

PIX/ASA 7.x: Enable VoIP (SIP, MGCP, H323, SCCP) Services Configuration Example

Document ID: 82446

Introduction

Prerequisites

- Requirements
- Components Used
- Related Products
- Conventions

Background Information

- SIP
- MGCP
- H.323
- SCCP

Configure

- Network Diagram for SIP
- Configurations for SIP
- Network Diagram for MGCP, H.323 and SCCP
- Configurations for MGCP
- Configurations for H.323
- Configurations for SCCP

Verify

Troubleshoot

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

This document describes how to allow the Voice over IP (VoIP) Protocols traffic on the outside interface and enable inspection for each protocol in the Cisco PIX/ASA Security Appliances.

These are the protocols:

- **Session Initiation Protocol (SIP)** SIP is an application–layer control (signaling) protocol that creates, modifies, and terminates sessions with one or more participants. These sessions include Internet telephone calls, multimedia distribution, and multimedia conferences.

SIP, as defined by the Internet Engineering Task Force (IETF), enables VoIP calls. SIP works with Session Description Protocol (SDP) for call signalling. SDP specifies the details of the media stream. The security appliance can support any SIP (VoIP) gateways and VoIP proxy servers when SIP is used. SIP and SDP are defined in these RFCs:

- ◆ SIP: Session Initiation Protocol, RFC 3261
- ◆ SDP: Session Description Protocol, RFC 2327

In order to support SIP calls through the security appliance, signaling messages for the media connection addresses, media ports, and embryonic connections for the media must be inspected. This is because while the signaling is sent over a well–known destination port (**UDP/TCP 5060**), the media streams are dynamically allocated. Also, SIP embeds IP addresses in the user–data portion of the IP packet. SIP inspection applies Network Address Translation (NAT) for these embedded IP

addresses.

Note: If a remote endpoint tries to register with a SIP proxy on a network protected by the security appliance, the registration fails under very specific conditions. These conditions are when Port Address Translation (PAT) is configured for the remote endpoint, the SIP registrar server is on the outside network, and when the port is missing in the contact field in the REGISTER message sent by the endpoint to the proxy server.

- **Media Gateway Control Protocol (MGCP)** MGCP is a client–server call control protocol, built on centralized control architecture. All the dial plan information resides on a separate call agent. The call agent, which controls the ports on the gateway, performs call control. The gateway does media translation between the Public Switched Telephone Network (PSTN) and the VoIP networks for external calls. In a Cisco–based network, CallManagers function as the call agents.

MGCP is an IETF standard that is defined in several RFCs, which includes 2705 and 3435 . Its capabilities can be extended by the use of packages that include, for example, the handling of dual–tone multifrequency (DTMF) tones, secure RTP, call hold, and call transfer.

An MGCP gateway is relatively easy to configure. Because the call agent has all the call–routing intelligence, you do not need to configure the gateway with all the dial peers it would otherwise need. A downside is that a call agent must always be available. Cisco MGCP gateways can use Survivable Remote Site Telephony (SRST) and MGCP fallback to allow the H.323 protocol to take over and provide local call routing in the absence of a CallManager. In that case, you must configure dial peers on the gateway for use by H.323.

- **H.323** H.323 inspection provides support for H.323 compliant applications such as Cisco CallManager and VocalTec Gatekeeper. H.323 is a suite of protocols defined by the International Telecommunication Union for multimedia conferences over LANs. The security appliance supports H.323 through Version 4, which includes H.323 v3 feature Multiple Calls on One Call Signaling Channel.

With H.323 inspection enabled, the security appliance supports multiple calls on the same call signaling channel, a feature introduced with H.323 Version 3. This feature reduces call setup time and reduces the use of ports on the security appliance.

These are the two major functions of H.323 inspection:

- ◆ NAT the necessary embedded IPv4 addresses in the H.225 and H.245 messages. Because H.323 messages are encoded in PER encoding format, the security appliance uses an ASN.1 decoder to decode the H.323 messages.
- ◆ Dynamically allocate the negotiated H.245 and RTP/RTCP connections.
- **Skippy (or Simple) Client Control Protocol (SCCP)** SCCP is a simplified protocol used in VoIP networks. Cisco IP Phones that use SCCP can coexist in an H.323 environment. When used with Cisco CallManager, the SCCP client can interoperate with H.323–compliant terminals. Application layer functions in the security appliance recognize SCCP Version 3.3. The functionality of the application layer software ensures that all SCCP signaling and media packets can traverse the security appliance by providing NAT of the SCCP Signaling packets.

There are 5 versions of the SCCP protocol: 2.4, 3.0.4, 3.1.1, 3.2, and 3.3.2. The security appliance supports all versions through Version 3.3.2. The security appliance provides both PAT and NAT support for SCCP. PAT is necessary if you have limited numbers of global IP addresses for use by IP phones.

Normal traffic between Cisco CallManager and Cisco IP Phones uses SCCP and is handled by SCCP inspection without any special configuration. The security appliance also supports DHCP options 150 and 66, which allow the security appliance to send the location of a TFTP server to Cisco IP Phones

and other DHCP clients. Refer to [Configuring DHCP, DDNS, and WCCP Services](#) for more information.

Prerequisites

Requirements

This document assumes that the necessary VPN configuration is made on all the devices and works properly.

Refer to [PIX/ASA 7.x Security Appliance to an IOS Router LAN-to-LAN IPsec Tunnel Configuration Example](#) in order to learn more about the VPN configuration.

Refer to [PIX/ASA 7.x: Enable Communication Between Interfaces](#) for more information on how to enable the communication between interfaces.

Components Used

The information in this document is based on the Cisco 5500 Series Adaptive Security Appliance (ASA) which runs software version 7.x.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Related Products

This configuration can also be used with the Cisco 500 Series PIX Firewall which runs software version 7.x.

Conventions

Refer to [Cisco Technical Tips Conventions](#) for more information on document conventions.

Background Information

SIP

SIP inspection NATs the SIP text-based messages, recalculates the content length for the SDP portion of the message, and recalculates the packet length and checksum. It dynamically opens media connections for ports specified in the SDP portion of the SIP message as address/ports on which the endpoint should listen.

SIP inspection has a database with indices CALL_ID/FROM/TO from the SIP payload that identifies the call, as well as the source and destination. Contained within this database are the media addresses and media ports that were contained in the SDP media information fields and the media type. There can be multiple media addresses and ports for a session. RTP/RTCP connections are opened between the two endpoints using these media addresses/ports.

The well-known port 5060 must be used on the initial call setup (INVITE) message. However, subsequent messages might not have this port number. The SIP inspection engine opens signaling connection pinholes, and marks these connections as SIP connections. This is done for the messages to reach the SIP application and be NATed.

As a call is set up, the SIP session is considered in the transient state. This state remains until a Response message is received which indicates the RTP media address and port on which the destination endpoint listens. If there is a failure to receive the response messages within one minute, the signaling connection is torn down.

Once the final handshake is made, the call state is moved to active and the signaling connection remains until a BYE message is received.

If an inside endpoint initiates a call to an outside endpoint, a media hole is opened to the outside interface to allow RTP/RTCP UDP packets to flow to the inside endpoint media address and media port specified in the INVITE message from the inside endpoint. Unsolicited RTP/RTCP UDP packets to an inside interface will not traverse the security appliance, unless the security appliance configuration specifically allows it.

The media connections are torn down within two minutes after the connection becomes idle. This is a configurable timeout and can be set for a shorter or longer period of time.

MGCP

In order to use MGCP, you usually need to configure at least two inspect commands: one for the port on which the gateway receives commands, and one for the port on which the call agent receives commands. Normally, a call agent sends commands to the default MGCP port for gateways, **2427**, and a gateway sends commands to the default MGCP port for call agents, **2727**.

MGCP messages are transmitted over **UDP**. A response is sent back to the source address (IP address and UDP port number) of the command, but the response might not arrive from the same address as the command was sent to. This can occur when multiple call agents are used in a failover configuration and the call agent that received the command has passed control to a backup call agent, which then sends the response.

H.323

The H.323 collection of protocols collectively can use up to two TCP connection and four to six UDP connections. FastConnect uses only one TCP connection, and Reliability, Availability, and Serviceability (RAS) uses a single UDP connection for registration, admissions, and status.

An H.323 client can initially establish a TCP connection to an H.323 server using TCP port 1720 to request Q.931 call setup. As part of the call setup process, the H.323 terminal supplies a port number to the client to use for an H.245 TCP connection. In environments where H.323 gatekeeper is in use, the initial packet is transmitted using UDP.

H.323 inspection monitors the Q.931 TCP connection to determine the H.245 port number. If the H.323 terminals do not use FastConnect, the security appliance dynamically allocates the H.245 connection based on the inspection of the H.225 messages.

Within each H.245 message, the H.323 endpoints exchange port numbers that are used for subsequent UDP data streams. H.323 inspection inspects the H.245 messages to identify these ports and dynamically creates connections for the media exchange. RTP uses the negotiated port number, while RTCP uses the next higher port number.

The H.323 control channel handles H.225 and H.245 and H.323 RAS. H.323 inspection uses these ports:

- 1718 Gate Keeper Discovery UDP port
- 1719 RAS UDP port
- 1720 TCP Control Port

You must permit traffic for the well-known H.323 port 1720 for the H.225 call signaling. However, the H.245 signaling ports are negotiated between the endpoints in the H.225 signaling. When an H.323 gatekeeper is used, the security appliance opens an H.225 connection based on inspection of the Admission Confirmation (ACF) message.

After the H.225 messages are inspected, the security appliance opens the H.245 channel and then inspects traffic sent over the H.245 channel. All H.245 messages that pass through the security appliance undergo H.245 application inspection, which translates embedded IP addresses and opens the media channels negotiated in H.245 messages.

The H.323 ITU standard requires that a Transport Protocol Data Unit Packet (TPKT) header, which defines the length of the message, precede the H.225 and H.245, before being passed on to the reliable connection. Because the TPKT header does not necessarily need to be sent in the same TCP packet as H.225 and H.245 messages, the security appliance must remember the TPKT length to process and decode the messages properly. For each connection, the security appliance keeps a record that contains the TPKT length for the next expected message.

If the security appliance needs to perform NAT on IP addresses in messages, it changes the checksum, the UIIE length, and the TPKT, if it is included in the TCP packet with the H.225 message. If the TPKT is sent in a separate TCP packet, the security appliance proxy acknowledgments (ACKs) that TPKT and appends a new TPKT to the H.245 message with the new length.

SCCP

In topologies where Cisco CallManager is located on the higher security interface with respect to the Cisco IP Phones, if NAT is required for the Cisco CallManager IP address, the mapping must be static as a Cisco IP Phone requires the Cisco CallManager IP address to be specified explicitly in its configuration. An identity static entry allows the Cisco CallManager on the higher security interface to accept registrations from the Cisco IP Phones.

Cisco IP Phones require access to a TFTP server in order to download the configuration information they need to connect to the Cisco CallManager server.

When the Cisco IP Phones are on a lower security interface compared to the TFTP server, you must use an access list in order to connect to the protected TFTP server on UDP port 69. While you do need a static entry for the TFTP server, this does not have to be an identity static entry. When NAT is used, an identity static entry maps to the same IP address. When PAT is used, it maps to the same IP address and port.

When the Cisco IP Phones are on a higher security interface compared to the TFTP server and Cisco CallManager, no access list or static entry is required to allow the Cisco IP Phones to initiate the connection.

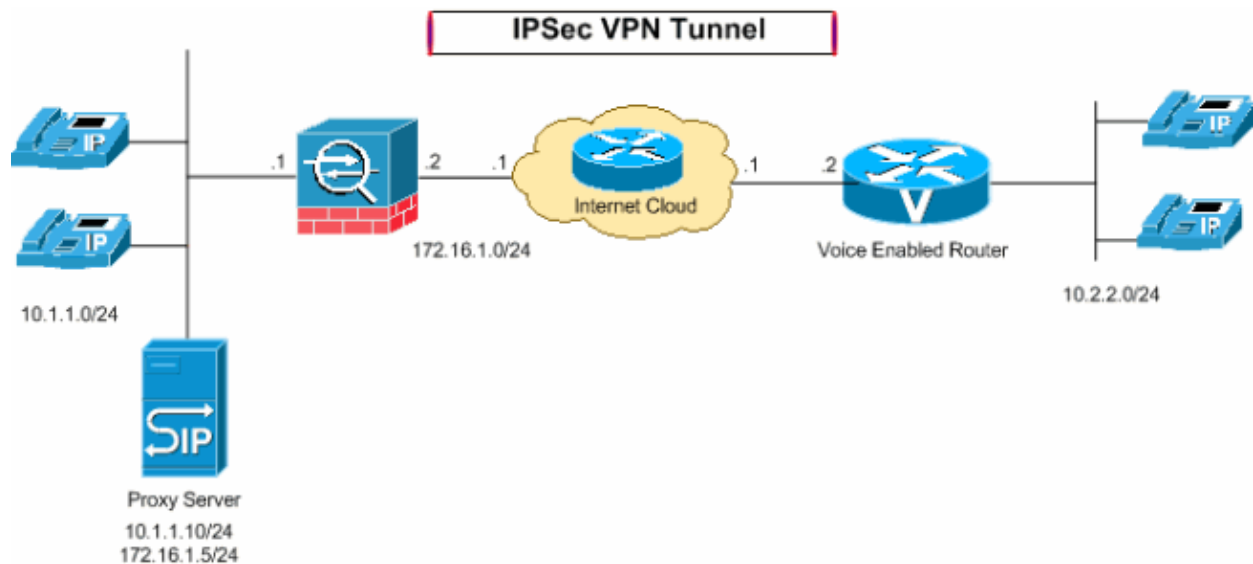
Configure

In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

Network Diagram for SIP

This section uses this network setup:



Configurations for SIP

This section uses these configurations:

The Security Appliance supports application inspection through the Adaptive Security Algorithm function. Through the stateful application inspection used by the Adaptive Security Algorithm, the Security Appliance tracks each connection that traverses the firewall and ensures that they are valid. The firewall, through stateful inspection, also monitors the state of the connection to compile information to place in a state table. With the use of the state table in addition to administrator-defined rules, filtering decisions are based on context that is established by packets previously passed through the firewall. The implementation of application inspections consists of these actions:

- Identify the traffic.
- Apply inspections to the traffic.
- Activate inspections on an interface.

Configure Basic SIP Inspection

By default, the configuration includes a policy that matches all default application inspection traffic and applies inspection to the traffic on all interfaces (a global policy). Default application inspection traffic includes traffic to the default ports for each protocol. You can only apply one global policy. Therefore, if you want to alter the global policy, for example, to apply inspection to non-standard ports or to add inspections that are not enabled by default, you need to either edit the default policy or disable it and apply a new one. For a list of all default ports, refer to the Default Inspection Policy.

1. Issue the **policy-map global_policy** command.

```
ASA5510(config)#policy-map global_policy
```

2. Issue the **class inspection_default** command.

```
ASA5510(config-pmap)#class inspection_default
```

3. Issue the **inspect sip** command.

```
ASA5510(config-pmap-c)#inspect sip
```

ASA Configuration for SIP

ASA Version 7.2(1)24

```

!
ASA5510 ASA5510
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0
!
interface Ethernet0/1
 nameif outside
 security-level 0
 ip address 172.16.1.2 255.255.255.0
!

/--- Output suppressed.

passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive

/--- Command to allow the incoming SIP traffic.

access-list 100 extended permit tcp 10.2.2.0 255.255.255.0
host 172.16.1.5 eq sip
pager lines 24
mtu inside 1500
mtu outside 1500
no failover
asdm image disk0:/asdm-522.bin
no asdm history enable
arp timeout 14400

/--- Command to redirect the SIP traffic received on outside interface to
/--- inside interface for the specified IP address.

static (inside,outside) 172.16.1.5 10.1.1.10 netmask 255.255.255.255
access-group 100 in interface outside
route outside 0.0.0.0 0.0.0.0 172.16.1.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp

```

```

inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp

!--- Command to enable SIP inspection.

inspect sip
inspect xdmcp
inspect ftp
!

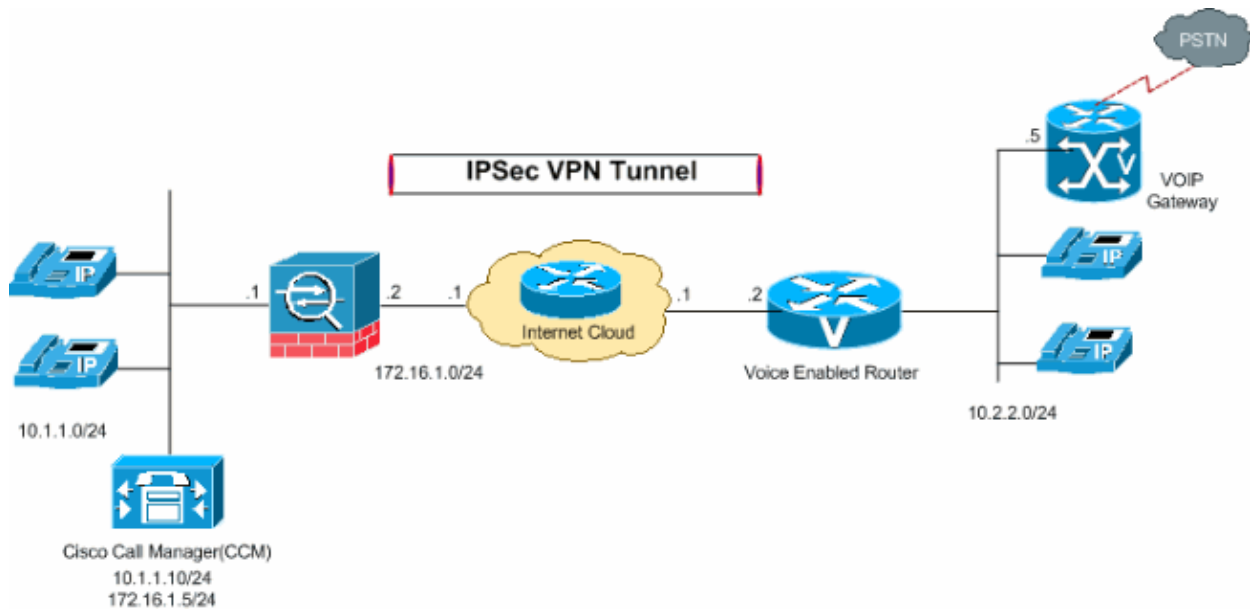
!--- This command tells the device to
!--- use the "global_policy" policy-map on all interfaces.

service-policy global_policy global
prompt ASA5510 context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
ASA5510#

```

Network Diagram for MGCP, H.323 and SCCP

This section uses this network setup:



Configurations for MGCP

This section uses these configurations:

The Security Appliance supports application inspection through the Adaptive Security Algorithm function. Through the stateful application inspection used by the Adaptive Security Algorithm, the Security Appliance tracks each connection that traverses the firewall and ensures that they are valid. The firewall, through stateful inspection, also monitors the state of the connection to compile information to place in a state table. With the use of the state table in addition to administrator-defined rules, filtering decisions are based on context that is established by packets previously passed through the firewall. The implementation of application inspections consists of these actions:

- Identify the traffic.
- Apply inspections to the traffic.
- Activate inspections on an interface.

Configure Basic MGCP Inspection

By default, the configuration includes a policy that matches all default application inspection traffic and applies inspection to the traffic on all interfaces (a global policy). Default application inspection traffic includes traffic to the default ports for each protocol. You can only apply one global policy. Therefore, if you want to alter the global policy, for example, to apply inspection to non-standard ports or to add inspections that are not enabled by default, you need to either edit the default policy or disable it and apply a new one. For a list of all default ports, refer to the Default Inspection Policy.

1. Issue the **policy-map global_policy** command.

```
ASA5510(config)#policy-map global_policy
```

2. Issue the **class inspection_default** command.

```
ASA5510(config-pmap)#class inspection_default
```

3. Issue the **inspect mgcp** command.

```
ASA5510(config-pmap-c)#inspect mgcp
```

Configure an MGCP Inspection Policy Map for Additional Inspection Control

If the network has multiple call agents and gateways for which the security appliance has to open pinholes, create an MGCP map. You can then apply the MGCP map when you enable MGCP inspection. Refer to Configuring Application Inspection for more information.

```
!--- Permits inbound 2427 port traffic.
```

```
ASA5510(config)#access-list 100 extended permit udp 10.2.2.0 255.255.255.0
host 172.16.1.5 eq 2427
```

```
!--- Permits inbound 2727 port traffic.
```

```
ASA5510(config)#access-list 100 extended permit udp 10.2.2.0 255.255.255.0
host 172.16.1.5 eq 2727
```

```
ASA5510(config)#class-map mgcp_port
ASA5510(config-cmap)#match access-list 100
ASA5510(config-cmap)#exit
```

```
!--- Command to create an MGCP inspection policy map.
```

```
ASA5510(config)#policy-map type inspect mgcp mgcpmap
```

```
!--- Command to configure parameters that affect the
!--- inspection engine and enters into parameter configuration mode.
```

```
ASA5510(config-pmap)#parameters
```

```
!--- Command to configure the call agents.
```

```
ASA5510(config-pmap-p)#call-agent 10.1.1.10 101
```

```
!--- Command to configure the gateways.
```

```
ASA5510(config-pmap-p)#gateway 10.2.2.5 101
```

```
!--- Command to change the maximum number of commands
```

!--- allowed in the MGCP command queue.

```
ASA5510(config-pmap-p)#command-queue 150
ASA5510(config-pmap-p)# exit
ASA5510(config)#policy-map inbound_policy
ASA5510(config-pmap)# class mgcp_port
ASA5510(config-pmap-c)#inspect mgcp mgcpmap
ASA5510(config-pmap-c)# exit
ASA5510(config)#service-policy inbound_policy interface outside
```

ASA Configuration for MGCP

```
ASA Version 7.2(1)24
!
hostname ASA5510
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0
!
interface Ethernet0/1
 nameif outside
 security-level 0
 ip address 172.16.1.2 255.255.255.0
!

!--- Permits inbound 2427 and 2727 port traffic.

access-list 100 extended permit udp 10.2.2.0 255.255.255.0 host 172.16.1.5 eq 2427
access-list 100 extended permit udp 10.2.2.0 255.255.255.0 host 172.16.1.5 eq 2727
pager lines 24
mtu inside 1500
mtu outside 1500
no failover
no asdm history enable
arp timeout 14400

!--- Command to redirect the MGCP traffic received on outside interface to
!--- inside interface for the specified IP address.

static (inside,outside) 172.16.1.5 10.1.1.10 netmask 255.255.255.255
access-group 100 in interface outside
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map mgcp_port
 match access-list 100
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
```

```

message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
inspect mgcp
policy-map type inspect mgcp mgcpmap
parameters
call-agent 10.1.1.10 101
gateway 10.2.2.5 101
command-queue 150
policy-map inbound_policy
class mgcp_port
inspect mgcp mgcpmap
!
service-policy global_policy global
service-policy inbound_policy interface outside
prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end

```

Configurations for H.323

This section uses these configurations:

The Security Appliance supports application inspection through the Adaptive Security Algorithm function. Through the stateful application inspection used by the Adaptive Security Algorithm, the Security Appliance tracks each connection that traverses the firewall and ensures that they are valid. The firewall, through stateful inspection, also monitors the state of the connection to compile information to place in a state table. With the use of the state table in addition to administrator-defined rules, filtering decisions are based on context that is established by packets previously passed through the firewall. The implementation of application inspections consists of these actions:

- Identify the traffic.
- Apply inspections to the traffic.
- Activate inspections on an interface.

Configure Basic H.323 Inspection

By default, the configuration includes a policy that matches all default application inspection traffic and applies inspection to the traffic on all interfaces (a global policy). Default application inspection traffic includes traffic to the default ports for each protocol. You can only apply one global policy. Therefore, if you want to alter the global policy, for example, to apply inspection to non-standard ports or to add inspections that are not enabled by default, you need to either edit the default policy or disable it and apply a new one. For a list of all default ports, refer to the Default Inspection Policy.

1. Issue the **policy-map global_policy** command.

```
ASA5510(config)#policy-map global_policy
```

2. Issue the **class inspection_default** command.

```
ASA5510(config-pmap)#class inspection_default
```

3. Issue the **inspect h323** command.

```
ASA5510(config-pmap-c)#inspect h323 h225
```

```
ASA5510(config-pmap-c)#inspect h323 ras
```

ASA Configuration for H.323

```
ASA Version 7.2(1)24
!
ASA5510 ASA5510
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0
!
interface Ethernet0/1
 nameif outside
 security-level 0
 ip address 172.16.1.2 255.255.255.0
!

!--- Output suppressed.

passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive

!--- Command to allow the incoming Gate Keeper Discovery UDP port traffic.

access-list 100 extended permit udp 10.2.2.0 255.255.255.0 host 172.16.1.5 eq 1718

!--- Command to allow the incoming RAS UDP port.

access-list 100 extended permit udp 10.2.2.0 255.255.255.0 host 172.16.1.5 eq 1719

!--- Command to allow the incoming h323 protocol traffic.

access-list 100 extended permit tcp 10.2.2.0 255.255.255.0 host 172.16.1.5 eq h323
pager lines 24
mtu inside 1500
mtu outside 1500
no failover
asdm image disk0:/asdm-522.bin
no asdm history enable
arp timeout 14400

!--- Command to redirect the h323 protocol traffic received on outside interface to
!--- inside interface for the specified IP address.

static (inside,outside) 172.16.1.5 10.1.1.10 netmask 255.255.255.255
access-group 100 in interface outside
route outside 0.0.0.0 0.0.0.0 172.16.1.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
no snmp-server location
```

```

no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
  match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum 512
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map

!--- Command to enable H.323 inspection.

inspect h323 h225
inspect h323 ras
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
inspect ftp
!

!--- This command tells the device to
!--- use the "global_policy" policy-map on all interfaces.

service-policy global_policy global
prompt ASA5510 context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
ASA5510#

```

Configurations for SCCP

This section uses these configurations:

The Security Appliance supports application inspection through the Adaptive Security Algorithm function. Through the stateful application inspection used by the Adaptive Security Algorithm, the Security Appliance tracks each connection that traverses the firewall and ensures that they are valid. The firewall, through stateful inspection, also monitors the state of the connection to compile information to place in a state table. With the use of the state table in addition to administrator-defined rules, filtering decisions are based on context that is established by packets previously passed through the firewall. The implementation of application inspections consists of these actions:

- Identify the traffic.
- Apply inspections to the traffic.
- Activate inspections on an interface.

Configure Basic SCCP Inspection

By default, the configuration includes a policy that matches all default application inspection traffic and applies inspection to the traffic on all interfaces (a global policy). Default application inspection traffic includes traffic to the default ports for each protocol. You can only apply one global policy. Therefore, if you want to alter the global policy, for example, to apply inspection to non-standard ports or to add inspections that are not enabled by default, you need to either edit the default policy or disable it and apply a new one. For a list of all default ports, refer to the Default Inspection Policy.

1. Issue the **policy-map global_policy** command.

```
ASA5510(config)#policy-map global_policy
```

2. Issue the **class inspection_default** command.

```
ASA5510(config-pmap)#class inspection_default
```

3. Issue the **inspect skinny** command.

```
ASA5510(config-pmap-c)#inspect skinny
```

ASA Configuration for SCCP

```
ASA Version 7.2(1)24
!
ASA5510 ASA5510
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0
!
interface Ethernet0/1
 nameif outside
 security-level 0
 ip address 172.16.1.2 255.255.255.0
!
!--- Output suppressed.

passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive

!--- Command to allow the incoming SCCP traffic.

access-list 100 extended permit tcp 10.2.2.0 255.255.255.0
host 172.16.1.5 eq 2000
pager lines 24
mtu inside 1500
mtu outside 1500
no failover
asdm image disk0:/asdm-522.bin
no asdm history enable
arp timeout 14400

!--- Command to redirect the SIP traffic received on outside interface to
!--- inside interface for the specified IP address.

static (inside,outside) 172.16.1.5 10.1.1.10 netmask 255.255.255.255
access-group 100 in interface outside
route outside 0.0.0.0 0.0.0.0 172.16.1.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
```

```

timeout uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
  message-length maximum 512
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
    inspect h323 h225
    inspect h323 ras
    inspect netbios
    inspect rsh
    inspect rtsp

!--- Command to enable SCCP inspection.

    inspect skinny
    inspect esmtp
    inspect sqlnet
    inspect sunrpc
    inspect tftp

    inspect sip
    inspect xdmcp
    inspect ftp
!

!--- This command tells the device to
!--- use the "global_policy" policy-map on all interfaces.

service-policy global_policy global
prompt ASA5510 context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
ASA5510#

```

Verify

Use this section to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

SIP:

In order to ensure the configuration has successfully taken, use the **show service-policy** command and limit the output to the SIP inspection only, using the **show service-policy inspect sip** command.

```

ASA5510#show service-policy inspect sip

Global policy:

```

```
Service-policy: global_policy
Class-map: inspection_default
Inspect: sip, packet 0, drop 0, reset-drop 0
ASA5510#
```

MGCP:

```
ASA5510#show service-policy inspect mgcp

Global policy:
Service-policy: global_policy
Class-map: inspection_default
Inspect: skinny, packet 0, drop 0, reset-drop 0
```

H.323:

```
ASA5510(config)#show service-policy inspect h323 h225

Global policy:
Service-policy: global_policy
Class-map: inspection_default
Inspect: h323 h225 _default_h323_map, packet 0, drop 0, reset-drop 0
h245-tunnel-block drops 0 connection
ASA5510(config)#show service-policy inspect h323 ras

Global policy:
Service-policy: global_policy
Class-map: inspection_default
Inspect: h323 ras _default_h323_map, packet 0, drop 0, reset-drop 0
h245-tunnel-block drops 0 connection
```

SCCP:

```
ASA5510(config)#show service-policy inspect skinny

Global policy:
Service-policy: global_policy
Class-map: inspection_default
Inspect: skinny, packet 0, drop 0, reset-drop 0
```

Troubleshoot

Problem

Office communicator cannot pass through the ASA.

Solution

Office communicator used no standard SIP, and by default, the ASA drops it. Disable the SIP inspection in order to solve this problem and also clear `xlate` and `local-host` in the ASA.

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

Security: Intrusion Detection [Systems]
Security: AAA
Security: General
Security: Firewalling

Related Information

- **PIX/ASA 7.x: Enable Communication Between Interfaces**
 - **Handle VoIP Traffic with the PIX Firewall**
 - **Cisco Unified CallManager 5.0 TCP and UDP Port Usage**
 - **Cisco ASA 5500 Series Adaptive Security Appliances Product Support**
 - **Cisco PIX 500 Series Security Appliances Product Support**
 - **Media Gateway Control Protocol (MGCP) Technology Support**
 - **Skinnny Call Control Protocol (SCCP) Technology Support**
 - **H.323 Technology Support**
 - **Technical Support & Documentation – Cisco Systems**
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2007 – 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Mar 29, 2007

Document ID: 82446
