Sipera Systems
UC-Sec v4.0 Software

Security Target

Evaluation Assurance Level: EAL3+
Document Version: 1.0

Prepared for:

Sipera Systems
1900 Firman Drive, Suite 600
Richardson, TX 75081

Phone: (214) 206-3210
Email: info@sipera.com
http://www.sipera.com

Prepared by:

Corsec Security, Inc.
10340 Democracy Lane, Suite 201
Fairfax, VA 22030

Phone: (703) 267-6050
Email: info@corsec.com
http://www.corsec.com

Table of Contents

Table of Figures

List of Tables

References

[CC] Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009

[AGD Supp] Sipera Systems, Inc. UC-Sec Software version 4.0 Guidance Supplement v0.1

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The Target of Evaluation is the Sipera UC-Sec v4.0 Software, and will hereinafter be referred to as the TOE throughout this document. The TOE is a real-time Unified Communications[1] (UC) security appliance that specializes in providing firewall, routing, and secure and private connection to access the UC core network, especially those that are exchanged in real-time such as Voice over Internet Protocol (VoIP) communications, video communication, Instant Messaging (IM) and others.

1.1 Purpose

This ST is divided into nine sections, as follows:

- Introduction (Section 1) – Provides a brief summary of the ST contents and describes the organization of other sections within this document. It also provides an overview of the TOE security functions and describes the physical and logical scope for the TOE, as well as the ST and TOE references.
- Conformance Claims (Section 2) – Provides the identification of any Common Criteria (CC), ST Protection Profile, and Evaluation Assurance Level (EAL) package claims. It also identifies whether the ST contains extended security requirements.
- Security Problem (Section 3) – Describes the threats, organizational security policies, and assumptions that pertain to the TOE and its environment.
- Security Objectives (Section 4) – Identifies the security objectives that are satisfied by the TOE and its environment.
- Extended Components (Section 5) – Identifies new components (extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs)) that are not included in CC Part 2 or CC Part 3.
- Security Requirements (Section 6) – Presents the SFRs and SARs met by the TOE.
- TOE Summary Specification (Section 7) – Describes the security functions provided by the TOE that satisfy the security functional requirements and objectives.
- Rationale (Section 8) - Presents the rationale for the security objectives, requirements, and SFR dependencies as to their consistency, completeness, and suitability.
- Acronyms (Section 9) – Defines the acronyms and terminology used within this ST.

[1] Unified Communications refers to a category of communications technologies that typically includes voice, video, data, IM, presence, and collaboration products. These communications are typically delivered in real time, although they may not be exchanged in real time (such as voice mail).

1.2 Security Target and TOE References

Table 1 - ST and TOE References

ST Title	Sipera Systems UC-Sec v4.0 Software Security Target
ST Version	Version 1.0
ST Author	Corsec Security Inc.
ST Publication Date	2010/07/28
TOE Reference	Sipera UC-Sec v4.0 Software build Q337
Keywords	Sipera , UC-Sec, unified communications, Voice over Internet Protocol, VoIP, firewall, router.

1.3 Product Overview

The product is the UC-Sec v4.0 Software running on a customized Debian or MontaVista Linux Operating System (OS) and purpose-built hardware. The UC-Sec software includes a centralized management and network monitoring console, called the Elements Management System (EMS) that runs on a Debian Linux OS either separately on general-purpose hardware, or on the same purpose-built appliance as the UC-Sec functionality. In the case where the EMS and the UC-Sec are running on the same hardware, the EMS can run on either the Debian or the Monta Vista Linux OS.

UC is an emerging class of products that provide communication and directory services to users. Users in UC systems can update their locations in real-time, allowing a sought user to be easily found by seeking users. When a seeking user finds the sought user, the seeking user can quickly identify the sought user's preferred method of communication, facilitating communications between the two parties. Additionally, UC products and services can be integrated into business processes, allowing increased productivity as users with needed skill sets can be quickly identified, located, and reached via multiple communication mechanisms. UC systems include the communications channels that users exercise to contact each other.

The nature of UC systems presents new problems that cannot be adequately addressed by existing security solutions. UC happens in real-time (such as with VoIP), and therefore UC security solutions must be able to perform in real-time. UC security solutions must protect data in many different formats, since sensitive data might be communicated through a UC system in a number of formats (e.g. voice, video, IM, etc.). The UC-Sec appliance is designed to be deployed in an enterprise De-Militarized Zone (DMZ) or core network to mitigate threats to the UC network.

UC traffic, and in particular real-time traffic such as VoIP, must be handled specially in order for UC services to function properly. In a typical network deployment, all incoming network traffic is blocked by a firewall, except for a small subset that is permitted to access hardened devices in a DMZ. In a UC deployment, for example with VoIP, blocking incoming traffic causes all calls that originate from outside of the local or Corporate Network to be blocked. As a result, external calls cannot be connected to their recipients. One workaround is to open a network port to each IP[2] phone on the internal network to allow calls through, but this also opens these systems to attack.

The way that UC firewalls handle these problems is to be application-aware. UC firewalls identify incoming voice traffic and allow well-formed call-initiation messages to pass through. If the internal

[2] IP – Internet Protocol

device accepts the connection, then the UC firewall keeps the connection open until the call ends. This method allows UC firewalls to block potentially malicious traffic, while allowing legitimate traffic to pass through unimpeded. Before, during, and after a call begins, all traffic is monitored to ensure legitimacy until the call ends. After the call ends, all open ports are dynamically closed to prevent malicious entities from exploiting vulnerable devices. Attacks or malicious behavior can also originate from inside the UC network in an enterprise. To protect against such attacks and unexpected anomalies, having an internal UC security network node that is application-aware and can monitor, detect, prevent, and report all unwanted activities is a requirement.

Since a large portion of UC data is exchanged in real-time (VoIP, streaming video, etc.), a special class of UC security nodes is needed to handle UC bandwidth requirements. A UC security node can address these bandwidth requirements by applying policies, traffic, and admission control on different types of traffic, and hence throttling[3] or guaranteeing bandwidth to specific classes of traffic. These two techniques ensure that an appropriate amount of bandwidth is available for UC devices when needed.

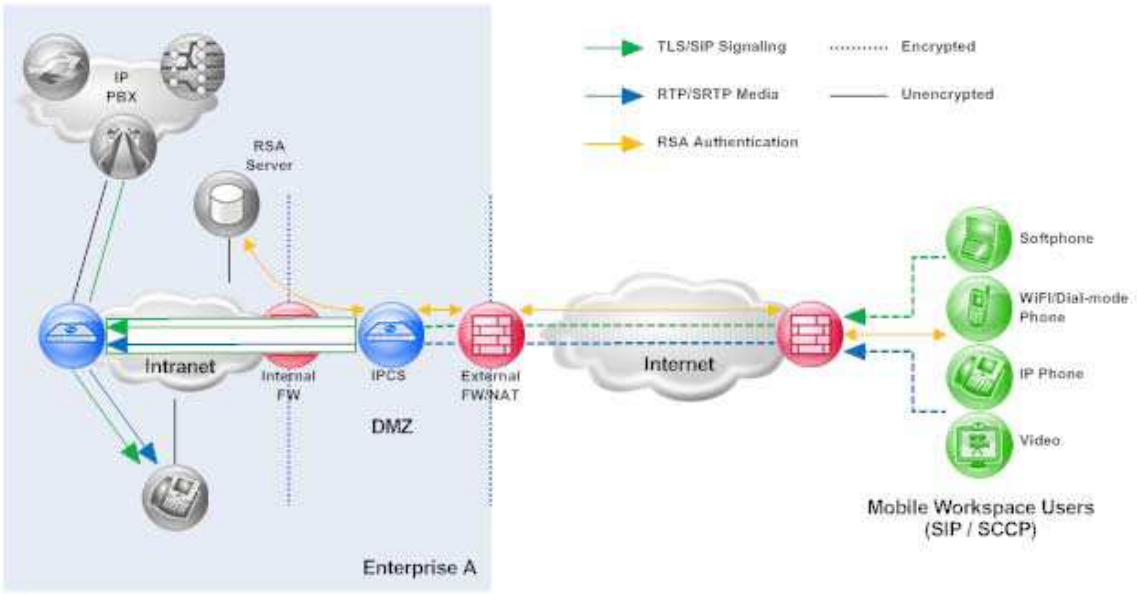
By throttling unimportant or non-time-sensitive data, UC routers allow time-sensitive UC traffic to access the remaining bandwidth as needed. As an alternative to throttling, guaranteeing bandwidth to UC applications ensures that a certain portion of available bandwidth is given to UC traffic when needed.

To support external users, UC-Sec can provide secure connections using Transport Layer Security (TLS) for the signaling traffic, and Secure Real-time Transport Protocol (SRTP) for the media traffic. The encryption provided via TLS/SRTP connections is necessary to preserve the confidentiality of digitized data streams that may contain classified information. In a UC network, data may not be encrypted end-to-end for several reasons. For example, endpoint devices may not support encryption mechanisms and call servers may not be able to scale properly while supporting encryption. In addition, decryption is required in the UC network for application-level inspection and processing, as well as discarding of messages that are not properly formatted or have characteristics that are indicative of a potential attack. A network node is needed that can scale and support encryption and decryption in real-time and connect different IP endpoints without introducing delay or performance impact.

The UC-Sec provides a security feature called topology hiding that allows administrators to mask the actual network topology protected by the UC-Sec from unauthorized or malicious users. The UC-Sec can be configured to learn caller behaviors. The TOE creates configurations as it monitors caller patterns and receives user input on callers. These configurations represent each caller's profile, which the TOE then applies special rules to, depending on the likelihood that the caller is making legitimate calls or is a spammer. Configurations for learned behaviors are written and rewritten via Trivial File Transfer Protocol.

[3] Throttling refers to the process of deliberately providing reduced bandwidth to a specific class of traffic or user.

Figure 1[4] – Remote User Tunneling

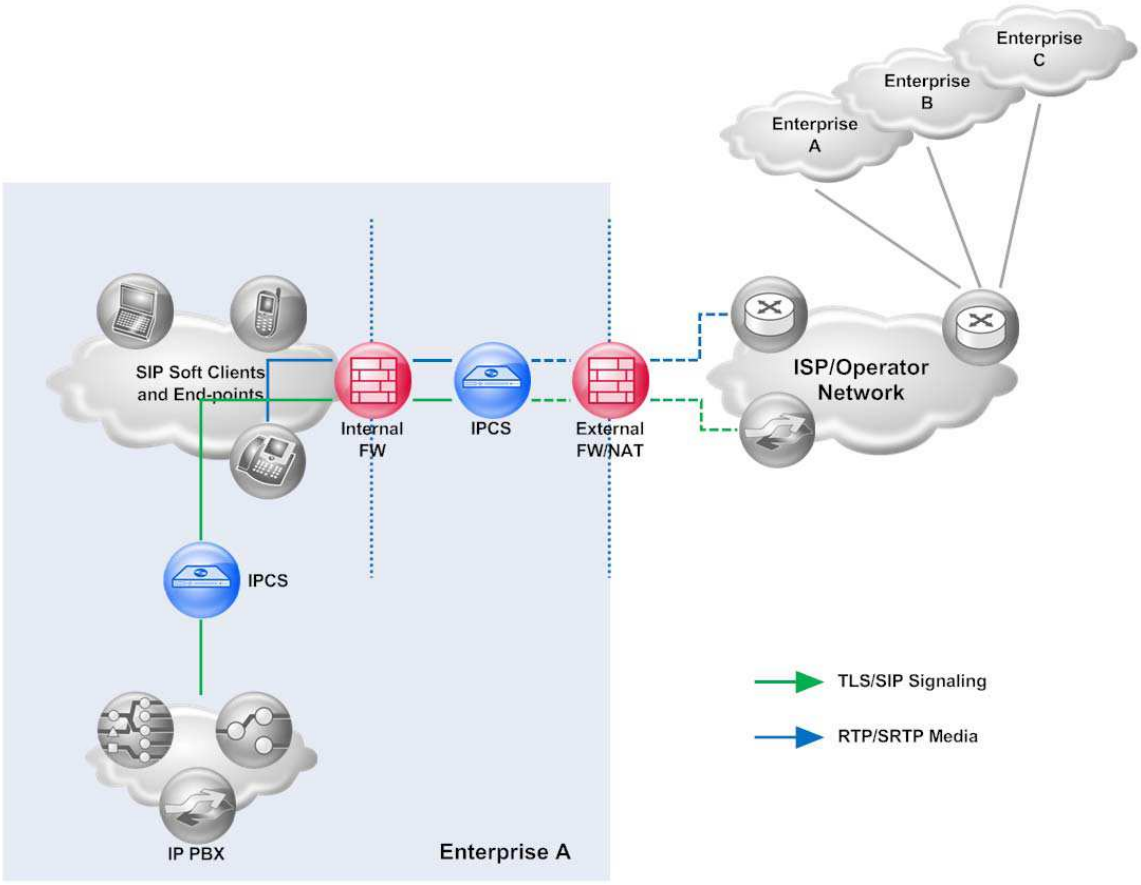


The UC-Sec provides a Session Initiation Protocol (SIP) Trunking capability. SIP Trunking allows the UC-Sec to protect the signaling traffic with TLS and the media traffic with SRTP as it leaves the enterprise network. Since the UC-Sec is a TLS endpoint, it retains the ability to inspect traffic for anomalous behavior. The TLS protection prevents snooping or modification of the media stream as it leaves the protected network.

[4] From the figure:

- FW – Firewall
- NAT –Network Address Translation,
- IPCS – Previous version of UC-Sec were referred to as IPCS,
- PBX – Public Branch Exchange.
- RTP – Real-time Transport Protocol
- SIP – Session Initiation Protocol
- WiFi – Wireless Fidelity (wireless networking)

Figure 2[5] – SIP Trunking



UC real-time traffic is open to unique vulnerabilities, requiring a special class of security solution. The UC-Sec fills this niche by providing access controls, application-specific threat mitigation, and UC traffic policy enforcement, thus protecting vulnerable data. Threats typically faced by UC systems and countered by the UC-Sec include:

- denial of service or distributed denial of service floods,
- fuzzing[6] or sending malformed messages,
- spoofing or masquerading,
- eavesdropping,
- toll fraud[7], and
- rogue media[8].

[5] From the diagram:

- ISP – Internet Service Provider

[6] Fuzzing refers to a technique where invalid, unexpected, or random data is provided to an application to invoke any kind of unexpected behavior (such as security vulnerabilities) that is subsequently recorded by the attacker.

[7] Toll fraud refers to the fraudulent, illegal use of a company's telecommunications equipment by a third party from a remote location.

The UC-Sec provides support for Network Address Translation (NAT) environments. UC connections may be allocated different ports by NAT devices during a session. NAT traversal solves this problem by handling external calls in such a way that calls are not interrupted by shifting NAT port allocations.

1.4 TOE Overview

The TOE Overview summarizes the usage and major security features of the TOE. The TOE Overview provides a context for the TOE evaluation by identifying the TOE type, describing the product, and defining the specific evaluated configuration.

1.4.1 TOE Type

The TOE is the software, MontaVista Linux, or the Debian Linux portion of the UC-Sec v4.0 Software. The TOE includes the EMS software for centralized management and the Debian Linux that EMS runs on running on separate hardware. Sipera provides the TOE as a UC security solution for small to enterprise-class deployments. The TOE specializes in real-time UC traffic monitoring and security, but is capable of handling UC traffic that is not exchanged in real-time. The parts that make up the TOE (the UC-Sec v4.0 Software) include:

- the UC-Sec functionality,
- the EMS centralized management and monitoring console software[9],
- the customized Debian Linux OS for EMS,
- the customized Debian Linux OS for the UC-Sec, and
- the customized MontaVista Linux OS for the UC-Sec.

Each UC-Sec can be managed through a locally-hosted web-based EMS Graphical User Interface (GUI), but for the CC-evaluated configuration, the UC-Secs will be managed via a second web-based EMS GUI on the EMS device. The GUI provides all of the tools that an administrator needs to define rules and operate the TOE, but EMS provides centralized monitoring services as well. Each UC-Sec device supports this centralized monitoring service by reporting important events and system health information to the EMS. The EMS allows administrators to set up and push configurations to all UC-Sec devices on the managed network[10]. Configurations contain rule sets and the security capabilities enabled or disabled for each device.

1.4.2 TOE Description

Since the TOE is intended to be a border or internal security device (accessible on an exposed portion of the network), only certain protocols are allowed to connect (restricted by port) to the management

---

[8] In this case, rogue media refers to the injection of a media stream onto the network without using the proper setup and monitoring protocols.

[9] Note that in the CC-evaluated configuration of the TOE, the EMS software runs on a separate general-purpose hardware platform with an instance of the customized Debian Linux OS.

[10] The managed network is the network that contains all of the UC-Sec appliances that are managed by the EMS device.

interfaces on the TOE. These include SSH[11], HTTPS[12], DNS[13], Syslog, NTP[14], SNMP[15], and SSL-VPN. The TOE blocks any other traffic that is addressed for the management interfaces. To prevent flooding, the TOE limits the number of Transmission Control Protocol (TCP) packets that are allowed from a single host within an administrator-specified time frame. The EMS acts as an NTP and Syslog server for UC-Sec appliances, and an NTP and Syslog client when talking to third-party servers. The UC-Sec can act as a DNS, NTP, and Syslog client. The TOE supports SNMPv3.

The TOE provides Configurable Media Anchoring for SIP and Skinny Client Control Protocol (SCCP)[16]. Configurable Media Anchoring allows the TOE to optionally provide a Media Release service for parties with a direct network path to one another. Media Release allows the data stream (e.g., voice, video, etc.) to flow directly among the participants, rather than being routed through the signaling path. This frees bandwidth for other users and applications, since data can be moved out-of-band[17] with no adverse effects. SIP and SCCP signaling traffic must continue to use the initially-established route for the duration of the communications.

The three major functionalities provided by the TOE to protect the network include monitoring, detection, and protection. Monitoring enables the TOE to gather and examine signaling and media traffic from various areas of the UC network, including all end points, media gateways, call servers, and application servers. Users of the TOE can define thresholds for event activity (such as the number of calls originating from a single source) and the TOE can trigger alarms to notify users when thresholds are reached. The TOE also reports monitored events to EMS to allow a centralized view of the state of network security. The aggregation of data at a single point of the network allows the TOE or administrators to identify attacks that might not be detected otherwise.

There are several detection techniques that the TOE uses to discover attacks against the UC network. One technique is to learn caller behavior through real-time observation of, for example, outgoing call rates toward the call server. These algorithms allow users to define time-of-day and day-of-week criteria for anticipated behavior (e.g., it would be expected that fewer calls would occur on weekends when fewer people are in the office), while accommodating weekends, holidays, and other user-specified special cases. The TOE notes abnormal behavior and can take automated action as a result or simply alert an administrator.

---

[11] SSH – Secure Shell

[12] HTTPS – Secure Hypertext Transfer Protocol

[13] DNS – Domain Name System

[14] NTP – Network Time Protocol

[15] SNMP – Simple Network Management Protocol

[16] SIP and SCCP are signaling protocols that are used to establish and manage sessions between user endpoints in UC systems. These protocols provide control data for connections, such as VoIP calls, while the actual media stream is provided by another protocol, typically Real-time Transport Protocol (RTP).

[17] Out-of-band data means that the data flows separately from the control or signaling data.

The TOE also applies user black listing and white listing by the user administrator via EMS, and black listing of specific sources by the endpoint user via the endpoint device.

As an application-layer device, the TOE can inspect the sequence and contents of protocol messages to detect anomalies and scanning attacks. These features allow the TOE to detect more advanced and dangerous attacks, including zero-day vulnerabilities. After detecting each attack, rules on the TOE can be configured to allow the TOE to take appropriate response actions as needed.

The TOE provides a UC-Device Configuration Proxy for management of remote UC devices on the network. The TOE is able to download configuration files from configuration servers of supported devices. These configuration files are for the UC devices connecting to the network that the UC-Sec protects. The UC-Sec then can rewrite some portions of the configuration files based on policies defined through EMS. For example, the TOE can rewrite internal IP addresses to the equivalent externally facing IP addresses to prevent reconnaissance. The UC-Sec then provides these files to supported UC devices in their modified form.

The TOE provides intrusion and attack protection services. Intrusion protection discovers anomalous events and mitigates potential intrusion events from inside or outside of the enterprise network. With its customized protocol-scrubbing rules, the TOE can detect and prevent malformed-packet-based Denial-Of-Service (DOS) attacks. The protection functionality allows the TOE to block attacks while allowing legitimate traffic to pass unobstructed. Users can define rules to extend this protection to individual end-points, specific groups of end-points, or to all UC devices in the network. This allows a fine-grained control of security, and lets users apply traffic filtering rules only to those entities that are vulnerable to each attack.

The TOE is capable of requiring two-factor authentication from callers. Two-factor authentication requires the caller to enter a Personal Identification Number (PIN), followed by an RSA SecurID token. The PIN is authenticated by a RADIUS[18] server and the SecurID token is authenticated by an RSA authentication server. TOE administrators can specify the duration that the caller stays logged-in after initial authentication, and this value can be on the order of minutes, hours, or days, after which the caller must authenticate again.

The TOE includes rules to limit the types of media that are allowed to be sent across the network. For example, video or modem signals can be blocked. This feature is useful if certain classes of traffic are undesirable, because they represent either a security risk or a misuse of enterprise resources. Elimination of undesirable traffic can also simplify network and security configurations across the network.

Using end-point validation techniques, the TOE can prevent spoofing attacks. These techniques rely on fingerprinting technology, which uses hashes or checksums of data that can be used to positively identify the device and endpoint. By applying fingerprinting technology to various message fields at the application layer, the TOE can differentiate between a user sending legitimate traffic and an attacker attempting to send traffic while masquerading as a valid user.

The TOE can discover attacker attempts to scan the UC network at the application level. The intrusion protection capabilities of the TOE allow the TOE to identify common scan signatures. When a scan is discovered, the TOE reports the scan to an administrator and blocks the attacker for an administrator-specified time period.

The security functionality for the TOE can be summarized into two functional entities: Signaling and Media. The Signaling entity provides support for User Datagram Protocol, Transmission Control Protocol,

[18] RADIUS – Remote Access Dial-In User Service

and TLS[19], and enhanced SIP and SCCP validation and attack prevention techniques. The Media entity provides enforcement of policy for media streams, protocol validation for RTP, support for timing and bandwidth validation techniques, codec validation for encoded data streams, and detection of Dual Tone Multi-Frequency (DTMF) digits. In the evaluated configuration, these entities are contained within a single UC-Sec device.

The UC-Sec provides a media forking feature that allows media streams to be duplicated for recording purposes. For example, calls to a help center might be recorded in this way for quality assurance purposes. With media forking, the original call progresses as normal, while the UC-Sec creates a copy of only the media stream (signaling information is not duplicated) and sends it to the alternate destination. The recording device extracts the IP source and port from the media packet and correlates it with the same information extracted or communicated with the Call Server. No signaling forking is required by the UC-Sec solution in order to perform the media forking function.

The TOE provides a Signaling Mirroring service. Signaling Mirroring allows the TOE to forward copies of signaling data to an external recording device. Signaling mirroring may be desirable for customers who wish to keep records of each calls signaling stream for quality assurance and debugging. With Signaling Mirroring, the original call progresses as normal, while the TOE creates a copy of only the signaling stream and sends it to the alternate destination.

The TOE supports a Reverse Turing Test that enhances user awareness of external calls and allows for external call screening. When a user answers the phone for an external call (originating outside of the organization), the user hears a prerecorded message with a TOE-generated random code. The length of the digit code is configurable by the TOE and can be set by the user administrator. The user can enter the code to connect the call, or can ignore the call and hang up to disconnect the caller. If the call is connected, the user is aware that the calling party is from outside the organization and to be careful about disclosing sensitive or confidential information.

The UC-Sec supports High-Availability (HA) deployments. HA functionality allows automatic takeover of security services by a standby UC-Sec device in the event that the active UC-Sec goes offline or enters an error state. In HA deployments, two UC-Sec devices are deployed as a pair, with one device in active mode and the other in standby mode. The active device operates normally at all times, and additionally synchronizes active UC session states with the standby appliance in real time. A health check is also done between the active and standby UC-Sec appliances in regular intervals. The standby appliance is configured with the same rules and interfaces as the active, including the same IP addresses for traffic interfaces. Any configuration changes on the active UC-Sec are also done automatically on the standby UC-Sec by the EMS node. During a failover, the standby device takes over for the active without dropping connections or packets of active sessions.

EMS has a replication feature that allows two EMS devices to be set up as active and standby appliances. Data is synchronized from the active EMS to the standby EMS at regular intervals. If the active EMS fails, then an administrator can configure the standby EMS to take over as the active EMS. This provides a manual failover to support business continuity for UC-Sec administrators.

Figure 3 shows the details of the deployment configuration of the TOE:

[19] Note: The encryption functionality of the UC-Sec has not been previously evaluated and has not been (or will not be) evaluated in the context of a Common Criteria evaluation.

Legend	VoIP/UC	Management
Active Data	UC data call/media	Configuration Management
Standby Data	UC data keepalive	Connection, keepalive
Synch Data	Heartbeat, synchronization, checkpoint	Periodic Database synchronization

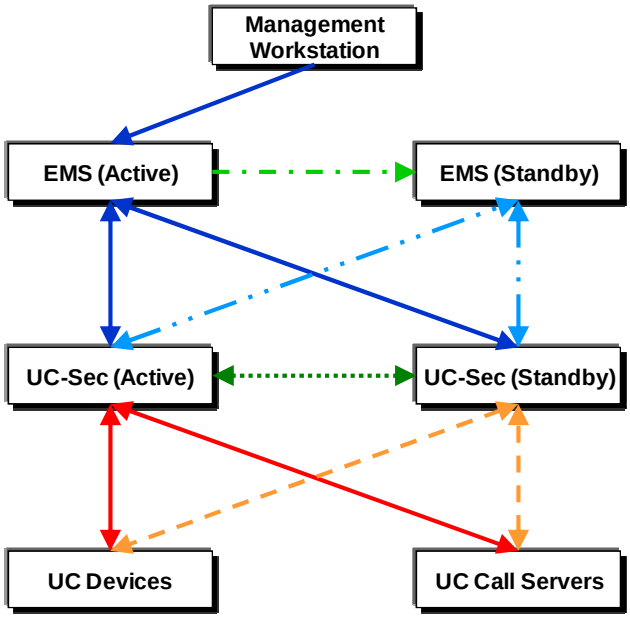


Figure 3 - Deployment Configuration of the TOE

1.4.3 Brief Description of the Components of the TOE

The TOE consists of the UC-Sec software running on a customized MontaVista or Debian Linux OS, and the EMS software running on a second customized Debian Linux OS. The UC-Sec software is the same regardless of the OS used, and provides the main UC routing, firewall, and secure connection functionality[20] for the TOE. The OS chosen is determined by the hardware appliance that the TOE is installed on. Each OS is optimized to suit a different hardware platform. The TOE can be deployed either in a DMZ or in the Core network of an enterprise.

EMS is a centralized management console. Administrators can connect to EMS to control and push configurations to one or more UC-Sec devices within the managed network. EMS is also used to manage,

[20] Note: The encryption functionality of the UC-Sec has not been previously evaluated and has not been (or will not be) evaluated in the context of a Common Criteria evaluation.

monitor, and collect information from each UC-Sec to which it is connected. The EMS provides a GUI-based environment to an Administrator to view, monitor, and manage the UC-Sec nodes in real-time.

Although not part of the TOE, the hardware and firmware on which the TOE runs is provided by Sipera based on the products that Sipera's customers order. Each model is a 1 Unit (U) or 2U appliance with hardware optimizations appropriate to provide service for the intended number of users. Customers can order customized hardware optimizations through Sipera upon request.

1.4.4 TOE Environment

The evaluated deployment configuration of the TOE requires the following environmental components in order to function properly:

- the UC-Sec hardware appliance appropriate for the intended deployment,
- the hardware device appropriate for the EMS deployment,
- UC devices to use the UC network that the TOE protects,
- call servers on the UC network that the TOE protects,
- cables, connectors, and switching and routing devices that allow all of the TOE and environmental components to communicate with each other,
- an administrator workstation with a web browser.

The TOE is intended to be deployed in a physically secure cabinet room or data center with the appropriate level of physical access control and physical protection (e.g., fire control, locks, alarms, etc.) The TOE is intended to be managed by administrators operating under a consistent security policy.

The TOE is intended to provide security for UC devices on the network. Depending on the services intended to be deployed on this network, certain additional devices may be needed (e.g., SIP-capable routers, IP phones, etc.) Devices specific to the service deployment for the UC network are considered environmental components.

The TOE is managed through a web GUI. Administrators must access this interface from a trusted workstation that supports a graphical web browser. The web GUI is part of the TOE, but the workstation and web browser are part of the TOE environment.

1.5 TOE Description

This section primarily addresses the physical and logical components of the TOE included in the evaluation.

1.5.1 Physical Scope

Figure 4 illustrates the physical scope and the physical boundary of the overall solution and ties together all of the components of the TOE and the constituents of the TOE Environment.

The TOE is a software and OS security solution that implements UC routing, firewall, and secure connection to access the UC core network for UC endpoint products, UC network solutions, and UC applications[21]. The TOE runs on the UC-Sec line of purpose-built hardware platforms. The TOE is installed on a hardware appliance as depicted in Figure 4 below. The essential logical components for the proper operation of the TOE in the evaluated configuration are the UC-Sec, Debian Linux, MontaVista Linux, and EMS software. The TOE must run on the appliance hardware provided by Sipera. The appliance hardware, physical network cables and devices, and servers running required network services (such as DNS) are the only required physical components for the proper operation of the TOE.

[21] Note: The encryption functionality of the UC-Sec has not been previously evaluated and has not been (or will not be) evaluated in the context of a Common Criteria evaluation.

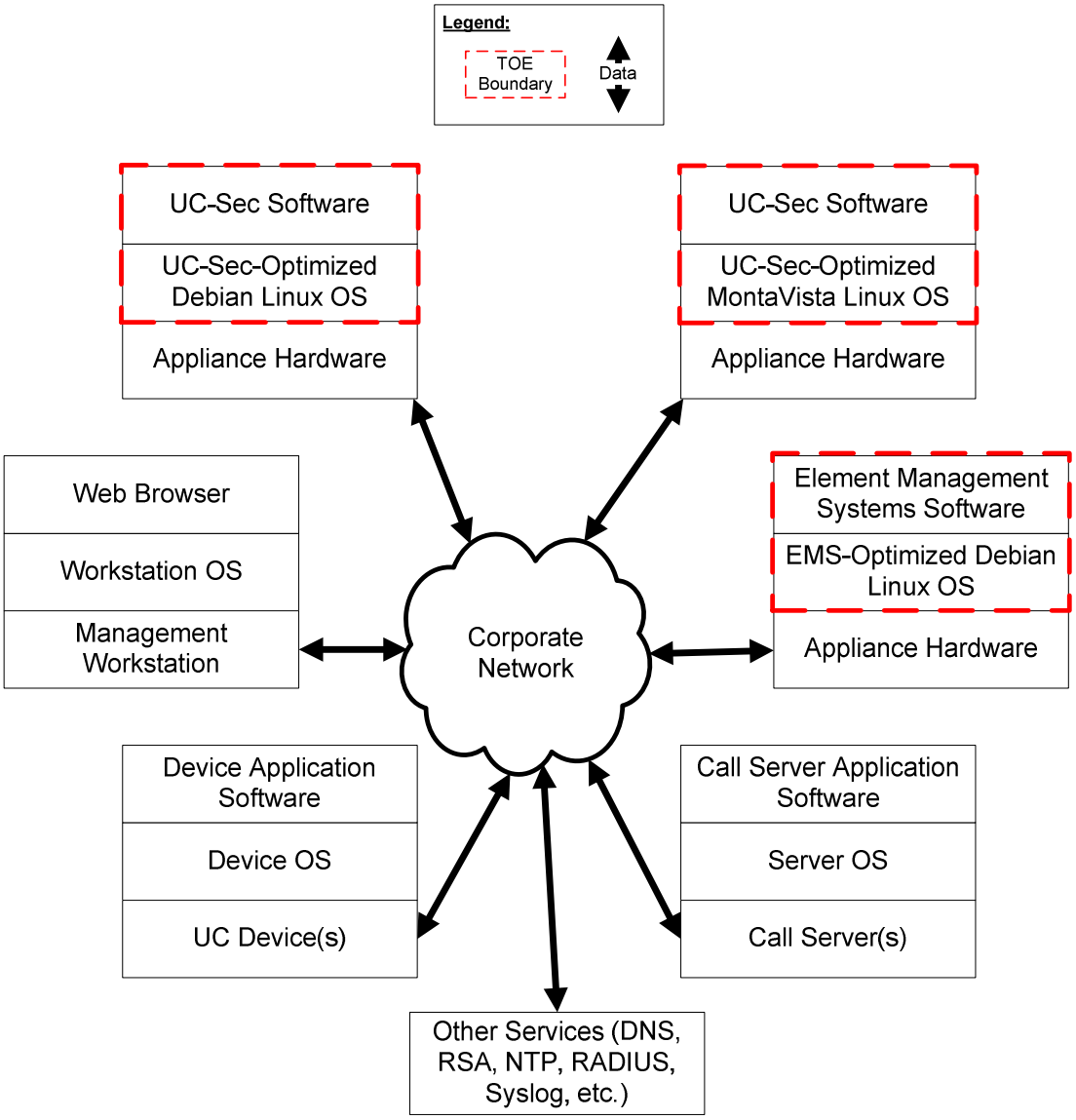


Figure 4 - Physical TOE Boundary

The TOE can be deployed in the DMZ or in the Core network. When deployed in the DMZ, the TOE provides its services to UC devices that lie outside the corporate network and must connect remotely to gain access to devices and services within. When deployed inside the Core network, the TOE provides its services to UC devices operating within the corporate network only.

1.5.1.1 Guidance Documentation

The following guides are required reading and part of the TOE:

- Sipera Systems UC-Sec Release Notes Release 4.0, Part Number: 010-5524-400v1.00
- Sipera Systems UC-Sec Release Notes Release 4.0.0 (Addendum), Part Number: 010-5525-400v1.04
- Sipera Systems UC-Sec Administration Guide Release 4.0, Part Number: 010-5423-400v1.06
- Sipera Systems UC-Sec 1U Installation Guide Release 4.0, Part Number: 101-5224-400v1.01
- Sipera Systems UC-Sec 1U Maintenance Guide Release 4.0, Part Number: 101-5303-400v1.01
- Sipera Systems UC-Sec 2U Installation Guide Release 4.0, Part Number: 102-5224-400v1.01

- Sipera Systems UC-Sec 2U Maintenance Guide Release 4.0, Part Number: 102-5304-400v1.01
- Sipera Systems UC-Sec EMS Installation Guide Release 4.0, Part Number: 100-5224-400v1.01
- Sipera Systems UC-Sec EMS Maintenance Guide Release 4.0, Part Number: 100-5302-400v1.01

1.5.2 Logical Scope

The security functional requirements implemented by the TOE are usefully grouped under the following Security Function Classes:

- Security Audit,
- User Data Protection,
- Identification and Authentication,
- Security Management.

1.5.2.1 Security Audit

The TOE provides the ability to generate audit records for startup and shut down of the audit function, administrator login and logout actions. Within each audit record, the TOE records a timestamp of when the event occurred, the type of event that occurred, the identity of the subject responsible for the event (if applicable), and whether the event succeeded or failed. Administrators can review the audit records through the Syslog Viewer page of the web GUI.

1.5.2.2 User Data Protection

The TOE enforces a Signaling Information Flow Control Security Functional Policy (SFP). The Signaling Information Flow Control SFP controls traffic passed through the TOE between external entities (such as IP phones) based on the legitimacy of the traffic (i.e., no malformed packets) and the rules defined on the TOE.

1.5.2.3 Identification and Authentication

The TOE requires all administrators to identify themselves and authenticate their identities before accessing the management GUI of the TOE. The TOE does not provide any management functionality to unauthenticated administrators.

TOE users communicating via SIP must identify themselves and authenticate their identities before using the TOE if SIP user authentication is enabled. If SIP authentication is not enabled, these users may use the TOE's data interfaces without performing any identification or authentication steps. The TOE supports two-factor authentication for users.

Administrator passwords must conform to a password policy on the TOE. The policy specifies that passwords must be at least eight characters long, include upper- and lower-case letters, special characters and numbers.

1.5.2.4 Security Management

The TOE provides a web GUI that administrators can use to manage the behavior of security functions, security attributes, and TOE Security Function (TSF) data. This GUI on the EMS management device can be used to view statistics collected by UC-Sec appliances across the network, and to push configurations to any UC-Sec within the managed network. The GUI supports three roles: Admin, Manager, and Supervisor. Each role has different permissions depending on whether the UC-Sec appliance being managed is configured for SIP or SCCP traffic.

1.5.3 Product Physical/Logical Features and Functionality not included in the TOE

Features and functionality that are not part of the evaluated configuration of the TOE are:

- the command line interface into the UC-Sec or EMS devices[22],
- SNMP v1 and v2c,
- Cryptoraphic algorithms used by remote user secure tunneling encryption or secure management.

[22] This includes remote (SSH) and local (terminal) access.

2 Conformance Claims

This section provides the identification for any CC, Protection Profile (PP), and EAL package conformance claims. Rationale is provided for any extensions or augmentations to the conformance claims. Rationale for CC and PP conformance claims can be found in Section 8.1.

Table 2 - CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009; CC Part 2 extended; CC Part 3 conformant; Parts 2 and 3 Interpretations from the CEM[23] as of 2009/12/18 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL3 Augmented with Flaw Remediation (ALC_FLR.2)

[23] CEM – Common Evaluation Methodology

3 Security Problem

This section describes the security aspects of the environment in which the TOE will be used and the manner in which the TOE is expected to be employed. It provides the statement of the TOE security environment, which identifies and explains all:

- Known and presumed threats countered by either the TOE or by the security environment
- Organizational security policies with which the TOE must comply
- Assumptions about the secure usage of the TOE, including physical, personnel and connectivity aspects

3.1 Threats to Security

This section identifies the threats to the IT[24] assets against which protection is required by the TOE or by the security environment. The threat agents are divided into two categories:

- Attackers who are not TOE users: They have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources to alter TOE configuration settings or parameters and no physical access to the TOE.
- TOE users: They have extensive knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings or parameters and physical access to the TOE. (TOE users are, however, assumed not to be willfully hostile to the TOE.)

The TOE is intended to protect UC communications generally throughout an enterprise network, as opposed to specific communications channels. As a result, threat agents are assumed to have a low level of motivation. The IT assets requiring protection are the user data saved on or transitioning through the TOE and the hosts on the protected network. Removal, diminution and mitigation of the threats are through the objectives identified in Section 4 Security Objectives. The following threats are applicable:

Table 3 – Threats

Name	Description
T.NOAUTH	An unauthorized person may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.
T.AUDACC	Persons may not be accountable for the actions that they conduct because the audit records are not adequately generated or regularly reviewed, thus allowing an attacker to escape detection.
T.SPOOF	An unauthorized person on an external network may attempt to by-pass the information flow control policy by disguising authentication data (e.g., spoofing the source address) and masquerading as a legitimate user or entity on an internal network.
T.INTERCEPT	An unauthorized person may attempt to intercept a media stream as it is leaving the network protected by the TOE, thereby gaining access to the UC data being exchanged between two parties.
T.MEDIAT	An unauthorized person may send impermissible UC traffic through

[24] IT – Information Technology

Name	Description
	the TOE, which results in the exploitation of resources on the internal network.
T.FLOOD	An unauthorized person may attempt to disable the TOE by sending a flood of traffic intended to overwhelm the TOE's operating capacity.
T.SPAM	An unauthorized person may repeatedly call an individual user, resulting in the user disconnecting their UC device from the network.
T.ROGUE	Errors in the UC network may generate anomalous traffic that uses bandwidth that is needed for legitimate traffic.

3.2 Organizational Security Policies

An Organizational Security Policy (OSP) is a set of security rules, procedures, or guidelines imposed by an organization on the operational environment of the TOE. There are no OSPs defined for this ST.

3.3 Assumptions

This section describes the security aspects of the intended environment for the evaluated TOE. The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user guidance. The following specific conditions are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

Table 4 – Assumptions

Name	Description
A.PHYSEC	The TOE is physically secure.
A.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
A.SINGEN	Real-time UC traffic cannot flow among the internal and external networks unless it passes through the TOE.
A.REMACC	The internal network is configured to allow authorized administrators to access the TOE remotely from within the internal network via the management interface.
A.TUSAGE	The TOE shall not be inadvertently configured, used, and administered in an insecure manner by either authorized or unauthorized persons.
A.TIME	The IT Environment will provide reliable time stamps to the TOE.
A.REMMAN	The IT Environment will provide adequate protection for management and other communications between physically separate TOE components.

4 Security Objectives

Security objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition (see Section 3). The set of security objectives for a TOE form a high-level solution to the security problem. This high-level solution is divided into two part-wise solutions: the security objectives for the TOE, and the security objectives for the TOE's operational environment. This section identifies the security objectives for the TOE and its supporting environment.

4.1 Security Objectives for the TOE

The specific security objectives for the TOE are as follows:

Table 5 - Security Objectives for the TOE

Name	Description
O.SECFUN	The TOE must enable an authorized administrator to use the TOE security functions, and must ensure that only authorized administrators are able to access such functionality.
O.AUDREC	The TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times, and a means to review the audit trail.
O.ACCOUN	The TOE must provide user accountability for UC traffic flows through the TOE and for authorized administrator use of security functions related to audit.
O.MEDIAT	The TOE must mediate the flow of all UC traffic between clients and servers located on internal and external networks governed by the TOE.
O.IDAUTH	The TOE must require that the claimed identity of all administrative users be uniquely identified and authenticated before granting an administrative user access to TOE functions or, for certain specified services, to a connected network, when authentication is enabled for those administrative users.

4.2 Security Objectives for the Operational Environment

4.2.1 IT Security Objectives

The following IT security objectives are to be satisfied by the environment:

Table 6 - IT Security Objectives

Name	Description
OE.SINGEN	The TOE must be placed in the UC network in such a way that no UC traffic can enter or leave the network without traversing the TOE.

Name	Description
OE.TIME	The IT Environment will provide reliable timestamps to the TOE.
OE.AUTH	The IT Environment will provide a means by which the claimed identities of end-users and end-devices can be authenticated.
OE.REMACC	Authorized administrators may access the TOE remotely via the management interface from the internal network.
OE.REMMAN	The IT Environment will provide a means by which traffic between physically separate components of the TOE is protected from unauthorized disclosure and modification.

4.2.2 Non-IT Security Objectives

The following non-IT environment security objectives are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

Table 7 - Non-IT Security Objectives

Name	Description
NOE.PHYSEC	The TOE is physically secure.
NOE.NOEVIL	Authorized administrators are non-hostile, appropriately trained, and follow all administrator guidance; however, they are capable of error.
NOE.GUIDAN	The TOE must be delivered, installed, administered, and operated in a manner that maintains security.

5 Extended Components

This section defines the extended SFRs and extended SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.1.

5.1 Extended TOE Security Functional Components

This section specifies the extended SFRs for the TOE. The extended SFRs are organized by class. Table 8 identifies all extended SFRs implemented by the TOE

Table 8 - Extended TOE Security Functional Requirements

Name	Description
FIA_MAS.1	Multiple authentication support

5.1.1 Class FIA: Identification and Authentication

Identification and Authentication functions involve the requirements to establish and verify a claimed user identity. The extended family and related components for FIA_MAS: Multiple user authentication mechanisms in the environment was modeled after the CC family FIA_UAU: User authentication.

5.1.1.1 Multiple authentication support (FIA_MAS)

Family Behaviour

This family defines the types of user authentication mechanisms supported by the TSF and the TOE Environment.

Component Leveling

Figure 5 – FIA_MAS family decomposition

FIA_MAS.1 Multiple authentication support, provides the capability for administrators to define alternative methods for users or devices to authenticate to the TOE.

Management: FIA_MAS.1

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

- The management of authentication mechanisms;
- The management of the rules for authentication.

Audit: FIA_MAS.1

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

- Minimal: The final decision on authentication.

FIA_MAS.1 Multiple authentication support

Hierarchical to: No other components

Dependencies: No dependencies

This component will provide the capability for administrators to define alternative methods for users or devices to authenticate to the TOE.

FIA_MAS.1.1 The TSF shall ensure that the identity of each end-user or end-device is authenticated according to the [assignment: list of multiple authentication mechanisms].

FIA_MAS.1.2 The TSF shall ensure that each end-user's or end-device's identity is authenticated according to the [assignment: list of rules describing how the multiple authentication mechanisms provide authentication].

5.2 Extended TOE Security Assurance Components

There are no extended SARs defined for this evaluation.

6 Security Requirements

This section defines the SFRs and SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.1.

6.1.1 Conventions

There are several font variations used within this ST. Selected presentation choices are discussed here to aid the Security Target reader.

The CC allows for assignment, refinement, selection and iteration operations to be performed on security functional requirements. All of these operations are used within this ST. These operations are performed as described in Part 2 of the CC, and are shown as follows:

- Completed assignment statements are identified using [*italicized text within brackets*].
- Completed selection statements are identified using [*underlined italicized text within brackets*].
- Refinements are identified using **bold text**. Any text removed is stricken (Example: ~~TSF Data~~) and should be considered as a refinement.
- Extended Functional and Assurance Requirements are identified using a short name not already defined in the CC Standard.
- Iterations are identified by appending a letter in parentheses following the component title. For example, FAU_GEN.1(a) Audit Data Generation would be the first iteration and FAU_GEN.1(b) Audit Data Generation would be the second iteration.

6.2 Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 9 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 9 - TOE Security Functional Requirements

Name	Description	S	A	R	I
FAU_GEN.1	Audit Data Generation	✓	✓		
FAU_SAR.1	Audit review		✓	✓	
FDP_IFC.1	Subset information flow control		✓		
FDP_IFF.1	Simple security attributes		✓		
FIA_MAS.1	Multiple authentication support		✓		
FIA_SOS.1	Verification of secrets		✓		
FIA_UAU.1	Timing of authentication		✓	✓	
FIA_UAU.2	User authentication before any action			✓	
FIA_UID.1	Timing of identification		✓	✓	
FIA_UID.2	User identification before any action			✓	
FMT_MOF.1	Management of security functions behaviour	✓	✓		
FMT_MSA.3	Static attribute initialisation	✓	✓		
FMT_MTD.1	Management of TSF data	✓	✓	✓	
FMT_SMF.1	Specification of management functions		✓		

Name	Description	S	A	R	I
FMT_SMR.1	Security roles		✓	✓	

Note: S=Selection; A=Assignment; R=Refinement; I=Iteration

6.2.1 Class FAU: Security Audit

FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components.

FAU_GEN.1.1

The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events, for the [*not specified*] level of audit; and

c) [*administrator logins, logouts, and login expirations; configuration changes; VOIP activity; and user logins and logouts, device authentications, when authentication is enabled, and authentication failure]*.

FAU_GEN.1.2

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

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*no other audit relevant information*].

Dependencies: FPT_STM.1 Reliable time stamps

FAU_SAR.1 Audit review

Hierarchical to: No other components.

FAU_SAR.1.1

The TSF shall provide [*authorised administrators*] with the capability to read [*all audit information*] from the audit records.

FAU_SAR.1.2

The TSF shall provide the audit records in a manner suitable for the **administrative** users to interpret the information.

Dependencies: FAU_GEN.1 Audit data generation

6.2.2 Class FDP: User Data Protection

FDP_IFC.1 Subset information flow control

Hierarchical to: No other components.

FDP_IFC.1.1

The TSF shall enforce the [*Signaling Information Flow Control SFP*] on

[

a) subjects: external IT entities that send and receive information through the TOE to one another;

b) *Information: traffic sent through the TOE from one subject to another; and*

c) *Operation: pass information*

].

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFF.1 Simple security attributes

Hierarchical to: No other components.

FDP_IFF.1.1

The TSF shall enforce the [*Signaling Information Flow Control SFP*] based on the following types of subject and information security attributes:

[

a) *subject security attributes:*

i. *presumed source address*

b) *information security attributes:*

i. *presumed source address*

ii. *presumed destination address*

iii. *destination port*

iv. *transport layer protocol*

v. *application layer protocol*

vi. *TOE interface on which traffic arrives and departs*

].

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:

[

a) Subjects on an internal network[25] can cause information to flow through the TOE to another connected network if:

i. All the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of values of the information flow security attributes, created by the authorized administrator;

ii. The presumed address of the source subject, in the information, translates to an internal network address;

iii. And the presumed address of the destination subject, in the information, translates to an address on the other connected network.

[25] Internal network refers to the network controlled by the TOE.

b) *Subjects on the external network can cause information to flow through the TOE to another connected network if:*
   i. *All the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;*
   ii. *The presumed address of the source subject, in the information, translates to an external network address;*
   iii. *And the presumed address of the destination subject, in the information,, translates to an address on the other connected network.*

].

FDP_IFF.1.3

The TSF shall enforce the [*no additional rules*].

FDP_IFF.1.4

The TSF shall explicitly authorise an information flow based on the following rules:
[*the Reverse Turing Test function is enabled and the internal user enters the four-digit TOE-generated code*].

FDP_IFF.1.5

The TSF shall explicitly deny an information flow based on the following rules:
[

a) *For application protocols supported by the TOE (e.g., SIP, SCCP), the TOE shall deny any access or service requests that do not conform to its associated published protocol specification (e.g., RFC[26]). This shall be accomplished through protocol filtering proxies that are designed for that purpose.*
b) *The Reverse Turing Test function is enabled and the internal user fails to enter the four-digit TOE-generated code.*

].

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialisation

[26] RFC – Request For Comments

6.2.3 Class FIA: Identification and Authentication

FIA_MAS.1 Multiple authentication support

Hierarchical to: No other components.

FIA_MAS.1.1

The TSF shall ensure that the identity of each end-user or end-device is authenticated according to the [*authentication mechanism enabled for the applicable protocol listed in Table 10 below]*.

FIA_MAS.1.2

The TSF shall ensure that each end-user's or end-device's identity is authenticated according to the [*rules listed in Table 10 below*].

Table 10 – Multiple authentication support

Authentication Mechanism	Protocol	Rules
Single-factor authentication	SIP	When user authentication is enabled for SIP users, allow no TSF-mediated actions until user authenticates with username and password through the TOE Environment.
	SCCP	Authentication not available.
Two-factor authentication	SIP	When two-factor user authentication is enabled for SIP users, allow no TSF-mediated actions until user authenticates with PIN or password, and an authentication token through the TOE Environment.
	SCCP	When two-factor user authentication is enabled for SCCP users, allow no TSF-mediated actions until user authenticates with PIN or password, and an authentication token through the TOE Environment.

Dependencies: No dependencies

FIA_SOS.1 Verification of secrets

Hierarchical to: No other components.

FIA_SOS.1.1

The TSF shall provide a mechanism to verify that secrets meet [*the following password complexity policy for administrators logging in to the GUI: all passwords must at least eight characters long, and include:*

a) *mixed upper- and lower-case characters,*
b) *at least one special character*[27]*, and*
c) *at least one number*].

Dependencies: No dependencies

FIA_UAU.1 Timing of authentication

[27] A special character can be any character that is not one of the alphanumeric (52 upper- and lower-case letters and 10 numbers) characters available on a standard keyboard.

Hierarchical to: No other components.

FIA_UAU.1.1

The TSF shall allow [*no actions when authentication is enabled*] on behalf of the **SIP** user to be performed before the **SIP** user is authenticated.

FIA_UAU.1.2

The TSF shall require each **SIP** user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that **SIP** user **when authentication is enabled**.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

FIA_UAU.2.1

The TSF shall require each **administrative** user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that **administrative** user.

Dependencies: FIA_UID.1 Timing of identification

FIA_UID.1 Timing of identification

Hierarchical to: No other components.

FIA_UID.1.1

The TSF shall allow [*no actions when authentication is enabled*] on behalf of the **SIP** user to be performed before the **SIP** user is identified.

FIA_UID.1.2

The TSF shall require each **SIP** user to be successfully identified before allowing any other TSF-mediated actions on behalf of that **SIP** user **when authentication is enabled**.

Dependencies: No dependencies

FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

FIA_UID.2.1

The TSF shall require each **administrative** user to be successfully identified before allowing any other TSF-mediated actions on behalf of that **administrative** user.

Dependencies: No dependencies

6.2.4 Class FMT: Security Management

The table below represents the access control matrix for the UC-Sec administrator roles. It is referenced in the definition of FMT_MOF.1 and FMT_MTD.1.

Table 11 – FMT Access Control Matrix

Role / Functions	Admin		Manager		Supervisor	
	SIP	SCCP	SIP	SCCP	SIP	SCCP
Administration	determine the behaviour of, disable, enable, modify the behaviour of	determine the behaviour of, disable, enable, modify the behaviour of	modify the behaviour of (cannot create new users)	modify the behaviour of (cannot create new users)	Function not allowed	Function not allowed
Backup/Restore	determine the behaviour of, disable, enable, modify the behaviour of	determine the behaviour of, disable, enable, modify the behaviour of	Function not allowed	Function not allowed	Function not allowed	Function not allowed
Management of Global Parameters	determine the behaviour of, disable, enable, modify the behaviour of	determine the behaviour of, disable, enable, modify the behaviour of	determine the behaviour of, disable, enable, modify the behaviour of	determine the behaviour of, disable, enable, modify the behaviour of	Function not allowed	Function not allowed
Management of Global Profiles	determine the behaviour of, disable, enable, modify the behaviour of	n/a	determine the behaviour of, disable, enable, modify the behaviour of	n/a	Function not allowed	n/a
Management of SIP Cluster	determine the behaviour of, disable, enable, modify the behaviour of	n/a	determine the behaviour of, disable, enable, modify the behaviour of	n/a	Function not allowed	n/a
Management of SCCP Cluster	n/a	determine the behaviour of, disable, enable, modify the behaviour of	n/a	determine the behaviour of, disable, enable, modify the behaviour of	n/a	Function not allowed
Management of Domain Policies	determine the behaviour of, disable, enable, modify the behaviour of	n/a	determine the behaviour of, disable, enable, modify the behaviour of	n/a	Function not allowed	n/a

Role / Functions	Admin		Manager		Supervisor	
	SIP	SCCP	SIP	SCCP	SIP	SCCP
Management of Device Specific Settings	determine the behaviour of, disable, enable, modify the behaviour of	determine the behaviour of, disable, enable, modify the behaviour of	determine the behaviour of, disable, enable, modify the behaviour of	determine the behaviour of, disable, enable, modify the behaviour of	Function not allowed	Function not allowed
Troubleshooting	determine the behaviour of, disable, enable, modify the behaviour of	determine the behaviour of, disable, enable, modify the behaviour of	determine the behaviour of, disable, enable, modify the behaviour of	determine the behaviour of, disable, enable, modify the behaviour of	Function not allowed	Function not allowed
TLS Management	determine the behaviour of, disable, enable, modify the behaviour of	determine the behaviour of, disable, enable, modify the behaviour of	determine the behaviour of, disable, enable, modify the behaviour of	determine the behaviour of, disable, enable, modify the behaviour of	Function not allowed	Function not allowed
Management of IM Logging	determine the behaviour of, disable, enable, modify the behaviour of	n/a	determine the behaviour of, disable, enable, modify the behaviour of	n/a	Function not allowed	n/a
View Incidence and Statistical Logs	Determine the behaviour of	Determine the behaviour of	Determine the behaviour of	Determine the behaviour of	Determine the behaviour of	Determine the behaviour of
TSF Data						
Audit logs	Query, enable, disable	Query, enable, disable	Query, enable, disable	Query, enable, disable	Query Incidence and Statistical logs	Query Incidence and Statistical logs
Signaling Information Flow Control SFP rules	change_default, query, modify, delete	change_default, query, modify, delete	change_default, query, modify, delete	change_default, query, modify, delete	Function not allowed	Function not allowed

FMT_MOF.1 Management of security functions behaviour
Hierarchical to: No other components.
FMT_MOF.1.1

The TSF shall restrict the ability to [*determine the behaviour of, disable, enable, modify the behaviour of*] the functions [*listed in Table 11 above*] to [*the administrator roles listed in Table 11 above*].

Dependencies: **FMT_SMF.1 Specification of management functions**
FMT_SMR.1 Security roles

FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

FMT_MSA.3.1

The TSF shall enforce the [*Signaling Information Flow Control SFP*] to provide [*restrictive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2

The TSF shall allow the [*SIP Admin, SCCP Admin*] to specify alternative initial values to override the default values when an object or information is created.

Dependencies: **FMT_MSA.1 Management of security attributes**
FMT_SMR.1 Security roles

FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1

The TSF shall restrict the ability to [*change_default, query, modify, delete* **as specified in Table 11 above**] the [*TSF data listed in Table 11 above*] to [*the administrator roles listed in Table 11 above*].

Dependencies: **FMT_SMF.1 Specification of management functions**
FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1.1

The TSF shall be capable of performing the following management functions: [*management of security functions, management of security attributes, and management of TSF data*].

Dependencies: **No Dependencies**

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1

The TSF shall maintain the roles [*SIP Admin, SCCP Admin, SIP Manager, SCCP Manager, SIP Supervisor, SCCP Supervisor*].

FMT_SMR.1.2

The TSF shall be able to associate **administrative** users with roles.

Dependencies: **FIA_UID.1 Timing of identification**

6.3 Security Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL3 augmented with ALC_FLR.2. Table 12 - Assurance Requirements summarizes the requirements.

Table 12 - Assurance Requirements

Assurance Requirements	
Class ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
Class ALC : Life Cycle Support	ALC_CMC.3 Authorisation controls
	ALC_CMS.3 Implementation representation CM[28] coverage
	ALC_DEL.1 Delivery Procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_FLR.2 Flaw reporting procedures
Class ADV: Development	ADV_ARC.1 Security Architecture Description
	ADV_FSP.3 Functional Specification with complete summary
	ADV_TDS.2 Architectural design
Class AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Class ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Class AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

[28] CM – Configuration Management

7 TOE Summary Specification

This section presents information to detail how the TOE meets the functional requirements described in previous sections of this ST.

7.1 TOE Security Functions

Each of the security requirements and the associated descriptions correspond to the security functions. Hence, each function is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functions and rationalize that the security functions satisfy the necessary requirements.

Table 13 - Mapping of TOE Security Functions to Security Functional Requirements

TOE Security Function	SFR ID	Description
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_SAR.1	Audit review
User Data Protection	FDP_IFC.1	Subset information flow control
	FDP_IFF.1	Simple security attributes
Identification and Authentication	FIA_MAS.1	Multiple authentication support
	FIA_SOS.1	Verification of secrets
	FIA_UAU.1	Timing of authentication
	FIA_UAU.2	User authentication before any action
	FIA_UID.1	Timing of identification
	FIA_UID.2	User identification before any action
Security Management	FMT_MOF.1	Management of security functions behaviour
	FMT_MSA.3	Static attribute initialisation
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles

7.1.1 Security Audit

FAU_GEN.1

The TOE provides the ability to generate audit records for startup and shut down of the UC-Sec node, authentication success or failure, all configuration changes by administrator actions, and user events that are captured within billing call detail records.

The TOE audit records contain the following information:

Table 14 - Audit Record Contents

Field	Content
Timestamp	Date and time that the event occurred.
Category	Classifies events into relevant categories.
Device	Identity of the entity responsible for generating the audit message.
Incident/syslog specific data	Specifies for each message whether the audited action completed successfully or not.

FAU_SAR.1

All audit records can be viewed via the Syslog Viewer page of the web GUI.

TOE Security Functional Requirements Satisfied: FAU_GEN.1, FAU_SAR.1.

7.1.2 User Data Protection

FDP_IFC.1, FDP_IFF.1

The Signaling Information Flow Control SFP limits the information that external entities can pass through the TOE to one another. Decisions on whether to allow traffic to pass through the TOE are based upon an administrator-defined rule set and activated features, such as application layer message inspection and intrusion protection features. These features work together to ensure that only valid traffic is passed through the TOE and that any potentially harmful traffic is blocked.

TOE Security Functional Requirements Satisfied: FDP_IFC.1, FDP_IFF.1.

7.1.3 Identification and Authentication

FIA_UAU.1, FIA_UID.1, FIA_MAS.1

The TOE can require SIP users to identify themselves and authenticate their identities through a RADIUS server before passing traffic through the TOE, but this feature can be disabled or enabled by administrators. When enabled, users must authenticate based on a configured time period (e.g. once per day, once per week, etc.) If this feature is disabled, then all users can send legitimate traffic through the TOE.

The TOE offers a two-factor authentication mechanism for SIP or SCCP users. When enabled, users must authenticate their identities through a RADIUS server and an RSA authentication server via a two-factor authentication mechanism that requires a password or PIN and an RSA SecurID token.

FIA_UAU.2, FIA_UID.2

Administrators accessing the GUI to manage the TOE must identify themselves and authenticate their identities before access any of the management features available via the GUI. The TOE supports local authentication and RADIUS authentication.

FIA_SOS.1

The TOE enforces a password policy for all local administrator accounts. This password policy is hard-coded and requires that administrator passwords conform to the following rules:

- must be at least eight characters long,
- must contain mixed upper- and lower-case letters,
- must contain at least one special character, and
- must contain at least one number,

TOE Security Functional Requirements Satisfied: FIA_SOS.1, FIA_UAU.1, FIA_UAU.2, FIA_MAS.1, FIA_UID.1, FIA_UID.2.

7.1.4 Security Management

FMT_MOF.1, FMT_MTD.1, FMT_SMF.1

The GUI provided by the TOE allows administrators to manage the behavior of the security functions and TSF data as specified in Table 11 above. All management occurs through the EMS GUI. The EMS GUI allows remote centralized management and aggregation of all UC-Sec devices on the managed network. Permissions are based upon hard-coded roles that can only be assigned by an administrator with the "Admin" role.

FMT_MSA.3

The Signaling Information Flow Control SFP provides restrictive default values. Administrator-defined firewall rules control user UC traffic and default to a "Reject all" rule if no other rules apply.

FMT_SMR.1

The TOE maintains six roles on the GUI. Roles specify the type of protocol the UC network is based on (SIP or SCCP) and the permissions available to the administrator. The roles are: Admin for SIP or SCCP, Manager for SIP or SCCP, and Supervisor for SIP or SCCP. Each device is configured to run in a SIP or SCCP mode during the product installation. Therefore, only three roles are available for administrators at any given moment for a single UC-Sec appliance, although different configuration options are available depending on whether the UC-Sec is set to SIP or SCCP mode.

TOE Security Functional Requirements Satisfied: FMT_MOF.1, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1.

8 Rationale

8.1 Conformance Claims Rationale

This Security Target extends Part 2 and conforms to Part 3 of the Common Criteria Standard for Information Technology Security Evaluations, version 3.1 revision 3.

8.2 Security Objectives Rationale

This section provides a rationale for the existence of each threat, policy statement, and assumption that compose the Security Target. Sections 8.2.1, 8.2.2, and 8.2.3 demonstrate the mappings between the threats, polices, and assumptions to the security objectives is complete. The following discussion provides detailed evidence of coverage for each threat, policy, and assumption.

8.2.1 Security Objectives Rationale Relating to Threats

Table Table 15 displays the mapping of threats to objectives.

Table 15 – Threats:Objectives Mapping

Threats	Objectives	Rationale
T.NOAUTH An unauthorized person may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.	O.SECFUN The TOE must enable an authorized administrator to use the TOE security functions, and must ensure that only authorized administrators are able to access such functionality.	O.SECFUN counters this threat by requiring the TOE to provide functionality that enables an authorized administrator to use the TOE security functions, and ensure that only authorized administrators are able to access such functionality.
	O.IDAUTH The TOE must require that the claimed identity of all administrative users be uniquely identified and authenticated before granting an administrative user access to TOE functions or, for certain specified services, to a connected network, when authentication is enabled for those administrative users.	O.IDAUTH counters this threat by requiring that the claimed identity of all users be uniquely identified and authenticated users and administrators before granting access to TOE functions and data, or to a connected network, when authentication is enabled.
	OE.AUTH The IT Environment will provide a means by which the claimed identities of end-users and end-devices can be authenticated.	OE.AUTH counters this threat by requiring that the IT Environment provide a means by which the claimed identities of end-users and end-devices can be authenticated.
T.AUDACC Persons may not be accountable for the actions that they conduct because the audit records are not adequately generated or regularly reviewed, thus allowing an attacker	O.AUDREC The TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times, and a means to review the audit trail.	O.AUDREC counters this threat by requiring the TOE to provide a readable audit trail of security-related events, thereby allowing authorized administrators to discover attacker actions.

Threats	Objectives	Rationale
to escape detection.	O.ACCOUN The TOE must provide user accountability for UC traffic flows through the TOE and for authorized administrator use of security functions related to audit.	O.ACCOUN counters this threat by requiring the TOE to provide user accountability for UC traffic flows through the TOE and for authorized administrator use of security function.
T.SPOOF An unauthorized person on an external network may attempt to by-pass the information flow control policy by disguising authentication data (e.g., spoofing the source address) and masquerading as a legitimate user or entity on an internal network.	O.MEDIAT The TOE must mediate the flow of all UC traffic between clients and servers located on internal and external networks governed by the TOE.	O.MEDIAT counters this threat by requiring the TOE to enforce the Signaling Information Flow Control policy to mediate the flow of all information between clients and servers, thereby preventing unauthorized users from bypassing the Signaling Information Flow Control policy.
T.INTERCEPT An unauthorized person may attempt to intercept a media stream as it is leaving the network protected by the TOE, thereby gaining access to the UC data being exchanged between two parties.	O.MEDIAT The TOE must mediate the flow of all UC traffic between clients and servers located on internal and external networks governed by the TOE.	O.MEDIAT counters this threat by providing the TOE with the ability to adequately protect traffic being sent through the TOE between internal and external users.
T.MEDIAT An unauthorized person may send impermissible UC traffic through the TOE, which results in the exploitation of resources on the internal network.	O.MEDIAT The TOE must mediate the flow of all UC traffic between clients and servers located on internal and external networks governed by the TOE.	O.MEDIAT counters this threat by requiring the TOE to mediate the flow of all UC traffic between clients and servers, thereby restricting UC traffic flowing through the TOE to the internal network.
T.INTERCEPT An unauthorized person may attempt to intercept a media stream as it is leaving the network protected by the TOE, thereby gaining access to the UC data being exchanged between two parties.	OE.SINGEN The TOE must be placed in the UC network in such a way that no UC traffic can enter or leave the network without traversing the TOE.	OE.SINGEN counters this threat by ensuring that all traffic entering or leaving the network that the TOE protects passes through the TOE.
T.FLOOD An unauthorized person may attempt to disable the TOE by sending a flood of traffic intended to overwhelm the TOE's operating capacity.	O.MEDIAT The TOE must mediate the flow of all UC traffic between clients and servers located on internal and external networks governed by the TOE.	O.MEDIAT counters this threat by requiring the TOE to have control over UC data flows, thereby allowing the TOE to detect and stop flooding attacks.
T.SPAM An unauthorized person may repeatedly call an individual user, resulting in the user disconnecting their UC device from the network.	O.MEDIAT The TOE must mediate the flow of all UC traffic between clients and servers located on internal and external networks governed by the TOE.	O.MEDIAT counters this threat by allowing users to blacklist numbers, thereby preventing unwanted spam from reaching their UC devices.
T.ROGUE	O.MEDIAT	O.MEDIAT counters this threat

Threats	Objectives	Rationale
Errors in the UC network may generate anomalous traffic that uses bandwidth that is needed for legitimate traffic.	The TOE must mediate the flow of all UC traffic between clients and servers located on internal and external networks governed by the TOE.	by allowing administrators to configure the TOE to detect and remove rogue media, thereby freeing up bandwidth for legitimate traffic.

Every Threat is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives counter all defined threats.

8.2.2 Security Objectives Rationale Relating to Policies

There are no Organizational Security Policies defined for this Security Target. Therefore, there are no Security Objectives relating to policies.

8.2.3 Security Objectives Rationale Relating to Assumptions

Table 16 - Assumptions:Objectives Mapping

Assumptions	Objectives	Rationale
A.PHYSEC The TOE is physically secure.	NOE.PHYSEC The TOE is physically secure.	NOE.PHYSEC upholds this assumption by providing for the physical protection of the TOE hardware and software.
A.NOEVIL Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.	NOE.NOEVIL Authorized administrators are non-hostile, appropriately trained, and follow all administrator guidance; however, they are capable of error.	NOE.NOEVIL upholds this assumption by ensuring that all users assigned to manage the TOE are non-hostile, appropriately trained, and follow all administrator guidance.
A.SINGEN Real-time UC traffic cannot flow among the internal and external networks unless it passes through the TOE.	OE.SINGEN The TOE must be placed in the UC network in such a way that no UC traffic can enter or leave the network without traversing the TOE.	OE.SINGEN upholds this assumption by ensuring that information cannot flow among the internal and external networks without first passing through the TOE.
A.REMACC The internal network is configured to allow authorized administrators to access the TOE remotely from within the internal network via the management interface.	OE.REMACC Authorized administrators may access the TOE remotely via the management interface from the internal network.	OE.REMACC upholds this assumption by ensuring that authorized administrators may access the TOE remotely from the internal networks.
A.TUSAGE The TOE shall not be inadvertently configured, used, and administered in an insecure manner by either authorized or unauthorized	NOE.GUIDAN The TOE must be delivered, installed, administered, and operated in a manner that maintains security.	NOE.GUIDAN upholds this assumption by ensuring that the TOE must be delivered, installed, administered, and operated in a manner that maintains security.

Assumptions	Objectives	Rationale
persons.		
A.TIME The IT Environment will provide reliable time stamps to the TOE.	OE.TIME The IT Environment will provide reliable timestamps to the TOE.	The OE.TIME objective supports this assumption by requiring reliable time stamps to be available for the TOE's use.
A.REMMAN The IT Environment will provide adequate protection for management and other communications between physically separate TOE components.	OE.REMMAN The IT Environment will provide a means by which traffic between physically separate components of the TOE is protected from unauthorized disclosure and modification.	OE.REMMAN upholds this assumption by ensuring that the IT Environment protects traffic being exchanged by physically separate TOE components from unauthorized disclosure or modification.

Every assumption is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives uphold all defined assumptions.

8.3 Rationale for Extended Security Functional Requirements

FIA_MAS.1 was created to address the multiple authentication support that the TOE provides via the IT Environment. The actual two-factor authentication mechanisms are provided by third-party servers, and therefore an extended component was required to cover this feature as implemented.

8.4 Rationale for Extended TOE Security Assurance Requirements

There are no extended TOE security assurance requirements defined for this ST.

8.5 Security Requirements Rationale

The following discussion provides detailed evidence of coverage for each security objective.

8.5.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 17 - Objectives:SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.SECFUN The TOE must enable an authorized administrator to use the TOE security functions, and must ensure that only authorized	FIA_UAU.2 User authentication before any action	FIA_UAU.2 supports this objective by requiring administrators to authenticate before allowing them to perform any actions on the TOE.

Objective	Requirements Addressing the Objective	Rationale
administrators are able to access such functionality.	FIA_UID.2 User identification before any action	FIA_UID.2 supports this objective by requiring administrators to identify themselves before allowing them to perform any actions on the TOE.
	FMT_MOF.1 Management of security functions behaviour	FMT_MOF.1 supports this objective by providing the capability for administrators to manage the behaviour of security functions.
	FMT_MTD.1 Management of TSF data	FMT_MTD.1 supports this objective by providing the capability for administrators to manage the TSF data.
	FMT_SMF.1 Specification of management functions	FMT_SMF.1 supports this objective by specifying the management functions that administrators are capable of using.
	FMT_SMR.1 Security roles	FMT_SMR.1 supports this objective by defining roles for administrators, which are used to enforce the access control policy.
O.AUDREC The TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times, and a means to review the audit trail.	FAU_GEN.1 Audit Data Generation	FAU_GEN.1 supports this objective by providing an audit trail listing all authentication and configuration actions on the TOE and on the UC traffic passing through the TOE.
	FAU_SAR.1 Audit review	FAU_SAR.1 supports this objective by ensuring that authorized administrators are able to read and interpret all audit information from the audit records.
O.ACCOUN The TOE must provide user accountability for UC traffic flows through the TOE and for authorized administrator use of security functions related to audit.	FAU_GEN.1 Audit Data Generation	FAU_GEN.1 supports this objective by providing an audit trail listing all authentication and configuration actions on the TOE and on the UC traffic passing through the TOE.
O.MEDIAT The TOE must mediate the flow of all UC traffic between clients and servers located on internal and external networks governed by the TOE.	FDP_IFC.1 Subset information flow control	FDP_IFC.1 supports this objective by enforcing an information flow control policy on traffic passing through the TOE.
	FDP_IFF.1 Simple security attributes	FDP_IFF.1 supports this objective by defining the attributes that are

Objective	Requirements Addressing the Objective	Rationale
		used to enforce the information flow control policy.
	FMT_MSA.3 Static attribute initialisation	FMT_MSA.3 supports this objective by defining the information flow control policy as restrictive by default.
	FMT_SMF.1 Specification of management functions	FMT_SMF.1 supports this objective by specifying that administrators are capable of defining the information flow control policy rules.
O.IDAUTH The TOE must require that the claimed identity of all administrative users be uniquely identified and authenticated before granting an administrative user access to TOE functions or, for certain specified services, to a connected network, when authentication is enabled for those administrative users.	FIA_MAS.1 Multiple authentication support	FIA_MAS.1 supports this objective by requiring that all SIP or SCCP users be successfully authenticated using two- factor authentication before allowing any other TSF-mediated actions on behalf of that user when two-factor authentication is enabled for SIP or SCCP users.
	FIA_SOS.1 Verification of secrets	FIA_SOS.1 supports this objective by enforcing a password policy to be used by the TOE when authenticating administrators through the GUI.
	FIA_UAU.1 Timing of authentication	FIA_UAU.1 supports this objective by requiring that all SIP users be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user when authentication is enabled for SIP users.
	FIA_UAU.2 User authentication before any action	FIA_UAU.2 supports this objective by requiring that all administrators be successfully authenticated before allowing any other TSF-mediated actions on behalf of that administrator.
	FIA_UID.1 Timing of identification	FIA_UAU.1 supports this objective by requiring that all SIP users be successfully identified before allowing any other TSF-mediated actions on behalf of that user when authentication is enabled for SIP users.
	FIA_UID.2	FIA_UID.2 supports this objective

Objective	Requirements Addressing the Objective	Rationale
	User identification before any action	by requiring that all administrators be successfully identified before allowing any other TSF-mediated actions on behalf of that administrator.

8.5.2 Security Assurance Requirements Rationale

EAL3 was chosen to provide a moderate level of assurance that is consistent with good commercial practices. As such, minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. While the System may monitor a hostile environment and protect it against malicious entities, the TOE is expected to be placed in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. At EAL3, the System will have incurred a search for obvious flaws to support its introduction into the non-hostile environment.

The augmentation of ALC_FLR.2 was chosen to give greater assurance of the developer's on-going flaw remediation processes.

8.5.3 Dependency Rationale

This ST does satisfy all the requirement dependencies of the Common Criteria. Table 18 lists each requirement to which the TOE claims conformance with a dependency and indicates whether the dependent requirement was included. As the table indicates, all dependencies have been met.

Table 18 - Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	FPT_STM.1 is not included because reliable time stamps are provided by the environment. An environmental objective states that the TOE will receive reliable time stamps.
FAU_SAR.1	FAU_GEN.1	✓	
FDP_IFC.1	FDP_IFF.1	✓	
FDP_IFF.1	FDP_IFC.1	✓	
	FMT_MSA.3	✓	
FIA_MAS.1	No dependencies		
FIA_SOS.1	No dependencies		

SFR ID	Dependencies	Dependency Met	Rationale
FIA_UAU.1	FIA_UID.1	✓	
FIA_UAU.2	FIA_UID.1	✓	Although FIA_UID.1 for the administrative user is not included, FIA_UID.2, which is hierarchical to FIA_UID.1, is included. This satisfies this dependency.
FIA_UID.1	No dependencies		
FIA_UID.2	No dependencies		
FMT_MOF.1	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.3	FMT_MSA.1		FMT_MSA.1 is not required as a dependency for FMT_MSA.3 because the security attributes used by the Signaling Information Flow Control SFP are never queried, modified, or deleted by an administrator.
	FMT_SMR.1	✓	
FMT_MTD.1	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_SMF.1	No dependencies		
FMT_SMR.1	FIA_UID.1	✓	Although FIA_UID.1 is not included for administrative users, FIA_UID.2, which is hierarchical to FIA_UID.1, is included. This satisfies this dependency.

9 Acronyms

This section describes the acronyms.

9.1 Acronyms

Table 19 – Acronyms

Acronym	Definition
CC	Common Criteria
CEM	Common Evaluation Methodology
CM	Configuration Management
DMZ	De-Militarized Zone
DNS	Domain Name System
DOS	Denial-Of-Service
EAL	Evaluation Assurance Level
EMS	Elements Management System
FW	Firewall
GUI	Graphical User Interface
HA	High Availability
HTTPS	Secure Hypertext Transfer Protocol
IM	Instant Messaging
IP	Internet Protocol
IPCS	Previous versions of the UC-Sec were referred to as IPCS
ISP	Internet Service Provider
IT	Information Technology
NAT	Network Address Translation
NTP	Network Time Protocol
OS	Operating System
OSP	Organizational Security Policy
PBX	Public Branch Exchange
PIN	Personal Identification Number
PP	Protection Profile
RADIUS	Remote Access Dial-In User Service
RFC	Request For Comments
RTP	Real-time Transport Protocol
SAR	Security Assurance Requirement

Acronym	Definition
SCCP	Skinny Client Control Protocol
SFP	Security Functional Policy
SFR	Security Functional Requirement
SIP	Session Initiation Protocol
SNMP	Simple Network Management Protocol
SRTP	Secure Real-time Transport Protocol
SSH	Secure Shell
ST	Security Target
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
U	Unit
UC	Unified Communications
VoIP	Voice over Internet Protocol
WiFi	Wireless Fidelity

Prepared by:
Corsec Security, Inc.

10340 Democracy Lane, Suite 201
Fairfax, VA 22030

Phone: (703) 267-6050
Email: info@corsec.com
http://www.corsec.com