Network Device Collaborative Protection Profile (NDcPP) Extended Package
Session Border Controller

July 24, 2015
Version 1

Table of Contents

1 Introduction

This Extended Package (EP) describes the security requirements for a Session Border Controller (SBC) and provides a minimal baseline set of requirements targeted at mitigating well defined threats. This EP is not in itself complete, but rather extends the Security Requirements for Network Devices collaborative Protection Profile (NDcPP). However, this introduction will describe the features of a compliant Target of Evaluation (TOE), and will also discuss how this EP is to be used in conjunction with the NDcPP. Since this PP is designated for Session Border Controllers, the Target of Evaluation (TOE) is the Session Border Controller (SBC) and the terms "SBC" and "TOE" are used interchangeably within this document.

1.1 Conformance Claims

The Security Requirements for Network Devices collaborative Protection Profile (NDcPP) define the baseline Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) for network infrastructure devices in general. This EP extends the NDPP baseline with additional SFRs and associated "Assurance Activities" that are specific to SBC. Assurance Activities are the actions that the evaluator performs in order to determine a TOE's compliance to the SFRs.

This EP conforms to Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4. It is CC Part 2 extended and CC Part 3 conformant.

1.2 How to Use This Extended Package

As an EP of the NDcPP, it is expected that the content of both this EP and the NDcPP are appropriately combined in the context of each product-specific Security Target. This EP has been specifically defined so that it is possible to define a Target of Evaluation (TOE) that contains the security functional requirements (SFRs) of both the NDcPP and this EP without contradictions or ambiguities. An ST must identify the applicable versions of the NDcPP (see http://www.niap-ccevs.org/pp/ for the current version) and this EP in its conformance claims.

1.3 Compliant Targets of Evaluations

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

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

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

Since this EP builds on the NDcPP, conformant TOEs are obligated to implement the functionality required in the NDcPP along with the additional functionality defined in this EP in response to the threat environment discussed later in this document.

1.4 Deployment Scenario

An SBC is a security device composed of hardware and software connected to two or more distinct voice networks that provides security and interoperability functions. SBCs are deployed between peering service provider networks, service provider networks and enterprise networks, or service provider networks and residential customers.

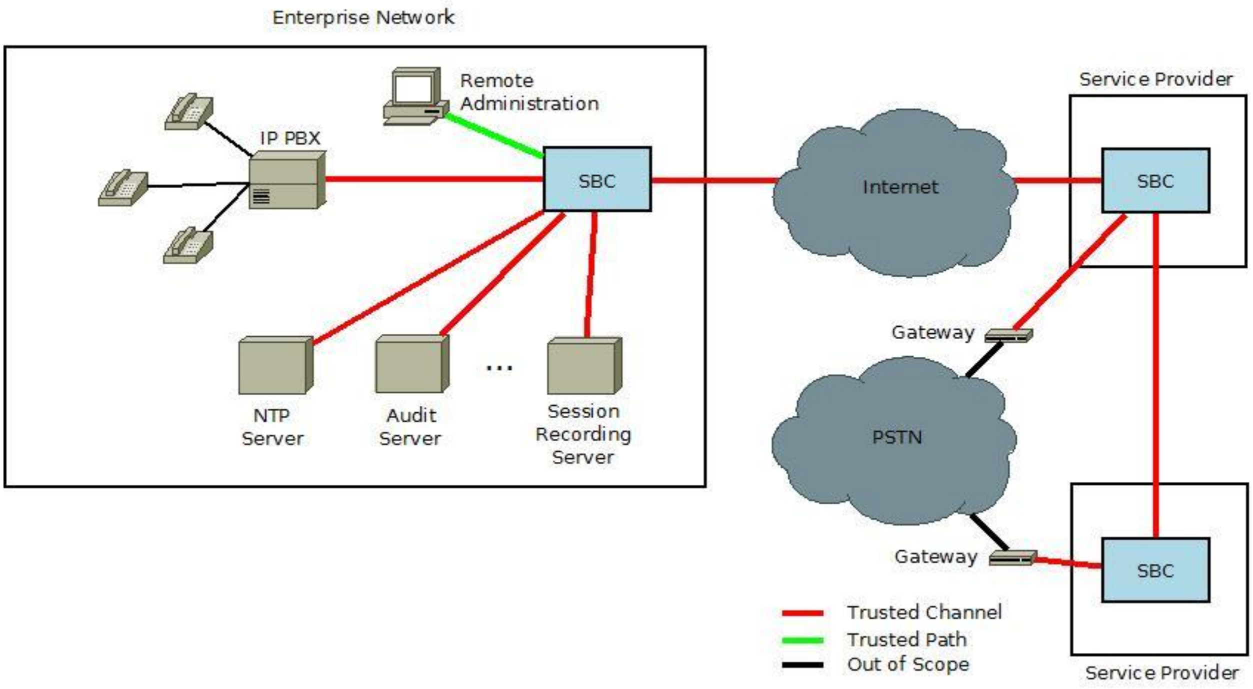

Figure 1: SBC Deployment Model

2 Security Problem Description

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

This EP details the functional requirements and threats specific to an SBC. Additional functional requirements pertaining to the SBC, functioning as a network device, are specified in the NDcPP and are not repeated here. Even though those functional requirements are not specified in this EP, they all apply, unless explicitly excluded.

2.1 Threats

As an extension to the Network Device cPP, the SBC will face the same threats that apply generally to all network devices. However, due to the specialized nature of the traffic handled by the SBC, some of these threats are applicable in a more specific context.

2.1.1 Unauthorized Disclosure of Information

Devices on a protected network may be exposed to threats presented by devices located outside the protected network, which may attempt to conduct unauthorized activities. If known malicious external devices are able to communicate with devices on the protected network, or if devices on the protected network can establish communications with those external devices, then those internal devices may be susceptible to the unauthorized disclosure of their identifying information or available network services. The SBC serves as a back-to-back user agent (B2BUA) that prevents outside entities from directly communicating with internal (or protected) entities. The SBC acts as a proxy wherein the only way an outside entity can communicate with a protected entity is by asking the SBC to communicate with the protected entity on its behalf. The SBC will maintain two separate connections: one with the outside entity and one with the protected entity to facilitate communications. Additionally, access can be limited to only specific source addresses and ports so that specific networks or network nodes can be blocked from accessing a protected network; thereby limiting the potential disclosure of information.

T.NETWORK_DISCLOSURE An attacker may attempt to “map” a subnet to determine the devices that reside on the network and to obtain the IP addresses of machines as well as the services (ports) those machines are offering. This information could be used to mount attacks to those machines via the services that are exposed.

2.1.3 Malicious Traffic

The SBC also provides protection against malicious or malformed packets. Malformed packets could cause the TOE, or the devices it protects, to grant unauthorized access or create a Denial of Service (DoS).

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

2.1.4 Untrusted Communication Channels

A generic network device may be threatened by the use of insecure communications channels to transmit sensitive data. The SBC's attack surface also includes secure communications that are specific to the user data that is transmitted through the TOE. 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.

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

2.1.5 Network Access

The SBC, as a device that sits on the periphery of a network, has 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 SBC allows unauthorized external devices to the internal network, devices on the internal network may be subject to compromise.

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.

2.1.6 User Data Reuse

As part of operating as a B2BUA, the SBC is responsible for ensuring that communications from remote entities are directed only to the appropriate recipient(s). Failure to do so would cause an inadvertent disclosure of user data that transits the TOE.

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

2.1.7 Resource Exhaustion

A SBC is responsible for facilitating communications between devices in the Operational Environment. However, the SBC has a limited pool of resources that it can use to perform this task. If these resources were exhausted by malicious means, the SBC would be unable to facilitate VoIP communications.

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

2.2 Assumptions

The assumptions defined for the SBC's Operational Environment are identical to those defined by the NDcPP, with the following exception:

The A.NO_THRU_TRAFFIC_PROTECTION assumption defined in the NDcPP does not apply to this EP. The SBC is intended to provide deep packet inspection (DPI) on traffic traversing its interfaces. DPI provides protection for the destined recipient and protection for itself against malicious traffic. The SBC also serves as the encryption endpoint. The SBC must correctly decrypt and protect traffic entering its interfaces and re-encrypt and protect traffic exiting its interfaces.

3 Security Objectives

3.1 Security Objectives for the TOE

The threats described in section 2 will be mitigated by a combination of TOE functionality and characteristics of the TOE's operational environment. Compliant TOEs will provide security functionality that address threats to the TOE and enforce any policies that are imposed by law or regulation. The following subsections provide a description of the security objectives required to meet the threats and policies previously discussed.

Note: Specific security objectives are identified (highlighted by *O.*) in each subsection below and are matched with the associated Security Functional Requirements (SFRs) that provide the mechanisms to satisfy the objectives. These include SFRs defined specifically for this EP (see section 4.2.2) as well as SFRs from the base NDcPP that are either refined in this EP or were optional in the base NDcPP but are mandatory for this EP (see section 4.2.1).

3.1.1 System Monitoring

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

(O.SYSTEM_MONITORING: FAU_ARP.1, FAU_GEN.1, FAU_SAA.1, FPT_STM.1)

3.1.2 Protected Communications

To mitigate the threat of data-in-transit disclosure, the SBC must ensure that remote communications are secured using appropriate means. This includes the security of VoIP signaling and media channels and SIP trunking, in addition to any secure communications channels that are prescribed by the base NDcPP (such as communication with audit, authentication, and/or update servers, as well as remote administrative interfaces).

(O.PROTECTED_COMMUNICATIONS: FCS_COP.1(1), FCS_DTLS_EXT.1, FCS_IPSEC_EXT.1, FCS_SRTP_EXT.1, FIA_SIPT_EXT.1, FCS_TLSC_EXT.2, FCS_TLSS_EXT.2, FTP_ITC.1, FTP_ITC.1(2), FTP_ITC.1(3), FTP_ITC.1(4))

3.1.3 Topology Hiding

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

(O.TOPOLOGY_HIDING: FDP_IFC.1, FDP_IFF.1, FFW_NAT_EXT.1)

3.1.4 Traffic Filtering

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

(O.TRAFFIC_FILTERING: FFW_ACL_EXT.1, FFW_ACL_EXT.2, FFW_DPI_EXT.1)

3.1.5 User Data Delivery

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

(O.USER_DATA_DELIVERY: FDP_IFC.1, FDP_IFF.1, FFW_NAT_EXT.1, FIA_SIPS_EXT.1, FIA_SIPT_EXT.1)

3.1.6 Resource Availability

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

(O.RESOURCE_AVAILABILITY: FRU_PRS_EXT.1, FRU_RSA.1)

3.1.7 Authorized Administration

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

(O.AUTHORIZED_ADMINISTRATION: FMT_SMF.1)

3.2 Security Objectives for the Operational Environment

The security objectives for the operational environment for this EP are the same as the security objectives for the operational environment of the base NDcPP with the exception of OE.NO_THRU_TRAFFIC_PROTECTION, which is excluded from this EP. The SBC provides through-traffic protection.

4 Security Requirements

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

4.1 Conventions

The CC defines operations on Security Functional Requirements: assignments, selections, assignments within selections and refinements. This document uses the following font conventions to identify the operations defined by the CC:

- Assignment: Indicated with italicized text;
- Refinement made by EP author: Indicated with bold text;
- Selection: Indicated with underlined text;
- Assignment within a Selection: Indicated with italicized and underlined text;
- Iteration: Indicated by appending the iteration number in parenthesis, e.g., (1), (2), (3); and
- Extended SFRs are identified by having a label "EXT" after the requirement name for TOE SFRs.

4.2 TOE Security Functional Requirements

Because this EP Extends the NDcPP, it is expected that the security functions that are defined in the base PP are inherited by this EP. For those functions that are defined in the NDcPP but are specified in more detail in this EP, the updated SFRs have been listed in section 4.2.1 below.

4.2.1 NDcPP Security Functional Requirement Direction

This section instructs the ST author on what selections must be made to certain SFRs contained in the NDcPP in order to satisfy the security objectives defined in this EP, or to mitigate a threat in a more specific or restrictive manner than is specified in the base PP.

This instruction describes the element where the mandatory selection has been made. The ST author may complete the remaining selection items as they wish, to ensure specific capabilities or behavior is present in the TOE.

Full assurance activities are not repeated for the requirements in this section; only the additional testing needed to supplement what has already been captured in the NDcPP is included. As the evaluator assesses the ST and TOE against the SFR, it is important that the proper selections have been made and the appropriate tests are performed to demonstrate compliance to the requirements.

4.2.1.2 FAU_GEN.1 Audit Data Generation

The NDcPP defines the set of auditable events that are required to be implemented by the TOE. This EP introduces additional functionality which necessitates the inclusion of additional auditable events. The following events must be combined with those of the NDcPP to conform to the Security Target.

The following auditable events are required for this EP:

SFR	Auditable Event	Additional Audit Record Contents
FIA_SIPS_EXT.1	Call Detail Record (CDR)	Calling party Called party Start time of the call Call duration Call type
FDP_IFF.1	Any modifications to the back-to-back user agent SFP	None
FFW_ACL_EXT.1	Configuration of VoIP traffic filtering rules	Information uniquely identifying the rule(s) that was modified
FIA_SIPS_EXT.1	All SIP REGISTER function requests	None
FIA_SIPT_EXT.1	All SIP trunk authentication attempts	Username and IP address of the service provider
FTP_ITC.1(2)	Initiation of the trusted channel, termination of the trusted channel, failure of the trusted channel functions	Identification of the initiator and target of the trusted channel
FTP_ITC.1(3)	Initiation of the trusted channel, termination of the trusted channel, failure of the trusted channel functions	Identification of the initiator and target of the trusted channel
FTP_ITC.1(4)	Initiation of the trusted channel, termination of the trusted channel, failure of the trusted channel functions	Identification of the initiator and target of the trusted channel

Table 1 - Auditable Events

The ST author may optionally also define environmental conditions, such as temperature violations, if the TOE claims the ability to detect this as a potential security violation in FAU_SAA.1.

Additionally, where the NDcPP requires "all administrative actions" to be audited, the ST author shall include the administrative actions that support this EP in the assignment text.

Application Note: A CDR shall 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.

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

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

This SFR is already mandated for the NDcPP but is also mentioned in this EP due to the additional implementation of AES by a SBC TOE in order to serve as a media encryption endpoint that is able to decrypt and re-encrypt call data that is traveling through the TSF.

Assurance Activity
No additional testing is required for this SFR unless the AES implementation used by the SBC functionality of the TOE uses a different cryptographic algorithm implementation. If this is the case, then the evaluator shall repeat the assurance activity defined in the NDcPP for this SFR for the new algorithm implementation.

4.2.1.4 FCS_IPSEC_EXT.1 IPsec

This SFR is optional in the NDcPP but is mandated by this EP because IPsec is used to secure the signaling and media channels.

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

4.2.1.5 FCS_TLSC_EXT.2 TLS Client Protocol with Authentication

This SFR is optional in the NDcPP but is mandated by this EP because TLS is used for SIP trunking.

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

4.2.1.6 FCS_TLSS_EXT.2 TLS Server Protocol with Authentication

This SFR is optional in the NDcPP but is mandated by this EP because TLS is used for SIP trunking.

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

4.2.1.7 FMT_SMF.1 Specification of Management Functions

Additional management functions extend the FMT_SMF.1 SFR found in the NDcPP. The following functions shall be combined with those of the NDcPP in the context of a conforming Security Target. 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 back-to-back user agent SFP
- Configure traffic filtering rules
- Configure NAT
- Configure SIP communications
- Enable or disable use of the SRTP NULL algorithm
- Specify the ports used for SRTP

Assurance Activity
Compliance with the SFRs in section 4.2.2 of this EP is sufficient to demonstrate that the TOE provides sufficient means to manage its SBC functions.

4.2.1.8 FPT_STM.1 Reliable Time Stamps

FPT_STM.1.1 Refinement: The TSF shall be able to provide reliable time stamps **using Network Time Protocol version 4 (NTPv4) as specified in RFC 5905**.

Assurance Activity	
TSS	The evaluator shall verify that the TSS describes the ability of the TOE to support NTP synchronization.
AGD	The evaluator shall review the guidance documentation to confirm that it provides instructions for how to enable NTP synchronization.
Test	The evaluator shall manually set the system time to an incorrect value. The evaluator shall then follow the guidance documentation to enable NTP synchronization, synchronize with an NTP server, and observe that the system time is set to the current time.

4.2.1.9 FTP_ITC.1 Inter-TSF Trusted Channel

FTP_ITC.1.1 Refinement: The TSF shall be **capable of using SNMPv3, SRTP, TLS, and** [selection: IPsec, SSH, HTTPS, no other protocol] **to** provide a trusted communication channel between itself and **authorized IT entities supporting the following capabilities: audit server, NTP server, [selection: authentication server, assignment: [*other capabilities*]]** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.

Application Note: As per Clause 13 of IEEE 802.1AE-2006, SNMPv3 is required for implementation of MACsec. This SFR has been further refined from the NDcPP to include this protocol.

Assurance Activity
This SFR is a refinement of FTP_ITC.1 as defined in the NDcPP. The evaluator shall repeat the assurance activities defined for FTP_ITC.1 in the NDcPP for this refined SFR.

4.2.2 TOE Security Functional Requirements

4.2.2.1 FAU_ARP.1 Specification of Management Functions

FAU_ARP.1.1 The TSF shall take [*the following action: transmit SNMPv3 trap-to-trap receiver in the Operational Environment*] upon detection of a potential security violation.

Assurance Activity	
TSS	The evaluator shall verify that the TSS describes the ability of the TOE to transmit potential security violations to an SNMPv3 trap-to-trap receiver.
AGD	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 SNMPv3 trap-to-trap receiver.
Test	The evaluator shall deploy the TOE in an environment that contains an SNMPv3 trap-to-trap receiver. The evaluator shall configure the TOE to communicate with the receiver in the manner that is specified by the AGD. The evaluator shall deploy a packet capture tool that is capable of sniffing the traffic between the TOE and the 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 receiver that the TSF transmitted the potential security violation and that it correctly used the SNMPv3 protocol.

4.2.2.2 FAU_SAA.1 Potential Violation Analysis

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:

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

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

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

4.2.2.3 FCS_DTLS_EXT.1 Datagram Transport Layer Security

FCS_DTLS_EXT.1.1 The TSF shall implement the Datagram Transport Layer Security (DTLS) protocol in accordance with RFC 6347.

FCS_DTLS_EXT.1.2 The TSF shall implement the requirements in FCS_TLSC_EXT.2 for the DLTS implementation, except where variations are allowed according to RFC 6347.

Application Note: Differences between DTLS and TLS are outlined in RFC 6347; otherwise the protocols are the same. In particular, for the applicable security characteristics defined for the TOE, the two protocols do not differ. Therefore, all application notes and assurance activities that are listed for FCS_TLSC_EXT.2 apply to the DTLS implementation.

Assurance Activity	
Note that this assurance activity involves the same procedures as specified by FCS_TLSC_EXT.2 as defined in the NDcPP except that they are applied to the TOE's DTLS implementation.	
TSS	The evaluator shall verify that the TSS describes the ability of the TOE to use DTLS and what ciphersuites are supported by the DTLS implementation.
AGD	If any aspects of the DTLS implementation require configuration, the evaluator shall verify that the method of doing so is described in the AGD.
Test	The evaluator shall perform the following test: 1. If necessary, configure the TOE to use DTLS. 2. Deploy a packet capture tool that is capable of sniffing traffic on the network interface where DTLS traffic will be transmitted. 3. Establish a DTLS connection with the TOE and verify using packet captures and audit logs that DTLS communications are established and that encrypted traffic is transmitted over the DTLS channel. 4. Repeat this test for each ciphersuite supported by the DTLS implementation.

4.2.2.4 FCS_SRTP_EXT.1 Secure Real-time Transport Protocol

FCS_SRTP_EXT.1.1 The TSF shall implement the Secure Real-time Transport Protocol (SRTP) that complies with RFC 3711, and use Security Descriptions for Media Streams (SDES) in compliance with RFC 4568 to provide key information for the SRTP connection.

FCS_SRTP_EXT.1.2 The TSF shall implement SDES-SRTP supporting the following ciphersuites in accordance with RFC 4568: AES_CM_128_HMAC_SHA1_80.

Application Note: This requirement specifies that the SRTP session that will be used to carry the VoIP traffic will be keyed according to an SDES dialog using the identified ciphersuite. In future versions of this EP, Suite B ciphersuites will be available.

FCS_SRTP_EXT.1.3 The TSF shall ensure the SRTP NULL algorithm can be disabled by a Security Administrator.

FCS_SRTP_EXT.1.4 The TSF shall allow the SRTP ports to be used for SRTP communications to be specified by a Security Administrator.

Assurance Activity	
TSS	The evaluator shall verify that the TSS describes the ability of the TOE to do the following: 1. Support the use of SRTP and the ciphersuites that are supported by the SRTP implementation. 2. Provide the ability for a Security Administrator to disable the SRTP NULL algorithm. 3. Provide the ability for a Security Administrator to specify the SRTP ports used for SRTP communications.
AGD	The evaluator shall verify that the Operational Guidance describes how to perform the following actions on the TOE: 1. How to configure the ciphersuites used by SRTP. 2. How to enable/disable use of the SRTP NULL algorithm. 3. How to specify the ports used for SRTP communications.

Test	The evaluator shall perform the following tests: **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 DTLS traffic will be transmitted. 3. Establish a DTLS connection with the TOE and verify using packet captures and audit logs that DTLS communications are established and that encrypted traffic is transmitted over the DTLS channel. 4. Repeat this test for each ciphersuite supported for the SRTP implementation. **Test 2:** 1. Configure the TOE to enable use of the SRTP NULL algorithm. 2. Deploy a packet capture tool that is capable of sniffing traffic on the network interface where DTLS traffic will be transmitted. 3. Transmit SRTP NULL message to the TOE and observe that it is accepted. 4. Configure the TOE to disable use of the SRTP NULL algorithm. 5. 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 DTLS 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.

4.2.2.5 FDP_IFC.1 Information Flow Control Policy

FDP_IFC.1.1 The TSF shall enforce the [*back-to-back user agent SFP*] on [*caller-callee pairs attempting to communicate through the TOE*].

Assurance Activity	
TSS	N/A – testing for this SFR is performed as part of FDP_IFF.1.
AGD	N/A – testing for this SFR is performed as part of FDP_IFF.1.
Test	N/A – testing for this SFR is performed as part of FDP_IFF.1.

4.2.2.6 FDP_IFF.1 Information Flow Control Functions

FDP_IFF.1.1 The TSF shall enforce the [*back-to-back user agent SFP*] 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:*

- *Default-deny (whitelist) posture: if configured, the TSF will implicitly deny all information flows except for those explicitly authorized by the TSF*
- *Default-allow (blacklist) 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 a whitelist posture, any calling parties that are present on the whitelist (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 blacklist posture, any calling parties that are present on the blacklist (identifiable by calling number or source IP address, or communications protocols) are explicitly denied*].

Assurance Activity	
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 a whitelist or a blacklist posture.
AGD	The evaluator shall review the Operational Guidance to verify that it provides instructions for setting the TOE into either a whitelist or a blacklist posture and for how to add or remove entries from the whitelist or blacklist.
Test	The evaluator shall perform the following tests: **Test 1** 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 2** Configure a custom ACL to only permit a call originating from an IP address or subnet. Make a call from that IP address or subnet and verify the call can be completed. **Test 3** Configure a custom ACL to deny a call destined for an IP address or subnet. Make a call to that IP address or subnet and verify the call cannot be completed. Verify calls to any other IP address or subnet will complete a call. **Test 4** Configure a custom ACL to only permit a call destined an IP address or subnet. Make a call to that IP address or subnet and verify the call can be completed. Verify calls to any other IP address or subnet will not complete a call. **Test 5** Configure a custom ACL to deny a call using a certain signaling (e.g. SIP) or media (e.g. RTP) protocol. Make a call using that protocol and verify the call cannot be completed. Verify calls using other signaling (e.g. H.323) or media (e.g. SRTP) protocols will complete a call.

	Test 6 Configure a custom ACL to only permit a call using a certain signaling (e.g., SIP) or media (e.g., RTP) protocol. Make a call using that protocol and verify the call can be completed. Verify calls using other signaling (e.g., H.323) or media (e.g., SRTP) protocols will not complete a call. **Test 7** On the TOE, configure a whitelist 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 whitelisted numbers. Verify that each number can complete. Attempt call through the TOE from other non-whitelisted numbers. Verify that the calls cannot complete. **Test 8** On the TOE, configure a whitelist 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 whitelisted IP addresses. Verify that each IP address can complete. Change the IP address of the end points; however, keep the calling number the same. Attempt call through the TOE from new IP addresses. Verify that the calls cannot complete. **Test 9** On the TOE, configure a blacklist 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 blacklisted numbers. Verify that each number cannot complete. Call through the TOE from other non-blacklisted numbers. Verify that the calls can complete. **Test 10** On the TOE, configure a blacklist 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 blacklisted IP addresses. Verify that each IP address cannot complete. Change the IP address of the end-points; however, keep the calling number the same. Attempt call through the TOE from new IP addresses. Verify that the calls can complete.

4.2.2.7 FFW_ACL_EXT.1 VoIP Traffic Filtering

FFW_ACL_EXT.1.1 The TSF shall perform traffic filtering on network packets processed by the TOE.

Assurance Activity	
TSS	The evaluator shall verify that the TSS provides a description of the TOE's initialization/startup process, which clearly indicates where processing of network packets begins to take place, and provides a discussion that supports the assertion that packets cannot flow during this process. The evaluator shall verify that the TSS also includes a narrative that identifies the components (e.g., active entity such as a process or task) involved in processing the network packets and describes the safeguards that would prevent packets flowing through the TOE without applying the ruleset in the event of a component failure. This could include the failure of a component, such as a process being terminated, or a failure within a component, such as memory buffers full and cannot process packets.
AGD	The guidance documentation associated with this requirement is assessed in the subsequent test assurance activities.

Test	The evaluator shall perform the following tests: **Test 1** The evaluator shall attempt to get network traffic to flow through the TOE while the TOE is being initialized. A steady flow of network packets that would otherwise be denied by the ruleset should be sourced and be directed to a host. The evaluator shall verify, using a packet sniffer, that none of the generated network traffic is permitted through the firewall during initialization. **Test 2** The evaluator shall attempt to get network traffic to flow through the TOE while the TOE is being initialized. A steady flow of network packets that would be permitted by the ruleset should be sourced and be directed at a host. The evaluator shall verify, using a packet sniffer, that none of the generated network traffic is permitted through the TOE during initialization and is only permitted once initialization is complete.

FFW_ACL_EXT.1.2 The TSF shall allow the definition of traffic filtering rules using the following network protocol fields:

- ICMPv4
    - Type
    - Code
- ICMPv6
    - Type
    - Code
- IPv4
    - Source address
    - Destination Address
    - Transport Layer Protocol
- IPv6
    - Source address
    - Destination Address
    - Transport Layer Protocol
    - [selection: IPv6 Extension header type [assignment: list of fields in IPv6 extension header], no other field]
- TCP
    - Source Port
    - Destination Port
- UDP
    - Source Port
    - Destination Port
- Distinct interface

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.

FFW_ACL_EXT.1.4 The TSF shall allow the traffic filtering rules to be assigned to each distinct network interface.

Assurance Activity	
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: • ICMPv4 o Type o Code • ICMPv6 o Type o Code • IPv4 o Source address o Destination address o Transport layer protocol • IPv6 o Source address o Destination address o Transport layer protocol, and where defined by ST author, extension header type, extension header fields • TCP o Source port o Destination port • UDP o Source port o Destination port 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.
AGD	The evaluators shall verify that the guidance documentation identifies the following attributes as being configurable within traffic filtering rules for the associated protocols: • ICMPv4 o Type o Code • ICMPv6 o Type o Code • IPv4 o Source address o Destination address o Transport layer protocol • IPv6 o Source address o Destination address o Transport layer protocol, and where defined by ST author, extension header type, extension header fields

	• TCP ○ Source port ○ Destination port • UDP ○ Source port ○ Destination port The evaluator shall verify that the guidance documentation indicates that each rule can identify the following actions: permit, drop, and log. The evaluator shall verify that the guidance documentation explains how rules are associated with distinct network interfaces.

Test	The evaluator shall perform the following tests: **Test 1** The evaluator shall use the instructions in the guidance documentation to test that stateful packet filter firewall rules can be created that permit, drop, and log packets for each of the following attributes: • ICMPv4 o Type o Code • ICMPv6 o Type o Code • IPv4 o Source address o Destination address o Transport layer protocol • IPv6 o Source address o Destination address o Transport layer protocol, and where defined by ST author, extension header type, extension header fields • TCP o Source port o Destination port • UDP o Source port o Destination port **Test 2** Repeat the test assurance activity above to ensure that traffic filtering rules can be defined for each distinct network interface type supported by the TOE.

FFW_ACL_EXT.1.5 The TSF shall:

a) Accept a network packet without further processing of traffic filtering rules if it matches an allowed established session for the following protocols: TCP, UDP, [selection: ICMP, no other protocols] based on the following network packet attributes:

1. TCP: source and destination addresses, source and destination ports, sequence number, flags;
2. UDP: source and destination addresses, source and destination ports;
3. [selection: 'ICMP: source and destination addresses, type, [selection: code, [*assignment: list of matching attributes*]]', no other protocols].

b) 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].

Assurance Activity	
TSS	The evaluator shall verify that the TSS identifies the protocols that support session handling. The

	TSS shall identify TCP, UDP, and ICMP if selected by the ST author. The evaluator shall verify that the TSS describes how sessions are established (including handshake processing) and maintained. The evaluator shall verify that for TCP, the TSS identifies and describes the use of the following attributes in session determination: source and destination addresses, source and destination ports, sequence number, and individual flags. The evaluator shall verify that for UDP, the TSS identifies and describes the following attributes in session determination: source and destination addresses, source and destination ports. The evaluator shall verify that for ICMP (if selected), the TSS identifies and describes the following attributes in session determination: source and destination addresses, other attributes chosen in FFW_ACL_EXT.1.5. The evaluator shall verify that the TSS describes how established sessions are removed. The TSS shall describe how connections are removed for each protocol based on normal completion and/or timeout conditions. The TSS shall also indicate when session removal becomes effective (e.g., before the next packet that might match the session is processed).
AGD	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
Test	The evaluator shall perform the following tests: **Test 1** The evaluator shall configure the TOE to permit and log TCP traffic. The evaluator shall initiate a TCP session. While the TCP session is being established, the evaluator shall introduce session establishment packets with incorrect flags to determine that the altered traffic is not accepted as part of the session (i.e., a log event is generated to show the ruleset was applied). After a TCP session is successfully established, the evaluator shall alter each of the session determining attributes (source and destination addresses, source and destination ports, sequence number, flags) one at a time in order to verify that the altered packets are not accepted as part of the established session. **Test 2** The evaluator shall terminate the TCP session established per Test 1 as described in the TSS. The evaluator shall then immediately send a packet matching the former session definition in order to ensure it is not forwarded through the TOE without being subject to the ruleset. **Test 3** The evaluator shall expire (i.e., reach timeout) the TCP session established per Test 1 as described in the TSS. The evaluator shall then send a packet matching the former session in order to ensure it is not forwarded through the TOE without being subject to the ruleset. **Test 4** The evaluator shall configure the TOE to permit and log UDP traffic. The evaluator shall establish a UDP session. Once a UDP session is established, the evaluator shall alter each of the session determining attributes (source and destination addresses, source and destination ports) one at a

	time in order to verify that the altered packets are not accepted as part of the established session. **Test 5** 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. **Test 6** If ICMP is selected, the evaluator shall configure the TOE to permit and log ICMP traffic. The evaluator shall establish a session for ICMP as defined in the TSS. Once an ICMP session is established, the evaluator shall alter each of the session determining attributes (source and destination addresses, other attributes chosen in FFW_ACL_EXT.1.5) one at a time in order to verify that the altered packets are not accepted as part of the established session. **Test 7** If applicable, the evaluator shall terminate the ICMP session established per Test 6 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 8** The evaluator shall expire (i.e., reach timeout) the ICMP session established per Test 6 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 The TSF shall process the applicable traffic filtering rules in an administratively defined order.

Assurance Activity	
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.
AGD	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.
Test	The evaluator shall perform the following tests: **Test 1** The evaluator shall devise two equal stateful traffic filtering rules with alternate operations – permit and drop. The rules should then be deployed in two distinct orders and in each case the evaluator shall ensure that the first rule is enforced in both cases by generating applicable packets and using packet capture and logs for confirmation. **Test 2** The evaluator shall repeat the procedure above, except that the two rules should be devised where one is a subset of the other (e.g., a specific address vs. a network segment). Again, the

	evaluator should test both orders to ensure that the first is enforced regardless of the specificity of the rule.

FFW_ACL_EXT.1.7 The TSF shall deny packet flow if a matching rule is not identified.

Assurance Activity	
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).
AGD	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.
Test	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.

4.2.2.8 FFW_ACL_EXT.2 Stateful VoIP Traffic Filtering

FFW_ACL_EXT.2.1 The TSF shall perform stateful traffic filtering on the following VoIP protocols: SIP, H.323 (H.225, H.245), [selection: [*assignment: other protocols*], no other protocols].

FFW_ACL_EXT.2.2 The TSF shall enforce the following default stateful traffic filtering rules on all network traffic matching protocol types identified in FFW_ACL_EXT.2.1:

a) SIP traffic where a BYE message precedes an INVITE message.
b) H.225 traffic where an RCF reply precedes any other traffic.
c) H.245 traffic where a ResponseMessage precedes a RequestMessage.
d) [*assignment: other default stateful traffic filtering rules*].

FFW_ACL_EXT.2.3 The TSF shall terminate any connection found to be in violation of the default stateful traffic filtering rules and generate an audit record of the event.

FFW_ACL_EXT.2.4 The TSF shall dynamically open media ports to VoIP protocol traffic upon negotiation of a session and close these ports upon termination of a session.

FFW_ACL_EXT.2.5 The TSF shall not define a static range of ports to remain open indefinitely for the purpose of allowing VoIP protocol traffic.

Assurance Activity	
TSS	The evaluator shall verify that the TSS describes the ability of the TOE to perform stateful traffic filtering of all VoIP 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 or 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 VoIP traffic such that the ports used to carry VoIP traffic are not predictable and ports are not open and listening for VoIP traffic.
AGD	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.
Test	The evaluator shall perform the following tests: **Test 1** 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 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 3** 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 4** If the ST specifies any additional default stateful traffic filtering rules, the evaluator shall transmit traffic streams to the TOE that violate each of these rules and observe using packet captures and audit logs that in call cases, the TOE drops and logs invalid traffic. **Test 5** 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 6** Complete a call and capture the packets. Examine the packet capture and take note of the ports the media channel (RTP, SRTP) is communicating over. Terminate the call. Using a packet generator, attempt to send traffic over the media ports that were active when the call was active. Using packet captures, verify the traffic does not traverse the TOE on these ports.

4.2.2.9 FFW_DPI_EXT.1 Deep Packet Inspection

FFW_DPI_EXT.1.1 The TSF shall implement deep packet inspection for the following protocols: H.323 (H.225, H.245), SIP, RTP, RTCP.

FFW_DPI_EXT.1.2 The TSF shall enforce the following rules for deep packet inspection: [*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 deep packet inspection rule, the TSF shall take the following action: [selection: drop the traffic, generate an audit record, generate an alarm].

Assurance Activity	
TSS	The evaluator shall examine the TSS to verify that it describes the ability of the TOE to perform deep packet inspection for H.323, SIP, RTP, and RTCP traffic 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.
AGD	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.
Test	The evaluator shall perform the following tests: **Test 1** If the deep packet function is configurable, the evaluator shall configure this function to flag, log, and/or drop malformed H.225 traffic, depending on the selections chosen in FFW_DPI_EXT.1.3. The evaluator shall then transmit malformed H.225 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 H.225 traffic that can be detected by the TOE as described in FFW_DPI_EXT.1.2. **Test 2** The evaluator shall repeat Test 1 above for H.245 traffic. **Test 3** The evaluator shall repeat Test 1 above for SIP traffic. **Test 4** The evaluator shall repeat Test 1 above for RTP traffic. **Test 5** The evaluator shall repeat Test 1 above for RTCP traffic.

4.2.2.10 FFW_NAT_EXT.1 Topology Hiding/NAT Traversal

FFW_NAT_EXT.1.1 The TSF shall support Network Address Translation (NAT) of signaling and media channel traffic through the TOE that is mediated by the back-to-back user agent SFP defined by FDP_IFC.1.

FFW_NAT_EXT.1.2 The TSF shall support NAT for the following protocols [selection: SIP, 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.

Assurance Activity	
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.
AGD	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.
Test	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.

4.2.2.11 FIA_SIPS_EXT.1 Session Initiation Protocol (SIP) Server

FIA_SIPS_EXT.1.1 The TSF shall implement the Session Initiation Protocol (SIP) that complies with RFC 3261 using the Session Description Protocol (SDP) complying with RFC 4566 to describe the multimedia session that will be used to carry the VOIP traffic.

FIA_SIPS_EXT.1.2 The 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 SIP 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]*].

Application Note: The only SIP request that is required to be authenticated (by the TOE) is the REGISTER request. The SIP Server will perform the enforcement and only register the user upon the presentation of the correct password; the TOE is required by the elements above to support passwords that are at least 8 characters long (the maximum length is defined in the first assignment) and can contain the characters identified in FIA_SIPS_EXT.1.3 (characters allowed by the TOE but not listed explicitly in the element should be identified in the second assignment; otherwise “no other characters” is an acceptable assignment.

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.

Assurance Activity	
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.
AGD	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.
Test	The evaluator shall perform the following tests: **Test 1** Attempt to have a SIP client issue a SIP REGISTER request without providing authentication credentials. Observe that the request is rejected and logged by the TSF. **Test 2** Attempt to have a SIP client issue a SIP REGISTER request with authentication credentials using characters not supported by the TSF. Observe that the request is rejected and logged by the TSF. **Test 3** Attempt to have a SIP client issue a SIP REGISTER request with valid authentication credentials using characters supported by the TSF. Observe that the request is accepted and logged by the TSF. Repeat this test as many times as necessary to ensure that passwords of the minimum and maximum supported lengths are used and that each supported character is used in at least one password. **Test 4** Configure the TOE to manipulate SIP header values. Place a call through the TOE. Capture traffic both before it is received by the TOE and after it exits the TOE. Verify that the SIP header values have been modified. Repeat for each supported header modification, as necessary.

4.2.2.12 FIA_SIPT_EXT.1 Session Initiation Protocol (SIP) 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 username 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 and SRTP in order to establish a SIP trunk.

Assurance Activity	
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.
AGD	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.
Test	The evaluator shall perform the following tests: **Test 1** Configure the TOE to support an encrypted SIP trunk. Configure a trunk peer to communicate with the TOE using the SIP trunk. Present a correct username/password combination 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 2** Repeat test 1 but provide incorrect username/password information with the trunk peer and verify via packet capture and audit log that the session was not established. **Test 3** Repeat test 1 but change the IP address of the trunk peer and verify via packet capture and audit log that the session was not established.

4.2.2.13 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 and R-factor.

Assurance Activity	
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.
AGD	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.

Test	The evaluator shall perform the following tests: **Test 1** Configure the TOE to support QoS. Set QoS tags for media and signaling traffic flows. Complete a call between calling parties that are connected to the TOE via two different external interfaces. Verify, using packet captures, that traffic between the TOE and the callee is tagged with appropriate QoS markings. **Test 2** Configure the TOE to support QoS. Set QoS tags for media and signaling traffic flows. Configure one remote endpoint to act as a calling party that sends a continuous stream of VoIP traffic (media and signaling) to another endpoint that is connected to the TOE via a different external interface. Verify using packet captures that traffic between the TOE and the callee is tagged with appropriate QoS markings, and that the QoS R-factor is being updated as the traffic persists.

4.2.2.14 FRU_RSA.1 Maximum Quotas

FAU_RSA.1.1 The TSF shall enforce maximum quotas of the following resources: [*CPU, memory, assignment: [other resources]*], that [subjects] can use [selection: simultaneously, over a specified period of time].

Application Note: The intent of this SFR is for the TOE to be resistant to Denial of Service attacks.

Assurance Activity	
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.
AGD	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.
Test	The evaluator shall perform the following tests: **Test 1** Using a tool of choice, attempt a DoS attack that creates excess CPU cycles. Place a call while this attack occurs. Verify through packet capture and audio file or screenshot that the call was successful. **Test 2** Using a tool of choice, attempt a DoS attack that attempts to exhaust the TOE's memory. Place a call while this attack occurs. Verify through packet capture and audio file or screenshot that the call was successful. **Test 3** Using a tool of choice, attempt a Distributed DoS attack (DDoS) against the TOE's external network interface(s). Place a call while this attack occurs. Verify through packet capture and audio file or screenshot that the call was successful. **Test 4**

	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.

4.2.2.15 FTP_ITC.1(2) Inter-TSF Trusted Channel

Application Note: FTP_ITC.1 is not iterated in the NDcPP. The ST author shall identify the SFR defined in the NDcPP (as refined in section 4.2.1.9 of this EP) as FTP_ITC.1(1) so that the correct iteration convention is followed.

FTP_ITC.1.1(2) Refinement: The TSF **shall be capable of using SIP-TLS, DTLS, SRTP, IPsec, H.235 [selection: [*assignment: other protocols*], no other protocols]** to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: **VoIP signaling and media channels** that are logically distinct from other communication channels and provide assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.

FTP_ITC.1.2(2) The TSF shall permit **the TSF, or the authorized IT entities** to initiate communication via the trusted channel.

FTP_ITC.1.3(2) The TSF shall initiate communication via the trusted channel for [*assignment: list of functions for which a trusted channel is required*].

Assurance Activity
This SFR is an iteration of FTP_ITC.1 as defined in the NDcPP. The evaluator shall repeat the assurance activities defined for FTP_ITC.1 in the NDcPP for this iteration of the SFR.

4.2.2.16 FTP_ITC.1(3) Inter-TSF Trusted Channel

Application Note: FTP_ITC.1 is not iterated in the NDcPP. The ST author shall identify the SFR defined in the NDcPP (as refined in section 4.2.1.9 of this EP) as FTP_ITC.1(1) so that the correct iteration convention is followed.

FTP_ITC.1.1(3) Refinement: The TSF shall provide a **signaling** channel between itself and **a SIP server using TLS as specified in FCS_TLSC_EXT.2 and [selection: DTLS as specified in FCS_DTLS_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.

FTP_ITC.1.2(3) The TSF shall permit **the TSF** to initiate communication via the trusted channel.

FTP_ITC.1.3(3) The TSF shall initiate communication via the trusted channel for [*all communications with the SIP server*].

Assurance Activity
This SFR is an iteration of FTP_ITC.1 as defined in the NDcPP. The evaluator shall repeat the assurance

activities defined for FTP_ITC.1 in the NDcPP for this iteration of the SFR.

4.2.2.17 FTP_ITC.1(4) Inter-TSF Trusted Channel

Application Note: FTP_ITC.1 is not iterated in the NDcPP. The ST author shall identify the SFR defined in the NDcPP (as refined in section 4.2.1.9 of this EP) as FTP_ITC.1(1) so that the correct iteration convention is followed.

FTP_ITC.1.1(4) Refinement: The TSF shall provide a**n H.323** communication channel **in accordance with ITU-REC H.235.0** between itself and **a gatekeeper using TLS as specified in FCS_TLSC_EXT.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.

FTP_ITC.1.2(4) The TSF shall permit **the TSF** to initiate communication via the trusted channel.

FTP_ITC.1.3(4) The TSF shall initiate communication via the trusted channel for [*all communications with the gatekeeper*].

Assurance Activity
This SFR is an iteration of FTP_ITC.1 as defined in the NDcPP. The evaluator shall repeat the assurance activities defined for FTP_ITC.1 in the NDcPP for this iteration of the SFR.

Appendix A - Rationale

The initial sections of this EP document provide a narrative presentation in order to increase the overall understandability of the threats addressed by Session Border Controllers, the methods used to mitigate those threats, and the extent of the mitigation achieved by compliant TOEs. Because the narrative presentation style does not readily lend itself to a formalized evaluation activity, this appendix contains the tabular artifacts that can be used for the evaluation activities associated with this document.

A.1 Security Problem Definition

A.1.1 Assumptions

No assumptions are defined for this EP. As an extended package to the NDcPP, the TOE inherits all assumptions defined by the base PP, with one exception as defined in section 2.2 of this EP.

A.1.2 Threats

The table below lists the threats that are mitigated by session border controllers that comply with this EP. Note that all threats defined in the base NDcPP are inherited by this EP. If a threat from the NDcPP is reproduced here, it means that this EP defines additional SFRs to mitigate the threat in a more specific manner than what is prescribed by the NDcPP.

Threat Name	**Threat Definition**
T.NETWORK_DISCLOSURE	An attacker may attempt to “map” a subnet to determine the devices that reside on the network and to obtain the IP addresses of machines as well as the services (ports) those machines are offering. This information could be used to mount attacks to those machines via the services that are exposed.
T.MALICIOUS_TRAFFIC	An attacker may attempt to send malformed packets to the SBC in hopes of causing the network stack or services listening on UDP/TCP ports on the SBC or protected network to crash.
T.UNTRUSTED_COMMUNICATION_CHANNELS	An attacker may acquire sensitive TOE or user data that is transmitted to or from the TOE because an untrusted communication channel causes a disclosure of data in transit.
T.NETWORK_ACCESS	An attacker may send traffic through the TOE that enables them to access devices in the TOE’s Operational Environment without authorization.
T.USER_DATA_REUSE	User data may be inadvertently sent to a destination not intended by the original sender, causing an unauthorized disclosure of the data.
T.RESOURCE_EXHAUSTION	An attacker may transmit network traffic to the TOE that causes it to be unable to perform its functions on legitimate network traffic.

Table 2: Threats

A.1.3 Organizational Security Policies

No organizational policies that are specific to SBCs have been identified. However, all the organizational security policies in the NDcPP apply to SBCs.

A.1.4 Security Problem Definition Correspondence

The following table maps the threats and assumptions defined in this EP to the security objectives defined or identified in this EP.

Threat or Assumption	Security Objectives
T.NETWORK_DISCLOSURE	O.TOPOLOGY_HIDING, O.USER_DATA_DELIVERY
T.MALICIOUS_TRAFFIC	O.TRAFFIC_FILTERING
T.UNTRUSTED_COMMUNICATION_CHANNELS	O.PROTECTED_COMMUNICATIONS
T.NETWORK_ACCESS	O.TRAFFIC_FILTERING, O.USER_DATA_DELIVERY
T.USER_DATA_REUSE	O.USER_DATA_DELIVERY
T.RESOURCE_EXHAUSTION	O.RESOURCE_AVAILABILITY

Table 3: Security Problem Definition Correspondence

Note that this EP also includes security objectives that address threats from the base NDcPP in a more refined manner, based on the specific functions provided by a SBC TOE, as follows:

- O.SYSTEM_MONITORING further mitigates NDcPP threat T.UNDETECTED_ACTIVITY
- O.AUTHORIZED_ADMINISTRATION further mitigates NDcPP threat T.UNAUTHORIZED_ADMINISTRATOR_ACCESS

A.2 Security Objectives

A.2.1 Security Objectives for the TOE

The following table contains security objectives specific to Session Border Controllers.

Objective Name	Objective Definition
O.SYSTEM_MONITORING	The TOE will provide the means to detect when security-relevant events occur and generate audit events and/or security alerts in response to this detection.
O.PROTECTED_COMMUNICATIONS	The TOE will provide the means to secure communications channels between the TOE and the Operational Environment.
O.TOPOLOGY_HIDING	The TOE will provide the ability to prevent disclosure of information relating to devices that are located on its protected network.
O.TRAFFIC_FILTERING	The TOE will provide the ability to apply filtering rules to network traffic and discard traffic that is found to be unauthorized or malformed.
O.USER_DATA_DELIVERY	The TOE will provide mechanisms for ensuring that user data transmitted between calling parties is directed only to the intended recipient(s).
O.RESOURCE_AVAILABILITY	The TOE will provide mechanisms to prioritize network traffic and protect against denial-of-service attacks in order to ensure that its bandwidth is used effectively.
O.AUTHORIZED_ADMINISTRATION	The TOE will provide management functions that can be used to securely manage the TSF.

Table 4: Security Objectives for the TOE

A.2.2 Security Objectives for the Operational Environment

No environmental security objectives are defined for this EP. As an extended package to the NDcPP, the TOE inherits all environmental security objectives defined by the base PP, with one exception as defined in section 3.2 of this EP.

A.2.3 Security Objective Correspondence

The correspondence between the Security Functional Requirements (SFRs) and Security Objectives identified or defined in this EP is provided in section 3.

Appendix B – Optional Requirements

The baseline requirements are contained in the body of this EP. Additional requirements can be included in the ST, but are not mandatory, in order for a TOE to claim conformance to this EP. It is not mandated that all Session Border Controllers be implemented as distributed systems. Therefore the requirements in this Appendix are not included in the body of this EP. In the case where the TOE is physically distributed among several components, communications between those components must be protected and the below requirements must be included in the ST.

Note: The ST author is responsible for ensuring that requirements that may be associated with those in Appendix B, Appendix C, and/or Appendix D but are not listed (e.g., FMT-type requirements) are also included in the ST.

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

Appendix C – Selection-Based Requirements

The baseline requirements (those that must be performed by the TOE or its underlying platform) are contained in the body of this EP. Additional requirements based on selections are contained in the body of the EP: if certain selections are made, then additional requirements below will need to be included.

Currently no selection-based requirements are prescribed by this EP.

Appendix D – Objective Requirements

The baseline requirements (those that must be performed by the TOE or its underlying platform) are contained in the body of this EP. Additional requirements that specify desirable security functionality are contained in this Appendix. It is expected that these requirements will transition from objective requirements to baseline requirements in future versions of this EP.

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