Oracle® Communications Session Border Controller

Security Guide

Release S-Cz9.3.0 - for Service Provider and Enterprise

F92222-01
March 2024

ORACLE

Oracle Communications Session Border Controller Security Guide, Release S-Cz9.3.0 - for Service Provider and Enterprise

F92222-01

Contents

About this Guide

The Oracle Session Border Controller (SBC) family of products are designed to increase security when deploying Voice over IP (VoIP) or Unified Communications (UC) solutions. Properly configured, Oracle's SBC family helps protect IT assets, safeguard confidential information, and mitigate risks—all while ensuring the high service levels which users expect from the corporate phone system and the public telephone network.

This publication is used with Oracle Communications Session Border Controller and Oracle Enterprise Session Border Controller.

Documentation Set

The following table lists related documentation.

Document Name	Document Description
Acme Packet 3900 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 3900.
Acme Packet 4600 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 4600.
Acme Packet 4900 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 3950 and Acme Packet 4900.
Acme Packet 6100 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 6100.
Acme Packet 6300 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 6300.
Acme Packet 6350 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 6350.
Release Notes	Contains information about the current documentation set release, including new features and management changes.
Known Issues & Caveats	Contains known issues and caveats
Configuration Guide	Contains information about the administration and software configuration of the Service Provider Session Border Controller (SBC).
ACLI Reference Guide	Contains explanations of how to use the ACLI, as an alphabetical listings and descriptions of all ACLI commands and configuration parameters.
Maintenance and Troubleshooting Guide	Contains information about SBC logs, performance announcements, system management, inventory management, upgrades, working with configurations, and managing backups and archives.

Document Name	Document Description
MIB Guide	Contains information about Management Information Base (MIBs), Oracle Communication's enterprise MIBs, general trap information, including specific details about standard traps and enterprise traps, Simple Network Management Protocol (SNMP) GET query information (including standard and enterprise SNMP GET query names, object identifier names and numbers, and descriptions), examples of scalar and table objects.
Accounting Guide	Contains information about the SBC's accounting support, including details about RADIUS and Diameter accounting.
HDR Guide	Contains information about the SBC's Historical Data Recording (HDR) feature. This guide includes HDR configuration and system-wide statistical information.
Admin Security Guide	Contains information about the SBC's support for its Administrative Security license.
Security Guide	Contains information about security considerations and best practices from a network and application security perspective for the SBC family of products.
Platform Preparation and Installation Guide	Contains information about upgrading system images and any pre-boot system provisioning.
Call Traffic Monitoring Guide	Contains information about traffic monitoring and packet traces as collected on the system. This guide also includes WebGUI configuration used for the SIP Monitor and Trace application.
HMR Guide	Contains information about configuring and using Header Manipulation Rules to manage service traffic.
REST API	Contains information about the supported REST APIs and how to use the REST API interface.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

My Oracle Support

My Oracle Support (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with My Oracle Support registration.

Call the CAS main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. When calling, make the selections in the sequence shown below on the Support telephone menu:

1. Select `2` for New Service Request.
2. Select `3` for Hardware, Networking, and Solaris Operating System Support.
3. Select one of the following options:
   - For technical issues such as creating a new Service Request (SR), select `1`.

- For non-technical issues such as registration or assistance with My Oracle Support, select 2.

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

Emergency Response

In the event of a critical service situation, emergency response is offered by the Customer Access Support (CAS) main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.

Locate Product Documentation on the Oracle Help Center Site

Oracle Communications customer documentation is available on the web at the Oracle Help Center (OHC) site, http://docs.oracle.com. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at http://www.adobe.com.

1. Access the Oracle Help Center site at http://docs.oracle.com.
2. Click **Industries**.
3. Under the Oracle Communications sub-header, click the **Oracle Communications documentation** link.
   The Communications Documentation page appears. Most products covered by these documentation sets appear under the headings "Network Session Delivery and Control Infrastructure" or "Platforms."
4. Click on your Product and then Release Number.
   A list of the entire documentation set for the selected product and release appears.
5. To download a file to your location, right-click the **PDF** link, select **Save target as** (or similar command based on your browser), and save to a local folder.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Revision History

The following table shows the dates and descriptions of revisions to the Security Guide.

Date	Description
March 2024	• Initial release

1 General Security Principles

The following principles are fundamental to using any application securely.

Keep Software Up To Date

One of the principles of good security practice is to keep all software versions up to date. Oracle maintains multiple SBC streams or versions that are updated with applicable security patches. Always review the Critical Patch Updates and Release Notes relevant to the stream installed to determine whether an update should be applied.

Restrict Network Access to Critical Services

By design, the SBC family defaults to a closed state. No signaling or media can pass through the system unless it is explicitly configured.

Only services required for initial configuration of the system are available on a dedicated management Ethernet port (wancom0) which should be connected to a management network. Insecure services such as telnet and FTP should be disabled. Access to management services should be protected through the use of system level Access Control Lists (ACL) specifying allowed IP address ranges.

Signaling and media are only available on a separate set of Ethernet ports designated for services. ACLs should also be used on services ports for SIP peering deployments where possible. Some management capabilities can be enabled on these services ports by an administrator, so care should be taken to determine the risk of doing so in individual cases. In general it is not recommended to enable services other than perhaps ICMP.

Services should also be protected from DoS abuse through configuration of call admission controls, signaling thresholds, blocklisting, and attack tool detection, elements covered as part of this guide.

Follow the Principle of Least Privilege

The SBC family provides some implicit least privilege because direct user access is usually not provided. In most cases, the system acts as a proxy device so there is no direct user interaction. In other cases the system may provide a registrar function. However, providing the registrar function does not give the user access to any system level commands.

Administrators are the only ones who have any sort of system logon permissions. The system provides Role Based Access Control with dedicated user accounts that have pre-assigned privilege levels in the Command Line Interface. These are discussed further in the section on management interfaces. RADIUS and TACACS+ can be enabled as well to enable an outside authentication and authorization function. The minimum authorization class for RADIUS and command set should be considered for the administrator’s role.

Monitor System Activity

Monitoring system activity is critical to determine if someone is attempting to abuse system services and to detect if there are performance or availability issues. Useful monitoring information can be acquired through SNMP, RADIUS accounting, Historical Data Recording

(HDR), and Syslog. At a minimum SNMP should be configured, and use of an external syslog server should be considered.

Keep Up To Date on Latest Security Information

Security issues that require a software or configuration update will be communicated in quarterly Critical Patch Updates (CPU). The latest CPUs as well as instructions to subscribe to them can be found at http://www.oracle.com/technetwork/topics/security/alerts-086861.html. A free Oracle Technology Network account is required to receive CPUs.

Overview

The Oracle Session Border Controller (SBC) family of products is designed to increase security, when deploying Voice over IP (VoIP) or Unified Communications (UC) solutions. Oracle's SBC family helps to protect IT assets, safeguard confidential information, and mitigate risks, while ensuring the high levels of service that users expect from the corporate phone system and the public telephone network.

Installed at the network perimeter, the SBC family of products provides a demarcation and enforcement point for the UC network. The primary security functions include:

- Overload protection to prevent DoS attacks and registration floods
- Access control to inhibit toll fraud and service theft
- Topology hiding to counter topology discovery through reconnaissance scans
- Encryption and authentication to ensure privacy and prevent loss of confidential information
- Protocol validation to combat fuzzing and other types of malicious attacks

Net-SAFE Security Framework

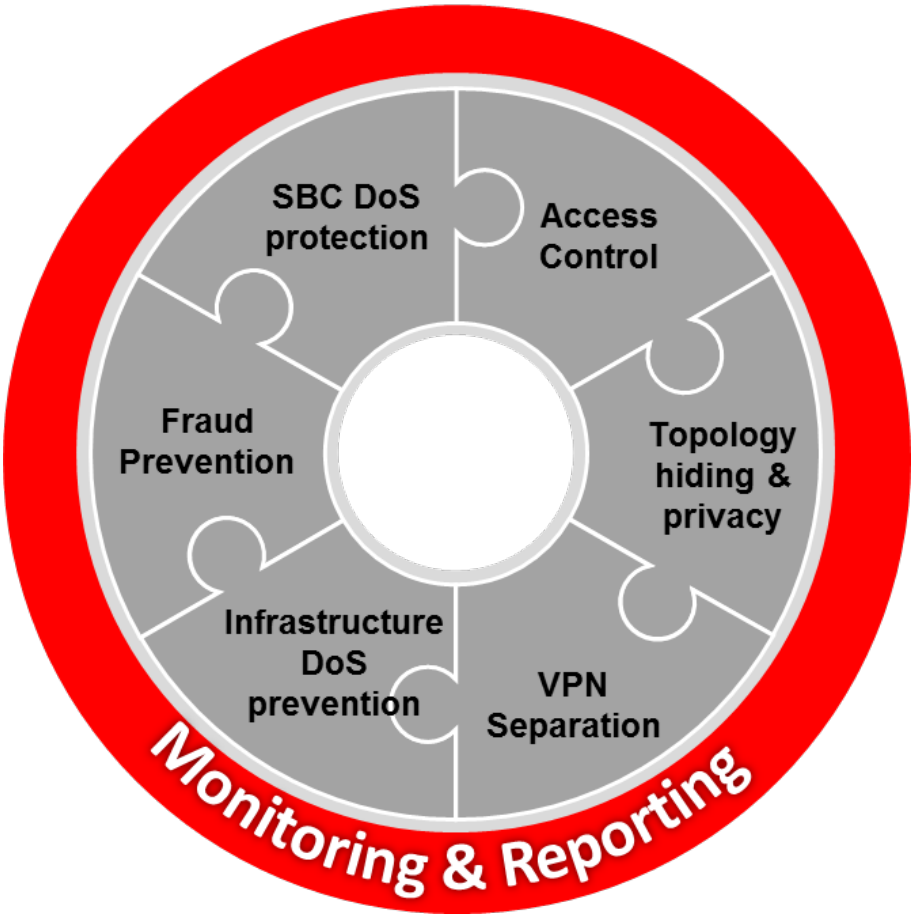
The Oracle Net-SAFE™ security framework addresses the unique security challenges of delivering SIP-based interactive IP communications over the Internet. The Net-SAFE framework includes advanced security features, a highly-scalable architecture, and comprehensive monitoring and reporting capabilities. The framework reduces risk in UC services and applications by ensuring confidentiality, integrity, and availability.

Net-SAFE goals are as follows:

- Protect the SBC—The first line of defense at the border is the SBC, which must be secure and resistant to attacks and overload.
- Protect the infrastructure—The infrastructure includes the customer’s network of multimedia equipment (soft switches, application servers, SIP proxies, H.323 gatekeepers, gateways, and others).
- Protect the service—Preventing attacks is not enough. UC services that generate revenue need to remain in service.

Example 1-1 Net-SAFE Requirements

The Net-SAFE framework identifies the requirements that an SBC must satisfy to meet the goals of the framework and provide confidentiality, integrity, and availability.



The Net-SAFE Framework spans seven general functions.

1. Denial of Service (DoS) protection
   - Dynamic self-protection against malicious and non-malicious DoS attacks and overloads at layers 3 and 4 (TCP, SYN, ICMP, fragments, and others) and layer 5 (SIP signaling floods, malformed messages, and others)
   - Traffic management queues for control and throttling of signaling and media
2. Access control
   - Session-aware access control for signaling and media using static and dynamic permit/deny ACLs at layers 3 and 5
   - ACL and DOS protection for the management interface
3. Topology hiding and privacy
   - Complete infrastructure topology hiding at all protocol layers for confidentiality and attack prevention as well as modification, removal, or insertion of call signaling application headers and fields
   - Confidentiality and integrity through use of industry-standard encryption methods such as TLS, SRTP, and IPSec
4. VPN separation
   - Support for Virtual Private Networks (VPNs) with full inter-VPN topology hiding and separation
   - Ability to create separate signaling-only and media-only VPNs

- Optional intra-VPN media hair-pinning to monitor calls within a VPN

5. Service infrastructure DoS prevention
   - Per-device signaling and media overload control, with deep packet inspection and call rate control to prevent DoS attacks from reaching service infrastructure
6. Fraud prevention
   - Session-based authentication, authorization, and contract enforcement for signaling and media
7. Monitoring and reporting
   - Audit trails, event logs, access violation logs and traps, and management access command recording
   - Call Detail Records (CDRs) with media performance monitoring
   - Raw packet capture ability
   - Lawful Intercept capability (For Service Provider products, only. Enterprise products do not support Lawful Intercept.)

SBC Specific Security Principles

(Security teams should consider the following guidelines when deploying a Unified Communications (UC) system. These are some of the areas where the SBC family will provide value.

- Create a demarcation and enforcement point for the UC network: The enforcement point provides demarcation between zones of varying trust, such as the internal enterprise network, a BYOD network, a guest network, a demilitarized zone, or the public Internet.
- Hide topology: Hackers can plan attacks by ascertaining information about network equipment (determining equipment types and software versions) or by detecting the IP addressing scheme a company employs. A UC demarcation device should remove any protocol fields that may assist in “fingerprinting” and should provide NAT (network address translation) at all protocol levels to conceal internal addressing schemes.
- Encrypt endpoint communications: Businesses should encrypt communications flows when transiting public networks to prevent eavesdropping or impersonation. Encryption should also be considered on private networks to verify identity and prevent eavesdropping on privileged communications. Encryption can hinder lawful interception or other regulatory and corporate compliance requirements, so be sure to understand any impacts in your environment. By establishing a UC demarcation point and anchoring, unencrypting, and re-encrypting sessions at the network perimeter, security teams can tap or replicate sessions in the clear for compliance purposes.
- Normalize protocol differences on-demand: Because UC venders implement SIP differently, using devices from multiple venders may cause interoperability problems. In extreme cases, the “normal” messaging from one manufacturer might cause failures or outages for another. Rather than depending on vendors to fix these interoperability issues, it is preferable to do so, in real-time, using an SBC.
- Prevent DoS attacks and overloads: DoS or Distributed DoS (DDoS) attacks and other non-malicious events such as registration floods can impair IP

communications infrastructure (border elements, application servers, endpoints) and disturb critical applications and services. Attackers may try to flood a network from one or more endpoints or may send malformed messages (protocol fuzzing) to overwhelm network devices. A UC demarcation device can ensure continued service availability by identifying DoS and DDoS attacks, and appropriately throttling or blocking traffic.

2

Secure Installation and Configuration

This chapter outlines the planning process for a secure installation and describes several recommended deployment topologies for the system.

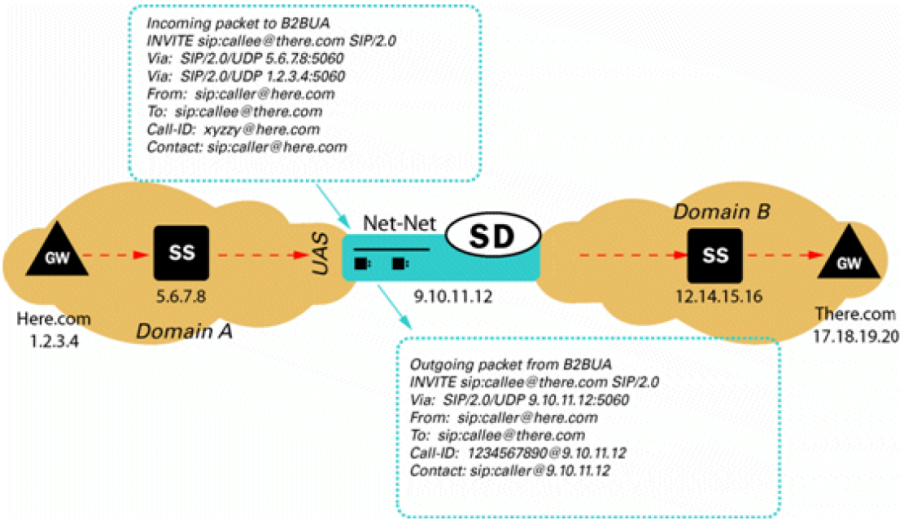
Recommended Deployment Topologies

This section outlines the planning process for a secure installation and describes several recommended deployment topologies for the system.

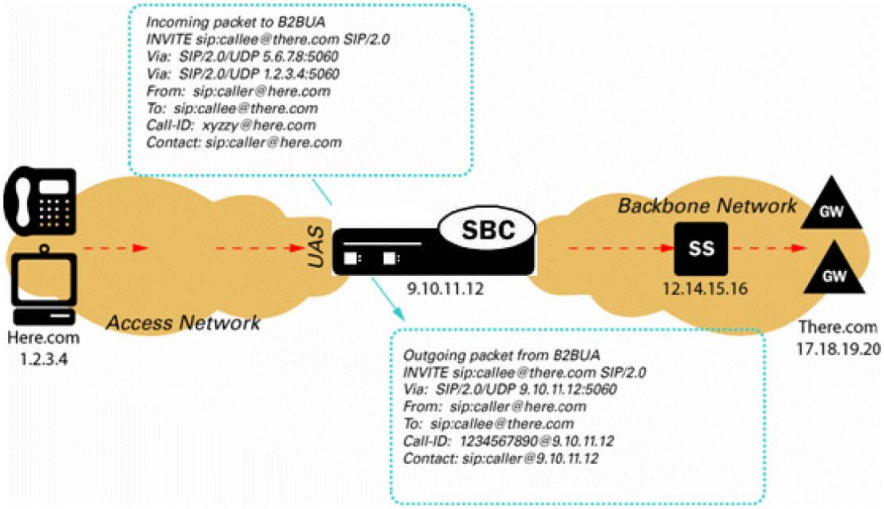
Session Border Controller

The SBC family products can be deployed following several generalized topology types; Peering (sometimes called Trunking), Access (also called Hosted IP Services), and Hybrid which combines the two models.

- Peering - In a peering model the SBC is contacted by a SIP server to relay endpoint signaling information. The SIP server may be a PBX, registrar, proxy, SBC, or other device. The IP of the device is usually trusted and pre-provisioned in the SBC as an endpoint (session agent) that will be relaying calls. Since the remote endpoint is already known, Access Control Lists (ACL) and Call Admission Controls (CAC) can be pre-provisioned for the appropriate level of protection or service level assurance.



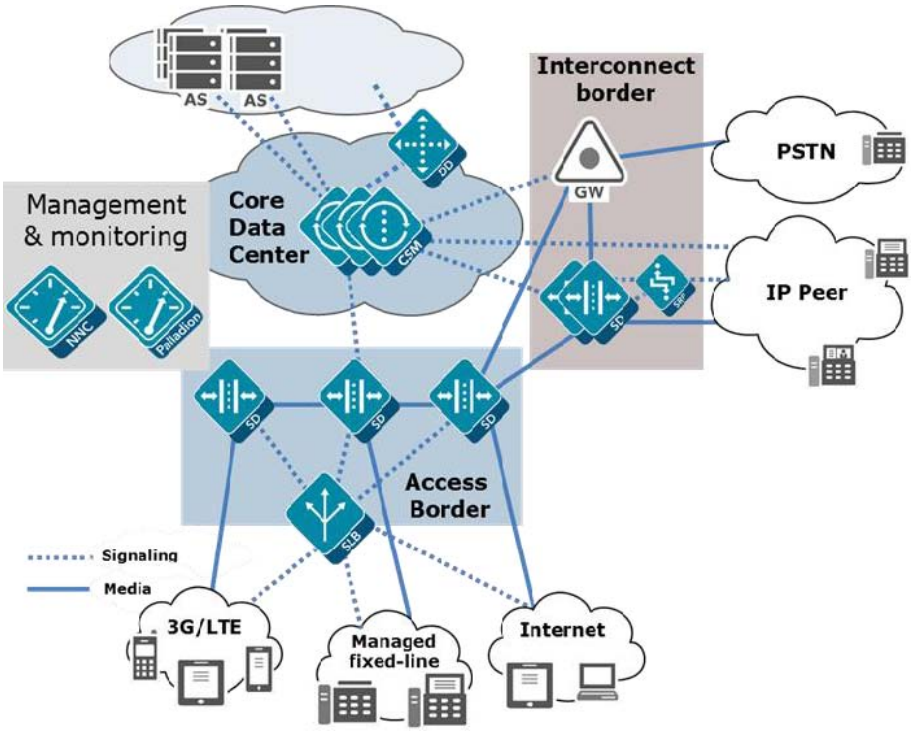
- Access - In an access model the SBC is contacted by a SIP endpoint to relay endpoint signaling information. The IP address of the endpoint is usually not known, so trust should be established through behavior such as establishment of a successful registration. Once the endpoint becomes trusted, dynamic Access Control Lists (ACL) and Call Admission Controls (CAC) can be applied. Monitoring of potentially abusive behaviors provides a mechanism to “demote” or place endpoints on a blocklist.



- Hybrid - A hybrid model combines both Peering and Access topologies into a single configuration. This is a fairly common model, where remote users use a registrar server in the core network, but their calls are forwarded to a service provider on one of the peer connections.

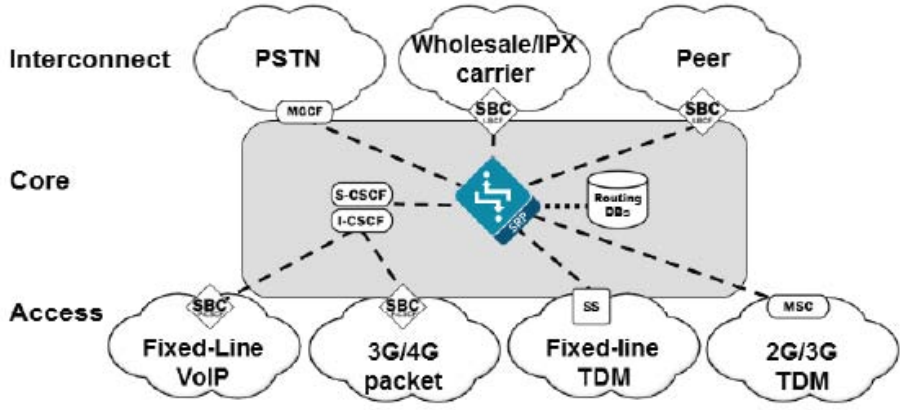
Core Session Manager

The Core Session Manager, which should never be positioned at a network edge, is used as a core session controller between multiple network types. It supports SIP in IMS and non-IMS environments, application servers, media servers, gateways, etc. It can be deployed in a distributed, virtualized model on COTS server hardware. The CSM can be used for session routing, interoperability assurance, CAC, and subscriber database integration through HSS, ENUM, or local subscriber table databases.



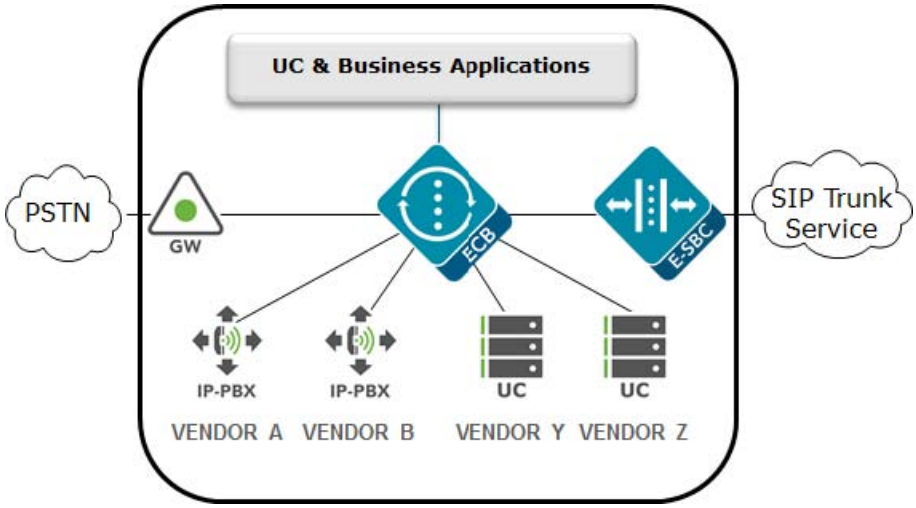
Session Router

The Session Router is a “pure” SIP session router that can be positioned in either a core network or at network borders. When installed at a border, the same SBC protections used in peering and access models can apply. In the network core, the emphasis is on routing and interoperability.



Enterprise Communications Broker

The Enterprise Communications Broker (ECB) should only be deployed within an enterprise core network, and not on the edge. Instead of perimeter security, the ECB is oriented towards functions such as dial plan management, centralized session, routing, CAC, load balancing, and interworking.



Realm Design Considerations

As a general rule, separate realms are created for external untrusted traffic and internal trusted traffic. However, there are many deployment complications that prevent that simple model from being used. Examples of these might include:

- A mix of user endpoints, gateways, or peer trunks on the untrusted network
- Varying capabilities or incompatibilities of user agents
- Impacts of blocking traffic to one group of users vs. another (i.e. trust low or medium)

- Service level agreements (SLA) that require Call Admission Controls (CAC)

A few of the general rules for Realm design include:

- Separate endpoints into realms based on trust level (high, medium, low) and that the response to detected abuse is appropriate for them (no action, demotion or blocking)
- Create multiple realms for endpoints based on the type of device – a user endpoint, a gateway, or a peer - since they will have very different considerations for SIP Header Manipulation, trust, signaling thresholds, endpoints behind NAT, and CAC.
- Consider increasing the deny-period from 30 seconds to something longer depending on how much abuse it is believed will be received from a public network and what type of delay users may tolerate.
- Set restricted-latching to sdp so only media received from the IP and port negotiated in signaling will be allowed.
- Pay close attention to the media management settings required for the endpoints and traffic flows (see the mm- parameters on the realm). If one way-audio is experienced this is one place to start investigating.

Management Interfaces

The Oracle SBC has two types of interfaces, one for management and the other for signaling and media (otherwise known as services interfaces). Security configuration for each interface is treated separately.

Two management interfaces allow access to the SBC for configuration, monitoring and troubleshooting purposes; a serial (console) interface and an Ethernet interface for remote management (wancom0).

Serial (Console) Interface

As with any industry standard serial interface to a network element, minimal security functions are available. The physical security of the installation location should be assured since console access cannot be blocklisted. However, the Admin Security license (discussed later) does allow for the console port to be disabled.

To avoid unauthorized access to the console interface the console-timeout should be configured to automatically disconnect the console session after an appropriate period of time (i.e. 300 seconds). Timeouts are disabled by default.

If the console port detects a cable disconnect it will also log out any logged in user to prevent unauthorized use.

The console interface should only be connected to a terminal server if the terminal server is deployed in a secure non-public network.

Configuration is detailed in Section 3 “System Configuration” of the ACLI Configuration Guide.

Management Port Configuration

The Wancom0 management interface MUST be connected to and configured on a management network or subnet separate from the service interfaces. If it is not, the SBC is subject to ARP overlap issues, and loss of system access when the network is

down or under DDoS attack. Oracle does not support SBC configurations with management and media and service interfaces on the same subnet.

Configuration is detailed in Section 2 “Getting Started” and Section 3 “System Configuration” of the ACLI Configuration Guide.

Accounts

The SBC provides two levels of factory default accounts through the Acme Packet Command Line Interface (ACLI): the user account and admin account. SBC no longer supports default passwords and requires these to be changed on first login. These accounts may be disabled with the factory-accounts command.

Another option is to use local accounts. You can create a local account and assign a user class for each person who needs to access the SBC. There are two user classes: "user" which has the same privileges as the user factory account, and "admin" which has the same privileges as the admin factory account.

When the Admin Security entitlement is enabled, the password policy and the login policy apply to local accounts. For more details, see the Access chapter in the *Admin Security Guide*.

Alternatively, the SBC supports the management of passwords via external RADIUS and TACACS+ servers for finer grain access control. The SBC supports communications with up to six RADIUS servers for this function. At least two entries should be configured to prevent service interruption.

The SBC encrypts sensitive configuration data in the configuration file using a Protected Configuration Password (PCP). This administratively configured password provides security and convenience when migrating configurations to different SBCs. All passwords should be changed; however, it is especially important to change the PCP (“config” user password) so passwords and keys stored in the config file are secure. TLS, IPsec, and HDR features are protected by the PCP:

CAUTION: Once the PCP password is changed the sensitive information (certificates, IPSec shared secrets, etc) in your configuration file will be re-encrypted using the new PCP the new encryption “salt.” As a result, previously backed up configuration files cannot be restored unless the password is restored to the value that configuration file was encrypted with.

Configuration is detailed in the Getting Started chapter of the *Configuration Guide*, and the System Management chapter of the *Maintenance and Troubleshooting Guide* in the subsection entitled “Setting a Protected Configuration Password: Matching Configurations.”

The SBC provides a backup account for HDR file synchronization that must be changed. The backup account password can be set using the command “secret backup”. The “secret” command is detailed in Section 3 of the ACLI Reference Guide.

The SBC provides one account for administration of legal intercept functions when a Lawful Intercept (“LI”) license is installed – li-admin. The first time lawful interception is configured you will be prompted to change the password. However if you have installed the license, but never configured lawful interception, the default password may be active and usable via SSH. Procedures to change the password are detailed in the LI Documentation Set.

Boot Flags

Boot parameters specify what information the system uses at boot time when it prepares to run applications. The boot parameters allow definition of an IP on the management interface, set the system prompt, and determine the software load that will be used. In addition, there is a boot flag setting that may modify the file location to be used, but may also enable additional

features. Administrator access to the command line interface is required to modify the bootflags.

There is seldom a reason to change the boot flag from its default value (0x08). Changes to the boot flags are usually only needed for hardware testing or recovery, debugging, etc.

A few boot flag values that are disabled by default have security implications. These should only be enabled at the direction of Oracle technical support.

- 0x01 – Turns off the hardened interface protection on the media interfaces, allowing all ingress traffic
- 0x10 – Enables a second sshd server that provides access to the linux system console. This server process is different from the ssh server used to access the ACLI for configuration.
- 0x80008 – enable source routing on the management port

The following bootflag can disable the R226 SFTP access restrictions:

- BOOTFLAG_MASK_SFTP_ACCESS 0x01000000

> **Note:**
>
> Once R226 is enabled this flag may only be modified in the bootloader, R226 prevents changes to bootflags from the acli.

For further information on boot flags refer to “Configuration Elements A-M” of the ACLI Reference Guide.

System ACLs

The Wancom0 Ethernet management interface should always be deployed in a secure non-public network.

The SBC provides static System Access Control List functionality (ACL) to protect the Wancom0 interface from other devices that can access the management LAN remotely. Only the management station(s) authorized for SBC access such as the Oracle Communications Session Element Manager should be permitted with ACLs. All system ACLs are considered "allow" ACLs, and include a specific IP source address / netmask and the IP protocol allowed. As the first ACL is created an implicit deny rule is inserted as the final ACL.

The maximum number of ACLs on Acme Packet platforms is 1024.

The "system-access-list" configuration is detailed in Section 3 "System Configuration" of the ACLI Configuration Guide.

SSH

A timeout can be configured to automatically disconnect the SSH session after an appropriate period of time (i.e. 59 minutes). Timeouts are disabled by default.

The SBC supports viewing, importing, and deleting public ssh keys used for authentication of SSHv2 sessions.

You can select the algorithms which the Oracle Communications Session Border Controller offers during SSH session negotiation.

In the **ssh-config** element, Oracle recommends:

- encr-algorithms = AEAD_AES_256_GCM,AEAD_AES_128_GCM,aes256-ctr,aes192-ctr,aes128-ctr
- hash-algorithm = hmac-sha2-256
- hostkey-algorithm = rsa-sha2-256
- keyex-algorithms = diffie-hellman-group14-sha256

Configuration is detailed in “Getting Started” of the ACLI Configuration Guide, and "System Management" of the Maintenance and Troubleshooting Guide.

SFTP

Only SFTP is supported for accessing the SBC.

FTP is allowed for push-receivers, although SFTP is recommended. The SBC uses push-recievers when it acts as an FTP/SFTP client.

GUI Management

The SBC can be managed by the Oracle Communications Session Element Manager via ACP through the management interface over TCP ports 3000 and 3001.

By default these ports are enabled in system-config > remote-control. If the SBCs are not remotely controlled by a Session Element Manager then this feature should be disabled.

For ACP to work, you must configure a TLS profile to protect ACP traffic. Enable ACP over TLS by configuring **acp-tls-profile** in system-config.

CAUTION: Disabling the remote-control feature is incompatible with the SBC HA architecture. Hence this functionality is considered optional and should only be deployed where HA and EMS are not used. If the SBCs are deployed in HA configuration, then the remote-control parameter needs to be enabled for the acquire-config feature to function properly.

Configuration is detailed in "System Configuration" of the ACLI Configuration Guide.

Web Management

Depending on the release, a web based management interface may be accessible via the management network connected to wancom0. The web interface is disabled and not supported for Service Provider SBCs, but Enterprise SBCs include a full featured management and provisioning system.

By default the web interface is disabled. It can be accessed via the wancom0 IP address when enabled. Note that even if the web interface is disabled that the SBC will respond on port 80 by default. However, all new connection requests are immediately torn down with a TCP RST since there is no web server process running, and no kernel rule to forward the request to the web server.

Oracle recommends that only HTTPS be enabled on this interface so TLS will be used instead of the default HTTP. Care should be taken when defining the cipher list in the tls-profile so that administrative traffic cannot be compromised. The default cipher list is "ALL", which includes some insecure ciphers for backwards compatibility. The cipher list should be set manually to remove insecure ciphers. Refer to the *Release Notes* to see which ciphers are supported and recommended.

Note that the DHE ciphers provide perfect forward secrecy, which prevents the session from being decrypted later even if the private key is discovered. Following is an example of **http-server**:

```
http-
server


    name                        web-interface
    state                       enabled
    realm
    ip-address
    http-state                  disabled
    http-port                   80
    https-state                 enabled
    https-port                  443
    http-interface-list         GUI
    tls-profile                 tls-webgui
    auth-profile
```

Configuration is detailed in Section 2 "Getting Started" of the ACLI Configuration Guide.

REST API

The REST API method of configuring and managing the SBC can only be used over HTTPS.

Resiliency

Several features enable availability, a key component of a secure deployment.

High Availability

It is strongly recommended that the SBC be deployed in a High Availability (HA) architecture with a Primary node and a Secondary node connected over both Wancom1 and Wancom2 interfaces for resiliency. It is also recommended that the two units in an HA pair be directly cabled together. While they can be separated and connected via an Ethernet switch or layer 2 VPN, this introduces latency and can significantly impact capacity. Since session replication is performed over a clear text connection, it may also expose call or configuration data sent in the replication process. In short, a geographically redundant pair of SBCs is not recommended. If geo-redundancy is an absolute requirement, a secure site-to-site VPN should be implemented for session replication, and thorough testing should be conducted to understand impacts to session capacity.

Configuration is detailed in the “High Availability Nodes” chapter of the ACLI Configuration Guide.

Link Detection and Gateway Polling

If the gateway-heartbeat is enabled, the SBC periodically sends ARP requests for each configured network-interface gateway. If the configured number of retransmissions has been exceeded, the SBC will mark that gateway as unreachable

and decrement its health score. If the health score decrements far enough, and the health score of the standby unit is higher, an HA failover will occur.

It is recommended that exactly one network-interface per physical interface have gateway-heartbeat enabled.

The following configuration fragment depicts the recommended default settings for the gateway heartbeat sub-element. It is also advisable to increment the health-score value by one with each new heartbeat configuration for ease of failure identification based on score.

```
gw-heartbeat
state         enabled
heartbeat          10
retry-count     3
retry-timeout      3
health-score      30
```

The feature is explained in detail in the “High Availability Nodes” chapter of the ACLI Configuration Guide.

3
Security Features

This section outlines specific SBC security mechanisms.

The Security Model

The Oracle Communications SBC is a purpose built device providing customers both centralized and distributed control of the management and security of UC networks. The SBC is a critical network security element for VoIP services designed to effectively manage sessions and protect core network elements from various types of DDoS attacks, including malicious and non-malicious signaling overload attacks. The SBC is the sole ingress and egress point for all signaling messages (SIP/H.323) and media streams to/from the core network and is therefore generally the demarcation point between trusted and untrusted network boundaries. Hence it is vital that the SBC be as secure and available as possible.

Oracle provides a number of industry leading techniques through SBC configuration to secure the network border. Some of these features are enabled “out of the box” and some require further analysis of the network architecture to determine the most optimal configuration for security.

For example, the SBC performs access control based on layer 5 signaling messages as one of its primary functions. The SBC is designed to allow authorized VoIP communications into the core network by opening/closing firewall ports and by performing NAPT (network address and port translations) on all signaling and media IP packets as one of its core functions. Signaling messages, going to and from the SIP core servers and residential gateways and/or peering affiliate infrastructure is therefore inspected and rewritten as necessary by the SBC.

The SBC follows a “closed” philosophy where ports and interfaces are closed by default and opened on an as-needed basis. Therefore the system will generally have ports, services and processes disabled unless configured.

R.226 Security Recommendations

For compliance with R.226, Oracle recommends:

- Users should change their login password after upgrading. Changing the login password forces the SBC to use the more secure SHA-2 hashing algorithm for storing password hashes.
- An Oracle Communications Session Border Controller ignores attempts to modify security related boot flags from the ACLI. The SBC still supports changing security related boot flags through the bootloader. See the R.226 Chapter in the Configuration Guide for details.
- The li-admin account should set the lawful intercept configuration password. Setting the li-config password encrypts the lawful intercept configuration.
- Users should only use IKEv2 for X2/X3 traffic.
- Users should configure the X1 interface (on a management interface) on a dedicated VLAN.

> **WARNING:**
>
> Selecting IKEv2 disables IKEv1.

Net-SAFE Architecture: SBC & Core Infrastructure Protection

The SBC provides several techniques for protecting the SBC, and therefore the service, from DDoS attacks.

First, traditional static ACLs should be configured to only permit signaling traffic from trusted devices. Permit ACLs are applicable for both unsecured networks (peering partner's SBCs, proxies, gateways) and secure network devices (core network softswitches, media servers, application servers, gateways). All other devices should be denied access to the SBC through the use of deny ACLs.

This solution does not scale for hosted NAT traversal (or hosted access) based applications where thousands of remote endpoint devices with dynamic IP addresses communicate directly to the SBC signaling interfaces.

The SBC provides the following tools for DDoS protection in Access networks:

- Protect the SBC core CPU via configurable sized queues and separation of signaling packets (trusted, untrusted)
- Configurable trust-level (none, low, medium, high)
- Wire speed hardware classification of every remote device trust-level
- Provide fair access for new/untrusted devices to signaling queue
- Multi-queue access fairness for unknown traffic
- Automatic behaviorally driven promotion/demotion/denial of devices
- Per-device constraints and authorization
- Protection against attack from behind NAT

Each device is classified as untrusted, trusted or denied. The entire system bandwidth is allocated for the trusted and untrusted queues according to the characteristics of the customer Access deployment (e.g. number of endpoints, rate of registration, packet size, etc.). The allocation of the CAM is configurable to tailor the sizes of the entries available for media, trusted and deny NAT entries according to the scale of the customer Access network. Separate configurable sized queues also exist for fragmented packets and ARP requests. In addition, a whole NAT device can be demoted based on the collective behavior of endpoints behind the NAT.

The trust-levels below determine promotion/demotion criteria between the deny list, untrusted and trusted queues.

- None: Device is always untrusted, no promotion or demotion
- Low: Device is initially untrusted, can be promoted to trusted, or demoted to denied
- Medium: Device is initially untrusted, can be promoted to trusted, cannot be denied

- High: Device is always trusted

A low or medium trust level is appropriate for Access or untrusted networks (realms). In contrast, a high trust level is appropriate only for Core or trusted networks (realms).

Promotion Criteria Examples

- SIP: 200OK received for either Register or Invite method

Demotion Criteria Examples

Exceeding any of the following thresholds:

- invalid-signal-threshold: maximum number of non-compliant signaling packets acceptable
- maximum-signal-threshold: maximum number of signaling packets acceptable while an endpoint is classified as trusted
- untrusted-signaling-threshold: maximum number of signaling packets while an endpoint is classified as untrusted

These thresholds are all measured in the configurable system wide tolerance-window (default 30s)

If an endpoint crosses one of these thresholds then a deny ACL is written to the CAM, and checked by the Network Processors (NP) upon receipt of a packet from the denied endpoint. The endpoint is denied for a configurable period of time.

The Whole NAT device demotion Criteria Examples

Exceeding any of the following thresholds:

- max-endpoints-per-nat: maximum number of end points behind a NAT at a realm level
- nat-invalid-message-threshold: Maximum number of invalid messages from all endpoints behind a NAT

Another related configuration is wait-time-for-invalid-register, the time period which the SBC will wait before counting the absence of the REGISTER message as an invalid message.

The goal of the DDoS protection tools detailed above is to assess and plan for a configuration that allows service to continue whether the SBC is under malicious attack or a non-malicious attack such as a recovery from a Softswitch outage or registration flood from endpoints. This involves allowing enough untrusted traffic such that endpoints can over time register successfully yet constraining all queues sufficiently to protect SBC resources (i.e. core CPU threshold).

Furthermore, the SIP Registration Overload Protection (SROP) feature is used to protect the SBC against mass endpoint avalanche restarts. The following sip-config options are recommended to be configured:

- cache-challenges and reg-overload-protect: The SBC will temporarily promote the endpoint to trusted level after the registrar challenges the REGISTER message with a 401/407 response.
- max-register-forward: Limit rate of REGISTERs to forward to the registrar. Set to 75% of max registers/sec the registrar can handle.
- max-register-refresh: Limit rate of REGISTER refreshes from endpoints. Set to 150% of number of endpoints divided by the refresh interval.
- register-grace-timer: Grace period in seconds before a cached registration is deleted from the SBC after expiration. Recommended to set this value to 32.

- reject-register=refresh: Lets the REGISTER in, but will check the load limit if there is not a cached registration that it can use for a response.

For the session-agent representing the core Registrar, the max-register-burst-rate should be configured to throttle REGISTER messages sent to it. In addition, session-constraints should be enabled with rate-constraints configured to limit the rate of REGISTER messages coming into the core network. Session-constraints are applied on the Access sip-interface or realm. In the sip-config parameter, extra-method-stats must be enabled for rate-constraints to take effect.

Please contact your Oracle Systems Engineer to discuss planning for DDoS protection configuration and deployment. Basic DDoS configuration is found in Appendix C: DDoS Prevention for Peering Environments and Appendix D: DDoS Prevention for Access or Hybrid Environments. Configuration is detailed in “SIP Signaling Services” and “Security” of the ACLI Configuration Guide.

Net-SAFE Architecture: Topology Hiding & SIP Manipulation

Topology hiding is primarily performed by the SBC’s Back-to-Back User Agent (B2BUA) function. Use of the SIP-NAT configuration object or the flexible SIP Manipulation feature provide capabilities to dynamically alter any identifying information pertaining to a customer core network in signaling messages.

SIP Manipulation rules allow the customer to check for a value in any element of any SIP message and take action if a rule matches. Actions include changing a value, deleting an element or parameter, completing a header, or adding a completely new header to the message. Requests can be rejected, and MIME types and bodies can also be manipulated. To provide further topology hiding in the SDP portion of a SIP message, the customer should enable SDP anonymization.

Configuration of SIP HMR (Header Manipulation Rules) is detailed in the HMR Resource Guide, a document in the SBC/ESBC documentation library. Configuration of SDP anonymization is detailed in “Security” chapter of the ACLI Configuration Guide.

Security Specific Feature Sets

This section details security-focused feature sets on the SBC.

IDS Reporting

The SBC supports a wide range of intrusion detection and protection capabilities for vulnerability and attack profiles identified to date. The IDS reporting feature provides more detailed reporting of intrusions the system detects. It is useful for enterprise customers’ requirement to report on intrusions and suspicious behavior that it currently monitors. This feature requires the IDS Reporting license, which is included in new purchases but was not in some older deployments. The “IDS Advanced” feature should be present in the output of the show features command.

See Appendix F: Intrusion Detection System for a detailed description of the functionality enabled. Configuration is also detailed in Section 15 “Security” of the ACLI Configuration Guide.

FIPS Feature (Optional)

FIPS is supported on the enterprise software release S-Cz9.0.0 on the Acme Packet 1100, Acme Packet 3900, Acme Packet 3950, Acme Packet 4600, Acme Packet 4900, Acme Packet 6350 and VM platforms. See the *Oracle Enterprise Session Border Controller FIPS Compliance Guide*.

Administrative Security Features (Optional)

See the *Oracle Enterprise Session Border Controller Administrative Security Guide*.

This feature set includes support for: multiple administrative accounts, enhanced password strength, password usage policies, account roles, management of administrative accounts, and serial console port control.

CAVEATS

- This feature set requires the Admin Security entitlement.
- This feature set is not intended for all customer use. The customer should consult their Oracle Systems Engineer to understand the security and restriction ramifications of enabling these features.
- Passwords can only be reset to factory defaults by running the diags image.
- Disabling the Admin Security entitlement does not remove its features. Once the entitlement is enabled, equipment must be returned to manufacturing to entirely remove all features.

With the Admin Security feature, access to the SBC is restricted. The SBC can be configured to lock out an interface for a specified time if the threshold of unsuccessful login attempts is exceeded. The factory account model is single-user, single-class. The 3 supported factory account names are user, admin and li-admin.

Login parameters are changed with the login-config element. Furthermore, when a local or RADIUS user logs into the system via console or SSH connection, a banner appears and must be acknowledged. The banner informs the user when they last logged in and whether there have been unsuccessful login attempts. Customers can also create a custom banner by uploading a banner.txt file in /code/banners. (Custom banners are available without the Admin Security entitlement) Banners can be disabled by the customer. No banner appears for SFTP connections.

Upon initial login, passwords must be changed from the factory defaults. Password strength and history are imposed only on local accounts. Password aging is applied from the date since the last password change. Password-policy can be configured to change password properties of both factory accounts and local accounts. With RADIUS or TACACS+ enabled, passwords are stored on the remote server, not on the SBC. Password policy therefore doesn’t apply when RADIUS or TACACS+ logins are enabled.

Optionally, SSH public keys can be imported into the SBC. Parameters surrounding SSH re-keying are set in the ssh-config. Key aging will be applied from the date of activating the config.

SFTP file access with RADIUS authentication requires a VSA called Acme-User-Privilege. These values are (non case-sensitive fields):

- sftpForAudit - allows audit log access.
- sftpForAccounting - allows system logs to be accessed.
- sftpForHDR - allows HDR to be accessed.

- sftpForAll - allows all logs to be accessed.

The Security Admin entitlement enables audit logs which provide data on all user driven system events such as changes to configuration and public keys. It is recommended to configure push servers to SFTP audit logs periodically to remote servers.

Configuring Monitoring and Performance Management Features

This section describes ways to monitor health and performance of your SBC.

SNMP

Simple Network Management Protocol (SNMP) is supported on the SBC Wancom0 management interface for polling and traps. To secure your SNMP interface, it is recommended to use a community name other than the standard “public”. Sufficiently obscure community names should adhere to the customer’s corporate naming policies. Further, the list of configured SNMP polling servers and trap receivers must be restricted to only those authorized (via SBC configuration) to manage the SBC. All management stations used for SNMP access should have a permit ACL configured.

The Oracle Communications Session Border Controller supports SNMPv3 by default. To secure your SNMPv3 system, you must configure SNMP users and groups, SNMP managers, and view access to MIB trees. SNMPv3 provides the SNMP agent and SNMP Network Management System (NMS) with protocol security enhancements used to protect your system against a variety of attacks, such as increased authentication, privacy, MIB object access control and trap filtering capabilities.

SNMP Recommendation

- Set **system**, **system-config**, **snmp-agent-mode** to v3
- Set **system**, **snmp-user-entry**, **auth-protocol** to SHA-256 or SHA-512
- Set **system**, **snmp-user-entry**, **priv-protocol** to AES-128

Further detail on SNMP traps and MIBS that should be examined can be found in the MIB Reference Guide.

RADIUS Accounting

The SBC Wancom0 management interface uses RADIUS requests to send accounting and monitoring data to remote RADIUS servers. For reliability, the SBC supports the configuration of multiple RADIUS servers deployed in a number of HA schemes: hunt, failover, round robin, fastest round trip time (RTT) and fewest pending.

The most appropriate scheme according to customer’s corporate policies should be chosen. It is recommended that at least two RADIUS servers be deployed. The secret shared between the SBC and the RADIUS server should be configured to be suitably obscure according to the customer’s corporate naming policies. All management stations used for accounting monitoring services should have a permit ACL configured.

Configuration is detailed in the ACLI Accounting Guide.

HDR over SFTP

The Historical Data Recording (HDR) feature allows the SBC to record data in comma-separated files and periodically sends them to a remote file server. For added security, transfer the HDR record files using SFTP. Note that public key authentication is not available for this feature so the SBC uses password authentication. All management stations used for SFTP access should have a permit ACL configured.

Configuration is detailed in “System Configuration” of the ACLI Configuration Guide.

Syslog

The syslog service should be used for sending system events from the SBC to a Security Event & Incident Monitoring (SEIM) platform or to another operations monitoring platform. The information sent via syslog is also contained locally on the SBC in the acmelog file.

See Appendix I: for examples of important syslog messages to monitor. The default syslog log level is WARNING.

Configuration is detailed in “Syslog and Process Logs” of the ACLI Configuration Guide.

Configuring AAA Integration

The SBC supports RADIUS and TACACS+.

SSH RADIUS Authentication

The SBC management interface sends RADIUS requests containing login authentication and authorization data to remote RADIUS servers.

The SBC supports the use of the Cisco Systems Inc.™ “Cisco-AVPair” vendor specific attribute (VSA). The Vendor-ID is 1 and the Vendor-Type is 9. This attribute allows for successful administrator login to servers that do not support the Oracle authorization VSA. While using RADIUS-based authentication, the SBC authorizes you to enter administrator mode locally even when your RADIUS server does not return the ACME_USER_CLASS VSA or the Cisco-AVPair VSA.

All management stations used for SSH access should have a permit ACL configured. An ACL should also be configured to allow RADIUS traffic to the RADIUS server.

For more information, see Section 4 “System Management” of the Maintenance and Troubleshooting Guide.

TACACS+

TACACS+ is a protocol that was originally developed by Cisco Systems. It provides functions for authentication, authorization, and encryption of the administrative traffic. Unlike RADIUS, it separates authentication and authorization functions. The SBC acts as a TACACS+ client.

The SBC uses TACACS+ services to provide administrative authorization. With TACACS+ authorization enabled, each individual ACLI command issued by an admin-class account is authorized by the TACACS+ authorization service. The SBC replicates each ACLI command in its entirety, sends the command string to the authorization service, and suspends command execution until it receives an authorization response. If TACACS+ grants authorization, the pending command is executed; if authorization is not granted, the SBC does not execute the ACLI command, and displays an appropriate error message.

All management stations used for SSH access should have a permit ACL configured. An ACL should also be configured to allow TACACS+ traffic to the Network Access Server. TACACS+ is disabled by default.

For increased security, configure TACACS+ over IPsec for the management traffic on the wancom0 interface. Refer to the TACACS+ section under "User Accounts" in the Getting Started chapter of the *Configuration Guide*. For information on how TACACS+ interacts with the Admin Security entitlement, see the Access chapter of the *Admin Security Guide*.

Signaling and Media Interface Security Configuration

Securing the service interfaces is an important consideration because they are typically deployed in public unsecured networks and are usually the demarcation or access point to the core network infrastructure.

Signaling and Media Management Functions

The phy-card is intended for signaling and media traffic, only. The SBC disables ICMP, Telnet, SNMP, and FTP on signaling and media interfaces by default. Oracle recommends that you do not enable any of these protocols on a service interface for any length of time longer than required for troubleshooting purposes.

See “System Configuration” in the *ACLI Configuration Guide*.

SIP Interface Security

As well as the layer 3 ACLs, the SBC provides layer 5 SIP protection to its signaling interfaces. By default, the SBC sip-interface, sip-port parameter allows and routes signaling from any device.

For Access-untrusted networks, Oracle recommends configuring the sip-interface, sip-port, allow-anonymous setting to one of the following values:

- registered: This is the most widely deployed setting, allowing only non-REGISTER SIP requests from either a defined session-agent or a previously registered device. (All REGISTER requests are processed.)
- realm-prefix: Allows SIP requests only from defined session-agents or previously registered endpoints. Allows only REGISTER requests from endpoints within the configured realm-prefix (subnet).

Although SIP interface security will deny service to a malicious user, the SIP daemon and the core CPU is utilized to parse and process each request. Oracle recommends deploying this feature in conjunction with the Net-SAFE architecture.

For SIP-interfaces communicating with non-registering devices (peering partner SBCs or core devices such as softswitches), Oracle recommends that you set **allow-anonymous** for agents-only.

Oracle recommends that you configure an Enforcement Profile with the list of allowable SIP methods, and that you configure only the minimum set of SIP methods necessary for your deployment. You can configure more protection in Access scenarios where SIP endpoints send SUBSCRIBE dialogs. You can limit the rate of these messages per user.

Oracle recommends that you apply session constraints to the sip-interface to limit the max-sessions, max-burst-rate, max-sustain-rate, and rate constraints for individual

method types. For more information, see Section 5.3 “Constraint Limiting” of “520-0013-05 TECH NOTE Theory of the Session-agent.”

The SBC default SIP routing behavior is to comply with Route headers, as received. This behavior leaves a security gap, where a trusted device can construct a Route header and use the SBC as a reflector for signaling to another known device. The SBC also uses the Request-URI to route traffic, even when there is no matching local policy. This is mitigated by using techniques such as stripping Route headers on ingress (proceed with caution) and configuring null routes with 0.0.0.0, as the next hop.

See “SIP Signaling Services” and “Session Routing and Load Balancing” in the *ACLI Configuration Guide*.

Service ACLs

ACLs on service ports provide more functions than the basic permit and deny operations provided by the ACLs on management ports. Service ACLs effect traffic management through average rate limitations, trust level, and signaling thresholds similar to those specified on a realm.

To prevent misunderstanding these traffic management settings, note the following general rules:

- Define an ACL for all peering partners and all core systems to which traffic will be routed. The ACL is used to permit trusted hosts, deny untrusted hosts, and guarantee bandwidth in peak periods.
- Note that the minimum-reserved-bandwidth setting does not permanently reserve bandwidth. The setting is used only in peak periods to prioritize traffic. Set the minimum-reserved-bandwidth to the maximum signaling bandwidth capable for the system. If more than one core device is used, divide the bandwidth number equally. The number is not really bandwidth, but a priority metric.
- Hosts with a trust levels of high will never be demoted or blocklisted. However, if an invalid-signal-threshold of one is configured on the ACL, a syslog event will be written which might help detect attempted abuse.
- The trust level specified on the ACL should match the trust level on the realm from which it will communicate. Trust level mismatches can have unintended consequences such as permitting traffic that is intended to be denied. Refer to the following scenario that illustrates how this can be problematic.

This scenario shows a trusted core PBX on a private network, and two PBXs on an external public network. The trust level on the ACL applied to the external interface and the trust level on the external realm are depicted in the following tables, along with what happens to traffic sent from a source IP of “.100” or “.111.” In the first table: IP .111 permitted in ACL, the effects of having the 192.168.1.111 address permitted are depicted. The second table shows the opposite, when the 192.168.1.111 address is denied. Note what access the 192.168.1.100

address has is based on the trust level of the realm and ACL.

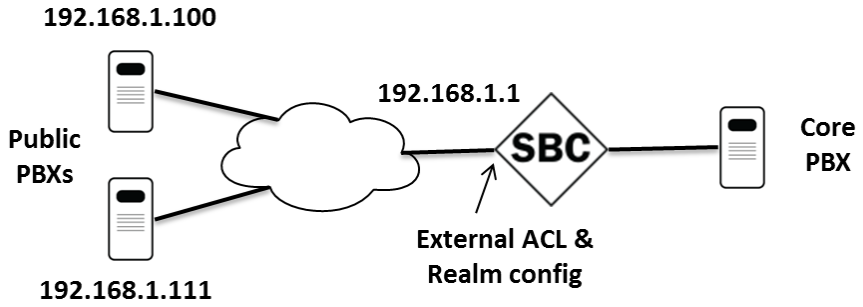


Table 3-1 .111 permitted in ACL

Realm Trust Level	ACL Trust Level	src:100	src:111
None	none	Permit	Permit
None	low	Deny	Permit
None	medium	Deny	Permit
None	high	Deny	Permit
Low	none	Permit	Permit
Low	low	Deny	Permit
Low	medium	Permit	Permit
Low	high	Permit	Permit
Medium	none	Permit	Permit
Medium	low	Permit	Permit
Medium	medium	Deny	Permit
Medium	high	Permit	Permit
High	none	Permit	Permit
High	low	Permit	Permit
High	medium	Permit	Permit
High	high	Deny	Permit

Table 3-2 .111 denied in ACL

Realm Trust Level	ACL Trust Level	src:100	src:111
None	none	Deny	Deny
None	low	Deny	Deny
None	medium	Deny	Deny
None	high	Deny	Deny
Low	none	Permit	Deny
Low	low	Permit	Deny
Low	medium	Permit	Deny
Low	high	Permit	Deny
Medium	none	Permit	Deny
Medium	low	Permit	Deny
Medium	medium	Permit	Deny
Medium	high	Permit	Deny
High	none	Permit	Deny

Table 3-2 (Cont.) .111 denied in ACL

Realm Trust Level	ACL Trust Level	src:100	src:111
High	low	Permit	Deny
High	medium	Permit	Deny
High	high	Permit	Deny

TLS for SIP

Transport Layer Security (TLS) provides end-to-end authentication and encryption of SIP signaling. TLS protects against eavesdropping, tampering, forgery, and potential theft of service. For this reason, Oracle recommends using TLS wherever possible.

All supported products have TLSv1.2 and TLSv1.3.

The SBC supports mutual-authentication within a TLS profile. Although disabled by default, Oracle recommends enabling mutual-authentication when endpoints support it.

The SBC supports the following TLS Exchange and Authentication models:

- Basic—The client authenticates the SBC certificate by using the CA public key, and checks expiration, common name, and ciphers supported. Basic provides confidentiality and integrity through encryption, but does not establish the identity of the endpoint. Credential cracking is still possible, and the move to TLS (based on TCP) may make port exhaustion DoS a bit easier for an attacker.
- Mutual—A step is added in which the client certificate is sent to the SBC for verification. You can use single or individual client certificates. Mutual provides the same characteristics of the basic model with the advantage of verifying that the client is likely trusted because an issued certificate is present. If a single certificate is used for all clients then theft or compromise of an endpoint may allow access to an attacker. Individual certificates are more secure, but require more administrative effort to issue and manage.
- Mutual with certificate revocation—Certificate revocation for individual clients is possible, which guarantees only expired or revoked clients are refused access. An external Online Certificate Status Protocol (OCSP) server is required to check against the Certificate Revocation List.

> **Note:**
>
> The SBC does not support local CRLs due to onboard storage limitations.

Other key information regarding TLS includes:

- Oracle recommends enabling notifications for TLS certificates that are about to expire. For details, see the "Notifications for Certificate Expiration" section in the *ACLI Configuration Guide*.
- Certificates installed on the SBC must be derived from a local Certificate Signing Request in PKCS-10 PEM/Base 64 format. Certificates cannot be installed without a CSR.
- Certificate key lengths can go up to 4096 bits, with 2048 bits as the default.
- Certificates are currently signed with a SHA-2 hash by default. Oracle recommends signing with SHA-2 or above.

- If site-to-site failover is required, the main site's fully qualified domain name (FQDN) and the FQDN for any alternate site should be specified as alternate-names in the certificate record prior to CSR generation.
- TLS session caching (tls-global element) allows a previously authenticated user to reuse a previous session so authentication is sped up. This may help reduce time to recovery due to outages, though it is best suited for environments where user IP does not vary significantly.

The list of available TLS ciphers is located in the *Release Notes*. The default cipher list when creating a tls-profile is "DEFAULT." The default list includes all current, secure ciphers. The "ALL" cipher list includes all available, non-debug ciphers, some of which may be potentially unsecure. The "NONE" cipher list does not provide encryption; only authentication.

Because TLS is based on TCP, TCP DoS protections should be configured to limit the number of connections per source IP and per sip-interface. Consider the following settings in your environment:

- sip-config, inactive-dynamic-conn—Defines global timer for tearing down idle TCP and TLS connections where no SIP data has been sent. The timer used is twice as long for TLS.
- sip-interface settings to limit connections:
  - untrusted-conn-timeout—Closes socket if untrusted entity does not become trusted, such as if the register didn't complete.
  - inactive-conn-timeout—Tears down idle TCP/TLS connections when no further data is being sent, such as if a trusted host sends an INVITE but nothing else.
  - max-incoming-conns—Set to max incoming sessions you want the SIP interface to host plus overhead for setup / teardown (depends on call rate).
  - per-src-ip-max-incoming-conns—Usually 1 or 2 but affected by NAT use and application.

See "Security" in the *ACLI Configuration Guide*.

OCSP

The Online Certificate Status Protocol (OCSP) is defined in RFC 2560, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. The protocol enables you to determine the revocation state of a specific certificate, and may provide a more efficient source of revocation information than is possible with Certificate Revocation Lists (CRL).

The protocol specifies the data exchanged between an OCSP client (such as the Oracle Communications SBC) and an OCSP responder, the Certification Authority (CA), or its delegate, that issued the target certificate. An OCSP client issues a request to an OCSP responder and suspends acceptance of the certificate in question until the responder replies with a certificate status. Certificate status is reported as

- good
- revoked
- unkown

OCSP can be especially useful in environments where individual certificates have been issued to a single user or user device. Certificates for devices that are stolen or

misplaced can be revoked, so even if valid credentials are known the device will not be able to connect.

See “Security” in the *ACLI Configuration Guide*.

SRTP

Many customers require the ability to encrypt and authenticate the content and signaling of their real time communications sessions. The SBC supports the Secure Real-Time Transport Protocol (SRTP). Authentication provides assurance that packets are from the purported source, and that the packets have not been tampered with during transmission. Encryption provides assurance that the call content and associated signaling has remained private during transmission.

With two exceptions, SRTP requires an IPsec NIU. The 1100, 3900, 3950, and 4900 platforms support software-based SRTP.

RTP and RTCP traffic are encrypted as described in RFC 3711, The Secure Real-time Transport Protocol (SRTP). The negotiation and establishment of keys and other cryptographic materials that support SRTP is described in RFC 4568, Session Description Protocol (SDP) Security Description for Media Streams. Cryptographic parameters are established with only a single message or in single round-trip exchange using the offer–answer model defined in RFC 3264. An Offer–Answer Model with the Session Description Protocol (SDP).

See the Security chapter in the *Configuration Guide*.

Securing Media Interfaces with IPsec

IPsec provides another mechanism for encrypting and securing media interface traffic, including SIP, RADIUS, etc, on supported platforms.

Security Associations and Security Policies allow for flexibility in defining local and remote IP address, ports and subnet masks. These should be defined to only allow IPsec communications between authorized gateways or hosts and the SBC. Refer to the Security chapter of the *Configuration Guide* for more information on security policy.

The SBC supports IKEv2 to create IPsec tunnels dynamically. This is based on the Internet Key Exchange (IKE) Protocol as defined in RFC5996 and RFC 2409, Internet Key Exchange, and for the Dead Peer Detection (DPD) protocol as defined in RFC 3706, A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers. Refer to the "IKEv2 Protocol" section in the Security chapter of the *Configuration Guide* to setup and configure IKEv2 tunnels.

The following IKEv1 functionality is supported:

- IKE pre-shared secret support
- IKE/ISAKMP Main Mode support
- IKE/ISAKMP Aggressive Mode support
- Phase 2 Quick Mode support

The following IKEv2 functionality is supported:

- IKE pre-shared secret support
- X.509 certificate-based authentication

In addition, with IKE enabled, the SBC can support IPsec between itself and an endpoint behind a NAT device.

Oracle recommends you use IKEv2.. See “Security” in the *ACLI Configuration Guide*.

Call Admission Control

Call Admission Controls (CAC) limit the number of allowed resources such as bandwidth or sessions to abide by customer Service Level Agreements (SLA) and to avoid abuse. Oracle recommends that you enable the following features wherever possible:

- Bandwidth (codec) based—for bandwidth CAC settings see “Media Profiles”
- SIP Per-User CAC
- Session Capacity
- Session Rate (sustained and burst)

Bandwidth CAC

You can implement bandwidth based CAC through a media profile on the realm level. Media profiles specify or limit the range of the codecs, bandwidth, and packet rate used. See “Realms and Nested Realms” in the *ACLI Configuration Guide*.

SIP Per-User CAC

When you enable SIP per-user CAC, the SBC changes its default behavior to allow only the configured number of calls or total bandwidth to and from each individual user in a particular realm. You can apply CAC to an individual Address of Record (AoR) or IP address. Tracking based on IP address can cause complications when a NAT is involved, so the use of a nat-trust-threshold may be required to set the maximum number of untrusted endpoints behind NAT devices. This also enables the ability of the SBC to track endpoints based on both IP and the TCP or UDP port in use.

See “SIP Signaling Services” in the *ACLI Configuration Guide*.

Session Capacity and Session Rate using Constraints

Constraints is a CAC method that limits messaging based on session count and rate. You can apply constraints to SIP interfaces or realms. Oracle recommends using constraints on all external interfaces and core session-agents.

A session-agent can be configured for max-outbound-sessions, max-sessions, max-burst-rate and max-sustain-rate.

Max-outbound-sessions and max-sessions give the max number of allowed concurrent sessions. Set these to match what should be sent to an upstream session-agent (for example a service provider) or accepted into a core session-agent.

The session-agent's max-burst-rate and max-sustain-rate are used to throttle the calls per second (CPS) of traffic sent to and by that session-agent. Each of these parameters has its own configurable window by which the statistics are gauged for constraint exceptions.

For the sustained-rate, the average is calculated over the previous window (equal to the sustained-rate-window) and current window fragment. The window fragment will be between 0 and the configured sustained-rate-window upon receipt of an Invite. Once the window fragment increments and reaches the sustained-rate-window, this rotates and becomes the previous window -- and a new window fragment begins at 0. At this point all calculations are re-calibrated accordingly.

For example, consider the scenario where the sustain-rate is set to 15 and the sustain-rate-window is set to 10 seconds. When an invite is received the SD will add the amount of Invites received in the current window fragment and the previous window and divide by the number of seconds to get the average for that period. This average is then compared to the 15 CPS derived from the sustain-rate and the sustain-rate window. If the session-agent per the previous and current window is above 15 CPS when the Invite is received, the Invite will be rejected.

The max-burst-rate and burst-rate-window interact by limiting the CPS rate for a burst of traffic over the window. Using the example below, with a max-burst-rate of 20 and a burst-rate-window of 10, the SD will permit 200 sessions within the first 10 seconds and then reject all new sessions until it exits constraint mode.

Burst rate is much easier to understand and configure, so it is preferable over sustain rate.

As for a session-agent in constraint, it does not come out of constraint mode when traffic drops below its constraint thresholds; it comes out of constraint mode after 60 seconds, unless a configured time-to-resume value dictates otherwise. Even though the session-agent is out of the constraint mode after time-to-resume seconds “show sipd agent” will show it back into In-Service mode only if the traffic flows to or from that session-agent. On exceeding its constraint the session-agent is marked “C”.

Core registrars should have a max registration burst rate configured to the maximum rate (or just below) what the registrar can handle.

See “SIP Signaling Services” and “Admission Control and Quality of Service Reporting” in the *ACLI Configuration Guide*.

Media Policing

Media policing controls the throughput of individual session media flows (RTP and RTCP) in the SBC. It also allows the SBC to police static flows. Oracle recommends enabling media policing to protect against RTP media flooding and bandwidth piracy.

For each individual codec being used in sessions, a media-profile must be created with average-rate-limit thresholds configured.

See “Security” in the *ACLI Configuration Guide*.

DoS/DDoS Prevention

DoS and DDoS settings can protect against malicious and non-malicious SIP flooding attacks from untrusted sources without adversely affecting service to trusted peers.

You can prevent attacks through configuration of Access Control Lists, appropriately sized traffic queues, and trust level settings that limit or blocklist endpoints that become abusive.

Configuration of these parameters will differ based upon the configuration model used – peering, access, or hybrid. Refer to either Appendix C: DDoS Prevention for Peering Environments or Appendix D: DDoS Prevention for Access or Hybrid Environments, depending on the architectural model implemented.

> **Note:**
>
> Note that a comprehensive and effective DDoS prevention design requires analysis of traffic patterns, SIP message contents and performance characteristics of all peer devices to provide message thresholds, CAC, and traffic policing settings. Please contact your Oracle Sales representative for information on professional services designed to implement customized DDoS settings.

Attack Tool Prevention

Many SIP scanning and attack tools employed by fraudsters can be prevented through employment of restrictive signaling thresholds and trust levels – the same ones used for DDoS protection. However, some deployments do not allow for this without impacting legitimate traffic. Attackers may also use commonly available tools that have identifiable signaling patterns. In these situations, additional attack tool identification and prevention may limit or prevent an attack from being successful.

Oracle recommends that any deployment with internet-connected interfaces comply with the settings described in Appendix E: Mitigating SIP Attacks.

Lawful Interception

The SBC supports a Lawful Intercept (LI) capability as mandated by national laws in various countries. Multiple interface types are supported. The feature purchasing and documentation are controlled, and you must enable the LI capability with the installation of a license key. You must configure LI to communicate with a server that provides the authorization tickets to enable recording. After installing the LI license, a separate administrative user dedicated for LI configuration “li-admin” becomes active.

> **Note:**
>
> LI applies to Service Provider products, only. Enterprise products do not support Lawful Interception.

IKE Configuration

IKEv2 can be configured either for media ports or for the wancom0 management port.

IKE Configuration for Media Ports

There are two parts to configuring IKE security parameters. First you must configure the **ike-config** element (located under **security**, and then **ike**). The **ike-config** element defines IKE parameters globally for all **ike-interface** configuration elements. Next you must configure the **ike-interface** element (located under **security**, and then **ike**). The following recommendation is the same for both configuration methods:

- Use IKEv2 by setting ike-version to 2. IKEv2 is more secure than IKEv1.
- Enable IKEv2 rekey by setting v2-rekey to enabled.
- Ensure that the IKE SA rekey interval for IKEv2 rekey is set: v2-ike-life-secs. The recommended value is 24 hours (86400 secs).

- Ensure that the time interval for IKEv2 IPSec SAs is set: v2-ipsec-life-secs: The recommended value is one hour (3600 secs).
- Use certificates for SBC authentication by setting sd-authentication-method to certificate. This is more secure than shared-password.

The following recommendation is only for the **ike-config** configuration element.:

- negotiation-timeout: Recommended value is 15 seconds or smaller
- event-timeout Recommended value is 60 seconds
- anti-replay: Recommended value is to enable anti-reply
- overload-threshold Recommended value is 85%
- overload-interval Recommended value is 30 seconds
- overload-action: Recommended value is to drop new connection
- overload-critical-threshold: Recommended value is 95%
- overload-critical-interval: Recommended value is 30 seconds

The **ike-sainfo** configuration element is used for IPSec security associations negotiated by IKEv2. The following recommendations apply:

- security-protocol: Recommended value is esp-auth
- auth-algo: Recommended value is either sha2-256 or sha2-384
- encryption-algo: Recommended value is aes-ctr

Refer to the "IKEv1 Configuration" section in the Security chapter of the *Configuration Guide* for more information.

IKE Configuration for Wancom0 Management Port

If you want to enable IKEv2/IPsec on the wancom0 management interface, configure the **ikev2-ipsec-wancom0-params** element (under **security**). See the *Configuration Guide* for details.

A

Secure Deployment Checklist

The following security checklist includes guidelines that help secure your system

The following security checklist includes guidelines that help secure your system

1. Do NOT connect your system to any untrusted networks, especially the Internet, until all protections have been configured. Customers have reported systems under configuration compromised in minutes due to incomplete configurations.
2. Harden the management environment.
    a. Install HA connections between units over a direct cable vs. a network.
    b. Make sure all equipment is in locked cabinets or at least in a secure room.
    c. Configure console timeouts.
    d. Ensure that the wancom0 management port is connected to a private management LAN with an IP address that is not Internet routable.
    e. Set strong passwords for all default accounts prior to configuration.
    f. Disable telnet and FTP if they are enabled.
    g. Configure system ACLs to limit management traffic to users that really need access.
    h. If implementing SNMP, change the default community string and follow the SNMP configuration recommendations in Appendix H:
    i. Use strong ciphers for HTTPS web management connection.
3. Practice the principle of least privilege.
    a. Carefully consider who has access to the admin password.
    b. Implement RADIUS or TACACS+ authentication if available.
4. Restrict network access.
    a. Use services ACLs where possible.
    b. Refrain from configuring host-in-path addresses.
    c. Ensure that users coming from an untrusted network have to register prior to providing service.
    d. Implement DoS and CAC protections.
    e. Mitigate known fraud schemes by implementing sipShield or HMRs.
    f. Use strong ciphers for any TLS connections.
    g. Enable OCSP and mutual authentication if possible for TLS connections.
5. Monitor the system for unusual events.
    a. Configure the SNMP trap receiver and syslog receiver.
    b. Send either CDRs or RADIUS accounting records to a fraud management system or implement a solution that can actively monitor SIP signaling.

B
Port Matrix

Standard Port Matrix for SBC security hardening.

Refer to this port matrix as part of deploying a secure Oracle SBC.

Ethernet	Ports	Protocol	Service	Optional	Configurable Port	Default Port State	Server or Client	Description
Wancom0	21	TCP	FTP	Yes	Yes	Closed	Client	FTP push receiver
Wancom0	22	TCP	SSH / SFTP	Yes	No	Open	Server	SSH for ACLI admin
Wancom0	49	TCP	TACACS+	Yes	Yes	Closed	Client	TACACS+ AAA
Wancom0	80	TCP	HTTP	Yes	Yes	Closed	Server	HTTP SIP monitoring and tracing or provisioning GUI
Wancom0	123	UDP	NTP	Yes	No	Closed	Client	NTP time update requests
Wancom0	161	UDP	SNMP	Yes	No	Closed	Client	SNMP traps
Wancom0	162	UDP	SNMP	Yes	No	Closed	Server	SNMP MIB retrieval
Wancom0	443	TCP	TLS/ HTTPS	Yes	Yes	Closed	Server	HTTP SIP monitoring and tracing or provisioning GUI
Wancom0	514	UDP	Syslog	Yes	Yes	Closed	Client	Syslog message feed
Wancom0	1812	UDP	Radius	Yes	Yes	Closed	Client	RADIUS AAA
Wancom0	1813	UDP	Radius	Yes	Yes	Closed	Client	RADIUS Accounting
Wancom0	2200	TCP	SSH/ SFTP	Yes	No	Closed	Server	Enable root shell access when boot flag is 0x10

Ethernet	Ports	Protocol	Service	Optional	Configurable Port	Default Port State	Server or Client	Description
Wancom0	3000	TCP	ACP	Yes	No	Open	Server	Acme Control Protocol for GUI
Wancom0	3001	TCP	ACP	Yes	No	Open	Server	Acme Control Protocol for GUI
Wancom0	ANY	UDP	Process Log	Yes	Yes (any)	Closed	Client	Internal process log feed
Wancom0	n/a	1	ICMP Echo Reply	Yes	No	Open	Server	Echo Request (Ping) used by SIP trunk between ASM and its application server (CM)
Wancom1 & 2	22	TCP	SSH / SFTP	Yes	No	Closed	Server	
Wancom1 & 2	1987	UDP	HA CFG	Yes	Yes	Closed	Both	Primary is server, client is secondary
Wancom1 & 2	9090	UDP	HA BERPD	Yes	Yes	Closed	Both	Primary is server, client is secondary
Services Ports	n/a	50	ESP	Yes	No	Closed	Server	
Services Ports	n/a	51	AH	Yes	No	Closed	Server	
Services Ports	n/a	1	ICMP Echo Reply	Yes		Closed	Server	
Services Ports	21	TCP	FTP	Yes	No	Closed	Server	
Services Ports	22	TCP	SSH / SFTP	Yes	No	Open	Server	
Services Ports	23	TCP	Telnet	Yes	No	Closed	Server	
Services Ports	53	UDP	DNS	Yes	No	Closed	Client	
Services Ports	80	TCP	OCSP	Yes	Yes	Closed	Client	

Ethernet	Ports	Protocol	Service	Optional	Configurable Port	Default Port State	Server or Client	Description
Services Ports	80	TCP	COPS, A-COPS, DIAMETER	Yes	Yes	Closed	Client	Policy server
Services Ports	161	UDP	SNMP	Yes	No	Closed	Client	SNMP traps
Services Ports	162	UDP	SNMP	Yes	No	Closed	Server	SNMP MIB retrieval
Services Ports	500	UDP	ISAKMP	Yes	Yes	Closed	Server	
Services Ports	1986	TCP	MCGP HA	Yes	Yes	Closed	Server	
Services Ports	1988	TCP	MCGP SIP Checkpoint	Yes	Yes	Closed	Server	
Services Ports	1719	TCP	H.323 RAS	Yes	Yes	Closed	Server	
Services Ports	1720	TCP	H.323 Q931	Yes	Yes	Closed	Server	Set, dynamic from 0 up
Services Ports	1994	TCP	IPsec	Yes	Yes	Closed	Server	Ipsec sync messages
Services Ports	2200	TCP	SSH/ SFTP	Yes	No	Closed	Server	Enable root shell access when boot flag is 0x10
Services Ports	2427	TCP/UDP	MGCP	Yes	Yes	Closed	Client	MGCP signaling
Services Ports	2727	TCP/UDP	MGCP	Yes	Yes	Closed	Server	MGCP signaling
Services Ports	3478	TCP/UDP	STUN	Yes	Yes	Closed	Both	
Services Ports	3479	TCP/UDP	STUN	Yes	Yes	Closed	Both	
Services Ports	3868	TCP/ SCTP	Diameter	Yes	Yes	Closed	Both	HSS Connection, client port dynamic
Services	4500	UDP	ISAKMP/ NAT	Yes	Yes	Closed	Server	
Services Ports	5060	TCP/UDP /SCTP	SIP	Yes	Yes	Closed	Both	SIP, client port dynamic

Ethernet	Ports	Protocol	Service	Optional	Configurable Port	Default Port State	Server or Client	Description
Services Ports	5061	TCP	SIP TLS	Yes	Yes	Closed	Both	SIP over TLS carried by TCP
Services Ports	1025-65535	TCP/UDP	RTP/ SRTP	Yes	Yes	Closed	Both	Media traffic
Services Ports	1025-65535	TCP	IMS AKA	Yes	Yes	Closed	Both	IMS AKA protected server port
Services Ports	1025-65535	TCP	IMS AKA	Yes	Yes	Closed	Client	IMS AKA protected client port

C

Mitigating SIP Attacks

The goal of this appendix is to provide configuration recommendations to be implemented on the Session Border Controller (SBC) to reduce the negative effects of SIP scanning tools.

The configuration techniques described will reduce the impact of attacks by known tools. The intent is to drop all packets received from these tools without responding wherever possible. This is not possible in all cases. DDoS configuration adjustments will be recommended to reduce the impact of attacks on SBC resources and allow uninterrupted service to legitimate, trusted users.

Overview

SIP scanning and attack tools employed by fraudsters may target specific IP address ranges directly, but most tend to be random scans of a whole range of IP addresses. The scanning and attack methodology seen most frequently includes:

1. OPTIONS - Discover whether a SIP process is open and listening by asking for supported SIP options
2. INVITE - Check for an open service that will forward calls without authorization or challenge for registration by sending an initial call request
3. INVITE or REGISTER – Send calls and/or user authentication requests; Based on the error received it may be possible to enumerate user extensions, or in other words determine what accounts are available for password cracking.
4. REGISTER - Guess weak or default passwords; The attacker sends tens, hundreds, or even thousands of passwords per discovered extension until a password is found.
5. Start making calls. The attacker then registers a soft client and makes call attempts. The initial call attempt may not work if a dial prefix is needed, so attackers try all of those until they get an outside line

Most of the scanning tools such as SIPVicious, SIPScan, smap, and Sipsak are open source and freely available. Other tools are used exclusively by specific segments of criminals. As of the end of 2012, 99% of the attacks on customer systems and public SIP honeypots that we tracked were committed using an open source tool with easily identifiable characteristics.

This appendix provides configuration recommendations and references for more detailed information used to mitigate attacks by SIP scanning and attack tools. Several methods will be discussed since not all solutions may be acceptable in all customer environments.

Deployment Archetypes

Oracle classifies SIP deployments in three different major archetypes:

Peering: Calls are sent from a SIP proxy to the SD. The proxy may host SIP user agents or analog devices if a gateway function is provided. Peering is deployed either over a private network such as MPLS from service provider to customer, or over-the-top (OTT) via the Internet.

Customers using SIP peering or “trunking” deployments can usually implement a combination of trusted Session Agents (SA) and Access Control Lists (ACLs) to limit what remote IP

addresses are able to communicate with the SD. In a peering network there is an implicit level of trust since the remote IP address is known and provisioned. When the trunk is delivered over a private network we are not usually concerned with SIP scanning prevention since there is no direct Internet access. In deployments where peering does happen over an untrusted network, such as OTT, the ACL entry drops incoming requests from unknown sources.

It then falls to the operator to determine if their particular architecture might see SIP scans from behind a trusted IP address. With multiple layers of NAT in IPv4 networks, it is always possible that messages are transiting through a firewall or gateway rather than just an individual SIP proxy.

Access: Calls are sent directly from a SIP endpoint to the SBC. A SIP registration may be required to authenticate and authorize the services available to the endpoint.

Access deployments will benefit the most from SIP scanner mitigation. This deployment model relies on the ability for users to roam, so ACLs based on known IP addresses cannot be used. Access to the network needs to be controlled via other means, usually through the use of a SIP registration.

Hybrid: Many networks have a mix of peering and access. In these cases, calls from remote subscribers may be sent to a trusted peer such as a service provider.

Strategies for Mitigating Against SIP Scanners

Mitigation against SIP scanners can be provided through several complementary strategies.

1. Access Control: Ensure proper configuration to block unauthorized end-points. Proper configuration of access control settings such as realm trust levels, access control lists (ACL), and SIP port allow-anonymous settings can limit traffic to known session agents and/or registered endpoints.
2. Threat Identification: Identify and drop messages from SIP scanners and avoid responding to the sender whenever possible - fraudulent messages can be dropped based on patterns found in the SIP messaging.
3. Enforcement: Limit attacks that cannot be identified as a scan from a known tool. Enforcement of message thresholds (DoS configuration) can demote or blocklist endpoints that do not become trusted or abuse their existing trust potentially limiting the damage of a scan.

There are several types of access control that apply to deployments over untrusted networks.

Denial of Service Prevention: The section regarding DoS in this appendix covesr proper configuration of access control parameters. Guidelines are provided for configuring trust levels, ACLs, allow-anonymous settings, and message thresholds.

Signaling Authentication and Encryption: SIP can be encrypted using the Transport Layer Security (TLS) protocol. If the connection is established using mutual certificate authentication, then a resulting benefit is effective access control. During the TLS connection establishment, the endpoint verifies the SBC certificate, and the SBC verifies the endpoint certificate was issued by a trusted Certificate Authority (CA). That mutual authentication provides assurance that the device is legitimate, and not an attack tool. When combined with the use of online certificate status protocol (OCSP), it is possible for administrators to refuse network access to devices that are lost or have left the organization. If TLS with mutual authentication is used, then the effects of all SIP scanning tools are mitigated.

Not all endpoints support installation of third party certificates or TLS encryption, and it may be difficult for an organization to issue and manage individual client certificates. TLS (and optionally SRTP) may also require additional hardware for encryption acceleration.

Endpoint Allowlisting: If an organization manages the endpoints in use it can fingerprint them the same way we fingerprint attack tools. Endpoints will advertise a SIP User-Agent value or may have proprietary SIP headers that provide identifying values. Messages from endpoints that do not have these characteristics can be rejected using a Header Manipulation Rule. Section 3 of this Tech Note describes the Header Manipulation Rules required to perform User-Agent allowlisting.

Threat Identification Alternative 1: sipShield SPL plug-in

The Session Plug-in Language (SPL) is an Oracle API library that exposes core functions to an embedded LUA processor via call-backs. A plug-in is an additional piece of software written using SPL that runs on the SBC to implement a custom feature. It is supported via Oracle Consulting Services.

sipShield enables the SBC to drop SIP messages containing the identifying characteristics of known malicious tools with absolutely no response to the attacker. The sipShield plug-in examines multiple characteristics of each message, and is superior to our second option, “Header Manipulation Rules for Scanner Mitigation” described below. It is recommended that sipShield should be used wherever possible.

Since sipShield requires a specific SPL API version, it is not available for all software releases. Only recent releases of software support sipShield at this time. To determine if sipShield is supported issue the “show spl” command in the ACLI. If the SPL version found is 2.0.1 or greater then sipShield is supported. If the command is not found then SPL is not included in the software release.

```
ACMEPACKET# show sp
SPL Version: C2.0.1
```

Threat Identification Alternative 2: Header Manipulation Rules for Scanner Mitigation

If sipShield is not appropriate for your environment, the second alternative is to use SIP header manipulation rules (HMR) to drop messages received from known, fraudulent User-Agent(s). The HMR rule processes each inbound message, and if a match is found, it marks the message as invalid or “Rogue”. Subsequent responses back to the attacker are dropped. Unfortunately the SD’s B2BUA will usually respond with an initial response (“100 Trying” or a 4xx error) prior to evaluation with the HMR (the specific response depends on realm settings). This gives the attacker the knowledge that there is a SIP process running (even though the INVITE response is dropped). As they continue their attack, INVITE and REGISTER messages will be dropped without reaching the core, and they will eventually be demoted or blocklisted depending on your DoS settings.

Header Manipulation Rules for Scanner Mitigation are covered below.

Enforcement: Implement DoS Prevention

Some scanning tools will not match a known pattern because they are either new, or a skilled attacker has changed SIP fields to make them less detectable. DoS/DDoS prevention settings can protect against attacks that cannot be identified by their SIP messaging. Endpoint actions can be limited by requiring them to register first, and by enforcing defined message thresholds. The administrator can determine what happens when the thresholds are exceeded – either a ‘demotion’ to a queue with less bandwidth, or blocklisting for a configurable period.

Basic DDoS configuration settings are outlined in the other appendices. However, for the best DDoS protection, the configuration should be customized based on the customer environment and the traffic levels they actually receive.

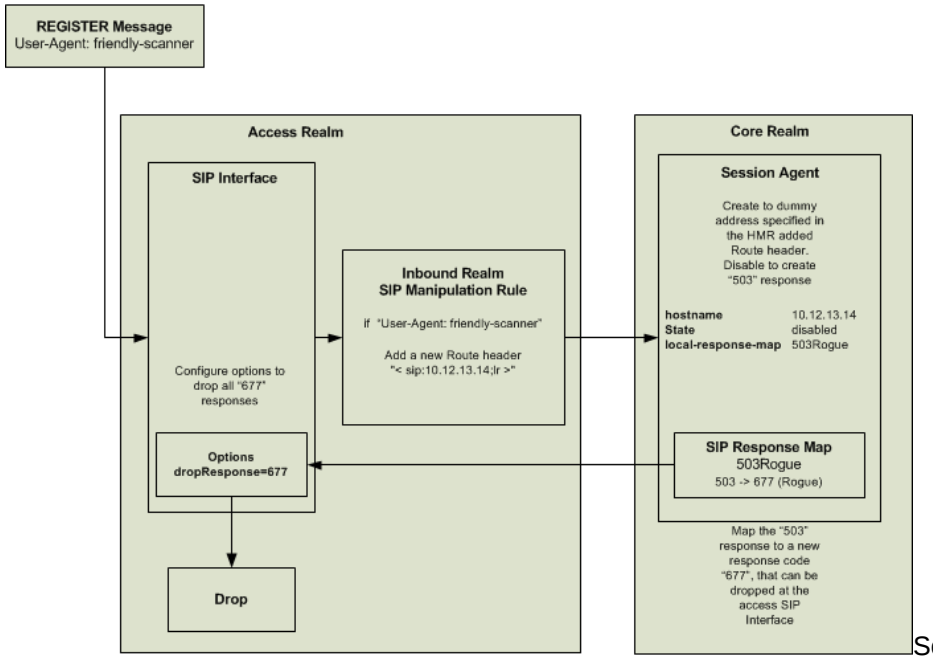
DoS settings that help mitigate SIP scanning risks are also depicted below.

SIP Header Manipulation Rule Logic

One way to drop all packets sent from an endpoint running an SIP scanner is to use a combination of SIP Manipulation Rules in conjunction with a dummy Session Agent. In this case, a dummy session agent is defined that is not an externally routable target.

As a message enters the SBC it is passed by the SIP interface to the incoming HMR. The HMR applies a regular expression against the message to determine if it is a scanning tool. If there is a match, the HMR can take action to mark it as invalid by inserting an additional route header and forwarding it to a “dummy” session agent. Provisioning the dummy session agent with the state disabled will cause the call to be refused. Custom mapping this to a unique error response can in turn be used in conjunction with a sip-interface option configurable to drop specific error responses.

Below is a flow diagram of how a SIP REGISTER message with a User-Agent header of “friendly-scanner” will be dropped.



Some customers have asked about using the “reject” action in HMRs to send a “677 Rogue” response rather than routing to a dummy session agent. However, the “reject” action is evaluated immediately, and therefore is not affected by the sip-interface dropResponse parameter so the attacker will receive many more responses than you intend.

Header Manipulation Rules Configuration

An inbound SIP Manipulation Rule needs to be created to modify any messages that contain a User-Agent header that is known (or suspected) to be fraudulent. The manipulation rule will add a Route header that directs the message to a “dummy” Session Agent.

Two rule examples are given. The first one identifies fraudulent User-Agent values, and the second allowlists only the desired User-Agent values and denies all others.

Note:

- The list of User-Agents in the match-value shown in the example should be entered without spaces between the pipe symbols. There is an extra space for formatting.
- Release S-CX7.2.0 and greater allows you to log attack messages to the /ramdrv/logs/matched.log file if you wish. Simply change the store action in the isScanner rule to log.
- If you already have inbound sip-manipulations the header rules identified in the examples below can be added to them.

WARNING:

If you have valid users of Counterpath Eyebeam in your environment then you should delete the final "|eyeBeam" string from the match-value below.

Identifying fraudulent User-Agent values

In this HMR, the first header-rule uses a logical OR and performs a regular expression match on multiple known User-Agent values. If any of these partial matches is found then the value is stored. The second rule checks to see if the first rule stored a value, and inserts the Route header if it did.

```
sip-manipulation
        name                    AddRoutHdr
        description
        split-headers
        join-headers
        header-rule
                name                    isScanner
                header-name             User-Agent
                action                  store
                comparison-type         pattern-rule
                msg-type                any
                methods
                match-value             friendly|sundayddr|SIPScan|
                                        smap|sipsak|sipcli|sipv|
                                        VaxIPUserAgent|eyeBeam
                new-value
        header-rule
                name                    addNullRoute
                header-name             Route
                action                  add
                comparison-type         boolean
                msg-type                request
                methods
                match-value             $isScanner.$0
                new-value               "<sip:10.12.13.14;lr>"
```

Allowlisting known User-Agents

A similar HMR is used here. The first header rule is replaced with one that uses a logical OR with multiple values, but its regular expression match is for valid User-Agents. If a valid User-Agent match is found, it is stored. The expressions used can match a part of the User-Agent string, and can be as specific (or unspecific) as required. The final rule has been modified to insert the invalid route if a valid User-Agent was NOT found.

> **Note:**
>
> If endpoint firmware is updated and the User-Agent string changes then the allowlist rule may start failing and endpoints will be denied. Make sure to perform lab testing prior to any endpoint software updates.

```
sip-manipulation
        name                    AddRoutHdr
        description
        split-headers
        join-headers
        header-rule
                name                    allowlist
                header-name             User-Agent
                action                  store
                comparison-type         pattern-rule
                msg-type                out-of-dialog
                methods
                match-value             (Bria Professional release 2.4.3
                                        stamp 50906|UCCAPI|Avaya SIP R2.2
                                        Endpoint Brcm)
                new-value
        header-rule
                name                    addNullRoute
                header-name             Route
                action                  add
                comparison-type         boolean
                msg-type                request
                methods
                match-value             !($allowlist.$0)
                new-value               "<sip:10.12.13.14;lr>
```

Realm: The access realm-config must also be modified to assign the SIP manipulation rule defined above as the inbound manipulation. Add the addRouteHdr manipulation for both fraudulent and allowlisting scenarios.

```
realm-config
        identifier              access
        description             Serving all access endpoints
        .
        .
        .
```

```
        in-translationid
        out-translationid
        in-manipulationid        addRouteHeader
```

Session Agent: A dummy Session Agent needs to be created with the state disabled. This is important so that the Session Agent will reply with a 503 response to any request. The 503 response will then be mapped to a new response code that can be easily dropped. A SIP Response Mapping is created to map any 503 from this Session Agent to a 677 SIP response code. We use an error code that is not valid according to RFCs so it can easily be distinguished from other traffic. Any 677 responses can then be dropped at the SIP Interface level without dropping any valid 503 responses from other endpoints. The SIP Response Mapping must be assigned in the Session Agent as shown below.

```
session-agent
        hostname                10.12.13.14
        ip-address
        port                    5060
        state                   disabled
        app-protocol            SIP
        transport-method        UDP
        realm-id                *
        .
        .
        .
        local-response-map      503Rogue
```

SIP Response Mapping: A SIP Response Mapping must be configured to map 503 responses from this Session Agent to a dummy response code (677). The response-map ACLI level can be found in configuration mode under session-router > sip-response-map.

```
response-map
        name              503Rogue
        entries           503 -> 677 (Rogue)
```

SIP Interface: All SIP interfaces that receive messages from SIP scanners require the option “dropResponse=677” to drop the 677 responses received from the dummy Session Agent.

```
sip-interface
        state              enabled
        realm-id           access
        .
        .
        .
        options            dropResponse=677
```

Scanner Mitigation using DDoS Settings

The DDoS settings recommended in the appendices will protect the SBC, but more strict trust levels and thresholds need to be defined to deny endpoints that are attempting to scan the system. To accomplish this, the access-control-trust-level on the access realm-config must be configured to low, which will cause endpoints to be blocklisted when they exceed thresholds. The untrusted-signal-threshold parameter defines the threshold of SIP messages received within the global tolerance-window (set under media-manager) before an untrusted user will

be demoted to denied. The untrusted-signal-threshold should be set to a value that is just greater than the number of messages required by an untrusted endpoint to become trusted through SIP registration. The untrusted-signal-threshold value should be confirmed by collecting and analyzing a packet capture from the targeted network deployment. In many cases a registration will be two or three messages, but endpoint behavior and requirements vary. When this threshold is exceeded, the endpoint will be placed on the denied list for the amount of time defined in the deny-period. This period should be determined based on your individual needs. Setting the deny period to a long duration may cause problems for endpoints that simply entered an incorrect password or had a connection issue with some packet loss.

The following parameters should also be customized to your needs based on expected call flows.

```
realm-config
        identifier                      access
        description                     Serving all access endpoints
        .
        .
        .
        access-control-trust-level      low
        invalid-signal-threshold        1
        maximum-signal-threshold        4000
        untrusted-signal-threshold      5
        nat-trust-threshold             0
        deny-period                     120
```

Configure the media-manager settings per the recommendations in the DDoS prevention appendix that is applicable for your architecture. The max-untrusted-signaling parameter will limit the amount of untrusted traffic the SBC will process.

If any media-manager settings are changed you MUST save, activate, and reboot the SBC so they will take effect.

Peering Environments

As noted earlier, this appendix does not focus on scanning attacks in SIP Peering environments. In these environments it is recommended to create static ACLs with a trust level appropriate for the peer. It is recommended when peering over a trusted network, such as an MPLS connection delivered from a service provider, that a “high” trust level should be used. If your trust in the peer is not assured, it may be appropriate to set trust level to “medium” or “low” so they will be limited or blocklisted for abuse. Keep in mind that signaling thresholds will then need to be set on the realm.

The realm-config, access-control-trust-level should match the trust-level of the ACL so that all traffic from any endpoint that does not have an ACL will be denied. Always make sure that the realm-id, source-address, destination-address, and application-protocol are specified.

```
realm-config
        identifier                      peer
        description
        addr-prefix                     172.16.101.6
        .
        .
        .
```

```
        access-control-trust-level      high

access-control
        realm-id                        peer
        description
        source-address                  172.16.101.6
        destination-address             197.168.11.100
        application-protocol            SIP
        transport-protocol              ALL
        acces                           permit
        average-rate-limit              0
        trust-level                     high
```

D

Intrusion Detection System

The Oracle Communications Session Border Controller (SBC) supports intrusion detection and protection capabilities using anomaly based detection. SIP messages are compared to their expected format per the SIP RFCs, and may be repaired or rejected based on the severity of the issue and the settings defined by the administrator. The Intrusion Detection System (IDS) provides notification of unexpected events using all of the configured monitoring methods for the SD, though the amount of detail in each may vary. An optional IDS Reporting Feature Group license provides additional detail for attempted intrusions and suspicious behavior. The IDS feature is part of the SBC Base Entitlement Group, and no extra license is required.

The following sections detail the security related events and statistics the SBC monitoring features can provide, some of which may be used as input to a security monitoring platform. Some of the following information may be partially repeated in other sections, but the intent is to provide further details and depict the relationship of various indicators here.

IDS Details

The IDS Reporting Feature Group includes the following additional capabilities.

- Media manager configuration elements visible after installing the license:
  - trap-on-demote-to-deny – controls traps for deny events
  - trap-on-demote-to-untrusted – controls traps for untrust demotion events
  - syslog-on-demote-to-deny – controls syslogs for deny events
- Access control list configuration elements visible after installing the license:
  - cac-failure-threshold –contributes to demotion
  - untrust-cac-failure-threshold –contributes to demotion
- Endpoint demotions based on admission control failures
- When you install the IDS license, the apSysMgmtInetAddrWithReason-DOSTrap trap (described below) is available and the apSysMgmtExpDOSTrap is disabled. Without an IDS license installed, only the apSysMgmtExpDOSTrap trap is available.

Endpoint Promotions and Demotions

Endpoints, whether or not they are defined as session-agents, are promoted and demoted between hardware-enforced trusted, untrusted, and denied Access Control List traffic queues based on trust level configuration. Static ACLs are also configurable to further classify signaling traffic as being permanently assigned to the appropriate trust queue.

Trust is assigned through several mechanisms including the access-control-trust-level parameter of the realm the session-agent or end point is a member of, trust-level of provisioned ACLs, and the allow-anonymous setting on the applicable sip-interface.

The SBC will demote an endpoint when:

1. It receives too many signaling messages within the configured time window (maximum-signal-threshold in the realm or static ACL)

2. It receives too many invalid signaling messages within the configured time window (invalid-signal-threshold in the realm or static ACL)
3. It receives too many signaling messages from an untrusted source within the configured time window (untrusted-signal-threshold in the realm or static ACL)
4. A trusted endpoint exceeds the call admission controls and the cac-failure-threshold defined in an ACL (the call admission control limits are defined in media profiles)
5. An untrusted endpoint exceeds call admission controls and the untrust-cac-failure-threshold defined in an ACL

The SBC will promote an endpoint when:

1. It receives a 200 OK response to a registration
2. The registration overload protection (reg-overload-protect) option has been set globally in the sip-config element (this is temporary, and only when a 401 or 407 response is received)
3. The deny-period expires

Statistics

Each promotion and demotion event, between trusted, untrusted, and deny queues is counted and kept as an ACL statistic. These counts are maintained separately for signaling applications.

Statistics for ACL status and operations can be seen using the ACLI commands show sipd.

```
ACMESBC# show sipd acls
16:25:48-180
SIP ACL Status            -- Period -- -------- Lifetime --------
                Active    High   Total      Total  PerMax    High
Total Entries        0       0       0          0       0       0
Trusted              0       0       0          0       0       0
Blocked              0       0       0          0       0       0

ACL Operations         ---- Lifetime ----
                Recent      Total  PerMax
ACL Requests         0          0       0
Bad Messages         0          0       0
Promotions           0          0       0
Demotions            0          0       0
Trust->Untrust       0          0       0
Untrust->Deny        0          0       0
```

SNMP MIB OIDS

The ACL statistics counters described previously are also available for SNMP polling under APSYSMGMT-MIB -> acmepacketMgmt -> apSystemManagementModule -> apSysMgmtMIBObjects -> apSysMgmtMIBGeneralObjects

- apSysSipEndptDemTrustToUntrust (.1.3.6.1.4.1.9148.3.2.1.1.19) - Global counter for SIP endpoint demotions from trusted to untrusted.
- apSysSipEndptDemUntrustToDeny (.1.3.6.1.4.1.9148.3.2.1.1.20) - Global counter for SIP endpoint demotions from untrusted to denied.

SNMP Traps

Enabling the trap-on-demote-to-deny parameter located in the media-manager-config configuration element enables SNMP traps to be sent for demotions to the denied queue.

When the IDS license is installed, the apSysMgmtInetAddrWithReasonDOSTrap trap is sent. Otherwise, only the apSysMgmtInetAddrDOSTrap trap is sent.

The IDS Reporting Feature Group added the capability for the SBC to send a trap when the SBC demotes an endpoint to the untrusted queue. Enabling the trap-on-demote-to-untrusted parameter located in the media-manager-config configuration element enables these. The same apSysMgmtI-netAddrWithReasonDOSTrap is sent.

When the IDS license is installed and the trap-on-demote-to-deny or trap-on-demote-to-untrusted parameters are disabled, the apSysMgmtI-netAddrWithReasonDOSTrap trap is not sent from the SBC, even when an endpoint is demoted.

When sent, the apSysMgmtInetAddrWithReasonDOSTrap contains the following data:

- apSysMgmtDOSInetAddressType—Blocked IP address family (IPv4 or IPv6)
- apSysMgmtDOSInetAddress—Blocked IP address
- apSysMgmtDOSRealmID—Blocked Realm ID
- apSysMgmtDOSFromURI—The FROM header of the message that caused the block (If available)
- apSysMgmtDOSReason—The reason for demoting the endpoint to the denied queue: Reports the following three values:
  - Too many errors
  - Too many messages
  - Too many admission control failures

HDR

The SIP (sip-ACL-oper) and MGCP (mgcp-oper) HDR ACL status collection groups include the following metrics:

- Demote Trust-Untrust - Global counter of endpoint demotion from trusted to untrusted queue
- Demote Untrust-Deny - Global counter of endpoint demotion from untrusted to denied queue

```
TimeStamp  ACL Requests Bad Msgs Promo Demo Demote Trust-Untrust Demote
Untrust-Deny
1369338880 0            0        0     0    0                    0
1369338940 0            0        0     0    0                    0
1369339000 0            0        0     0    0                    0
1369339060 0            0        0     0    0                    0
```

Syslog

A syslog message can also be generated when an endpoint is demoted. Setting the media-manager config -> syslog-on-demote-to-deny parameter to enabled writes an endpoint demotion warning to the syslog every time an endpoint is demoted to the denied queue. Demotions from trusted to untrusted can also be reported by setting the media-manager ->

syslog-on-demote-to-untrusted parameter to enabled. By default, these configuration options are set to disabled.

Without the IDS Reporting Feature Group license applied, the syslog messages have a WARNING level and look like this:

```
Jan 15 12:22:48 172.30.60.12 ACMESYSTEM sipd[1c6e0b90] WARNING
SigAddr[access:192.168.24.40:0=low:DENY] ttl=3632 guard=798 exp=30
Demoted to Block-List (Too many admission control failures)
```

The IDS Reporting Feature Group will provide an ERROR message with further detail like this:

```
Nov 28 17:53:47 172.41.3.41 ACMESYSTEM sipd[2dcc32a4] ERROR [IDS_LOG]
SigAddr[access:192.168.101.120:0=low:DENY] ttl=86400 exp=30 Demoted to
Block-List (Too many messages) last msg rcvd=REGISTER sip:192.168.66.2
SIP/2.0
Nov 28 17:53:47 172.41.3.41 CSE-4500-6 sipd[2dcc32a4] ERROR Via:
SIP/2.0/UDP 192.168.190.144:20928;branch=z9hG4bKdeadb33f
Nov 28 17:53:47 172.41.3.41 CSE-4500-6 sipd[2dcc32a4] ERROR From:
<sip:47097@192.168.190.144:20928>
Nov 28 17:53:47 172.41.3.41 CSE-4500-6 sipd[2dcc32a4] ERROR To:
<sip:47097@192.168.66.2:5060>
Nov 28 17:53:47 172.41.3.41 CSE-4500-6 sipd[2dcc32a4] ERROR Call-ID:
f9844fbe7dec140ca36500a0c9119870@192.168.66.2
Nov 28 17:53:47 172.41.3.41 CSE-4500-6 sipd[2dcc32a4] ERROR CSeq: 1
REGISTER
Nov 28 17:53:47 172.41.3.41 CSE-4500-6 sipd[2dcc32a4] ERROR Contact:
<sip:47097@192.168.190.144>
Nov 28 17:53:47 172.41.3.41 CSE-4500-6 sipd[2dcc32a4] ERROR User-
agent: UAC
Nov 28 17:53:47 172.41.3.41 CSE-4500-6 sipd[2dcc32a4] ERROR Max-
Forwards: 5
Nov 28 17:53:47 172.41.3.41 CSE-4500-6 sipd[2dcc32a4] ERROR Content-
Length: 0
```

Some small number of demotions will be normal in a network, and there may be an initial learning period where it is crucial to understand:

- What are the stable and “common” values of these counters
- On-going demotions and promotions on ACLs and to which SIP UAs they refer

Monitoring systems need to be configured to take these normal variations into account, and have appropriate thresholds defined. Note that the thresholds, as well as the SBC DoS or CAC parameters may need to be adjusted over time as the network being monitored grows and changes.

Authentication Failures used for Endpoint Demotion

Endpoints that have become trusted due to successful registration are entered into the registration cache. The cache is used to store the user and location information for authenticated endpoints. It may also be used to shield the registrar from having to respond to re-registrations by providing the SBC the data to reply to a portion of re-registrations locally. When an endpoint fails re-registration, it will be demoted from trusted to untrusted.

When an endpoint sends an INVITE with authentication, but the credentials do not match what is known to the registrar, it will be demoted.

In these scenarios, 401 or 407 responses are received from the registrar, and the demotion occurs.

Per-endpoint Call Admission Control

The SBC can demote endpoints from trusted to untrusted, or untrusted to denied queues when CAC failures exceed a configured threshold. The SBC maintains CAC failures per-endpoint. The CAC failure counter is incremented upon certain admission control failures only if either: cac-failure-threshold or untrust-cac-fail-threshold is set to a non-zero integer.

The cac-failure-threshold parameter is configurable in the access control and realm configuration elements. Exceeding the threshold integer defined in this parameter demotes an endpoint from the trusted queue to the untrusted queue. Additionally, the untrust-cac-failure-threshold parameter is configurable in the access control and realm configuration elements. Exceeding the threshold integer defined in this parameter demotes an endpoint from the untrusted queue to the denied queue. When both the cac-failure-threshold and untrust-cac-failure-threshold are configured to 0, admission control failures are considered and counted as invalid signaling messages for determining if the invalid-signal-threshold parameter value has been exceeded.

CAC failures used for Endpoint Demotion

The SBC determines CAC failures only by considering the number of signaling messages sent FROM an endpoint TO the realm its signaling messages traverse

When an endpoint exceeds the following CAC thresholds, the SBC demotes the endpoint when the CAC failure thresholds are enabled.

- sip-interface user CAC sessions (realm-config > user-cac-sessions)
- sip-interface user CAC bandwidth (realm-config > user-cac-bandwidth)
- External policy server rejects a session

Thresholds and Trending Analysis

Thresholds and trending analysis are important concepts that must be well understood and implemented during initial installation of the SBC. Thresholds should be monitored and settings periodically adjusted as network usage or capacity requirements change. To be supported by Oracle TAC, SBC deployments require a minimum set of standard configurations explained in the DDoS Prevention appendices. These settings are considered the minimum configuration required to protect the SD. Upon deployment of a DDoS provisioned SBC Oracle recommends that you continuously monitor common traffic load and patterns of services traversing your SBC, and understand any alarms received.

Regardless of the monitoring method used (for example, SNMP, CDR, HDR, Syslogs), during the initial period after implementation it is crucial to understand:

- The number of active SIP sessions seen during normal and peak periods
- Average call hold times
- Average signaling messages for a call (usually best collected through Wireshark or other network capture tool)
- What are the stable and “common” values of these for the different counters
  - Trusted to Untrusted Demotions

  - Untrusted to Deny Demotions
  - Demotions
  - Promotions
- On-going demotions and promotions on ACLs, and to which SIP UAs they refer
- Why there are any deny entries and to which SIP UAs they refer
- Whether the deny period set is helping or causing more issues
- Whether the assigned trust level is denying more than one endpoint (for example, issues with NAT)
- CAC or session count thresholds, and whether they are impacting service

When this knowledge base is built and properly documented for future reference, threshold values for reasonable variations in these counters should be defined and implemented in the monitoring platforms handling the SNMP Traps, HDR data, Sys-logs provided by the SBC.

Oracle recommends parsing and evaluating the information provided in any apSysMgmtInetAddrWithReasonDOSTrap SNMP traps received. Using this information it should be possible to identify SIP UAs and accounts involved, and understand whether legitimate traffic is being denied. Further actions may be required after this analysis; for example: configuration improvements to avoid illegitimate traffic from reaching the Host CPU may be needed, or, if the traffic is expected, adjustment of the appropriate constraints to allow the legitimate traffic to flow properly.

This process is an iterative loop where the fine-tuning and documenting illegal behavior flows can be continuously improved. This is especially true if the SBC is exposed to the Internet in an Access Scenario. When connected to the Internet, different trends and attempted illegal behaviors may be seen as the complexity of SIP attacks and trends evolve.

Constraints Limiting

The SBC provides two distinct mechanisms to throttle any SIP method: session constraints and rate-constraints. While session constraints are responsible for throttling both INVITE and REGISTER methods, rate constraints are used for throttling any other type of SIP method. Session constraints and rate constraints can be configured in either Session-Agent or SIP-interface config objects (via session-constraints). Note: Make sure to enable the sip-config > extra-method-stats option before configuring any constraints since this enables the constraint counters.

Session-Constraints

The session-constraints configuration element defines session layer constraints for session measurements such as maximum concurrent sessions, maximum outbound concurrent sessions, maximum session burst rate, and maximum session sustained rate.

The SIP interface configuration’s constraint-name parameter applies a pre-defined session-constraint configuration. Using the constraints defined, the SBC checks and limits traffic according to those settings for the SIP interface. When session constraints are not configured or applied on the SIP interface, the SIP interface will be unconstrained. When a single session-constraint element is applied to multiple SIP interfaces, each SIP interface will maintain its own copy of the session-constraint statistics.

- name - name of the session-constraint, this must be an unique identifier
- max-sessions - maximum sessions allowed for this constraint
- max-inbound-sessions - maximum inbound sessions allowed for this constraint
- max-outbound-sessions - maximum outbound sessions allowed for this constraint
- max-burst-rate - maximum burst rate (invites per second) allowed for this constraint
- max-inbound-burst-rate - maximum inbound burst rate (number of session invitations per second) for this constraint
- max-inbound-sustain-rate - maximum inbound sustain rate (of session invitations allowed within the current window) for this constraint
- max-outbound-burst-rate - maximum outbound burst rate (number of session invitations per second) for this constraint
- max-sustain-rate - maximum rate of session invitations allowed within the current window for this constraint
- max-inbound-sustain-rate - maximum inbound sustain rate (of session invitations allowed within the current window) for this constraint
- max-outbound-sustain-rate - maximum outbound sustain rate (of session invitations allowed within the current window) for this constraint
- min-seizures - minimum number of seizures for a no-answer scenario
- min-asr - Enter the minimum ASR in percentage
- time-to-resume - number of seconds after which the Session Agent (SA) is put back in service (after the SA is taken out-of-service because it exceeded some constraint)
- in-service-period - Enter the time in seconds that elapses before an element (like a session agent) can return to active service after being placed in the standby state
- ttr-no-response - Enter the time delay in seconds to wait before changing the status of an element (like a session agent) after it has been taken out of service because of excessive transaction timeouts
- burst-rate-window - Enter the time in seconds used to measure the burst rate
- sustain-rate-window - Enter the time in seconds used to measure the sustained rate

Oracle recommends use of session constraints on external SIP interfaces to limit the total number of sessions and traffic bursts that the combined configured session agents can handle for that service. Additionally, having multiple public SIP interfaces defined can limit the resources a particular SIP interface can provide based on service level agreements or the trust level of the endpoint.

Rate constraints

The rate-constraints sub-element is configurable under both the session-constraints and session-agent configuration elements (though they are not shared). It allows configuration of rate limiting based on specific method types. These further restrict any defined constraints of the parent, so they cannot exceed the rates defined at the level under which they are set.

- method—the SIP method name for the method to throttle, possible values are: NOTIFY, OPTIONS, MESSAGE, PUBLISH, REGISTER
- max-inbound-burst-rate—For the SIP method configured in the method parameter, this number will restrict the inbound burst rate on the SIP interface.

- max-outbound-burst-rate—For the SIP method configured in the methods parameter, this number will restrict the outbound burst rate on the SIP interface.
- max-inbound-sustain-rate—For the SIP method configured in the methods parameter, this number will restrict the inbound sustain rate on the SIP.
- max-outbound-sustain-rate—For the SIP method configured in the methods parameter, this number will restrict the outbound sustain rate on the SIP interface.

Each rate constraint configured for a SIP method maintains its own counters. For example, if a rate constraint for the PUBLISH method is configured, the burst and sustain rates set for it apply only to the PUBLISH method and not to any other methods.

The SBC captures statistics for SIP methods that have already been throttled by rate constraints for SIP interfaces and session agents; it does not capture these statistics for the global SIP configuration. SIP interfaces have two states: “In Service” and “Constraints Exceeded.” When any one of the constraints is exceeded, the status of the SIP interface changes to “Constraints Exceeded” and stops accepting traffic. It remains in that state until the time-to-resume period ends. The session constraint timers that apply to the SIP interface are the time-to-resume, burst window, and sustain window.

Oracle recommends configuration of INVITE and REGISTER method rate constraints on session agents.

For SIP access deployments, rate constraints for individual method types along with a set of burst and sustain rates should be considered. These constraints can help to avoid overloading the core network. In addition, they restrain the load non-INVITE messages use, thus reserving capacity for INVITE-based sessions and registrations.

In order to properly configure constraint limiting, either at SIP interface level or per Session-Agent (SA), it’s essential to have an accurate understanding of the SIP Message flows that exist in the network. Contributing factors include: factors such as which SIP requests are authenticated, what Call flows and Session Agents require re-INVITEs, maximum CPS per SA, etc. The reason why these details are so important is the SBC is making dynamic decisions and acting on this traffic in real time.

SNMP traps will be sent when constraints are exceeded. Constraint threshold crossing alarms or statistics are not necessarily a security issue since legitimate traffic overloads or mass network restarts may also cause them. It is up to the customer to assess if they should investigate alarms as possible security incidents.

To monitor SIP interface and Session Agents, two commands are most useful. The following commands include statistics on how many times the constraints were exceeded and the interface or session agent was temporarily taken out of service.

```
show sipd interface <realm name> and show sipd agents <agent name>
```

```
ACMEPACKET# show sipd interface access
00:51:55-34
Sip Interface access
                          -- Period -- -------- Lifetime --------
                  Active    High   Total      Total  PerMax    High
Inbound Sessions    9000    9002    1715   14244739    1501    9009
  Rate Exceeded        5       5       5          5       5       5
  Num Exceeded         -       -       0          0       0       -
```

```
  Burst Rate             0      50       0          0       0      51
Outbound Sessions        0       0       0          0       0       0
  Rate Exceeded          -       -       0          0       0       -
  Num Exceeded           -       -       0          0       0       -
  Burst Rate             0       0       0          0       0       0
Local Contacts           0       0       0          0       0       0
HNT Entries              0       0       0          0       0       0
Non-HNT Entries          0       0       0          0       0       0
Subscriptions            0       0       0          0       0       0
Out of Service           -       -       0          0       0       -
Trans Timeout            0       0       0          0       0       0
Requests Sent            -       -       0        284       1       -
Requests Complete        -       -       0          0       0       -
Seizure                  -       -       0          0       0       -
Answer                   -       -       0          0       0       -
  ASR Exceeded           -       -       0          0       0       -
Messages Received        -       -   14097  114313292   12405       -
Latency=0.000; max=0.000
```

```
ACMEPACKET# show sipd agents 192.168.60.10
00:54:10-49
Session Agent 192.168.60.10() [In Service]
                          -- Period -- -------- Lifetime --------
                   Active    High   Total      Total  PerMax    High
Inbound Sessions        0       0       0          0       0       0
  Rate Exceeded         -       -       0          0       0       -
  Num Exceeded          -       -       0          0       0       -
  Burst Rate            0       0       0          0       0       0
  Reg Rate Exceeded     -       7      21         21      21      21
  Reg Burst Rate        0       0       0          0       0       0
Outbound Sessions    9000    9003    2452   14251475    1501    9009
  Rate Exceeded         -       -       0          0       0       -
  Num Exceeded          -       -       0          0       0       -
  Burst Rate            0      50       0          0       0      51
  Reg Rate Exceeded     -       -       0          0       0       -
Local Contacts          0       0       0          0       0       0
HNT Entries             0       0       0          0       0       0
Non-HNT Entries         0       0       0          0       0       0
Subscriptions           0       0       0          0       0       0
Out of Service          -       -       0          3       1       -
Trans Timeout           0       0       0         44       1      40
Requests Sent           -       -   17666  100035216   10906       -
Requests Complete       -       -   17671  100035175   10905       -
Seizure                 -       -    2456   14251479    1501       -
Answer                  -       -    2456   14250766    1502       -
  ASR Exceeded          -       -       0          0       0       -
Messages Received       -       -   22595  128521055   13904       -
Latency=0.002; max=0.033
```

Message Rejections

The action type called reject is available to all header manipulation rules. When this action type is used, and a condition matching the manipulation rule arises, the SBC rejects the request, provides a SIP error, and increments a counter.

- If the msg-type parameter is set to any and the message is a response, the SBC increments a counter to show the intention to reject the message—but the message will continue to be processed.
- If the msg-type parameter is set to any and the message is a request, the SBC performs the rejection and increments the counter.

The header manipulation rule -> new-value parameter is designed to supply the status code and reason phrase corresponding to the reject. The following syntax is used to supply this information: status-code[:reason-phrase] . The status-code and reason phrase information is not required since by default the system uses 400:Bad Request.

If this information is not supplied, the status code must be a positive integer between 300 and 699. With this defined, the SBC will use the applicable reason phrase corresponding to the status code in responses. To customize the reason phrase, enter the status code followed by a colon (:). NOTE: be sure to enclose the entire entry in quotation marks (ex: “400:Go Away”) if the reason phrase includes spaces.

When the SBC performs the reject action, the current SIP manipulation stops processing and does not act on any of the rules following the reject rule. This course of action is also true for nested SIP manipulations that might have been constructed using the sip-manip action type. Keeping that in mind, the reject rule is usually the last rule in a long HMR.

Reject actions may also indirectly generate SNMP traps. Two parameters in the session-router-config define how many messages within a window of time cause the SBC to generate an SNMP trap.

- reject-message-threshold— defines the minimum number of message rejections allowed in the reject-message-window time on the SBC (when using the SIP manipulation action reject) before generating an SNMP trap.
- reject-message-window—defines the time in seconds that defines the window for maximum message rejections allowed before generating an SNMP trap. This should be set to something like 30 seconds to a minute. If set too low traps may be missed.

The SBC tracks messages that have been flagged for rejection using the reject action type. In the show sipd display, refer to the Rejected Messages category. Note that there is no distinction between requests and responses.

```
SIP Status                -- Period -- -------- Lifetime --------
                  Active     High   Total       Total   PerMax     High
Sessions               0        0       0         538      211       38
Subscriptions          0        0       0           0        0        0
Dialogs                0        0       0         276       74       74
CallID Map             0        0       0        1076      422      386
Rejections             -        -       0           0        0
ReINVITEs              -        -       0           0        0
ReINV Suppress         -        -       0           0        0
Media Sessions         0        0       0         538      211       76
Media Pending          0        0       0           0        0        0
```

```
Client Trans          0       0       0        814     241      76
Server Trans          0       0       0       3626     366     193
Resp Contexts         0       0       0        538     211     193
Saved Contexts        0       0       0          0       0       0
Sockets               3       3       0          3       3       3
Req Dropped           -       -       0          0       0
DNS Trans             0       0       0          0       0       0
DNS Sockets           0       0       0          0       0       0
DNS Results           0       0       0          0       0       0
Rejected Msgs         0       0       0        200     108     108
```

SNMP support

- apSysRejectedMessages (.1.3.6.1.4.1.9148.3.2.1.1.18.0) - Number of messages rejected by the SBC due to matching criteria
- apSysMgmtRejectedMesagesThresholdExeededTrap (.1.3.6.1.4.1.9148.3.2.6.0.57) - The trap will be generated when the number of rejected messages exceeds the configured threshold within the configured window.
- apSysMgmtSipRejectionTrap (.1.3.6.1.4.1.9148.3.2.10.0.1) - Generated when a SIP INVITE or REGISTRATION request fail.

Log Action

The action type called: “log” is available to all header manipulation rules. When this action type is used, and a condition matching the manipulation rule arises, the SBC logs information about the current message to a separate log file.

This feature can be used to log important details from specific suspicious users, such as well-known SIP User-Agents, call attempts to undesirable destinations (known “hotlist” numbers, unassigned numbers, Premium Rate numbers, etc.).

If a match is found in an HMR, and the action is set to “log”, a logfile called matched.log will be created. The matched.log file contains a log message that contains a timestamp, destination IP address:port information, and the source IP address:port. It also specifies the rule that triggered the log action. The request URI, Contact header, To Header, and From header are also recorded. See the example below.

```
Apr 17 14:17:54.526 On [0:0]192.168.1.84:5060 sent to 192.168.1.60:5060
element-rule[checkRURIPort]
INVITE sip:service@192.168.1.84:5060 SIP/2.0
From: sipp <sip:+2125551212@192.168.1.60:5060>;tag=3035SIPpTag001
To: sut <sip:service@192.168.1.84>
Contact: sip:sipp@192.168.1.60:5060
```

E

Blocklisting with Local Routing Tables

Several industry groups such as the GSMA Fraud Forum and the Communications Fraud Control Association (CFCA) track phone numbers and number prefixes that have been verified as participating in various types of fraud. These numbers are published as a list for their members. Many organizations also track numbers that abuse their network on a regular basis.

While it can be more of an art than a science, some customers wish to blocklist incoming or outgoing calls based on a dialed number prefix, or the entire dialed number. While complex or expensive fraud management solutions can be used, this Appendix provides a simple way to perform this blocklisting on the SBC.

> **Note:**
>
> This procedure will end up denying calls coming into your network. Be sure to test your local route tables (LRT) in a test environment before deploying in production.

It is assumed that as calls have been sent to the SBC or as they enter the SBC that they will be “normalized” by either the directly connected agent or an incoming HMR to match the local dial plan. For example in North America it is necessary to include the leading “1” for NANP and remove the “011” for calls outside of the NANP. If this is not possible, then the “011” can be pre-pended onto the number matches in the LRT file.

Depending on what you are trying to prevent, you may want to check both the FROM and TO fields in SIP messages. This same strategy can be used on your access realm, or even your core realm if you so choose.

To create the blocklist for routing you need to:

1. Enter your FROM or TO blocklist numbers into one or more LRTs - and save them with an “.xml” extension. Next gzip them (.gz format). A sample LRT format is found below.
2. Upload the .xml.gz file to the to SBC in the /code/lrt directory (which will need to be created the first time)
3. Update SBC config as depicted below

Apply an LRT check for the SIP From and To headers as the first two policy-attributes on all incoming realms, and on the core side if you want to detect outgoing fraudulent calls.

```
local-policy
        from-address
                                        *
        to-address
                                        *
        source-realm
                                        access
        description
        activate-time                   N/A
```

```
        deactivate-time                 N/A
        state                           enabled
        policy-priority                 none
        last-modified-by                admin@10.0.240.19
        last-modified-date              2012-10-26 17:13:15
```

(The first policy checks the FROM field. Note that the .xml.gz file extension is not specified.)

```
  policy-attribute
                next-hop                        lrt:blocklist;key=$FROM
                realm
                action                          none
                terminate-recursion             enabled
                carrier
                start-time                      0000
                end-time                        2400
                days-of-week                    U-S
                cost                            0
                app-protocol
                state                           enabled
                methods
                media-profiles
                lookup                          single
                next-key
                eloc-str-lkup                   disabled
                eloc-str-match
```

(The second policy checks the TO field. This is OPTIONAL, and only if you want to check the number being dialed. You can use the same LRT file, or a different file.)

```
        policy-attribute
                next-hop                        lrt:blocklist;key=$TO
                realm
                action                          none
                terminate-recursion             enabled
                carrier
                start-time                      0000
                end-time                        2400
                days-of-week                    U-S
                cost                            0
                app-protocol
                state                           enabled
                methods
                media-profiles
                lookup                          single
                next-key
                eloc-str-lkup                   disabled
                eloc-str-match
```

(The third and last policy is essentially a default SIP route that forwards calls onto the core.)

```
        policy-attribute
                next-hop                        192.168.60.10
                realm                           core
                action                          none
                terminate-recursion             disabled
                carrier
                start-time                      0000
                end-time                        2400
                days-of-week                    U-S
                cost                            0
                app-protocol
                state                           enabled
                methods
                media-profiles
                lookup                          single
                next-key
                eloc-str-lkup                   disabled
                eloc-str-match
```

Create the LRT configuration referenced above. Note that the “best” match mode matches from most specific to least specific in the LRT table (greatest number of digits matched to fewest).

```
local-routing-config
        name                            blocklist
        file-name                       blocklist.xml.gz
        prefix-length                   15
        string-lookup                   disabled
        retarget-requests               enabled
        match-mode                      best
        last-modified-by                admin@10.0.240.19
        last-modified-date              2012-10-26 15:40:48
```

Sample Entries from the LRT are seen below. In this case I’ve opted to forward the blocklist call onto a “dummy” session agent. You may opt to forward the call onto a recording, or session agent that handles fraud calls.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<localRoutes xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <route>
        <user type="E164">3712900</user>
        <next type="regex">!(^.*$)!sip:\110.11.12.13!</next>
    </route>
    <route>
        <user type="E164">88183521</user>
        <next type="regex">!(^.*$)!sip:\1@10.11.12.13!</next>
    </route>
    <route>
        <user type="E164">2637749</user>
        <next type="regex">!(^.*$)!sip:\1@10.11.12.13!</next>
    </route>
    <route>
```

```
        <user type="E164">3718104</user>
        <next type="regex">!(^.*$)!sip:\1@10.11.12.13!</next>
    </route>
    <route>
        <user type="E164">3718103</user>
        <next type="regex">!(^.*$)!sip:\1@10.11.12.13!</next>
    </route>
    <route>
        <user type="E164">3716852</user>
        <next type="regex">!(^.*$)!sip:\1@10.11.12.13!</next>
    </route>
    <route>
        <user type="E164">447924</user>
        <next type="regex">!(^.*$)!sip:\1@10.11.12.13!</next>
    </route>
    <route>
        <user type="E164">3712769</user>
        <next type="regex">!(^.*$)!sip:\1@10.11.12.13!</next>
    </route>
</localRoutes>
```

Once the configuration has been saved and activated, the LRT file contents can be confirmed by executing the command “show lrt route-entry blocklist 3712900” at the ACLI (or any of the other blocklist prefixes, or numbers that contain the prefix).

Next, the dummy session agent must be set up. The hostname must match the LRT host entry. Note that the response-map AND local-response map are required to identify blocklisted calls vs. just valid errors.

Make sure the session-agent state is disabled so traffic or error messages are not sent to a real host. It should be noted that use of a real hostname will not work due to the way DNS resolution works in conjunction with disabled session-agents.

```
session-agent
        hostname                        10.11.12.13
        ip-address
        port                            5060
        state                           disabled
        app-protocol                    SIP
        app-type
        transport-method                UDP
        realm-id
      response-map                 503Fraud
        local-response-map              503Fraud
```

Next, map the error to an error code we can identify and log / reject for trap.

```
session-router > sip-response-map
response-map
        last-modified-by                admin@10.0.240.19
        last-modified-date              2012-10-26 17:06:07
        name                            503Fraud
        entries                         503 -> 678 (Fraud)
```

On the access realm, the out-manipulationid should reference the “logBlocklist” HMR below. Note that if there is already an outbound HMR in ploce that the header rules below can be added to the existing HMR.

```
sip-manipulation
        name                            logBlocklist
        description
        split-headers
        join-headers
        header-rule
                name                            logBlocklist
                header-name                     @status-line
                action                          manipulate
                comparison-type                 case-sensitive
                msg-type                        reply
                methods
                match-value
                new-value
```

(Log the call that matched the blocklist to a local file “matched.log” on the SBC)

```
element-rule
        name                            logstatus
        parameter-name
        type                            status-code
        action                          log
        match-val-type                  any
        comparison-type                 case-sensitive
        match-value                     678
        new-value
```

(Replace the SIP status code and reason message with whatever you want to send back to the service provider or client.)

```
element-rule
        name                            replaceStatus
        parameter-name
        type                            status-code
        action                          replace
        match-val-type                  any
        comparison-type                 case-sensitive
        match-value                     678
        new-value                       603
element-rule
        name                            replaceReason
        parameter-name
        type                            reason-phrase
        action                          replace
        match-val-type                  any
        comparison-type                 case-sensitive
        match-value                     Fraud
        new-value                       Declined
```

(Finally, invoke the SBC message rejection via HMR.)

```
element-rule
        name                            rejectDeclined
        parameter-name
        type                            reason-phrase
        action                          reject
        match-val-type                  any
        comparison-type                 case-sensitive
        match-value                     Declined
        new-value
```

Notice that this config will send along the 603 error code which should be enough to refuse a call and stop recursion. If your trunking provider has a different standard message this can easily be changed.

The “reject” action in “rejectDeclined” will cause the “Rejected Messages” count to increment in the show sipd display. If you wish to send traps to a management station when this HMR fires, update the settings in session-router-config. The configuration below will send a apSysMgmtRejectedMesagesThresholdExeededTrap whenever more than one blocklisted call is seen inside a 30 second window. This is an indicator that the administrator should examine the matched.log file to determine the number pattern that was seen.

```
session-router > session-router > sel
reject-message-threshold    1
reject-message-window        30
```

Blocklist Table Maintenance

As new blocklist tables are released the customer can upload to /code/lrt and execute the following commands:

```
ACMEPACKET# config t
ACMEPACKET(configure)# session-router
ACMEPACKET(session-router)# local-routing-config
ACMEPACKET(local-routing-config)# select
<name>:
1: name=blocklist file name=blocklist.xml.gz prefixLength=15

selection: 1
```

Use the “show” command to verify the local-routing-config entry’s configuration

```
ACMEPACKET(local-routing-config)# show
local-routing-config
        name                            blocklist
        file-name                       blocklist.xml.gz
        prefix-length                   15
        string-lookup                   disabled
      match-mode                best
```

Change the “file-name” parameter to reflect the original compressed XML file

```
ACMEPACKET(local-routing-config)# file-name lookup.xml.gz
ACMEPACKET(local-routing-config)# done
local-routing-config
        name                            blocklist
        file-name                       blocklist102612.xml.gz
        prefix-length                   15
        string-lookup                   disabled
      match-mode                best
```

Exit out of configuration mode, save, and activate the configuration.

```
ACMEPACKET(local-routing-config)# exit
ACMEPACKET(session-router)# exit
ACMEPACKET(configure)# exit
ACMEPACKET#save-config
ACMEPACKET#activate-config
Activate-Config received, processing.
waiting for request to finish
Request to 'ACTIVATE-CONFIG' has Finished,
Activate Complete
```

After applying a new LRT, verify if by doing the same command from above “show lrt route-entry blocklist 3712900” at the ACLI (again, any of the hotlist numbers can be used). If something went wrong, change your config back to the old file and re-test.

After you have a few LRT files on the SBC you may want to clean the old ones up.

F

SNMP Monitoring

Simple Network Management Protocol (SNMP) polling (GET and SET) requests are used to retrieve operational data and modify configuration are supported by SBC. The SBC supports SNMPv1 and SNMPv2c for GET and SET requests. Oracle recommends using SNMPv3. Oracle release-specific SNMP MIBs can be found on docs.oracle.com for the release in use.

Below is a recommended list of SNMP OIDs to retrieve regularly from the Oracle System Management MIB (ap-smgmt.mib). Use the snmpgetnext, snmpgetbulk, snmpwalk, or snmpwalkbulk commands. These will provide useful data on overall system performance and security issues.

apSysMgmtGeneralObjects (1.3.6.1.4.1.9148.3.2.1.1)

- apSysCPUUtil (1.3.6.1.4.1.9148.3.2.1.1.1) - Percentage of CPU utilization
- apSysMemoryUtil (1.3.6.1.4.1.9148.3.2.1.1.2) - Percentage of memory utilization
- apSysHealthScore (1.3.6.1.4.1.9148.3.2.1.1.3) - System health percentage
- apSysRedundancy (1.3.6.1.4.1.9148.3.2.1.1.4) - Active or Standby SD
- apSysGlobalConSess (1.3.6.1.4.1.9148.3.2.1.1.5) - Total instant number of system concurrent sessions
- apSysGlobalCPS (1.3.6.1.4.1.9148.3.2.1.1.6) - Instant number of system calls per second
- apSysNATCapacity (1.3.6.1.4.1.9148.3.2.1.1.7) - Percentage of NAT table in CAM utilization
- apSysARPCapacity (1.3.6.1.4.1.9148.3.2.1.1.8) - Percentage of ARP table in CAM utilization
- apSysLicenseCapacity (1.3.6.1.4.1.9148.3.2.1.1.10) - Percentage of licensed sessions in use
- apSysSipStatsActiveLocalContacts (1.3.6.1.4.1.9148.3.2.1.1.11) - Current number of cached SIP registered contacts
- apSysApplicationCPULoadRate (1.3.6.1.4.1.9148.3.2.1.1.16) - Average load rate of applications over past 10 seconds
- apSysSipEndptDemTrustToUntrust (1.3.6.1.4.1.9148.3.2.1.1.19) - Number of SIP endpoints demoted from trusted to untrusted queue
- apSysSipEndptDemUntrustToDeny (1.3.6.1.4.1.9148.3.2.1.1.20) - Number of SIP endpoints demoted from untrusted queue to denied
- apSysRejectedMessages (.1.3.6.1.4.1.9148.3.2.1.1.18.0)- Number of messages rejected by the SBC due to matching criteria
- apSysStorageSpaceTable (1.3.6.1.4.1.9148.3.2.1.1.23), apSysStorageSpaceEntry (1.3.6.1.4.1.9148.3.2.1.1.23.1)
- apSysVolumeAvailSpace (1.3.6.1.4.1.9148.3.2.1.1.23.1.4) - Space remaining on the Storage Expansion Module (in MB)

apSysMgmtInterfaceObjects (1.3.6.1.4.1.9148.3.2.1.8), apSysMgmtPhyUtilTable (11.3.6.1.4.1.9148.3.2.1.8.1)

- apPhyUtilTableRxUtil (1.3.6.1.4.1.9148.3.2.1.8.1.1.1) - Received Network Interface utilization over one second period
- apPhyUtilTableTxUtil (1.3.6.1.4.1.9148.3.2.1.8.1.1.2) - Transmitted Network Interface utilization over one second period

See the *MIB Guide* for more information about MIBs.

G
Syslog

You can configure the Session Border Controller (SBC) to send system event logs to logging servers [1]. Oracle recommends that you configure as few logging servers as required to reduce impact on SBC performance. Monitoring through SNMP is the preferred option over using syslog. The syslog messages are not as efficient because they may contain many extraneous informational messages that need to be filtered out or parsed. SNMP has the advantage of sending clearly defined trap notifications only in the event of a problem, and you can configure the system-config and trap-receiver settings to filter on specific SNMP traps to send.

If a syslog parser is used to escalate SBC issues, it is easy to classify syslog events preceded with a MAJOR or CRITICAL designation as issues that require further investigation. Be cautious of writing any parsing rules for events that are classified as GENERAL, REDUNDANCY, CONFIG WARNING, ERROR, or MINOR (among others). Some of these may be important to escalate, but others may be strictly informational in nature.

The following table shows a sample of some of the common syslog messages that you may see. Note that IDS_LOG examples given require the IDS Reporting Feature Group license discussed in Appendix F. Some of the examples may seem redundant because sometimes more than one message may be written to syslog as the result of an event.

An unsuccessful log in attempt was detected on the console port.

```
Jun 16 15:26:02.355 [GENERAL] (0) loginLocal: [0:2801] user: admin
authenticate
Jun 16 15:26:02.800 [MINOR] (0) loginLocal:[0:2801] user: admin failed to
log in to console
```

An endpoint exceeded a defined constraint and was blocklisted. This is the result of DoS configuration with the IDS license.

```
Nov 28 17:53:47 172.41.3.41 CSE-4500-6 sipd[2dcc32a4] ERROR [IDS_LOG]
SigAddr[access:192.168.101.120:0=low:DENY] ttl=86400 exp=30 Demoted to BLock-
List (Too many messages) last msg rcvd=REGISTER sip:192.168.66.2 SIP/2.0
Nov 28 17:53:47 172.41.3.41 CSE-4500-6 sipd[2dcc32a4] ERROR Via: SIP/2.0/UDP
192.168.190.144:20928;branch=z9hG4bKdeadb33f
Nov 28 17:53:47 172.41.3.41 CSE-4500-6 sipd[2dcc32a4] ERROR From: hacker
<sip:47097@192.168.190.144:20928>
Nov 28 17:53:47 172.41.3.41 CSE-4500-6 sipd[2dcc32a4] ERROR To:
<sip:47097@192.168.66.2:5060>
Nov 28 17:53:47 172.41.3.41 CSE-4500-6 sipd[2dcc32a4] ERROR Call-ID:
f9844fbe7dec140ca36500a0c9119870@192.168.66.2
Nov 28 17:53:47 172.41.3.41 CSE-4500-6 sipd[2dcc32a4] ERROR CSeq: 1 REGISTER
Nov 28 17:53:47 172.41.3.41 CSE-4500-6 sipd[2dcc32a4] ERROR Contact:
<sip:47097@192.168.190.144>
Nov 28 17:53:47 172.41.3.41 CSE-4500-6 sipd[2dcc32a4] ERROR User-agent:
Flooder_script
```

```
Nov 28 17:53:47 172.41.3.41 CSE-4500-6 sipd[2dcc32a4] ERROR Max-
Forwards: 5
Nov 28 17:53:47 172.41.3.41 CSE-4500-6 sipd[2dcc32a4] ERROR Content-
Length: 0
```

An endpoint exceeded a defined constraint and was blocklisted. This message is a result of DoS configuration without the IDS license.

```
Jan 15 16:29:46.289 sipd@SBC1: FLOW[15]
SigAddr[Access:192.168.135.29:0=low:DENY] ttl=86400 guard=50 exp=30
Demoted to Block-List; send SNMP trap
```

An endpoint exceeded a defined constraint and was demoted from trusted to untrusted.

```
Apr  1 11:36:53.377 sipd@CSE-4500-6: WARNING
SigAddr[access:172.41.0.3:5060=medium:PERMIT] ttl=64 exp=57 Demoted to
Grey-List (errors)
```

The sipShield SPL plug-in (v1.3) detected a message from a known SIP scanner and dropped it.

```
Mar 28 15:05:42.500 sipd@CSE-4500-6: WARNING Scanner or attack field
detected! Src IP: 172.41.0.3, User-Agent: smap 0.6.0
OR
Mar 28 15:05:42.500 sipd@CSE-4500-6: WARNING Scanner or attack field
detected! Src IP: 172.41.0.3, To: victim@example.edu
OR
Mar 28 15:05:42.500 sipd@CSE-4500-6: WARNING Scanner or attack field
detected! Src IP: 172.41.0.3, From: user@example.edu
OR
Mar 28 15:05:42.500 sipd@CSE-4500-6: WARNING Scanner or attack field
detected! Src IP: 172.41.0.3, Subject: SiVuS
```

A message was rejected by the SD. The status code and reason given in parenthesis will change based on the type of malformation. Examples given here include:

An INVITE received from a forbidden endpoint. In this case, allow-anonymous on the SIP interface was set to agents-only, and the INVITE was not from an agent.

An INVITE had a Max-Forwards parameter that had decremented to zero, and the SBC could not forward it further

Four examples of malformed messages that were generated from a Protos attack (too large, missing header, bad request URI, unsupported URI).

```
Apr  1 11:26:27.603 sipd@CSE-4500-6: IDS[64] [IDS_LOG]INVITE from
source 172.41.0.3:5060 to dest 172.41.0.2:5060[UDP] realm=access;
From=sipp <sip:sipp@127.0.1.1:5060>;tag=10387SIPpTag001;
target=sip:service@172.41.0.2:5060 rejected!; status=403 (Forbidden)
OR
Nov 28 19:52:40 172.41.3.41 CSE-4500-6 sipd[2dcc32a4] ERROR
[IDS_LOG]INVITE from source 192.168.66.54:5060 to dest
```

```
192.168.66.2:5060[UDP] realm=access;
From="hacker"<sip:666@192.168.66.54:30000>;
target=sip:9195551212@192.168.66.2 rejected!; status=483 (Too Many Hops);
error=invalid message
OR
IDS_LOG]INVITE from source 192.168.222.1:5060 to dest
192.168.222.50:5060[UDP] realm=access; From=227
<sip:evil@127.0.1.1>;tag=227; target=sip <omitted message> rejected!;
status=513 (Message Too Big)
OR
May 22 14:40:39.033 sipd@: IDS[64] [IDS_LOG]INVITE from source
192.168.222.1:5060 to dest 192.168.222.50:5060[UDP] realm=access; From=389
<sip:evil@127.0.1.1>;tag=389; target=sip:1111@192.168.222.50 rejected!;
status=400 (Invalid/Missing Via Header)
OR
May 22 15:08:02.015 sipd@: IDS[64] [IDS_LOG]INVITE from source
192.168.222.1:5060 to dest 192.168.222.50:5060[UDP] realm=access; From=206
<sip:evil@127.0.1.1>;tag=206; target=%s%s%s%s%s:noone@sip.no.invalid
rejected!; status=400 (Bad Request-URI)
OR
May 22 15:08:01.088 sipd@: IDS[64] [IDS_LOG]INVITE from source
192.168.222.1:5060 to dest 192.168.222.50:5060[UDP] realm=access; From=197
<sip:evil@127.0.1.1>;tag=197;
target=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa:noone@sip.no.invalid rejected!;
status=416 (Unsupported URI Scheme)
```

A user entered enable mode (administrator level). This is not necessarily an issue, but may be an interesting event.

```
May  3 17:06:37 172.41.3.90 CSE-4500-20 acliConsole[31ac9b6c]  raised
privileges on session from acliConsole
```

A user enabled SIP debugging traces. This can use large amounts of CPU if run on a production network or potentially reveal sensitive information. This is not necessarily an issue, but may be an interesting event.

```
May  3 17:09:26 172.41.3.90 CSE-4500-20 sipd[2fa7cc00] SIP enable SIP
Debugging
```

The configuration file was updated. This should be investigated if changes were not authorized.

```
Dec 19 13:28:27.060 lemd@SBC1: CONFIG[32] Save Config has completed
successfully
```

A new configuration was activated. This should be investigated if changes were not authorized.

```
Dec 19 13:28:29.863 lemd@SBC1: CONFIG[32] Configuration successfully
activated
OR
Dec 19 13:28:31.864 lemd@SBC1: CONFIG[32] Activate Config Successfully
```

```
Complete
OR
Mar 20 10:11:02.919 acliSSH0@: CONFIG[34] ACTIVATE-CONFIG done
```

One or more licenses has expired and unit functionality may be impacted.

```
Apr  1 00:00:10.523 brokerd@CSE-4500-6: MINOR ALARM[00050016]
Task[0615c064] 1 license has expired!
```

One or more licenses is nearing expiration.

```
Mar 31 00:00:10.521 sysmand@CSE-4500-6: MINOR License will expire in
less than 7 days.
```

The number of sessions is approaching licensed capacity.

```
Jan  1 00:02:57.480 brokerd@SBC1: MAJOR ALARM[00050004] Task[0cf72188]
total number of sessions (1977) is approaching licensed capacity (2000)
```

The unit was powered on. This may be an indication that a power failure occurred.

```
Jan  8 11:33:06.545 bootstrap@SBC1: GENERAL[0] Bringing up box...
```

The SIP protocol stack is now active. This may be an indication that a power failure occurred or that the SIP process crashed and restarted.

```
May  3 17:30:08 172.41.3.90 CSE-4500-20 sipd[2fa7cc00] SIP Change to
In-Service state and Start accepting messages...
```

Unit CPU usage has reached a critical threshold.

```
Oct  8 19:02:02.381 brokerd@SBC1: CRITICAL ALARM[0002001b]
Task[0578324c] cpu usage 93 percent is over critical threshold of 90
percent.
```

Unit CPU usage has reached a major threshold.

```
Oct  8 19:02:12.708 brokerd@SBC1: MAJOR ALARM[0002001b] Task[0578324c]
cpu usage 87 percent is over major threshold of 80 percent.
```

Unit CPU usage has reached a minor threshold.

```
Oct  8 19:06:57.062 brokerd@SBC1: MINOR ALARM[0002001b] Task[0578324c]
cpu usage 74 percent is over minor threshold of 70 percent.
```

A high-availability switchover was detected from the active unit. If this was not an administrative failover then it is likely that a port or process was unsuccessful.

```
Dec  3 17:30:46.275 berpd@SBC1: CRITICAL ALARM[00020021] Task[2834f658]
Switchover, Active to RelinquishingActive
```

The standby unit has become the active unit. If this was not a result of an administrative action then a port or process on the active unit likely stopped responding.

```
Jan  8 11:34:41.652 berpd@SBC1: CRITICAL ALARM[00020020] Task[03c3a840]
Switchover, Standby to BecomingActive, active peer SBC2 has timed out
```

The standby unit is having difficulty reaching the active unit. Verify that all wancom ports are operational.

```
Dec  3 17:33:46.384 berpd@SBC1: CRITICAL ALARM[00020023] Task[2834f658]
Unable to synchronize with Active redundant peer within BecomingStandby
timeout, going OutOfService
```

An ethernet port used for management has stopped responding.

```
Jan  8 11:34:42.171 brokerd@SBC1: MAJOR ALARM[00020009] Task[0e723a98]
wancom1 link down
```

A ethernet port used for management has recovered from failure.

```
Jan  8 11:34:44.788 brokerd@SBC1: MINOR ALARM[00020006] Task[0e723a98]
wancom1 link up
```

An ethernet port used for services has stopped responding. Note that slot and port numbers will vary.

```
Mar 20 21:56:29.504 brokerd@: MAJOR ALARM[00020027] Task[00000003] Slot 1
Port 0 DOWN
```

All servers that can receive accounting files (CDR) are not available

```
May  3 17:20:11 172.41.3.90 CSE-4500-20 brokerd[10661b38] CRITICAL All of
collector's push receivers are down
```

Transfer of an HDR file was unsuccessful because the key used for authentication is incorrect.

```
May  3 17:20:11 172.41.3.90 CSE-4500-20 collect[2eb37454] WARNING Error: HDR
push failed due to bad host key.
```

An error occurred when attempting to transfer accounting logs.

```
Dec 31 07:47:53.192 collect@SBC1: MINOR Error pushing collected data
to 172.17.5.24 for group: system
```

Transfer of an HDR file was unsuccessful due to invalid authentication.

```
May  3 17:20:11 172.41.3.90 CSE-4500-20 collect[2eb37454] ERROR Error:
Could not log in to host '172.41.1.118
```

Media port usage is exceeding capacity. Calls may not succeed or experience audio issues. The severity is based on the percentage of unsuccessful attempts to allocate a steering port. Jan 17 12:14:26.513 mbcd@SBC1: MINOR ALARM[00040006] Task[1b963548] out of steering ports for realm 'CORE'; 296 of 592 failed (50%)

```
OR
Jan 17 12:18:14.865 mbcd@SBC1: WARNING ALARM[00040006] Task[1b963548]
out of steering ports for realm 'CORE'; 80 of 310 failed (25%)
```

A session agent (SIP server) did not pass a health check and has been taken out of service.

```
Jan 15 16:28:19.901 sipd@SBC1: SIP[13] SA 192.168.136.69[PBX1]PING
TRANSACTION TIMEOUT to 192.168.136.69
Jan 15 16:28:19.902 sipd@SBC1: SIP[13]   was 'In Service'; set to 'Out
of Service' status
```

A session agent (SIP server) did not pass a health check and has been taken out of service.

```
Jan 15 16:28:22.969 sipd@SBC1: SIP[13] SA 192.168.135.29[PBX2]Non-Ping
TRANSACTION TIMEOUT to 192.168.135.29
Jan 15 16:28:22.970 sipd@SBC1: SIP[13]   was 'In Service'; set to 'Out
of Service' status
```

There were no routes found for an incoming session. This may mean that the called destination is out of service, the destination address is incorrect, or that the routing table is not sufficient.

```
Mar 30 15:02:27.307 sipd@CSE-4500-6: IDS[64] [IDS_LOG]INVITE from
source 192.168.60.10:5061 to dest 192.168.60.2:5060[UDP] realm=core;
From=sipp <sip:sipp@127.0.0.1:5061>;tag=9165SIPpTag00143;
target=sip:service@192.168.60.2:5060 rejected!; status=480 (No Routes
Found)
```

H

Call Detail Records (CDR)

The SBC can be configured to send Accounting CDR packets to a RADIUS server [3]. This data can be trended for monitoring purposes as well as traditional billing uses. For example, determining call completion rates at various high and low points during the day. This approach requires the implementation of a RADIUS server with the release specific Oracle Radius Dictionary (available in Downloads on the support portal), and a database backend / reporting mechanism.

If RADIUS is not the desired approach, the SBC store CDRs locally and then push them to a FTP/SFTP server on a scheduled basis [3]. Since that may require more local storage, an optional Storage Expansion Module can be used to extend the storage of CDRs locally on the SBC [3].

The following is a list of useful RADIUS attributes for characterizing and troubleshooting the VoIP network:

- Acct-Session-Time (46) - Call Duration: useful for detecting abnormally short or long call hold times
- Acct-Terminate-Cause (49) & Acme-Disconnect-Cause (62)
  - Call Disconnect Cause Code: useful for detecting abnormal call failures
  - See [3] for list of causes
- RTCP & RTP QoS Statistics -The SBC can incorporate call quality measurements (QoS) in CDR and for up to two RTP/RTCP bidirectional media flows per SIP session. Each bidirectional flow is referred to as a flow-set (FS1 and FS2). QoS collection requires an NIU with QoS capabilities and a QoS measurement setting to be enabled in configuration.
  - Acme-Called-RTCP-Packets-Lost_FS1 / FS2 (46 / 104) - integer, total for call
  - Acme-Called-RTCP-Avg-Jitter_FS1 / FS2 (47 / 105) - measured in ms
  - Acme-Called-RTCP-Avg-Latency_FS1 / FS2 (48 / 106) - measured in ms
  - Acme-Called-RTCP-MaxJitter_FS1 / FS2 (49 / 107) - measured in ms
  - Acme-Called-RTCP-MaxLatency_FS1 / FS2 (50 / 108) - measured in ms
  - Acme-Called-RTP-Packets-Lost_FS1 / FS2 (51 / 109) - integer, total for call
  - Acme-Called-RTP-Avg-Jitter_FS1 / FS2 (52 / 110) - measured in ms
  - Acme-Called-RTP-MaxJitter_FS1 / FS2 (53 / 111) - measured in ms
- Acme-Post-Dial-Delay (58) - Call Setup time in ms: Detect abnormal delays between SIP INVITE and 180 Ringing
- Acme-Session-Disposition (60)
  - Status of call attempt from SIP INVITE to answered or unanswered
  - 0 = unknown, 1 = call attempt, 2 = ringing, 3 = answered
- Acme-Disconnect-Initiator (61)

- Party that disconnects the call
- 0 = unknown, 1 = calling party, 2 = called party, 3 = internal

Historical Data Records (HDR)

HDR refers to a management feature that collects statistics about SBC system operation and function, and then sends those records to a configured FTP/SFTP server [1]. This is roughly the same data available via SNMP, but collected and stored in CSV files on configured intervals, and then sent to the server on a configured period. These files can be used for capacity planning and analysis of trends or long term issues.

HDR data consists of a “Group” with associated “Group Statistics” that apply to each group. HDR data comes from two sources: SNMP MIBs and Oracle’s Command Line Interface (ACLI), i.e. the output of show commands.

For more information and details about Historical Data Recording please read the HDR Resource Guide applicable to the release on the SD.

Specific HDR groups of interest to collect are:

- system - global system statistics
- session-realm - session and rate statistics on a per realm basis
- temperature - environmental temperature statistics
- sip-sessions - SIP status statistics
- sip-errors - error statistics for SIP, media, and SDP
- sip-policy - SIP routing, session-agent groups and constraints statistics
- sip-ACL-status - statistics on trusted and blocked ACLs

The following is an example of information collected in the sip-errors HDR for one collection interval.

```
TimeStamp,Message/Event,Server Totals,Client Totals
1369336364,INVITE Requests,1200,0
1369336364,Retransmissions,0,0
1369336364,100 Trying          ,800,0
1369336364,180 Ringing         ,800,0
1369336364,181 Forwarded       ,0,0
1369336364,182 Queued          ,0,0
1369336364,183 Progress        ,0,0
1369336364,1xx Provisional     ,0,0
1369336364,200 OK              ,800,0
1369336364,202 Accepted        ,0,0
1369336364,2xx Success         ,0,0
1369336364,30x Moved           ,0,0
1369336364,305 Use Proxy       ,0,0
1369336364,380 Alternative     ,0,0
1369336364,3xx Redirect        ,0,0
1369336364,400 Bad Request     ,200,0
1369336364,401 Unauthorized    ,0,0
1369336364,403 Forbidden       ,200,0
1369336364,404 Not Found       ,0,0
```

```
1369336364,405 Not Allowed     ,0,0
1369336364,406 Not Acceptable  ,0,0
1369336364,407 Proxy Auth Req  ,0,0
1369336364,408 Request Timeout ,0,0
1369336364,415 Bad Media Type  ,0,0
1369336364,420 Bad Extension   ,0,0
1369336364,421 Extension Reqd  ,0,0
1369336364,422 Too Short       ,0,0
1369336364,423 Too Brief       ,0,0
1369336364,480 Unavailable     ,0,0
1369336364,481 Does Not Exist  ,0,0
1369336364,482 Loop Detected   ,0,0
1369336364,483 Too Many Hops   ,0,0
1369336364,484 Address Incompl ,0,0
1369336364,485 Ambiguous       ,0,0
1369336364,486 Busy Here       ,0,0
1369336364,487 Terminated      ,0,0
1369336364,488 Not Acceptable  ,0,0
1369336364,489 Bad Event       ,0,0
1369336364,491 Req Pending     ,0,0
1369336364,4xx Client Error    ,0,0
1369336364,500 Internal Error  ,0,0
1369336364,501 Not Implemented ,0,0
1369336364,502 Bad Gateway     ,0,0
1369336364,503 Service Unavail ,0,0
1369336364,504 Gateway Timeout ,0,0
1369336364,513 Msg Too Large   ,0,0
1369336364,580 Precon Failure  ,0,0
1369336364,5xx Server Error    ,0,0
1369336364,600 Busy Everywhere ,0,0
1369336364,603 Decline         ,0,0
1369336364,604 Not Found       ,0,0
1369336364,606 Not Acceptable  ,0,0
1369336364,6xx Global Error    ,0,0
1369336364,Response Retrans,0,0
1369336364,Transaction Timeouts,  -  ,0
1369336364,Locally Throttled,  -  ,0
```

J

ACLI Commands for Monitoring

Data available via HDR, SNMP, CDR, or Syslog is usually sufficient for analysis and troubleshooting. However, some ACLI show and display commands have additional data that is not available with those methods. The commands referenced here are some of the most common ones that should be used for troubleshooting and additional statistics collection (most commonly automated with a script). It should be noted that Oracle may update the fields or format used in these commands periodically as enhancements are made, so automation may not function correctly after an upgrade.

System Statistics

Below is a recommended list of ACLI commands to execute every 5 minutes on the Active SBC in addition to the SNMP OID polling (outlined in Section 0). These will provide useful data on overall system performance [2].

- display-alarms - View active alarms reported on the system
- show health - Verify active/standby system health and switchover alarms reported
- show arp - Verify all configured gateways are reachable
- show media physical - Displays statistics for media ports
- show media utilization - Percentage bandwidth utilization for each media port
- show accounting - Displays statistics for configured RADIUS servers and CDRs sent
- show acl summary - Displays statistics for system DDOS activity
- show acl info - Displays statistics for ACL usage of CAM space
- check-space-remaining [code | ramdrv] - Displays flash space available for the directories code and ramdrv

Application Statistics

Below is a recommended list of ACLI commands to execute every 5 minutes on the Active SBC in addition to the SNMP OID polling (outlined in Section 0). These will provide useful data on application performance [2].

SIP

- show registration - Verify no unexpected spikes or drops in expected number of concurrently registered endpoints
- show sip invite - Displays statistics for SIP INVITE messages received/sent by the SD. Important to monitor 4xx and 5xx response errors and retransmissions.
- show sipd agents - Displays statistics for all session-agents configured
- show sipd realms - Displays statistics for each realm
- show sipd errors - Error count related to SIP

Media

- show mbcd realms - Displays media (RTP) related information presented in a per-realm manner
- show mbcd errors - Error count related to media

H.323

- show sessions - Displays the concurrent sessions active on the system. It further details the number of sessions for an IWF scenario, as being SIP-to-H.323 and H.323-to-SIP.
- show h323 stackCallstats - Displays summary of H.323 call Stats for all stacks.
- show h323 stackDisconnectInstats - Displays summary of H.323 pvt Stats for all stacks Incoming
- show h323 stackDisconnectOutstats - Displays summary of H.323 pvt Stats for all stacks Outgoing
- show h323 stackPvtstats - Displays summary of H.323 pvt Stats for all stacks
- show h323 agentstats - Displays summary of all H.323 Session Agents

K

SRTP Configuration and Troubleshooting

The Secure Real-time Transport Protocol (SRTP) provides encryption and authentication for the call content and call signaling streams. Authentication provides assurance that packets are from the purported source, and that the packets have not been tampered with during transmission. Encryption provides assurance that the call content and associated signaling has remained private during transmission.

Real-time Transport Protocol (RTP) and Real-time Transport Control Protocol (RTCP) traffic are encrypted as described in RFC 3711: The Secure Real-time Transport Protocol (SRTP). The negotiation and establishment of keys and other cryptographic materials that support SRTP is described in RFC 4568: Session Description Protocol (SDP) Security Description for Media Streams. Cryptographic parameters are established with only a single message or in single round-trip exchange using the offer/answer model defined in RFC 3264: An Offer/Answer Model with the Session Description Protocol.

Session Description Protocol Security Descriptions for Media Streams (SDES), defined in RFC 4568, provides an alternative method for creating keys used to encrypt RTP and RTCP transactions.

This document should be used as a base reference only, outlining procedures to configure SRTP on the SBC node from its base configuration. An Oracle Systems Engineer should be consulted with regards to specific concerns as they apply to customer specific SBC configurations.

Configuration guides are available for download from https://docs.oracle.com/.

SRTP Topologies

End-to-end SRTP is supported, and the Session Border Controller (SBC) can be transparent to the SRTP key negotiation and the SRTP flow. It just adds its own IP to the media path and then relays the SRTP packets as it does with RTP flows, so in terms of functionality, RTP and SRTP caused no difference in the SBC configuration and functionality.

However, SBC also supports termination of SRTP. This includes special configuration and treatment of RTP and SRTP flows.

SRTP topologies can be reduced to three basic topologies:

Single Ended SRTP Termination	SRTP enabled on inbound interface, disabled on outbound interface (or vice versa) If SRTP is enabled for the inbound realm/interface, the SBC will handle the request according to the capabilities defined in the SRTP configuration. If there is a crypto attribute in the offer, the SBC will attempt to parse the crypto attributes and parameters in the SDP. It accepts exactly one of the offered crypto attributes for a given media stream, if this is configured as a valid crypto-suite on the SBC. If there is no crypto-suite configured on the SBC in the list of crypto-suites received, the SBC will reject the call with a “488 Not Acceptable Here” response.

	Before the request is forwarded to the callee, the SBC allocates resources, updates the SDP with proper media addresses and ports, and the original crypto attribute is removed from the SDP. Once the reply from the callee is received, SBC inserts the appropriate crypto attribute to form a new SDP, and forwards the response back to the caller. At this point, SRTP traffic is allowed between the caller and the SBC.
Back-to-back SRTP Termination	SRTP enabled on inbound interface, enabled on outbound interface. Separate crypto keys on either side. Similarly to the “Single End SRTP Termination” case above, before the request is forwarded to the callee, the SBC allocates resources and updates the SDP with proper media addresses and ports; however, at this point, the original crypto attribute is replaced with one generated by the SBC. The construction of the crypto attribute in the SDP will be based on the configuration for the outbound realm/interface. Once the reply from the callee is received, the SBC could also accept or reject the “answer” from the callee according to the configuration and the list of crypto-suites supported. If accepted, the SBC will replace the original crypto attribute from the callee with its own to form a new SDP. The new SDP is forwarded back to the caller. At this point, SRTP media sessions are established on both sides.
Pass-through SRTP	Crypto attribute is not intercepted, just forwarded, and the key negotiation is done end-to-end. If the configuration specifies “pass-through” mode, the SBC will not intercept the crypto attribute exchange between the caller and the callee. The crypto attribute will be forwarded as it is from the caller to the callee and vice versa. The SBC simply modifies media IP addresses and ports to enable media anchoring (if configured); hence SRTP flows pass transparently through the SBC.

Hardware Requirements

The Acme Packet platforms and VNF all support SRTP.

SSM is required for TLS on Acme Packet 4600, 6100, 6300, and 6350. SSM is not required for TLS on Acme Packet 1100, 3900, 3950, 4900, and VME/VNF. TLS is used for encrypting signaling, and SRTP is used for encrypting media. In this case, then the SSM module is also required to run TLS.

```
# show security ssm
SSM (Security Service Module) v3 present.
```

If UDP/TCP is used for SIP, then SSM module is not a requirement.

Design Aspects - Configuration Elements

Here is a brief explanation on the elements needed for SRTP configuration. This is just a basic reference, the configuration of each element will depend on the desired design and will be described in the following sections.

Security, media-security, sdes-profile
This is the first element to configure, where the algorithm and the cryptos to be used are configured.

For sdes-profile, it is required to define the crypto-suites accepted, and also whether or not authentication and/or encryption are used for SRTP and if encryption is used for SRTCP. The “use-ingress-session-params” attribute is used to override previous parameters, specifying that the SBC will accept encryption/no-encryption, authentication/no-authentication in SRTP/SRTCP, using in the egress SDP the same session parameter that was received in the ingress SDP.

Finally “egress-offer-format” is used to instruct the SBC on how to build the egress SDP in the case of both RTP and SRTP are supported at the same time. This is further explained in the next section.

```
# show running-config sdes-profile
sdes-profile
    name                sdes1
    crypto-list                 AES_CM_128_HMAC_SHA1_80
AES_CM_128_HMAC_SHA1_32
    srtp-auth                   enabled
    srtp-encrypt                enabled
    srtcp-encrypt               enabled
    egress-offer-format          same-as-ingress
    use-ingress-session-params     srtcp-encrypt
                                    srtp-auth
                                      srtp-encrypt
    mki                         disabled
    key
    salt
```

Security, media-security, media-sec-policy
Media-sec-policy instructs the SBC how to handle the SDP received/sent under a realm (RTP, SRTP or any of them) and, if SRTP needs to be used, the sdes-profile that needs to be used.

The media-sec-policy should be assigned to a realm under the realm-config configuration.

```
(media-sec-policy)# show
media-sec-policy
        name                            msp1
        pass-through                    disabled
        inbound
                profile                         sdes1
                mode                            srtp
                protocol                        sdes
        outbound
                profile                         sdes1
                mode                            srtp
                protocol                        sdes
```

Design Considerations

The intents of the design considerations explained here are to:

- Minimize interoperability issues by standardizing field configurations
- Provide guidelines for new users to the Session Border Controller
- Document when and why configuration elements should be changed from their default values
- Facilitate transition of customers from Systems Engineering to Technical Support by making configurations consistent (yielding predictable behavior)

Further, each design considers the following aspects:

- Flexibility: how resilient the configuration is, and how adaptable the configuration is (i.e. when turning up new connected networks)
- Scalability: minimizing redundant configuration objects and setting a templated foundation to allow overlay configuration with minimal disruption
- Compatibility: working with other popular devices in carriers' VoIP networks

The main aspects treated here focused on which traffic is desired under a realm, so each design needs to consider the following, previous to any configuration:

1. SIP Traffic: SIP over UDP/TCP (unsecured transport) or over TLS (secured transport protocol).
2. Media Traffic: media over RTP, media over SRTP or media over both RTP and SRTP allowed at the same time. This would differentiate the IP design, since:
    a. For media over RTP only or SRTP only, just one IP address will be used for them
    b. For media over both RTP/SRTP allowed at the same time, then the recommendation is to use two different IPs on the same network-interface. One will send RTP traffic and the other IP will be used for SRTP traffic. This should be considered for correct IP plan under the network.

Secured/Unsecured Network - By default, the SBC considers that SIP traffic, when SRTP is configured, should run over secured transport protocol, TLS. If this is not the case, the SBC needs to be instructed to allow SIP traffic over non-secured transport protocol (UDP/TCP).

```
sip-interface
        state                           enabled
        realm-id                        access1
        description
        sip-port
                address                         11.0.0.11
                port                            5060
                transport-protocol              UDP
                tls-profile
                allow-anonymous                 all
                ims-aka-profile
        carriers
…
        secured-network                 enabled
```

When secured-network is set to DISABLED under a sip-interface where SRTP is configured, the sip-interface will only allow SIP over TLS. If SIP is received over UDP/TCP, the SBC will reject the call with "488 Not Acceptable Here".

When secured-network is set to ENABLED, the SBC understands the network is secured and it accepts SIP traffic on UDP/TCP.

Media traffic - Every realm under the configuration should be instructed to the type of media that should handle whether that be RTP only, SRTP only or both RTP and SRTP. For each realm, it can be differentiated between the inbound and outbound media type, giving the flexibility of having different protocols for inbound or for outbound.

The “mode” parameter under the media-sec-policy controls the media protocol defined for each inbound/outbound flow under a realm.

- RTP Only

The “mode” parameter under the inbound/outbound section of the media-sec-policy should be set to RTP. In this case, no profile should be defined, and the protocol should be set to “None”.

```
(media-sec-policy)# show
media-sec-policy
        name                            removeCrypto
        pass-through                    disabled
        inbound
                profile
                mode                            rtp
                protocol                        none
        outbound
                profile
                mode                            rtp
                protocol                        none
```

This is mostly used in single ended SRTP termination configurations, where this media-sec-policy removes the SRTP component part from the SDP to offer/accept only SRTP. This media-sec-policy should be applied under the realm where only RTP is desired.

```
realm-config
        identifier                      backbone
        description
        addr-prefix                     0.0.0.0
        network-interfaces
                                        M10:0
…
        media-sec-policy                removeCrypto
```

In the case of RTP only, no sdes-profile and no security-policy are needed.

- SRTP Only

The “mode” parameter under the media-sec-policy should be set to SRTP. The “profile” parameter should be set to the configured sdes-profile, and the protocol should be set to SDES.

In this case, only SRTP is accepted in the realm. An INVITE arriving to the realm without SRTP capabilities is rejected by the SBC with a “488 Not Acceptable Here”.

```
(media-sec-policy)# show
media-sec-policy
```

```
        name                            SRTP1
        pass-through                    disabled
        inbound
                profile                         sdes1
                mode                            srtp
                protocol                        SDES
        outbound
                profile                         sdes1
                mode                            srtp
                protocol                        SDES
```

Where “sdes1” is the configured sdes-profile used for this implementation. Here are the default sdes-profile suggested, to be superseded only by specific customer requirements.

```
# show running-config sdes-profile
sdes-profile
    name               sdes1
    crypto-list                AES_CM_128_HMAC_SHA1_80
AES_CM_128_HMAC_SHA1_32
    srtp-auth                  enabled
    srtp-encrypt               enabled
    srtcp-encrypt              enabled
    egress-offer-format         same-as-ingress
    use-ingress-session-params     srtcp-encrypt
                                    srtp-auth
                                      srtp-encrypt
    mki                        disabled
    key
    salt
```

The media-sec-profile configured for SRTP should be applied under the desired realm.

```
realm-config
        identifier                      access1
        description
        addr-prefix                     0.0.0.0
        network-interfaces              M00:0
        …
        media-sec-policy                SRTP1
```

The local-port-match is set to 0 for an SRTP security-policy, meaning all ports on the IP address configured in local-ip-match are subject to this security-policy. Hence, to avoid a clash with the SIP signaling port (typically 5060) when signaling and media are managed on the same IP address, a second security-policy with a higher priority is required to exempt the SIP signaling port from the media security-policy.

Note that in the case where the SIP traffic runs on a different IP/Subnet from media, then this second security-policy for SIP signaling is not required.

- Both RTP/SRTP support

The “mode” under the media-sec-policy should be set to ANY. Also, the profile should be configured with the sdes-profile that would be used in case of SRTP and the protocol should be set to SDES, depending on which protocol is required.

When inbound mode=any, the SBC will accept SDP with only RTP description, SDP with only SRTP description and SDP with 2 m lines having both RTP and SRTP description.

When outbound mode=any, the SBC will insert an SDP with only RTP, only SRTP or with 2 m lines, supporting both RTP and SRTP, this is controlled under the sdes-profile:

```
(sdes-profile)# egress-offer-format

<enumeration> format of offer SDP in 'any' mode
              {same-as-ingress | simultaneous-best-effort}
```

- Same-as-ingress: The SBC will use to build the egress SDP offer the mode received in the ingress realm. So if the SBC received only RTP in the ingress realm, it will insert only RTP in the egress SDP, and if it received only SRTP in the ingress SDP, it will set the egress SDP to only SRTP.
- Simultaneous-best-effort: The SBC will insert additional SRTP description in the SDP if the ingress SDP contained only RTP and vice-versa, so the resultant SDP should contain both RTP and SRTP media profiles contained in 2 different media lines in the SDP.

```
# show running-config sdes-profile
sdes-profile
    name                sdes1
    crypto-list                 AES_CM_128_HMAC_SHA1_80
AES_CM_128_HMAC_SHA1_32
    srtp-auth                   enabled
    srtp-encrypt                enabled
    srtcp-encrypt               enabled
    egress-offer-format          same-as-ingress
    use-ingress-session-params     srtcp-encrypt
                                    srtp-auth
                                      srtp-encrypt
    mki                         disabled
    key
    salt


(media-sec-policy)# show
media-sec-policy
        name                            SRTP1
        pass-through                    disabled
        inbound
                profile                         sdes1
                mode                            any
                protocol                        SDES
        outbound
                profile                         sdes1
                mode                            any
                protocol                        SDES
(media-sec-policy)#
```

And this media-sec-policy should be applied under the realm where RTP+SRTP are desired:

```
realm-config
        identifier                      access1
        description
        addr-prefix                     0.0.0.0
        network-interfaces
                                        M00:0
…
        media-sec-policy                SRTP1
```

The SRTP IP must be in the same subnet (network-interface) as the IP used for RTP. For its definition, the IP used for RTP will continue being defined under the steering-pool. When RTP needs to be used, the SBC will use the IP configured in the steering-pool, whereas when SRTP needs to be inserted into the SDP, the SBC will choose the IP from the security-policy AND an available port from the steering-pool configured for RTP, so the dimensioning of the port range of the steering-pool should consider both RTP and SRTP estimated traffic.

If SIP traffic runs over the same subnet (network-interface), it is recommended not to use the IP used for SRTP traffic. That way, it is not necessary to configure a second security-policy for SIP traffic.

In the example below, 11.0.0.10 is used for RTP and 11.0.0.11 is used for SRTP. In the case that SIP traffic is desired under the same network, it would be recommended not to use 11.0.0.11, as this is reserved for SRTP use and the security-policy configured for it would apply.

```
steering-pool
        ip-address                      11.0.0.10
        start-port                      20000
        end-port                        49999
        realm-id                        access
```

High Availability

In order for SIP and SRTP to work properly in the HA environment, the sip-config element should be configured.

```
sip-config
        … …
        red-sip-port                    1988
        red-max-trans                   10000
        red-sync-start-time             5000
        red-sync-comp-time              1000
```

Notes on the Reference Configuration

The intention of this document is not to provide a full set of configurations, as the flexibility of the SRTP configuration makes valid a high number of different possible configurations. The objective is to present some common and valid configurations that have been tested and verified in Oracle labs.

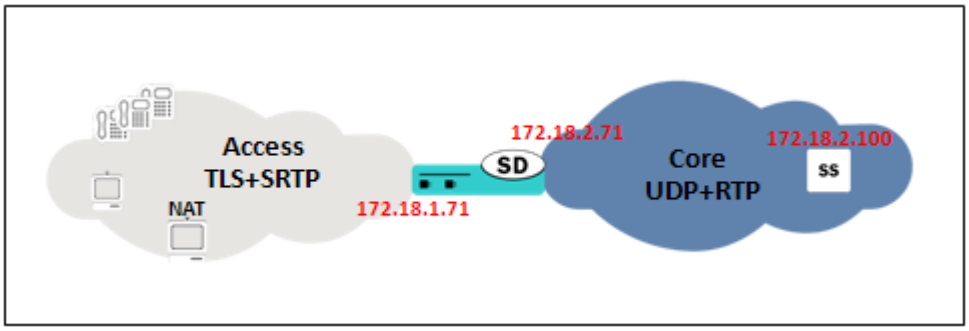
In the cases considered here, there is a considered “access” or “peer1A” network, in the 172.18.1.0/24 network, and a considered “core” or “peer1B” in the 172.18.2.0/24 network. In all cases SIP and media traffic runs on the same subnets.

To simplify the use of this information, no other elements are configured in this case, so no redundancy or DDoS prevention are configured in the configurations exposed. The configurations follow the guides of BCP for access (using policy based realm bridging) and peering scenarios. For TLS, it is assumed single-side authentication in all cases.

The configurations presented use SDES mechanism for SRTP encryption. No SRTP pass-through cases are presented here, as there is nothing required for the SBC to be transparent to the SRTP negotiation end-to-end.

Single-Ended SRTP Termination on secured networks.

This is the typical access scenario where SRTP is deployed completely in the access network, allowing the users to use TLS for SIP and SRTP for media. In the core network, UDP is used for SIP and RTP is used for media.



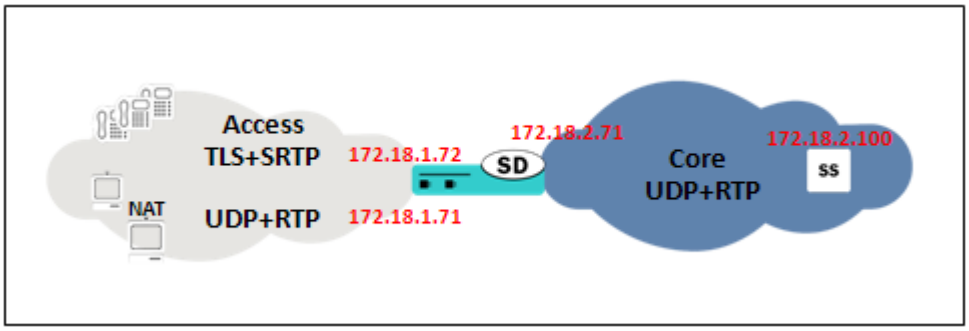
The IP used for SIP and SRTP in the SBC in the access network is 172.18.1.71, and the IP used for SIP and RTP in the core network is 172.18.2.71. The SIP Registrar/Proxy in the core network is in 172.18.2.100.

In this case, secured-network is set to DISABLED under the access sip-interface and ENABLED on the core sip-interface. Two security-policies are configured, one for SRTP and one that creates the exception for SIP signaling. Also, two media-sec-policies are created, one in the access network with mode=SRTP and one in the core with mode=RTP.

RTP and Single-Ended SRTP Termination on unsecured networks.

This is a very common architecture, where both RTP and SRTP endpoints reside in the access network, especially while in transition from RTP to SRTP. This means that both UDP/RTP and TLS/SRTP can be present in the access network. In the core network, UDP for SIP and RTP for media will be used.

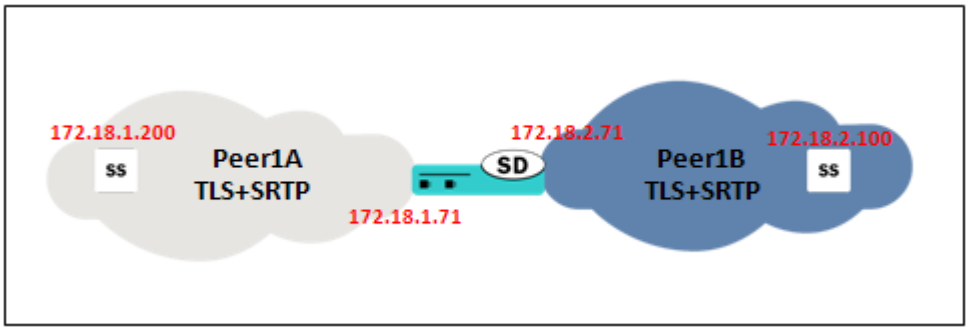
In this case, in the access network we will use 172.18.1.71 for SIP traffic (UDP and TLS) and also for RTP traffic. 172.18.1.72 will be used for SRTP traffic. In the core network, 172.18.2.71 will be used for SIP and RTP. The SIP Proxy/Registrar uses 172.18.2.100.



Secured-network parameter is set to ENABLED under the access sip-interface and ENABLED on the core sip-interface. Only one security-policy is configured for SRTP under 172.181.72. Two media-sec-policies are created, one in the access network with mode=any and one in the core with mode=RTP. As in the access network both RTP and SRTP endpoints could be present, the egress-offer-format is set to simultaneous-best-effort.

Back-to-back SRTP Termination

Normally deployed in peering scenarios where SRTP is needed in both networks that the SBC is interconnecting. In that case, the Session Border Controller is doing SRTP termination so the SRTP key exchange is different in the two connected networks.



In the SBC, 172.18.1.71 will be used for SIP (TLS) and SRTP in the peer1A network, while 172.18.2.71 will be used in the 172.18.2.71.

The peer element sending traffic in the peer1A network will be in 172.18.1.200, while the peer element in the peer1B will be 172.18.2.100.

Secured-network is set to DISABLED under both sip-interfaces. Two security-policies are configured per peer1 realm, one for SRTP and one that creates the exception for SIP signaling, so four security-policies are configured in total. Also, two media-sec-policies are created, one in the peer1A network with mode=SRTP and one in the peer1B with mode=SRTP, where each one is linked with a different SDES profile, to allow different cryptos between networks. Note that this is not required, and the same SDES profile could be used for both networks, the key exchange would keep different as the SBC would terminate the SRTP anyway, so configuring different SDES profiles would be only needed in the case where the crypto-suites supported in each network are different or have different characteristics.

Troubleshooting

A network capture taken on both access and core network should show RTP packets with the same sequence number, however, if SRTP termination is done in the SBC, the

payload contained in RTP packets with the same sequence number will be different because of the encryption/unencryption done by the SD.

Show security srtp commands show the security association created for SRTP encryption and its detailed information. `show security srtp <network_interface> debug/brief/detail/raw`

> **Note:**
>
> there is a warning when these commands want to be run, as it should be done carefully in production systems:
>
> ```
> WARNING: This action might affect system performance and take a long
> time to finish.
> Are you sure [y/n]?:
> ```

- Show security srtp status <network_interface>
- Show security spd <network_interface>

```
# show security srtp sad M00 debug
WARNING: This action might affect system performance and take a long time to
finish.
Are you sure [y/n]?: y
SRTP security-association-database for interface 'M00':
Displaying SA's that match the following criteria -
direction                 : both
src-addr-prefix           : any
src-port                  : any
dst-addr-prefix           : any
dst-port                  : any
trans-proto               : ALL
Inbound:
destination-address       : 62.2.139.213
destination-port          : 10012
vlan-id                   : 0
sal-index                 : 2
sad-index                 : 10
ssrc                      : 1514612894
encr-algo                 : aes-128-ctr
auth-algo                 : hmac-sha1
auth-tag-length           : 80
flags -
ms:  5489040, ls:        8
mtu                        : 1500
mki                        : 0
mki length                 : 0
lifetime byte count -
ms: 0x       0, ls: 0x       0
packet count -
ms: 0x       0, ls: 0x     12F
roll over count           : 0
```

```
anti replay highest seq num : 11814
highest seq num           : 0
auth error count          : 0
anti replay count         : 0
mki mismatch count        : 0
ssrc mismatch count       : 1


# show security srtp sad M00 raw
WARNING: This action might affect system performance and take a long
time to finish.
Are you sure [y/n]?: y
SRTP security-association-database for interface 'M00':
Displaying SA's that match the following criteria -
    direction                 : both
    src-addr-prefix           : any
    src-port                  : any
    dst-addr-prefix           : any
    dst-port                  : any
    trans-proto               : ALL
Inbound:
 Index I                                VLN    P   <-- Masks -->
SAD  Next
         TP  Dest. IP Address    SPI    Pr  ID TS P V Pr VLN TS P V
Index Link
 0000a 0 01 00000000 00000000 00000000 11 000 00 0 0 ff 000 00 0 0
0000a 00000
            00000000 d58b023e
 Index Flags MS Flags LS EX Flg  MTU SSRC     MKI      MKI Len  ROC
 0000a 05489040 00000008 00202a 05dc 5a47289e 00000000 00000000
00000000
       Primary key:  f6 8e c5 af 6c af 96 72 64 78 04 97 14 44 c1 a9
       Primary salt: 59 da 31 4d c2 3d 15 ca b6 3b 39 e1 27 2d
       E-IV:        59 da 31 4d 98 7a 3d 54 b6 3b 39 e1 27 2d 00 00
       HMAC ipad:   7a cc 93 f9 72 44 2d df ee df cc 89 3d a2 35 74 18
32 bb 25
       HMAC opad:   2b 6d cc 43 49 fa 65 8e 4a d2 03 50 90 00 9f 10 16
6d 1a 90
       Sequence Number   Anti-replay window (128 bits wide)
       00002f68          ffffffff ffffffff ffffffff ffffffff secondary
       Life Byte Count  Packet Count     Auth Err Anti-replay Err
       0000000000000000 0000000000000271 00000000 00000000
       ICV Len HSN      MKI Mismatch SSRC Mismatch
       04      00000000 00000000     00000001
```

Log.secured provides logs of the security-association activities related to SRTP.

Enhanced Traffic Controller (ETC) NIU support

The ETC NIU supports only the SDES protocol for SRTP. The configuration element “security-policy” is no longer required for SRTP using the ETC NIU. AES_CM_128 encryption and HMAC_SHA1_80 or HMAC_SHA1_32 authentication suites are supported on the ETC NIU. ARIA Cipher suite are also supported.

The ETC NIU contains one Cavium hardware chip that provides encryption/decryption. In order to support 10,000 concurrent sessions and overcome the 1 GB bandwidth limitation per port, a major design goal is to split the traffic between any 2 ports on ingress and remaining 2 ports on egress. Upon reaching 10,000 concurrent sessions limit, subsequent calls will be rejected.

Following is the list of commands to be used in order to get SRTP and ETC specific information.

show nat flow-info srtp statistics will show the global statistics for all SRTP flows.

```
SBASNQ06# show nat flow-info srtp statistics
PPM_ID_SRTP_E:
PPX Global Statistics
---------------------
        alloc_count              : 50
        dealloc_count            : 16
        input-packets            : 0
        output-packets           : 0
        sessions-count           : 2
        init-requests            : 4
        init-success             : 4
        init-fail                : 0
        modify-requests          : 0
        modify-success           : 0
        modify-fail              : 0
        delete-requests          : 2
        delete-success           : 2
        delete-fail              : 0
        query-requests           : 0
        query-success            : 0
        query-fail               : 0
        resources-error          : 0
        protect-fail             : 0
        unprotect-fail           : 0
        status-err               : 0
        bad-param                : 0
        alloc-fail               : 0
        dealloc-fail             : 0
        terminus                 : 0
        auth-fail                : 0
        cipher-fail              : 0
        replay-fail              : 0
        replay-old               : 0
        algo-fail                : 0
        no-such-op               : 0
        no-ctx                   : 0
        cant-check               : 0
        key-expired              : 0
        nonce-bad                : 0
        read-failed              : 0
        write-failed             : 0
        parse-err                : 0
        encode-err               : 0
        pfkey-err                : 0
        mki-changed              : 0
```

```
        srtp-pkt-too-small        : 0
        srtcp-pkt-too-small       : 0

PPM_ID_SRTP_D:
PPX Global Statistics
---------------------
        alloc_count               : 50
        dealloc_count             : 16
        input-packets             : 0
        output-packets            : 0
        sessions-count            : 3
        init-requests             : 2
        init-success              : 2
        init-fail                 : 0
        modify-requests           : 1
        modify-success            : 1
        modify-fail               : 0
        delete-requests           : 0
        delete-success            : 0
        delete-fail               : 0
        query-requests            : 0
        query-success             : 0
        query-fail                : 0
        resources-error           : 0
        protect-fail              : 0
        unprotect-fail            : 0
        status-err                : 0
        bad-param                 : 0
        alloc-fail                : 0
        dealloc-fail              : 0
        terminus                  : 0
        auth-fail                 : 0
        cipher-fail               : 0
        replay-fail               : 0
        replay-old                : 0
        algo-fail                 : 0
        no-such-op                : 0
        no-ctx                    : 0
        cant-check                : 0
        key-expired               : 0
        nonce-bad                 : 0
        read-failed               : 0
        write-failed              : 0
        parse-err                 : 0
        encode-err                : 0
        pfkey-err                 : 0
        mki-changed               : 0
        srtp-pkt-too-small        : 0
        srtcp-pkt-too-small       : 0

show nat flow-info srtp by-addr 3.0.0.2 all
This command will show the crypto information details for a flow with
the given   source address. If “all” is used, the details for all the
SRTP flows will be displayed. However, “all” does not to display the
statistics from the octeon srtp code.
```

```
SBASNQ06# show nat flow-info srtp by-addr 3.0.0.2 all

Crypto Parameters 3.0.0.2:7001 -> 7.0.0.2:6058
==================

        Collapsed                : false
        SRTCP Only               : false
Crypto In
------------------
        destination-address      : 208.54.47.80
        destination-port         : 40000
        vlan-id                  : 632
        encr-algo                : aes-128-ctr
        auth-algo                : hmac-sha1
        auth-tag-length          : 32
                key index                : 0
                mki                      : none
                roll-over-count          : 0


---No Crypto Out---

PPM_ID_SRTP_D
PPX Statistics
--------------
Stream #1
        ssrc                     : 3879260980
        rtp-cipher-id            : AES-128-ICM
        rtp-auth-id              : HMAC-SHA1
        rtp-security-level       : Crypto + Auth
        rtp-total-packets        : 5423
        rtp-total-bytes          : 954448
        rtp-cipher-bytes         : 867680
        rtp-auth-bytes           : 932756
        rtcp-cipher-id           : AES-128-ICM
        rtcp-auth-id             : HMAC-SHA1
        rtcp-security-level      : Crypto + Auth
        rtcp-total-packets       : 0
        rtcp-total-bytes         : 0
        rtcp-cipher-bytes        : 0
        rtcp-auth-bytes          : 0
        key-lifetime             : 42949672954294961871
        direction                : Receiver

Crypto Parameters 3.0.0.2:7001 -> 7.0.0.2:6058
==================

        Collapsed                : false
        SRTCP Only               : true
Crypto In
------------------
        destination-address      : 208.54.47.80
        destination-port         : 40000
        vlan-id                  : 632
        encr-algo                : aes-128-ctr
```

```
        auth-algo                : hmac-sha1
        auth-tag-length          : 32
                key index                : 0
                mki                      : none
                roll-over-count          : 0


---No Crypto Out---

PPM_ID_SRTP_D
PPX Statistics
--------------
Stream #1
        ssrc                     : 0
        rtp-cipher-id            : NULL
        rtp-auth-id              : NULL
        rtp-security-level       : None
        rtp-total-packets        : 0
        rtp-total-bytes          : 0
        rtp-cipher-bytes         : 0
        rtp-auth-bytes           : 0
        rtcp-cipher-id           : NULL
        rtcp-auth-id             : NULL
        rtcp-security-level      : None
        rtcp-total-packets       : 0
        rtcp-total-bytes         : 0
        rtcp-cipher-bytes        : 0
        rtcp-auth-bytes          : 0
        key-lifetime             : 0
        direction                : Unknown

show mbcd errors
This command will show counters for SRTP errors, including SRTP Flow
Add Failed, SRTP Flow Delete Failed, and SRTP Flow Update Failed.
SBASNQ06# show mbcd errors
22:29:33-160
MBC Errors/Events              ---- Lifetime ----
                        Recent      Total   PerMax
Client Errors                0          0        0
Client IPC Errors            0          0        0
Open Streams Failed          0          0        0
Drop Streams Failed          0          0        0
Exp Flow Events              1          1        1
Exp Flow Not Found           0          0        0
Transaction Timeouts         0          0        0

Server Errors                0          0        0
Server IPC Errors            0          0        0
Flow Add Failed              0          2        2
Flow Delete Failed           0          0        0
Flow Update Failed           0          0        0
Flow Latch Failed            0          0        0
Pending Flow Expired         0          0        0
ARP Wait Errors              0          0        0
Exp CAM Not Found            0          0        0
```

```
Drop Unknown Exp Flow        0          0       0
Drop/Exp Flow Missing        0          0       0
Exp Notify Failed            0          0       0
Unacknowledged Notify        0          0       0
Invalid Realm                0          0       0
No Ports Available           0          0       0
Insufficient Bandwidth       0          0       0
Stale Ports Reclaimed        0          0       0
Stale Flows Replaced         0          0       0
Telephone Events Gen         0          0       0
Pipe Alloc Errors            0          0       0
Pipe Write Errors            0          0       0
Not Found In Flows           0          0       0
SRTP Flow Add Failed         0          0       0
SRTP Flow Delete Faile       0          0       0
SRTP Flow Update Faile       0          0       0
SRTP Capacity Exceeded       0          0       0
```

show mbcd statistics
This command will show counters for number of active SRTP/SRTCP flows, as well as the number of SRTP Sessions maintained.

```
SBASNQ06# show mbcd statistics
22:29:40-168
MBCD Status                -- Period -- -------- Lifetime --------
                  Active     High   Total      Total   PerMax     High
Client Sessions        1        1       1          1        1        1
Client Trans           0        1       3          3        3        1
Contexts               3        3       2          3        2        3
Flows                 14       14       3         14       11       14
Flow-Port              2        2       2          2        2        2
Flow-NAT              13       13       5         16       11       13
Flow-RTCP              2        2       4          4        4        2
Flow-Hairpin           0        0       0          0        0        0
Flow-Released          0        0       0          0        0        0
MSM-Release            0        0       0          0        0        0
Rel-Port               0        0       0          0        0        0
Rel-Hairpin            0        0       0          0        0        0
NAT Entries           15       15       9         20       11       15
Free Ports         80000    80004       0      80004    80004    80004
Used Ports             4        4       4          4        4        4
Port Sorts             -        -       0          0        0
Queued Notify          0        0       0          0        0        0
MBC Trans              0        3       3          3        3        3
MBC Ignored            -        -       0          0        0
ARP Trans              0        0       0          0        0        0
Relatch NAT            0        0       0          0        0        0
Relatch RTCP           0        0       0          0        0        0
SRTP Only Flows        1        1       3          3        3        1
SRTCP Only Flow        3        3       3          3        3        3
SRTP Collapsed         0        0       0          0        0        0
SRTP Sessions          1        1       3          3        3        1

Flow Rate = 0.0
Load Rate = 0.0
```

```
show mbcd all
This command will show counters for number of active SRTP/SRTCP flows,
as well as the number of SRTP Sessions maintained.
SBASNQ06# show mbcd all
22:29:44-172
MBCD Status                -- Period -- -------- Lifetime --------
                  Active    High   Total      Total  PerMax    High
Client Sessions        1       1       1          1       1       1
Client Trans           0       1       3          3       3       1
Contexts               3       3       2          3       2       3
Flows                 14      14       3         14      11      14
Flow-Port              2       2       2          2       2       2
Flow-NAT              13      13       5         16      11      13
Flow-RTCP              2       2       4          4       4       2
Flow-Hairpin           0       0       0          0       0       0
Flow-Released          0       0       0          0       0       0
MSM-Release            0       0       0          0       0       0
Rel-Port               0       0       0          0       0       0
Rel-Hairpin            0       0       0          0       0       0
NAT Entries           15      15       9         20      11      15
Free Ports         80000   80004       0      80004   80004   80004
Used Ports             4       4       4          4       4       4
Port Sorts             -       -       0          0       0
Queued Notify          0       0       0          0       0       0
MBC Trans              0       3       3          3       3       3
MBC Ignored            -       -       0          0       0
ARP Trans              0       0       0          0       0       0
Relatch NAT            0       0       0          0       0       0
Relatch RTCP           0       0       0          0       0       0
SRTP Only Flows        1       1       3          3       3       1
SRTCP Only Flow        3       3       3          3       3       3
SRTP Collapsed         0       0       0          0       0       0
SRTP Sessions          1       1       3          3       3       1

Flow Rate = 0.0
Load Rate = 0.0
22:29:44-172
NAT Entries              ---- Lifetime ----
                  Recent      Total  PerMax
Adds                   9         20      11
Deletes                4          5       4
Updates                2          2       2
Non-Starts             0          0       0
Stops                  0          0       0
Timeouts               0          0       0
22:29:44-172
ACL Entries                -- Period -- -------- Lifetime --------
                  Active    High   Total      Total  PerMax    High
Static Trusted         4       4       0          4       4       4
Static Blocked         4       4       0          4       4       4
Dynamic Trusted        1       1       1          1       1       1
Dynamic Blocked        0       0       0          0       0       0

ACL Operations           ---- Lifetime ----
                  Recent      Total  PerMax
```

```
App Requests          1          2       1
Added                 1          9       8
Removed               0          1       1
Dropped               0          0       0
22:29:44-172
MBC Errors/Events                ---- Lifetime ----
                        Recent      Total   PerMax
Client Errors                0          0       0
Client IPC Errors            0          0       0
Open Streams Failed          0          0       0
Drop Streams Failed          0          0       0
Exp Flow Events              1          1       1
Exp Flow Not Found           0          0       0
Transaction Timeouts         0          0       0

Server Errors                0          0       0
Server IPC Errors            0          0       0
Flow Add Failed              0          2       2
Flow Delete Failed           0          0       0
Flow Update Failed           0          0       0
Flow Latch Failed            0          0       0
Pending Flow Expired         0          0       0
ARP Wait Errors              0          0       0
Exp CAM Not Found            0          0       0
Drop Unknown Exp Flow        0          0       0
Drop/Exp Flow Missing        0          0       0
Exp Notify Failed            0          0       0
Unacknowledged Notify        0          0       0
Invalid Realm                0          0       0
No Ports Available           0          0       0
Insufficient Bandwidth       0          0       0
Stale Ports Reclaimed        0          0       0
Stale Flows Replaced         0          0       0
Telephone Events Gen         0          0       0
Pipe Alloc Errors            0          0       0
Pipe Write Errors            0          0       0
Not Found In Flows           0          0       0
SRTP Flow Add Failed         0          0       0
SRTP Flow Delete Faile       0          0       0
SRTP Flow Update Faile       0          0       0
SRTP Capacity Exceeded       0          0       0
22:29:44-172
                                 ---- Lifetime ----
                        Recent      Total   PerMax
Add incoming:
 Request received            1          1       1
 Duplicates received         0          0       0
 Replies sent                1          1       1
 Errors sent                 0          0       0
Add outgoing:
 Requests sent               1          1       1
 Req retransmissions         0          0       0
 Replies received            1          1       1
 Errors received             0          0       0
```

```
Avg Latency=0.000 for 1
Max Latency=0.000
22:29:44-172
SRTP Flows              ---- Lifetime ----
                Recent      Total   PerMax
Adds                 3          3        3
Deletes              2          2        2
Updates              0          0        0
---< NO DATA AVAILABLE >----(Subtract)
22:29:45-172
                             ---- Lifetime ----
                       Recent      Total   PerMax
Notify incoming:
 Request received           1          1        1
 Duplicates received        0          0        0
 Replies sent               1          1        1
 Errors sent                0          0        0
Notify outgoing:
 Requests sent              1          1        1
 Req retransmissions        0          0        0
 Replies received           1          1        1
 Errors received            0          0        0

Avg Latency=0.000 for 1
Max Latency=0.000
---< NO DATA AVAILABLE >----(Other)
---< NO DATA AVAILABLE >----(Unknown)

show sipd errors
This command will show the counter for number of SIP sessions that
failed to setup due to problems related to SRTP signaling.
SBASNQ06# show sipd errors
22:29:50-178
SIP Errors/Events            ---- Lifetime ----
                      Recent      Total   PerMax
SDP Offer Errors           0          0        0
SDP Answer Errors          0          0        0
Drop Media Errors          0          0        0
Transaction Errors         0          0        0
Application Errors         0          0        0
Media Exp Events           0          0        0
Early Media Exps           0          0        0
Exp Media Drops            0          0        0
Expired Sessions           0          0        0
Multiple OK Drops          0          0        0
Multiple OK Terms          0          0        0
Media Failure Drops        0          0        0
Non-ACK 2xx Drops          0          0        0
Invalid Requests           0          0        0
Invalid Responses          0          0        0
Invalid Messages           0          0        0
CAC Session Drop           0          0        0
Nsep User Exceeded         0          0        0
Nsep SA   Exceeded         0          0        0
CAC BW Drop                0          0        0
```

```
SRTP Errors                0          0       0

show security srtp sessions
This command will be used to show the active srtp/srtcp sessions and the
total allowed capacity of 10,000 sessions.
SBASNQ06# show security srtp sessions
Capacity=10000
SRTP Sessions       -- Period -- ---- Lifetime ----
  Active    High   Total  Recent      Total  PerMax
       1       1       3          3       3       1

show nat flow-info all
This command will also show the crypto information for the SRTP flows. This
should not be executed in a production environment, since it dumps
information about all the flows.
SBASNQ06# show nat flow-info all
Output curtailed due to size.
. . . . . continued

-----------------------------------------------
SA_flow_key       : 7.0.0.2               SA_prefix : 32
DA_flow_key       : 10.176.28.218         DA_prefix : 32
SP_flow_key       : 6058                  SP_prefix : 16
DP_flow_key       : 40000                 DP_prefix : 16
VLAN_flow_key     : 980
Protocol_flow_key : 17
Ingress_flow_key  : 1
Ingress Slot      : 1
Ingress Port      : 0
NAT IP Flow Type  : IPv4 to IPv4
XSA_data_entry    : 208.54.47.80
XDA_data_entry    : 3.0.0.2
XSP_data_entry    : 40000
XDP_data_entry    : 7001
Egress_data_entry : 0
Egress Slot       : 0
Egress Port       : 0
flow_action       : 0X1
optional_data     : 0
FPGA_handle       : 0x000000c1
assoc_FPGA_handle : 0x00000000
VLAN_data_entry   : 632
host_table_index  : 6
Switch ID         : 0x00000005
average-rate      : 0
weight            : 0x0
init_flow_guard   : 300
inact_flow_guard  : 300
max_flow_guard    : 86400
payload_type_2833 : 0
index_2833        : 0
pt_2833_egress    : 0
qos_vq_enabled    : 0
codec_type        : 0
HMU_handle        : 0
```

```
SRTP Crypto In    : NONE
SRTP Crypto Out   : AES_CM_128_HMAC_SHA1_32
-----------------------------------------------

    Input Link Parameters -  IFD Index: 0x5
    -------------------------------------------
                IFD Byte Enable: false
                EPD Mode Enable: true
                         Retain: false
                       ABJ Mode: true
                  Disable Empty: false
                Ignore On Empty: false
                           TGID: 0x6
                          WRGID: 0x0
                     TG Enable: true
                    WRG Enable: false

    Output Link Parameters -  OFD Index: 0x5
    --------------------------------------------
                    shaped_flow: false
               latency_sensitive: false
                        pkt_mode: Packet Mode
              zero_min_credit_flow: false
                   parent_pipe_num: 0x1
                             delta: 0x1
             flow_credit_min_exp: 0x0
             flow_credit_min_man: 0x0

IFD 0x00000005:       dropCount = 0x00000000


IFD 0x00000005:       acceptCount = 0x00001f35

-----------------------------------------------

dump-np-stats
```

Increase SSRC changes allowed in a SRTP stream

By default, SBC allows only seven SSRC changes and blocks SRTP streams with new SSRC on the same port. This happens for both audio and video streams. If you revert to plain RTP there are no limitations on the number of SSRC streams on the same RTP port. To increase the limit of SSRC changes allowed by SBC, configure the **allowed-ssrc-change-limit** under **realm-config**.

- Default: 7
- Values: Min : 7 / Max : 15

Adding allowed-ssrc-change-limit option

To change the default value of allowed-ssrc-change-limit:

```
ORACLE# configure terminal
ORACLE(configure)# media-manager
ORACLE(media-manager)# realm-config
ORACLE(realm-config)# options +allowed-ssrc-change-limit=<value>
```

If you type the option without the plus sign, you overwrite any previously configured options. To append the new option to the options list, prepend the new option with a plus sign as shown in the previous example.