



CHAPTER 25

Configuring Application Layer Protocol Inspection

This chapter describes how to configure application layer protocol inspection. Inspection engines are required for services that embed IP addressing information in the user data packet or that open secondary channels on dynamically assigned ports. These protocols require the security appliance to do a deep packet inspection instead of passing the packet through the fast path (see the “[Stateful Inspection Overview](#)” section on page 1-4 for more information about the fast path). As a result, inspection engines can affect overall throughput.

Several common inspection engines are enabled on the security appliance by default, but you might need to enable others depending on your network. This chapter includes the following sections:

- [Inspection Engine Overview, page 25-2](#)
 - [When to Use Application Protocol Inspection, page 25-2](#)
 - [Inspection Limitations, page 25-2](#)
 - [Default Inspection Policy, page 25-3](#)
- [Configuring Application Inspection, page 25-5](#)
- [CTIQBE Inspection, page 25-9](#)
- [DCERPC Inspection, page 25-11](#)
- [DNS Inspection, page 25-13](#)
- [ESMTP Inspection, page 25-24](#)
- [FTP Inspection, page 25-27](#)
- [GTP Inspection, page 25-34](#)
- [H.323 Inspection, page 25-40](#)
- [HTTP Inspection, page 25-47](#)
- [Instant Messaging Inspection, page 25-52](#)
- [ICMP Inspection, page 25-55](#)
- [ICMP Error Inspection, page 25-55](#)
- [ILS Inspection, page 25-56](#)
- [IPSec Pass Through Inspection, page 25-57](#)
- [MGCP Inspection, page 25-58](#)
- [NetBIOS Inspection, page 25-63](#)

- [PPTP Inspection, page 25-65](#)
- [RADIUS Accounting Inspection, page 25-65](#)
- [RSH Inspection, page 25-66](#)
- [RTSP Inspection, page 25-66](#)
- [SIP Inspection, page 25-68](#)
- [Skinny \(SCCP\) Inspection, page 25-74](#)
- [SMTP and Extended SMTP Inspection, page 25-78](#)
- [SNMP Inspection, page 25-79](#)
- [SQL*Net Inspection, page 25-79](#)
- [Sun RPC Inspection, page 25-80](#)
- [TFTP Inspection, page 25-83](#)
- [XDMCP Inspection, page 25-83](#)

Inspection Engine Overview

This section includes the following topics:

- [When to Use Application Protocol Inspection, page 25-2](#)
- [Inspection Limitations, page 25-2](#)
- [Default Inspection Policy, page 25-3](#)

When to Use Application Protocol Inspection

When a user establishes a connection, the security appliance checks the packet against access lists, creates an address translation, and creates an entry for the session in the fast path, so that further packets can bypass time-consuming checks. However, the fast path relies on predictable port numbers and does not perform address translations inside a packet.

Many protocols open secondary TCP or UDP ports. The initial session on a well-known port is used to negotiate dynamically assigned port numbers.

Other applications embed an IP address in the packet that needs to match the source address that is normally translated when it goes through the security appliance.

If you use applications like these, then you need to enable application inspection.

When you enable application inspection for a service that embeds IP addresses, the security appliance translates embedded addresses and updates any checksum or other fields that are affected by the translation.

When you enable application inspection for a service that uses dynamically assigned ports, the security appliance monitors sessions to identify the dynamic port assignments, and permits data exchange on these ports for the duration of the specific session.

Inspection Limitations

See the following limitations for application protocol inspection:

- State information for multimedia sessions that require inspection are not passed over the state link for stateful failover. The exception is GTP, which is replicated over the state link.
- Some inspection engines do not support PAT, NAT, outside NAT, or NAT between same security interfaces. See “[Default Inspection Policy](#)” for more information about NAT support.
- For all the application inspections, the adaptive security appliance limits the number of simultaneous, active data connections to 200 connections. For example, if an FTP client opens multiple secondary connections, the FTP inspection engine allows only 200 active connections and the 201 connection is dropped and the adaptive security appliance generates a system error message.

Default Inspection Policy

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, so 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.

[Table 25-1](#) lists all inspections supported, the default ports used in the default class map, and the inspection engines that are on by default, shown in bold. This table also notes any NAT limitations.

Table 25-1 Supported Application Inspection Engines

Application ¹	Default Port	NAT Limitations	Standards ²	Comments
CTIQBE	TCP/2748	—	—	—
DNS over UDP	UDP/53	No NAT support is available for name resolution through WINS.	RFC 1123	No PTR records are changed.
FTP	TCP/21	—	RFC 959	—
GTP	UDP/3386 UDP/2123	—	—	Requires a special license.
H.323 H.225 and RAS	TCP/1720 UDP/1718 UDP (RAS) 1718-1719	No NAT on same security interfaces. No static PAT.	ITU-T H.323, H.245, H225.0, Q.931, Q.932	—
HTTP	TCP/80	—	RFC 2616	Beware of MTU limitations stripping ActiveX and Java. If the MTU is too small to allow the Java or ActiveX tag to be included in one packet, stripping may not occur.
ICMP	—	—	—	All ICMP traffic is matched in the default class map.
ICMP ERROR	—	—	—	All ICMP traffic is matched in the default class map.
ILS (LDAP)	TCP/389	No PAT.	—	—
MGCP	UDP/2427, 2727	—	RFC 2705bis-05	—

Table 25-1 Supported Application Inspection Engines (continued)

Application ¹	Default Port	NAT Limitations	Standards ²	Comments
NetBIOS Name Server over IP	UDP/137, 138 (Source ports)	—	—	NetBIOS is supported by performing NAT of the packets for NBNS UDP port 137 and NBDS UDP port 138.
PPTP	TCP/1723	—	RFC 2637	—
RADIUS Accounting	1646	—	RFC 2865	—
RSH	TCP/514	No PAT	Berkeley UNIX	—
RTSP	TCP/554	No PAT. No outside NAT.	RFC 2326, 2327, 1889	No handling for HTTP cloaking.
SIP	TCP/5060 UDP/5060	No outside NAT. No NAT on same security interfaces.	RFC 3261	—
SKINNY (SCCP)	TCP/2000	No outside NAT. No NAT on same security interfaces.	—	Does not handle TFTP uploaded Cisco IP Phone configurations under certain circumstances.
SMTP and ESMTP	TCP/25	—	RFC 821, 1123, 1870	—
SNMP	UDP/161, 162	No NAT or PAT.	RFC 1155, 1157, 1212, 1213, 1215	v.2 RFC 1902-1908; v.3 RFC 2570-2580.
SQL*Net	TCP/1521	—	—	v.1 and v.2.
Sun RPC over UDP and TCP	UDP/111	No NAT or PAT.	—	The default class map includes UDP port 111; if you want to enable Sun RPC inspection for TCP port 111, you need to create a new class map that matches TCP port 111, add the class to the policy, and then apply the inspect sunrpc command to that class.
TFTP	UDP/69	—	RFC 1350	Payload IP addresses are not translated.
XDCMP	UDP/177	No NAT or PAT.	—	—

1. Inspection engines that are enabled by default for the default port are in bold.
2. The security appliance is in compliance with these standards, but it does not enforce compliance on packets being inspected. For example, FTP commands are supposed to be in a particular order, but the security appliance does not enforce the order.

The default policy configuration includes the following commands:

```
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 rsh
inspect rtsp
inspect esmtp
inspect sqlnet
inspect skinny
inspect sunrpc
inspect xdmcp
inspect sip
inspect netbios
inspect tftp
service-policy global_policy global
```

Configuring Application Inspection

This feature uses Modular Policy Framework, so that implementing application inspection consists of identifying traffic, applying inspections to the traffic, and activating inspections on an interface. For some applications, you can perform special actions when you enable inspection. See [Chapter 21, “Using Modular Policy Framework,”](#) for more information.

Inspection is enabled by default for some applications. See the [“Default Inspection Policy”](#) section for more information. Use this section to modify your inspection policy.

To configure application inspection, perform the following steps:

- Step 1** To identify the traffic to which you want to apply inspections, add either a Layer 3/4 class map for through traffic or a Layer 3/4 class map for management traffic. See the [“Creating a Layer 3/4 Class Map for Through Traffic”](#) section on page 21-5 and [“Creating a Layer 3/4 Class Map for Management Traffic”](#) section on page 21-7 for detailed information. The management Layer 3/4 class map can be used only with the RADIUS accounting inspection.

The default Layer 3/4 class map for through traffic is called “inspection_default.” It matches traffic using a special **match** command, **match default-inspection-traffic**, to match the default ports for each application protocol.

You can specify a **match access-list** command along with the **match default-inspection-traffic** command to narrow the matched traffic to specific IP addresses. Because the **match default-inspection-traffic** command specifies the ports to match, any ports in the access list are ignored.

If you want to match non-standard ports, then create a new class map for the non-standard ports. See the [“Default Inspection Policy”](#) section on page 25-3 for the standard ports for each inspection engine. You can combine multiple class maps in the same policy if desired, so you can create one class map to match certain traffic, and another to match different traffic. However, if traffic matches a class map that contains an inspection command, and then matches another class map that also has an inspection command, only the first matching class is used. For example, SNMP matches the inspection_default class. To enable SNMP inspection, enable SNMP inspection for the default class in [Step 5](#). Do not add another class that matches SNMP.

For example, to limit inspection to traffic from 10.1.1.0 to 192.168.1.0 using the default class map, enter the following commands:

```
hostname(config)# access-list inspect extended permit ip 10.1.1.0 255.255.255.0
192.168.1.0 255.255.255.0
hostname(config)# class-map inspection_default
hostname(config-cmap)# match access-list inspect
```

View the entire class map using the following command:

```
hostname(config-cmap)# show running-config class-map inspection_default
!
class-map inspection_default
 match default-inspection-traffic
 match access-list inspect
!
```

To inspect FTP traffic on port 21 as well as 1056 (a non-standard port), create an access list that specifies the ports, and assign it to a new class map:

```
hostname(config)# access-list ftp_inspect extended permit tcp any any eq 21
hostname(config)# access-list ftp_inspect extended permit tcp any any eq 1056
hostname(config)# class-map new_inspection
hostname(config-cmap)# match access-list ftp_inspect
```

Step 2 (Optional) Some inspection engines let you control additional parameters when you apply the inspection to the traffic. See the following sections to configure an inspection policy map for your application:

- DCERPC—See the “Configuring a DCERPC Inspection Policy Map for Additional Inspection Control” section on page 25-12
- DNS—See the “Configuring a DNS Inspection Policy Map for Additional Inspection Control” section on page 25-21
- ESMTP—See the “Configuring an ESMTP Inspection Policy Map for Additional Inspection Control” section on page 25-24
- FTP—See the “Configuring an FTP Inspection Policy Map for Additional Inspection Control” section on page 25-29.
- GTP—See the “Configuring a GTP Inspection Policy Map for Additional Inspection Control” section on page 25-36.
- H323—See the “Configuring an H.323 Inspection Policy Map for Additional Inspection Control” section on page 25-42
- HTTP—See the “Configuring an HTTP Inspection Policy Map for Additional Inspection Control” section on page 25-48.
- Instant Messaging—See the “Configuring an Instant Messaging Inspection Policy Map for Additional Inspection Control” section on page 25-52
- MGCP—See the “Configuring an MGCP Inspection Policy Map for Additional Inspection Control” section on page 25-61.
- NetBIOS—See the “Configuring a NetBIOS Inspection Policy Map for Additional Inspection Control” section on page 25-63
- RADIUS Accounting—See the “Configuring a RADIUS Inspection Policy Map for Additional Inspection Control” section on page 25-66
- SIP—See the “Configuring a SIP Inspection Policy Map for Additional Inspection Control” section on page 25-70
- Skinny—See the “Configuring a Skinny (SCCP) Inspection Policy Map for Additional Inspection Control” section on page 25-76
- SNMP—See the “SNMP Inspection” section on page 25-79.

Step 3 To add or edit a Layer 3/4 policy map that sets the actions to take with the class map traffic, enter the following command:

```
hostname(config)# policy-map name
hostname(config-pmap)#
```

The default policy map is called “global_policy.” This policy map includes the default inspections listed in the “[Default Inspection Policy](#)” section on page 25-3. If you want to modify the default policy (for example, to add or delete an inspection, or to identify an additional class map for your actions), then enter **global_policy** as the name.

- Step 4** To identify the class map from [Step 1](#) to which you want to assign an action, enter the following command:

```
hostname(config-pmap)# class class_map_name
hostname(config-pmap-c)#
```

If you are editing the default policy map, it includes the inspection_default class map. You can edit the actions for this class by entering **inspection_default** as the name. To add an additional class map to this policy map, identify a different name. You can combine multiple class maps in the same policy if desired, so you can create one class map to match certain traffic, and another to match different traffic. However, if traffic matches a class map that contains an inspection command, and then matches another class map that also has an inspection command, only the first matching class is used. For example, SNMP matches the inspection_default class map. To enable SNMP inspection, enable SNMP inspection for the default class in [Step 5](#). Do not add another class that matches SNMP.

- Step 5** Enable application inspection by entering the following command:

```
hostname(config-pmap-c)# inspect protocol
```

The *protocol* is one of the following values:

Table 25-2 Protocol Keywords

Keywords	Notes
ctiqbe	—
dcerpc [<i>map_name</i>]	If you added a DCERPC inspection policy map according to “ Configuring a DCERPC Inspection Policy Map for Additional Inspection Control ” section on page 25-12, identify the map name in this command.
dns [<i>map_name</i>]	If you added a DNS inspection policy map according to “ Configuring a DNS Inspection Policy Map for Additional Inspection Control ” section on page 25-21, identify the map name in this command. The default DNS inspection policy map name is “preset_dns_map.” The default inspection policy map sets the maximum DNS packet length to 512 bytes.
esmtplib [<i>map_name</i>]	If you added an ESMTP inspection policy map according to “ Configuring an ESMTP Inspection Policy Map for Additional Inspection Control ” section on page 25-24, identify the map name in this command.
ftp [strict [<i>map_name</i>]]	Use the strict keyword to increase the security of protected networks by preventing web browsers from sending embedded commands in FTP requests. See the “ Using the strict Option ” section on page 25-28 for more information. If you added an FTP inspection policy map according to “ Configuring an FTP Inspection Policy Map for Additional Inspection Control ” section on page 25-29, identify the map name in this command.

Table 25-2 Protocol Keywords

Keywords	Notes
gtp [<i>map_name</i>]	If you added a GTP inspection policy map according to the “ Configuring a GTP Inspection Policy Map for Additional Inspection Control ” section on page 25-36, identify the map name in this command.
h323 h225 [<i>map_name</i>]	If you added an H323 inspection policy map according to “ Configuring an H.323 Inspection Policy Map for Additional Inspection Control ” section on page 25-42, identify the map name in this command.
h323 ras [<i>map_name</i>]	If you added an H323 inspection policy map according to “ Configuring an H.323 Inspection Policy Map for Additional Inspection Control ” section on page 25-42, identify the map name in this command.
http [<i>map_name</i>]	If you added an HTTP inspection policy map according to the “ Configuring an HTTP Inspection Policy Map for Additional Inspection Control ” section on page 25-48, identify the map name in this command.
icmp	—
icmp error	—
ils	—
im [<i>map_name</i>]	If you added an Instant Messaging inspection policy map according to “ Configuring an Instant Messaging Inspection Policy Map for Additional Inspection Control ” section on page 25-52, identify the map name in this command.
mgcp [<i>map_name</i>]	If you added an MGCP inspection policy map according to “ Configuring an MGCP Inspection Policy Map for Additional Inspection Control ” section on page 25-61, identify the map name in this command.
netbios [<i>map_name</i>]	If you added a NetBIOS inspection policy map according to “ Configuring a NetBIOS Inspection Policy Map for Additional Inspection Control ” section on page 25-63, identify the map name in this command.
pptp	—
radius-accounting [<i>map_name</i>]	The radius-accounting keyword is only available for a management class map. See the “ Creating a Layer 3/4 Class Map for Management Traffic ” section on page 21-7 for more information about creating a management class map. If you added a RADIUS accounting inspection policy map according to “ Configuring a RADIUS Inspection Policy Map for Additional Inspection Control ” section on page 25-66, identify the map name in this command.
rsh	—
rtsp	—

Table 25-2 Protocol Keywords

Keywords	Notes
<code>sip</code> [<i>map_name</i>]	If you added a SIP inspection policy map according to “ Configuring a SIP Inspection Policy Map for Additional Inspection Control ” section on page 25-70, identify the map name in this command.
<code>skinny</code> [<i>map_name</i>]	If you added a Skinny inspection policy map according to “ Configuring a Skinny (SCCP) Inspection Policy Map for Additional Inspection Control ” section on page 25-76, identify the map name in this command.
<code>snmp</code> [<i>map_name</i>]	If you added an SNMP inspection policy map according to “ SNMP Inspection ” section on page 25-79, identify the map name in this command.
<code>sqlnet</code>	—
<code>sunrpc</code>	The default class map includes UDP port 111; if you want to enable Sun RPC inspection for TCP port 111, you need to create a new class map that matches TCP port 111, add the class to the policy, and then apply the inspect sunrpc command to that class.
<code>tftp</code>	—
<code>xdmcp</code>	—

Step 6 To activate the policy map on one or more interfaces, enter the following command:

```
hostname(config)# service-policy polycymap_name {global | interface interface_name}
```

Where **global** applies the policy map to all interfaces, and **interface** applies the policy to one interface. By default, the default policy map, “global_policy,” is applied globally. Only one global policy is allowed. You can override the global policy on an interface by applying a service policy to that interface. You can only apply one policy map to each interface.

CTIQBE Inspection

This section describes CTIQBE application inspection. This section includes the following topics:

- [CTIQBE Inspection Overview, page 25-9](#)
- [Limitations and Restrictions, page 25-10](#)
- [Verifying and Monitoring CTIQBE Inspection, page 25-10](#)

CTIQBE Inspection Overview

CTIQBE protocol inspection supports NAT, PAT, and bidirectional NAT. This enables Cisco IP SoftPhone and other Cisco TAPI/JTAPI applications to work successfully with Cisco CallManager for call setup across the security appliance.

TAPI and JTAPI are used by many Cisco VoIP applications. CTIQBE is used by Cisco TSP to communicate with Cisco CallManager.

Limitations and Restrictions

The following summarizes limitations that apply when using CTIQBE application inspection:

- CTIQBE application inspection does not support configurations with the **alias** command.
- Stateful failover of CTIQBE calls is not supported.
- Entering the **debug ctiqbe** command may delay message transmission, which may have a performance impact in a real-time environment. When you enable this debugging or logging and Cisco IP SoftPhone seems unable to complete call setup through the security appliance, increase the timeout values in the Cisco TSP settings on the system running Cisco IP SoftPhone.

The following summarizes special considerations when using CTIQBE application inspection in specific scenarios:

- If two Cisco IP SoftPhones are registered with different Cisco CallManagers, which are connected to different interfaces of the security appliance, calls between these two phones fails.
- When Cisco CallManager is located on the higher security interface compared to Cisco IP SoftPhones, if NAT or outside NAT is required for the Cisco CallManager IP address, the mapping must be static as Cisco IP SoftPhone requires the Cisco CallManager IP address to be specified explicitly in its Cisco TSP configuration on the PC.
- When using PAT or Outside PAT, if the Cisco CallManager IP address is to be translated, its TCP port 2748 must be statically mapped to the same port of the PAT (interface) address for Cisco IP SoftPhone registrations to succeed. The CTIQBE listening port (TCP 2748) is fixed and is not user-configurable on Cisco CallManager, Cisco IP SoftPhone, or Cisco TSP.

Verifying and Monitoring CTIQBE Inspection

The **show ctiqbe** command displays information regarding the CTIQBE sessions established across the security appliance. It shows information about the media connections allocated by the CTIQBE inspection engine.

The following is sample output from the **show ctiqbe** command under the following conditions. There is only one active CTIQBE session setup across the security appliance. It is established between an internal CTI device (for example, a Cisco IP SoftPhone) at local address 10.0.0.99 and an external Cisco CallManager at 172.29.1.77, where TCP port 2748 is the Cisco CallManager. The heartbeat interval for the session is 120 seconds.

```
hostname# # show ctiqbe

Total: 1
-----
LOCAL          FOREIGN        STATE    HEARTBEAT
-----
1             10.0.0.99/1117 172.29.1.77/2748    1        120
-----
RTP/RTCP: PAT xlates: mapped to 172.29.1.99(1028 - 1029)
-----
MEDIA: Device ID 27      Call ID 0
      Foreign 172.29.1.99    (1028 - 1029)
      Local   172.29.1.88      (26822 - 26823)
-----
```

The CTI device has already registered with the CallManager. The device internal address and RTP listening port is PATed to 172.29.1.99 UDP port 1028. Its RTCP listening port is PATed to UDP 1029.

The line beginning with `RTP/RTCP: PAT xlates:` appears only if an internal CTI device has registered with an external CallManager and the CTI device address and ports are PATed to that external interface. This line does not appear if the CallManager is located on an internal interface, or if the internal CTI device address and ports are translated to the same external interface that is used by the CallManager.

The output indicates a call has been established between this CTI device and another phone at 172.29.1.88. The RTP and RTCP listening ports of the other phone are UDP 26822 and 26823. The other phone locates on the same interface as the CallManager because the security appliance does not maintain a CTIQBE session record associated with the second phone and CallManager. The active call leg on the CTI device side can be identified with Device ID 27 and Call ID 0.

The following is sample output from the `show xlate debug` command for these CTIQBE connections:

```
hostname# show xlate debug
3 in use, 3 most used
Flags: D - DNS, d - dump, I - identity, i - inside, n - no random,
      r - portmap, s - static
TCP PAT from inside:10.0.0.99/1117 to outside:172.29.1.99/1025 flags ri idle 0:00:22
timeout 0:00:30
UDP PAT from inside:10.0.0.99/16908 to outside:172.29.1.99/1028 flags ri idle 0:00:00
timeout 0:04:10
UDP PAT from inside:10.0.0.99/16909 to outside:172.29.1.99/1029 flags ri idle 0:00:23
timeout 0:04:10
```

The `show conn state ctiqbe` command displays the status of CTIQBE connections. In the output, the media connections allocated by the CTIQBE inspection engine are denoted by a 'C' flag. The following is sample output from the `show conn state ctiqbe` command:

```
hostname# show conn state ctiqbe
1 in use, 10 most used
hostname# show conn state ctiqbe detail
1 in use, 10 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
      B - initial SYN from outside, C - CTIQBE media, D - DNS, d - dump,
      E - outside back connection, F - outside FIN, f - inside FIN,
      G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
      i - incomplete, J - GTP, j - GTP data, k - Skinny media,
      M - SMTP data, m - SIP media, O - outbound data, P - inside back connection,
      q - SQL*Net data, R - outside acknowledged FIN,
      R - UDP RPC, r - inside acknowledged FIN, S - awaiting inside SYN,
      s - awaiting outside SYN, T - SIP, t - SIP transient, U - up
```

DCERPC Inspection

This section describes the DCERPC inspection engine. This section includes the following topics:

- [DCERPC Overview, page 25-11](#)
- [Configuring a DCERPC Inspection Policy Map for Additional Inspection Control, page 25-12](#)

DCERPC Overview

DCERPC is a protocol widely used by Microsoft distributed client and server applications that allows software clients to execute programs on a server remotely.

DCERPC inspection maps inspection for native TCP communication between a server called the Endpoint Mapper (EPM) and client on the well-known TCP port 135. Map and lookup operations of the EPM are supported for clients. Client and server can be located in any security zone. The embedded server IP address and port number are received from the applicable EPM response messages. Because a client can attempt multiple connections to the server port returned by EPM, creation of multiple pinholes is allowed. User configurable timeouts are allowed for multiple pinholes.

**Note**

DCERPC inspection only supports communication between an EPM server and clients to open pinholes through the security appliance. Clients using RPC communication that does not use an EPM server is not supported with DCERPC inspection.

Typically, software clients remotely execute programs on an EPM server in the following way:

- Step 1** A client queries an EPM server for the dynamically-allocated port number of a required DCERPC service. The EPM server listens on the well-known TCP port 135.
- Step 2** The security appliance, located between the client and EPM server, intercepts the communication.
- Step 3** The EPM server indicates the port number on which the DCERPC service is available.
- Step 4** The security appliance opens a pinhole for that DCERPC service.

**Note**

Because the pinhole does not have a value for the source port, the source port value is set to 0. The source IP address, destination IP address, and destination port are indicated.

- Step 5** Using that pinhole, the client attempts to connect to the DCERPC service on the indicated port.
- Step 6** The security appliance detects that the connection is permitted and creates a secondary connection to the server instance providing the DCERPC service. When creating the secondary connection, the security appliance applies NAT if necessary.

**Note**

When the pinhole timeout is reached, the security appliance destroys the pinhole and permits new connections from the client to the EPM server; existing connections remain, however, because they are independent.

Configuring a DCERPC Inspection Policy Map for Additional Inspection Control

To specify additional DCERPC inspection parameters, create a DCERPC inspection policy map. You can then apply the inspection policy map when you enable DCERPC inspection according to the [“Configuring Application Inspection” section on page 25-5](#).

To create a DCERPC inspection policy map, perform the following steps:

- Step 1** Create a DCERPC inspection policy map, enter the following command:

```
hostname(config)# policy-map type inspect dcerpc policy_map_name
hostname(config-pmap)#
```

Where the *policy_map_name* is the name of the policy map. The CLI enters policy-map configuration mode.

Step 2 (Optional) To add a description to the policy map, enter the following command:

```
hostname(config-pmap)# description string
```

Step 3 To configure parameters that affect the inspection engine, perform the following steps:

a. To enter parameters configuration mode, enter the following command:

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b. To configure the timeout for DCERPC pinholes and override the global system pinhole timeout of two minutes, enter the following command:

```
hostname(config-pmap-p)# timeout pinhole hh:mm:ss
```

Where the *hh:mm:ss* argument is the timeout for pinhole connections. Value is between 0:0:1 and 1193:0:0.

c. To configure options for the endpoint mapper traffic, enter the following command:

```
hostname(config-pmap-p)# endpoint-mapper [service-only] [lookup-operation
timeout hh:mm:ss]
```

Where the *hh:mm:ss* argument is the timeout for pinholes generated from the lookup operation. If no timeout is configured for the lookup operation, the timeout pinhole command or the default is used. The **epm-service-only** keyword enforces endpoint mapper service during binding so that only its service traffic is processed. The **lookup-operation** keyword enables the lookup operation of the endpoint mapper service.

The following example shows how to define a DCERPC inspection policy map with the timeout configured for DCERPC pinholes.

```
hostname(config)# policy-map type inspect dcerpc dcerpc_map
hostname(config-pmap)# timeout pinhole 0:10:00

hostname(config)# class-map dcerpc
hostname(config-cmap)# match port tcp eq 135

hostname(config)# policy-map global-policy
hostname(config-pmap)# class dcerpc
hostname(config-pmap-c)# inspect msrpc dcerpc-map

hostname(config)# service-policy global-policy global
```

DNS Inspection

This section describes DNS application inspection. This section includes the following topics:

- [How DNS Application Inspection Works, page 25-14](#)
- [How DNS Rewrite Works, page 25-14](#)
- [Configuring DNS Rewrite, page 25-15](#)
- [Verifying and Monitoring DNS Inspection, page 25-20](#)

How DNS Application Inspection Works

The security appliance tears down the DNS session associated with a DNS query as soon as the DNS reply is forwarded by the security appliance. The security appliance also monitors the message exchange to ensure that the ID of the DNS reply matches the ID of the DNS query.

When DNS inspection is enabled, which is the default, the security appliance performs the following additional tasks:

- Translates the DNS record based on the configuration completed using the **alias**, **static** and **nat** commands (DNS Rewrite). Translation only applies to the A-record in the DNS reply; therefore, DNS Rewrite does not affect reverse lookups, which request the PTR record.



Note DNS Rewrite is not applicable for PAT because multiple PAT rules are applicable for each A-record and the PAT rule to use is ambiguous.

- Enforces the maximum DNS message length (the default is 512 bytes and the maximum length is 65535 bytes). The security appliance performs reassembly as needed to verify that the packet length is less than the maximum length configured. The security appliance drops the packet if it exceeds the maximum length.



Note If you enter the **inspect dns** command without the **maximum-length** option, DNS packet size is not checked

- Enforces a domain-name length of 255 bytes and a label length of 63 bytes.
- Verifies the integrity of the domain-name referred to by the pointer if compression pointers are encountered in the DNS message.
- Checks to see if a compression pointer loop exists.

A single connection is created for multiple DNS sessions, as long as they are between the same two hosts, and the sessions have the same 5-tuple (source/destination IP address, source/destination port, and protocol). DNS identification is tracked by *app_id*, and the idle timer for each *app_id* runs independently.

Because the *app_id* expires independently, a legitimate DNS response can only pass through the security appliance within a limited period of time and there is no resource build-up. However, if you enter the **show conn** command, you will see the idle timer of a DNS connection being reset by a new DNS session. This is due to the nature of the shared DNS connection and is by design.

How DNS Rewrite Works

When DNS inspection is enabled, DNS rewrite provides full support for NAT of DNS messages originating from any interface.

If a client on an inside network requests DNS resolution of an inside address from a DNS server on an outside interface, the DNS A-record is translated correctly. If the DNS inspection engine is disabled, the A-record is not translated.

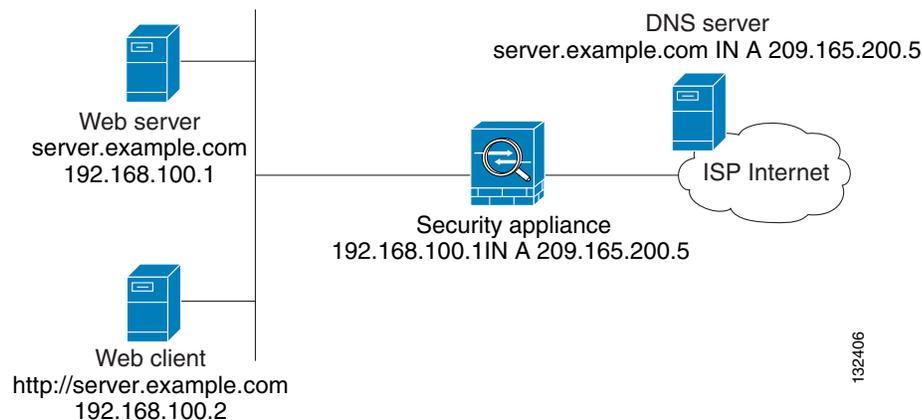
As long as DNS inspection remains enabled, you can configure DNS rewrite using the **alias**, **static**, or **nat** commands. For details about the configuration required see the [“Configuring DNS Rewrite” section on page 25-15](#).

DNS Rewrite performs two functions:

- Translating a public address (the routable or “mapped” address) in a DNS reply to a private address (the “real” address) when the DNS client is on a private interface.
- Translating a private address to a public address when the DNS client is on the public interface.

In [Figure 25-1](#), the DNS server resides on the external (ISP) network. The real address of the server (192.168.100.1) has been mapped using the **static** command to the ISP-assigned address (209.165.200.5). When a web client on the inside interface attempts to access the web server with the URL `http://server.example.com`, the host running the web client sends a DNS request to the DNS server to resolve the IP address of the web server. The security appliance translates the non-routable source address in the IP header and forwards the request to the ISP network on its outside interface. When the DNS reply is returned, the security appliance applies address translation not only to the destination address, but also to the embedded IP address of the web server, which is contained in the A-record in the DNS reply. As a result, the web client on the inside network gets the correct address for connecting to the web server on the inside network. For configuration instructions for scenarios similar to this one, see the “[Configuring DNS Rewrite with Two NAT Zones](#)” section on [page 25-16](#).

Figure 25-1 Translating the Address in a DNS Reply (DNS Rewrite)



DNS rewrite also works if the client making the DNS request is on a DMZ network and the DNS server is on an inside interface. For an illustration and configuration instructions for this scenario, see the “[DNS Rewrite with Three NAT Zones](#)” section on [page 25-17](#).

Configuring DNS Rewrite

You configure DNS rewrite using the **alias**, **static**, or **nat** commands. The **alias** and **static** command can be used interchangeably; however, we recommend using the **static** command for new deployments because it is more precise and unambiguous. Also, DNS rewrite is optional when using the **static** command.

This section describes how to use the **alias** and **static** commands to configure DNS rewrite. It provides configuration procedures for using the **static** command in a simple scenario and in a more complex scenario. Using the **nat** command is similar to using the **static** command except that DNS Rewrite is based on dynamic translation instead of a static mapping.

This section includes the following topics:

- [Using the Static Command for DNS Rewrite, page 25-16](#)
- [Using the Static Command for DNS Rewrite, page 25-16](#)

- [Configuring DNS Rewrite with Two NAT Zones, page 25-16](#)
- [DNS Rewrite with Three NAT Zones, page 25-17](#)
- [Configuring DNS Rewrite with Three NAT Zones, page 25-19](#)

For detailed syntax and additional functions for the **alias**, **nat**, and **static** command, see the appropriate command page in the *Cisco Security Appliance Command Reference*.

Using the Static Command for DNS Rewrite

The **static** command causes addresses on an IP network residing on a specific interface to be translated into addresses on another IP network on a different interface. The syntax for this command is as follows:

```
hostname(config)# static (real_ifc,mapped_ifc) mapped-address real-address dns
```

The following example specifies that the address 192.168.100.10 on the inside interface is translated into 209.165.200.5 on the outside interface:

```
hostname(config)# static (inside,outside) 209.165.200.225 192.168.100.10 dns
```



Note

Using the **nat** command is similar to using the **static** command except that DNS Rewrite is based on dynamic translation instead of a static mapping.

Using the Alias Command for DNS Rewrite

The **alias** command causes the security appliance to translate addresses on an IP network residing on any interface into addresses on another IP network connected through a different interface. The syntax for this command is as follows:

```
hostname(config)# alias (interface_name) mapped-address real-address
```

The following example specifies that the real address (192.168.100.10) on any interface except the inside interface will be translated to the mapped address (**209.165.200.225**) on the inside interface. Notice that the location of 192.168.100.10 is not precisely defined.

```
hostname(config)# alias (inside) 209.165.200.225 192.168.100.10
```



Note

If you use the **alias** command to configure DNS Rewrite, proxy ARP will be performed for the mapped address. To prevent this, disable Proxy ARP by entering the **sysopt noproxyarp** command after entering the **alias** command.

Configuring DNS Rewrite with Two NAT Zones

To implement a DNS Rewrite scenario similar to the one shown in [Figure 25-1](#), perform the following steps:

- Step 1** Create a static translation for the web server, as follows:

```
hostname(config)# static (real_ifc,mapped_ifc) mapped-address real-address netmask  
255.255.255.255 dns
```

where the arguments are as follows:

- *real_ifc*—The name of the interface connected to the real addresses.
- *mapped_ifc*—The name of the interface where you want the addresses to be mapped.
- *mapped-address*—The translated IP address of the web server.
- *real-address*—The real IP address of the web server.

Step 2 Create an access list that permits traffic to the port that the web server listens to for HTTP requests.

```
hostname(config)# access-list acl-name extended permit tcp any host mapped-address eq port
```

where the arguments are as follows:

acl-name—The name you give the access list.

mapped-address—The translated IP address of the web server.

port—The TCP port that the web server listens to for HTTP requests.

Step 3 Apply the access list created in [Step 2](#) to the mapped interface. To do so, use the **access-group** command, as follows:

```
hostname(config)# access-group acl-name in interface mapped_ifc
```

Step 4 If DNS inspection is disabled or if you want to change the maximum DNS packet length, configure DNS inspection. DNS application inspection is enabled by default with a maximum DNS packet length of 512 bytes. For configuration instructions, see the [“Configuring Application Inspection”](#) section on [page 25-5](#).

Step 5 On the public DNS server, add an A-record for the web server, such as:

```
domain-qualified-hostname. IN A mapped-address
```

where *domain-qualified-hostname* is the hostname with a domain suffix, as in server.example.com. The period after the hostname is important. *mapped-address* is the translated IP address of the web server.

The following example configures the security appliance for the scenario shown in [Figure 25-1](#). It assumes DNS inspection is already enabled.

```
hostname(config)# static (inside,outside) 209.165.200.225 192.168.100.1 netmask  
255.255.255.255 dns  
hostname(config)# access-list 101 permit tcp any host 209.165.200.225 eq www  
hostname(config)# access-group 101 in interface outside
```

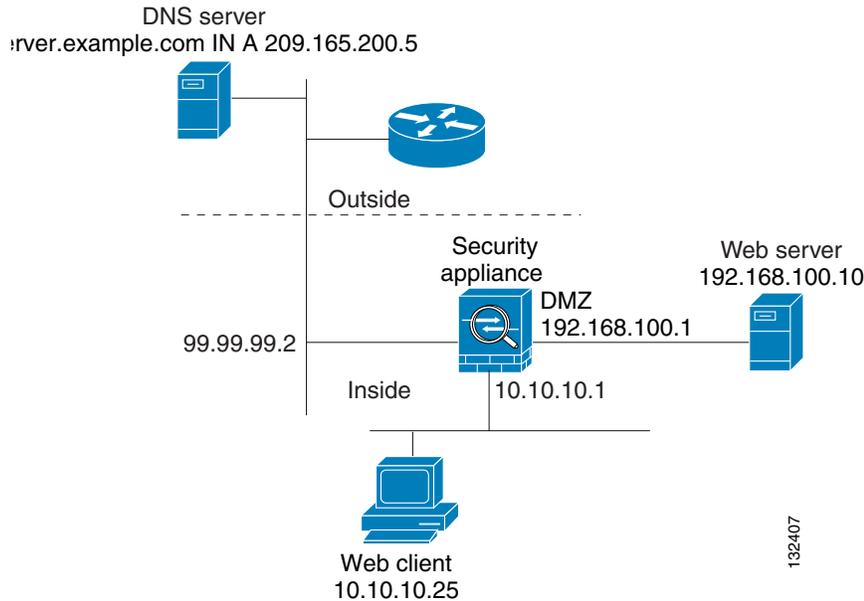
This configuration requires the following A-record on the DNS server:

```
server.example.com. IN A 209.165.200.225
```

DNS Rewrite with Three NAT Zones

[Figure 25-2](#) provides a more complex scenario to illustrate how DNS inspection allows NAT to operate transparently with a DNS server with minimal configuration. For configuration instructions for scenarios like this one, see the [“Configuring DNS Rewrite with Three NAT Zones”](#) section on [page 25-19](#).

Figure 25-2 DNS Rewrite with Three NAT Zones



In [Figure 25-2](#), a web server, `server.example.com`, has the real address `192.168.100.10` on the DMZ interface of the security appliance. A web client with the IP address `10.10.10.25` is on the inside interface and a public DNS server is on the outside interface. The site NAT policies are as follows:

- The outside DNS server holds the authoritative address record for `server.example.com`.
- Hosts on the outside network can contact the web server with the domain name `server.example.com` through the outside DNS server or with the IP address `209.165.200.5`.
- Clients on the inside network can access the web server with the domain name `server.example.com` through the outside DNS server or with the IP address `192.168.100.10`.

When a host or client on any interface accesses the DMZ web server, it queries the public DNS server for the A-record of `server.example.com`. The DNS server returns the A-record showing that `server.example.com` binds to address `209.165.200.5`.

When a web client on the *outside* network attempts to access `http://server.example.com`, the sequence of events is as follows:

1. The host running the web client sends the DNS server a request for the IP address of `server.example.com`.
2. The DNS server responds with the IP address `209.165.200.225` in the reply.
3. The web client sends its HTTP request to `209.165.200.225`.
4. The packet from the outside host reaches the security appliance at the outside interface.
5. The static rule translates the address `209.165.200.225` to `192.168.100.10` and the security appliance directs the packet to the web server on the DMZ.

When a web client on the *inside* network attempts to access `http://server.example.com`, the sequence of events is as follows:

1. The host running the web client sends the DNS server a request for the IP address of `server.example.com`.
2. The DNS server responds with the IP address `209.165.200.225` in the reply.

3. The security appliance receives the DNS reply and submits it to the DNS application inspection engine.
 4. The DNS application inspection engine does the following:
 - a. Searches for any NAT rule to undo the translation of the embedded A-record address “[outside]:209.165.200.5”. In this example, it finds the following static configuration:


```
static (dmz, outside) 209.165.200.225 192.168.100.10 dns
```
 - b. Uses the static rule to rewrite the A-record as follows because the **dns** option is included:


```
[outside]:209.165.200.225 --> [dmz]:192.168.100.10
```
-
-  **Note** If the **dns** option were not included with the **static** command, DNS Rewrite would not be performed and other processing for the packet continues.
-
- c. Searches for any NAT to translate the web server address, [dmz]:192.168.100.10, when communicating with the inside web client.

No NAT rule is applicable, so application inspection completes.

If a NAT rule (nat or static) were applicable, the **dns** option must also be specified. If the **dns** option were not specified, the A-record rewrite in step b would be reverted and other processing for the packet continues.
5. The security appliance sends the HTTP request to server.example.com on the DMZ interface.

Configuring DNS Rewrite with Three NAT Zones

To enable the NAT policies for the scenario in [Figure 25-2](#), perform the following steps:

-
- Step 1** Create a static translation for the web server on the DMZ network, as follows:
- ```
hostname(config)# static (dmz, outside) mapped-address real-address dns
```
- where the arguments are as follows:
- *dmz*—The name of the DMZ interface of the security appliance.
  - *outside*—The name of the outside interface of the security appliance.
  - *mapped-address*—The translated IP address of the web server.
  - *real-address*—The real IP address of the web server.
- Step 2** Create an access list that permits traffic to the port that the web server listens to for HTTP requests.
- ```
hostname(config)# access-list acl-name extended permit tcp any host mapped-address eq port
```
- where the arguments are as follows:
- acl-name*—The name you give the access list.
- mapped-address*—The translated IP address of the web server.
- port*—The TCP port that the web server listens to for HTTP requests.
- Step 3** Apply the access list created in [Step 2](#) to the outside interface. To do so, use the **access-group** command, as follows:
- ```
hostname(config)# access-group acl-name in interface outside
```

**Step 4** If DNS inspection is disabled or if you want to change the maximum DNS packet length, configure DNS inspection. DNS application inspection is enabled by default with a maximum DNS packet length of 512 bytes. For configuration instructions, see the “[Configuring Application Inspection](#)” section on [page 25-5](#).

**Step 5** On the public DNS server, add an A-record for the web server, such as:

```
domain-qualified-hostname. IN A mapped-address
```

where *domain-qualified-hostname* is the hostname with a domain suffix, as in `server.example.com`. The period after the hostname is important. *mapped-address* is the translated IP address of the web server.

The following example configures the security appliance for the scenario shown in [Figure 25-2](#). It assumes DNS inspection is already enabled.

```
hostname(config)# static (dmz,outside) 209.165.200.225 192.168.100.10 dns
hostname(config)# access-list 101 permit tcp any host 209.165.200.225 eq www
hostname(config)# access-group 101 in interface outside
```

This configuration requires the following A-record on the DNS server:

```
server.example.com. IN A 209.165.200.225
```

## Verifying and Monitoring DNS Inspection

To view information about the current DNS connections, enter the following command:

```
hostname# show conn
```

For connections using a DNS server, the source port of the connection may be replaced by the IP address of DNS server in the `show conn` command output.

A single connection is created for multiple DNS sessions, as long as they are between the same two hosts, and the sessions have the same 5-tuple (source/destination IP address, source/destination port, and protocol). DNS identification is tracked by `app_id`, and the idle timer for each `app_id` runs independently.

Because the `app_id` expires independently, a legitimate DNS response can only pass through the security appliance within a limited period of time and there is no resource build-up. However, when you enter the `show conn` command, you see the idle timer of a DNS connection being reset by a new DNS session. This is due to the nature of the shared DNS connection and is by design.

To display the statistics for DNS application inspection, enter the `show service-policy` command. The following is sample output from the `show service-policy` command:

```
hostname# show service-policy
Interface outside:
 Service-policy: sample_policy
 Class-map: dns_port
 Inspect: dns maximum-length 1500, packet 0, drop 0, reset-drop 0
```

## Configuring a DNS Inspection Policy Map for Additional Inspection Control

DNS application inspection supports DNS message controls that provide protection against DNS spoofing and cache poisoning. User configurable rules allow filtering based on DNS header, domain name, resource record type and class. Zone transfer can be restricted between servers with this function, for example.

The Recursion Desired and Recursion Available flags in the DNS header can be masked to protect a public server from attack if that server only supports a particular internal zone. In addition, DNS randomization can be enabled to avoid spoofing and cache poisoning of servers that either do not support randomization, or utilize a weak pseudo random number generator. Limiting the domain names that can be queried also restricts the domain names which can be queried, which protects the public server further.

A configurable DNS mismatch alert can be used as notification if an excessive number of mismatching DNS responses are received, which could indicate a cache poisoning attack. In addition, a configurable check to enforce a Transaction Signature be attached to all DNS messages is also supported.

To specify actions when a message violates a parameter, create a DNS inspection policy map. You can then apply the inspection policy map when you enable DNS inspection according to the [“Configuring Application Inspection”](#) section on page 25-5.

To create a DNS inspection policy map, perform the following steps:

- 
- Step 1** (Optional) Add one or more regular expressions for use in traffic matching commands according to the [“Creating a Regular Expression”](#) section on page 21-12. See the types of text you can match in the **match** commands described in Step 3.
  - Step 2** (Optional) Create one or more regular expression class maps to group regular expressions according to the [“Creating a Regular Expression Class Map”](#) section on page 21-14.
  - Step 3** (Optional) Create a DNS inspection class map by performing the following steps.

A class map groups multiple traffic matches. Traffic must match *all* of the **match** commands to match the class map. You can alternatively identify **match** commands directly in the policy map. The difference between creating a class map and defining the traffic match directly in the inspection policy map is that the class map lets you create more complex match criteria, and you can reuse class maps.

To specify traffic that should not match the class map, use the **match not** command. For example, if the **match not** command specifies the string “example.com,” then any traffic that includes “example.com” does not match the class map.

For the traffic that you identify in this class map, you can specify actions such as drop, drop-connection, reset, mask, set the rate limit, and/or log the connection in the inspection policy map.

If you want to perform different actions for each **match** command, you should identify the traffic directly in the policy map.

- a. Create the class map by entering the following command:

```
hostname(config)# class-map type inspect dns [match-all] class_map_name
hostname(config-cmap)#
```

Where *class\_map\_name* is the name of the class map. The **match-all** keyword specifies that traffic must match all criteria to match the class map. **match-all** is the default and only option. The CLI enters class-map configuration mode, where you can enter one or more **match** commands.

- b. (Optional) To add a description to the class map, enter the following command:

```
hostname(config-cmap)# description string
```

- c. (Optional) To match a specific flag that is set in the DNS header, enter the following command:

```
hostname(config-cmap)# match [not] header-flag [eq] {f_well_known | f_value}
```

Where the *f\_well\_known* argument is the DNS flag bit. The *f\_value* argument is the 16-bit value in hex. The **eq** keyword specifies an exact match.

- d. (Optional) To match a DNS type, including Query type and RR type, enter the following command:

```
hostname(config-cmap)# match [not] dns-type [eq t_well_known | t_val] {range t_val1 t_val2}
```

Where the *t\_well\_known* argument is the DNS flag bit. The *t\_val* arguments are arbitrary values in the DNS type field (0-65535). The **range** keyword specifies a range and the **eq** keyword specifies an exact match.

- e. (Optional) To match a DNS class, enter the following command:

```
hostname(config-cmap)# match [not] dns-class [eq c_well_known | c_val] {range c_val1 c_val2}
```

Where the *c\_well\_known* argument is the DNS class. The *c\_val* arguments are arbitrary values in the DNS class field. The **range** keyword specifies a range and the **eq** keyword specifies an exact match.

- f. (Optional) To match a DNS question or resource record, enter the following command:

```
hostname(config-cmap)# match {question | {resource-record answer | authority | any}}
```

Where the **question** keyword specifies the question portion of a DNS message. The **resource-record** keyword specifies the resource record portion of a DNS message. The **answer** keyword specifies the Answer RR section. The **authority** keyword specifies the Authority RR section. The **additional** keyword specifies the Additional RR section.

- g. (Optional) To match a DNS message domain name list, enter the following command:

```
hostname(config-cmap)# match [not] domain-name {regex regex_id | regex class class_id}
```

The **regex** *regex\_name* argument is the regular expression you created in [Step 1](#). The **class** *regex\_class\_name* is the regular expression class map you created in [Step 2](#).

- Step 4** Create a DNS inspection policy map, enter the following command:

```
hostname(config)# policy-map type inspect dns policy_map_name
hostname(config-pmap)#
```

Where the *policy\_map\_name* is the name of the policy map. The CLI enters policy-map configuration mode.

- Step 5** (Optional) To add a description to the policy map, enter the following command:

```
hostname(config-pmap)# description string
```

- Step 6** To apply actions to matching traffic, perform the following steps.

- a. Specify the traffic on which you want to perform actions using one of the following methods:

- Specify the DNS class map that you created in [Step 3](#) by entering the following command:

```
hostname(config-pmap)# class class_map_name
hostname(config-pmap-c)#
```

- Specify traffic directly in the policy map using one of the **match** commands described in [Step 3](#). If you use a **match not** command, then any traffic that does not match the criterion in the **match not** command has the action applied.

- b. Specify the action you want to perform on the matching traffic by entering the following command:

```
hostname(config-pmap-c)# {[drop [send-protocol-error] |
drop-connection [send-protocol-error] | mask | reset] [log] | rate-limit message_rate}
```

Not all options are available for each **match** or **class** command. See the CLI help or the *Cisco Security Appliance Command Reference* for the exact options available.

The **drop** keyword drops all packets that match.

The **send-protocol-error** keyword sends a protocol error message.

The **drop-connection** keyword drops the packet and closes the connection.

The **mask** keyword masks out the matching portion of the packet.

The **reset** keyword drops the packet, closes the connection, and sends a TCP reset to the server and/or client.

The **log** keyword, which you can use alone or with one of the other keywords, sends a system log message.

The **rate-limit message\_rate** argument limits the rate of messages.

You can specify multiple **class** or **match** commands in the policy map. For information about the order of **class** and **match** commands, see the “[Defining Actions in an Inspection Policy Map](#)” section on page 21-8.

- Step 7** To configure parameters that affect the inspection engine, perform the following steps:

- a. To enter parameters configuration mode, enter the following command:

```
hostname(config-pmap) # parameters
hostname(config-pmap-p) #
```

- b. To randomize the DNS identifier for a DNS query, enter the following command:

```
hostname(config-pmap-p) # id-randomization
```

- c. To enable logging for excessive DNS ID mismatches, enter the following command:

```
hostname(config-pmap-p) # id-mismatch [count number duration seconds] action log
```

Where the **count string** argument specifies the maximum number of mismatch instances before a system message log is sent. The **duration seconds** specifies the period, in seconds, to monitor.

- d. To require a TSIG resource record to be present, enter the following command:

```
hostname(config-pmap-p) # tsig enforced action {drop [log] | [log]}
```

Where the **count string** argument specifies the maximum number of mismatch instances before a system message log is sent. The **duration seconds** specifies the period, in seconds, to monitor.

The following example shows a how to define a DNS inspection policy map.

```
hostname(config)# regex domain_example "example\.com"
hostname(config)# regex domain_foo "foo\.com"

hostname(config)# ! define the domain names that the server serves
hostname(config)# class-map type inspect regex match-any my_domains
hostname(config-cmap)# match regex domain_example
hostname(config-cmap)# match regex domain_foo

hostname(config)# ! Define a DNS map for query only
hostname(config)# class-map type inspect dns match-all pub_server_map
```

```

hostname(config-cmap)# match not header-flag QR
hostname(config-cmap)# match question
hostname(config-cmap)# match not domain-name regex class my_domains

hostname(config)# policy-map type inspect dns serv_prot
hostname(config-pmap)# class pub_server_map
hostname(config-pmap-c)# drop log
hostname(config-pmap-c)# match header-flag RD
hostname(config-pmap-c)# mask log

hostname(config)# class-map dns_serv_map
hostname(config-cmap)# match default-inspection-traffic

hostname(config)# policy-map pub_policy
hostname(config-pmap)# class dns_serv_map
hostname(config-pmap-c)# inspect dns serv_prot

hostname(config)# service-policy pub_policy interface dmz

```

## ESMTP Inspection

ESMTP inspection detects attacks, including spam, phishing, malformed message attacks, buffer overflow/underflow attacks. It also provides support for application security and protocol conformance, which enforce the sanity of the ESMTP messages as well as detect several attacks, block senders/receivers, and block mail relay.

## Configuring an ESMTP Inspection Policy Map for Additional Inspection Control

To specify actions when a message violates a parameter, create an ESMTP inspection policy map. You can then apply the inspection policy map when you enable ESMTP inspection according to the [“Configuring Application Inspection”](#) section on page 25-5.

To create an ESMTP inspection policy map, perform the following steps:

- 
- Step 1** (Optional) Add one or more regular expressions for use in traffic matching commands according to the [“Creating a Regular Expression”](#) section on page 21-12. See the types of text you can match in the **match** commands described in [Step 3](#).
  - Step 2** (Optional) Create one or more regular expression class maps to group regular expressions according to the [“Creating a Regular Expression Class Map”](#) section on page 21-14.
  - Step 3** Create an ESMTP inspection policy map, enter the following command:
 

```
hostname(config)# policy-map type inspect esmtp policy_map_name
hostname(config-pmap)#
```

Where the *policy\_map\_name* is the name of the policy map. The CLI enters policy-map configuration mode.

- Step 4** (Optional) To add a description to the policy map, enter the following command:
 

```
hostname(config-pmap)# description string
```

**Step 5** To apply actions to matching traffic, perform the following steps.

- a. Specify traffic directly in the policy map using one of the **match** commands described in [Step 3](#). If you use a **match not** command, then any traffic that does not match the criterion in the **match not** command has the action applied.
- b. Specify the action you want to perform on the matching traffic by entering the following command:

```
hostname(config-pmap-c)# [[drop [send-protocol-error] |
drop-connection [send-protocol-error] | mask | reset] [log] | rate-limit message_rate}
```

Not all options are available for each **match** or **class** command. See the CLI help or the *Cisco Security Appliance Command Reference* for the exact options available.

The **drop** keyword drops all packets that match.

The **send-protocol-error** keyword sends a protocol error message.

The **drop-connection** keyword drops the packet and closes the connection.

The **mask** keyword masks out the matching portion of the packet.

The **reset** keyword drops the packet, closes the connection, and sends a TCP reset to the server and/or client.

The **log** keyword, which you can use alone or with one of the other keywords, sends a system log message.

The **rate-limit message\_rate** argument limits the rate of messages.

You can specify multiple **class** or **match** commands in the policy map. For information about the order of **class** and **match** commands, see the “[Defining Actions in an Inspection Policy Map](#)” section on [page 21-8](#).

**Step 6** To configure parameters that affect the inspection engine, perform the following steps:

- a. To enter parameters configuration mode, enter the following command:

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

- b. To configure a local domain name, enter the following command:

```
hostname(config-pmap-p)# mail-relay domain-name action [drop-connection / log]]
```

Where the **drop-connection** action closes the connection. The **log** action sends a system log message when this policy map matches traffic.

- c. To enforce banner obfuscation, enter the following command:

```
hostname(config-pmap-p)# mask-banner
```

- d. (Optional) To detect special characters in sender or receiver email addresses, enter the following command:

```
hostname(config-pmap-p)# special-character action [drop-connection | log]]
```

Using this command detects pipe (|), backquote (`) and null characters.

- e. (Optional) To match the body length or body line length, enter the following command:

```
hostname(config-pmap-p)# match body [line] length gt length
```

Where *length* is the length of the message body or the length of a line in the message body.

- f. (Optional) To match an ESMTP command verb, enter the following command:

```
hostname(config-pmap-p)# match cmd verb verb
```

Where *verb* is any of the following ESMTP commands:

```
AUTH|DATA|EHLO|ETRN|HELO|HELP|MAIL|NOOP|QUIT|RCPT|RSET|SAML|SOML|VRFY
```

- g. (Optional) To match the number of recipient addresses, enter the following command:

```
hostname(config-pmap-p)# match cmd RCPT count gt count
```

Where *count* is the number of recipient addresses.

- h. (Optional) To match the command line length, enter the following command:

```
hostname(config-pmap-p)# match cmd line length gt length
```

Where *length* is the command line length.

- i. (Optional) To match the ehlo-reply-parameters, enter the following command:

```
hostname(config-pmap-p)# match ehlo-reply-parameter extensions
```

Where *extensions* are the ESMTP service extensions sent by the server in response to the EHLO message from the client. These extensions are implemented as a new command or as parameters to an existing command. *extensions* can be any of the following:

```
8bitmime|binarymime|checkpoint|dsn|ecode|etrn|others|pipelining|size|vrfy
```

- j. (Optional) To match the header length or header line length, enter the following command:

```
hostname(config-pmap-p)# match header [line] length gt length
```

Where *length* is the number of characters in the header or line.

- k. (Optional) To match the header to-fields count, enter the following command:

```
hostname(config-pmap-p)# match header to-fields count gt count
```

Where *count* is the number of recipients in the to-field of the header.

- l. (Optional) To match the number of invalid recipients, enter the following command:

```
hostname(config-pmap-p)# match invalid-recipients count gt count
```

Where *count* is the number of invalid recipients.

- m. (Optional) To match the type of MIME encoding scheme used, enter the following command:

```
hostname(config-pmap-p)# match mime encoding [7bit|8bit|base64|binary|others|
quoted-printable]
```

- n. (Optional) To match the MIME filename length, enter the following command:

```
hostname(config-pmap-p)# match mime filename length gt length
```

Where *length* is the length of the *filename* in the range 1 to 1000.

- o. (Optional) To match the MIME file type, enter the following command:

```
hostname(config-pmap-p)# match mime filetype regex [name | class name]
```

Where *name* or *class name* is the regular expression that matches a file type or a class map. The regular expression used to match a class map can select multiple file types.

- p. (Optional) To match a sender address, enter the following command:

```
hostname(config-pmap-p)# match sender-address regex [name | class name]
```

Where *name* or *class name* is the regular expression that matches a sender address or a class map. The regular expression used to match a class map can select multiple sender addresses.

- q. (Optional) To match the length of a sender's address, enter the following command:

```
hostname(config-pmap-p)# match sender-address length gt length
```

Where *length* is the number of characters in the sender's address.

---

The following example shows how to define an ESMTP inspection policy map.

```
hostname(config)# regex user1 "user1@cisco.com"
hostname(config)# regex user2 "user2@cisco.com"
hostname(config)# regex user3 "user3@cisco.com"
hostname(config)# class-map type regex senders_black_list
hostname(config-cmap)# description "Regular expressions to filter out undesired senders"
hostname(config-cmap)# match regex user1
hostname(config-cmap)# match regex user2
hostname(config-cmap)# match regex user3

hostname(config)# policy-map type inspect esmtp advanced_esmtp_map
hostname(config-pmap)# match sender-address regex class senders_black_list
hostname(config-pmap-c)# drop-connection log

hostname(config)# policy-map outside_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect esmtp advanced_esmtp_map

hostname(config)# service-policy outside_policy interface outside
```

## FTP Inspection

This section describes the FTP inspection engine. This section includes the following topics:

- [FTP Inspection Overview, page 25-27](#)
- [Using the strict Option, page 25-28](#)
- [Configuring an FTP Inspection Policy Map for Additional Inspection Control, page 25-29](#)
- [Verifying and Monitoring FTP Inspection, page 25-32](#)

## FTP Inspection Overview

The FTP application inspection inspects the FTP sessions and performs four tasks:

- Prepares dynamic secondary data connection
- Tracks the FTP command-response sequence
- Generates an audit trail
- Translates the embedded IP address

FTP application inspection prepares secondary channels for FTP data transfer. Ports for these channels are negotiated through PORT or PASV commands. The channels are allocated in response to a file upload, a file download, or a directory listing event.

**Note**

If you disable FTP inspection engines with the **no inspect ftp** command, outbound users can start connections only in passive mode, and all inbound FTP is disabled.

## Using the strict Option

Using the **strict** option with the **inspect ftp** command increases the security of protected networks by preventing web browsers from sending embedded commands in FTP requests.

**Note**

To specify FTP commands that are not permitted to pass through the security appliance, create an FTP map according to the [“Configuring an FTP Inspection Policy Map for Additional Inspection Control” section on page 25-29](#).

After you enable the **strict** option on an interface, FTP inspection enforces the following behavior:

- An FTP command must be acknowledged before the security appliance allows a new command.
- The security appliance drops connections that send embedded commands.
- The **227** and **PORT** commands are checked to ensure they do not appear in an error string.

**Caution**

Using the **strict** option may cause the failure of FTP clients that are not strictly compliant with FTP RFCs.

If the **strict** option is enabled, each FTP command and response sequence is tracked for the following anomalous activity:

- Truncated command—Number of commas in the **PORT** and **PASV** reply command is checked to see if it is five. If it is not five, then the **PORT** command is assumed to be truncated and the TCP connection is closed.
- Incorrect command—Checks the FTP command to see if it ends with **<CR><LF>** characters, as required by the RFC. If it does not, the connection is closed.
- Size of **RETR** and **STOR** commands—These are checked against a fixed constant. If the size is greater, then an error message is logged and the connection is closed.
- Command spoofing—The **PORT** command should always be sent from the client. The TCP connection is denied if a **PORT** command is sent from the server.
- Reply spoofing—**PASV** reply command (227) should always be sent from the server. The TCP connection is denied if a **PASV** reply command is sent from the client. This prevents the security hole when the user executes “227 xxxxx a1, a2, a3, a4, p1, p2.”
- TCP stream editing—The security appliance closes the connection if it detects TCP stream editing.
- Invalid port negotiation—The negotiated dynamic port value is checked to see if it is less than 1024. As port numbers in the range from 1 to 1024 are reserved for well-known connections, if the negotiated port falls in this range, then the TCP connection is freed.
- Command pipelining—The number of characters present after the port numbers in the **PORT** and **PASV** reply command is cross checked with a constant value of 8. If it is more than 8, then the TCP connection is closed.

- The security appliance replaces the FTP server response to the SYST command with a series of Xs. To prevent the server from revealing its system type to FTP clients. To override this default behavior, use the **no mask-syst-reply** command in the FTP map.

## Configuring an FTP Inspection Policy Map for Additional Inspection Control

FTP command filtering and security checks are provided using strict FTP inspection for improved security and control. Protocol conformance includes packet length checks, delimiters and packet format checks, command terminator checks, and command validation.

Blocking FTP based on user values is also supported so that it is possible for FTP sites to post files for download, but restrict access to certain users. You can block FTP connections based on file type, server name, and other attributes. System message logs are generated if an FTP connection is denied after inspection.

If you want FTP inspection to allow FTP servers to reveal their system type to FTP clients, and limit the allowed FTP commands, then create and configure an FTP map. You can then apply the FTP map when you enable FTP inspection according to the [“Configuring Application Inspection” section on page 25-5](#).

To create an FTP map, perform the following steps:

- 
- Step 1** (Optional) Add one or more regular expressions for use in traffic matching commands according to the [“Creating a Regular Expression” section on page 21-12](#). See the types of text you can match in the **match** commands described in [Step 3](#).
- Step 2** (Optional) Create one or more regular expression class maps to group regular expressions according to the [“Creating a Regular Expression Class Map” section on page 21-14](#).
- Step 3** (Optional) Create an FTP inspection class map by performing the following steps.

A class map groups multiple traffic matches. Traffic must match *all* of the **match** commands to match the class map. You can alternatively identify **match** commands directly in the policy map. The difference between creating a class map and defining the traffic match directly in the inspection policy map is that the class map lets you create more complex match criteria, and you can reuse class maps.

To specify traffic that should not match the class map, use the **match not** command. For example, if the **match not** command specifies the string “example.com,” then any traffic that includes “example.com” does not match the class map.

For the traffic that you identify in this class map, you can specify actions such as drop, drop-connection, reset, mask, set the rate limit, and/or log the connection in the inspection policy map.

If you want to perform different actions for each **match** command, you should identify the traffic directly in the policy map.

- a. Create the class map by entering the following command:

```
hostname(config)# class-map type inspect ftp [match-all] class_map_name
hostname(config-cmap)#
```

Where *class\_map\_name* is the name of the class map. The **match-all** keyword specifies that traffic must match all criteria to match the class map. **match-all** is the default and only option. The CLI enters class-map configuration mode, where you can enter one or more **match** commands.

- b. (Optional) To add a description to the class map, enter the following command:

```
hostname(config-cmap)# description string
```

- c. (Optional) To match a filename for FTP transfer, enter the following command:

```
hostname(config-cmap)# match [not] filename regex [regex_name |
class regex_class_name]
```

Where the *regex\_name* is the regular expression you created in [Step 1](#). The **class** *regex\_class\_name* is the regular expression class map you created in [Step 2](#).

- d. (Optional) To match a file type for FTP transfer,, enter the following command:

```
hostname(config-cmap)# match [not] filetype regex [regex_name |
class regex_class_name]
```

Where the *regex\_name* is the regular expression you created in [Step 1](#). The **class** *regex\_class\_name* is the regular expression class map you created in [Step 2](#).

- e. (Optional) To disallow specific FTP commands, use the following command:

```
hostname(config-cmap)# match [not] request-command ftp_command [ftp_command...]
```

Where *ftp\_command* with one or more FTP commands that you want to restrict. See [Table 25-3](#) for a list of the FTP commands that you can restrict.

**Table 25-3 FTP Map request-command deny Options**

| request-command deny Option | Purpose                                                                                               |
|-----------------------------|-------------------------------------------------------------------------------------------------------|
| <b>appe</b>                 | Disallows the command that appends to a file.                                                         |
| <b>cdup</b>                 | Disallows the command that changes to the parent directory of the current working directory.          |
| <b>dele</b>                 | Disallows the command that deletes a file on the server.                                              |
| <b>get</b>                  | Disallows the client command for retrieving a file from the server.                                   |
| <b>help</b>                 | Disallows the command that provides help information.                                                 |
| <b>mkd</b>                  | Disallows the command that makes a directory on the server.                                           |
| <b>put</b>                  | Disallows the client command for sending a file to the server.                                        |
| <b>rmd</b>                  | Disallows the command that deletes a directory on the server.                                         |
| <b>rnfr</b>                 | Disallows the command that specifies rename-from filename.                                            |
| <b>rnto</b>                 | Disallows the command that specifies rename-to filename.                                              |
| <b>site</b>                 | Disallows the command that are specific to the server system. Usually used for remote administration. |
| <b>stou</b>                 | Disallows the command that stores a file using a unique file name.                                    |

- f. (Optional) To match an FTP server, enter the following command:

```
hostname(config-cmap)# match [not] server regex [regex_name | class regex_class_name]
```

Where the *regex\_name* is the regular expression you created in [Step 1](#). The **class** *regex\_class\_name* is the regular expression class map you created in [Step 2](#).

- g. (Optional) To match an FTP username, enter the following command:

```
hostname(config-cmap)# match [not] username regex [regex_name |
class regex_class_name]
```

Where the *regex\_name* is the regular expression you created in [Step 1](#). The **class** *regex\_class\_name* is the regular expression class map you created in [Step 2](#).

- Step 4** Create an FTP inspection policy map, enter the following command:

```
hostname(config)# policy-map type inspect ftp policy_map_name
hostname(config-pmap)#
```

Where the *policy\_map\_name* is the name of the policy map. The CLI enters policy-map configuration mode.

**Step 5** (Optional) To add a description to the policy map, enter the following command:

```
hostname(config-pmap)# description string
```

**Step 6** To apply actions to matching traffic, perform the following steps.

a. Specify the traffic on which you want to perform actions using one of the following methods:

- Specify the FTP class map that you created in [Step 3](#) by entering the following command:

```
hostname(config-pmap)# class class_map_name
hostname(config-pmap-c)#
```

- Specify traffic directly in the policy map using one of the **match** commands described in [Step 3](#). If you use a **match not** command, then any traffic that does not match the criterion in the **match not** command has the action applied.

b. Specify the action you want to perform on the matching traffic by entering the following command:

```
hostname(config-pmap-c)# {[drop [send-protocol-error] |
drop-connection [send-protocol-error] | mask | reset] [log] | rate-limit message_rate}
```

Not all options are available for each **match** or **class** command. See the CLI help or the *Cisco Security Appliance Command Reference* for the exact options available.

The **drop** keyword drops all packets that match.

The **send-protocol-error** keyword sends a protocol error message.

The **drop-connection** keyword drops the packet and closes the connection.

The **mask** keyword masks out the matching portion of the packet.

The **reset** keyword drops the packet, closes the connection, and sends a TCP reset to the server and/or client.

The **log** keyword, which you can use alone or with one of the other keywords, sends a system log message.

The **rate-limit** *message\_rate* argument limits the rate of messages.

You can specify multiple **class** or **match** commands in the policy map. For information about the order of **class** and **match** commands, see the “[Defining Actions in an Inspection Policy Map](#)” section on [page 21-8](#).

**Step 7** To configure parameters that affect the inspection engine, perform the following steps:

a. To enter parameters configuration mode, enter the following command:

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b. To mask the greeting banner from the FTP server, enter the following command:

```
hostname(config-pmap-p)# mask-banner
```

c. To mask the reply to **syst** command, enter the following command:

```
hostname(config-pmap-p)# mask-syst-reply
```

Before submitting a username and password, all FTP users are presented with a greeting banner. By default, this banner includes version information useful to hackers trying to identify weaknesses in a system. The following example shows how to mask this banner:

```
hostname(config)# policy-map type inspect ftp mymap
hostname(config-pmap)# parameters
hostname(config-pmap-p)# mask-banner

hostname(config)# class-map match-all ftp-traffic
hostname(config-cmap)# match port tcp eq ftp

hostname(config)# policy-map ftp-policy
hostname(config-pmap)# class ftp-traffic
hostname(config-pmap-c)# inspect ftp strict mymap

hostname(config)# service-policy ftp-policy interface inside
```

## Verifying and Monitoring FTP Inspection

FTP application inspection generates the following log messages:

- An Audit record 303002 is generated for each file that is retrieved or uploaded.
- The FTP command is checked to see if it is RETR or STOR and the retrieve and store commands are logged.
- The username is obtained by looking up a table providing the IP address.
- The username, source IP address, destination IP address, NAT address, and the file operation are logged.
- Audit record 201005 is generated if the secondary dynamic channel preparation failed due to memory shortage.

In conjunction with NAT, the FTP application inspection translates the IP address within the application payload. This is described in detail in RFC 959.

During FTP inspection, the security appliance can drop packets silently. To see whether the security appliance has dropped any packets internally, enter the **show service-policy inspect ftp** command.



### Note

The command output does not display drop counters that are zero. The security appliance infrequently drops packets silently; therefore, the output of this command rarely displays drop counters.

Table 25-4 describes the output from the **show service-policy inspect ftp** command:

**Table 25-4** FTP Drop Counter Descriptions

| Drop Counter                  | Counter increments...                                                                                                                        |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| Back port is zero drop        | If the port value is 0 when processing APPE, STOR, STOU, LIST, NLIST, RETR commands.                                                         |
| Can't allocate back conn drop | When an attempt to allocate a secondary data connection fails.                                                                               |
| Can't allocate CP conn drop   | When the security appliance attempts to allocate a data structure for a CP connection and the attempt fails.<br>Check for low system memory. |

**Table 25-4 FTP Drop Counter Descriptions**

| <b>Drop Counter</b>                 | <b>Counter increments...</b>                                                                                                               |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| Can't alloc FTP data structure drop | When the security appliance attempts to allocate a data structure for FTP inspection and the attempt fails.<br>Check for low system memory |
| Can't allocate TCP proxy drop       | When the security appliance attempts to allocate a data structure for a TCP proxy and the attempt fails.<br>Check for low system memory    |
| Can't append block drop             | When the FTP packet is out of space and data cannot be added to the packet.                                                                |
| Can't PAT port drop                 | When the security appliance fails to configure PAT for a port.                                                                             |
| Cmd in reply mode drop              | When a command is received in REPLY mode.                                                                                                  |
| Cmd match failure drop              | When the security appliance encounters an internal error in regex matching.<br>Contact Cisco TAC.                                          |
| Cmd not a cmd drop                  | When the FTP command string contains invalid characters, such as numeric characters.                                                       |
| Cmd not port drop                   | When the security appliance expects to receive a PORT command but receives another command.                                                |
| Cmd not supported drop              | When the security appliance encounters an unsupported FTP command.                                                                         |
| Cmd not supported in IPv6 drop      | When an FTP command is not supported in IPv6.                                                                                              |
| Cmd not terminated drop             | When the FTP command is not terminated with NL or CR.                                                                                      |
| Cmd retx unexpected drop            | When a retransmitted packet is received unexpectedly.                                                                                      |
| Cmd too short drop                  | When the FTP command is too short.                                                                                                         |
| ERPT too short drop                 | When the ERPT command is too short.                                                                                                        |
| IDS internal error drop             | When an internal error is encountered during FTP ID checks.<br>Contact Cisco TAC.                                                          |
| Invalid address drop                | When an invalid IP address is encountered during inspection.                                                                               |
| Invalid EPSV format drop            | When a formatting error is found in the ESPV command.                                                                                      |
| Invalid ERPT AF number drop         | When the Address Family (AF) is invalid in the ERPT command.                                                                               |
| Invalid port drop                   | When an invalid port is encountered during inspection.                                                                                     |
| No back port for data drop          | If the packet does not contain a port when processing APPE, STOR, STOU, LIST, NLIST, RETR commands.                                        |
| PORT command/reply too long drop    | When the length of PORT command or passive reply is greater than 8.                                                                        |
| Reply code invalid drop             | When the reply code is invalid.                                                                                                            |
| Reply length negative drop          | When a reply has a negative length value.                                                                                                  |
| Reply unexpected drop               | If the security appliance receives a reply when a reply is not expected.                                                                   |
| Retx cmd in cmd mode drop           | When a retransmitted command is received in CMD mode.                                                                                      |

**Table 25-4 FTP Drop Counter Descriptions**

| Drop Counter                  | Counter increments...                                                                                        |
|-------------------------------|--------------------------------------------------------------------------------------------------------------|
| Retx port not old port drop   | When a packet is retransmitted but the port in the packet is different from the originally transmitted port. |
| TCP option exceeds limit drop | When the length value in a TCP option causes the length of the option to exceed the TCP header limit.        |
| TCP option length error drop  | When the length value in a TCP option is not correct.                                                        |

The following is sample output from the **show service-policy inspect ftp** command:

```
hostname# show show show service-policy inspect ftp

Global policy:
Service-policy: global_policy
Class-map: inspection_default
Inspect: ftp, packet 0, drop 0, reset-drop 0
Can't alloc CP conn drop 1, Can't alloc proxy drop 2
TCP option exceeds limit drop 3, TCP option length error drop 4
Can't alloc FTP structure drop 1, Can't append block drop 2
PORT cmd/reply too long drop 3, ERPT too short drop 4
Invalid ERPT AF number drop 5, IDS internal error drop 6
Invalid address drop 7, Invalid port drop 8
Can't PAT port drop 9, Invalid EPSV format drop 10
Retx port not old port drop 11, No back port for data drop 12
Can't alloc back conn drop 13, Back port is zero drop 14
Cmd too short drop 15, Cmd not terminated drop 16
Cmd not a cmd drop 17, Cmd match failure drop 18
Cmd not supported drop 19, Cmd not supported in IPv6 drop 20
Cmd not port drop 21, Retx cmd in cmd mode drop 22
Cmd retx unexpected drop 23, Cmd in reply mode drop 24
Reply length negative drop 25, Reply unexpected drop 26
Reply code invalid drop 27
```

## GTP Inspection

This section describes the GTP inspection engine. This section includes the following topics:

- [GTP Inspection Overview, page 25-35](#)
- [Configuring a GTP Inspection Policy Map for Additional Inspection Control, page 25-36](#)
- [Verifying and Monitoring GTP Inspection, page 25-39](#)



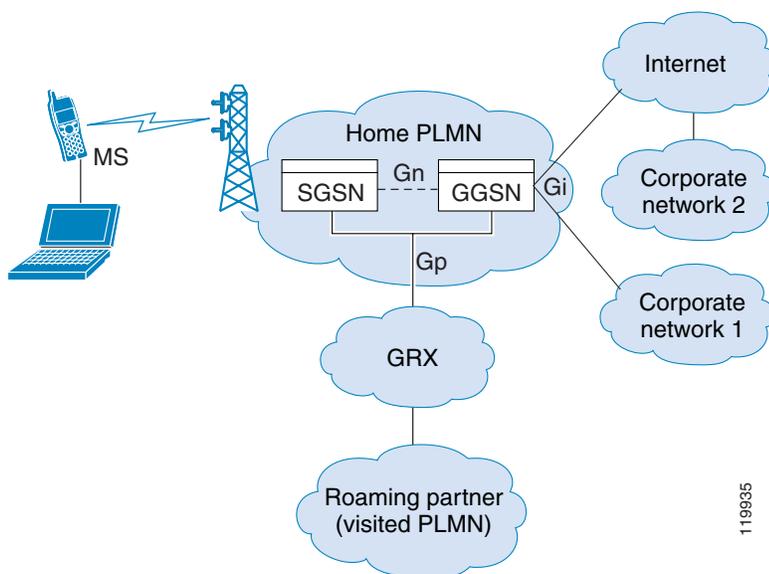
### Note

GTP inspection requires a special license. If you enter GTP-related commands on a security appliance without the required license, the security appliance displays an error message.

## GTP Inspection Overview

GPRS provides uninterrupted connectivity for mobile subscribers between GSM networks and corporate networks or the Internet. The GGSN is the interface between the GPRS wireless data network and other networks. The SGSN performs mobility, data session management, and data compression (See Figure 25-3).

**Figure 25-3 GPRS Tunneling Protocol**



The UMTS is the commercial convergence of fixed-line telephony, mobile, Internet and computer technology. UTRAN is the networking protocol used for implementing wireless networks in this system. GTP allows multi-protocol packets to be tunneled through a UMTS/GPRS backbone between a GGSN, an SGSN and the UTRAN.

GTP does not include any inherent security or encryption of user data, but using GTP with the security appliance helps protect your network against these risks.

The SGSN is logically connected to a GGSN using GTP. GTP allows multiprotocol packets to be tunneled through the GPRS backbone between GSNs. GTP provides a tunnel control and management protocol that allows the SGSN to provide GPRS network access for a mobile station by creating, modifying, and deleting tunnels. GTP uses a tunneling mechanism to provide a service for carrying user data packets.



### Note

When using GTP with failover, if a GTP connection is established and the active unit fails before data is transmitted over the tunnel, the GTP data connection (with a “j” flag set) is not replicated to the standby unit. This occurs because the active unit does not replicate embryonic connections to the standby unit.

## Configuring a GTP Inspection Policy Map for Additional Inspection Control

If you want to enforce additional parameters on GTP traffic, create and configure a GTP map. If you do not specify a map with the **inspect gtp** command, the security appliance uses the default GTP map, which is preconfigured with the following default values:

- **request-queue 200**
- **timeout gsn 0:30:00**
- **timeout pdp-context 0:30:00**
- **timeout request 0:01:00**
- **timeout signaling 0:30:00**
- **timeout tunnel 0:01:00**
- **tunnel-limit 500**

To create and configure a GTP map, perform the following steps. You can then apply the GTP map when you enable GTP inspection according to the “[Configuring Application Inspection](#)” section on page 25-5.

---

**Step 1** Create a GTP inspection policy map, enter the following command:

```
hostname(config)# policy-map type inspect gtp policy_map_name
hostname(config-pmap)#
```

Where the *policy\_map\_name* is the name of the policy map. The CLI enters policy-map configuration mode.

**Step 2** (Optional) To add a description to the policy map, enter the following command:

```
hostname(config-pmap)# description string
```

**Step 3** To match an Access Point name, enter the following command:

```
hostname(config-pmap)# match [not] apn regex [regex_name | class regex_class_name]
```

Where the *regex\_name* is the regular expression you created in [Step 1](#). The **class** *regex\_class\_name* is the regular expression class map you created in [Step 2](#).

**Step 4** To match a message ID, enter the following command:

```
hostname(config-pmap)# match [not] message id [message_id | range lower_range upper_range]
```

Where the *message\_id* is an alphanumeric identifier between 1 and 255. The *lower\_range* is lower range of message IDs. The *upper\_range* is the upper range of message IDs.

**Step 5** To match a message length, enter the following command:

```
hostname(config-pmap)# match [not] message length min min_length max max_length
```

Where the *min\_length* and *max\_length* are both between 1 and 65536. The length specified by this command is the sum of the GTP header and the rest of the message, which is the payload of the UDP packet.

**Step 6** To match the version, enter the following command:

```
hostname(config-pmap)# match [not] version [version_id | range lower_range upper_range]
```

Where the *version\_id* is between 0 and 255. The *lower\_range* is lower range of versions. The *upper\_range* is the upper range of versions.

**Step 7** To configure parameters that affect the inspection engine, perform the following steps:

- a. To enter parameters configuration mode, enter the following command:

```
hostname(config-pmap) # parameters
hostname(config-pmap-p) #
```

The **mnc network\_code** argument is a two or three-digit value identifying the network code.

By default, the security appliance does not check for valid MCC/MNC combinations. This command is used for IMSI Prefix filtering. The MCC and MNC in the IMSI of the received packet is compared with the MCC/MNC configured with this command and is dropped if it does not match.

This command must be used to enable IMSI Prefix filtering. You can configure multiple instances to specify permitted MCC and MNC combinations. By default, the security appliance does not check the validity of MNC and MCC combinations, so you must verify the validity of the combinations configured. To find more information about MCC and MNC codes, see the ITU E.212 recommendation, *Identification Plan for Land Mobile Stations*.

- b. To allow invalid GTP packets or packets that otherwise would fail parsing and be dropped, enter the following command:

```
hostname(config-pmap-p) # permit errors
```

By default, all invalid packets or packets that failed, during parsing, are dropped.

- c. To enable support for GSN pooling, use the **permit response** command.

If the security appliance performs GTP inspection, by default the security appliance drops GTP responses from GSNs that were not specified in the GTP request. This situation occurs when you use load-balancing among a pool of GSNs to provide efficiency and scalability of GPRS.

You can enable support for GSN pooling by using the **permit response** command. This command configures the security appliance to allow responses from any of a designated set of GSNs, regardless of the GSN to which a GTP request was sent. You identify the pool of load-balancing GSNs as a network object. Likewise, you identify the SGSN as a network object. If the GSN responding belongs to the same object group as the GSN that the GTP request was sent to and if the SGSN is in a object group that the responding GSN is permitted to send a GTP response to, the security appliance permits the response.

- d. To create an object to represent the pool of load-balancing GSNs, perform the following steps:

Use the **object-group** command to define a new network object group representing the pool of load-balancing GSNs.

```
hostname(config) # object-group network GSN-pool-name
hostname(config-network) #
```

For example, the following command creates an object group named gsnpool32:

```
hostname(config) # object-group network gsnpool32
hostname(config-network) #
```

- e. Use the **network-object** command to specify the load-balancing GSNs. You can do so with one **network-object** command per GSN, using the **host** keyword. You can also using **network-object** command to identify whole networks containing GSNs that perform load balancing.

```
hostname(config-network) # network-object host IP-address
```

For example, the following commands create three network objects representing individual hosts:

```
hostname(config-network) # network-object host 192.168.100.1
hostname(config-network) # network-object host 192.168.100.2
hostname(config-network) # network-object host 192.168.100.3
hostname(config-network) #
```

- f. To create an object to represent the SGSN that the load-balancing GSNs are permitted to respond to, perform the following steps:

- a. Use the **object-group** command to define a new network object group that will represent the SGSN that sends GTP requests to the GSN pool.

```
hostname(config)# object-group network SGSN-name
hostname(config-network)#
```

For example, the following command creates an object group named `sgsn32`:

```
hostname(config)# object-group network sgsn32
hostname(config-network)#
```

- b. Use the **network-object** command with the **host** keyword to identify the SGSN.

```
hostname(config-network)# network-object host IP-address
```

For example, the following command creates a network objects representing the SGSN:

```
hostname(config-network)# network-object host 192.168.50.100
hostname(config-network)#
```

- g. To allow GTP responses from any GSN in the network object representing the GSN pool, defined in c., d, to the network object representing the SGSN, defined in c., f., enter the following commands:

```
hostname(config)# gtp-map map_name
hostname(config-gtp-map)# permit response to-object-group SGSN-name from-object-group
GSN-pool-name
```

For example, the following command permits GTP responses from any host in the object group named `gsnpool32` to the host in the object group named `sgsn32`:

```
hostname(config-gtp-map)# permit response to-object-group sgsn32 from-object-group
gsnpool32
```

The following example shows how to support GSN pooling by defining network objects for the GSN pool and the SGSN. An entire Class C network is defined as the GSN pool but you can identify multiple individual IP addresses, one per **network-object** command, instead of identifying whole networks. The example then modifies a GTP map to permit responses from the GSN pool to the SGSN.

```
hostname(config)# object-group network gsnpool32
hostname(config-network)# network-object 192.168.100.0 255.255.255.0
hostname(config)# object-group network sgsn32
hostname(config-network)# network-object host 192.168.50.100
hostname(config)# gtp-map gtp-policy
hostname(config-gtp-map)# permit response to-object-group sgsn32 from-object-group
gsnpool32
```

- h. To specify the maximum number of GTP requests that will be queued waiting for a response, enter the following command:

```
hostname(config-gtp-map)# request-queue max_requests
```

where the *max\_requests* argument sets the maximum number of GTP requests that will be queued waiting for a response, from 1 to 4294967295. The default is 200.

When the limit has been reached and a new request arrives, the request that has been in the queue for the longest time is removed. The Error Indication, the Version Not Supported and the SGSN Context Acknowledge messages are not considered as requests and do not enter the request queue to wait for a response.

- i. To change the inactivity timers for a GTP session, enter the following command:

```
hostname(config-gtp-map)# timeout {gsn | pdp-context | request | signaling | tunnel}
hh:mm:ss
```

Enter this command separately for each timeout.

The **gsn** keyword specifies the period of inactivity after which a GSN will be removed.

The **pdp-context** keyword specifies the maximum period of time allowed before beginning to receive the PDP context.

The **request** keyword specifies the maximum period of time allowed before beginning to receive the GTP message.

The **signaling** keyword specifies the period of inactivity after which the GTP signaling will be removed.

The **tunnel** keyword specifies the period of inactivity after which the GTP tunnel will be torn down.

The *hh:mm:ss* argument is the timeout where *hh* specifies the hour, *mm* specifies the minutes, and *ss* specifies the seconds. The value **0** means never tear down.

- j. To specify the maximum number of GTP tunnels allowed to be active on the security appliance, enter the following command:

```
hostname(config-gtp-map)# tunnel-limit max_tunnels
```

where the *max\_tunnels* argument is the maximum number of tunnels allowed, from 1 to 4294967295. The default is 500.

New requests will be dropped once the number of tunnels specified by this command is reached.

The following example shows how to limit the number of tunnels in the network:

```
hostname(config)# policy-map type inspect gtp gmap
hostname(config-pmap)# parameters
hostname(config-pmap-p)# tunnel-limit 3000

hostname(config)# policy-map global_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect gtp gmap

hostname(config)# service-policy global_policy global
```

## Verifying and Monitoring GTP Inspection

To display GTP configuration, enter the **show service-policy inspect gtp** command in privileged EXEC mode. For the detailed syntax for this command, see the command page in the *Cisco Security Appliance Command Reference*.

Use the **show service-policy inspect gtp statistics** command to show the statistics for GTP inspection. The following is sample output from the **show service-policy inspect gtp statistics** command:

```
hostname# show service-policy inspect gtp statistics
GPRS GTP Statistics:
 version_not_support 0 msg_too_short 0
 unknown_msg 0 unexpected_sig_msg 0
 unexpected_data_msg 0 ie_duplicated 0
 mandatory_ie_missing 0 mandatory_ie_incorrect 0
```

```

optional_ie_incorrect 0 ie_unknown 0
ie_out_of_order 0 ie_unexpected 0
total_forwarded 0 total_dropped 0
signalling_msg_dropped 0 data_msg_dropped 0
signalling_msg_forwarded 0 data_msg_forwarded 0
total_created_pdp 0 total_deleted_pdp 0
total_created_pdpmcb 0 total_deleted_pdpmcb 0
pdp_non_existent 0

```

You can use the vertical bar (|) to filter the display. Type ?| for more display filtering options.

The following is sample GSN output from the **show service-policy inspect gtp statistics gsn** command:

```

hostname# show service-policy inspect gtp statistics gsn 9.9.9.9
1 in use, 1 most used, timeout 0:00:00

GTP GSN Statistics for 9.9.9.9, Idle 0:00:00, restart counter 0
Tunnels Active 0Tunnels Created 0
Tunnels Destroyed 0
Total Messages Received 2
Signaling Messages Data Messages
total received 2 0
dropped 0 0
forwarded 2 0

```

Use the **show service-policy inspect gtp pdp-context** command to display PDP context-related information. The following is sample output from the **show service-policy inspect gtp pdp-context** command:

```

hostname# show service-policy inspect gtp pdp-context detail
1 in use, 1 most used, timeout 0:00:00

Version TID MS Addr SGSN Addr Idle APN
v1 1234567890123425 10.0.1.1 10.0.0.2 0:00:13 gprs.cisco.com

user_name (IMSI): 214365870921435 MS address: 1.1.1.1
primary pdp: Y
sgsn_addr_signal: 10.0.0.2 sgsn_addr_data: 10.0.0.2
ggsn_addr_signal: 10.1.1.1 ggsn_addr_data: 10.1.1.1
sgsn control teid: 0x000001d1 sgsn data teid: 0x000001d3
ggsn control teid: 0x6306ffa0 ggsn data teid: 0x6305f9fc
seq_tpdu_up: 0 seq_tpdu_down: 0
signal_sequence: 0
upstream_signal_flow: 0 upstream_data_flow: 0
downstream_signal_flow: 0 downstream_data_flow: 0
RAupdate_flow: 0

```

The PDP context is identified by the tunnel ID, which is a combination of the values for IMSI and NSAPI. A GTP tunnel is defined by two associated PDP contexts in different GSN nodes and is identified with a Tunnel ID. A GTP tunnel is necessary to forward packets between an external packet data network and a MS user.

You can use the vertical bar (|) to filter the display, as in the following example:

```

hostname# show service-policy inspect gtp statistics | grep gsn

```

## H.323 Inspection

This section describes the H.323 application inspection. This section includes the following topics:

- [H.323 Inspection Overview, page 25-41](#)

- [How H.323 Works, page 25-41](#)
- [Limitations and Restrictions, page 25-42](#)
- [Configuring H.323 and H.225 Timeout Values, page 25-45](#)
- [Verifying and Monitoring H.323 Inspection, page 25-45](#)

## H.323 Inspection Overview

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, including H.323 v3 feature Multiple Calls on One Call Signaling Channel.

With H323 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.

The two major functions of H.323 inspection are as follows:

- 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.

## How H.323 Works

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

An H.323 client may 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 are not using 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 the following 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 ACF message.

After inspecting the H.225 messages, the security appliance opens the H.245 channel and then inspects traffic sent over the H.245 channel as well. All H.245 messages passing 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 TPKT header, defining 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 UUIE 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 ACKs that TPKT and appends a new TPKT to the H.245 message with the new length.


**Note**


---

The security appliance does not support TCP options in the Proxy ACK for the TPKT.

---

Each UDP connection with a packet going through H.323 inspection is marked as an H.323 connection and times out with the H.323 timeout as configured with the **timeout** command.

## Limitations and Restrictions

The following are some of the known issues and limitations when using H.323 application inspection:

- Static PAT may not properly translate IP addresses embedded in optional fields within H.323 messages. If you experience this kind of problem, do not use static PAT with H.323.
- H.323 application inspection is not supported with NAT between same-security-level interfaces.
- When a NetMeeting client registers with an H.323 gatekeeper and tries to call an H.323 gateway that is also registered with the H.323 gatekeeper, the connection is established but no voice is heard in either direction. This problem is unrelated to the security appliance.
- If you configure a network static address where the network static address is the same as a third-party netmask and address, then any outbound H.323 connection fails.

## Configuring an H.323 Inspection Policy Map for Additional Inspection Control

To specify actions when a message violates a parameter, create an H.323 inspection policy map. You can then apply the inspection policy map when you enable H.323 inspection according to the [“Configuring Application Inspection” section on page 25-5](#).

To create an H.323 inspection policy map, perform the following steps:

- 
- Step 1** (Optional) Add one or more regular expressions for use in traffic matching commands according to the [“Creating a Regular Expression” section on page 21-12](#). See the types of text you can match in the **match** commands described in [Step 3](#).

**Step 2** (Optional) Create one or more regular expression class maps to group regular expressions according to the “[Creating a Regular Expression Class Map](#)” section on page 21-14.s

**Step 3** (Optional) Create an H.323 inspection class map by performing the following steps.

A class map groups multiple traffic matches. Traffic must match *all* of the **match** commands to match the class map. You can alternatively identify **match** commands directly in the policy map. The difference between creating a class map and defining the traffic match directly in the inspection policy map is that the class map lets you create more complex match criteria, and you can reuse class maps.

To specify traffic that should not match the class map, use the **match not** command. For example, if the **match not** command specifies the string “example.com,” then any traffic that includes “example.com” does not match the class map.

For the traffic that you identify in this class map, you can specify actions such as drop-connection, reset, and/or log the connection in the inspection policy map.

If you want to perform different actions for each **match** command, you should identify the traffic directly in the policy map.

- a. Create the class map by entering the following command:

```
hostname(config)# class-map type inspect h323 [match-all] class_map_name
hostname(config-cmap)#
```

Where *the class\_map\_name* is the name of the class map. The **match-all** keyword specifies that traffic must match all criteria to match the class map. **match-all** is the default and only option. The CLI enters class-map configuration mode, where you can enter one or more **match** commands.

- b. (Optional) To add a description to the class map, enter the following command:

```
hostname(config-cmap)# description string
```

Where *string* is the description of the class map (up to 200 characters).

- c. (Optional) To match a called party, enter the following command:

```
hostname(config-cmap)# match [not] called-party regex {class class_name | regex_name}
```

Where the **regex** *regex\_name* argument is the regular expression you created in [Step 1](#). The **class** *regex\_class\_name* is the regular expression class map you created in [Step 2](#).

- d. (Optional) To match a media type, enter the following command:

```
hostname(config-cmap)# match [not] media-type {audio | data | video}
```

**Step 4** Create an H.323 inspection policy map, enter the following command:

```
hostname(config)# policy-map type inspect h323 policy_map_name
hostname(config-pmap)#
```

Where the *policy\_map\_name* is the name of the policy map. The CLI enters policy-map configuration mode.

**Step 5** (Optional) To add a description to the policy map, enter the following command:

```
hostname(config-pmap)# description string
```

**Step 6** To apply actions to matching traffic, perform the following steps.

- a. Specify the traffic on which you want to perform actions using one of the following methods:

- Specify the H.323 class map that you created in [Step 3](#) by entering the following command:

```
hostname(config-pmap)# class class_map_name
hostname(config-pmap-c)#
```

- Specify traffic directly in the policy map using one of the **match** commands described in [Step 3](#). If you use a **match not** command, then any traffic that does not match the criterion in the **match not** command has the action applied.
- b. Specify the action you want to perform on the matching traffic by entering the following command:

```
hostname(config-pmap-c)# {[drop [send-protocol-error] |
drop-connection [send-protocol-error] | mask | reset] [log] | rate-limit message_rate}
```

Not all options are available for each **match** or **class** command. See the CLI help or the *Cisco Security Appliance Command Reference* for the exact options available.

The **drop** keyword drops all packets that match.

The **send-protocol-error** keyword sends a protocol error message.

The **drop-connection** keyword drops the packet and closes the connection.

The **mask** keyword masks out the matching portion of the packet.

The **reset** keyword drops the packet, closes the connection, and sends a TCP reset to the server and/or client.

The **log** keyword, which you can use alone or with one of the other keywords, sends a system log message.

The **rate-limit message\_rate** argument limits the rate of messages.

You can specify multiple **class** or **match** commands in the policy map. For information about the order of **class** and **match** commands, see the “[Defining Actions in an Inspection Policy Map](#)” section on [page 21-8](#).

**Step 7** To configure parameters that affect the inspection engine, perform the following steps:

- a. To enter parameters configuration mode, enter the following command:

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

- b. To define the H.323 call duration limit, enter the following command:

```
hostname(config-pmap-p)# call-duration-limit time
```

Where *time* is the call duration limit in seconds. Range is from 0:0:0 to 1163:0:0. A value of 0 means never timeout.

- c. To enforce call party number used in call setup, enter the following command:

```
hostname(config-pmap-p)# call-party-number
```

- d. To enforce H.245 tunnel blocking, enter the following command:

```
hostname(config-pmap-p)# h245-tunnel-block action {drop-connection | log}
```

- e. To define an hsi group and enter hsi group configuration mode, enter the following command:

```
hostname(config-pmap-p)# hsi-group id
```

Where *id* is the hsi group ID. Range is from 0 to 2147483647.

To add an hsi to the hsi group, enter the following command in hsi group configuration mode:

```
hostname(config-h225-map-hsi-grp)# hsi ip_address
```

Where *ip\_address* is the host to add. A maximum of five hosts per hsi group are allowed.

To add an endpoint to the hsi group, enter the following command in hsi group configuration mode:

```
hostname(config-h225-map-hsi-grp)# endpoint ip_address if_name
```

Where *ip\_address* is the endpoint to add and *if\_name* is the interface through which the endpoint is connected to the security appliance. A maximum of ten endpoints per hsi group are allowed.

- f. To check RTP packets flowing on the pinholes for protocol conformance, enter the following command:

```
hostname(config-pmap-p)# rtp-conformance [enforce-payloadtype]
```

Where the **enforce-payloadtype** keyword enforces the payload type to be audio or video based on the signaling exchange.

- g. To enable state checking validation, enter the following command:

```
hostname(config-pmap-p)# state-checking {h225 | ras}
```

The following example shows how to configure phone number filtering:

```
hostname(config)# regex caller 1 "5551234567"
hostname(config)# regex caller 2 "5552345678"
hostname(config)# regex caller 3 "5553456789"

hostname(config)# class-map type inspect h323 match-all h323_traffic
hostname(config-pmap-c)# match called-party regex caller1
hostname(config-pmap-c)# match calling-party regex caller2

hostname(config)# policy-map type inspect h323 h323_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# class h323_traffic
hostname(config-pmap-c)# drop
```

## Configuring H.323 and H.225 Timeout Values

To configure the idle time after which an H.225 signalling connection is closed, use the **timeout h225** command. The default for H.225 timeout is one hour.

To configure the idle time after which an H.323 control connection is closed, use the **timeout h323** command. The default is five minutes.

## Verifying and Monitoring H.323 Inspection

This section describes how to display information about H.323 sessions. This section includes the following topics:

- [Monitoring H.225 Sessions, page 25-46](#)
- [Monitoring H.245 Sessions, page 25-46](#)
- [Monitoring H.323 RAS Sessions, page 25-47](#)

## Monitoring H.225 Sessions

The **show h225** command displays information for H.225 sessions established across the security appliance. Along with the **debug h323 h225 event**, **debug h323 h245 event**, and **show local-host** commands, this command is used for troubleshooting H.323 inspection engine issues.

Before entering the **show h225**, **show h245**, or **show h323-ras** commands, we recommend that you configure the **pager** command. If there are a lot of session records and the **pager** command is not configured, it may take a while for the **show** command output to reach its end. If there is an abnormally large number of connections, check that the sessions are timing out based on the default timeout values or the values set by you. If they are not, then there is a problem that needs to be investigated.

The following is sample output from the **show h225** command:

```
hostname# show h225
Total H.323 Calls: 1
1 Concurrent Call(s) for
 Local: 10.130.56.3/1040 Foreign: 172.30.254.203/1720
 1. CRV 9861
 Local: 10.130.56.3/1040 Foreign: 172.30.254.203/1720
0 Concurrent Call(s) for
 Local: 10.130.56.4/1050 Foreign: 172.30.254.205/1720
```

This output indicates that there is currently 1 active H.323 call going through the security appliance between the local endpoint 10.130.56.3 and foreign host 172.30.254.203, and for these particular endpoints, there is 1 concurrent call between them, with a CRV for that call of 9861.

For the local endpoint 10.130.56.4 and foreign host 172.30.254.205, there are 0 concurrent calls. This means that there is no active call between the endpoints even though the H.225 session still exists. This could happen if, at the time of the **show h225** command, the call has already ended but the H.225 session has not yet been deleted. Alternately, it could mean that the two endpoints still have a TCP connection opened between them because they set “maintainConnection” to TRUE, so the session is kept open until they set it to FALSE again, or until the session times out based on the H.225 timeout value in your configuration.

## Monitoring H.245 Sessions

The **show h245** command displays information for H.245 sessions established across the security appliance by endpoints using slow start. Slow start is when the two endpoints of a call open another TCP control channel for H.245. Fast start is where the H.245 messages are exchanged as part of the H.225 messages on the H.225 control channel.) Along with the **debug h323 h245 event**, **debug h323 h225 event**, and **show local-host** commands, this command is used for troubleshooting H.323 inspection engine issues.

The following is sample output from the **show h245** command:

```
hostname# show h245
Total: 1
LOCAL TPKT FOREIGN TPKT
1 10.130.56.3/1041 0 172.30.254.203/1245 0
MEDIA: LCN 258 Foreign 172.30.254.203 RTP 49608 RTCP 49609
 Local 10.130.56.3 RTP 49608 RTCP 49609
MEDIA: LCN 259 Foreign 172.30.254.203 RTP 49606 RTCP 49607
 Local 10.130.56.3 RTP 49606 RTCP 49607
```

There is currently one H.245 control session active across the security appliance. The local endpoint is 10.130.56.3, and we are expecting the next packet from this endpoint to have a TPKT header because the TPKT value is 0. The TKTP header is a 4-byte header preceding each H.225/H.245 message. It gives the length of the message, including the 4-byte header. The foreign host endpoint is 172.30.254.203, and we are expecting the next packet from this endpoint to have a TPKT header because the TPKT value is 0.

The media negotiated between these endpoints have an LCN of 258 with the foreign RTP IP address/port pair of 172.30.254.203/49608 and an RTCP IP address/port of 172.30.254.203/49609 with a local RTP IP address/port pair of 10.130.56.3/49608 and an RTCP port of 49609.

The second LCN of 259 has a foreign RTP IP address/port pair of 172.30.254.203/49606 and an RTCP IP address/port pair of 172.30.254.203/49607 with a local RTP IP address/port pair of 10.130.56.3/49606 and RTCP port of 49607.

## Monitoring H.323 RAS Sessions

The **show h323-ras** command displays information for H.323 RAS sessions established across the security appliance between a gatekeeper and its H.323 endpoint. Along with the **debug h323 ras event** and **show local-host** commands, this command is used for troubleshooting H.323 RAS inspection engine issues.

The **show h323-ras** command displays connection information for troubleshooting H.323 inspection engine issues. The following is sample output from the **show h323-ras** command:

```
hostname# show h323-ras
Total: 1
 GK Caller
 172.30.254.214 10.130.56.14
```

This output shows that there is one active registration between the gatekeeper 172.30.254.214 and its client 10.130.56.14.

# HTTP Inspection

This section describes the HTTP inspection engine. This section includes the following topics:

- [HTTP Inspection Overview, page 25-47](#)
- [Configuring an HTTP Inspection Policy Map for Additional Inspection Control, page 25-48](#)

## HTTP Inspection Overview

Use the HTTP inspection engine to protect against specific attacks and other threats that may be associated with HTTP traffic. HTTP inspection performs several functions:

- Enhanced HTTP inspection
- URL screening through N2H2 or Websense
- Java and ActiveX filtering

The latter two features are configured in conjunction with the **filter** command. For more information about filtering, see [Chapter 20, “Applying Filtering Services.”](#)



**Note**

The **no inspect http** command also disables the **filter url** command.

The enhanced HTTP inspection feature, which is also known as an application firewall and is available when you configure an HTTP map (see [“Configuring an HTTP Inspection Policy Map for Additional Inspection Control”](#)), can help prevent attackers from using HTTP messages for circumventing network security policy. It verifies the following for all HTTP messages:

- Conformance to RFC 2616
- Use of RFC-defined methods only.
- Compliance with the additional criteria.

## Configuring an HTTP Inspection Policy Map for Additional Inspection Control

To specify actions when a message violates a parameter, create an HTTP inspection policy map. You can then apply the inspection policy map when you enable HTTP inspection according to the [“Configuring Application Inspection”](#) section on page 25-5.



### Note

When you enable HTTP inspection with an inspection policy map, strict HTTP inspection with the action reset and log is enabled by default. You can change the actions performed in response to inspection failure, but you cannot disable strict inspection as long as the inspection policy map remains enabled.

To create an HTTP inspection policy map, perform the following steps:

- 
- Step 1** (Optional) Add one or more regular expressions for use in traffic matching commands according to the [“Creating a Regular Expression”](#) section on page 21-12. See the types of text you can match in the **match** commands described in [Step 3](#).
- Step 2** (Optional) Create one or more regular expression class maps to group regular expressions according to the [“Creating a Regular Expression Class Map”](#) section on page 21-14.
- Step 3** (Optional) Create an HTTP inspection class map by performing the following steps.

A class map groups multiple traffic matches. Traffic must match *all* of the **match** commands to match the class map. You can alternatively identify **match** commands directly in the policy map. The difference between creating a class map and defining the traffic match directly in the inspection policy map is that the class map lets you create more complex match criteria, and you can reuse class maps.

To specify traffic that should not match the class map, use the **match not** command. For example, if the **match not** command specifies the string “example.com,” then any traffic that includes “example.com” does not match the class map.

For the traffic that you identify in this class map, you can specify actions such as drop, drop-connection, reset, mask, set the rate limit, and/or log the connection in the inspection policy map.

If you want to perform different actions for each **match** command, you should identify the traffic directly in the policy map.



### Note

If you need to change a **match** command for HTTP inspection after configuring the inspection, you must remove the attached service policy by using the **no service policy** command and then reconfigure the service policy. Changing the class map by removing a **match** command causes HTTP inspection to block all HTTP traffic until you remove and reconfigure the attached service policy so that all the **match** commands are reprocessed.

- a. Create the class map by entering the following command:

```
hostname(config)# class-map type inspect http [match-all] class_map_name
hostname(config-cmap)#
```

Where *class\_map\_name* is the name of the class map. The **match-all** keyword specifies that traffic must match all criteria to match the class map. **match-all** is the default and only option. The CLI enters class-map configuration mode, where you can enter one or more **match** commands.

- b. (Optional) To add a description to the class map, enter the following command:

```
hostname(config-cmap)# description string
```

- c. (Optional) To match traffic with a content-type field in the HTTP response that does not match the accept field in the corresponding HTTP request message, enter the following command:

```
hostname(config-cmap)# match [not] req-resp content-type mismatch
```

- d. (Optional) To match text found in the HTTP request message arguments, enter the following command:

```
hostname(config-cmap)# match [not] request args regex [regex_name | class
regex_class_name]
```

Where the *regex\_name* is the regular expression you created in [Step 1](#). The **class regex\_class\_name** is the regular expression class map you created in [Step 2](#).

- e. (Optional) To match text found in the HTTP request message body or to match traffic that exceeds the maximum HTTP request message body length, enter the following command:

```
hostname(config-cmap)# match [not] request body {regex [regex_name | class
regex_class_name] | length gt max_bytes}
```

Where the **regex regex\_name** argument is the regular expression you created in [Step 1](#). The **class regex\_class\_name** is the regular expression class map you created in [Step 2](#). The **length gt max\_bytes** is the maximum message body length in bytes.

- f. (Optional) To match text found in the HTTP request message header, or to restrict the count or length of the header, enter the following command:

```
hostname(config-cmap)# match [not] request header {[field]
[regex [regex_name | class regex_class_name]] |
[length gt max_length_bytes | count gt max_count_bytes]}
```

Where the *field* is the predefined message header keyword. The **regex regex\_name** argument is the regular expression you created in [Step 1](#). The **class regex\_class\_name** is the regular expression class map you created in [Step 2](#). The **length gt max\_bytes** is the maximum message body length in bytes. The **count gt max\_count** is the maximum number of header fields.

- g. (Optional) To match text found in the HTTP request message method, enter the following command:

```
hostname(config-cmap)# match [not] request method {[method] |
[regex [regex_name | class regex_class_name]]
```

Where the *method* is the predefined message method keyword. The **regex regex\_name** argument is the regular expression you created in [Step 1](#). The **class regex\_class\_name** is the regular expression class map you created in [Step 2](#).

- h. (Optional) To match text found in the HTTP request message URI, enter the following command:

```
hostname(config-cmap)# match [not] request uri {regex [regex_name | class
regex_class_name] | length gt max_bytes}
```

Where the **regex regex\_name** argument is the regular expression you created in [Step 1](#). The **class regex\_class\_name** is the regular expression class map you created in [Step 2](#). The **length gt max\_bytes** is the maximum message body length in bytes.

- i. (Optional) To match text found in the HTTP response message body, or to comment out Java applet and Active X object tags in order to filter them, enter the following command:

```
hostname(config-cmap)# match [not] response body {[active-x] | [java-applet] |
[regex [regex_name] | class regex_class_name] | length gt max_bytes}
```

Where the **regex** *regex\_name* argument is the regular expression you created in [Step 1](#). The **class** *regex\_class\_name* is the regular expression class map you created in [Step 2](#). The **length gt** *max\_bytes* is the maximum message body length in bytes.

- j. (Optional) To match text found in the HTTP response message header, or to restrict the count or length of the header, enter the following command:

```
hostname(config-cmap)# match [not] response header {[field]
[regex [regex_name] | class regex_class_name] |
[length gt max_length_bytes | count gt max_count]}
```

Where the *field* is the predefined message header keyword. The **regex** *regex\_name* argument is the regular expression you created in [Step 1](#). The **class** *regex\_class\_name* is the regular expression class map you created in [Step 2](#). The **length gt** *max\_bytes* is the maximum message body length in bytes. The **count gt** *max\_count* is the maximum number of header fields.

- k. (Optional) To match text found in the HTTP response message status line, enter the following command:

```
hostname(config-cmap)# match [not] response status-line {regex [regex_name] | class
regex_class_name}
```

Where the **regex** *regex\_name* argument is the regular expression you created in [Step 1](#). The **class** *regex\_class\_name* is the regular expression class map you created in [Step 2](#).

- Step 4** Create an HTTP inspection policy map, enter the following command:

```
hostname(config)# policy-map type inspect http policy_map_name
hostname(config-pmap)#
```

Where the *policy\_map\_name* is the name of the policy map. The CLI enters policy-map configuration mode.

- Step 5** (Optional) To add a description to the policy map, enter the following command:

```
hostname(config-pmap)# description string
```

- Step 6** To apply actions to matching traffic, perform the following steps.

- a. Specify the traffic on which you want to perform actions using one of the following methods:

- Specify the HTTP class map that you created in [Step 3](#) by entering the following command:

```
hostname(config-pmap)# class class_map_name
hostname(config-pmap-c)#
```

- Specify traffic directly in the policy map using one of the **match** commands described in [Step 3](#). If you use a **match not** command, then any traffic that does not match the criterion in the **match not** command has the action applied.

- b. Specify the action you want to perform on the matching traffic by entering the following command:

```
hostname(config-pmap-c)# {[drop [send-protocol-error] |
drop-connection [send-protocol-error] | mask | reset] [log] | rate-limit message_rate}
```

Not all options are available for each **match** or **class** command. See the CLI help or the *Cisco Security Appliance Command Reference* for the exact options available.

The **drop** keyword drops all packets that match.

The **send-protocol-error** keyword sends a protocol error message.

The **drop-connection** keyword drops the packet and closes the connection.

The **mask** keyword masks out the matching portion of the packet.

The **reset** keyword drops the packet, closes the connection, and sends a TCP reset to the server and/or client.

The **log** keyword, which you can use alone or with one of the other keywords, sends a system log message.

The **rate-limit** *message\_rate* argument limits the rate of messages.

You can specify multiple **class** or **match** commands in the policy map. For information about the order of **class** and **match** commands, see the “[Defining Actions in an Inspection Policy Map](#)” section on page 21-8.

**Step 7** To configure parameters that affect the inspection engine, perform the following steps:

- a. To enter parameters configuration mode, enter the following command:

```
hostname(config-pmap) # parameters
hostname(config-pmap-p) #
```

- b. To check for HTTP protocol violations, enter the following command:

```
hostname(config-pmap-p) # protocol-violation [action [drop-connection / reset / log]]
```

Where the **drop-connection** action closes the connection. The **reset** action closes the connection and sends a TCP reset to the client. The **log** action sends a system log message when this policy map matches traffic.

- c. To substitute a string for the server header field, enter the following command:

```
hostname(config-pmap-p) # spoof-server string
```

Where the *string* argument is the string to substitute for the server header field. Note: WebVPN streams are not subject to the **spoof-server** command.

The following example shows how to define an HTTP inspection policy map that will allow and log any HTTP connection that attempts to access “www\.xyz.com/\*.asp” or “www\.xyz[0-9][0-9]\.com” with methods “GET” or “PUT.” All other URL/Method combinations will be silently allowed.

```
hostname(config) # regex url1 "www\.xyz.com/*.asp"
hostname(config) # regex url2 "www\.xyz[0-9][0-9]\.com"
hostname(config) # regex get "GET"
hostname(config) # regex put "PUT"

hostname(config) # class-map type regex match-any url_to_log
hostname(config-cmap) # match regex url1
hostname(config-cmap) # match regex url2
hostname(config-cmap) # exit

hostname(config) # class-map type regex match-any methods_to_log
hostname(config-cmap) # match regex get
hostname(config-cmap) # match regex put
hostname(config-cmap) # exit

hostname(config) # class-map type inspect http http_url_policy
hostname(config-cmap) # match request uri regex class url_to_log
hostname(config-cmap) # match request method regex class methods_to_log
hostname(config-cmap) # exit
```

```
hostname(config)# policy-map type inspect http http_policy
hostname(config-pmap)# class http_url_policy
hostname(config-pmap-c)# log
```

## Instant Messaging Inspection

This section describes the IM inspection engine. This section includes the following topics:

- [IM Inspection Overview, page 25-52](#)
- [Configuring an Instant Messaging Inspection Policy Map for Additional Inspection Control, page 25-52](#)

### IM Inspection Overview

The IM inspect engine lets you apply fine grained controls on the IM application to control the network usage and stop leakage of confidential data, propagation of worms, and other threats to the corporate network.

## Configuring an Instant Messaging Inspection Policy Map for Additional Inspection Control

To specify actions when a message violates a parameter, create an IM inspection policy map. You can then apply the inspection policy map when you enable IM inspection according to the [“Configuring Application Inspection”](#) section on page 25-5.

To create an IM inspection policy map, perform the following steps:

- 
- Step 1** (Optional) Add one or more regular expressions for use in traffic matching commands according to the [“Creating a Regular Expression”](#) section on page 21-12. See the types of text you can match in the **match** commands described in [Step 3](#).
- Step 2** (Optional) Create one or more regular expression class maps to group regular expressions according to the [“Creating a Regular Expression Class Map”](#) section on page 21-14.s
- Step 3** (Optional) Create an IM inspection class map by performing the following steps.

A class map groups multiple traffic matches. Traffic must match *all* of the **match** commands to match the class map. You can alternatively identify **match** commands directly in the policy map. The difference between creating a class map and defining the traffic match directly in the inspection policy map is that the class map lets you create more complex match criteria, and you can reuse class maps.

To specify traffic that should not match the class map, use the **match not** command. For example, if the **match not** command specifies the string “example.com,” then any traffic that includes “example.com” does not match the class map.

For the traffic that you identify in this class map, you can specify actions such as drop-connection, reset, and/or log the connection in the inspection policy map.

If you want to perform different actions for each **match** command, you should identify the traffic directly in the policy map.

- a. Create the class map by entering the following command:

```
hostname(config)# class-map type inspect im [match-all] class_map_name
hostname(config-cmap)#
```

Where *the class\_map\_name* is the name of the class map. The **match-all** keyword specifies that traffic must match all criteria to match the class map. **match-all** is the default and only option. The CLI enters class-map configuration mode, where you can enter one or more **match** commands.

- b. (Optional) To add a description to the class map, enter the following command:

```
hostname(config-cmap)# description string
```

Where *the string* is the description of the class map (up to 200 characters).

- c. (Optional) To match traffic of a specific IM protocol, such as Yahoo or MSN, enter the following command:

```
hostname(config-cmap)# match [not] protocol {im-yahoo | im-msn}
```

- d. (Optional) To match a specific IM service, such as chat, file-transfer, webcam, voice-chat, conference, or games, enter the following command:

```
hostname(config-cmap)# match [not] service {chat | file-transfer | webcam | voice-chat | conference | games}
```

- e. (Optional) To match the source login name of the IM message, enter the following command:

```
hostname(config-cmap)# match [not] login-name regex {class class_name | regex_name}
```

Where the **regex** *regex\_name* argument is the regular expression you created in [Step 1](#). The **class** *regex\_class\_name* is the regular expression class map you created in [Step 2](#).

- f. (Optional) To match the destination login name of the IM message, enter the following command:

```
hostname(config-cmap)# match [not] peer-login-name regex {class class_name | regex_name}
```

Where the **regex** *regex\_name* argument is the regular expression you created in [Step 1](#). The **class** *regex\_class\_name* is the regular expression class map you created in [Step 2](#).

- g. (Optional) To match the source IP address of the IM message, enter the following command:

```
hostname(config-cmap)# match [not] ip-address ip_address ip_address_mask
```

Where the *ip\_address* and the *ip\_address\_mask* is the IP address and netmask of the message source.

- h. (Optional) To match the destination IP address of the IM message, enter the following command:

```
hostname(config-cmap)# match [not] peer-ip-address ip_address ip_address_mask
```

Where the *ip\_address* and the *ip\_address\_mask* is the IP address and netmask of the message destination.

- i. (Optional) To match the version of the IM message, enter the following command:

```
hostname(config-cmap)# match [not] version regex {class class_name | regex_name}
```

Where the **regex** *regex\_name* argument is the regular expression you created in [Step 1](#). The **class** *regex\_class\_name* is the regular expression class map you created in [Step 2](#).

- j. (Optional) To match the filename of the IM message, enter the following command:

```
hostname(config-cmap)# match [not] filename regex {class class_name | regex_name}
```

Where the **regex** *regex\_name* argument is the regular expression you created in [Step 1](#). The **class** *regex\_class\_name* is the regular expression class map you created in [Step 2](#).



**Note** Not supported using MSN IM protocol.

**Step 4** Create an IM inspection policy map, enter the following command:

```
hostname(config)# policy-map type inspect im policy_map_name
hostname(config-pmap)#
```

Where the *policy\_map\_name* is the name of the policy map. The CLI enters policy-map configuration mode.

**Step 5** (Optional) To add a description to the policy map, enter the following command:

```
hostname(config-pmap)# description string
```

**Step 6** Specify the traffic on which you want to perform actions using one of the following methods:

- Specify the IM class map that you created in [Step 3](#) by entering the following command:

```
hostname(config-pmap)# class class_map_name
hostname(config-pmap-c)#
```

- Specify traffic directly in the policy map using one of the **match** commands described in [Step 3](#). If you use a **match not** command, then any traffic that does not match the criterion in the **match not** command has the action applied.

You can specify multiple **class** or **match** commands in the policy map. For information about the order of **class** and **match** commands, see the “[Defining Actions in an Inspection Policy Map](#)” section on [page 21-8](#).

**Step 7** Specify the action you want to perform on the matching traffic by entering the following command:

```
hostname(config-pmap-c)# {drop-connection | reset | log}
```

Where the **drop-connection** action closes the connection. The **reset** action closes the connection and sends a TCP reset to the client. The **log** action sends a system log message when this policy map matches traffic.

The following example shows how to define an IM inspection policy map.

```
hostname(config)# regex loginname1 "ying@yahoo.com"
hostname(config)# regex loginname2 "Kevin@yahoo.com"
hostname(config)# regex loginname3 "rahul@yahoo.com"
hostname(config)# regex loginname4 "darshant@yahoo.com"
hostname(config)# regex yahoo_version_regex "1\\.0"
hostname(config)# regex gif_files "\.gif"
hostname(config)# regex exe_files "\.exe"

hostname(config)# class-map type regex match-all yahoo_src_login_name_regex
hostname(config-cmap)# match regex loginname1
hostname(config-cmap)# match regex loginname2

hostname(config)# class-map type regex match-all yahoo_dst_login_name_regex
hostname(config-cmap)# match regex loginname3
hostname(config-cmap)# match regex loginname4

hostname(config)# class-map type inspect im match-all yahoo_file_block_list
hostname(config-cmap)# match filename regex gif_files
hostname(config-cmap)# match filename regex exe_files

hostname(config)# class-map type inspect im match-all yahoo_im_policy
```

```

hostname(config-cmap)# match login-name regex class yahoo_src_login_name_regex
hostname(config-cmap)# match peer-login-name regex class yahoo_dst_login_name_regex

hostname(config)# class-map type inspect im match-all yahoo_im_policy2
hostname(config-cmap)# match version regex yahoo_version_regex

hostname(config)# class-map im_inspect_class_map
hostname(config-cmap)# match default-inspection-traffic

hostname(config)# policy-map type inspect im im_policy_all
hostname(config-pmap)# class yahoo_file_block_list
hostname(config-pmap-c)# match service file-transfer
hostname(config-pmap)# class yahoo_im_policy
hostname(config-pmap-c)# drop-connection
hostname(config-pmap)# class yahoo_im_policy2
hostname(config-pmap-c)# reset
hostname(config)# policy-map global_policy_name
hostname(config-pmap)# class im_inspect_class_map
hostname(config-pmap-c)# inspect im im_policy_all

```

## ICMP Inspection

The ICMP inspection engine allows ICMP traffic to have a “session” so it can be inspected like TCP and UDP traffic. Without the ICMP inspection engine, we recommend that you do not allow ICMP through the security appliance in an access list. Without stateful inspection, ICMP can be used to attack your network. The ICMP inspection engine ensures that there is only one response for each request, and that the sequence number is correct.

## ICMP Error Inspection

When this feature is enabled, the security appliance creates translation sessions for intermediate hops that send ICMP error messages, based on the NAT configuration. The security appliance overwrites the packet with the translated IP addresses.

When disabled, the security appliance does not create translation sessions for intermediate nodes that generate ICMP error messages. ICMP error messages generated by the intermediate nodes between the inside host and the security appliance reach the outside host without consuming any additional NAT resource. This is undesirable when an outside host uses the traceroute command to trace the hops to the destination on the inside of the security appliance. When the security appliance does not translate the intermediate hops, all the intermediate hops appear with the mapped destination IP address.

The ICMP payload is scanned to retrieve the five-tuple from the original packet. Using the retrieved five-tuple, a lookup is performed to determine the original address of the client. The ICMP error inspection engine makes the following changes to the ICMP packet:

- In the IP Header, the mapped IP is changed to the real IP (Destination Address) and the IP checksum is modified.
- In the ICMP Header, the ICMP checksum is modified due to the changes in the ICMP packet.
- In the Payload, the following changes are made:
  - Original packet mapped IP is changed to the real IP
  - Original packet mapped port is changed to the real Port
  - Original packet IP checksum is recalculated

# ILS Inspection

The ILS inspection engine provides NAT support for Microsoft NetMeeting, SiteServer, and Active Directory products that use LDAP to exchange directory information with an ILS server.

The security appliance supports NAT for ILS, which is used to register and locate endpoints in the ILS or SiteServer Directory. PAT cannot be supported because only IP addresses are stored by an LDAP database.

For search responses, when the LDAP server is located outside, NAT should be considered to allow internal peers to communicate locally while registered to external LDAP servers. For such search responses, xlates are searched first, and then DNAT entries to obtain the correct address. If both of these searches fail, then the address is not changed. For sites using NAT 0 (no NAT) and not expecting DNAT interaction, we recommend that the inspection engine be turned off to provide better performance.

Additional configuration may be necessary when the ILS server is located inside the security appliance border. This would require a hole for outside clients to access the LDAP server on the specified port, typically TCP 389.

Because ILS traffic only occurs on the secondary UDP channel, the TCP connection is disconnected after the TCP inactivity interval. By default, this interval is 60 minutes and can be adjusted using the **timeout** command.

ILS/LDAP follows a client/server model with sessions handled over a single TCP connection. Depending on the client's actions, several of these sessions may be created.

During connection negotiation time, a BIND PDU is sent from the client to the server. Once a successful BIND RESPONSE from the server is received, other operational messages may be exchanged (such as ADD, DEL, SEARCH, or MODIFY) to perform operations on the ILS Directory. The ADD REQUEST and SEARCH RESPONSE PDUs may contain IP addresses of NetMeeting peers, used by H.323 (SETUP and CONNECT messages) to establish the NetMeeting sessions. Microsoft NetMeeting v2.X and v3.X provides ILS support.

The ILS inspection performs the following operations:

- Decodes the LDAP REQUEST/RESPONSE PDUs using the BER decode functions
- Parses the LDAP packet
- Extracts IP addresses
- Translates IP addresses as necessary
- Encodes the PDU with translated addresses using BER encode functions
- Copies the newly encoded PDU back to the TCP packet
- Performs incremental TCP checksum and sequence number adjustment

ILS inspection has the following limitations:

- Referral requests and responses are not supported
- Users in multiple directories are not unified
- Single users having multiple identities in multiple directories cannot be recognized by NAT

**Note**

Because H225 call signalling traffic only occurs on the secondary UDP channel, the TCP connection is disconnected after the interval specified by the TCP **timeout** command. By default, this interval is set at 60 minutes.

# IPSec Pass Through Inspection

This section describes IPSec Pass Through application inspection. This section includes the following topics:

- [IPSec Pass Through Inspection Overview, page 25-57](#)
- [Configuring an IPSec Pass Through Inspection Policy Map for Additional Inspection Control, page 25-57](#)

## IPSec Pass Through Inspection Overview

The IPSec Pass Through inspection engine lets the security appliance pass ESP (IP protocol 50) and AH (IP protocol 51) traffic that is formed between two hosts because of successful IKE (UDP port 500) negotiation without the requirement of specific ESP or AH access lists.

The inspection engine works on IKE UDP port 500 to create the control flow. The **inspect ipsec-pass-thru** command is attached to an UDP flow as defined in the MPF framework. When an ESP or AH packet between the two peers arrives at the device, or an UDP packet with either source or destination port equal to 500, the packet is sent to the inspect module.

The ESP or AH traffic is permitted by the inspection engine with the configured idle timeout if there is an existing control flow and it is within the connection limit defined in the MPF framework. A new control flow is created for IKE UDP port 500 traffic with the configured UDP idle timeout if there isn't one, or it uses the existing flow.

To ensure that the packet arrives into the inspection engine, a hole is punched for all such traffic (ESP and AH). This inspect is attached to the control flow. The control flow is present as long as there is at least one data flow (ESP or AH) established, but the traffic always flows on the same connection. Since this IKE connection is kept open as long as data flows, a rekey would always succeed. The flows are created irrespective of NAT or no NAT.

**Note**

PAT is not supported.

## Configuring an IPSec Pass Through Inspection Policy Map for Additional Inspection Control

Inspect IPSec Pass Through is disabled by default. When enabled without using a parameter map, the inspection uses the default IPSec Pass Through parameter map, which allows only ESP traffic with unlimited connections and the default idle timeout of 10 minutes for the ESP connection.

To pass ESP or AH traffic, IPSec Pass Through parameter map is required.

To create an IPSec Pass Through map, perform the following steps:

**Step 1** To create an IPSec Pass Through inspection policy map, enter the following command:

```
hostname(config)# policy-map type inspect IPsec-pass-thru map_name
hostname(config-pmap)#
```

Where the *policy\_map\_name* is the name of the policy map. The CLI enters policy-map configuration mode.

**Step 2** (Optional) To add a description to the policy map, enter the following command:

```
hostname(config-pmap)# description string
```

**Step 3** To configure parameters that affect the inspection engine, perform the following steps:

a. To enter parameters configuration mode, enter the following command:

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b. To configure for ESP traffic, enter the following command:

```
hostname(config-pmap-p)# esp per-client-max value timeout timeout
```

c. To configure for AH traffic, enter the following command:

```
hostname(config-pmap-p)# ah per-client-max value timeout timeout
```

---

The following example shows how to define an IPSec Pass Through map:

```
hostname(config)# access-list test-udp-acl extended permit udp any any eq 500

hostname(config)# class-map test-udp-class
hostname(config-cmap)# match access-list test-udp-acl

hostname(config)# policy-map type inspect IPSec-pass-thru IPsec-map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# esp per-client-max 32 timeout 00:06:00
hostname(config-pmap-p)# ah per-client-max 16 timeout 00:05:00

hostname(config)# policy-map test-udp-policy
hostname(config-pmap)# class test-udp-class
hostname(config-pmap-c)# inspect IPSec-pass-thru IPsec-map
```

This policy is applied on the interface that has the policy to permit UDP 500 traffic through initially. In this example it is the outside interface.

To verify that the inspection engine opens the ESP or AH data flows for IPSec Pass Through based on the IKE control flow, use the **show conn** command:

```
hostname(config)# show conn
ESP out 192.168.51.25 in 192.168.52.49 idle 0:00:00 bytes 108
AH out 192.168.51.25 in 192.168.52.49 idle 0:00:01 bytes 0
ESP out 192.168.51.25 in 192.168.52.49 idle 0:00:01 bytes 0
UDP out 192.168.51.25:500 in 192.168.52.49:500 idle 0:00:00 flags -
AH out 192.168.51.25 in 192.168.52.50 idle 0:00:22 bytes 0
ESP out 192.168.51.25 in 192.168.52.50 idle 0:00:22 bytes 0
UDP out 192.168.51.25:500 in 192.168.52.50:500 idle 0:00:00 flags -
ESP out 192.168.51.25 in 192.168.52.49 idle 0:00:00 bytes 108
AH out 0.0.0.0 in 0.0.0.0 idle 0:00:01 bytes 0
ESP out 0.0.0.0 in 0.0.0.0 idle 0:00:01 bytes 0
AH out 192.168.51.25 in 192.168.52.50 idle 0:00:00 bytes 2080
AH out 0.0.0.0 in 0.0.0.0 idle 0:00:22 bytes 0
ESP out 0.0.0.0 in 0.0.0.0 idle 0:00:22 bytes 0
```

## MGCP Inspection

This section describes MGCP application inspection. This section includes the following topics:

- [MGCP Inspection Overview, page 25-59](#)
- [Configuring an MGCP Inspection Policy Map for Additional Inspection Control, page 25-61](#)
- [Configuring MGCP Timeout Values, page 25-62](#)
- [Verifying and Monitoring MGCP Inspection, page 25-62](#)

## MGCP Inspection Overview

MGCP is a master/slave protocol used to control media gateways from external call control elements called media gateway controllers or call agents. A media gateway is typically a network element that provides conversion between the audio signals carried on telephone circuits and data packets carried over the Internet or over other packet networks. Using NAT and PAT with MGCP lets you support a large number of devices on an internal network with a limited set of external (global) addresses. Examples of media gateways are:

- Trunking gateways, that interface between the telephone network and a Voice over IP network. Such gateways typically manage a large number of digital circuits.
- Residential gateways, that provide a traditional analog (RJ11) interface to a Voice over IP network. Examples of residential gateways include cable modem/cable set-top boxes, xDSL devices, broad-band wireless devices.
- Business gateways, that provide a traditional digital PBX interface or an integrated soft PBX interface to a Voice over IP network.



### Note

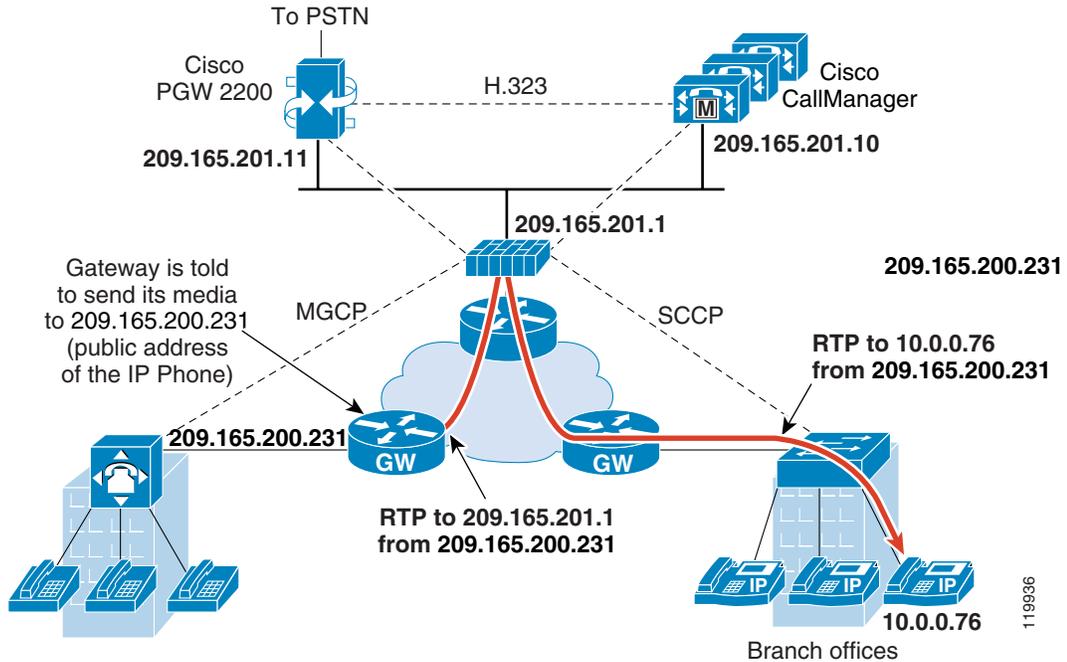
---

To avoid policy failure when upgrading from ASA version 7.1, all layer 7 and layer 3 policies must have distinct names. For instance, a previously configured policy map with the same name as a previously configured MGCP map must be changed before the upgrade.

---

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 may not arrive from the same address as the command was sent to. This can happen when multiple call agents are being 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. [Figure 25-4](#) illustrates how NAT can be used with MGCP.

Figure 25-4 Using NAT with MGCP



MGCP endpoints are physical or virtual sources and destinations for data. Media gateways contain endpoints on which the call agent can create, modify and delete connections to establish and control media sessions with other multimedia endpoints. Also, the call agent can instruct the endpoints to detect certain events and generate signals. The endpoints automatically communicate changes in service state to the call agent.

MGCP transactions are composed of a command and a mandatory response. There are eight types of commands:

- CreateConnection
- ModifyConnection
- DeleteConnection
- NotificationRequest
- Notify
- AuditEndpoint
- AuditConnection
- RestartInProgress

The first four commands are sent by the call agent to the gateway. The Notify command is sent by the gateway to the call agent. The gateway may also send a DeleteConnection. The registration of the MGCP gateway with the call agent is achieved by the RestartInProgress command. The AuditEndpoint and the AuditConnection commands are sent by the call agent to the gateway.

All commands are composed of a Command header, optionally followed by a session description. All responses are composed of a Response header, optionally followed by a session description.

- The port on which the gateway receives commands from the call agent. Gateways usually listen to UDP port 2427.

- The port on which the call agent receives commands from the gateway. Call agents usually listen to UDP port 2727.

**Note**

MGCP inspection does not support the use of different IP addresses for MGCP signaling and RTP data. A common and recommended practice is to send RTP data from a resilient IP address, such as a loopback or virtual IP address; however, the security appliance requires the RTP data to come from the same address as MGCP signalling.

## Configuring 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 according to the [“Configuring Application Inspection” section on page 25-5](#)

To create an MGCP map, perform the following steps:

**Step 1** To create an MGCP inspection policy map, enter the following command:

```
hostname(config)# policy-map type inspect mgcp map_name
hostname(config-pmap)#
```

Where the *policy\_map\_name* is the name of the policy map. The CLI enters policy-map configuration mode.

**Step 2** (Optional) To add a description to the policy map, enter the following command:

```
hostname(config-pmap)# description string
```

**Step 3** To configure parameters that affect the inspection engine, perform the following steps:

a. To enter parameters configuration mode, enter the following command:

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b. To configure the call agents, enter the following command for each call agent:

```
hostname(config-pmap-p)# call-agent ip_address group_id
```

Use the **call-agent** command to specify a group of call agents that can manage one or more gateways. The call agent group information is used to open connections for the call agents in the group (other than the one a gateway sends a command to) so that any of the call agents can send the response. call agents with the same *group\_id* belong to the same group. A call agent may belong to more than one group. The *group\_id* option is a number from 0 to 4294967295. The *ip\_address* option specifies the IP address of the call agent.

**Note**

MGCP call agents send AUEP messages to determine if MGCP end points are present. This establishes a flow through the security appliance and allows MGCP end points to register with the call agent.

c. To configure the gateways, enter the following command for each gateway:

```
hostname(config-pmap-p)# gateway ip_address group_id
```

Use the **gateway** command to specify which group of call agents are managing a particular gateway. The IP address of the gateway is specified with the *ip\_address* option. The *group\_id* option is a number from 0 to 4294967295 that must correspond with the *group\_id* of the call agents that are managing the gateway. A gateway may only belong to one group.

- d. If you want to change the maximum number of commands allowed in the MGCP command queue, enter the following command:

```
hostname(config-pmap-p)# command-queue command_limit
```

The following example shows how to define an MGCP map:

```
hostname(config)# policy-map type inspect mgcp sample_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# call-agent 10.10.11.5 101
hostname(config-pmap-p)# call-agent 10.10.11.6 101
hostname(config-pmap-p)# call-agent 10.10.11.7 102
hostname(config-pmap-p)# call-agent 10.10.11.8 102
hostname(config-pmap-p)# gateway 10.10.10.115 101
hostname(config-pmap-p)# gateway 10.10.10.116 102
hostname(config-pmap-p)# gateway 10.10.10.117 102
hostname(config-pmap-p)# command-queue 150
```

## Configuring MGCP Timeout Values

The **timeout mgcp** command lets you set the interval for inactivity after which an MGCP media connection is closed. The default is 5 minutes.

The **timeout mgcp-pat** command lets you set the timeout for PAT xlates. Because MGCP does not have a keepalive mechanism, if you use non-Cisco MGCP gateways (call agents), the PAT xlates are torn down after the default timeout interval, which is 30 seconds.

## Verifying and Monitoring MGCP Inspection

The **show mgcp commands** command lists the number of MGCP commands in the command queue. The **show mgcp sessions** command lists the number of existing MGCP sessions. The **detail** option includes additional information about each command (or session) in the output. The following is sample output from the **show mgcp commands** command:

```
hostname# show mgcp commands
1 in use, 1 most used, 200 maximum allowed
CRCX, gateway IP: host-pc-2, transaction ID: 2052, idle: 0:00:07
```

The following is sample output from the **show mgcp detail** command.

```
hostname# show mgcp commands detail
1 in use, 1 most used, 200 maximum allowed
CRCX, idle: 0:00:10
 Gateway IP host-pc-2
 Transaction ID 2052
 Endpoint name aaln/1
 Call ID 9876543210abcdef
 Connection ID
 Media IP 192.168.5.7
 Media port 6058
```

The following is sample output from the **show mgcp sessions** command.

```
hostname# show mgcp sessions
1 in use, 1 most used
Gateway IP host-pc-2, connection ID 6789af54c9, active 0:00:11
```

The following is sample output from the **show mgcp sessions detail** command.

```
hostname# show mgcp sessions detail
1 in use, 1 most used
Session active 0:00:14
 Gateway IP host-pc-2
 Call ID 9876543210abcdef
 Connection ID 6789af54c9
 Endpoint name aaln/1
 Media lcl port 6166
 Media rmt IP 192.168.5.7
 Media rmt port 6058
```

## NetBIOS Inspection

NetBIOS inspection is enabled by default. The NetBios inspection engine translates IP addresses in the NetBios name service (NBNS) packets according to the security appliance NAT configuration.

### Configuring a NetBIOS Inspection Policy Map for Additional Inspection Control

To specify actions when a message violates a parameter, create a NETBIOS inspection policy map. You can then apply the inspection policy map when you enable NETBIOS inspection according to the [“Configuring Application Inspection” section on page 25-5](#).

To create a NETBIOS inspection policy map, perform the following steps:

---

**Step 1** (Optional) Add one or more regular expressions for use in traffic matching commands according to the [“Creating a Regular Expression” section on page 21-12](#). See the types of text you can match in the **match** commands described in [Step 3](#).

**Step 2** (Optional) Create one or more regular expression class maps to group regular expressions according to the [“Creating a Regular Expression Class Map” section on page 21-14](#).

**Step 3** Create a NetBIOS inspection policy map, enter the following command:

```
hostname(config)# policy-map type inspect netbios policy_map_name
hostname(config-pmap)#
```

Where the *policy\_map\_name* is the name of the policy map. The CLI enters policy-map configuration mode.

**Step 4** (Optional) To add a description to the policy map, enter the following command:

```
hostname(config-pmap)# description string
```

**Step 5** To apply actions to matching traffic, perform the following steps.

a. Specify the traffic on which you want to perform actions using one of the following methods:

- Specify the NetBIOS class map that you created in [Step 3](#) by entering the following command:

```
hostname(config-pmap)# class class_map_name
hostname(config-pmap-c)#
```

- Specify traffic directly in the policy map using one of the **match** commands described in [Step 3](#). If you use a **match not** command, then any traffic that does not match the criterion in the **match not** command has the action applied.
- b. Specify the action you want to perform on the matching traffic by entering the following command:

```
hostname(config-pmap-c)# {[drop [send-protocol-error] |
drop-connection [send-protocol-error] | mask | reset] [log] | rate-limit message_rate}
```

Not all options are available for each **match** or **class** command. See the CLI help or the *Cisco Security Appliance Command Reference* for the exact options available.

The **drop** keyword drops all packets that match.

The **send-protocol-error** keyword sends a protocol error message.

The **drop-connection** keyword drops the packet and closes the connection.

The **mask** keyword masks out the matching portion of the packet.

The **reset** keyword drops the packet, closes the connection, and sends a TCP reset to the server and/or client.

The **log** keyword, which you can use alone or with one of the other keywords, sends a system log message.

The **rate-limit message\_rate** argument limits the rate of messages.

You can specify multiple **class** or **match** commands in the policy map. For information about the order of **class** and **match** commands, see the “[Defining Actions in an Inspection Policy Map](#)” section on [page 21-8](#).

**Step 6** To configure parameters that affect the inspection engine, perform the following steps:

- a. To enter parameters configuration mode, enter the following command:

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

- b. To check for NETBIOS protocol violations, enter the following command:

```
hostname(config-pmap-p)# protocol-violation [action [drop-connection | reset | log]]
```

Where the **drop-connection** action closes the connection. The **reset** action closes the connection and sends a TCP reset to the client. The **log** action sends a system log message when this policy map matches traffic.

The following example shows how to define a NETBIOS inspection policy map.

```
hostname(config)# policy-map type inspect netbios netbios_map
hostname(config-pmap)# protocol-violation drop log
```

```
hostname(config)# policy-map netbios_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect netbios netbios_map
```

## PPTP Inspection

PPTP is a protocol for tunneling PPP traffic. A PPTP session is composed of one TCP channel and usually two PPTP GRE tunnels. The TCP channel is the control channel used for negotiating and managing the PPTP GRE tunnels. The GRE tunnels carries PPP sessions between the two hosts.

When enabled, PPTP application inspection inspects PPTP protocol packets and dynamically creates the GRE connections and xlates necessary to permit PPTP traffic. Only Version 1, as defined in RFC 2637, is supported.

PAT is only performed for the modified version of GRE [RFC 2637] when negotiated over the PPTP TCP control channel. Port Address Translation is *not* performed for the unmodified version of GRE [RFC 1701, RFC 1702].

Specifically, the security appliance inspects the PPTP version announcements and the outgoing call request/response sequence. Only PPTP Version 1, as defined in RFC 2637, is inspected. Further inspection on the TCP control channel is disabled if the version announced by either side is not Version 1. In addition, the outgoing-call request and reply sequence are tracked. Connections and xlates are dynamic allocated as necessary to permit subsequent secondary GRE data traffic.

The PPTP inspection engine must be enabled for PPTP traffic to be translated by PAT. Additionally, PAT is only performed for a modified version of GRE (RFC2637) and only if it is negotiated over the PPTP TCP control channel. PAT is not performed for the unmodified version of GRE (RFC 1701 and RFC 1702).

As described in RFC 2637, the PPTP protocol is mainly used for the tunneling of PPP sessions initiated from a modem bank PAC (PPTP Access Concentrator) to the headend PNS (PPTP Network Server). When used this way, the PAC is the remote client and the PNS is the server.

However, when used for VPN by Windows, the interaction is inverted. The PNS is a remote single-user PC that initiates connection to the head-end PAC to gain access to a central network.

## RADIUS Accounting Inspection

One of the well known problems is the over-billing attack in GPRS networks. The over-billing attack can cause consumers anger and frustration by being billed for services that they have not used. In this case, a malicious attacker sets up a connection to a server and obtains an IP address from the SGSN. When the attacker ends the call, the malicious server will still send packets to it, which gets dropped by the GGSN, but the connection from the server remains active. The IP address assigned to the malicious attacker gets released and reassigned to a legitimate user who will then get billed for services that the attacker will use.

RADIUS accounting inspection prevents this type of attack by ensuring the traffic seen by the GGSN is legitimate. With the RADIUS accounting feature properly configured, the security appliance tears down a connection based on matching the Framed IP attribute in the Radius Accounting Request Start message with the Radius Accounting Request Stop message. When the Stop message is seen with the matching IP address in the Framed IP attribute, the security appliance looks for all connections with the source matching the IP address.

You have the option to configure a secret pre-shared key with the RADIUS server so the security appliance can validate the message. If the shared secret is not configured, the security appliance does not need to validate the source of the message and will only check that the source IP address is one of the configured addresses allowed to send the RADIUS messages.

**Note**

When using RADIUS accounting inspection with GPRS enabled, the security appliance checks for the 3GPP-Session-Stop-Indicator in the Accounting Request STOP messages to properly handle secondary PDP contexts. Specifically, the security appliance requires that the Accounting Request STOP messages include the 3GPP-SGSN-Address attribute before it will terminate the user sessions and all associated connections. Some third-party GGSNs might not send this attribute by default.

## Configuring a RADIUS Inspection Policy Map for Additional Inspection Control

In order to use this feature, the **radius-accounting-map** will need to be specified in the **policy-map** and then applied to the service-policy to specify that this traffic is for to-the-box inspection.

The following example shows the complete set of commands in context to properly configure this feature:

**Step 1** Configure the class map and the port:

```
class-map type management c1
 match port udp eq 1813
```

**Step 2** Create the policy map, and configure the parameters for RADIUS accounting inspection using the parameter command to access the proper mode to configure the attributes, host, and key.

```
policy-map type inspect radius-accounting radius_accounting_map
 parameters
 host 10.1.1.1 inside key 123456789
 send response
 enable gprs
 validate-attribute 31
```

**Step 3** Configure the service policy.

```
policy-map global_policy
 class c1
 inspect radius-accounting radius_accounting_map

service-policy global_policy global
```

## RSH Inspection

RSH inspection is enabled by default. The RSH protocol uses a TCP connection from the RSH client to the RSH server on TCP port 514. The client and server negotiate the TCP port number where the client listens for the STDERR output stream. RSH inspection supports NAT of the negotiated port number if necessary.

## RTSP Inspection

This section describes RTSP application inspection. This section includes the following topics:

- [RTSP Inspection Overview, page 25-67](#)
- [Using RealPlayer, page 25-67](#)
- [Restrictions and Limitations, page 25-67](#)

## RTSP Inspection Overview

The RTSP inspection engine lets the security appliance pass RTSP packets. RTSP is used by RealAudio, RealNetworks, Apple QuickTime 4, RealPlayer, and Cisco IP/TV connections.

**Note**

For Cisco IP/TV, use RTSP TCP port 554 and TCP 8554.

RTSP applications use the well-known port 554 with TCP (rarely UDP) as a control channel. The security appliance only supports TCP, in conformity with RFC 2326. This TCP control channel is used to negotiate the data channels that is used to transmit audio/video traffic, depending on the transport mode that is configured on the client.

The supported RDT transports are: rtp/avp, rtp/avp/udp, x-real-rdt, x-real-rdt/udp, and x-pn-tng/udp.

The security appliance parses Setup response messages with a status code of 200. If the response message is travelling inbound, the server is outside relative to the security appliance and dynamic channels need to be opened for connections coming inbound from the server. If the response message is outbound, then the security appliance does not need to open dynamic channels.

Because RFC 2326 does not require that the client and server ports must be in the SETUP response message, the security appliance keeps state and remembers the client ports in the SETUP message. QuickTime places the client ports in the SETUP message and then the server responds with only the server ports.

RTSP inspection does not support PAT or dual-NAT. Also, the security appliance cannot recognize HTTP cloaking where RTSP messages are hidden in the HTTP messages.

## Using RealPlayer

When using RealPlayer, it is important to properly configure transport mode. For the security appliance, add an **access-list** command from the server to the client or vice versa. For RealPlayer, change transport mode by clicking **Options>Preferences>Transport>RTSP Settings**.

If using TCP mode on the RealPlayer, select the **Use TCP to Connect to Server** and **Attempt to use TCP for all content** check boxes. On the security appliance, there is no need to configure the inspection engine.

If using UDP mode on the RealPlayer, select the **Use TCP to Connect to Server** and **Attempt to use UDP for static content** check boxes, and for live content not available via Multicast. On the security appliance, add an **inspect rtsp port** command.

## Restrictions and Limitations

The following restrictions apply to the **inspect rtsp** command.

- The security appliance does not support multicast RTSP or RTSP messages over UDP.
- PAT is not supported.
- The security appliance does not have the ability to recognize HTTP cloaking where RTSP messages are hidden in the HTTP messages.
- The security appliance cannot perform NAT on RTSP messages because the embedded IP addresses are contained in the SDP files as part of HTTP or RTSP messages. Packets could be fragmented and security appliance cannot perform NAT on fragmented packets.

- With Cisco IP/TV, the number of translates the security appliance performs on the SDP part of the message is proportional to the number of program listings in the Content Manager (each program listing can have at least six embedded IP addresses).
- You can configure NAT for Apple QuickTime 4 or RealPlayer. Cisco IP/TV only works with NAT if the Viewer and Content Manager are on the outside network and the server is on the inside network.

## SIP Inspection

This section describes SIP application inspection. This section includes the following topics:

- [SIP Inspection Overview, page 25-68](#)
- [SIP Instant Messaging, page 25-69](#)
- [Configuring SIP Timeout Values, page 25-73](#)
- [Verifying and Monitoring SIP Inspection, page 25-73](#)

## SIP Inspection Overview

SIP, as defined by the IETF, enables call handling sessions, particularly two-party audio conferences, or “calls.” SIP works with SDP for call signalling. SDP specifies the ports for the media stream. Using SIP, the security appliance can support any SIP VoIP gateways and VoIP proxy servers. SIP and SDP are defined in the following RFCs:

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

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, 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 NAT for these embedded IP addresses.

The following limitations and restrictions apply when using PAT with SIP:

- 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, as follows:
  - PAT is configured for the remote endpoint.
  - The SIP registrar server is on the outside network.
  - The port is missing in the contact field in the REGISTER message sent by the endpoint to the proxy server.
- If a SIP device transmits a packet in which the SDP portion has an IP address in the owner/creator field (o=) that is different than the IP address in the connection field (c=), the IP address in the o= field may not be properly translated. This is due to a limitation in the SIP protocol, which does not provide a port value in the o= field.

## SIP Instant Messaging

Instant Messaging refers to the transfer of messages between users in near real-time. SIP supports the Chat feature on Windows XP using Windows Messenger RTC Client version 4.7.0105 only. The MESSAGE/INFO methods and 202 Accept response are used to support IM as defined in the following RFCs:

- Session Initiation Protocol (SIP)-Specific Event Notification, RFC 3265
- Session Initiation Protocol (SIP) Extension for Instant Messaging, RFC 3428

MESSAGE/INFO requests can come in at any time after registration/subscription. For example, two users can be online at any time, but not chat for hours. Therefore, the SIP inspection engine opens pinholes that time out according to the configured SIP timeout value. This value must be configured at least five minutes longer than the subscription duration. The subscription duration is defined in the Contact Expires value and is typically 30 minutes.

Because MESSAGE/INFO requests are typically sent using a dynamically allocated port other than port 5060, they are required to go through the SIP inspection engine.

**Note**

Only the Chat feature is currently supported. Whiteboard, File Transfer, and Application Sharing are not supported. RTC Client 5.0 is not supported.

SIP inspection translates 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. These indices identify the call, the source, and the destination. This database contains the media addresses and media ports found in the SDP media information fields and the media type. There can be multiple media addresses and ports for a session. The security appliance opens RTP/RTCP connections 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 may 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 translated.

As a call is set up, the SIP session is in the “transient” state until the media address and media port is received from the called endpoint in a Response message indicating the RTP port the called endpoint listens on. 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 does not traverse the security appliance, unless the security appliance configuration specifically allows it.

## Configuring a SIP Inspection Policy Map for Additional Inspection Control

To specify actions when a message violates a parameter, create a SIP inspection policy map. You can then apply the inspection policy map when you enable SIP inspection according to the “[Configuring Application Inspection](#)” section on page 25-5.

To create a SIP inspection policy map, perform the following steps:

- 
- Step 1** (Optional) Add one or more regular expressions for use in traffic matching commands according to the “[Creating a Regular Expression](#)” section on page 21-12. See the types of text you can match in the **match** commands described in [Step 3](#).
  - Step 2** (Optional) Create one or more regular expression class maps to group regular expressions according to the “[Creating a Regular Expression Class Map](#)” section on page 21-14.s
  - Step 3** (Optional) Create a SIP inspection class map by performing the following steps.

A class map groups multiple traffic matches. Traffic must match *all* of the **match** commands to match the class map. You can alternatively identify **match** commands directly in the policy map. The difference between creating a class map and defining the traffic match directly in the inspection policy map is that the class map lets you create more complex match criteria, and you can reuse class maps.

To specify traffic that should not match the class map, use the **match not** command. For example, if the **match not** command specifies the string “example.com,” then any traffic that includes “example.com” does not match the class map.

For the traffic that you identify in this class map, you can specify actions such as drop-connection, reset, and/or log the connection in the inspection policy map.

If you want to perform different actions for each **match** command, you should identify the traffic directly in the policy map.

- a. Create the class map by entering the following command:

```
hostname(config)# class-map type inspect sip [match-all] class_map_name
hostname(config-cmap)#
```

Where *the class\_map\_name* is the name of the class map. The **match-all** keyword specifies that traffic must match all criteria to match the class map. **match-all** is the default and only option. The CLI enters class-map configuration mode, where you can enter one or more **match** commands.

- b. (Optional) To add a description to the class map, enter the following command:

```
hostname(config-cmap)# description string
```

Where *string* is the description of the class map (up to 200 characters).

- c. (Optional) To match a called party, as specified in the To header, enter the following command:

```
hostname(config-cmap)# match [not] called-party regex {class class_name | regex_name}
```

Where the **regex regex\_name** argument is the regular expression you created in [Step 1](#). The **class regex\_class\_name** is the regular expression class map you created in [Step 2](#).

- d. (Optional) To match a calling party, as specified in the From header, enter the following command:

```
hostname(config-cmap)# match [not] calling-party regex {class class_name | regex_name}
```

Where the **regex regex\_name** argument is the regular expression you created in [Step 1](#). The **class regex\_class\_name** is the regular expression class map you created in [Step 2](#).

- e. (Optional) To match a content length in the SIP header, enter the following command:

```
hostname(config-cmap)# match [not] content length gt length
```

Where *length* is the number of bytes the content length is greater than. 0 to 65536.

- f. (Optional) To match an SDP content type or regular expression, enter the following command:

```
hostname(config-cmap)# match [not] content type {sdp | regex {class class_name | regex_name}}
```

Where the **regex** *regex\_name* argument is the regular expression you created in [Step 1](#). The **class** *regex\_class\_name* is the regular expression class map you created in [Step 2](#).

- g. (Optional) To match a SIP IM subscriber, enter the following command:

```
hostname(config-cmap)# match [not] im-subscriber regex {class class_name | regex_name}
```

Where the **regex** *regex\_name* argument is the regular expression you created in [Step 1](#). The **class** *regex\_class\_name* is the regular expression class map you created in [Step 2](#).

- h. (Optional) To match a SIP via header, enter the following command:

```
hostname(config-cmap)# match [not] message-path regex {class class_name | regex_name}
```

Where the **regex** *regex\_name* argument is the regular expression you created in [Step 1](#). The **class** *regex\_class\_name* is the regular expression class map you created in [Step 2](#).

- i. (Optional) To match a SIP request method, enter the following command:

```
hostname(config-cmap)# match [not] request-method method
```

Where *method* is the type of method to match (ack, bye, cancel, info, invite, message, notify, options, prack, refer, register, subscribe, unknown, update).

- j. (Optional) To match the requester of a third-party registration, enter the following command:

```
hostname(config-cmap)# match [not] third-party-registration regex {class class_name | regex_name}
```

Where the **regex** *regex\_name* argument is the regular expression you created in [Step 1](#). The **class** *regex\_class\_name* is the regular expression class map you created in [Step 2](#).

- k. (Optional) To match an URI in the SIP headers, enter the following command:

```
hostname(config-cmap)# match [not] uri {sip | tel} length gt length
```

Where *length* is the number of bytes the URI is greater than. 0 to 65536.

- Step 4** Create a SIP inspection policy map, enter the following command:

```
hostname(config)# policy-map type inspect sip policy_map_name
hostname(config-pmap)#
```

Where the *policy\_map\_name* is the name of the policy map. The CLI enters policy-map configuration mode.

- Step 5** (Optional) To add a description to the policy map, enter the following command:

```
hostname(config-pmap)# description string
```

- Step 6** To apply actions to matching traffic, perform the following steps.

- a. Specify the traffic on which you want to perform actions using one of the following methods:

- Specify the SIP class map that you created in [Step 3](#) by entering the following command:

```
hostname(config-pmap)# class class_map_name
hostname(config-pmap-c)#
```

- Specify traffic directly in the policy map using one of the **match** commands described in [Step 3](#). If you use a **match not** command, then any traffic that does not match the criterion in the **match not** command has the action applied.

- Specify the action you want to perform on the matching traffic by entering the following command:

```
hostname(config-pmap-c)# {[drop [send-protocol-error] |
drop-connection [send-protocol-error] | mask | reset] [log] | rate-limit message_rate}
```

Not all options are available for each **match** or **class** command. See the CLI help or the *Cisco Security Appliance Command Reference* for the exact options available.

The **drop** keyword drops all packets that match.

The **send-protocol-error** keyword sends a protocol error message.

The **drop-connection** keyword drops the packet and closes the connection.

The **mask** keyword masks out the matching portion of the packet.

The **reset** keyword drops the packet, closes the connection, and sends a TCP reset to the server and/or client.

The **log** keyword, which you can use alone or with one of the other keywords, sends a system log message.

The **rate-limit message\_rate** argument limits the rate of messages.

You can specify multiple **class** or **match** commands in the policy map. For information about the order of **class** and **match** commands, see the “[Defining Actions in an Inspection Policy Map](#)” section on [page 21-8](#).

- Step 7** To configure parameters that affect the inspection engine, perform the following steps:

- To enter parameters configuration mode, enter the following command:

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

- To enable or disable instant messaging, enter the following command:

```
hostname(config-pmap-p)# im
```

- To enable or disable IP address privacy, enter the following command:

```
hostname(config-pmap-p)# ip-address-privacy
```

- To enable check on Max-forwards header field being 0 (which cannot be 0 before reaching the destination), enter the following command:

```
hostname(config-pmap-p)# max-forwards-validation action {drop | drop-connection |
reset | log} [log]
```

- To enable check on RTP packets flowing on the pinholes for protocol conformance, enter the following command:

```
hostname(config-pmap-p)# rtp-conformance [enforce-payloadtype]
```

Where the **enforce-payloadtype** keyword enforces the payload type to be audio or video based on the signaling exchange.

- To identify the Server and User-Agent header fields, which expose the software version of either a server or an endpoint, enter the following command:

```
hostname(config-pmap-p)# software-version action {mask | log} [log]
```

Where the **mask** keyword masks the software version in the SIP messages.

- g. To enable state checking validation, enter the following command:

```
hostname(config-pmap-p)# state-checking action {drop | drop-connection | reset | log} [log]
```

- h. To enable strict verification of the header fields in the SIP messages according to RFC 3261, enter the following command:

```
hostname(config-pmap-p)# strict-header-validation action {drop | drop-connection | reset | log} [log]
```

- i. To allow non SIP traffic using the well-known SIP signaling port, enter the following command:

```
hostname(config-pmap-p)# traffic-non-sip
```

- j. To identify the non-SIP URIs present in the Alert-Info and Call-Info header fields, enter the following command:

```
hostname(config-pmap-p)# uri-non-sip action {mask | log} [log]
```

---

The following example shows how to disable instant messaging over SIP:

```
hostname(config)# policy-map type inspect sip mymap
hostname(config-pmap)# parameters
hostname(config-pmap-p)# no im

hostname(config)# policy-map global_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect sip mymap

hostname(config)# service-policy global_policy global
```

## Configuring SIP Timeout Values

The media connections are torn down within two minutes after the connection becomes idle. This is, however, a configurable timeout and can be set for a shorter or longer period of time. To configure the timeout for the SIP control connection, enter the following command:

```
hostname(config)# timeout sip hh:mm:ss
```

This command configures the idle timeout after which a SIP control connection is closed.

To configure the timeout for the SIP media connection, enter the following command:

```
hostname(config)# timeout sip_media hh:mm:ss
```

This command configures the idle timeout after which a SIP media connection is closed.

## Verifying and Monitoring SIP Inspection

The **show sip** command assists in troubleshooting SIP inspection engine issues and is described with the **inspect protocol sip udp 5060** command. The **show timeout sip** command displays the timeout value of the designated protocol.

The **show sip** command displays information for SIP sessions established across the security appliance. Along with the **debug sip** and **show local-host** commands, this command is used for troubleshooting SIP inspection engine issues.

**Note**

We recommend that you configure the **pager** command before entering the **show sip** command. If there are a lot of SIP session records and the **pager** command is not configured, it takes a while for the **show sip** command output to reach its end.

The following is sample output from the **show sip** command:

```
hostname# show sip
Total: 2
call-id c3943000-960ca-2e43-228f@10.130.56.44
 state Call init, idle 0:00:01
call-id c3943000-860ca-7e1f-11f7@10.130.56.45
 state Active, idle 0:00:06
```

This sample shows two active SIP sessions on the security appliance (as shown in the Total field). Each call-id represents a call.

The first session, with the call-id c3943000-960ca-2e43-228f@10.130.56.44, is in the state Call Init, which means the session is still in call setup. Call setup is not complete until a final response to the call has been received. For instance, the caller has already sent the INVITE, and maybe received a 100 Response, but has not yet seen the 200 OK, so the call setup is not complete yet. Any non-1xx response message is considered a final response. This session has been idle for 1 second.

The second session is in the state Active, in which call setup is complete and the endpoints are exchanging media. This session has been idle for 6 seconds.

## Skinny (SCCP) Inspection

This section describes SCCP application inspection. This section includes the following topics:

- [SCCP Inspection Overview, page 25-74](#)
- [Supporting Cisco IP Phones, page 25-75](#)
- [Restrictions and Limitations, page 25-75](#)
- [Verifying and Monitoring SCCP Inspection, page 25-75](#)

## SCCP Inspection Overview

Skinny (SCCP) is a simplified protocol used in VoIP networks. Cisco IP Phones using 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. 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 supports PAT and NAT for SCCP. PAT is necessary if you have more IP phones than global IP addresses for the IP phones to use. By supporting NAT and PAT of SCCP Signaling packets, Skinny application inspection ensures that all SCCP signalling and media packets can traverse the security appliance.

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 it accomplishes by sending the location of a TFTP server to Cisco IP Phones and other

DHCP clients. Cisco IP Phones might also include DHCP option 3 in their requests, which sets the default route. For more information, see the [“Using Cisco IP Phones with a DHCP Server”](#) section on page 10-4.

## Supporting Cisco IP Phones

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 static identity 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 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 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 using NAT, an identity static entry maps to the same IP address. When using PAT, 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.

## Restrictions and Limitations

The following are limitations that apply to the current version of PAT and NAT support for SCCP:

- PAT does not work with configurations containing the **alias** command.
- Outside NAT or PAT is *not* supported.

If the address of an internal Cisco CallManager is configured for NAT or PAT to a different IP address or port, registrations for external Cisco IP Phones fail because the security appliance currently does not support NAT or PAT for the file content transferred over TFTP. Although the security appliance supports NAT of TFTP messages and opens a pinhole for the TFTP file, the security appliance cannot translate the Cisco CallManager IP address and port embedded in the Cisco IP Phone configuration files that are transferred by TFTP during phone registration.



### Note

The security appliance supports stateful failover of SCCP calls except for calls that are in the middle of call setup.

## Verifying and Monitoring SCCP Inspection

The **show skinny** command assists in troubleshooting SCCP (Skinny) inspection engine issues. The following is sample output from the **show skinny** command under the following conditions. There are two active Skinny sessions set up across the security appliance. The first one is established between an internal Cisco IP Phone at local address 10.0.0.11 and an external Cisco CallManager at 172.18.1.33. TCP port 2000 is the CallManager. The second one is established between another internal Cisco IP Phone at local address 10.0.0.22 and the same Cisco CallManager.

```
hostname# show skinny
```

|   | LOCAL                 | FOREIGN           | STATE |
|---|-----------------------|-------------------|-------|
| 1 | 10.0.0.11/52238       | 172.18.1.33/2000  | 1     |
|   | MEDIA 10.0.0.11/22948 | 172.18.1.22/20798 |       |
| 2 | 10.0.0.22/52232       | 172.18.1.33/2000  | 1     |
|   | MEDIA 10.0.0.22/20798 | 172.18.1.11/22948 |       |

The output indicates that a call has been established between two internal Cisco IP Phones. The RTP listening ports of the first and second phones are UDP 22948 and 20798 respectively.

The following is sample output from the **show xlate debug** command for these Skinny connections:

```
hostname# show xlate debug
2 in use, 2 most used
Flags: D - DNS, d - dump, I - identity, i - inside, n - no random,
 r - portmap, s - static
NAT from inside:10.0.0.11 to outside:172.18.1.11 flags si idle 0:00:16 timeout 0:05:00
NAT from inside:10.0.0.22 to outside:172.18.1.22 flags si idle 0:00:14 timeout 0:05:00
```

## Configuring a Skinny (SCCP) Inspection Policy Map for Additional Inspection Control

To specify actions when a message violates a parameter, create an SCCP inspection policy map. You can then apply the inspection policy map when you enable SCCP inspection according to the [“Configuring Application Inspection”](#) section on page 25-5.

To create an SCCP inspection policy map, perform the following steps:

**Step 1** (Optional) Add one or more regular expressions for use in traffic matching commands according to the [“Creating a Regular Expression”](#) section on page 21-12. See the types of text you can match in the **match** commands described in [Step 3](#).

**Step 2** (Optional) Create one or more regular expression class maps to group regular expressions according to the [“Creating a Regular Expression Class Map”](#) section on page 21-14.

**Step 3** Create an SCCP inspection policy map, enter the following command:

```
hostname(config)# policy-map type inspect skinny policy_map_name
hostname(config-pmap)#
```

Where the *policy\_map\_name* is the name of the policy map. The CLI enters policy-map configuration mode.

**Step 4** (Optional) To add a description to the policy map, enter the following command:

```
hostname(config-pmap)# description string
```

**Step 5** To apply actions to matching traffic, perform the following steps.

a. Specify the traffic on which you want to perform actions using one of the following methods:

- Specify the SCCP class map that you created in [Step 3](#) by entering the following command:

```
hostname(config-pmap)# class class_map_name
hostname(config-pmap-c)#
```

- Specify traffic directly in the policy map using one of the **match** commands described in [Step 3](#). If you use a **match not** command, then any traffic that does not match the criterion in the **match not** command has the action applied.

- b. Specify the action you want to perform on the matching traffic by entering the following command:

```
hostname(config-pmap-c)# {[drop [send-protocol-error] |
drop-connection [send-protocol-error] | mask | reset] [log] | rate-limit message_rate}
```

Not all options are available for each **match** or **class** command. See the CLI help or the *Cisco Security Appliance Command Reference* for the exact options available.

The **drop** keyword drops all packets that match.

The **send-protocol-error** keyword sends a protocol error message.

The **drop-connection** keyword drops the packet and closes the connection.

The **mask** keyword masks out the matching portion of the packet.

The **reset** keyword drops the packet, closes the connection, and sends a TCP reset to the server and/or client.

The **log** keyword, which you can use alone or with one of the other keywords, sends a system log message.

The **rate-limit message\_rate** argument limits the rate of messages.

- Step 6** You can specify multiple **class** or **match** commands in the policy map. For information about the order of **class** and **match** commands, see the “[Defining Actions in an Inspection Policy Map](#)” section on page 21-8. To configure parameters that affect the inspection engine, perform the following steps:

- a. To enter parameters configuration mode, enter the following command:

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

- b. To enforce registration before calls can be placed, enter the following command:

```
hostname(config-pmap-p)# enforce-registration
```

- c. To set the maximum SCCP station message ID allowed, enter the following command:

```
hostname(config-pmap-p)# message-ID max hex_value
```

Where the *hex\_value* argument is the station message ID in hex.

- d. To check RTP packets flowing on the pinholes for protocol conformance, enter the following command:

```
hostname(config-pmap-p)# rtp-conformance [enforce-payloadtype]
```

Where the **enforce-payloadtype** keyword enforces the payload type to be audio or video based on the signaling exchange.

- e. To set the maximum and minimum SCCP prefix length value allowed, enter the following command:

```
hostname(config-pmap-p)# sccp-prefix-len {max | min} value_length
```

Where the *value\_length* argument is a maximum or minimum value.

- f. To configure the timeout value for signaling and media connections, enter the following command:

```
hostname(config-pmap-p)# timeout
```

---

The following example shows how to define an SCCP inspection policy map.

```
hostname(config)# policy-map type inspect skinny skinny-map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# enforce-registration
```

```

hostname(config-pmap-p)# match message-id range 200 300
hostname(config-pmap-p)# drop log
hostname(config)# class-map inspection_default
hostname(config-cmap)# match default-inspection-traffic
hostname(config)# policy-map global_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect skinny skinny-map
hostname(config)# service-policy global_policy global

```

## SMTP and Extended SMTP Inspection

ESMTP application inspection provides improved protection against SMTP-based attacks by restricting the types of SMTP commands that can pass through the security appliance and by adding monitoring capabilities.

ESMTP is an enhancement to the SMTP protocol and is similar in most respects to SMTP. For convenience, the term SMTP is used in this document to refer to both SMTP and ESMTP. The application inspection process for extended SMTP is similar to SMTP application inspection and includes support for SMTP sessions. Most commands used in an extended SMTP session are the same as those used in an SMTP session but an ESMTP session is considerably faster and offers more options related to reliability and security, such as delivery status notification.

Extended SMTP application inspection adds support for eight extended SMTP commands, including AUTH, EHLO, ETRN, HELP, SAML, SEND, SOML and VRFY. Along with the support for seven RFC 821 commands (DATA, HELO, MAIL, NOOP, QUIT, RCPT, RSET), the security appliance supports a total of fifteen SMTP commands.

Other extended SMTP commands, such as ATRN, STARTLS, ONEX, VERB, CHUNKING, and private extensions are not supported. Unsupported commands are translated into Xs, which are rejected by the internal server. This results in a message such as “500 Command unknown: 'XXX'.” Incomplete commands are discarded.

The ESMTP inspection engine changes the characters in the server SMTP banner to asterisks except for the “2”, “0”, “O” characters. Carriage return (CR) and linefeed (LF) characters are ignored.

With SMTP inspection enabled, a Telnet session used for interactive SMTP may hang if the following rules are not observed: SMTP commands must be at least four characters in length; must be terminated with carriage return and line feed; and must wait for a response before issuing the next reply.

An SMTP server responds to client requests with numeric reply codes and optional human-readable strings. SMTP application inspection controls and reduces the commands that the user can use as well as the messages that the server returns. SMTP inspection performs three primary tasks:

- Restricts SMTP requests to seven basic SMTP commands and eight extended commands.
- Monitors the SMTP command-response sequence.
- Generates an audit trail—Audit record 108002 is generated when invalid character embedded in the mail address is replaced. For more information, see RFC 821.

SMTP inspection monitors the command and response sequence for the following anomalous signatures:

- Truncated commands.
- Incorrect command termination (not terminated with <CR><LR>).

- The MAIL and RCPT commands specify who are the sender and the receiver of the mail. Mail addresses are scanned for strange characters. The pipeline character (|) is deleted (changed to a blank space) and “<” ,”>” are only allowed if they are used to define a mail address (“>” must be preceded by “<”).
- Unexpected transition by the SMTP server.
- For unknown commands, the security appliance changes all the characters in the packet to X. In this case, the server generates an error code to the client. Because of the change in the packed, the TCP checksum has to be recalculated or adjusted.
- TCP stream editing.
- Command pipelining.

## SNMP Inspection

SNMP application inspection lets you restrict SNMP traffic to a specific version of SNMP. Earlier versions of SNMP are less secure; therefore, denying certain SNMP versions may be required by your security policy. The security appliance can deny SNMP versions 1, 2, 2c, or 3. You control the versions permitted by creating an SNMP map. You then apply the SNMP map when you enable SNMP inspection according to the [“Configuring Application Inspection” section on page 25-5](#).

To create an SNMP inspection policy map, perform the following steps:

---

**Step 1** To create an SNMP map, enter the following command:

```
hostname(config)# snmp-map map_name
hostname(config-snmp-map)#
```

where *map\_name* is the name of the SNMP map. The CLI enters SNMP map configuration mode.

**Step 2** To specify the versions of SNMP to deny, enter the following command for each version:

```
hostname(config-snmp-map)# deny version version
hostname(config-snmp-map)#
```

where *version* is 1, 2, 2c, or 3.

---

The following example denies SNMP Versions 1 and 2:

```
hostname(config)# snmp-map sample_map
hostname(config-snmp-map)# deny version 1
hostname(config-snmp-map)# deny version 2
```

## SQL\*Net Inspection

SQL\*Net inspection is enabled by default.

The SQL\*Net protocol consists of different packet types that the security appliance handles to make the data stream appear consistent to the Oracle applications on either side of the security appliance.

The default port assignment for SQL\*Net is 1521. This is the value used by Oracle for SQL\*Net, but this value does not agree with IANA port assignments for Structured Query Language (SQL). Use the **class-map** command to apply SQL\*Net inspection to a range of port numbers.

**Note**

Disable SQL\*Net inspection when SQL data transfer occurs on the same port as the SQL control TCP port 1521. The security appliance acts as a proxy when SQL\*Net inspection is enabled and reduces the client window size from 65000 to about 16000 causing data transfer issues.

The security appliance translates all addresses and looks in the packets for all embedded ports to open for SQL\*Net Version 1.

For SQL\*Net Version 2, all DATA or REDIRECT packets that immediately follow REDIRECT packets with a zero data length will be fixed up.

The packets that need fix-up contain embedded host/port addresses in the following format:

```
(ADDRESS=(PROTOCOL=tcp) (DEV=6) (HOST=a.b.c.d) (PORT=a))
```

SQL\*Net Version 2 TNSFrame types (Connect, Accept, Refuse, Resend, and Marker) will not be scanned for addresses to NAT nor will inspection open dynamic connections for any embedded ports in the packet.

SQL\*Net Version 2 TNSFrames, Redirect, and Data packets will be scanned for ports to open and addresses to NAT, if preceded by a REDIRECT TNSFrame type with a zero data length for the payload. When the Redirect message with data length zero passes through the security appliance, a flag will be set in the connection data Structure to expect the Data or Redirect message that follows to be translated and ports to be dynamically opened. If one of the TNS frames in the preceding paragraph arrive after the Redirect message, the flag will be reset.

The SQL\*Net inspection engine will recalculate the checksum, change IP, TCP lengths, and readjust Sequence Numbers and Acknowledgment Numbers using the delta of the length of the new and old message.

SQL\*Net Version 1 is assumed for all other cases. TNSFrame types (Connect, Accept, Refuse, Resend, Marker, Redirect, and Data) and all packets will be scanned for ports and addresses. Addresses will be translated and port connections will be opened.

## Sun RPC Inspection

This section describes Sun RPC application inspection. This section includes the following topics:

- [Sun RPC Inspection Overview, page 25-80](#)
- [Managing Sun RPC Services, page 25-81](#)
- [Verifying and Monitoring Sun RPC Inspection, page 25-81](#)

## Sun RPC Inspection Overview

The Sun RPC inspection engine enables or disables application inspection for the Sun RPC protocol. Sun RPC is used by NFS and NIS. Sun RPC services can run on any port. When a client attempts to access an Sun RPC service on a server, it must learn the port that service is running on. It does this by querying the port mapper process, usually rpcbnd, on the well-known port of 111.

The client sends the Sun RPC program number of the service and the port mapper process responds with the port number of the service. The client sends its Sun RPC queries to the server, specifying the port identified by the port mapper process. When the server replies, the security appliance intercepts this packet and opens both embryonic TCP and UDP connections on that port.

**Note**

NAT or PAT of Sun RPC payload information is not supported.

## Managing Sun RPC Services

Use the Sun RPC services table to control Sun RPC traffic through the security appliance based on established Sun RPC sessions. To create entries in the Sun RPC services table, use the **sunrpc-server** command in global configuration mode:

```
hostname(config)# sunrpc-server interface_name ip_address mask service service_type
protocol {tcp | udp} port[-port] timeout hh:mm:ss
```

You can use this command to specify the timeout after which the pinhole that was opened by Sun RPC application inspection will be closed. For example, to create a timeout of 30 minutes to the Sun RPC server with the IP address 192.168.100.2, enter the following command:

```
hostname(config)# sunrpc-server inside 192.168.100.2 255.255.255.255 service 100003
protocol tcp 111 timeout 00:30:00
```

This command specifies that the pinhole that was opened by Sun RPC application inspection will be closed after 30 minutes. In this example, the Sun RPC server is on the inside interface using TCP port 111. You can also specify UDP, a different port number, or a range of ports. To specify a range of ports, separate the starting and ending port numbers in the range with a hyphen (for example, 111-113).

The service type identifies the mapping between a specific service type and the port number used for the service. To determine the service type, which in this example is 100003, use the **sunrpcinfo** command at the UNIX or Linux command line on the Sun RPC server machine.

To clear the Sun RPC configuration, enter the following command.

```
hostname(config)# clear configure sunrpc-server
```

This removes the configuration performed using the **sunrpc-server** command. The **sunrpc-server** command allows pinholes to be created with a specified timeout.

To clear the active Sun RPC services, enter the following command:

```
hostname(config)# clear sunrpc-server active
```

This clears the pinholes that are opened by Sun RPC application inspection for specific services, such as NFS or NIS.

## Verifying and Monitoring Sun RPC Inspection

The sample output in this section is for a Sun RPC server with an IP address of 192.168.100.2 on the inside interface and a Sun RPC client with an IP address of 209.168.200.5 on the outside interface.

To view information about the current Sun RPC connections, enter the **show conn** command. The following is sample output from the **show conn** command:

```
hostname# show conn
15 in use, 21 most used
UDP out 209.165.200.5:800 in 192.168.100.2:2049 idle 0:00:04 flags -
UDP out 209.165.200.5:714 in 192.168.100.2:111 idle 0:00:04 flags -
UDP out 209.165.200.5:712 in 192.168.100.2:647 idle 0:00:05 flags -
UDP out 192.168.100.2:0 in 209.165.200.5:714 idle 0:00:05 flags i
hostname(config)#
```

To display the information about the Sun RPC service table configuration, enter the **show running-config sunrpc-server** command. The following is sample output from the **show running-config sunrpc-server** command:

```
hostname(config)# show running-config sunrpc-server
sunrpc-server inside 192.168.100.2 255.255.255.255 service 100003 protocol UDP port 111
timeout 0:30:00
sunrpc-server inside 192.168.100.2 255.255.255.255 service 100005 protocol UDP port 111
timeout 0:30:00
```

This output shows that a timeout interval of 30 minutes is configured on UDP port 111 for the Sun RPC server with the IP address 192.168.100.2 on the inside interface.

To display the pinholes open for Sun RPC services, enter the **show sunrpc-server active** command. The following is sample output from **show sunrpc-server active** command:

```
hostname# show sunrpc-server active
LOCAL FOREIGN SERVICE TIMEOUT

1 209.165.200.5/0 192.168.100.2/2049 100003 0:30:00
2 209.165.200.5/0 192.168.100.2/2049 100003 0:30:00
3 209.165.200.5/0 192.168.100.2/647 100005 0:30:00
4 209.165.200.5/0 192.168.100.2/650 100005 0:30:00
```

The entry in the LOCAL column shows the IP address of the client or server on the inside interface, while the value in the FOREIGN column shows the IP address of the client or server on the outside interface.

To view information about the Sun RPC services running on a Sun RPC server, enter the **rpcinfo -p** command from the Linux or UNIX server command line. The following is sample output from the **rpcinfo -p** command:

```
sunrpcserver:~ # rpcinfo -p
program vers proto port
100000 2 tcp 111 portmapper
100000 2 udp 111 portmapper
100024 1 udp 632 status
100024 1 tcp 635 status
100003 2 udp 2049 nfs
100003 3 udp 2049 nfs
100003 2 tcp 2049 nfs
100003 3 tcp 2049 nfs
100021 1 udp 32771 nlockmgr
100021 3 udp 32771 nlockmgr
100021 4 udp 32771 nlockmgr
100021 1 tcp 32852 nlockmgr
100021 3 tcp 32852 nlockmgr
100021 4 tcp 32852 nlockmgr
100005 1 udp 647 mountd
100005 1 tcp 650 mountd
100005 2 udp 647 mountd
100005 2 tcp 650 mountd
100005 3 udp 647 mountd
100005 3 tcp 650 mountd
```

In this output, port 647 corresponds to the mountd daemon running over UDP. The mountd process would more commonly be using port 32780. The mountd process running over TCP uses port 650 in this example.

## TFTP Inspection

TFTP inspection is enabled by default.

TFTP, described in RFC 1350, is a simple protocol to read and write files between a TFTP server and client.

The security appliance inspects TFTP traffic and dynamically creates connections and translations, if necessary, to permit file transfer between a TFTP client and server. Specifically, the inspection engine inspects TFTP read request (RRQ), write request (WRQ), and error notification (ERROR).

A dynamic secondary channel and a PAT translation, if necessary, are allocated on a reception of a valid read (RRQ) or write (WRQ) request. This secondary channel is subsequently used by TFTP for file transfer or error notification.

Only the TFTP server can initiate traffic over the secondary channel, and at most one incomplete secondary channel can exist between the TFTP client and server. An error notification from the server closes the secondary channel.

TFTP inspection must be enabled if static PAT is used to redirect TFTP traffic.

## XDMCP Inspection

XDMCP inspection is enabled by default; however, the XDMCP inspection engine is dependent upon proper configuration of the **established** command.

XDMCP is a protocol that uses UDP port 177 to negotiate X sessions, which use TCP when established.

For successful negotiation and start of an XWindows session, the security appliance must allow the TCP back connection from the Xhosted computer. To permit the back connection, use the **established** command on the security appliance. Once XDMCP negotiates the port to send the display, The **established** command is consulted to verify if this back connection should be permitted.

During the XWindows session, the manager talks to the display Xserver on the well-known port 6000 + *n*. Each display has a separate connection to the Xserver, as a result of the following terminal setting.

```
setenv DISPLAY Xserver:n
```

where *n* is the display number.

When XDMCP is used, the display is negotiated using IP addresses, which the security appliance can NAT if needed. XDCMP inspection does not support PAT.

