inspect ctiqbe through inspect xdmcp Commands

inspect ctiqbe

To enable CTIQBE protocol inspection, use the **inspect ctiqbe** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To disable inspection, use the **no** form of this command.

inspect ctiqbe

no inspect ctiqbe

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced and replaces the previously existing **fixup** command, which has been deprecated.

Usage Guidelines

The **inspect ctiqbe** command enables CTIQBE protocol inspection, which 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 ASA.

The Telephony Application Programming Interface (TAPI) and Java Telephony Application Programming Interface (JTAPI) are used by many Cisco VoIP applications. Computer Telephony Interface Quick Buffer Encoding (CTIQBE) is used by Cisco TAPI Service Provider (TSP) to communicate with Cisco CallManager.

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

- CTIQBE application inspection does not support configurations using the **alias** command.
- Stateful Failover of CTIQBE calls is *not* supported.
- Using 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 ASA, increase the timeout values in the Cisco TSP settings on the system running Cisco IP SoftPhone.
- CTIQBE application inspection does *not* support CTIQBE messages fragmented in multiple TCP packets.

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 ASA, calls between these two phones will fail.
- 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.

Inspecting Signaling Messages

For inspecting signaling messages, the **inspect ctiqbe** command often needs to determine locations of the media endpoints (for example, IP phones).

This information is used to prepare access control and NAT state for media traffic to traverse the firewall transparently without manual configuration.

In determining these locations, the **inspect ctiqbe** command does not use the tunnel default gateway route. A tunnel default gateway route is a route of the form **route** *interface* **0 0** *metric* **tunneled**. This route overrides the default route for packets that egress from IPsec tunnels. Therefore, if the **inspect ctiqbe** command is desired for VPN traffic, do not configure the tunnel default gateway route. Instead, use other static routing or dynamic routing.

Examples

The following example enables the CTIQBE inspection engine, which creates a class map to match CTIQBE traffic on the default port (2748). The service policy is then applied to the outside interface.

```
hostname(config)# class-map ctiqbe-port
hostname(config-cmap)# match port tcp eq 2748
hostname(config-cmap)# exit
hostname(config)# policy-map ctiqbe_policy
hostname(config-pmap)# class ctiqbe-port
hostname(config-pmap-c)# inspect ctiqbe
hostname(config-pmap-c)# exit
hostname(config)# service-policy ctiqbe_policy interface outside
```

To enable CTIQBE inspection for all interfaces, use the **global** parameter in place of **interface outside**.

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
show conn	Displays the connection state for different connection types.
show ctiqbe	Displays information regarding the CTIQBE sessions established across the ASA and the media connections allocated by the CTIQBE inspection engine.
timeout	Sets the maximum idle time duration for different protocols and session types.

inspect dcerpc

To enable inspection of DCERPC traffic destined for the endpoint-mapper, use the **inspect dcerpc** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect dcerpc [*map_name*]

no inspect dceprc [*map_name*]

Syntax Description

map_name	(Optional) The name of the DCERPC map.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

The **inspect dcerpc** command enables or disables application inspection for the DCERPC protocol.

Examples

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 dcerpc dcerpc_map

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

Related Commands

Commands	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.
timeout pinhole	Configures the timeout for DCERPC pinholes and overrides the global system pinhole timeout.

inspect dns

To enable DNS inspection (if it has been previously disabled) or to configure DNS inspection parameters, use the **inspect dns** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To disable DNS inspection, use the **no** form of this command.

inspect dns [*map_name*] [**dynamic-filter-snoop**]

no inspect dns [*map_name*] [**dynamic-filter-snoop**]

Syntax Description

dynamic-filter-snoop	(Optional) Enables DNS inspection with Botnet Traffic Filter snooping.
map_name	(Optional) Specifies the name of the DNS map.

Defaults

This command is enabled by default. Botnet Traffic Filter snooping is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced, replacing the **fixup** command, which has been deprecated.
7.2(1)	This command was modified to allow configuration of additional DNS inspection parameters.
8.2(1)	The **dynamic-filter-snoop** keyword was added.

Usage Guidelines

DNS guard tears down the DNS session associated with a DNS query as soon as the DNS reply is forwarded by the ASA. DNS guard 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 it is the default, the ASA 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, reverse lookups, which request the PTR record, are not affected by DNS rewrite.

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). Reassembly is performed as necessary to verify that the packet length is less than the maximum length configured. The packet is dropped if it exceeds the maximum length.
- 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 ASA within a limited period of time and there is no resource buildup. 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.

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.

As long as DNS inspection remains enabled, you can configure DNS rewrite using the **alias**, **static**, or **nat** commands. For details about the syntax and function of these commands, see the appropriate command page.

Botnet Traffic Filter Snooping and the DNS Reverse Lookup Cache

Botnet Traffic Filter snooping compares the domain name with those on the dynamic database or the static database, and adds the name and IP address to the Botnet Traffic Filter DNS reverse lookup cache. This cache is then used by the Botnet Traffic Filter when connections are made to the suspicious address.

We suggest that you enable Botnet Traffic Filter snooping only on interfaces where external DNS requests are going. Enabling Botnet Traffic Filter snooping on all UDP DNS traffic, including that going to an internal DNS server, creates unnecessary load on the ASA.

When you use the dynamic database with DNS snooping, entries are added to the DNS reverse lookup cache. If you use the static database, entries are added to the DNS host cache.

Entries in the DNS reverse lookup cache and the DNS host cache have a time-to-live (TTL) value provided by the DNS server. The largest TTL value allowed is 1 day (24 hours); if the DNS server provides a larger TTL, it is truncated to the 1-day maximum.

For the DNS reverse lookup cache, after an entry times out, the ASA renews the entry when an infected host initiates a connection to a known address, and DNS snooping occurs.

For the DNS host cache, after an entry times out, the ASA periodically requests a refresh for the entry.

For the DNS host cache, the maximum number of blacklist entries and whitelist entries is 1000 each.

Table 25-1 lists the maximum number of entries in the DNS reverse lookup cache per model.

Table 25-1 DNS Reverse Lookup Cache Entries Per Model

ASA Model	Maximum Entries
ASA 5505	5000
ASA 5510	10,000
ASA 5520	20,000
ASA 5540	40,000
ASA 5550	40,000
ASA 5580	100,000

Examples

The following example shows how to set the maximum DNS message length:

```
hostname(config)# policy-map type inspect dns dns-inspect
hostname(config-pmap)# parameters
hostname(config-pmap-p)# message-length maximum 1024
```

The following example creates a class map for all UDP DNS traffic, enables DNS inspection and Botnet Traffic Filter snooping with the default DNS inspection policy map, and applies it to the outside interface:

```
hostname(config)# class-map dynamic-filter_snoop_class
hostname(config-cmap)# match port udp eq domain
hostname(config-cmap)# policy-map dynamic-filter_snoop_policy
hostname(config-pmap)# class dynamic-filter_snoop_class
hostname(config-pmap-c)# inspect dns preset_dns_map dynamic-filter-snoop
hostname(config-pmap-c)# service-policy dynamic-filter_snoop_policy interface outside
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
debug dns	Enables debugging information for DNS.
dynamic-filter enable	Enables the Botnet Traffic Filter for a class of traffic or for all traffic if you do not specify an access list.
dynamic-filter updater-client enable	Enables downloading of the dynamic database.
dynamic-filter use-database	Enables use of the dynamic database.
dynamic-filter whitelist	Edits the Botnet Traffic Filter whitelist.
name	Adds a name to the blacklist or whitelist.

Commands	Description
policy-map	Associates a class map with specific security actions.
service-policy	Applies a policy map to one or more interfaces.

inspect esmtp

To enable SMTP application inspection or to change the ports to which the ASA listens, use the **inspect** e**smtp** command in class configuration mode. The class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect esmtp [*map_name*]

no inspect esmtp [*map_name*]

Syntax Description

map_name	(Optional) The name of the ESMTP map.

Defaults

This command is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced, replacing the **fixup** command, which has been deprecated.

Usage Guidelines

ESMTP application inspection provides improved protection against SMTP-based attacks by restricting the types of SMTP commands that can pass through the ASA 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.

The **inspect esmtp** command includes the functionality previously provided by the **fixup smtp** command, and provides additional support for some extended SMTP commands. Extended SMTP application inspection adds support for these extended SMTP commands, including AUTH, EHLO, ETRN, HELP, SAML, SEND, SOML, STARTLS, and VRFY. Along with the support for seven RFC 821 commands (DATA, HELO, MAIL, NOOP, QUIT, RCPT, RSET), the ASA supports a total of fifteen SMTP commands.

Other extended SMTP commands, such as ATRN, ONEX, VERB, CHUNKING, and private extensions and 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 **inspect esmtp** command changes the characters in the server SMTP banner to asterisks except for the "2", "0", "0" characters. Carriage return (CR) and linefeed (LF) characters are ignored.

With SMTP inspection enabled, a Telnet session used for interactive SMTP waits for a valid command and the firewall esmtp state machine keeps the correct states for the session 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 "<"). To close the session when the PIPE character is found as a parameter to a MAIL from or RCPT to command, include the **special-character** command in the configuration as part of the inspection parameters (**parameters** command).
- Unexpected transition by the SMTP server.
- For unknown commands, the ASA changes all the characters in the packet to X. In this case, the server will generate an error code to the client. Because of the change in the packet, the TCP checksum has to be recalculated or adjusted.
- TCP stream editing.
- Command pipelining.

To enable SMTP inspection for all interfaces, use the **global** parameter in place of **interface outside**.

Examples

The following example enables the SMTP inspection engine, which creates a class map to match SMTP traffic on the default port (25). The service policy is then applied to the outside interface.

```
hostname(config)# class-map smtp-port
hostname(config-cmap)# match port tcp eq 25
hostname(config-cmap)# exit
hostname(config)# policy-map smtp_policy
hostname(config-pmap)# class smtp-port
hostname(config-pmap-c)# inspect esmtp
hostname(config-pmap-c)# exit
hostname(config)# service-policy smtp_policy interface outside
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
debug esmtp	Enables debugging information for SMTP.
policy-map	Associates a class map with specific security actions.
service-policy	Applies a policy map to one or more interfaces.
show conn	Displays the connection state for different connection types, including SMTP.

inspect ftp

To configure the port for FTP inspection or to enable enhanced inspection, use the **inspect ftp** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect ftp [**strict** [*map_name*]]

no inspect ftp [**strict** [*map_name*]]

Syntax Description

map_name	The name of the FTP map.
strict	(Optional) Enables enhanced inspection of FTP traffic and forces compliance with RFC standards.

Caution Use caution when moving FTP to a higher port. For example, if you set the FTP port to 2021, all connections that initiate to port 2021 will have their data payload interpreted as FTP commands.

Defaults

The ASA listens to port 21 for FTP by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced, replacing the **fixup** command, which has been deprecated. The *map_name* option was added.

Usage Guidelines

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

- Prepares dynamic secondary data connections
- Tracks **ftp** command-response sequence
- Generates an audit trail
- NATs embedded IP addresses

Note Except for the banner, **inspect ftp** does not support FTP servers that segment FTP command or response.

FTP application inspection prepares secondary channels for FTP data transfer. The channels are allocated in response to a file upload, a file download, or a directory listing event and must be prenegotiated. The port is negotiated through the PORT or PASV commands.

Note Only specify the port for the FTP control connection and not the data connection. The ASA stateful inspection engine dynamically prepares the data connection as necessary.

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

The **strict** option prevents web browsers from sending embedded commands in FTP requests. Each **ftp** command must be acknowledged before a new command is allowed. Connections sending embedded commands are dropped. The **strict** option only lets an FTP server generate the 227 command and only lets an FTP client generate the PORT command. The 227 and PORT commands are checked to ensure they do not appear in an error string.

To enable strict FTP application inspection for all interfaces, use the **global** parameter in place of **interface** command.

Caution The use of the **strict** option may break FTP clients that do not comply with the RFC standards.

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.
- 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 ASA 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 FTP map configuration mode.

Note To identify specific FTP commands that are not permitted to pass through the ASA, identify an FTP map and use the **request-command deny** command. For details, see the **ftp-map** and the **request-command deny** command pages.

FTP Log Messages

FTP application inspection generates the following log messages:

- An Audit record 302002 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.

Examples

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-pmap-p)# exit
hostname(config-pmap)# exit
hostname(config)# class-map match-all ftp-traffic
hostname(config-cmap)# match port tcp eq ftp
hostname(config-cmap)# exit
hostname(config)# policy-map ftp-policy
hostname(config-pmap)# class ftp-traffic
hostname(config-pmap-c)# inspect ftp strict mymap
hostname(config-pmap-c)# exit
hostname(config-pmap)# exit
hostname(config)# service-policy ftp-policy interface inside
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
mask-syst-reply	Hides the FTP server response from clients.
policy-map	Associates a class map with specific security actions.
request-command deny	Specifies FTP commands to disallow.
service-policy	Applies a policy map to one or more interfaces.

inspect gtp

To enable or disable GTP inspection or to define a GTP map for controlling GTP traffic or tunnels, use the **inspect gtp** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. Use the **no** form of this command to remove the command.

inspect gtp [*map_name*]

no inspect gtp [*map_name*]

Note GTP inspection requires a special license. If you enter the **inspect gtp** command on an ASA without the required license, the ASA displays an error message.

Syntax Description

map_name	(Optional) Name for the GTP map.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

GTP is the tunnelling protocol for GPRS, and helps provide secure access over wireless networks. GPRS is a data network architecture that is designed to integrate with existing GSM networks. It offers mobile subscribers uninterrupted, packet-switched data services to corporate networks and the Internet. For an overview of GTP, see the the CLI configuration guide**.**

Use the **gtp-map** command to identify a specific map to use for defining the parameters for GTP. When you enter this command, the system enters a configuration mode that lets you enter the different commands used for defining the specific map. The actions that you can specify for messages that fail the criteria set using the different configuration commands include **drop** and **rate-limit**. In addition to these actions, you can specify to **log** the event or not.

After defining the GTP map, you use the **inspect gtp** command to enable the map. Then you use the **class-map**, **policy-map**, and **service-policy** commands to define a class of traffic, to apply the **inspect** command to the class, and to apply the policy to one or more interfaces.

The well-known ports for GTP are as follows:

- 3386
- 2123

The following features are not supported in 7.0(1):

- NAT, PAT, Outside NAT, alias, and Policy NAT
- Ports other than 3386, 2123, and 2152
- Validating the tunneled IP packet and its contents

Inspecting Signaling Messages

For inspecting signaling messages, the **inspect gtp** command often needs to determine locations of the media endpoints (for example, IP phones).

This information is used to prepare access control and NAT state for media traffic to traverse the firewall transparently without manual configuration.

In determining these locations, the **inspect gtp** command does **not** use the tunnel default gateway route. A tunnel default gateway route is a route of the form **route** *interface* **0 0** *metric* **tunneled**. This route overrides the default route for packets that egress from IPsec tunnels. Therefore, if the **inspect gtp** command is desired for VPN traffic, do not configure the tunnel default gateway route. Instead, use other static routing or dynamic routing.

Examples

The following example shows how to use access lists to identify GTP traffic, define a GTP map, define a policy, and apply the policy to the outside interface:

```
hostname(config)# access-list gtp-acl permit udp any any eq 3386
hostname(config)# access-list gtp-acl permit udp any any eq 2123
hostname(config)# class-map gtp-traffic
hostname(config)# match access-list gtp-acl
hostname(config)# gtp-map gtp-policy
hostname(config)# policy-map inspection_policy
hostname(config-pmap)# class gtp-traffic
hostname(config-pmap-c)# inspect gtp gtp-policy
hostname(config)# service-policy inspection_policy interface outside
```

Note This example enables GTP inspection with the default values. To change the default values, refer to the **gtp-map** command page and to the command pages for each command that is entered from GTP map configuration mode.

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
clear service-policy inspect gtp	Clears global GTP statistics.
debug gtp	Displays detailed information about GTP inspection.
service-policy	Applies a policy map to one or more interfaces.
show service-policy inspect gtp	Shows that status and statistics of the **inspect gtp** policy.

inspect h323

To enable H.323 application inspection or to change the ports to which the ASA listens, use the **inspect h323** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect h323 {**h225** | **ras**} [*map_name*]

no inspect h323 {**h225** | **ras**} [*map_name*]

Syntax Description

h225	Enables H.225 signalling inspection.
map_name	(Optional) The name of the H.323 map.
ras	Enables RAS inspection.

Defaults

The default port assignments are as follows:

- h323 h225 1720
- h323 ras 1718-1719

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced, replacing the **fixup** command, which has been deprecated.

Usage Guidelines

The **inspect h323** command 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 (ITU) for multimedia conferences over LANs. The ASA supports H.323 through Version 6, including the H.323 v3 feature Multiple Calls on One Call Signaling Channel.

With H.323 inspection enabled, the ASA 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 ASA.

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 ASA 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. FastStart 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. The H.245 connection is for call negotiation and media channel setup. 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 FastStart, the ASA dynamically allocates the H.245 connection based on the inspection of the H.225 messages.

Note The H.225 connection can also be dynamically allocated when using RAS.

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. Real-Time Transport Protocol (RTP) uses the negotiated port number, while RTP Control Protocol (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—UDP port used for gatekeeper discovery
- 1719—UDP port used for RAS and for gatekeeper discovery
- 1720—TCP Control Port

If the ACF message from the gatekeeper goes through the ASA, a pinhole will be opened for the H.225 connection. The H.245 signaling ports are negotiated between the endpoints in the H.225 signaling. When an H.323 gatekeeper is used, the ASA opens an H.225 connection based on inspection of the ACF message. If the ASA does not see the ACF message, you might need to open an access list for the well-known H.323 port 1720 for the H.225 call signaling.

The ASA dynamically allocates the H.245 channel after inspecting the H.225 messages and then hooks up to the H.245 channel to be fixed up as well. That means whatever H.245 messages pass through the ASA pass through the H.245 application inspection, NATing embedded IP addresses and opening the negotiated media channels.

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 the H.225/H.245 message, the ASA must remember the TPKT length to process/decode the messages properly. The ASA keeps a data structure for each connection and that data structure contains the TPKT length for the next expected message.

If the ASA needs to NAT any IP addresses, then it will have to change the checksum, the UUIE (user-user information element) length, and the TPKT, if included in the TCP packet with the H.225 message. If the TPKT is sent in a separate TCP packet, then the ASA will proxy ACK that TPKT and append a new TPKT to the H.245 message with the new length.

Note The ASA 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 will time out with the H.323 timeout as configured using the **timeout** command.

H.239 Support in H.245 Messages

The ASA sits between two H.323 endpoints. When the two H.323 endpoints set up a telepresentation session so that the endpoints can send and receive a data presentation, such as spreadsheet data, the ASA ensures successful H.239 negotiation between the endpoints.

H.239 is a standar that provides the ability for H.300 series endpoints can to open an additional video channel in a single call. In a call, an endpoint (such as a video phone), sends a channel for video and a channel for data presentation. The H.239 negotiation occurs on the H.245 channel.

The ASA opens a pinhole for the additional media channel. The endpoints use open logical channel message (OLC) to signal a new channel creation. The message extension is part of H.245 version 13.

The decoding and encoding of of the telepresentation session is enabled by default. H.239 encoding and decoding is preformed by ASN.1 coder.

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.
- It has been observed that 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 ASA.
- If you configure a network static where the network static is the same as a third-party netmask and address, then any outbound H.323 connection fails.
- To enable H.323 inspection for all interfaces, use the **global** parameter in place of **interface outside**.

Inspecting Signaling Messages

For inspecting signaling messages, the **inspect h323** command often needs to determine locations of the media endpoints (for example, IP phones).

This information is used to prepare access control and NAT state for media traffic to traverse the firewall transparently without manual configuration.

In determining these locations, the **inspect h323** command does **not** use the tunnel default gateway route. A tunnel default gateway route is a route of the form **route** *interface* **0 0** *metric* **tunneled**. This route overrides the default route for packets that egress from IPsec tunnels. Therefore, if the **inspect h323** command is desired for VPN traffic, do not configure the tunnel default gateway route. Instead, use other static routing or dynamic routing.

Examples

The following example enables the H.323 inspection engine, which creates a class map to match H.323 traffic on the default port (1720). The service policy is then applied to the outside interface.

```
hostname(config)# class-map h323-port
hostname(config-cmap)# match port tcp eq 1720
hostname(config-cmap)# exit
hostname(config)# policy-map h323_policy
hostname(config-pmap)# class h323-port
hostname(config-pmap-c)# inspect h323
hostname(config-pmap-c)# exit
hostname(config)# service-policy h323_policy interface outside
```

Related Commands

Commands	Description
debug h323	Enables the display of debugging information for H.323.
show h225	Displays information for H.225 sessions established across the ASA.
show h245	Displays information for H.245 sessions established across the ASA by endpoints using slow start.
show h323-ras	Displays information for H.323 RAS sessions established across the ASA.
timeout {**h225** | **h323**}	Configures idle time after which an H.225 signalling connection or an H.323 control connection will be closed.

inspect http

To enable HTTP application inspection or to change the ports to which the ASA listens, use the **inspect http command** in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect http [*map_name*]

no inspect http [*map_name*]

Syntax Description

map_name	(Optional) The name of the HTTP map.

Defaults

The default port for HTTP is 80.

Enhanced HTTP inspection is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced, replacing the **fixup** command, which has been deprecated.

Usage Guidelines

The **inspect http** command protects 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.

Enhanced HTTP inspection verifies that HTTP messages conform to RFC 2616, use RFC-defined methods or supported extension methods, and comply with various other criteria. In many cases, you can configure these criteria and the system response when the criteria are not met. The actions that you can specify for messages that fail the criteria set using the different configuration commands include **allow**, **reset**, or **drop**. In addition to these actions, you can specify to log the event or not.

The criteria that you can apply to HTTP messages include the following:

- Does not include any method on a configurable list.

- Specific transfer encoding method or application type.
- HTTP transaction adheres to RFC specification.
- Message body size is within configurable limits.
- Request and response message header size is within a configurable limit.
- URI length is within a configurable limit.
- The content type in the message body matches the header.
- The content type in the response message matches the *accept-type* field in the request message.
- The content type in the message is included in a predefined internal list.
- Message meets HTTP RFC format criteria.
- Presence or absence of selected supported applications.
- Presence or absence of selected encoding types.

Note The actions that you can specify for messages that fail the criteria set using the different configuration commands include **allow**, **reset**, or **drop**. In addition to these actions, you can specify to log the event or not.

To enable enhanced HTTP inspection, enter the **inspect http** *http-map* command. The rules that this applies to HTTP traffic are defined by the specific HTTP map, which you configure by entering the **http-map** command and HTTP map configuration mode commands.

Note When you enable HTTP inspection with an HTTP 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 HTTP map remains enabled.

Examples

The following example shows how to identify HTTP traffic, define an HTTP map, define a policy, and apply the policy to the outside interface:

```
hostname(config)# class-map http-port
hostname(config-cmap)# match port tcp eq 80
hostname(config-cmap)# exit
hostname(config)# http-map inbound_http
hostname(config-http-map)# content-length min 100 max 2000 action reset log
hostname(config-http-map)# content-type-verification match-req-rsp reset log
hostname(config-http-map)# max-header-length request bytes 100 action log reset
hostname(config-http-map)# max-uri-length 100 action reset log
hostname(config-http-map)# exit
hostname(config)# policy-map inbound_policy
hostname(config-pmap)# class http-port
hostname(config-pmap-c)# inspect http inbound_http
hostname(config-pmap-c)# exit
hostname(config-pmap)# exit
hostname(config)# service-policy inbound_policy interface outside
```

The following example causes the ASA to reset the connection and create a syslog entry when it detects any traffic that contains the following:

- Messages less than 100 bytes or exceeding 2000 bytes

- Unsupported content types
- HTTP headers exceeding 100 bytes
- URIs exceeding 100 bytes

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
debug appfw	Displays detailed information about HTTP application inspection.
debug http-map	Displays detailed information about traffic associated with an HTTP map.
http-map	Defines an HTTP map for configuring enhanced HTTP inspection.
policy-map	Associates a class map with specific security actions.

inspect icmp

To configure the ICMP inspection engine, use the **inspect icmp** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect icmp

no inspect icmp

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced, replacing the **fixup** command, which has been deprecated.

Usage Guidelines

The ICMP inspection engine allows ICMP traffic to be inspected like TCP and UDP traffic. Without the ICMP inspection engine, we recommend that you do not allow ICMP through the ASA in an ACL. 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

When ICMP inspection is disabled, which is the default configuration, ICMP echo reply messages are denied from a lower security interface to a higher security interface, even if it is in response to an ICMP echo request.

To enable ICMP inspection for all interfaces, use the **global** parameter in place of **interface outside**.

Examples

You enable the ICMP application inspection engine as shown in the following example, which creates a class map to match ICMP traffic using the ICMP protocol ID, which is 1 for IPv4 and 58 for IPv6. The service policy is then applied to the outside interface.

```
hostname(config)# class-map icmp-class
hostname(config-cmap)# match default-inspection-traffic
hostname(config-cmap)# exit
hostname(config)# policy-map icmp_policy
hostname(config-pmap)# class icmp-class
hostname(config-pmap-c)# inspect icmp
hostname(config-pmap-c)# exit
hostname(config)# service-policy icmp_policy interface outside
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
icmp	Configures access rules for ICMP traffic that terminates at an ASA interface.
policy-map	Defines a policy that associates security actions with one or more traffic classes.
service-policy	Applies a policy map to one or more interfaces.

inspect icmp error

To enable application inspection for ICMP error messages, use the **inspect icmp error** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect icmp error

no inspect icmp error

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced, replacing the **fixup** command, which has been deprecated.

Usage Guidelines

Use the **inspect icmp error** command to create xlates for intermediate hops that send ICMP error messages, based on the static/NAT configuration. By default, the ASA hides the IP addresses of intermediate hops. However, using the **inspect icmp error** command makes the intermediate hop IP addresses visible. The ASA overwrites the packet with the translated IP addresses.

Cisco ASA 5500 Series software uses the egress interface address as the source address when generating ICMP error messages for path MTU discovery or hop-by-hop discovery. If you enable application inspection for ICMP error messages using the **inspect icmp error** command, NAT is also independently applied to this source address.

When enabled, the ICMP error inspection engine makes the following changes to the ICMP packet:

- In the IP Header, the NAT IP is changed to the Client IP (Destination Address and Intermediate Hop 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 NAT IP is changed to the Client IP
  - Original packet NAT port is changed to the Client Port
  - Original packet IP checksum is recalculated

When an ICMP error message is retrieved, whether ICMP error inspection is enabled or not, the ICMP payload is scanned to retrieve the five-tuple (src ip , dest ip, src port, dest port, and ip protocol) from the original packet. A lookup is performed, using the retrieved five-tuple, to determine the original address of the client and to locate an existing session associated with the specific five-tuple. If the session is not found, the ICMP error message is dropped.

To enable ICMP error inspection for all interfaces, use the **global** parameter in place of **interface outside**.

Examples

The following example enables the ICMP error application inspection engine, which creates a class map to match ICMP traffic using the ICMP protocol ID, which is 1 for IPv4 and 58 for IPv6. The service policy is then applied to the outside interface.

```
hostname(config)# class-map icmp-class
hostname(config-cmap)# match default-inspection-traffic
hostname(config-cmap)# exit
hostname(config)# policy-map icmp_policy
hostname(config-pmap)# class icmp-class
hostname(config-pmap-c)# inspect icmp error
hostname(config-pmap-c)# exit
hostname(config)# service-policy icmp_policy interface outside
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
icmp	Configures access rules for ICMP traffic that terminates at an ASA interface.
inspect icmp	Enables or disables the ICMP inspection engine.
policy-map	Defines a policy that associates security actions with one or more traffic classes.
service-policy	Applies a policy map to one or more interfaces.

inspect ils

To enable ILS application inspection, use the **inspect ils command** in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect ils

no inspect ils

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced, replacing the **fixup** command, which has been deprecated.

Usage Guidelines

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

The ASA 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 ASA 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 H.225 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.

To enable ILS inspection for all interfaces, use the **global** parameter in place of **interface outside**.

Examples

You enable the ILS inspection engine as shown in the following example, which creates a class map to match ILS traffic on the default port (389). The service policy is then applied to the outside interface.

```
hostname(config)# class-map ils-port
hostname(config-cmap)# match port tcp eq 389
hostname(config-cmap)# exit
hostname(config)# policy-map ils_policy
hostname(config-pmap)# class ils-port
hostname(config-pmap-c)# inspect ils
hostname(config-pmap-c)# exit
hostname(config)# service-policy ils_policy interface outside
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
debug ils	Enables debugging information for ILS.
policy-map	Associates a class map with specific security actions.
service-policy	Applies a policy map to one or more interfaces.

inspect im

To enable inspection of IM traffic, use the **inspect im** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect im *map_name*

no inspect im *map_name*

Syntax Description

map_name	The name of the IM map.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

The **inspect im** command enables or disables application inspection for the IM protocol.

Examples

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

```
hostname(config)# regex loginname1 "user1\@example.com"
hostname(config)# regex loginname2 "user2\@example.com"
hostname(config)# regex loginname3 "user3\@example.com"
hostname(config)# regex loginname4 "user4\@example.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-any yahoo_src_login_name_regex
hostname(config-cmap)# match regex loginname1
hostname(config-cmap)# match regex loginname2

hostname(config)# class-map type regex match-any 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-any 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
```

Related Commands

Commands	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.
match protocol	Matches a specific IM protocol in an inspection class or policy map.

inspect ip-options

To enable inspection of IP options in a packet, use the **inspect ip-options** command in class or policy map type inspect configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect ip-options *map_name*

no inspect ip-options *map_name*

Syntax Description

map_name	The name of the IP Options map.

Defaults

This command is enabled by default the global policy.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Policy or class map configuration	•	•	•	•	—

Command History

Release	Modification
8.2(2)	This command was introduced.

Usage Guidelines

In a packet, the IP header contains the Options field. The Options field, commonly referred to as IP Options, provide for control functions that are required in some situations but unnecessary for most common communications. In particular, IP Options include provisions for time stamps, security, and special routing. Use of IP Options is optional and the field can contain zero, one, or more options.

You can configure IP Options inspection to control which IP packets with specific IP options are allowed through the ASA. Configuring this inspection instructs the ASA to allow a packet to pass or to clear the specified IP options and then allow the packet to pass.

IP Options inspection can check for the following three IP options in a packet:

- End of Options List (EOOL) or IP Option 0—This option, which contains just a single zero byte, appears at the end of all options to mark the end of a list of options. This might not coincide with the end of the header according to the header length.
- No Operation (NOP) or IP Option 1—The Options field in the IP header can contain zero, one, or more options, which makes the total length of the field variable. However, the IP header must be a multiple of 32 bits. If the number of bits of all options is not a multiple of 32 bits, the NOP option is used as “internal padding” to align the options on a 32-bit boundary.

- Router Alert (RTRALT) or IP Option 20—This option notifies transit routers to inspect the contents of the packet even when the packet is not destined for that router. This inspection is valuable when implementing RSVP and similar protocols require relatively complex processing from the routers along the packets delivery path.

You configure inspection of these three IP options by using the **parameter** command in the policy-map type inspect configuration mode. For details about the syntax of these commands, see the **eool**, **nop**, and **router-alert** command pages.

Note IP Options inspection is included by default in the global inspection policy. Therefore, the ASA allows RSVP traffic that contains packets with the Router Alert option (option 20) when the ASA is in routed mode.

Dropping RSVP packets containing the Router Alert option can cause problems in VoIP implementations.

When you configure ASA to clear the Router Alert option from IP headers, the IP header changes in the following ways:

- The Options field is padded so that the field ends on a 32 bit boundary.
- Internet header length (IHL) changes.
- The total length of the packet changes.
- The checksum is recomputed.

If an IP header contains additional options other than EOOL, NOP, or RTRALT, regardless of whether the ASA is configured to allow these options, the ASA will drop the packet.

Examples

The following example shows how to define an IP Options inspection policy map that allows the ASA to pass packets that contain the EOOL, NOP, and RTRALT options in the packet header.

```
hostname(config)# policy-map type inspect ip-options ip-options-map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# eool action allow
hostname(config-pmap-p)# nop action allow
hostname(config-pmap-p)# router-alert action allow
```

Entering the **clear** command clears the IP option from the packet before allowing the packet through the ASA.

Related Commands

Commands	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.

inspect ipsec-pass-thru

To enable IPsec pass-through inspection, use the **inspect ipsec-pass-thru** command in class map configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect ipsec-pass-thru [*map_name*]

no inspect ipsec-pass-thru [*map_name*]

Syntax Description

map_name	(Optional) The name of the IPsec pass-through map.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **inspect ipsec-pass-thru** command enables or disables application inspection. IPsec pass-through application inspection provides convenient traversal of ESP (IP protocol 50) and/or AH (IP protocol 51) traffic associated with an IKE UDP port 500 connection. It avoids lengthy access list configuration to permit ESP and AH traffic and also provides security using timeout and maximum connections.

Use the IPsec pass-through parameter map to identify a specific map to use for defining the parameters for the inspection. Use the **policy-map type inspect** command to access the parameters configuration, which lets you specify the restrictions for ESP or AH traffic. You can set the per-client maximum connections and the idle timeout in parameters configuration mode.

Use the **class-map**, **policy-map**, and **service-policy** commands to define a class of traffic, to apply the **inspect** command to the class, and to apply the policy to one or more interfaces. The parameter map defined is enabled when used with the **inspect ipsec-pass-thru** command.

NAT and non-NAT traffic is permitted. However, PAT is not supported.

Note In ASA 7.0(1), the **inspect ipsec-pass-thru** command allowed only ESP traffic to pass through. To retain the same behavior in later versions, a default map that permits ESP is created and attached if the **inspect ipsec-pass-thru** command is specified without any arguments. This map can be seen in the output of the **show running-config all** command.

Examples

The following example shows how to use access lists to identify IKE traffic, define an IPsec pass-through parameter map, define a policy, and apply the policy to the outside interface:

```
hostname(config)# access-list ipsecpassthruacl permit udp any any eq 500
hostname(config)# class-map ipsecpassthru-traffic
hostname(config-cmap)# match access-list ipsecpassthruacl
hostname(config)# policy-map type inspect ipsec-pass-thru iptmap
hostname(config-pmap)# parameters
hostname(config-pmap-p)# esp per-client-max 10 timeout 0:11:00
hostname(config-pmap-p)# ah per-client-max 5 timeout 0:06:00
hostname(config)# policy-map inspection_policy
hostname(config-pmap)# class ipsecpassthru-traffic
hostname(config-pmap-c)# inspect ipsec-pass-thru iptmap
hostname(config)# service-policy inspection_policy interface outside
```

Related Commands

Commands	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.
match protocol	Matches a specific IM protocol in an inspection class or policy map.

inspect ipv6

To enable IPv6 inspection, use the **inspect ipv6** command in class configuration mode. Class configuration mode is accessible from policy-map configuration mode. To remove the configuration, use the **no** form of this command.

inspect ipv6 [*map_name*]

no inspect ipv6 [*map_name*]

Syntax Description

map_name	The name of the IPv6 inspection policy map.

Defaults

IPv6 inspection is disabled by default. If you enable IPv6 inspection and do not specify an inspection policy map, then the default IPv6 inspection policy map is used, and the following actions are taken:

- Allows only known IPv6 extension headers
- Enforces the order of IPv6 extension headers as defined in the RFC 2460 specification

If you create an inspection policy map, the above actions are taken by default unless you explicitly disable them.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
8.2(1)	This command was introduced.

Usage Guidelines

IPv6 inspection lets you selectively log or drop IPv6 traffic based on the extension header. In addition, IPv6 inspection can check conformance to RFC 2460 for type and order of extension headers in IPv6 packets.

Examples

The following example drops all IPv6 traffic with the hop-by-hop, destination-option, routing-address, and routing type 0 headers:

```
policy-map type inspect ipv6 ipv6-pm
 parameters
 match header hop-by-hop
  drop
 match header destination-option
  drop
 match header routing-address count gt 0
  drop
 match header routing-type eq 0
  drop
policy-map global_policy
 class class-default
  inspect ipv6 ipv6-pm
!
service-policy global_policy global
```

Related Commands

Commands	Description
class	Identifies a class map name in the policy map.
match header	Matches IPv6 headers in an IPv6 inspection policy map.
policy-map type inspect ipv6	Creates an inspection class map to match traffic specific to IPv6.
policy-map	Creates a Layer 3/4 policy map.
verify-header	Configures IPv6 inspection parameters.

inspect mgcp

To enable MGCP application inspection or to change the ports to which the ASA listens, use the **inspect mgcp** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect mgcp [*map_name*]

no inspect mgcp [*map_name*]

Syntax Description

map_name	(Optional) The name of the MGCP map.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced, replacing the **fixup** command, which has been deprecated.

Usage Guidelines

To use MGCP, you usually need to configure at least two **inspect** commands: one for the port on which the gateway receives commands, and one for the port on which the Call Agent receives commands. Normally, a Call Agent sends commands to the default MGCP port for gateways, 2427, and a gateway sends commands to the default MGCP port for Call Agents, 2727.

MGCP is used for controlling 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, and 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.

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.

Note MGCP call agents send AUEP messages to determine if MGCP end points are present. This establishes a flow through the ASA and allows MGCP end points to register with the call agent.

Use the **call-agent** and **gateway** commands in MGCP map configuration mode to configure the IP addresses of one or more call agents and gateways. Use the **command-queue** command in MGCP map configuration mode to specify the maximum number of MGCP commands that will be allowed in the command queue at one time.

Inspecting Signaling Messages

For inspecting signaling messages, the **inspect mgcp** command often needs to determine locations of the media endpoints (for example, IP phones).

This information is used to prepare access-control and NAT state for media traffic to traverse the firewall transparently without manual configuration.

In determining these locations, the **inspect mgcp** command does **not** use the tunnel default gateway route. A tunnel default gateway route is a route of the form **route** *interface* **0 0** *metric* **tunneled**. This route overrides the default route for packets that egress from IPsec tunnels. Therefore, if the **inspect mgcp** command is desired for VPN traffic, do not configure the tunnel default gateway route. Instead, use other static routing or dynamic routing.

To enable MGCP inspection for all interfaces, use the **global** parameter in place of **interface outside**.

The maximum number of MGCP commands that can be queued is 150.

Examples

The following example shows how to identify MGCP traffic, define a MGCP map, define a policy, and apply the policy to the outside interface. This creates a class map to match MGCP traffic on the default ports (2427 and 2727). The service policy is then applied to the outside interface. This configuration allows call agents 10.10.11.5 and 10.10.11.6 to control gateway 10.10.10.115, and allows call agents 10.10.11.7 and 10.10.11.8 to control both gateways 10.10.10.116 and 10.10.10.117.

```
hostname(config)# access-list mgcp_acl permit tcp any any eq 2427
hostname(config)# access-list mgcp_acl permit tcp any any eq 2727
hostname(config)# class-map mgcp_port
hostname(config-cmap)# match access-list mgcp_acl
hostname(config-cmap)# exit
hostname(config)# mgcp-map inbound_mgcp
hostname(config-mgcp-map)# call-agent 10.10.11.5 101
hostname(config-mgcp-map)# call-agent 10.10.11.6 101
hostname(config-mgcp-map)# call-agent 10.10.11.7 102
hostname(config-mgcp-map)# call-agent 10.10.11.8 102
hostname(config-mgcp-map)# gateway 10.10.10.115 101
hostname(config-mgcp-map)# gateway 10.10.10.116 102
hostname(config-mgcp-map)# gateway 10.10.10.117 102
hostname(config-mgcp-map)# command-queue 150
hostname(config-mgcp-map)# exit
hostname(config)# policy-map inbound_policy
hostname(config-pmap)# class mgcp_port
hostname(config-pmap-c)# inspect mgcp mgcp-map inbound_mgcp
hostname(config-pmap-c)# exit
hostname(config)# service-policy inbound_policy interface outside
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
debug mgcp	Enables MGCP debugging information.
mgcp-map	Defines an MGCP map and enables mgcp map configuration mode.
show mgcp	Displays information about MGCP sessions established through the ASA.
timeout	Sets the maximum idle time duration for different protocols and session types.

inspect mmp

To configure the MMP inspection engine, use the **inspect mmp** command in class configuration mode. To remove MMP inspection, use the **no** form of this command.

inspect mmp tls-proxy [*name*]

no inspect mmp tls-proxy [*name*]

Syntax Description

name	Species the TLS proxy instance name.
tls-proxy	Enables the TLS proxy for MMP inspection. The MMP protocol can additionally use the TCP transport; however, the CUMA client only supports the TLS transport. Therefore, the **tls-proxy** keyword is required to enable MMP inspection.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		**Security Context**		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Class configuration	•	•	•	•	—

Command History

Release	**Modification**
8.0(4)	The command was introduced.

Usage Guidelines

The ASA includes an inspection engine to validate the CUMA Mobile Multiplexing Protocol (MMP). MMP is a data transport protocol for transmitting data entities between CUMA clients and servers. Use the **inspect mmp** command when the ASA is deployed between CUMA clients and servers and inspection of MMP packets is required.

MMP inspection must be enabled with the TLS proxy because MMP traffic is transported only over a TLS connection.

Note While configuring the MMP inspection engine, please note that it can only be added under a non-deafult inspection class. If you attempt to add the inspect mmp <tls-proxy> command under the default inspection class, it will generate an error.

Examples

The following example shows the use of the **inspect mmp** command to inspect MMP traffic:

```
hostname(config)# class-map mmp
hostname(config-cmap)# match port tcp eq 5443
hostname(config-cmap)# exit
hostname(config)# policy-map mmp-policy
hostname(config-pmap)# class mmp
hostname(config-pmap-c)# inspect mmp tls-proxy myproxy
hostname(config-pmap-c)# exit
hostname(config-pmap)# exit
hostname(config)# service-policy mmp-policy interface outside
```

Related Commands

Command	Description
tls-proxy	Configures the TLS proxy instance.
debug mmp	Displays inspect MMP events.

inspect netbios

To enable NetBIOS application inspection or to change the ports to which the ASA listens, use the **inspect netbios command** in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect netbios [*map_name*]

no inspect netbios [*map_name*]

Syntax Description

map_name	(Optional) The name of the NetBIOS map.

Defaults

This command is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced, replacing the **fixup** command, which has been deprecated.

Usage Guidelines

The **inspect netbios** command enables or disables application inspection for the NetBIOS protocol.

Examples

The following example shows how to define a NetBIOS inspection policy map:

```
hostname(config)# policy-map type inspect netbios netbios_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# protocol-violation drop
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
policy-map	Associates a class map with specific security actions.
service-policy	Applies a policy map to one or more interfaces.

inspect pptp

To enable PPTP application inspection or to change the ports to which the ASA listens, use the **inspect pptp** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect pptp

no inspect pptp

Syntax Description

This command has no arguments or keywords.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced, replacing the **fixup** command, which has been deprecated.

Usage Guidelines

The Point-to-Point Tunneling Protocol (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 ASA 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.

To enable PPTP inspection for all interfaces, use the **global** parameter in place of **interface outside**.

Examples

You enable the PPTP inspection engine as shown in the following example, which creates a class map to match PPTP traffic on the default port (1723). The service policy is then applied to the outside interface.

```
hostname(config)# class-map pptp-port
hostname(config-cmap)# match port tcp eq 1723
hostname(config-cmap)# exit
hostname(config)# policy-map pptp_policy
hostname(config-pmap)# class pptp-port
hostname(config-pmap-c)# inspect pptp
hostname(config-pmap-c)# exit
hostname(config)# service-policy pptp_policy interface outside
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
debug pptp	Enables debugging information for PPTP.
policy-map	Associates a class map with specific security actions.
service-policy	Applies a policy map to one or more interfaces.

inspect radius-accouting

To enable or disable RADIUS accounting inspection or to define a map for controlling traffic or tunnels, use the **inspect radius-accounting** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect radius-accounting [*map_name*]

no inspect radius-accounting [*map_name*]

Syntax Description

map_name	(Optional) Name for the RADIUS accounting map.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

Use the **radius-accounting** command to create a specific map to use for defining the parameters for RADIUS accounting. When you enter this command, the system enters a configuration mode that lets you enter the different commands used for defining the specific map. The actions that you can specify for messages that fail the criteria set using the different configuration commands include **send**, **host**, **validate-attribute**, **enable gprs**, and **timeout users**. You can access these commands from **parameter** mode.

After defining the RADIUS accounting map, you use the **inspect gtp** command to enable the map. Then you use the **class-map**, **policy-map**, and **service-policy** commands to define a class of traffic, to apply the **inspect** command to the class, and to apply the policy to one or more interfaces.

Note The **inspect radius-accounting** command can only be used with the **class-map type management** command.

Examples

The following example shows how to use access lists to identify RADIUS accounting traffic, define a RADIUS accounting map, define a policy, and apply the policy to the outside interface:

```
hostname(config)# policy-map type inspect radius-accountin ra
```

Note This example enables RADIUS accounting inspection with the default values. To change the default values, see the **parameters** command and each command that is entered from RADIUS accounting configuration mode.

Related Commands

Commands	Description
parameters	Defines the traffic class to which to apply security actions.
class-map type management	Lets you identify Layer 3 or 4 management traffic destined for the ASA to which you want to apply actions.
show and **clear service-policy**	Lets you view and clear service policy settings.
debug inspect radius-accounting	Lets you debug RADIUS accounting inspection.
service-policy	Applies a policy map to one or more interfaces.

inspect rsh

To enable RSH application inspection or to change the ports to which the ASA listens, use the **inspect rsh** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect rsh

no inspect rsh

Syntax Description

This command has no arguments or keywords.

Defaults

This command is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced, replacing the **fixup** command, which has been deprecated.

Usage Guidelines

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.

To enable RSH inspection for all interfaces, use the **global** parameter in place of **interface outside**.

Examples

The following example enables the RSH inspection engine, which creates a class map to match RSH traffic on the default port (514). The service policy is then applied to the outside interface.

```
hostname(config)# class-map rsh-port
hostname(config-cmap)# match port tcp eq 514
hostname(config-cmap)# exit
hostname(config)# policy-map rsh_policy
hostname(config-pmap)# class rsh-port
hostname(config-pmap-c)# inspect rsh
hostname(config-pmap-c)# exit
hostname(config)# service-policy rsh_policy interface outside
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
policy-map	Associates a class map with specific security actions.
service-policy	Applies a policy map to one or more interfaces.

inspect rtsp

To enable RTSP application inspection or to change the ports to which the ASA listens, use the **inspect rtsp** command in class configuration mode. Class configuration mode is accessible from policy-map configuration mode. To remove the configuration, use the **no** form of this command.

inspect rtsp [*map_name*]

no inspect rtsp [*map_name*]

Syntax Description

map_name	(Optional) The name of the RTSP map.

Defaults

This command is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced, replacing the **fixup** command, which has been deprecated.

Usage Guidelines

The **inspect rtsp** command lets the ASA 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 ASA only supports TCP, in conformity with RFC 2326. This TCP control channel is used to negotiate the data channels that will be 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 ASA parses setup response messages with a status code of 200. If the response message is traveling inbound, the server is outside relative to the ASA and dynamic channels need to be opened for connections coming inbound from the server. If the response message is outbound, then the ASA 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 ASA will need to keep state and remember 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.

Using RealPlayer

When using RealPlayer, it is important to properly configure transport mode. For the ASA, add an **access-list** command statement from the server to the client or vice versa. For RealPlayer, change transport mode by choosing **Options** > **Preferences** > **Transport** > **RTSP Settings**.

If using TCP mode on the RealPlayer, check the **Use TCP to Connect to Server** and **Attempt to use TCP for all content** check boxes. On the ASA, there is no need to configure the inspection engine.

If using UDP mode on the RealPlayer, check 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 ASA, add a **inspect rtsp** *port* command statement.

Restrictions and Limitations

The following restrictions apply to the **inspect rtsp** command:

- The ASA does not support multicast RTSP or RTSP messages over UDP.
- The ASA does not have the ability to recognize HTTP cloaking where RTSP messages are hidden in the HTTP messages.
- The ASA 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 the ASA cannot perform NAT on fragmented packets.
- With Cisco IP/TV, the number of NATs the ASA 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.
- Media streams delivered over HTTP are not supported by RTSP application inspection. This is because RTSP inspection does not support HTTP cloaking (RTSP wrapped in HTTP).
- To enable RTSP inspection for all interfaces, use the **global** parameter in place of **interface outside**.

Examples

The following example enables the RTSP inspection engine, which creates a class map to match RTSP traffic on the default ports (554 and 8554). The service policy is then applied to the outside interface.

```
hostname(config)# access-list rtsp-acl permit tcp any any eq 554
hostname(config)# access-list rtsp-acl permit tcp any any eq 8554
hostname(config)# class-map rtsp-traffic
hostname(config-cmap)# match access-list rtsp-acl
hostname(config-cmap)# exit
hostname(config)# policy-map rtsp_policy
hostname(config-pmap)# class rtsp-traffic
hostname(config-pmap-c)# inspect rtsp
hostname(config-pmap-c)# exit
hostname(config)# service-policy rtsp_policy interface outside
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
debug rtsp	Enables debugging information for RTSP.
policy-map	Associates a class map with specific security actions.
service-policy	Applies a policy map to one or more interfaces.

inspect scansafe

To enables Cloud Web Security inspection on the traffic in a class, use the **inspect scansafe** command in class configuration mode. You can access the class configuration mode by first entering the **policy-map** command. To remove the inspect action, use the **no** form of this command.

inspect scansafe *scansafe_policy_name* [**fail-open** | **fail-close**]

no inspect scansafe *scansafe_policy_name* [**fail-open** | **fail-close**]

Syntax Description

scansafe_policy_name	Specifies the inspection class map name defined by the **policy-map type inspect scansafe** command.
fail-open	(Optional) Allows traffic to pass through the ASA if the Cloud Web Security servers are unavailable.
fail-close	(Optional) Drops all traffic if the Cloud Web Security servers are unavailable. **fail-close** is the default.

Command Default

fail-close is the default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
9.0(1)	We introduced this command.

Usage Guidelines

Cisco Cloud Web Security provides web security and web filtering services through the Software-as-a-Service (SaaS) model. Enterprises with the ASA in their network can use Cloud Web Security services without having to install additional hardware.

Note This feature is also called "ScanSafe," so the ScanSafe name appears in some commands.

Configure this command using Modular Policy Framework:

1. Create inspection policy maps using the **policy-map type inspect scansafe** command, at least one for HTTP and one for HTTPS (assuming you want to inspect both types of traffic).
2. (Optional) Configure a whitelist using the **class-map type inspect scansafe** command.

3. Define the traffic that you want to inspect using the **class-map** command. You must configure separate class maps for HTTP and HTTPS traffic.
4. Enter the **policy-map** command to define the policy.
5. For HTTP, enter the **class** command to reference the HTTP class map.
6. Enter the **inspect scansafe** command, referencing the HTTP inspection policy map.
7. For HTTPS, enter the **class** command to reference the HTTPS class map.
8. Enter the **inspect scansafe** command, referencing the HTTPS inspection policy map.
9. Finally, apply the policy map to an interface using the **service-policy** command.

For more information about how Modular Policy Framework works, see the CLI configuration guide.

Examples

The following example configures two classes: one for HTTP and one for HTTPS. Each ACL exempts traffic to www.cisco.com and to tools.cisco.com, and to the DMZ network, for both HTTP and HTTPS. All other traffic is sent to Cloud Web Security, except for traffic from several whitelisted users and groups. The policy is then applied to the inside interface.

```
hostname(config)# class-map type inspect scansafe match-any whitelist1
hostname(config-cmap)# match user user1 group cisco
hostname(config-cmap)# match user user2
hostname(config-cmap)# match group group1
hostname(config-cmap)# match user user3 group group3

hostname(config)# policy-map type inspect scansafe cws_inspect_pmap1
hostname(config-pmap)# parameters
hostname(config-pmap-p)# http
hostname(config-pmap-p)# default group default_group
hostname(config-pmap-p)# class whitelist1
hostname(config-pmap-c)# whitelist

hostname(config)# policy-map type inspect scansafe cws_inspect_pmap2
hostname(config-pmap)# parameters
hostname(config-pmap-p)# https
hostname(config-pmap-p)# default group2 default_group2
hostname(config-pmap-p)# class whitelist1
hostname(config-pmap-c)# whitelist

hostname(config)# object network cisco1
hostname(config-object-network)# fqdn www.cisco.com
hostname(config)# object network cisco2
hostname(config-object-network)# fqdn tools.cisco.com
hostname(config)# object network dmz_network
hostname(config-object-network)# subnet 10.1.1.0 255.255.255.0

hostname(config)# access-list SCANSAFE_HTTP extended deny tcp any4 object cisco1 eq 80
hostname(config)# access-list SCANSAFE_HTTP extended deny tcp any4 object cisco2 eq 80
hostname(config)# access-list SCANSAFE_HTTP extended deny tcp any4 object dmz_network eq
80
hostname(config)# access-list SCANSAFE_HTTP extended permit tcp any4 any4 eq 80

hostname(config)# access-list SCANSAFE_HTTPS extended deny tcp any4 object cisco1 eq 443
hostname(config)# access-list SCANSAFE_HTTPS extended deny tcp any4 object cisco2 eq 443
hostname(config)# access-list SCANSAFE_HTTP extended deny tcp any4 object dmz_network eq
443
hostname(config)# access-list SCANSAFE_HTTPS extended permit tcp any4 any4 eq 443

hostname(config)# class-map cws_class1
hostname(config-cmap)# match access-list SCANSAFE_HTTP
hostname(config)# class-map cws_class2
hostname(config-cmap)# match access-list SCANSAFE_HTTPS

hostname(config)# policy-map cws_policy
hostname(config-pmap)# class cws_class1
hostname(config-pmap-c)# inspect scansafe cws_inspect_pmap1 fail-open
hostname(config-pmap)# class cws_class2
hostname(config-pmap-c)# inspect scansafe cws_inspect_pmap2 fail-open
hostname(config)# service-policy cws_policy inside
```

Related Commands

Command	Description
class-map type inspect scansafe	Creates an inspection class map for whitelisted users and groups.
default user group	Specifies the default username and/or group if the ASA cannot determine the identity of the user coming into the ASA.
http[**s**] (parameters)	Specifies the service type for the inspection policy map, either HTTP or HTTPS.
license	Configures the authentication key that the ASA sends to the Cloud Web Security proxy servers to indicate from which organization the request comes.
match user group	Matches a user or group for a whitelist.
policy-map type inspect scansafe	Creates an inspection policy map so you can configure essential parameters for the rule and also optionally identify the whitelist.
retry-count	Enters the retry counter value, which is the amount of time that the ASA waits before polling the Cloud Web Security proxy server to check its availability.
scansafe	In multiple context mode, allows Cloud Web Security per context.
scansafe general-options	Configures general Cloud Web Security server options.
server {**primary** | **backup**}	Configures the fully qualified domain name or IP address of the primary or backup Cloud Web Security proxy servers.
show conn scansafe	Shows all Cloud Web Security connections, as noted by the capitol Z flag.
show scansafe server	Shows the status of the server, whether it's the current active server, the backup server, or unreachable.
show scansafe statistics	Shows total and current http connections.
user-identity monitor	Downloads the specified user or group information from the AD agent.
whitelist	Performs the whitelist action on the class of traffic.

inspect sip

To enable SIP application inspection or to change the ports to which the ASA listens, use the **inspect sip** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect sip [*sip_map*] [**tls-proxy** *proxy_name*] [**phone-proxy** *proxy_name*] [**uc-ime** *proxy_name*]

no inspect sip [*sip_map*] [**tls-proxy** *proxy_name*] [**phone-proxy** *proxy_name*] [**uc-ime** *proxy_name*]

Syntax Description

phone-proxy *proxy_name*	Enables the phone proxy for the specified inspection session.
sip_map	Specifies a SIP policy map name.
tls-proxy *proxy_name*	Enables TLS proxy for the specified inspection session. The keyword **tls-proxy** cannot be used as a Layer 7 policy map name.
uc-ime *proxy_name*	Enable the Cisco Intercompany Media Engine Proxy for SIP inspection.

Defaults

This command is enabled by default.

The default port assignment for SIP is 5060.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
8.0(2)	The **tls-proxy** keyword was added.
7.0(1)	This command was introduced, replacing the **fixup** command, which has been deprecated.

Usage Guidelines

SIP, as defined by the IETF, enables VoIP calls. SIP works with SDP for call signaling. SDP specifies the details of the media stream. Using SIP, the ASA can support any SIP Voice over IP (VoIP) gateways and VoIP proxy servers. SIP and SDP are defined in the following RFCs:

- SIP: Session Initiation Protocol, RFC 2543
- SDP: Session Description Protocol, RFC 2327

To support SIP calls through the ASA, 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.

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

Instant Messaging

Instant Messaging refers to the transfer of messages between users in near real-time. 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, which will 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.

Technical Details

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

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

The well-known port 5060 must be used on the initial call setup (INVITE) message. However, subsequent messages 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 NATed.

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

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

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

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.

Inspecting Signaling Messages

For inspecting signaling messages, the **inspect sip** command often needs to determine locations of the media endpoints (for example, IP phones).

This information is used to prepare access-control and NAT state for media traffic to traverse the firewall transparently without manual configuration.

In determining these locations, the **inspect sip** command does **not** use the tunnel default gateway route. A tunnel default gateway route is a route of the form **route** *interface* **0 0** *metric* **tunneled**. This route overrides the default route for packets that egress from IPsec tunnels. Therefore, if the **inspect sip** command is desired for VPN traffic, do not configure the tunnel default gateway route. Instead, use other static routing or dynamic routing.

To enable SIP inspection for all interfaces, use the **global** parameter in place of **interface outside**.

Examples

The following example enables the SIP inspection engine, which creates a class map to match SIP traffic on the default port (5060). The service policy is then applied to the outside interface.

```
hostname(config)# class-map sip-port
hostname(config-cmap)# match port tcp eq 5060
hostname(config-cmap)# exit
hostname(config)# policy-map sip_policy
hostname(config-pmap)# class sip-port
hostname(config-pmap-c)# inspect sip
hostname(config-pmap-c)# exit
hostname(config)# service-policy sip_policy interface outside
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
show sip	Displays information about SIP sessions established through the ASA.
debug sip	Enables debugging information for SIP.
show conn	Displays the connection state for different connection types.
timeout	Sets the maximum idle time duration for different protocols and session types.
tls-proxy	Defines a TLS proxy instance and sets the maximum sessions.

inspect skinny

T o enable SCCP (Skinny) application inspection or to change the ports to which the ASA listens, use the **inspect skinny** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect skinny [*skinny_map*] [**tls-proxy** *proxy_name*] [**phone-proxy** *proxy_name*]

no inspect skinny [*skinny_map*] [**tls-proxy** *proxy_name*] [**phone-proxy** *proxy_name*]

Syntax Description

phone-proxy *proxy_name*	Enables the phone proxy for the specified inspection session.
skinny_map	Specifies a skinny policy map name.
tls-proxy *proxy_name*	Enables TLS proxy for the specified inspection session. The keyword **tls-proxy** cannot be used as a Layer 7 policy map name.

Defaults

This command is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
8.0(2)	The keyword **tls-proxy** was added.
7.0(1)	This command was introduced, replacing the **fixup** command, which has been deprecated.

Usage Guidelines

Skinny (or Simple) Client Control Protocol (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 ASA recognize SCCP Version 3.3. The functionality of the application layer software ensures that all SCCP signaling and media packets can traverse the ASA by providing NAT of the SCCP Signaling packets.

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

Normal traffic between the Cisco CallManager and Cisco IP Phones uses SCCP and is handled by SCCP inspection without any special configuration.The ASA also supports DHCP options 150 and 66, which allow the ASA to send the location of a TFTP server to Cisco IP Phones and other DHCP clients. For more information, see the **dhcp-server** command.

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, because a Cisco IP Phone requires the Cisco CallManager IP address to be specified explicitly in its configuration. An identity static entry allows the Cisco CallManager on the higher security interface to accept registrations from the Cisco IP Phones.

Cisco IP Phones require access to a TFTP server 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 will not work with configurations using the **alias** command.
- Outside NAT or PAT is not supported.

Note Stateful Failover of SCCP calls is supported, except for calls that are in the middle of call setup.

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 will fail because the ASA currently does not support NAT or PAT for the file content transferred via TFTP. Although the ASA does support NAT of TFTP messages, and opens a pinhole for the TFTP file to traverse the ASA, the ASA cannot translate the Cisco CallManager IP address and port embedded in the Cisco IP Phone's configuration files that are being transferred using TFTP during phone registration.

Inspecting Signaling Messages

For inspecting signaling messages, the **inspect skinny** command often needs to determine locations of the media endpoints (for example, IP phones).

This information is used to prepare access-control and NAT state for media traffic to traverse the firewall transparently without manual configuration.

In determining these locations, the **inspect skinny** command does **not** use the tunnel default gateway route. A tunnel default gateway route is a route of the form **route** *interface* **0 0** *metric* **tunneled**. This route overrides the default route for packets that egress from IPsec tunnels. Therefore, if the **inspect skinny** command is desired for VPN traffic, do not configure the tunnel default gateway route. Instead, use other static routing or dynamic routing.

To enable SCCP inspection for all interfaces, use the **global** parameter in place of **interface outside**.

Examples

The following example enables the SCCP inspection engine, which creates a class map to match SCCP traffic on the default port (2000). The service policy is then applied to the outside interface.

```
hostname(config)# class-map skinny-port
hostname(config-cmap)# match port tcp eq 2000
hostname(config-cmap)# exit
hostname(config)# policy-map skinny_policy
hostname(config-pmap)# class skinny-port
hostname(config-pmap-c)# inspect skinny
hostname(config-pmap-c)# exit
hostname(config)# service-policy skinny_policy interface outside
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
debug skinny	Enables SCCP debugging information.
show skinny	Displays information about SCCP sessions established through the ASA.
show conn	Displays the connection state for different connection types.
timeout	Sets the maximum idle time duration for different protocols and session types.
tls-proxy	Defines a TLS proxy instance and sets the maximum sessions.

inspect snmp

To enable SNMP application inspection or to change the ports to which the ASA listens, use the **inspect snmp** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect snmp *map_name*

no inspect snmp *map_name*

Syntax Description

map_name	The name of the SNMP map.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Use the **inspect snmp** command to enable SNMP inspection, using the settings configured with an SNMP map, which you create using the **snmp-map** command. Use the **deny version** command in SNMP map configuration mode to restrict SNMP traffic to a specific version of SNMP.

Earlier versions of SNMP are less secure so restricting SNMP traffic to Version 2 may be required by your security policy. To deny a specific version of SNMP, use the **deny version** command within an SNMP map, which you create using the **snmp-map** command. After configuring the SNMP map, you enable the map using the **inspect snmp** command and then apply it to one or more interfaces using the **service-policy** command.

To enable strict snmp application inspection for all interfaces, use the **global** parameter in place of **interface outside**.

Examples

The following example identifies SNMP traffic, defines an SNMP map, defines a policy, enables SNMP inspection, and applies the policy to the outside interface:

```
hostname(config)# access-list snmp-acl permit tcp any any eq 161
hostname(config)# access-list snmp-acl permit tcp any any eq 162
hostname(config)# class-map snmp-port
hostname(config-cmap)# match access-list snmp-acl
hostname(config-cmap)# exit
hostname(config)# snmp-map inbound_snmp
hostname(config-snmp-map)# deny version 1
hostname(config-snmp-map)# exit
hostname(config)# policy-map inbound_policy
hostname(config-pmap)# class snmp-port
hostname(config-pmap-c)# inspect snmp inbound_snmp
hostname(config-pmap-c)# exit
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
deny version	Disallows traffic using a specific version of SNMP.
snmp-map	Defines an SNMP map and enables SNMP map configuration mode.
policy-map	Associates a class map with specific security actions.
service-policy	Applies a policy map to one or more interfaces.

inspect sqlnet

To enable Oracle SQL*Net application inspection, use the **inspect sqlnet** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect sqlnet

no inspect sqlnet

Syntax Description

This command has no arguments or keywords.

Defaults

This command is enabled by default.

The default port assignment is 1521.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced, replacing the **fixup** command, which has been deprecated.

Usage Guidelines

The SQL*Net protocol consists of different packet types that the ASA handles to make the data stream appear consistent to the Oracle applications on either side of the ASA.

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 ASA 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 ASA NATs 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 ASA, a flag will be set in the connection data structure to expect the Data or Redirect message that follows to be NATed 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 NATed and port connections will be opened.

To enable SQL*Net inspection for all interfaces, use the **global** parameter in place of **interface outside**.

Examples

The following example enables the SQL*Net inspection engine, which creates a class map to match SQL*Net traffic on the default port (1521). The service policy is then applied to the outside interface.

```
hostname(config)# class-map sqlnet-port
hostname(config-cmap)# match port tcp eq 1521
hostname(config-cmap)# exit
hostname(config)# policy-map sqlnet_policy
hostname(config-pmap)# class sqlnet-port
hostname(config-pmap-c)# inspect sqlnet
hostname(config-pmap-c)# exit
hostname(config)# service-policy sqlnet_policy interface outside
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
debug sqlnet	Enables debugging information for SQL*Net.
policy-map	Associates a class map with specific security actions.
service-policy	Applies a policy map to one or more interfaces.
show conn	Displays the connection state for different connection types, including SQL*net.

inspect sunrpc

To enable Sun RPC application inspection or to change the ports to which the ASA listens, use the **inspect sunrpc** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect sunrpc

no inspect sunrpc

Syntax Description

This command has no arguments or keywords.

Defaults

This command is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced, replacing the **fixup** command, which has been deprecated.

Usage Guidelines

To enable Sun RPC application inspection or to change the ports to which the ASA listens, use the **inspect sunrpc** command in policy map class configuration mode, which is accessible by using the **class** command within policy map configuration mode. To remove the configuration, use the **no** form of this command.

The **inspect sunrpc** command 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 on the system. When a client attempts to access an Sun RPC service on a server, it must find out which port that service is running on. It does this by querying the portmapper process on the well-known port of 111.

The client sends the Sun RPC program number of the service, and gets back the port number. From this point on, the client program sends its Sun RPC queries to that new port. When a server sends out a reply, the ASA 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.

To enable RPC inspection for all interfaces, use the **global** parameter in place of **interface outside**.

Examples

The following example enables the RPC inspection engine, which creates a class map to match RPC traffic on the default port (111). The service policy is then applied to the outside interface.

```
hostname(config)# class-map sunrpc-port
hostname(config-cmap)# match port tcp eq 111
hostname(config-cmap)# exit
hostname(config)# policy-map sample_policy
hostname(config-pmap)# class sunrpc-port
hostname(config-pmap-c)# inspect sunrpc
hostname(config-pmap-c)# exit
hostname(config)# service-policy sample_policy interface outside
```

Related Commands

Commands	Description
clear configure sunrpc_server	Removes the configuration performed using the **sunrpc-server** command.
clear sunrpc-server active	Clears the pinholes that are opened by Sun RPC application inspection for specific services, such as NFS or NIS.
show running-config sunrpc-server	Displays the information about the Sun RPC service table configuration.
sunrpc-server	Allows pinholes to be created with a specified timeout for Sun RPC services, such as NFS or NIS.
show sunrpc-server active	Displays the pinholes open for Sun RPC services.

inspect tftp

To disable TFTP application inspection, or to enable it if it has been previously disabled, use the **inspect tftp** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect tftp

no inspect tftp

Syntax Description

This command has no arguments or keywords.

Defaults

This command is enabled by default.

The default port assignment is 69.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced, replacing the **fixup** command, which has been deprecated.

Usage Guidelines

Trivial File Transfer Protocol (TFTP), described in RFC 1350, is a simple protocol to read and write files between a TFTP server and client.

The ASA 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.

To enable TFTP inspection for all interfaces, use the **global** parameter in place of **interface outside**.

Examples

The following example enables the TFTP inspection engine, which creates a class map to match TFTP traffic on the default port (69). The service policy is then applied to the outside interface.

```
hostname(config)# class-map tftp-port
hostname(config-cmap)# match port udp eq 69
hostname(config-cmap)# exit
hostname(config)# policy-map tftp_policy
hostname(config-pmap)# class tftp-port
hostname(config-pmap-c)# inspect tftp
hostname(config-pmap-c)# exit
hostname(config)# service-policy tftp_policy interface outside
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
policy-map	Associates a class map with specific security actions.
service-policy	Applies a policy map to one or more interfaces.

inspect waas

To enable WAAS application inspection, use the **inspect waas** command in class configuration mode. The class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect waas

no inspect waas

Syntax Description

This command has no arguments or keywords.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example shows how to enable WAAS application inspection:

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

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
policy-map	Associates a class map with specific security actions.
service-policy	Applies a policy map to one or more interfaces.

inspect xdmcp

To enable XDMCP application inspection or to change the ports to which the ASA listens, use the **inspect xdmcp command** in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect xdmcp

no inspect xdmcp

Syntax Description

This command has no arguments or keywords.

Defaults

This command is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced, replacing the **fixup** command, which has been deprecated.

Usage Guidelines

The **inspect xdmcp** command enables or disables application inspection for the XDMCP protocol.

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 ASA must allow the TCP back connection from the Xhosted computer. To permit the back connection, use the **established** command on the ASA. 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 ASA can NAT if needed. XDCMP inspection does not support PAT.

To enable XDMCP inspection for all interfaces, use the **global** parameter in place of **interface outside**.

Examples

The following example enables the XDMCP inspection engine, which creates a class map to match XDMCP traffic on the default port (177). The service policy is then applied to the outside interface.

```
hostname(config)# class-map xdmcp-port
hostname(config-cmap)# match port tcp eq 177
hostname(config-cmap)# exit
hostname(config)# policy-map xdmcp_policy
hostname(config-pmap)# class xdmcp-port
hostname(config-pmap-c)# inspect xdmcp
hostname(config-pmap-c)# exit
hostname(config)# service-policy xdmcp_policy interface outside
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
debug xdmcp	Enables debugging information for XDMCP.
policy-map	Associates a class map with specific security actions.
service-policy	Applies a policy map to one or more interfaces.