP-Configuration that includes the PP-Module for :

- Session Border Controllers, Version 1.0

As such it defines Evaluation Activities for the functionality described in the PP-Module as well as any impacts to the Evaluation Activities to the Base-PP(s) it modifies.

Although Evaluation Activities are defined mainly for the evaluators to follow, in general they also help developers to prepare for evaluation by identifying specific requirements for their TOE. The specific requirements in Evaluation Activities may in some cases clarify the meaning of Security Functional Requirements (SFR), and may identify particular requirements for the content of Security Targets (ST) (especially the TOE Summary Specification), user guidance documentation, and possibly supplementary information (e.g. for entropy analysis or cryptographic key management architecture).

1.2 Structure of the Document

Evaluation Activities can be defined for both SFRs and Security Assurance Requirements (SAR), which are themselves defined in separate sections of the SD.

If any Evaluation Activity cannot be successfully completed in an evaluation, then the overall verdict for the evaluation is a 'fail'. In rare cases there may be acceptable reasons why an Evaluation Activity may be modified or deemed not applicable for a particular TOE, but this must be approved by the Certification Body for the evaluation.

In general, if all Evaluation Activities (for both SFRs and SARs) are successfully completed in an evaluation then it would be expected that the overall verdict for the evaluation is a ‘pass’. To reach a ‘fail’ verdict when the Evaluation Activities have been successfully completed would require a specific justification from the evaluator as to why the Evaluation Activities were not sufficient for that TOE.

Similarly, at the more granular level of assurance components, if the Evaluation Activities for an assurance component and all of its related SFR Evaluation Activities are successfully completed in an evaluation then it would be expected that the verdict for the assurance component is a ‘pass’. To reach a ‘fail’ verdict for the assurance component when these Evaluation Activities have been successfully completed would require a specific justification from the evaluator as to why the Evaluation Activities were not sufficient for that TOE.

1.3 Terms

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

1.3.1 Common Criteria Terms

Assurance	Grounds for confidence that a TOE meets the SFRs [CC].
Base Protection Profile (Base-	Protection Profile used as a basis to build a PP-Configuration.

PP)	
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.

1.3.2 Technical Terms

Enterprise Session Controller (ESC)	A voice/video over IP (VVoIP) infrastructure device that is used to set up and tear down calls between VVoIP endpoints.
H.323	A communications protocol defined by the ITU Telecommunications Standardization Sector (ITU-T) that is used for creating, modifying, and terminating multimedia sessions with multiple participants.
Media Gateway Control Protocol	A means of communication between a media gateway and a media gateway controller.

(MGCP)

Secure Real-Time Transport Protocol (SRTP)	A protocol that is used to provide multimedia (voice/video) streaming services with added security of encryption, message authentication and integrity, and replay protection.
Session Initiation Protocol (SIP)	A communications protocol defined by the Internet Engineering Task Force (IETF) that is used for creating, modifying, and terminating multimedia sessions with multiple participants.

2 Evaluation Activities for SFRs

The EAs presented in this section capture the actions the evaluator performs to address technology specific aspects covering specific SARs (e.g. ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, and ATE_IND.1) – this is in addition to the CEM workunits that are performed in Section 3 Evaluation Activities for SARs.

Regarding design descriptions (designated by the subsections labeled TSS, as well as any required supplementary material that may be treated as proprietary), the evaluator must ensure there is specific information that satisfies the EA. For findings regarding the TSS section, the evaluator's verdicts will be associated with the CEM workunit ASE_TSS.1-1. Evaluator verdicts associated with the supplementary evidence will also be associated with ASE_TSS.1-1, since the requirement to provide such evidence is specified in ASE in the PP.

For ensuring the guidance documentation provides sufficient information for the administrators/users as it pertains to SFRs, the evaluator's verdicts will be associated with CEM workunits ADV_FSP.1-7, AGD_OPE.1-4, and AGD_OPE.1-5.

Finally, the subsection labeled Tests is where the authors have determined that testing of the product in the context of the associated SFR is necessary. While the evaluator is expected to develop tests, there may be instances where it is more practical for the developer to construct tests, or where the developer may have existing tests. Therefore, it is acceptable for the evaluator to witness developer-generated tests in lieu of executing the tests. In this case, the evaluator must ensure the developer's tests are executing both in the manner declared by the developer and as mandated by the EA. The CEM workunits that are associated with the EAs specified in this section are: ATE_IND.1-3, ATE_IND.1-4, ATE_IND.1-5, ATE_IND.1-6, and ATE_IND.1-7.

2.1 Collaborative Protection Profile for Network Devices

The EAs defined in this section are only applicable in cases where the TOE claims conformance to a PP-Configuration that includes the NDcPP.

2.1.1 Modified SFRs

2.1.1.1 Cryptographic Support (FCS)

FCS_TLSC_EXT.1 TLS Client Protocol without Mutual Authentication

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

FCS_TLSS_EXT.2 TLS Server Support for Mutual Authentication

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

2.1.1.2 Identification and Authentication (FIA)

FIA_X509_EXT.1/Rev X.509 Certificate Validation

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

2.1.1.3 Trusted Path/Channels (FTP)

FTP_ITC.1 Inter-TSF Trusted Channel

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.

2.2 TOE SFR Evaluation Activities

2.2.1 Security Audit (FAU)

FAU_ARP_EXT.1 Security Audit Automatic Response

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/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
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.

FAU_SEL.1 Selective Audit

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 the 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 and 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.

2.2.2 Cryptographic Support (FCS)

FCS_SRTP_EXT.1 Secure Real-Time Transport Protocol

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

- Support the use of SRTP and the ciphersuites that are supported by the SRTP implementation.
- Disable the SRTP NULL algorithm automatically or provide the ability for it to be disabled by a Security Administrator.
- 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:

- How to configure the ciphersuites used by SRTP.
- [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.
- How to specify the ports used for SRTP communications.

Tests

The evaluator shall perform the following tests: [JF] Testlists do not appear to be working properly with the current transforms - the tests below are 1.1 through 1.3 rather than being 1-3. The next testlist, in FDP_IFF.1, is tests 2.1 through 2.10 rather than restarting at 1.

- Test 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 ciphersuite supported for the SRTP implementation.
- Test 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 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.

2.2.3 User Data Protection (FDP)

FDP_IFC.1 Subset Information Flow Control

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
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 4: 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 5: 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 6: 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 7: 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 8: 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 9: 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 10: 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 11: 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 12: 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 13: 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.

2.2.4 Firewall (FFW)

FFW_ACL_EXT.1 Real-Time Communications Traffic Filtering

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 14: 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 15: 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 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 16: 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 17: 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 18: 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 19: 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 20: 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 21: 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 22: 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
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 23: [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 24: [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 25: [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 26: [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 27: 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 28: 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
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
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.

2.2.5 Identification and Authentication (FIA)

FIA_SIPT_EXT.1 Session Initiation Protocol Trunking

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 29: 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 30: Repeat Test 1 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 31: 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.

2.2.6 Security Management (FMT)

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

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.

2.2.7 Resource Utilization (FRU)

FRU_PRS_EXT.1 Limited Priority of Service

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 32: 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 33: 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
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 34: 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 35: 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 36: 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.

2.2.8 Trusted Path/Channels (FTP)

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

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/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.

2.3 Evaluation Activities for Optional SFRs

The PP-Module does not define any optional requirements.

2.4 Evaluation Activities for Selection-Based SFRs

2.4.1 Trusted Path/Channels (FTP)

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

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.

2.5 Evaluation Activities for Objective SFRs

The PP-Module does not define any objective requirements.

3 Evaluation Activities for SARs

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

4 Required Supplementary Information

This Supporting Document has no required supplementary information beyond the ST, operational guidance, and testing.

Appendix A - References

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