Avaya Aura® Session Manager Security Design

Release 6.1
January 2011

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document may be incorporated in future releases

For full hardware support, please see the document, *Avaya Support Notices for Hardware Documentation*, document number 03–600759 on the Avaya support web site, http://www.avaya.com/support.

Documentation disclaimer

Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: http://www.avaya.com/support. Please note that if you acquired the product from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER, AND AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users. “Software” means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone products or pre-installed on Hardware. “Hardware” means the standard hardware originally sold by Avaya and ultimately utilized by End User.

Concurrent User License

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A “Unit” means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation(s) and Product(s) provided by Avaya. All content on this site, the documentation(s) and the product(s) provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil, offense under the applicable law.

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements (“Third Party Components”), which may contain terms that expand or limit rights to use certain portions of the Product (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://www.avaya.com/support/Copyright/.

Preventing toll fraud

“Toll fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of toll fraud associated with your system and that, if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya fraud intervention

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support Web site: http://www.avaya.com/support/. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

Avaya, the Avaya logo, Avaya Aura® System Manager, and Avaya Aura® Session Manager are registered trademarks of Avaya Inc. in the United States of America and/or other jurisdictions. All other trademarks are the property of their respective owners.

Downloading documents

For the most current versions of documentation, see the Avaya Support Web site: http://www.avaya.com/support

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://www.avaya.com/ support

Contents

Introduction

How this book is organized

This book contains four major sections and four appendices that are described in Table 1 below.

Table 1: Avaya Session Manager Security guide

Chapter / section	Description
Introduction	• Session Manager security philosophy overview • Avaya's multi-layer hardening strategy • How this guide complements other Avaya product security guides
Secure by default	Describes the security features that Avaya has designed into its products.
Configurable security	Discusses security issues that customers must consider before designing and implementing a corporate security strategy
Network Security Integration	Helps customers integrate their corporate security strategy into their network.
Operational security	Recommendations for maintaining and monitoring security in an Avaya enterprise.
Appendices	• Appendix A: Physical interfaces and associated network services • Appendix B: Network services on Avaya Session Manager • Appendix C: Additional security resources o Documents mentioned in this security guide o Security documents on the Avaya support site o Appendix D: Default Certificates

Session Manager Security overview

This book describes the security-related considerations, features, and services for Session Manager. As the SIP routing element for all SIP communications, Session Manager needs to be resilient to attacks that can cause service disruption, malfunction or theft of service. Avaya's products inherit a number of mechanisms from legacy communications systems to protect against toll fraud or the unauthorized use of communications resources. However, Unified Communications capabilities, which converge telephony services with data services on the enterprise data network, have the additional need for protections previously specific only to data networking. That is, telephony services need to be protected from security threats such as:

- Denial of Service (DoS) attacks
- Malware (viruses, worms and other malicious code)
- Theft of data
- Theft of service

Avaya's multi-layer hardening strategy

To prevent security violations and attacks, Session Manager uses Avaya's multilayer hardening strategy:

- Secure by design
- Secure by default
- Secure communications

Secure by design

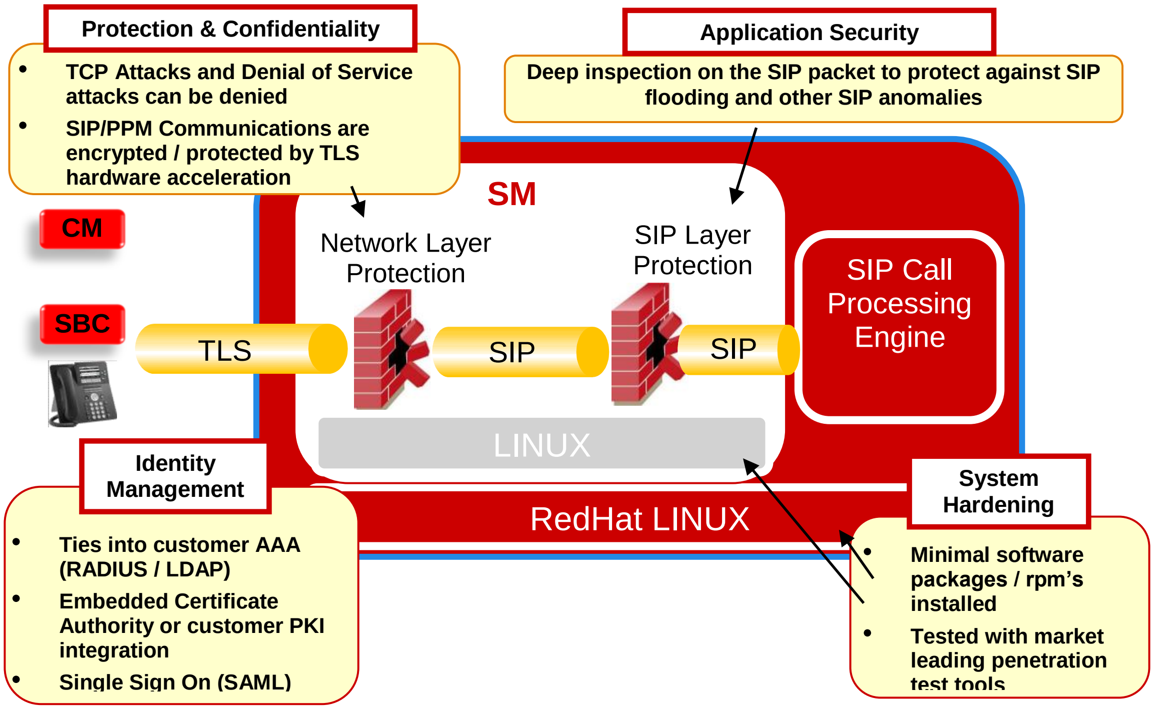
Secure by design encompasses a secure deployment strategy that separates Unified Communications (UC) applications and servers from the enterprise production network. Since all SIP sessions flow through Session Manager, being the SIP routing element, Session manager is able to protect the UC applications and servers from Network and Transport Denial of Service (DoS) attacks, SIP DoS attacks as well as protect against other network attacks. For customers that deploy SIP trunks to SIP Service providers, Avaya recommends the usage of Avaya Aura™ Session Border Controller to provide an additional layer of security between the SIP Service Provider and Session Manager. The architecture is related to the trusted communication framework infrastructure security layer and allows for the specification of trust relationships for:

- Administration
- Enterprise network
- SIP Elements

Secure by default

Secure by default incorporates a hardened Linux operating system with inherent security features for Session Manager. This hardened operating system provides only those functions that are necessary for securing mission-critical call processing applications, and protect the customers from toll fraud and other malicious attacks.

The Linux operating system limits the number of access ports, services, and executables and helps protect the system from typical modes of attack. At the same time, the reduction of Linux services limits the attack surface.



Protection & Confidentiality

- TCP Attacks and Denial of Service attacks can be denied
- SIP/PPM Communications are encrypted / protected by TLS hardware acceleration

Application Security

Deep inspection on the SIP packet to protect against SIP flooding and other SIP anomalies

Identity Management

- Ties into customer AAA (RADIUS / LDAP)
- Embedded Certificate Authority or customer PKI integration
- Single Sign On (SAML)

System Hardening

- Minimal software packages / rpm's installed
- Tested with market leading penetration test tools

Secure communications

Secure communications uses numerous features and protocols to protect access to and the transmissions from Avaya communications systems. Avaya uses media encryption to ensure privacy for the voice stream. Alongside media encryption, integrated signaling security protects and authenticates messages to all connected SIP elements, minimizes an attackers ability to tamper with confidential call information. These features protect sensitive information like caller and called party numbers, user authorization, barrier codes, sensitive credit card numbers, and other personal information that is dialed during calls to banks or automated retailers.

Critical adjunct connections are also encrypted.

Avaya IP endpoints can additionally authenticate to the network infrastructure by supporting supplicant 802.1X. Network infrastructure devices like gateways or data switches act as an authenticator and forward this authentication request to a customer authentication service.

Who is responsible for Session Manager Security?

Avaya is responsible for designing and testing its products for security. When Avaya sells a product as a hardware/software package, Avaya's design and testing includes the operating system and ensuring the operating system is up to date with security patches.

The customer is responsible for the appropriate security configurations on their data network. The customer is also responsible for using and configuring the security features available on Session Manager. However, Avaya offers services for assessing the customer’s network based performance and security issues. Avaya also offers configuration services for its products.

Software-only applications versus software-plus-hardware solutions

Some Avaya communications applications are sold as software only and must be installed on a customer-provided computer that runs an off-the-shelf operating system. For these products, the customer is responsible for ensuring that the operating system and other third-party software provided by Avaya are secure. Other Avaya applications that are sold with Avaya-only hardware and software, Avaya ensures that the operating system and any third-party software are secure.

Responsibility for security updates

When security-related application or operating software updates become available, Avaya tests the updates, if applicable, and then makes them available to customers. In some cases, Avaya modifies the update software and then makes it available to customers.

Avaya notifies customers of the availability of security updates through Security Advisories. Customers can subscribe to be notified about Security Advisories by email. See What is an Avaya Security Advisory and How do I get Avaya Security Advisories?

When Session Manager software security updates become available, the customer can install the updates or employ an installer from the customer’s services support group to install the updates. When Avaya installs the updates, the installer follows the best security practices for server access, file transfers, and data backups and/or restores. For back up and data restoration, the customer is responsible for providing a secure backup and restore repository on the customer’s LAN.

How this guide complements other Avaya product security guides

This document describes security-related issues and security features of Session Manager. Avaya Aura™ System Manager is used to manager Session Manager and this document also covers the security management features of System Manager that are relevant to Session Manager. This document is part of a set of security guides that describes the potential security risks to Avaya products and the features that Avaya products offer to mitigate these security risks.

This document is a descriptive guide, not a procedural guide. Where appropriate, the guide references other product documentation for the actual procedures for configuring and using security features.

Other product-specific security guides cover the following products:

- Call center products, including Call Management System and Interactive Response

- Integrated Management suite of management tools, including the Avaya Network Console, Secure Access Administration, Fault and Performance Manager, and Avaya Site Administration.
- Unified Communications, including Communication Manager, Modular Messaging, Video Telephony Solution, Meeting Exchange, and Web Conferencing, and Provisioning and Installation Manager.
- Secure gateways and C360 stackable switches

Secure by default

Operating system hardening

Why Avaya chose the Linux operating system for Session Manager

Avaya uses the open-source Red Hat Enterprise Linux operating system as a secure foundation for communications. Benefits of the open source foundation include:

- Security experts worldwide review the source code looking for defects or vulnerabilities.
- Avaya works diligently to monitor both the enhancements and improvements created by the Linux community and to carefully review the changes before incorporating them into Avaya products.
- Linux-based Avaya servers and gateways protect against many (DoS) attacks such as SYN floods, ping floods, malformed packets, oversized packets, and sequence number spoofing, among others.

How Avaya modifies Linux to improve security

Avaya has modified, or hardened, the Linux operating system in several ways to improve minimize vulnerabilities and to improve security.

Unused RPMs removed

The Linux general distribution includes Red Hat Package Management (RPM) modules that install, uninstall, verify, query, and update software packages. Since Avaya's IP telephony application does not need all of the RPMS provided by Red Hat, Avaya has removed unused RPMs from the general RPM distribution. In addition to making the software file images smaller and more manageable, the operating system is more secure because attackers cannot compromise RPMs that are not present.

To determine which RPMs Avaya employs, use the **rpm -qa** command at the Session Manager server's command line interface (CLI) to see the RPM list.

Unnecessary IP ports closed

Many Linux modules like SSH or Apache or SSL/TLS (HTTPS) are applications that open Ingress network services. Avaya reduces the Ingress network services only to those that are necessary for its telephony applications, thus minimizing exposure of the operating system to network-based attacks. By default, Avaya disables the less secure network services like TELNET and FTP (see Why using SSH/SCP is more secure than Telnet, FTP, or SNMP).

System Services are executed with least privileges

In accordance with Avaya’s security practices, Session Manager and other OS services within Session Manager are run or owned by an account with the least privilege that is required for correct operation of those services. This is to prevent an attacker from potentially gaining privileged access to the operating system by exploiting a known vulnerability in a particular service.

Secure connections

Why using HTTPS, SSH/SCP is more secure than HTTP, Telnet or FTP

Connection protocols that send data--especially logins and passwords--in plaintext, that is, unencrypted or "in the clear," can pose a serious security risk to a VoIP enterprise. Using protocols that send data encrypted, such as SSH and SFTP, avoids exposing critical data on the wire. Partly due to new legislation and stricter auditing requirements, Avaya has implemented more secure protocols in its secure connection design.

Disabled by default

By default, Avaya disables these inherently insecure network services:

- TELNET (TELetype NETwork) does not encrypt data (logins, passwords, or PIN information) sent over the connection between the two desired hosts.
- FTP sends information in unencrypted (clear) text, which permits interception by eavesdroppers relatively easily. Also, FTP has no integrity check, meaning that if a file transfer is interrupted, the receiver cannot tell if the transfer is complete.

Avaya products ensure that authentication credentials and file transfers are protected when sent across the network by using:

- HTTPS
- Secure Shell (SSH)
- Secure Copy (SCP) or SFTP
- SNMP with these stipulations:
  - SNMPv1 or v2c, while supported, provide only a limited security capability based on community names:
  - The community name for SNMPv1 and SNMPv2c is protected when accessing writable MIBs.
    - For read-only MIBs SNMPv1 and SNMPv2c community names are unprotected.
- Other protocols protected using a TLS or IPSEC connection
  - JMX over TLS
  - JMS over a TLS bisocket
  - HTTPS

Privilege escalation and root logins

Avaya's Linux-based products adopt the "privilege escalation" concept that requires lower-privileged accounts to log in at their normal level before they can escalate their privileges to perform more restrictive tasks, such as software replacement. Each privilege escalation requires a separate authentication and creates a log entry for monitoring.

How Avaya incorporates security updates in its applications

When a third-party update (also called a patch) is available to mitigate a security vulnerability, Avaya might recommend that the customer apply the patch from the third-party. This action, if recommended, is stated explicitly in the Avaya Security Advisory.

For some third-party updates, Avaya might not recommend installation due to interoperability, stability, or reliability issues with the update and Session Manager. In this case, before Avaya releases a security update, Avaya thoroughly tests it on a non-production system, along with all the other software that is normally loaded (and not loaded) on Session Manager. Accordingly, Avaya modifies the update before it works correctly. Customers who apply non-recommended 3rd-party-provided patches may void their warranty.

In some instances, when a software vendor provides an update to address a vulnerability, Avaya might address the vulnerability through other means to avoid potential risks to Session Manager. This might include modification of existing software through an Avaya-issued update which is released separately or incorporated into future releases of the product. Such decision to offer an alternative remediation is described in the advisory.

For more information on Avaya Security Advisories, see:

- What is an Avaya Security Advisory
- How do I get Avaya Security Advisories?
- How to interpret an Avaya Security Advisory

Network Security

VLAN Segregation

Session Manager supports VLAN segregation of SIP and Management networks. Session Manager has a separate management access interface for all management communication between Session Manager and System Manager.

The Session Manager SIP interface and Session Manager Management interface should be placed in different VLAN segments. The Session Manager Management interface should be placed in a management VLAN which shall not be accessible from the SIP Network. System Manager must be accessible through the management VLAN to be able to manage Session Manager. VLAN segregation is strongly recommended from a security perspective.

Session Manager Firewall protection

Session Manager uses Network/Transport and SIP firewall to protect Session Manager from Network and SIP DoS attacks.

Network/Transport firewall

Avaya's Session Manager uses the IPTables network firewall to protect Session Manager against various network-based Denial of Service (DoS) attacks. IPTables is also used to open all the TCP/UDP ports which are used by Session Manager. All unused TCP/UDP ports (ports not used by services running inside Session Manager) are closed by default. Session Manager has the IPTables Network Firewall running in the:

- Session Manager SIP Server (For filtering Management traffic)

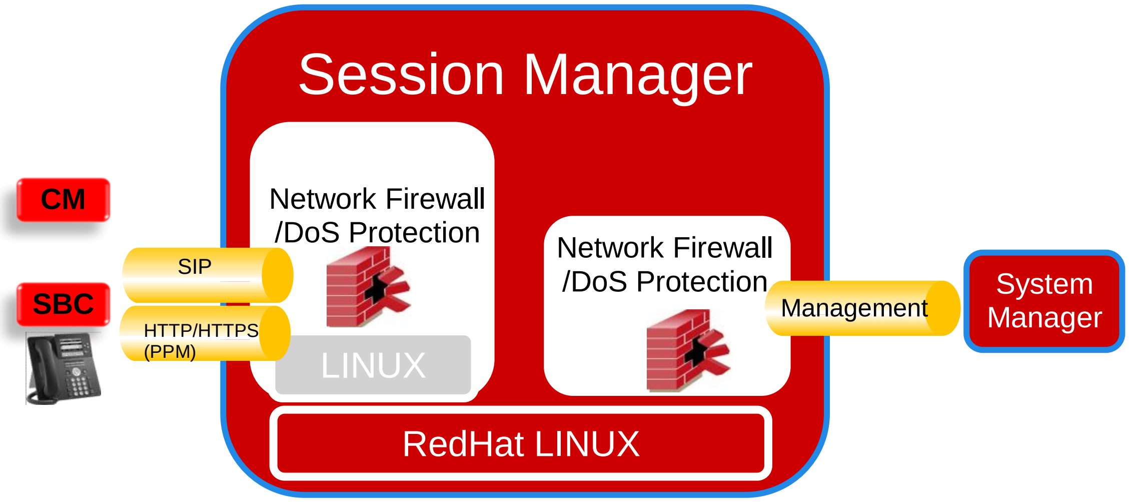


Figure-2 Session Manager Network Firewall/DoS Protection

The Network Firewall default rules are configured automatically during installation. The default rules ensure that all of the ports used by Session Manager SIP Server as defined in the Session Manager ports and protocols document (refer to Appendix B) are opened, and that all unused TCP/UDP ports are closed. SIP Listen ports are opened/closed dynamically per the customer's Network Routing Policy (NRP) defined in the SIP Entity configuration in System Manager. The Network Firewall also provides Network Layer DoS Protection. The following is a list of the default protections provided by the Network Firewall:

- TCP Syn Flood
- IP Options
- ICMP timestamps
- ICMP Redirects
- Source Routed Packets
- Reverse Path Forwarding
- Invalid IP Packets
- Bad TCP Packets

Please refer to Appendix B for information on the ports and protocol used by Session Manager.

SIP Firewall

Session Manager uses the SIP Firewall to provide SIP DoS Protection. Additionally, all encrypted SIP TLS is decrypted before applying the SIP Firewall Policy.

Default SIP Firewall Rules

The SIP Firewall default configuration provides a default rule set to use. Avaya recommends the use of the default rules in Session Manager after initial installation.

The following section describes the default rules for the SIP firewall:

Rules (Enabled)
The Following are the default rules enabled in the default rule set. Threshold parameters may need to be adjusted as per specific deployment needs.

1. **Rule Name**: "ratelimit_and_alarm_high_traffic_from_same_remote_ip"
Description: This rule will rate limit and alarm high traffic rates by applying track on Remote IP Address. This rule limits SIP messages from any SIP entity to a maximum of 30,000 SIP messages in 30 seconds.

2. **Rule Name**: "alarm_INVITE_flood_from_same_remote_ip"
Description: This rule alarms a high rate of SIP INVITE messages by applying track on Remote IP Address. This rule is for logging only and it does not drop any packets. This rule generates an alarm when a SIP

entity sends more than 300 SIP INVITE messages within a 30 second period.

3. **Rule Name**: "alarm_high_traffic_from_same_user"
Description: This rule alarms a high traffic rate by applying track on From (From-URI). This rule is for logging only and it does not drop any packets. This rule will generate an alarm when a user sends more than 200 SIP messages within a 15 second period

4. **Rule Name**: "alarm_slow_INVITE_flood_from_same_user"
Description: This rule alarms a high rate of SIP INVITE messages by applying track on From (From-URI). This rule is for logging only and it does not drop any packets. This rule will generate an alarm when a user sends more than 15 SIP INVITE messages within a 60 second period.

5. **Rule Name**: "alarm_high_REGISTER_rate_from_same_user"
Description: This rule alarms a high rate of SIP REGISTER messages by applying track on From (From-URI). This rule is for logging only and it does not drop any packets. This rule will generate an alarm when a user sends more than 10 SIP REGISTER messages within a 60 second period.

6. **Rule Name**: "alarm_high_OPTIONS_rate_from_same_user"
Description: This rule alarms a high rate of SIP OPTIONS messages by applying track on From (From-URI). This rule is for logging only and does not drop packets. This rule will generate an alarm when a user sends more than 10 SIP OPTIONS messages within a 60 second period.

Whitelist (Enabled)
The Whitelist is enabled by default in the default rule set and has one rule.

1. Key = Remote IP Address, Value = 192.11.13.2, Mask = 255.255.255.255

This rule allows traffic from the internal Session Manager SIP IP Address used by the Session Manager SIP Server.

Blacklist (Disabled)
No Blacklist rules are present in the default rule set.

HTTP/HTTPS DoS Protection

Avaya telephones use HTTP/HTTPS connections for connecting to Personal Profile Manager (PPM) Server in Session Manager. These connections are terminated on SM100 security module.

Session Manager provides the following default security for these HTTP/HTTPS connections

1. Connection Limiting
This provides DoS Protection from a hacker opening a large number of HTTP/HTTPS connections with Session Manager and consuming all the resources. By default a remote entity will be limited to a maximum of 3 HTTP/HTTPS connections to Session Manager.

In addition, Session Manager limits the maximum number of total HTTP/HTTPS connections to 1000 to preserve resources for SIP connections.

2. PPM Connection Timeout
This provides resource optimization in Session Manager by closing connections that are no longer in use (no activity on a connection).

3. Packet Rate Limiting
This provides DoS Protection from a hacker sending a flood of packets over HTTP/HTTPS connections with Session Manager. By default a remote entity is limited to a maximum of 50 packets per second on a HTTP/HTTPS connection to Session Manager.

Note: If all PPM (HTTP/HTTPS) traffic is redirected to an HTTP proxy and Session Manager is receiving all HTTP/HTTPS requests from an HTTP proxy, Connection Limit and Packet Rate Limit thresholds will need to be adjusted accordingly (or may even need to be disabled).

Prevented DoS Attacks

A denial-of-service (DoS) attack is an incident causing denial of access to a resource. Regardless of the method, the net effect of DoS attacks is to deny legitimate access to a server or an application.

Session Manager is designed to survive the DoS attacks as listed in the table below, without rebooting or restarting, or reloading, and automatically recovers to full service after the DoS attack has subsided.

Avaya’s design against types of DoS attacks

Attack type	Description
SYN flood (TCP SYN)	Phony TCP SYN packets from random IP addresses at a rapid rate fill up the connection queue and deny TCP services to legitimate users.

Land and LaTierra	The Land attack combines IP spoofing with opening a TCP connection. It sends a request to open a TCP connection (SYN flag in the header is on) but changes the IP address so that both the source and destination IP addresses are the same as the destination host IP address. When the destination host receives the packet, it sets a SYN, ACK to itself because destination and source IP addresses are the same with the same sequence number. The system expects a different sequence number related to the SYN, ACK packet from the other host, so it keeps sending the ACK packet back expecting an updated sequence number. This puts the host into an ACK loop. The LaTierra attack is similar to the Land attack but sends TCP packets to multiple ports at once.
Smurf / Pong	Large numbers of ICMP echo (PING) messages sent with the forged address of the intended victim, and Layer 2 devices issue an echo reply (pong), multiplying the traffic by the number of responding hosts.
Fraggle	Like Smurf, Fraggle is a UDP flood that uses an IP broadcast address of the victim (IP spoofing) that results in an infinite loop of echo and reply messages.
Jolt1 and Jolt 2	The Jolt2 attack raises the CPU utilization to 100% causing instability in the system until the Jolt2 attack stops. Most instances of this attack are from illegally fragmented packets: • If no port number is passed as an argument then it sends illegally fragmented ICMP ECHO (pings) packets to the specified port. • If a port number is provided then it sends illegally fragmented UDP packets to the specified port. In both cases jolt2 sends a continuous stream of same fragmented packet in which • The fragment offset is 65520. • The TTL is set to 255. • The IP MF flag is set to zero. These settings cause the IP checksum of the last fragment to equal zero, which is illegal. Jolt2 then sends 9 bytes of IP data including the IP header 20 bytes (total of 29 bytes) but sets the total length to 68 bytes. The offset and the packet length (65520 + 68) exceeds the maximum size of an IP datagram imposed by the 16-bit total packet length field in the IP header (maximum allowed packet size is 65563 bytes). This packet should fail the integrity check and discarded right away, however some systems do not do the integrity check

	and continue buffering these fragments. This can utilize 100% of the CPU and in some cases crash the system.
Packet replay attack	Packet replay refers to the recording and re-transmission of message packets in the network. Packet replay is a significant threat for programs that require authentication sequences, because an intruder could replay legitimate authentication sequence messages to gain access to a system. An attacker can replay the same packet at different rate, and the system attempts processing duplicate packets causing • Total resource depletion • Termination of existing connections • Chaos and/or confusion in the internal buffers of the running applications • System crashes in some cases
Gratuitous ARPs	Most systems send out an Address Resolution Protocol (ARP) request for its own IP address to check for a duplicate IP address on the network. Some systems update their own ARP cache when they receive a gratuitous ARP packet. The attacker uses this vulnerability to change the ARP table with the host's router's MAC address, so all the packets start to flow either through their system or with an invalid MAC address for a router or important server.
Teardrop, overlap, or fragmented packets	The teardrop and associated attacks exploit the packet reassembly code that breaks packets into smaller pieces (fragments) based on the network's maximum transmission unit (MTU). When reassembled, packets are often misaligned — the next fragment does not begin where the last fragment ended but inside the previous fragment memory allocation. This causes memory allocation failures and the system to crash.
PING flood	Because so many ping utilities support ICMP echo requests and an attacker does not need much knowledge, sending a huge number of PING requests can overload network links.
Finger of death	The attacker sends finger requests to a specific computer every minute but never disconnects. Failure to terminate the connection can quickly overload the server's process tables. The finger listen port number is 79 (see RFC 742).
Chargen packet storm	The attacker can spoof the chargen service port (19) from one service on one computer to another service on another computer causing an infinite loop and causing loss of performance or total shutdown of the affected network segments.

Malformed or oversized packets	Malformed packets attacks attempt to deny service by causing protocol handlers to cease operation due to the difficulty they have processing odd formations of a protocol or the packets sent as part of the protocol. Oversized attacks place data in an order that is out of specifications or create packets that are larger than the maximum allowed size.
OOB nuke	Continuous transmission of out-of-band packets with the TCP URGENT flag but without subsequent data to the most commonly-attacked port (135-Netbios Session Service), other ports are also possible targets.
SPANK	The target responds to TCP packets sent from a multicast address causing a DoS flood on the target's network.
SDP and SIP PROTOS	This attack utilizes the Protos SIP testing tool from OULU University to test SIP code for faulty implementations. The tool generates thousands of valid SIP packets with strange and anomalous values that cause error conditions in the implementation of the protocol. See http://www.ee.oulu.fi/research/ouspg/protos/testing/c07/sip/index.html.
SIP Flood	An attacker can send a huge number of SIP messages to Session Manager. INVITE/REGISTER flood are some of the examples of this attack.

Protection against impact of viruses, worms and other malicious code

Most viruses and worms (often called "malware") has the effect of

- Disrupting or delaying normal functionality
- Changing configurations by rewriting code
- Retrieving sensitive data

Although similar in their effects, viruses and worms differ in their behavior. A virus needs a host (an application, an e-mail, or a file) and a user action (for example, opening an e-mail attachment) to propagate, but a worm does not need a host or any user action. Viruses and worms are commonly delivered through email, visiting infected Web sites, or sharing file systems.

Security impacts of viruses and worms

Security implementation	Security impact
Natural immunity	Avaya's Linux-based servers do not support: • Incoming or forwarding email • User Web browsing
File permissions	Standard program binaries are

Security implementation	Security impact
	normally installed with write permissions only to the super-user (root) and cannot be modified, resulting in very few virus outbreaks within the Linux operating system.
Performance degradation	Avaya has tested 3rd-party, host-based antivirus products on its Linux-based servers and uncovered significant performance degradation attributable to the 3rd-party software. Avaya does not recommend installation of such products on its Linux-based servers.

Secure Management

Avaya Services Access

Data transmission to and from Avaya Services in support of customer equipment is protected through non-secure data networks like the Internet, over modems, and through SNMP notifications. Contact Avaya Services for more information.

Avaya Services Accounts

Avaya uses a multi-tiered user privilege model. There are the two default accounts: **sroot** and **craft**. These accounts are available only to authorized Avaya personnel or business partners. The passwords for these accounts are managed using Avaya's Maestro Password change system which is an automated password changing system that changes Avaya services login passwords on a periodic basis.

Account	**Service Level**	**Privileges**
sroot	Root	Services Root, same as 'root', protected by Avaya's Password Change System authentication.
craft	susers	craft cannot perform login administration or change customer services

Credentials management

Credentials (usernames and passwords) for standard Linux accounts in Session Manager are stored in /etc/passwd, /etc/shadow, and /etc/group, plus the backup files for those files, for example, /etc/group- and /etc/passwd-. Session Manager does not use a database to store credentials information.

- Passwords for local accounts are stored in /etc/shadow. Passwords in /etc/shadow are stored as a 1-way hash. The file /etc/shadow is root restricted.
- Usernames and group membership for local accounts can be viewed by any user logged into Linux.
- Credentials configured for an external AAA server such as RADIUS or LDAP are stored on the external server, not within the application.

Privilege escalation

Session Manager supports privilege escalation. Technicians who need higher privileges are required to log in using their normal service accounts and then escalate their privileges to perform more restrictive tasks, for example, software upgrades.
To escalate access privileges, a technician uses **`sudo`**, a Linux/Unix escalation utility that allows the user to login to another account. The user specifies the login account and must correctly respond to the authentication request for that account.

You can read the superuser permissions and restrictions by issuing the **`sudo -l`** command at the server CLI. This command escalates the user's permissions to the superuser level and the output lists the commands that a superuser can and cannot run on the current host.

Session Manager Element Management

The Management functionality for Session Manager is provided by System Manager which has two primary components,

- **A Management framework**, that provides a basic set of services for user management, trust management and network routing policy management. These services provide management capabilities used by both the Session Manager and the System Manager.

- **Element Management**, that provides a service integrated into System Manager but specifically designed to manage multiple Session Manager instances.

Administrative access to these management interfaces is controlled by providing Authentication and Authorization capabilities within System Manager. Configuration changes made using System Manager can also be monitored via the built-in Logging and Alarming infrastructure to ensure compliance with Enterprise Security Policies. The following sections describe these capabilities.

Authentication

In the current release, System Manager can be configured to authenticate administrative users using external authentication services like Enterprise Directory, a Database or a RADIUS server. An administrative account is provisioned within the System Manager during installation for initial access.

Note: Access to the Session Manager host (OS) is not recommended in this release and all management functionality of Session Manager is expected to be performed via System Manager. See the book **Administering Avaya Aura™ Session Manager** on specific instances when local access may be required.

Avaya System Manager's support of external authentication services allows,

- Centralized control of enterprise logins and passwords
- Enforcement of password aging, complexity, minimum length, and reuse requirements
- Avaya product adherence to the enterprise corporate security standards regarding logins and passwords

Authentication Mechanism	**Description and Interoperability information**
DB	(Default) This is the default mechanism and is configured to be done against the embedded database (Postgres). Interoperability: This release of System Manager has been tested to interoperate with Postgres
LDAP	System Manager can be configured to authenticate against the enterprise LDAP for administrator authentication. These users still need to be provisioned in the System Manager database since System Manager requires the authorization information to provide privilege based access to the users. Interoperability: This release of System Manager has been tested to interoperate with openLDAP
RADIUS	Administrative users can also be authenticated against a RADIUS server, and this setup should also allow support for token based authentication mechanisms like SecurID. But like LDAP authentication, the users authenticating using this mechanism need to be provisioned in the System Manager Database for authorized access. Interoperability: This release of System Manager has been tested to interoperate with FreeRADIUS

Authorization (Role-Based Access Control)

All users within the System Manager are only allowed to perform operations that they are authorized for. System Manager allows the creation and assignment of roles to users. System Manager supports the following default roles,

Role name	Job function and access permissions
System Manager Auditor	A read-only role for observing the system. The auditor is a user assigned to the Auditor role that has read only access to logs, configuration information and audit files. The user assigned to the Auditor role is not allowed to execute any command that may allow them to access another host (host containment).
System Manager System Administrator	A role with read-write access to system parameters (e.g., IP addresses, upgrade software), and ability to modify, assign, or define other roles and read/write access to create and modify logins.
Session Manager System Administrator	System Administrative role for Session Manager which has read-write access to all Session Manager configuration parameters.
Backup Administrator	Ability to perform only backups and restores.
System Manager Security Administrator	A role with read-write access to create other logins, create, modify or assign roles, install ASG keys, install licenses, install PKI certificates and keys
Avaya Services Maintenance and Support	A role with read-only access to maintenance logs, the ability to run diagnostics and view the output of diagnostics tools. The user assigned to the Avaya Services and Maintenance role is not allowed to execute any command that may allow them to access another host (host containment)

Note: In the current release, only the Session Manager System Administrator Role is allowed access to Session Manager Element Management functionality.

Logging and Alarming

To ensure compliance with enterprise security policies, System Manager provides capabilities to monitor configuration changes and other security events using the logging and alarming infrastructure

The logging and alarm event displays show details such as event timestamp, severity, description, and originating host/application. Log messages follow the Avaya Common Logging Format. Alarms are administered (i.e. cleared, acknowledged) and exported to a spreadsheet.
Configuration options include defining severity level of application’s events to be collected, log file sizes and locations, and event data retention policy.

For more information on logging please refer to the Logging and Alarming section

Configurable security

Encryption

Avaya's encryption overview

Digital encryption can reduce the risk of intercepting phone conversations, voice mail, and the signaling messages that support them both. A digital phone call consists of voice (bearer) data and call signaling (control) messages. Both bearer and signaling data can pass through many devices and networks, sometimes over a separate network or virtual path from each other. Without encrypting both data types anyone with access could intercept:

- Digitized voice signals in phone calls and voice mail
- Call signaling messages that:
  - Setup, maintain, and tear down calls
  - Contain call duration
  - Reveal the callers' names and numbers
  - Transmit encryption keys
- Translation (administration) data in transit to or saved on a storage device include IP addresses and routing information from which an attacker can analyze traffic patterns.
- Configuration data through TLS connections
- Application-specific traffic
- Data exchanged during management and administration sessions

The following table compares how encryption mitigates the vulnerabilities in signaling and bearer media.

Media	**Unencrypted** (cleartext)	**Encrypted**
Bearer	Vulnerable to eavesdropping	Prevents eavesdropping
Signaling	Susceptible to message spoofing and registration hijacking	Prevents message spoofing and hides sensitive information

Session Manager Supported encryption algorithms

Session Manager implements cryptographic algorithms and methodologies that are generally accepted in the INFOSEC community. Furthermore, the selection of cryptographic functions is based on their ability to be approved under a FIPS-140-2 or Common Criteria certification assessment.

Note: The use of SRTP to encrypt media or bearer traffic is transparent to Session Manager.

Encryption supported in Session Manager

Encryption technique	Available algorithms	Description
SSH		Secure Shell, a standard security protocol to protect shell access to Unix based and Linux operating systems.
	aes128-cbc, 3des-cbc, blowfish-cbc, cast128-cbc, arcfour, aes192-cbc, aes256-cbc	Session Manager SSH server supported encryption algorithms
	Hmac-md5, hmac-sha1, hmac-ripemd160, hmac-sha1-96	Session Manager SSH server supported hashed message authentication codes.
HTTPS, STUNNEL for Secure Access Link (SAL)		Secure link between the SAL Agent that's co-resident on Session Manager to the Agent Management service hosted with Avaya System Manager
	TLS_RSA_with_AES_128_CBC_SHA	RSA authentication with AES encryption and MD5 message authentication
	TLS_DHE_RSA_with_AES_128_CBC_SHA	RSA authentication ephemeral Diffie-Hellman key agreement with AES encryption and SHA1 message authentication
	SSL_RSA_WITH_3DES_EDE_CBC_SHA	RSA authentication with Triple DES EDE CBC encryption and SHA1 message authentication
	SSL_DHE_RSA_with_3DES_EDE_CBC_SHA	RSA authentication with ephemeral Diffie Hellman key agreement with 3DES EDE CBC encryption and SHA1 message authentication
	SSL_DHE_RSA_with_DES_CBC_SHA	RSA authentication with ephemeral Diffie-Hellman key agreement with DES CBC encryption and SHA1 message authentication
	SSL_RSA_EXPORT_with_DES40_CBC_SHA	512 bit RSA keys with 40 bit DES encryption with SHA1

		message authentication
HTTPS, SIP TLS		
	TLS_RSA_with_AES_128_CBC_SHA	RSA authentication with AES encryption and SHA1 message authentication
	TLS_RSA_with_DES_CBC3_SHA	RSA authentication with Triple DES encryption and SHA1 message authentication
	TLS_RSA_with_RC4_128_CBC_SHA	RSA authentication with RC4 encryption and SHA1 message authentication
	TLS_DHE_RSA_with_DES_CBC_SHA	RSA authentication with Diffie Hellman ephemeral key negotiation with AES encryption and SHA1 message authentication
Jgroups		Jgroups provides security for multicast streams that are exchanged between Session Manager instances.
	AES_128_cbc-hmacSHA1	AES 128 bit encryption with SHA1 message authentication

Encryption summary

Session Manager secure protocols

Link	**Description**	**Transport protocol**	**Encryption / authentication algorithm**	**Key exchange**
SIP signaling	SIP Trunks to/from Session Manager	TLS	See encryption table	TLS
Personal profile manager (PPM) download	SIP telephone to Session Manager	HTTPS	See encryption table	TLS
Admin access	Access to the System Manager console for Session	https	See encryption table	TLS

	Manager administration			
Jgroups	State information shared between Session Manager instances	Jgroups/multicast	See encryption table	Pre-shared secrets
Logging	Log messages sent from Session Manager to System Manager	STUNNEL	See encryption table	TLS

Digital certificates and server trust relationships

Trust Management

Introduction

Digital certificates certify that a public key belongs to its reputed owner. To ensure greater trust, a trusted party can sign the public key and the information about its owner, creating a public-key certificate, usually called a certificate. Similar to a driver's license, a certificate guarantees the identity of its bearer.
A trusted party that issues digital certificates is called a certification authority (CA), similar to a governmental agency that issues drivers' licenses. A CA can be an external certification service provider or even a government, or the CA can belong to the same organization as the entities it serves. CAs can also issue certificates to other sub-CAs, which creates a tree-like certification hierarchy called a public-key infrastructure (PKI).

In the context of the Session Manager, the certificate that is used by the Session Manager to assert its identity to the far end is called its Identity Certificate. While the issuer/CA certificates that it uses to verify/validate the identity of the far end is referred to as Trusted Certificates.

System Manager Trust Management

System Manager Trust Management is used to provision and manage certificates of various applications (servers/devices) enabling them to have secure inter-element communication.

It provides Identity (Server) and Trusted (Root/CA) certificates that can be used by applications to establish mutually authenticated TLS sessions.

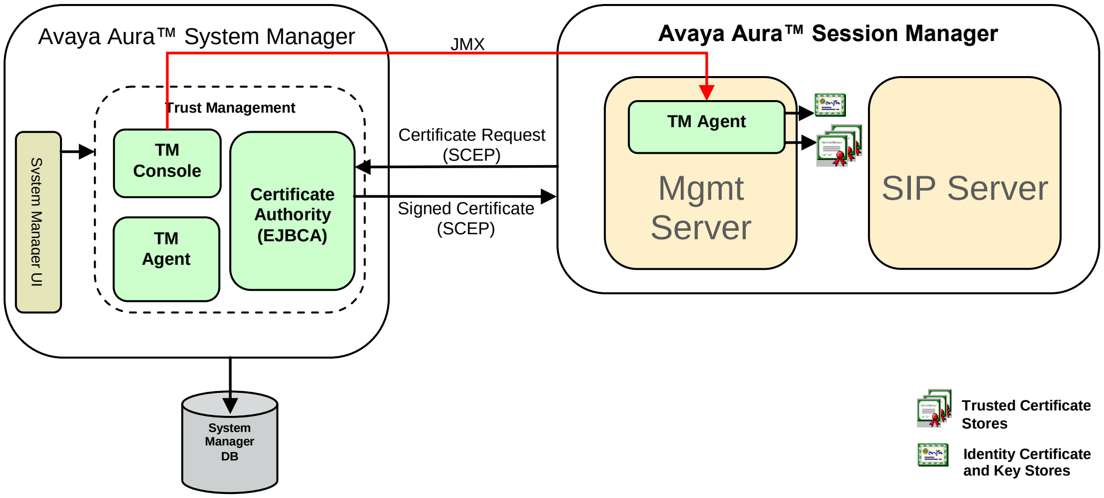

Avaya Aura™ System Manager
JMX
Avaya Aura™ Session Manager
Trust Management
System Manager UI
TM Console
TM Agent
Certificate Authority (EJBCA)
Certificate Request (SCEP)
Signed Certificate (SCEP)
TM Agent
Mgmt Server
SIP Server
System Manager DB
Trusted Certificate Stores
Identity Certificate and Key Stores

Figure-3 System Manager Trust Management

System Manager as a Certificate Authority

System Manager's Trust Management service is deployed with certificate authority software (EJBCA) that is, by default, configured to be a root CA.

Session Manager Certificate Management

Default Certificate in Session Manager

Session Manager ships with a default Identity certificate issued by the Avaya SIP-CA, which is an Avaya Certificate Authority that is controlled by Avaya and is only used to issue non-unique certificates to enable out of box support for SIP-TLS and PPM-HTTPS sessions. Additionally, Session Manager also bundles a default set of trusted certificates that are used to verify far-end certificates during SIP-TLS session establishment.

Caution: Session Manager is shipped with a default identity certificate to enable out-of-box support for TLS sessions. It is **not** recommended to use this default certificate in a production environment since it is common across all instances of Session Manager. A compromise of the corresponding private key on one instance can allow an attacker to act as a man in the middle to either hijack or snoop on sessions being established with any Session Manager.

Note: Please read all certificate related sections (including section on Establishing SIP Trunks) of this guide before making a decision on certificate related changes to your setup.

Please find the certificate of the Avaya CA (SIP-CA) that issued the default certificate to Session Manager in Appendix-D. Also provided in that section are all the default trusted certificates that are shipped with Session Manager. These default trusted certificates, as mentioned before, are used to support out-of-box SIP-TLS sessions.

Updating Session Manager’s trusted certificates

Establishing TLS sessions with customer/3rd-party devices requires exchanging issuer certificates between Session Manager and the 3rd-party device. Use the System Manager Interface to provision additional trusted certificates to Session Manager.

Issuing a unique identity or server certificate to Session Manager

Session Manager uses the Trust Management service within System Manager to request an identity/server certificate. During installation, Session Manager prompts the user for the location information of the System Manager and also prompts the user for an enrollment password. This information is used by Session Manager to request for a unique identity certificate from System Manager’s Trust Management service.

You can add a third-party identity certificate for Session Manager. This is an alternative to using the internal CA signed certificate which is the default certificate from Avaya CA. The basic steps followed for switching to third party certificates are:

1. Administration of Session Managers
2. Importing of the new certificate into System Manager
3. On each Session Manager, replacing of operating certificates from the default to the downloaded one (third party certificate).

See the book **Administering Avaya Aura™ Session Manager** for steps on how to obtain an enrollment password from the System Manager Administration screens.

Important points on Branch Session Manager (BSM) Security

- All PPM communication between BSM and core (SMGR/SM) are secure via TLS (with mutual TLS authentication)
- All PPM user authentication and DoS protection as applicable on the core SM are applicable on BSM as well.
- BSM has separate IP addresses for SM Security Module and management (similar to core SM). Network firewall rules can be slightly different as per BSM needs (as per BSM port matrix)
- Dynamic port opening/closing in BSM (for SIP/PPM as present in hardware Security Module) is similar to SM.
- Before install or upgrade of Branch Session Manager, ensure that the date and time is in sync between the System Manager and the System Platform. A clock shift causes certificate and DRS replication problems.
- During installation of an active BSM, ensure that it has been administered on System Manager and that an Enrollment password is active.

- During following cases, trust may need to be initialized on a BSM.
    1. BSM failed during an install
    2. The enrollment password changed and an upgrade was performed
    3. The enrollment password was expired when an install or upgrade was performed
    4. DRS did not initialize properly

Configuring Trust Relationships

Defining server trust relationships with Digital Certificates

To establish mutually authenticated SIP TLS Trunks between Session Manager and any other Avaya or 3rd-Party application/server/telephone it is essential that either end is able to establish the identity of the other party during the initial TLS handshake and establish the relationship back to a known trusted 3rd party. To enable this exchange and establish this trust relationship both parties should provide their chain of trust.

To establish a trust relationship between Session Manager and a 3rd party product, the Avaya SIP Certificate Authority certificate should be imported into the 3rd party product. The Avaya SIP CA certificate is provided in Appendix D of this document. Session Manager's set of trusted certificates must also be updated to trust the 3rd party's CA certificate (see Updating Session Manager's trusted certificates, earlier in this document).

Session Manager to Avaya applications/servers

Avaya Communication Manager (Example)

For newer versions of CM (5.x+) that support installing additional trusted certificates, it is recommended that Session Manager is configured to use a unique, non-default identity/server certificate.

This can easily be achieved, after a successful installation of Session Manager, by choosing the option of using the System Manager issued certificate instead of the SIPCA issued certificate within System Manager (See the book **Administering Avaya Aura™ Session Manager**).

Since Session Manager trusts the certificates used by Avaya Communication Manager (by default) the only interchange that needs to be completed is to import the System Manager's CA certificate into Avaya Communication Manager. Please contact Avaya technical support for help with importing the System Manager CA certificate into Avaya Communication Manager.

Exception: Older versions of Avaya Communication Manager (prior to CM 4.x) do not support the addition of 3rd party trusted or root certificates. If secure connections to an older version of CM are required, the default SIP server certificate issued by the SIP-CA must still be used. In this case, no interchange of certificates is required.

Session Manager to 3rd party applications/servers

It is recommended that only unique, non-default identity/server certificates be used within Session Manager when interoperating with 3rd party applications/servers.

Session Border Controllers

To establish secure SIP Trunks between 3rd Party SBCs and Avaya Session Manager, the Issuer certificate of the SBC's identity certificate must be added as a trusted certificate to Session Manager and the Avaya System Manager CA certificate must be added to the 3rd party SBC's trusted certificate repository. This interchange ensures that the two devices trust each other and a successful TLS negotiation can occur.

If the SBC does not have an identity certificate and allows external identity certificates to be imported, then the System Manager CA can be used to issue (manually) a certificate to the SBC.

Comparing Session Manager and SBC service features for connecting to SIP Service Provider network

Features	SBC	Session Manager
Enhanced Security	Protects network and other devices against DoS / DDoS attacks and overloads.	Protects UC applications and servers from DoS, SIP DoS attacks.
	Protects Identity and session privacy where necessary with signaling and/or media encryption.	Supports media encryption to ensure privacy for the voice stream.
	Enforces access control policies by limiting incoming sessions to the IP addresses of service provider.	Enforces access control policies and user authentication using System Manager User Management functionality.
	Employs Network Address Translation (NAT) to hide the topology of UC servers and internal endpoints, thereby defending against directed	SM does not support network address translation. SM expects NAT to be done by an SBC or firewall.

	attacks and protecting user privacy.	
	Inspects traffic coming from the IP trunk to eliminate viruses, worms, SPIT and eliminate fraud by preventing unauthorized use of the IP trunk. This includes deep packet inspection.	SM inspects and filters SIP traffic to prevent malformed or malicious payloads from reaching Applications
Enhanced connectivity and interoperability options	Supported number of simultaneous sessions equals 750.	Supported number of simultaneous sessions equals 20,000 (simultaneous registered sessions/Session Manager)
	Supports number, URI manipulation and signaling message header manipulation.	Supports number, URI manipulation and signaling message header manipulation.
	Supports protocol interworking - signaling, transport & encryption protocols and response code translations. SIP, H.323, and SIP/H.323 IWF.	SM supports encryption protocol interworking for SIP TLS.
	Provides IP address translation between overlapping private IP address spaces or between IPv4 and IPv6 addresses.	None
	Enables SDP & DTMF manipulation and transcoding.	N/A
Quality of service enforcement	Provides redundancy and high availability for SIP connectivity to service providers and enterprise network. Also supports active and standby model ensuring no loss of active sessions.	Provides redundancy and high availability and supports active-active redundancy ensuring the uptime and performance of the network.
	Monitors the health of logically-adjacent elements (router, session agent, peer SBC) and, then re-route and redistribute traffic for elements that suffer performance degradation or failure.	Monitoring of health of connected elements and re-route according to administered routing policies.

	Ensures high session quality and CAC to prevent SIP trunk saturation and signaling element overload.	Enables policy based routing and supports CAC, load balancing.
	Provide transport control for incoming sessions with QoS marking and VLAN mapping, peer-peer media release.	-
Cost optimization	Reduces service provider charges for media and voice traffic via flexible session routing policies based on a variety of metrics, including least-cost routing, observed call quality, and codec types.	Enables policy based routing and supports Time of day routing, alternate routing, TEHO (Tail end hop off), Sequenced Applications.
Regulatory compliance	Identifies emergency sessions like E911 and session replication for recording.	Supports 911 based emergency calling service.

Configuring SIP connections for enabling TLS sessions between Session Border Controller and Session Manager

This section provides an overview of installing Session Border Controller and the related steps for configuring TLS connections between Session Border Controller and Session Manager at the Aura core.
Note: Before installing Session Border Controller, you must install System Platform on the system.

The full SBC installation involves the following high level steps.

1. Configure network settings
2. Configure services and business partner logins
3. Configure VPN access
4. Configure Session Border Controller data settings
5. Review installation summary
6. Finish installation

During the configuration of Session Border Controller parameters, you need to administer Session Manager configuration details in the fields of SBC Network Data — Private (Management) Interface section.

This installs the necessary certificates and enables setting up of TLS connection between SM and SBC.

Note: For changing the transport protocol configured during the SBC installation to TLS type, you need to manually load and configure appropriate certificates. If you need to configure TLS on the public interface, or you need to manually configure it after installation, refer to the standard Acme documentation.

The identify certificate that should be loaded on SBC for the TLS connection to SM is a certificate that is manually generated using the System Manager in the Aura core.

There are two ways to request a certificate from the System Manager

1. Request for a Server Certificate – This option is used for SBCs that generate a private key locally and require an external CA to sign the corresponding certificate request. Use this option to sign a PKCS#10 certificate request generated by a SBC, and receive a certificate that can be installed on that device.
2. Request for Keystore – This option is used for SBCs that can import an identity

certificate and corresponding private key. Use this option to create an System Manager generated keystore in PEM format and save to your disc. This keystore can then be installed in a SBC.

The SM uses an identity certificate signed by the Avaya SIP Product Certificate Authority for its TLS connection to SBC. This CA certificate is pre-loaded on the SBC as /cxc/certs/sipca.pem. This is the CA that should be configured on SBC for the TLS connection to SM. SM already trusts the root CA that signs the SBC certificate described above, so no additional trusted CA configuration is needed on SM.

For details about the SBC installation procedure, refer to the book Installing and configuring Avaya Aura™ Session Border Controller.

Network Routing Policy and Trust Relationships

Network Routing Policy (NRP) in System Manager defines “SIP Entities” and “Entity Links”. The following information within NRP is used for authenticating SIP Entities by performing validation on IP/Transport Layer and TLS Layer.

1) “FQDN or IP Address” of SIP Entity.
2) “Credential name” of SIP Entity
3) “Protocol” of Entity Links. This is SIP connection transport type (TCP/TLS/UDP)
4) Trust State of the Entity Link (This defines whether the entity link is Trusted or not).

IP/Transport Layer Validation

When a SIP entity connects to Session Manager over TCP or TLS port, Session Manager validates that

1) IP address is matching one of the SIP Entities configured in NRP which have Trusted Entity Links with the Session Manager. If SIP entities are

configured as FQDN, DNS resolution is made before this verification is made.

2) Transport for the incoming SIP connection matches with one of the Entity Link associated with this SIP Entity and the Session Manager. Also the "Trust State" of the Entity Link must be configured as trusted. Session Manager does not accept connections matching untrusted Entity Links.

For SIP packets over UDP, above validation is performed for each packet. For SIP TLS connections further validation is performed as described in next section.

TLS Layer Validation

Session Manager applies the following validations for SIP TLS connections:

1) **Mutual TLS Authentication:** During the TLS handshake, mutual TLS authentication is performed where the SIP entity and Session Manager each validate the other's certificate.
2) **Additional Validation of the SIP Entity Identity Certificate:** If mutual TLS authentication is successful, further validation is performed using the SIP Entity Identity Certificate's Credential name, or the far end IP address.
    a. If the Credential Name string is empty, the connection is accepted.
    b. If the Credential Name string is not empty, the Credential Name and the IP address of the SIP Entity is searched at following places in the identity certificate provided by the SIP Entity.
        i. CN value from the subject
        ii. subjectAltName.dNSName
        iii. subjectAltName.uniformResourceIdentifier (For IP Address comparison, the IP address string is converted to SIP:W.X.Y.Z before comparison. W.X.Y.Z is the remote socket IPV4 address. Also case insensitive search is performed in this case)

Credential Name Configuration

Use cases for credential name configuration:

1) If you do not want to perform addition validation on SIP Entity identity certificate or are not using SIP TLS for connecting to the SIP entity, leave this field empty.
2) If you want to verify that a specific string or SIP Entity FQDN is present within the SIP Entity identity certificate, enter that string or SIP Entity FQDN using regular expression syntax.
3) If you want to verify that SIP entity IP Address is present within the SIP Entity identity certificate, enter the SIP Entity IP Address using regular expression syntax. Please note that IP Address is searched by default when any string is configured in the Credential name.

Please note that **Credential name** is a regular expression and follows Perl version 5.8 syntax. Here are some of the examples

1) For "www.sipentity.domain.com", use string "www\.sipentity\.domain\.com".
2) For "192.14.11.22", use string "192\.14\.11\.22".
3) You can search a subset of string or can create a wild card search. for example for searching "domain.com" as a substring, use string "domain\.com"

The regular expression processing engine of the SIP Firewall uses a Perl 5.8 compatible language, so signature patterns can be tested offline with a Perl script, or by installing the **pcre** (Perl Compatible Regular Expression) library on a separate system and verifying the proposed signature with variations of the threat message using **pcretest**.

Session Manager to SIP Telephones

Session Manager maintains two SIP TLS connections with each SIP Telephone.

1) When a SIP Telephone sends a new SIP request to Session Manager, it creates a new TLS connection (if does not have already) to Session Manager. Session Manager provides its identity certificate to the SIP Telephone for this SIP TLS connection. Session Manager does not require an identity certificate from the SIP Telephone for this TLS connection.
2) When Session Manager sends a new SIP request to a SIP Telephone, it creates a TLS connection (if one doesn't already exist) to the SIP Telephone. Session Manager verifies the identity certificate of the SIP Telephone against its trusted certificate repository.

Note: As per mechanism explained above, a SIP Telephone is required to have an identity certificate to have SIP TLS communication with Session Manager. Session Manager must have the corresponding trusted certificate to be able to verify telephone's identity certificate.

For Personal Profile Manager (PPM) connections SIP Telephone creates a new HTTPS connection to Session Manager. As part of this TLS handshake, Session Manager provides its identity certificate to SIP Telephone. However Session Manager does not require an identity certificate from SIP Telephone.

SIP/PPM requests Authentication

Session Manager performs user authentication on the SIP and PPM (Personal Profile Manager) requests by issuing a challenge (similar to HTTP digest authentication defined by RFC 2617). Only after successful challenge/response handshake, SIP/PPM requests are processed by Session Manager. After successful authentication, Session Manager creates and inserts an identity SIP header (P-Asserted-Identity) that can be displayed by a receiving telephone for displaying the identity of the caller.

Note: For SIP requests received from SIP Entity Links that are configured as “Trusted” in NRP, Session Manager does not issue any challenges.

Authentication of Emergency calls

Session Manager provides a configurable option for emergency calls to be authenticated by Session Manager or not. This option is present within System Manager (on Session Manager main web screen).

When authentication is disabled for emergency calls, any user can make an emergency call and Session Manager does not authenticate/challenge these requests. This option leaves Session Manager vulnerable to DoS attacks as an attacker can send a large number of emergency calls. It is recommended that a rate limit rule is created in SIP Firewall to limit the # of emergency calls to an appropriate limit.

Firewall Configuration

Network Firewall Configuration

The IPTables Network Firewall is not administrable in Session Manager. As described in the previous sections, default rules are installed in Network Firewall during initial installation.

Session Manager dynamically opens and closes SIP listen ports. The SIP listen ports for the Session Manager are managed via the SIP Entity within Network Routing Policy (NRP) in Systems Manager. No additional administration steps are required for opening/closing these ports.

SIP Firewall Configuration

This section provides general guidelines for configuring the rules in the SIP Firewall. It also discusses methods to evaluate specific deployment needs to provide DoS protection without affecting valid traffic. Customers should refer to the previous section describing the SIP Firewall configuration and the Session Manager Installation Administration Guide for additional information on configuring the SIP Firewall.

Reporting

Each SIP Firewall rule has the capability to send log/alarm messages to SAL. Logging can be combined with other Actions. Logging should always be enabled for each SIP firewall rule in order to have a record of actions taken by SIP Firewall.

Logging can be used independently (with None Action) to generate log/alarms for flood tracking without dropping any packets. This can be used to understand the SIP Firewall behavior and the threshold of the Session Manager deployments.

When a rate limit or rate block rule is applied, a log is sent immediately. In addition at the end of the time period a summary log is sent to specify what was the overall packet rate sent by the offender. This can be useful information regards to whether the offender was breaching the threshold for rate limit or rate block rule by a small or big margin. This can also be useful in understanding the peak rates of the topology and adjusting the rules threshold accordingly.

Protection from SIP Flood Attacks

The SIP Firewall provides the following functionality to protect Session Manager from SIP flood attacks.

1. Flood Protection from a specific source
2. Advanced Flood Protection: A rule may be defined to detect or mitigate flood attacks within live SIP stream without the knowledge of flood source in advance. In other words, the host causing the flood need not be known when the rule is configured; a high performance database tracks all matched messages.
3. Rate Limiting: A SIP firewall rule with the “Rate Limit” action may be configured to limit the number of SIP packets above and beyond an allowed threshold.
4. Rate-Blocking: A “Rate Block” action may be configured to completely block an offending SIP source once traffic has reached a specified threshold within a given period. Traffic is then blocked until the configured timeout expires.

Threshold Configuration

Threshold configuration is important and must be used with caution. To understand the threshold of the Session Manager deployments, use Rule Action “None” and enable the Log Type. It is strongly recommended that the worst case heavy traffic situations are analyzed and the threshold covers these scenarios to avoid filtering of valid SIP traffic.

Connection Type

SIP Firewall rules can have a specific Connection Type to add a filtering criteria based on type of the connection. For example a rule can be added that is applied only for SIP UA (Telephone) connections or Trusted SIP Entity Connections (as per NRP configuration). This provides flexibility to restrict the SIP UA (Telephone) connections to a reduced traffic rate (threshold) compare to a SIP Entity Connections that may be aggregating SIP connections and need to send higher rate of SIP traffic.

Note: If there are any untrusted SIP Entities connected to the Session Manager, these are treated/filtered as SIP UA connection by SIP Firewall (if there are any rules defined and enabled in SIP Firewall with connection type as SIP UA connection). If this behavior is undesirable, specific rules can be added for the untrusted SIP Entity IP Address/port. These rules need to be defined before SIP Firewall rules for SIP UA connection (Note: SIP Firewall traverse rules in the rule list from top to bottom).

To understand how advanced flood tracking works, consider the following examples:

Flood Tracking Examples

Following examples provide detailed filtering description for flood tracking rules with Rate Limit and Rate Block actions.

Example-1

Rule Name: Block INVITE Flood from any “From-uri”

Action: Rate Block
SIP Layer Match Options: Key Type = “REQUEST-METHOD”, Value Type = String, Value = “INVITE”
IP/SIP Layer Track: “From”
Threshold:

Count:	30
Period:	10
Timeout:	900

SIP Firewall Filtering Description
The above firewall rule prevents more than 30 SIP INVITE messages, with the same “From” header URI (e.g. bad-user@example.com), being received within a 10 second time period. Once that threshold is reached, flood protection takes effect, and for the next 15 minutes (900 seconds) any messages received with bad-user@example.com as “From” header URI are dropped. After 15 minutes, SIP Firewall again unblocks INVITES with bad-user@example.com as “From” URI, until flooding is again detected. Please note that while bad-user@example.com is being blocked, SIP Firewall continues to detect flood attacks from any other source (from-URI) and blocks any additional sources as applicable.

This firewall rule can also detect a flood within a SIP trunk (SIP connection to a Gateway/proxy). This rule blocks flood coming from a single user without affecting other users in the SIP connection.

Example-2

Rule Name: Rate Limit REGISTER Flood from any IP Address from SIP UA connections

Action: Rate Limit
Log Type: Alarm
SIP Layer Match Options: Key Type = "REQUEST-METHOD", Value Type = String, Value = "REGISTER"
IP/SIP Layer Track: "Remote IP Address"
Threshold:
Count: 30
Period: 60
Connection Type: SIP UA Connection

Firewall Processing
This example demonstrates how a firewall rule can combine both SIP and IP layer parameters to detect a flood. The above firewall rule ensures that the same IP Address that belongs to a SIP UA (Telephone) does not send too many SIP REGISTER packets. Once a flood of REGISTER packets is detected from an IP Address that belongs to a SIP Telephone (e.g. IP Address 10.10.10.10 has sent 30 REGISTERs in the 10 seconds), SIP firewall drops all SIP REGISTER messages from 10.10.10.10 for the remaining period interval (50 seconds in this example). SIP Firewall also generates an alarm in the SAL specifying the source (10.10.10.10 in this example) which exceeded the threshold limit. Please note that while IP Address 10.10.10.10 is blocked by SIP Firewall, SIP Firewall continues to detect flood attacks from any other SIP UA (telephone) source (IP Address) and rate limits any additional sources as applicable.

Rule Traversal

SIP Firewall is a packet based filtering engine. The following is the precedence order for traversing the rules which are applied to each SIP message.

1. Blacklist
2. Whitelist
3. Rules

Each list above may contain more than one rule. Rules within any of the above list are traversed from top to bottom. SIP Firewall is a packet based filtering engine. Any time a packet is matched with a rule, the rule traversal is stopped and packet is either permitted or dropped as per rule action. The only exception to this is the rules defined with "None" Action.

When configuring SIP Firewall rules, ordering of the rules can play an important role on how packets are processed.

Example

Consider the following rules in the SIP Firewall Rules list.

Rule 1: Action = Rate Block, Key = Request Method, Value = INVITE, Track = Remote IP Address, Count = 5, Period = 30, Timeout = 300.
Rule 2-5: <Any rules here>
Rule 6: Permit remote IP Address =10.10.10.10
Rule 7-10: <Any rules here>

Even though Rule 6 permits all SIP Traffic from 10.10.10.10, IP Address 10.10.10.10 is subject to the threshold limit applied by Rate Block (Rule 1). If this is not the desired behavior, either Rule-6 can move before Rule-1 or use Whitelist for permitting SIP Traffic from IP Address 10.10.10.10.

Blocking SIP Signatures

A rule may be configured to perform signature detection and drop those packets matching signature. Both simple and regular-expression string searching is supported across the entire SIP header region of the message or across the full message (headers and body). A signature search can also be performed within a SIP header. A signature is created if it is known to cause harm to Session Manager or other entities linked to Session Manager.

Regular expressions are complex and must be created with caution. A rule with regular expression can be tested by first by using “None” action and enabling the Log Type. The regular expression processing engine of SIP Firewall uses a Perl 5.8 compatible language, so signature patterns can be tested offline with a Perl script, or by installing **pcre** (Perl Compatible Regular Expression) library on a separate system and verifying a proposed signature with variations of the threat message using **pcretest**

Example 1:

Rule Name: Drop Bad SIP packet
Action: Drop
Log Type: Alarm
SIP Layer Match Options: Key Type = “All SIP Header/body”, Value Type = Regular Expression, Value = <Perl Signature>

Firewall Processing
This rule will drop any SIP message which contains the matching regular expression <Perl Signature> anywhere in the SIP header or body portion.

Example-2:

Rule Name: Block OOD-REFER from Trusted Host
Action: Drop
Log Type: Yes
IP Layer options Enter Remote IP address if you wish block OOD REFER from a specific host Else Remote IP Address=”Any”

SIP Layer Match Options:

1) Key Type = “REQUEST-METHOD”, Value Type = String, Value = REFER
2) Key Type = “TO”, Value Type = Regular Expression, Value = ^((?!;[\s]*tag=).)*$

Connection Options Connection Type= “NRP Trusted SIP Entity”

Firewall Processing
This rule will drop any Out-Of-Dialog REFER Messages from a Trusted SIP Entity.

Example-3:

Rule Name: Block INVITE with fnu from Trusted Host
Action: Drop
Log Type: Yes
IP Layer options Enter Remote IP address if you wish block OOD REFER from a specific host Else Remote IP Address=”Any”

SIP Layer Match Options:

3) Key Type = “REQUEST-METHOD”, Value Type = String, Value = INVITE
4) Key Type = “TO”, Value Type = String, Value = “;avaya-cm-fnu=”

Connection Options Connection Type= “NRP Trusted SIP Entity”

Firewall Processing
This rule will drop any SIP INVITE with fnu from a Trusted SIP Entity.

Blacklist Usage

SIP Blacklist allows an easy configuration for blocking any known bad SIP elements. Blacklist is the first list processed in the rule traversal sequence. It ensures that any SIP packets matching with a Blacklist rule are dropped without consuming CPU resources.

It is recommended that any bad sources are blocked using Blacklist rule rather than creating a rule in the Rules list.

Whitelist Usage

SIP Whitelist allow an easy configuration for permitting any known good SIP elements. Any SIP packet matching a Whitelist rule is allowed immediately and no other filtering rules (within Rules list) are applied.

Whitelist shall be used for any known good SIP Elements to avoid wasting processing power for these SIP Elements and also avoid applying the restrictions by filtering rules in the Rules list. For example if an Avaya Communication Manager has a SIP connection with Session Manager, Communication Manager IP Address can be added in the White List (only if the sources coming from behind Communication Manager are also trusted and need not be processed by SIP Firewall Rules).

Administrative Accounts

Management and maintenance of Avaya Session Manager is done through the System Manager console, however maintenance and troubleshooting often require operating system level access to the Session Manager server. The following sections describe local accounts in the Session Manager server and administrative accounts in System Manager.

Session Manager Local host accounts

At installation the Avaya Services accounts described in the Avaya Services Accounts table above as well as the following accounts are created:

Account	Service Level	Privileges
CDR_User		The CDR_User and password is used by an external Call Detail Recording processing adjunct for connecting to Session Manager and to transfer the generated CDR files. These CDR systems can be used to generate billing or other call analysis reports. The CDR_User password is customer configurable.
Customer or ‘cust’	Same as craft	Optional customer account

		that's enabled by the customer at installation. The cust login has the same permissions as 'craft' but does not have root permissions.

Access to the Session Manager 'root' account is disabled by default.

Session Manager Administrative accounts

Avaya Session Manager administration is done through Avaya Aura™ System Manager. System Manager supports user authentication via its UCM framework. Both Basic (default) and Enterprise Authentication types are supported via this infrastructure. Customers who wish to configure SMGR to support external authentication can do so via its use of three authentication authorities,

- local users
- external RADIUS users
- external LDAP users

The authentication scheme policy determines the order that the three authentication authorities are used. Please refer the System Manager Administrative Guide for further information on how various external authentication schemes can be configured. For users that are managed via System Manager, called local users, the password policy is enforced at user creation and during password change. Customers who wish to use a centralized identity or directory server to store and maintain administrator account (login) credentials external to System Manager may do so through the configuration of the IAM framework. Avaya's support of external Identity and Access Management (IAM) services allows customers with compatible authentication servers to:

- Centralize control of enterprise logins and passwords used by System Manager
- Enforce password aging and complexity requirements
- Enforce password re-use requirements

User Profile Manager-based account authentication

System Manager is configured by default to support only accounts defined within the User Profile Manager (UPM) subsystem delivered with System Manager. To avoid unintentional lockout to the system you should administer at least one local UPM account on IMSM to avoid administrator lockout should access to the external IAM server become unavailable. Note the UPM subsystem does not support the password aging, complexity and re-use requirements that are available via external IAM services, so Avaya recommends that external IAM services be used when such requirements exist.

Configuring System Manager to use an external AAA server

Refer to the Administering Avaya Aura® System Manager 6.1 for instructions on configuring System Manager to authenticate customer accounts to an external AAA server.

Authorization-related services in System Manager

Role based access control (RBAC) allows organizations to assign server, gateway, and application access permissions based on a user's job function, or role. RBAC within Systems Manager consists of two services: an Authorization service and RBAC Management service. The RBAC management service allows customers to configure and assign roles and permissions. The Authorization service is used to enforce the authorization based on the roles and permissions defined in Systems Manager.

Account administration recommendations

For login account management, take into consideration the following recommendations and constraints:

- Administer at least one local host account in all servers so that access is possible even if external AAA servers are not reachable.
- Take care in enabling password aging for accounts authenticated through external servers, for example RADIUS accounts, that do not support changing of password by users using application server.
- Since system access by Avaya Services is occasional yet often required to maintain maximum uptime, do not enable password aging for Avaya Services accounts.
- Simple Authentication and Security Layer (SASL) authentication is not supported.

Network integration

Session Manager’s use of DNS

The Session Manager SIP Entity table, Entity Link table, Local Hostname IP table, and enterprise DNS records are used to determine the destination to route to.

An administrator can specify for a SIP entity whether or not to use DNS resolution per SIP: Locating SIP Servers RFC 3263. If the administrator specifies the use of DNS, then the transport and port information are determined using DNS information. DNS information is determined by first looking up the hostname in the provisioned local hostname resolution table and then, if no match was found, using enterprise DNS. DNS resolution is generally used if it is desirable to route to a large set of servers serving an enterprise. An example hostname would be "sip.avaya.com" using SRV and record lookups, sip.avaya.com maps to a number of specific servers potentially using different ports, transports, weight, and priorities. If the administrator does not specify the use of DNS, the transport and port information are determined using the data administered in the Entity Link table and DNS is used to obtain the set of IP addresses for the FQDN. In either case, a sips: URI forces the use of a secure transport.

Operational Security

Operational security

Backup and Restore

Backup and Restore of Session Manager configuration is performed from the System Manager console.

Backup

The Session Manager backup operation from the System Manager console creates a backup image of the System Manager database where much of the Session Manager data persists. Customers are responsible for the security of their backup data.

Restore

The Session Manager restore operation is initiated from the System Manager console. The restore operation restores the System Manager database with the configuration data contained in the backup data.

See the book **Administering Avaya Aura™ Session Manager** for more details on Backup and Restore operations.

Logging and Alarming

Session Manager and System Manager Applications contain agents that collect logging and alarming events. Integrated Management System Manager communicates with these agents to retrieve, process, and centralize the administration of the events.

The logging and alarm event displays show details such as event timestamp, severity, description, and originating host/application. Log messages follow the Avaya Common Logging Format. Alarms can be administered (i.e. cleared, acknowledged) and exported to a spreadsheet.

Configuration options include defining severity level at which an application's events will be collected, log file sizes and locations, and event data retention policy.

What security-related events are logged?

Security events are related to the following actions or activities:

- Attempted login or log off, whether successful or not
- Establishment of a new administrative access session regardless of port of entry
- Assignment of a user profile to an administrative session
- Display, list, change, add or delete of a user profile
- Any administrative access to local user accounts (view, add, change, delete)
- Failed attempt to access an object or execute an action to which the user does not have access
- Any access to the security control configuration of the server: logging configuration, the PAM configuration, the SIP firewall configuration.
- Trust management activities, as in certificate administration
- Result of request by application to open or close a pinhole in network firewall
- A change in SIP firewall mitigation policy
- SIP firewall identifies that SIP message has matched one of its rules (may be information only or notification that mitigation action in effect)

Note: You cannot disable logging of security events.

There is no special facility reserved for security-related events.

Where is security information logged?

Security information is logged in or notified through:

- Sysco security log
- Miscellaneous logs that track security-related information:
    - Linux access security log
    - Platform command history log
    - HTTP/web access log
    - IP events
- Session Manager logs
- Web Services application logs
- SIP A/S application logs
- System Manager central log

There are currently no SNMP Mobs. SNMPv3 is not currently supported, so exercise caution when choosing/sharing the community string name.

<u>Avaya Security Advisories</u>

What is an Avaya Security Advisory

The Avaya Product Security Support Team (PSST) is responsible for the following:

- Managing Avaya product vulnerabilities and threats
- Maintaining information posted at http://support.avaya.com/security.
- Performing security testing and auditing of Avaya's core products
- Resolving security-related field problems in support of Avaya Global Services
- Managing the securityalerts@avaya.com mailbox.

As a result, the PSST actively monitors security issues related to the following topics:

- Avaya products
- Products that are incorporated into Avaya products
- General data networking and telecommunications, as identified by government agencies

When a security vulnerability is identified, the PSST determines susceptibility of Avaya products to those vulnerabilities and assigns one of four risk levels: High, Medium, Low, and None (see How to interpret an Avaya Security Advisory).

Depending on the category of risk, the PSST creates an Avaya Security Advisory to notify customers of the vulnerability.

Depending on the vulnerability and its risk level, the advisory might include a recommended mitigation action, a recommendation regarding the use of a 3rd-party-provided patch, a planned Avaya software patch or upgrade, and/or additional guidance regarding the vulnerability.

How do I get Avaya Security Advisories?

Avaya Security Advisories are posted on the Security Support Web site at http://support.avaya.com/security. Customers can register at Avaya's support web site to receive email notifications of Avaya security advisories. The advisories are distributed in a time frame as indicated in the following table:

Avaya's vulnerability classification	**Target intervals between assessment and notification**
High	Within 24 hours
Medium	Within 2 weeks
Low	Within 30 days
None	At Avaya's discretion

Customers can sign up to receive advisories by email on the Avaya Security Support Web site by following these steps:

1. Browse to http://support.avaya.com.
2. If you do not have an account, go to http://sso.avaya.com and 'click' on "Register Now" and follow the instructions. To register, you need an Avaya SSO login and a Sold To number.
3. Once you have set up an SSO user ID and password you can enroll for the E-Notifications you wish to receive.

4. To do that, click on the "My E-Notifications" link, which can be accessed from the home page for the Web site (http://support.avaya.com) or by selecting the "My E-Notifications" link under "Online Service Manager."
5. To enroll for the E-Notifications you wish to receive, click on "Add New E-Notifications."
6. If you select one of the five radio buttons on the top portion of the page, you will receive e-mail notifications when new content is added or revised for all Avaya products under the following content areas:
   - Product Correction Notices
   - Security Advisories
   - Product Support Notices – High Priority
   - End of Sale Notices
   - Services Support Notices

7. To receive an e-mail notification for a particular product, select the radio button next to "Choose from the Product list" and then select the product for which you are interested in receiving notifications. You will then be asked to select the release and content types from available release/content type combinations for the selected product.

If you have any questions about enrolling for My E-Notifications on the Avaya Customer Self Service Web site, please send an e-mail message to support@avaya.com.

How to interpret an Avaya Security Advisory

Precise definitions that the Avaya Product Security Support Team (PSST) follows in classifying vulnerabilities relative to their potential threat to Avaya products is in Avaya's Security Vulnerability Classification document (https://support.avaya.com/css/P8/documents/100066674)
The following table summarizes the three main categories.

Avaya's security vulnerability classification

Vulnerability classification	Criteria for classification
High	The product is vulnerable to: • Attacks from a remote unauthenticated user who can easily access high-level administrative control of a system or critical application without interaction with a user of the product beyond standard operating procedures. • Attacks from remote unauthenticated user who can easily cause the system or a critical application to shutdown, reboot, or become unusable without requiring interaction with a product user. For example, see the advisory at http://support.avaya.com/css/P8/documents/100062710

Medium	The product does not meet criteria for high vulnerability, but is vulnerable to: • Attack from a user who can access a user account, and access does not directly require the privileges of a high-level administrative account. • The system and/or critical application shutting down, rebooting, or becoming unusable, and an existing administrative or local account are used for this attack. • Attack from a user who can access a local user account from which higher-level privileges are available. For example, see the advisory at http://support.avaya.com/css/P8/documents/100064239
Low	The product does not meet criteria for medium or high vulnerability, but is vulnerable to: • Compromise of the confidentiality, integrity, or availability of resources, although any compromise is difficult or unlikely without non-standard direct user interaction. • Non-critical applications shutting down, rebooting, or becoming unusable. For example, see the advisory at http://support.avaya.com/css/P8/documents/100064944
None	A related third-party product has a vulnerability but the affected software package(s), module(s), or configuration(s) are not used on an Avaya product and there is therefore no vulnerability. For example, see the advisory at http://support.avaya.com/css/P8/documents/100064240

How an advisory is organized

Overview

The overview provides a description of the vulnerability. For operating system or third-party software, a link is also provided for quick access to a Web site for more information. The linked information provides:

- A description of the risk
- Instructions on how to correct the problem, which might include:
  - Installing an update
  - Revising administration of the product
- A description of what additional security fixes, if any, are included in the update.

Avaya Software-Only Products

For Avaya software only products, the advisory provides a listing of the specific Avaya products that use, but are not bundled with, operating system software that might be vulnerable. Information includes:

- The product version affected

- Possible actions to take to reduce or eliminate the risk

Avaya System Products

For Avaya system or turnkey products, the advisory provides a listing of the specific Avaya products that are vulnerable or are bundled with operating system software that might be vulnerable. Information includes:

- The level of risk
- The product version affected
- Possible actions to take to reduce or eliminate the risk

Recommended Actions

The advisory provides a list and description of steps to take to remove the vulnerability. The steps might include installing a security update, administering a security feature, or performing a software upgrade. For operating system and third-party software, the recommended actions are normally identified in detail through the Web site links in the security advisory.

Software/Firmware updates

How Avaya delivers security updates

Generally, Avaya makes security updates available on or through the Avaya Security Web site at http://support.avaya.com/security. In addition, Avaya incorporates security updates, if applicable, in subsequent software release packages.

Based on the classification of vulnerability and the availability of a vendor-supplied update, Avaya makes a best effort attempt to provide remediation actions based on the following target intervals:

Vulnerability	Target remediation intervals
High	If Avaya needs to develop a software update, the Avaya Security Advisory provides a timeline for availability of the update. Avaya incorporates the fix into a separate service pack or update (30 days maximum delivery time). If a software patch is available for installation or another action is recommended, the Avaya Security Advisory describes the actions.
Medium	If Avaya needs to develop a software update, Avaya includes the update in the next major release that can reasonably incorporate the update. If no new major releases are scheduled for a product, and Avaya is providing maintenance support, Avaya incorporates the fix into a separate service pack or update (1 year maximum delivery time).

	If a software patch is available for installation or another action is recommended, the Avaya Security Advisory describes the actions.
Low	If Avaya needs to develop a software update, Avaya includes the update in the next major release that can reasonably incorporate the update. If no new major releases are scheduled for a product, and Avaya is providing maintenance support, Avaya incorporates the fix into a separate service pack or update (1 year maximum delivery time). If a software patch is available for installation or another action is recommended, the Avaya Security Advisory describes the actions.
None	No remediation actions are required.

Avaya product development staff incorporates a third-party update into its software in one of three ways:

- Avaya simply bundles the specific update or the new release of the affected software with the Avaya Session Manager software such that the security-related updates are automatically incorporated into the Avaya product operation.
- Avaya modifies the Session Manager software so that the specific update or the new release of the affected software is appropriately incorporated into the Session Manager operation.
- Avaya modifies the specific update or the new release of the affected software so that the security-related updates are automatically incorporated into the Session Manager operation.

When Avaya incorporates one or more security fixes into its software, the fixes might be delivered in one of three forms:

- A security update: includes operating system and/or third-party software security fixes.
- An Avaya software update: includes software security fixes to the Avaya application software.
- An Avaya full release of software: includes all software for the Avaya product, including software security fixes to the Avaya application software and/or security fixes for the operating system and third-party fixes.

Validating a security update

When Avaya determines that a third-party security update applies to one or more of its products, Avaya product development tests the update on the affected current products to ensure there are no adverse affects to the published functionality of the products. In addition, when third-party updates are included in new software releases, the products are thoroughly tested.

Avaya-generated security updates are likewise tested on all affected products prior to release. Avaya security updates are likewise tested before incorporation into subsequent releases. Testing meets requirements of internal Avaya testing standards, including testing for the following:

- Denial of Service

- Encryption standards
- Certificate management
- Audits and logging
- Access control

Regulatory issues

Regulatory Issues

Considerations for customers who must comply with the Sarbanes-Oxley Act

Note: This law applies to U.S. customers only. Customers should rely on appropriate legal counsel and outside auditors for interpretation of the act’s requirements. Suggestions in this document are not to be construed as a substitute for legal advice or a definitive list of all possible legal considerations.

The Sarbanes-Oxley Act of 2002 is a federal law enacted in response to a number of accounting scandals involving major U.S. corporations. A key requirement of the act is that public companies evaluate and disclose the effectiveness of their internal controls as they relate to financial reporting. One major area of internal control consists of information technology controls. As a result, the Sarbanes-Oxley Act holds chief information officers responsible for the security, accuracy and the reliability of the systems that manage and report the financial data.

To the extent that a company uses data collected or transmitted by Session Manager as part of its overall cost or revenue reporting and financial management, the company can use its security-related features to secure the data. Use of these features can further demonstrate the company’s good faith data management and reporting.

Session Manager security features also help prevent unauthorized access to the customer’s network, in general.

Features related to data security and documented in more detail in other sections of this document are:

Feature	How related to Sarbanes-Oxley	Where documented
Encryption	Transmitted data is protected from packet-sniffing and eavesdropping	See: Avaya Encryption Overview in this document
Access control	Access to data is protected from unauthorized personnel	See: Role-Based Access Control in this document.
Authentication	Access to the system is restricted by login/password.	See: Administrative Accounts in this document.
Logging	Security-related events are logged	See: Operation Security

Feature	How related to Sarbanes-Oxley	Where documented
		Logging and Alarming in this document.
Backup of data	Data saved on backup media or backup server.	See: See Operational Security Backup and Restore in this document.

Considerations for customers who must comply with the Graham-Leach-Bliley Act

> **Note:** This law applies to U.S. customers only. Customers should rely on appropriate legal counsel and outside auditors for interpretation of the act's requirements. Suggestions in this document are not to be construed as a substitute for legal advice or a definitive list of all possible legal considerations.

The Gramm-Leach-Bliley Act (GLB) requires financial institutions to disclose privacy policies regarding customer data. This disclosure must describe the ways the institution may use and disclose private information.

Where indicated in their policy, financial institutions must protect the privacy of their customers, including customers' nonpublic, personal information. To ensure this protection, the Graham-Leach-Bliley Act mandates that all institutions establish appropriate administrative, technical and physical safeguards.

Session Manager data to which the Graham-Leach-Bliley Act might apply includes customer names and telephone numbers, called and calling number data, and abbreviated dial lists.

Use of the following key features can protect customer privacy and demonstrate the company's compliance with the interagency guidelines supporting the Graham-Leach-Bliley Act.

Feature	How related to Graham-Leach Bliley Act	Where documented
Encryption	Transmitted and stored data is protected from unauthorized individuals.	See: Avaya Encryption Overview in this document
System access control	Access to data is protected from unauthorized personnel.	See: Role-Based Access Control in this document.
Authentication	Access to the system is restricted by login/password.	See: Administrative Accounts in this document.
Backup of data	Protection against destruction, loss, or damage of customer information due to potential environmental hazards or technological failures; protected by	See: Operation Security Backup and Restore in this document.

Feature	How related to Graham-Leach Bliley Act	Where documented
	encryption and key	

Considerations for customers who must comply with HIPAA

> **Note:** This law applies to U.S. customers only. Customers should rely on appropriate legal counsel and outside auditors for interpretation of the act’s requirements. Suggestions in this document are not to be construed as a substitute for legal advice or a definitive list of all possible legal considerations.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires health care providers to disclose to health care recipients the ways in which the institution may use and disclose private information. HIPAA also requires health care providers to protect the privacy of certain individually identifiable health data for health care recipients.

Session Manager data to which HIPAA might apply includes customer names and telephone numbers, and called and calling number data.

Use of the following key features can protect patient privacy and demonstrate the health care provider’s compliance with HIPAA.

Feature	How related to HIPAA	Where documented
Encryption	Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate	See: Avaya Encryption Overview in this document
System access control	Implement technical policies and procedures for electronic information systems that maintain electronically-protected health information to allow access only to those persons or software programs that have been granted access rights.	See: Role-Based Access Control in this document.
Authentication	Implement procedures to verify that a person or entity seeking access to electronically-protected health information is the one claimed.	See: Administrative Accounts in this document.
Backup of data	Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronically-protected health information.	See: Operation Security Backup and Restore in this document.

Considerations for customers who must comply with the Payment Card Industry DSS

> **Note:** This standard global merchants and card processing service providers. Customers should rely on appropriate legal counsel and requirements of their card issuers for interpretation of the standard's requirements. Suggestions in this document are not to be construed as a substitute for legal advice or a definitive list of all possible legal considerations.

The PCI Data Security Standard (DSS), a set of comprehensive requirements for enhancing payment account data security, was developed by the founding payment card brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. Inc. International, to help facilitate the broad adoption of consistent data security measures on a global basis. This comprehensive standard is intended to help organizations proactively protect customer account data.

Communication Manager data to which PCI might apply includes customer cardholder data such as account numbers, CCV codes, and card holder names. To the extent that a company uses data collected or transmitted by Communication Manager as part of its overall card payment processing, the company can use security-related features of Communication Manager to secure the data and support PCI compliance. When Communication Manager is deployed in a customer network environment that touches card processing or cardholder data, all components of Communication Manager may be considered in scope for PCI assessment purposes.

Use of the following key features can protect cardholder information and demonstrate the merchant and service provider compliance with PCI:

Feature	How Related to PCI	Where Documented
Encryption	*Protect cardholder data;* *encrypt across open, public networks*	See:
System Access Control	*Strong access control;* *Restrict access by business need to know*	See:
Authentication	*Strong access control;* *Assign unique ID to each user*	See:
Logging	*Monitor and Test:* *Track and monitor all access*	See:
Backup of Data	*Protect cardholder data:* *Protect stored cardholder data*	See: ✍ Secure backups of Communication Manager data and translations on page 164
Secure Administration	*Secure Network;* *Do not use vendor-supplied defaults*	See:

Firewall Settings	*Secure Network;* *Firewall configuration to protect card holder data*	See: - Administering Settings Firewall on page 67

Considerations for customers who must comply with CALEA

> **Note:** This law applies to U.S. customers only. Customers should rely on appropriate legal counsel and outside auditors for interpretation of the act's requirements. Suggestions in this document are not to be construed as a substitute for legal advice or a definitive list of all possible legal considerations.

In response to concerns that emerging technologies such as digital and wireless communications are increasing the difficulty for law enforcement agencies to execute authorized surveillance, Congress enacted the Communication Assistance for Law Enforcement Act (CALEA) in 1994. CALEA is intended to preserve the ability of law enforcement agencies to conduct electronic surveillance by requiring that telecommunications carriers and manufacturers of telecommunications equipment modify and design their equipment, facilities, and services to ensure that the systems support the necessary surveillance capabilities of law enforcement agencies.

In an order effective September 23, 2005, the FCC concluded that CALEA applies to facilities-based broadband Internet access providers and interconnected VoIP service providers. To the extent that CALEA applies to Avaya offerings, such offerings have achieved compliance with the applicable CALEA requirements. In the event that an Avaya customer is subject to CALEA requirements, there are various third-party products, including Session Border Controller products that claim to provide or facilitate CALEA compliance. Examples of these products are:

- NexTone
- AcmePacket

In addition, Session Manager characteristics that can aid in CALEA compliance are the following:

- Standard architectures. For example:
  - Uses Open Systems Interconnection (OSI) standards for network communications. Therefore, transmissions are interceptable for surveillance tools established to work with the OSI standards.
  - Calls are always divided into call control signaling and voice or bearer signaling. This simplifies the task of determining what data to surveil.
- Authenticity and integrity assurance of the calls being surveilled through its encryption and authentication capabilities.
- Call Detail Records, which records called numbers, and other call data that might be useful to law enforcement.

Finally, Session Manager offers the service observing feature, which allows monitoring of calls with or without awareness of the parties on the call.

Considerations for customers who must comply with FISMA

> **Note:** This law applies to U.S. customers only. Customers should rely on appropriate legal counsel and outside auditors for interpretation of the act's requirements. Suggestions in this document are not to be construed as a substitute for legal advice or a definitive list of all possible legal considerations.

The Federal Information Security Management Act of 2002 provides for development and maintenance of minimum controls required to protect Federal information and information systems. Telecommunications systems and commercially-developed information security systems are included in the systems referenced under this act.

As a result, in most cases, government agencies can use Avaya's security-related features to secure telecommunications data. Session Manager security features can also help prevent unauthorized access to the customer's network, in general.

Features related to system security and documented in more detail in other sections of this document are:

Feature	**How related to FISMA**	**Where documented**
Encryption	Transmitted data is protected from packet-sniffing and eavesdropping and other unauthorized access.	See: Avaya Encryption Overview in this document
System access control	Access to data is protected from unauthorized personnel	See: Role-Based Access Control in this document.
Authentication	Access to the system is restricted by login/password.	See: Administrative Accounts in this document.
Logging	Security-related events are logged	See: Operation Security Logging and Alarming in this document.
Firewall	Access to network is protected	See: DoS Resistance in this document.
Backup of data	Data saved on backup media or backup server. Protected by encryption and key	See: Operational Security: Backup and Restore in this document.
Toll fraud prevention	Unauthorized use of long-distance is prevented	See: Avaya's Toll Fraud and Security Handbook (555-025-600) ttp://support.avaya.com

Considerations for customers who want to comply with ISO 17799

ISO 17799 of the International Standards Organization, "Information technology - Security techniques - Code of practice for information security management," is an internationally-accepted standard of good practice for information security. ISO 17799 suggests a well structured set of controls to address information security risks, covering confidentiality, integrity and availability aspects. None of the suggested controls is mandatory, however, an organization wishing to be in compliance should show a security strategy that explains the decision not to implement key controls.

ISO 17799 addresses the following broad categories of data security management:

ISO 17799 Security Guidelines	**Security features and processes**
Ensure that applications process information correctly	
Use validation checks to control processing	Use the System Log and Maintenance Alarm and Event logs. See: Operational Security – Logging and Alarming.
Validate data input into your applications	See: System Manager User's Guide.
Protect message integrity and authenticity	See: Avaya Encryption Overview on the use of Hashed Message Authentication Codes (HMAC) to guarantee message integrity.
Validate your applications' output data	Use audits and status reports to verify output. See: Operational Security Logging and Alarming in this document.
Use cryptographic controls to protect your information	See: Avaya Encryption Overview in this document.
Protect and control your organization's system files	
Control the installation of operational software	Session Manager requires the appropriate access control in order to install software. See the Session Manager Installation and Administration Guide.
Control the use of system data for testing	Avaya uses internal ISO-certified testing processes for software.
Control access to program source code	Session Manager source code is not accessible outside of Avaya. The Red Hat Linux operating system is also restricted. See

ISO 17799 Security Guidelines	**Security features and processes**
Control development and support processes	
Establish formal change control procedures	Avaya uses internal ISO-certified change control processes for software.
Review applications after operating system changes	Avaya uses internal ISO-certified test procedures after operating system changes.
Restrict changes to software packages	Avaya includes only the Linux software packages it needs. Avaya software is proprietary, and Linux software cannot be changed on an installed system. Standard program binaries are normally installed with write permissions only to the super-user (root) and cannot be modified.
Prevent information leakage	Session Manager does not have antivirus, antiworm, or antitrojan software, Avaya does not recommend using 3rd party antivirus software. For more information, see Planning against viruses and worms and other malicious code.
Control outsourced software development	Avaya software, if outsourced, is developed according to Avaya's ISO-certified processes.
Control your technical system vulnerabilities	Session Manager offers many features and processes to protect the customer's communications network.

Considerations for non-US customers who must comply with regulations

Any specific country might have unique regulations that raise compliance issues for Avaya products. For example, countries such as Switzerland and Liechtenstein have Banking Secrecy laws that require a financial organization to inform a customer when the customer's identity has been revealed or that information that might reveal the customer's identity has been released. Such revelations can have negative affect on a bank's business. Therefore, a bank's communications services must be secure to prevent unauthorized access to data such as names, telephone numbers, account codes, and so on. To that end, Session Manager, through its authentication processes, access control, and encryption methods, can protect call detail records, as well as the calls to customers. In this way, Avaya can help a customer comply with banking secrecy laws and protect the integrity of its business. Avaya also offers these security features to protect administered data that might reveal a customer's identity, as might be the case, for example, if a customer's IP address or phone number is contained within the firewall rules established for the product.

Basel II

Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework is a comprehensive set of banking standards compiled by the Basel Committee on Banking Supervision. The national banking overseers in many European countries seek to implement country-specific laws and procedures to meet the Basel II standards. To measure risk levels for a banking standards, Basel II mandates tracking of loss event data, which includes financial systems hacking, theft of data, and impersonation. To this end, Avaya systems offer a number of security features, such as those described in the previous paragraph, to minimize loss event data, and therefore, risk level measurements.

For any country in which Session Manager is sold, there might be a need to inform customers about Session Manager support for governmental regulations. In this case, the sales engineer or account executive should engage an Avaya legal officer, security specialist, or a compliance specialist to determine the specific ways in which Session Manager might help the customer comply with regulations.

Common Criteria

The Common Criteria for Information Technology Security Evaluation (CC) and the companion Common Methodology for Information Technology Security Evaluation (CEM) are the technical basis for an international agreement, the Common Criteria Recognition Agreement (CCRA), which ensures that:

Products' security properties are evaluated by competent and independent licensed laboratories to determine their assurance.

Supporting documents that are used within the Common Criteria certification process define how the criteria and evaluation methods are applied when certifying specific technologies.

The certification of the security properties of an evaluated product can be issued by a number of Certificate Authorizing Schemes, with this certification being based on the result of their evaluation.

These certificates are recognized by all the signatories of the CCRA.

The CC web portal (http://www.commoncriteriaportal.org/index.html) reports the status of the CCRA, the CC and the certification schemes, licensed laboratories, certified products and related information, news, and events.

Appendix A: Physical interfaces and associated network services

Avaya Session Manager is available on Avaya’s S8510 Server platform. For information on the S8510 server and its interfaces, see *Installing the Avaya S8510 Server Family and its Components* (03-602918).

Appendix B: Session Manager Network services

All the ports & protocols used by Session Manager are documented in the "Avaya Aura Session Manager Port Matrix". This document is available to Avaya Direct, Business Partners and Customers using InSite search which is available at the following main Support site
http://support.avaya.com/selfservice/microsites/microsite.do

After logging in via SSO Avaya Direct/BP/Customer can search for "Avaya Aura Session Manager Port Matrix".

Appendix C: Additional security resources

Documents mentioned in this security guide

This Avaya Session Manager security guide mentions the documents that are listed in the table below:

Avaya Session Manager documents in this security guide

Document title	Document number
Administration for Network Connectivity for Avaya Communication Manager	555-233-504
Administering Avaya Aura® Session Manager	03-603324
Administering Avaya Aura® System Manager	-
Installing the Avaya S8510 Server Family and its Components	03-602918

Security documents on the Avaya support site

Security-related documents that complement this security guide are listed in the table below:

Avaya Session Manager documents on the Avaya support site

Document title	Link
Avaya Enterprise Services Platform Security Overview	Requires non-disclosure agreement
Avaya Interactive Response Security	http://support.avaya.com/elmodocs2/ir/r2_0/print_Security.pdf
Avaya's Security Vulnerability Classification	http://support.avaya.com/elmodocs2/security/security_vulnerability_classification.pdf
Avaya's Toll Fraud & Security Handbook	http://support.avaya.com/selfservice/microsites/microsite.do

Appendix D: Default Certificates

Following is the Trusted/CA certificate of the issuer used to generate the default Identity certificate for SIP-TLS:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 0 (0x0)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US, O=Avaya Inc., OU=SIP Product Certificate
Authority, CN=SIP Product Certificate Authority
        Validity
            Not Before: Jul 25 00:33:17 2003 GMT
            Not After : Aug 17 05:19:39 2027 GMT
        Subject: C=US, O=Avaya Inc., OU=SIP Product Certificate
Authority, CN=SIP Product Certificate Authority
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:dc:3b:2b:72:c7:b6:11:cd:3e:d5:60:9a:2f:f0:
                    51:9e:ea:0d:46:27:48:7e:e1:8e:d8:67:3c:e6:80:
                    73:ea:a6:09:fe:da:39:6e:42:2d:4d:34:79:62:30:
                    b6:d8:2e:7a:ef:7f:ab:37:f9:7f:f3:87:b6:4d:0f:
                    6b:72:ac:a6:4c:09:86:88:f0:55:fa:5f:7b:58:4c:
                    e3:59:f4:4a:d3:62:78:12:24:2a:4b:78:2b:a3:73:
                    ea:a0:b7:54:a6:46:cc:9a:d7:ed:45:f6:2e:63:be:
                    b1:71:a0:eb:91:6f:93:74:e5:8b:f7:70:8f:39:48:
                    52:f0:ee:41:2b:e3:57:10:0e:fb:21:44:15:99:7e:
                    8e:ab:7f:76:c1:26:39:6a:45:31:dc:e7:21:9b:5d:
                    77:84:b3:e2:6b:b4:8b:de:10:21:41:d9:0f:f0:dc:
                    48:3f:19:b7:16:1a:13:f5:ba:a1:ea:38:f1:fb:e9:
                    a3:4c:63:24:0f:18:cc:c3:06:da:42:7c:68:7b:1e:
                    40:fb:8e:44:f6:12:5f:80:88:12:89:cb:47:0e:72:
                    3d:b6:f8:02:9b:2e:f8:79:6d:f7:c9:31:37:02:3d:
                    7d:81:6b:1d:82:0f:62:35:ba:c4:3e:a2:c4:c6:f8:
                    57:6f:ba:14:41:c7:e5:8f:a8:13:96:b1:0d:30:44:
                    a1:8d
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Certificate Policies:
                Policy: 2.16.840.1.114187.7.2.1.1
                  CPS: mailto:sipca@avaya.com;

            X509v3 Subject Key Identifier:

A0:82:07:29:5C:3A:A0:C4:29:B8:3D:C3:1D:B9:06:55:13:BE:56:2A
            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:1
            X509v3 Key Usage:
                Certificate Sign, CRL Sign
            X509v3 Authority Key Identifier:

keyid:A0:82:07:29:5C:3A:A0:C4:29:B8:3D:C3:1D:B9:06:55:13:BE:56:2A
```

```
                DirName:/C=US/O=Avaya Inc./OU=SIP Product Certificate
Authority/CN=SIP Product Certificate Authority
                serial:00

    Signature Algorithm: sha1WithRSAEncryption
        60:3e:b6:92:b6:8f:be:f8:a0:05:32:d5:12:19:59:b8:8e:c6:
        e4:9d:6c:1a:cd:1e:72:17:19:6d:5a:b8:28:a2:c3:0d:fb:5b:
        77:e7:50:04:25:e7:75:0c:2b:d4:5a:26:db:7d:2c:a5:87:5d:
        cf:37:36:0b:85:22:25:98:a3:d1:f7:c2:d5:43:83:f9:97:6e:
        82:da:cb:89:3d:ac:9e:11:45:fc:ef:00:c2:1d:ef:1e:34:d1:
        bd:de:f9:79:e1:4e:1a:40:3b:a6:f7:c1:52:4d:19:58:8d:d4:
        a2:2f:d4:77:b6:b2:8b:3a:28:98:94:b0:44:d6:82:47:04:63:
        e2:17:34:57:81:cd:17:54:65:97:31:f0:2a:b8:d4:34:d6:9c:
        ca:aa:ee:c4:4f:4f:40:5a:c6:1b:51:2e:1c:f8:9e:6d:75:89:
        3d:9d:89:37:e5:8d:56:b4:ac:0e:cf:c3:12:83:09:01:da:77:
        32:d6:b2:3a:22:e5:af:2c:05:1d:77:d0:4a:70:16:06:2d:23:
        15:ba:55:46:8e:5d:ce:8b:45:77:e7:1c:4d:a3:22:0a:43:df:
        11:3c:86:fd:45:c3:04:ce:18:88:92:15:0e:92:d9:9e:60:77:
        bd:05:89:fc:12:7e:fa:ab:9a:0e:5c:7d:02:68:84:0e:95:df:
        55:a2:87:7f
```

```
-----BEGIN CERTIFICATE-----
MIIEnTCCA4WgAwIBAgIBADANBgkqhkiG9w0BAQUFADB6MQswCQYDVQQGEwJVUzET
MBEGA1UEChMKQXZheWEgSW5jLjEqMCgGA1UECxMhU0lQIFByb2R1Y3QgQ2VydGlm
aWNhdGUgQXV0aG9yaXR5MSowKAYDVQQDEyFTSVAgUHJvZHVjdCBDZXJ0aWZpY2F0
ZSBBdXRob3JpdHkwHhcNMDMwNzI1MDAzMzE3WhcNMjcwODE3MDUxOTM5WjB6MQsw
CQYDVQQGEwJVUzETMBEGA1UEChMKQXZheWEgSW5jLjEqMCgGA1UECxMhU0lQIFBy
b2R1Y3QgQ2VydGlmaWNhdGUgQXV0aG9yaXR5MSowKAYDVQQDEyFTSVAgUHJvZHVj
dCBDZXJ0aWZpY2F0ZSBBdXRob3JpdHkwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQDcOytyx7YRzT7VYJov8FGe6g1GJ0h+4Y7YZzzmgHPqpgn+2jluQi1N
NHliMLbYLnrvf6s3+X/zh7ZND2tyrKZMCYaI8FX6X3tYTONZ9ErTYngSJCpLeCuj
c+qgt1SmRsya1+1F9i5jvrFxoOuRb5N05Yv3cI85SFLw7kEr41cQDvshRBWZfo6r
f3bBJjlqRTHc5yGbXXeEs+JrtIveECFB2Q/w3Eg/GbcWGhP1uqHqOPH76aNMYyQP
GMzDBtpCfGh7HkD7jkT2El+AiBKJy0cOcj22+AKbLvh5bffJMTcCPX2Bax2CD2I1
usQ+osTG+FdvuhRBx+WPqBOWsQ0wRKGNAgMBAAGjggEsMIIBKDA/BgNVHSAEODA2
MDQGC2CGSAGG/AsHAgEBMCUwIwYIKwYBBQUHAgEWF21haWx0bzpzaXBjYUBhdmF5
YS5jb207MB0GA1UdDgQWBBSgggcpXDqgxCm4PcMduQZVE75WKjASBgNVHRMBAf8E
CDAGAQH/AgEBMAsGA1UdDwQEAwIBBjCBpAYDVR0jBIGcMIGZgBSgggcpXDqgxCm4
PcMduQZVE75WKqF+pHwwejELMAkGA1UEBhMCVVMxEzARBgNVBAoTCkF2YXlhIElu
Yy4xKjAoBgNVBAsTIVNJUCBQcm9kdWN0IENlcnRpZmljYXRlIEF1dGhvcml0eTEq
MCgGA1UEAxMhU0lQIFByb2R1Y3QgQ2VydGlmaWNhdGUgQXV0aG9yaXR5ggEAMA0G
CSqGSIb3DQEBBQUAA4IBAQBgPraSto+++KAFMtUSGVm4jsbknWwazR5yFxltWrgo
osMN+1t351AEJed1DCvUWibbfSylh13PNzYLhSIlmKPR98LVQ4P5l26C2suJPaye
EUX87wDCHe8eNNG93vl54U4aQDum98FSTRlYjdSiL9R3trKLOiiYlLBE1oJHBGPi
FzRXgc0XVGWXMfAquNQ01pzKqu7ET09AWsYbUS4c+J5tdYk9nYk35Y1WtKwOz8MS
gwkB2ncy1rI6IuWvLAUdd9BKcBYGLSMVulVGjl3Oi0V35xxNoyIKQ98RPIb9RcME
zhiIkhUOktmeYHe9BYn8En76q5oOXH0CaIQOld9Vood/
-----END CERTIFICATE-----
```

- Following is the set of default certificates (in PEM format) that are trusted by the Session Manager Security module for SIP-TLS:

```
-----BEGIN CERTIFICATE-----
MIICaDCCAdECBEgQqykwDQYJKoZIhvcNAQEEBQAwezELMAkGA1UEBhMCVUsxEDAO
```

```
BgNVBAgTB1MgV2FsZXMxEDAOBgNVBAcTB0NhcmRpZmYxDjAMBgNVBAoTBWF2YXlh
MRcwFQYDVQQLEw5VSyBFbmdpbmVlcmluZzEfMB0GA1UEAxMWYXZheWEgZGV2ZWxv
cG1lbnQgdGVhbTAeFw0wODA0MjQxNTQ1NDVaFw0xODAzMDMxNTQ1NDVaMHsxCzAJ
BgNVBAYTAlVLMRAwDgYDVQQIEwdTIFdhbGVzMRAwDgYDVQQHEwdDYXJkaWZmMQ4w
DAYDVQQKEwVhdmF5YTEXMBUGA1UECxMOVUsgRW5naW5lZXJpbmcxHzAdBgNVBAMT
FmF2YXlhIGRldmVsb3BtZW50IHRlYW0wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
AoGBALpOPDPCHq8jpMs+Guaam66iBPOeFBB0SNrLu5Ua1K7fkqEmjG6O+xvnb0Dm
2keo87gZkgSnktazUHfqSQmK9UC12GpomBuJPTZPlSrhcovtadTvjBpnYylp7tVZ
cvsuQxVlaICqr067w6uq0woP4cGSG9kyuhzqvtLCmIiZOFKHAgMBAAEwDQYJKoZI
hvcNAQEEBQADgYEAnLwTrvc4WZsDWw3cuCZlTLYEEIoY9oebhx4EEgOKBz/HXjr5
yA0JiSd+KWdWdfGryhc7YYSbTruO6Hclmq7uJeaFqexdfEYtWQ0ZE1UFAZwLcz5c
Vast/vxri4NVsM+HZ4caayKPAio8csWhiQkfFDp783ho8dBW9uKQkImd8KU=
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
MIIE3zCCA8egAwIBAgIBWzANBgkqhkiG9w0BAQUFADBeMQswCQYDVQQGEwJVUzET
MBEGA1UEChMKQXZheWEgSW5jLjEaMBgGA1UECxMRQXZheWEgUHJvZHVjdCBQS0kx
HjAcBgNVBAMTFUF2YXlhIFByb2R1Y3QgUm9vdCBDQTAeFw0wNzEyMjExMTU0NDBa
Fw0yNzEyMDIxMTU0NDBaMGsxCzAJBgNVBAYTAlVTMRMwEQYDVQQKEwpBdmF5YSBJ
bmMuMRowGAYDVQQLExFBdmF5YSBQcm9kdWN0IFBLSTErMCkGA1UEAxMiQXZheWEg
TWFudWZhY3R1cmluZyBTdWJvcmRpbmF0ZSBDQTCCASAwDQYJKoZIhvcNAQEBBQAD
ggENADCCAQgCggEBAMNFdBihMGWSsTAx24rWE5sbjMVkHe0ybSAoZZliLrow9Jau
UfasJ7dm49GQAbeVWqYZ15kFjR9vxUj4ExGt/TcEbBcTau4wkG1tGrf9IsFLzJ9J
dWuC3EWuXcUr4N3UTuSuARh+Q/J31AsXOkSY+N0Tt2QhNedSeqCAXhUKhDp9FySS
ICcobqJgS70W34wXvbgXTrWvlWRanphiADN7lUoUtFpqS+qIfnpTABDG0TUGu9pk
ej3/ftzmfsACdPw5CzLUklglW5c8l6iJYH1stwkTPrrJkLPaCV1NOLZnpiSgQ9ru
3IbVXAn8MUPkiVU91bitZoB1bCS1WgkF+Q4tiM0CAQOjggGbMIIBlzAdBgNVHQ4E
FgQUbuW8D4RGjxrxDTFJElm8Mf7Bz+wwgYYGA1UdIwR/MH2AFMKatvFzIYImbROw
/v5R9l6b3DV7oWKkYDBeMQswCQYDVQQGEwJVUzETMBEGA1UEChMKQXZheWEgSW5j
LjEaMBgGA1UECxMRQXZheWEgUHJvZHVjdCBQS0kxHjAcBgNVBAMTFUF2YXlhIFBy
b2R1Y3QgUm9vdCBDQYIBADAMBgNVHRMEBTADAQH/MAsGA1UdDwQEAwIBBjCB0QYD
VR0gBIHJMIHGMIHDBgtghkgBhvwLBwEBATCBszAqBggrBgEFBQcCARYeaHR0cHM6
Ly93d3cuYXZheWEuY29tL3BraS9DUFM7MIGEBggrBgEFBQcCAjB4MBcWEEF2YXlh
IFByb2R1Y3QgQ0EwAwIBARpdQXZheWEgSW5jLiBMaW1pdGVkIExpYWJpbGl0eSBQ
S0kgQ0EuICBQbGVhc2UgdmlzaXQgaHR0cDovL3d3dy5hdmF5YS5jb20vcGtpL0NQ
UyBmb3IgZGV0YWlscy47MA0GCSqGSIb3DQEBBQUAA4IBAQBv40OigRG3iXiqmVwX
WUdK1DaNQ7wDYCVPteNa9smLrdswAohdqMpyBS0Fut+QfqWQkn2p4eL90ZICeqlr
hPYWUFKSmlpKhf93WH+0jsfvuzWefFg4JtlNsWgbVdi1wPdG9wddkgs4Bt6GzwOL
r0iUuZwnHyUahR8KEvFnab0+KA5gTIOqNnF0dGzaePzPzIJ2Tp8ybpSYQTjBVZmP
/YwkociqOMjUwbuUqDKlsARbeZMAUxmLx6V8fv96G+OPf3MUuvclTTVCP7+6i35y
dV5DG/qP4OpAZcFO/HNdtzreIYjDnlbplw2Fy9LClBZmUwHTmSzp1nJjk6Wg3OAD
DVSH
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
MIIE1DCCA7ygAwIBAgIBADANBgkqhkiG9w0BAQUFADBeMQswCQYDVQQGEwJVUzET
MBEGA1UEChMKQXZheWEgSW5jLjEaMBgGA1UECxMRQXZheWEgUHJvZHVjdCBQS0kx
HjAcBgNVBAMTFUF2YXlhIFByb2R1Y3QgUm9vdCBDQTAeFw0wMzA4MjIxMTI1MzZa
Fw0zMzA4MTQxMTI1MzZaMF4xCzAJBgNVBAYTAlVTMRMwEQYDVQQKEwpBdmF5YSBJ
bmMuMRowGAYDVQQLExFBdmF5YSBQcm9kdWN0IFBLSTEeMBwGA1UEAxMVQXZheWEg
UHJvZHVjdCBSb290IENBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
+EpellesygWvwACRNRh/6FbkPYDGrf5jpqIzgd3KG1w7gvvQ/ID953REm2DS7DEI
4y7l+zY0MLtNv+I3rASpdxufsFwkHa5zR1FjpkiaP7XhMKXNpSY7No78rko9uiGt
xCx9VdW20kcP4IiEN23jQWfKjGFzkZItCl/aOf2+peh8bSS2MIprGx4rnCMZN1dU
Nnw8nJFGu7IxRlGDA2XqJ7BWBn/pvPMLdaVU60oI1/4IT9lHPUCaRVAC56jJdtxq
F9sNW0ZsBy05/vtopUiStfq8aMtMWCqGkSwjWB2VDWhWj6HTuGk27YsTsFIREJuT
i7rXYBQqRJN0o15aERM6BwIDAQABo4IBmzCCAZcwHQYDVR0OBBYEFMKatvFzIYIm
```

```
bROw/v5R9l6b3DV7MIGGBgNVHSMEfzB9gBTCmrbxcyGCJm0TsP7+UfZem9w1e6Fi
pGAwXjELMAkGA1UEBhMCVVMxEzARBgNVBAoTCkF2YXlhIEluYy4xGjAYBgNVBAsT
EUF2YXlhIFByb2R1Y3QgUEtJMR4wHAYDVQQDExVBdmF5YSBQcm9kdWN0IFJvb3Qg
Q0GCAQAwDAYDVR0TBAUwAwEB/zALBgNVHQ8EBAMCAQYwgdEGA1UdIASByTCBxjCB
wwYLYIZIAYb8CwcBAQEwgbMwKgYIKwYBBQUHAgEWHmh0dHBzOi8vd3d3LmF2YXlh
LmNvbS9wa2kvQ1BTOzCBhAYIKwYBBQUHAgIweDAXFhBBdmF5YSBQcm9kdWN0IENB
MAMCAQEaXUF2YXlhIEluYy4gTGltaXRlZCBMaWFiaWxpdHkgUEtJIENBLiAgUGxl
YXNlIHZpc2l0IGh0dHA6Ly93d3cuYXZheWEuY29tL3BraS9DUFMgZm9yIGRldGFp
bHMuOzANBgkqhkiG9w0BAQUFAAOCAQEAQYNqOpJSkAn6tZOAbp7IW2RMFQO2rwNe
UFdyWywqWKdoCNv/+9dAkHXp8wSEwRGPuXRJLuSZloRlK7OnT4GBH+YaFMarHpUr
rChkrmcR9smgN1WvSjvTk1HiFXEyurvpRarLRem3spDdN6Cyu/fhroJJEHc0j97O
U2HTNgz0papOAFxYN497y3teENVmRBGNKoUo6NxayOCjv55JBxegvd6bOtabRv1L
OCNK8yeomL5ri9jiTLUgEEZIn3aFXetuKxTjhQqbxcpy16t70SQctIzLXqdp9ZZu
xz27CykJXlmexi5qREs+MLV0jrduRE50nTHMhkHKZBX7yKIgEb9GwQ==
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
MIIDvDCCAqSgAwIBAgIBADANBgkqhkiG9w0BAQUFADCBgDELMAkGA1UEBhMCVVMx
FzAVBgNVBAoTDk1vdG9yb2xhLCBJbmMuMTkwNwYDVQQLEzBTZWFtbGVzcyBDb252
ZXJnZWQgQ29tbXVuaWNhdGlvbiBBY3Jvc3MgTmV0d29ya3MxHTAbBgNVBAMTFFND
Q0FOIFNlcnZlciBSb290IENBMB4XDTAzMTIwNTIxMjg0M1oXDTMzMTIwNDIxMjg0
M1owgYAxCzAJBgNVBAYTAlVTMRcwFQYDVQQKEw5Nb3Rvcm9sYSwgSW5jLjE5MDcG
A1UECxMwU2VhbWxlc3MgQ29udmVyZ2VkIENvbW11bmljYXRpb24gQWNyb3NzIE5l
dHdvcmtzMR0wGwYDVQQDExRTQ0NBTiBTZXJ2ZXIgUm9vdCBDQTCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBANHrAz5BUuNXL3cH9eAodevZY+5C1IaBtmxe
K7+TweCWSljAeX/e2EKMQatNIOFHO3cXqV7ERBUp0ymmrnnmLeqVfbS9anWOzoGr
MCZ3grohkFWh41uBzxlgYhDoGhGc1H8RZJBEE3Rmo5djZrTzAutSuOi7iAO7S9IC
a9RBZF/db3Z8jkc0ucSi3pDTolIJvjVx5ccztRd133uUyvHSAoXAwyFVx/9trZHp
rQr76xUC/8nOAhXlUlt8Vnp5C30X5WywCOXWelIUaLldH55fxDVcGL5h7Yu8SLb9
iynrlJ6XeDKp+fDtWCVySIZBCLx0Ho29f8hOmLpg5/vb691Q6mUCAwEAAaM/MD0w
DwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUc50Q0MwSbfz43CTFP6gsFsrWv+Uw
CwYDVR0PBAQDAgEGMA0GCSqGSIb3DQEBBQUAA4IBAQA956Nf5ldsVXTLbRMRBMuS
y1mdFnbtFN3hd8j8PcqDH9du+411JR1DL7cOJEJWDJwO1qlG44A6Mj/JnvwIA0M4
s3AAKV+EBj1du+TBLhZluuEcvgpX1xiQehIFqTS6fp+CBLL2NYEeze0x1d/IHNNA
eBhYfGBNnhbU0YGOlNERYyT+nTgPgVVwuNaagJPyxHkZKWE2BmMT3OBt3vsdJS7S
c+8Xiivl/KSfF3003/hQrzFH6mDtqSwLgFzKadZ2QE3HVdcajt/fW9sGyaq5PfWO
mwyOTwtrcuo2/EQqX03XHeTEohEoqMTTiNXxTLOwaPgAf/dkwmqPDjuZohtAUphg
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
MIIC0DCCAjmgAwIBAgIBADANBgkqhkiG9w0BAQQFADBVMQswCQYDVQQGEwJVUzET
MBEGA1UEChMKQXZheWEgSW5jLjEVMBMGA1UECxMMTWVkaWEgU2VydmVyMRowGAYD
VQQDExFBdmF5YSBDYWxsIFNlcnZlcjAeFw0wMjAxMTAwMzQwNDdaFw0zMjAxMDMw
MzQwNDdaMFUxCzAJBgNVBAYTAlVTMRMwEQYDVQQKEwpBdmF5YSBJbmMuMRUwEwYD
VQQLEwxNZWRpYSBTZXJ2ZXIxGjAYBgNVBAMTEUF2YXlhIENhbGwgU2VydmVyMIGf
MA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDABs8TR5L3cDQNZTsA+t1HJZDOM/Sr
Ngq6TRWf3r8KdzUpYZVAxecODQ2gu9ccfLraxhi8Vn1X6DD/uBT90WdqkhpZs0+f
o6WE7fZZqGFJyVHhtqrN58IOOdQTfjKywhi0w+GTKfEvS/IHXLNM7Rr55KN4Jqa7
3GzklP0d//it4QIDAQABo4GvMIGsMB0GA1UdDgQWBBQ7f+X4y7uDnQ2lkDsVYuFr
ESzohDB9BgNVHSMEdjB0gBQ7f+X4y7uDnQ2lkDsVYuFrESzohKFZpFcwVTELMAkG
A1UEBhMCVVMxEzARBgNVBAoTCkF2YXlhIEluYy4xFTATBgNVBAsTDE1lZGlhIFNl
cnZlcjEaMBgGA1UEAxMRQXZheWEgQ2FsbCBTZXJ2ZXKCAQAwDAYDVR0TBAUwAwEB
/zANBgkqhkiG9w0BAQQFAAOBgQAa1P7y67oAqwsnM268fXWKTjhqixG2N2+BVkkk
2CEgKzFIjUuwV0kllR+RkyijKXsEnFBvXDdDDbuK+K9O2KO//i3I1eRIsMeVJ4Jj
wE9iYt8+Fniir4moMidQW9KT7SK0Db4ARY4GWezJQPFVoPng7Ny6rDooUIcNmZc4
YK9Wbw==
-----END CERTIFICATE-----
```

```
-----BEGIN CERTIFICATE-----
MIIEnTCCA4WgAwIBAgIBADANBgkqhkiG9w0BAQUFADB6MQswCQYDVQQGEwJVUzET
MBEGA1UEChMKQXZheWEgSW5jLjEqMCgGA1UECxMhU0lQIFByb2R1Y3QgQ2VydGlm
aWNhdGUgQXV0aG9yaXR5MSowKAYDVQQDEyFTSVAgUHJvZHVjdCBDZXJ0aWZpY2F0
ZSBBdXRob3JpdHkwHhcNMDMwNzI1MDAzMzE3WhcNMjcwODE3MDUxOTM5WjB6MQsw
CQYDVQQGEwJVUzETMBEGA1UEChMKQXZheWEgSW5jLjEqMCgGA1UECxMhU0lQIFBy
b2R1Y3QgQ2VydGlmaWNhdGUgQXV0aG9yaXR5MSowKAYDVQQDEyFTSVAgUHJvZHVj
dCBDZXJ0aWZpY2F0ZSBBdXRob3JpdHkwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQDcOytyx7YRzT7VYJov8FGe6g1GJ0h+4Y7YZzzmgHPqpgn+2jluQi1N
NHliMLbYLnrvf6s3+X/zh7ZND2tyrKZMCYaI8FX6X3tYTONZ9ErTYngSJCpLeCuj
c+qgt1SmRsya1+1F9i5jvrFxoOuRb5N05Yv3cI85SFLw7kEr41cQDvshRBWZfo6r
f3bBJjlqRTHc5yGbXXeEs+JrtIveECFB2Q/w3Eg/GbcWGhP1uqHqOPH76aNMYyQP
GMzDBtpCfGh7HkD7jkT2El+AiBKJy0cOcj22+AKbLvh5bffJMTcCPX2Bax2CD2I1
usQ+osTG+FdvuhRBx+WPqBOWsQ0wRKGNAgMBAAGjggEsMIIBKDA/BgNVHSAEODA2
MDQGC2CGSAGG/AsHAgEBMCUwIwYIKwYBBQUHAgEWF21haWx0bzpzaXBjYUBhdmF5
YS5jb207MB0GA1UdDgQWBBSgggcpXDqgxCm4PcMduQZVE75WKjASBgNVHRMBAf8E
CDAGAQH/AgEBMAsGA1UdDwQEAwIBBjCBpAYDVR0jBIGcMIGZgBSgggcpXDqgxCm4
PcMduQZVE75WKqF+pHwwejELMAkGA1UEBhMCVVMxEzARBgNVBAoTCkF2YXlhIElu
Yy4xKjAoBgNVBAsTIVNJUCBQcm9kdWN0IENlcnRpZmljYXRlIEF1dGhvcml0eTEq
MCgGA1UEAxMhU0lQIFByb2R1Y3QgQ2VydGlmaWNhdGUgQXV0aG9yaXR5ggEAMA0G
CSqGSIb3DQEBBQUAA4IBAQBgPraSto+++KAFMtUSGVm4jsbknWwazR5yFxltWrgo
osMN+1t351AEJed1DCvUWibbfSylh13PNzYLhSIlmKPR98LVQ4P5l26C2suJPaye
EUX87wDCHe8eNNG93vl54U4aQDum98FSTRlYjdSiL9R3trKLOiiYlLBE1oJHBGPi
FzRXgc0XVGWXMfAquNQ01pzKqu7ET09AWsYbUS4c+J5tdYk9nYk35Y1WtKwOz8MS
gwkB2ncy1rI6IuWvLAUdd9BKcBYGLSMVulVGjl3Oi0V35xxNoyIKQ98RPIb9RcME
zhiIkhUOktmeYHe9BYn8En76q5oOXH0CaIQOld9Vood/
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIBADANBgkqhkiG9w0BAQQFADBvMQswCQYDVQQGEwJVUzEL
MAkGA1UECBMCTUExEDAOBgNVBAcTB0FuZG92ZXIxDjAMBgNVBAoTBUFWQVlBMQ0w
CwYDVQQLEwRFTU1DMSIwIAYJKoZIhvcNAQkBFhNpZ29uemFsZXNAYXZheWEuY29t
MB4XDTA0MTAxMzE1Mzc1N1oXDTMyMDIyOTE1Mzc1N1owbzELMAkGA1UEBhMCVVMx
CzAJBgNVBAgTAk1BMRAwDgYDVQQHEwdBbmRvdmVyMQ4wDAYDVQQKEwVBVkFZQTEN
MAsGA1UECxMERU1NQzEiMCAGCSqGSIb3DQEJARYTaWdvbnphbGVzQGF2YXlhLmNv
bTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA3+P7zLbpBTyyvhYUsrAuh3x6
emQRxA6QtJlNOMWZKLtLSWuap+KFYOLtNd36MZl/KavEn6wCChR5IM1GAPwCIvZV
pG907FRxPoxdZOAZZRqgWzG7L9mC30NxBiBwA3DO9GbFqOdeW8zupf5SBZqpQ7k/
DZO7oAuYZE8GFhNkUVECAwEAAaOBzDCByTAdBgNVHQ4EFgQUixd7HNzpgfqPlLcc
uhqhDYZUX6QwgZkGA1UdIwSBkTCBjoAUixd7HNzpgfqPlLccuhqhDYZUX6Shc6Rx
MG8xCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJNQTEQMA4GA1UEBxMHQW5kb3ZlcjEO
MAwGA1UEChMFQVZBWUExDTALBgNVBAsTBEVNTUMxIjAgBgkqhkiG9w0BCQEWE2ln
b256YWxlc0BhdmF5YS5jb22CAQAwDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQQF
AAOBgQCLiZfxwyTbfC5C5KRnz9tbDLLEzCHoHqZASlUtIK/cY6fzmEtkNb/k6pdM
0CwYeY5u7rBMhj9UmnhvgGSqQKAMZHsFDIYZU6H3HmV6P+l7kKiWYvSag+adwYH4
T0m2+rzTOu/lYioczR5MIrxT3Txrovs8cEYgJNzewPm2/jQeXw==
-----END CERTIFICATE-----
```