tl – tz

tls-proxy

To configure a TLS proxy instance in TLS configuration mode or to set the maximum sessions, use the tls-proxy command in global configuration mode. To remove the configuration, use the **no** form of this command.

tls-proxy [**maximum-sessions** *max_sessions* | *proxy_name*] [**noconfirm**]
no tls-proxy [**maximum-sessions** *max_sessions* | *proxy_name*] [**noconfirm**]

Syntax Description

max_sessions *max_sessions*	Specifies the maximum number of TLS proxy sessions to support on the platform.
noconfirm	Runs the **tls-proxy** command without requiring confirmation.
proxy_name	Specifies the name of the TLS proxy instance.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

Use the tls-proxy command to enter TLS proxy configuration mode to create a TLS proxy instance, or to set the maximum sessions supported on the platform.

Examples

The following example shows how to create a TLS proxy instance:

```
ciscoasa(config)# tls-proxy my_proxy
ciscoasa(config-tlsp)# server trust-point ccm_proxy
ciscoasa(config-tlsp)# client ldc issuer ldc_server
ciscoasa(config-tlsp)# client ldc keypair phone_common
```

Related Commands

Commands	Description
client	Defines a cipher suite and sets the local dynamic certificate issuer or keypair.

Commands	Description
ctl-provider	Defines a CTL provider instance and enters provider configuration mode.
server trust-point	Specifies the proxy trustpoint certificate to be presented during the TLS handshake.
show tls-proxy	Shows the TLS proxies.

token

To configure the API token needed to register with Cisco Umbrella, use the **token** command in Umbrella configuration mode. Use the **no** form of this command to remove the token.

token *api_token*
no token *api_token*

Syntax Description

api_token	The API token needed to register with Cisco Umbrella. You must obtain the token from the Cisco Umbrella Network Devices Dashboard (https://login.umbrella.com/). A token will be a hexadecimal string, for example, AABBA59A0BDE1485C912AFE.

Command Default

There is no default API token.

Command Modes

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

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

Command History

Release	Modification
9.10(1)	This command was added.

Usage Guidelines

You must configure an API token to successfully register the device with Cisco Umbrella. The token is unique per customer, but not per device.

Registration is for a standalone device, cluster, or failover group. You do not register each device within a cluster or failover group separately. In multiple context mode, each context is a device, whether it is standalone or resides within a cluster or failover group.

Examples

The following example configures an API token for registration with Cisco Umbrella.

```
ciscoasa(config)# umbrella-global

ciscoasa(config-umbrella)# token AABBA59A0BDE1485C912AFE

Please make sure all the Umbrella Connector prerequisites are satisfied:
1. DNS server is configured to resolve api.opendns.com
2. Route to api.opendns.com is configured
3. Root certificate of Umbrella registration is installed
4. Unit has a 3DES license
```

Related Commands

Commands	Description
public-key	Configures the public key used with Cisco Umbrella.
timeout edns	Configures the idle timeout after which a connection from a client to the Umbrella server will be removed if there is no response from the server.
umbrella-global	Configures the Cisco Umbrella global parameters.

tos

To define a type of service byte in the IP header of an SLA operation request packet, use the **tos** command in SLA monitor protocol configuration mode. To restore the default value, use the **no** form of this command.

tos *number*
no tos

Syntax Description

number	The service type value to be used in the IP header. Valid values are from 0 to 255.

Command Default

The default type of service value is 0.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Sla monitor protocol configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This field contains information such as delay, precedence, reliability, and so on. This is can be used by other routers on the network for policy routing and features such as Committed Access Rate.

Examples

The following example configures an SLA operation with an ID of 123 that uses an ICMP echo request/response time probe operation. It sets the payload size of the echo request packets to 48 bytes, the number of echo requests sent during an SLA operation to 5, and the type of service byte to 80.

```
ciscoasa(config)# sla monitor 123
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside

ciscoasa(config-sla-monitor-echo)# num-packets 5
ciscoasa(config-sla-monitor-echo)# request-data-size 48
ciscoasa(config-sla-monitor-echo)# tos 80
ciscoasa(config-sla-monitor-echo)# timeout 4000
ciscoasa(config-sla-monitor-echo)# threshold 2500
ciscoasa(config-sla-monitor-echo)# frequency 10
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
```

Related Commands

Command	Description
num-packets	Specifies the number of request packets to send during an SLA operation.
request-data-size	Specifies the size of the request packet payload.
sla monitor	Defines an SLA monitoring operation.
type echo	Configures the SLA operation as an echo response time probe operation.

traceroute

To determine the route packets will take to their destination, use the **traceroute** command.

traceroute *destination_ip* | *hostname* [**source** *source_ip* | *source-interface*] [**numeric**] [**timeout** *timeout_value*] [**probe** *probe_num*] [**ttl** *min_ttl max_ttl*] [**port** *port_value*] [**use-icmp**]

Syntax Description

destination_ip	Specifies the destination IP address for the traceroute. Supports both IPv4 and IPv6 addresses.
hostname	The hostname of the host to which the route has to be traced. The host destination can be an IPv4 or IPv6 address. If the hostname is specified, define it with the **name** command, or configure a DNS server to enable traceroute to resolve the hostname to an IP address. Supports DNS domain names such as www.example.com.
max-ttl	The largest TTL value that can be used. The default is 30. The command terminates when the traceroute packet reaches the destination or when the value is reached.
min_ttl	The TTL value for the first probes. The default is 1, but it can be set to a higher value to suppress the display of known hops.
numeric	Specifies the output print only the IP addresses of the intermediate gateways. If this keyword is not specified the traceroute attempts to look up the hostnames of the gateways reached during the trace.
port *port_value*	The destination port used by the User Datagram Protocol (UDP) probe messages. The default is 33434.
probe *probe_num*	The number of probes to be sent at each TTL level. The default count is 3.
source	Specifies an IP address or interface is used as the source for the trace packets. IPv6 will accept only the IPv6 source address.
source_interface	Specifies the source interface for the packet trace. When specified, the IP address of the source interface is used.
source_ip	Specifies the source IP address for the packet trace. This IP address must be the IP address of one of the interfaces. In transparent mode, it must be the management IP address of the ASA.
timeout	Specifies a timeout value is used
timeout_value	Specifies the amount of time in seconds to wait for a response before the connection times out. The default is three seconds.
ttl	Keyword to specify the range of Time To Live values to use in the probes.
use-icmp	Specifies the use of ICMP probe packets instead of UDP probe packets.

Command Default

This command has no default settings.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.2(1)	This command was added.
9.7.(1)	This command was updated to accept IPv6 address.

Usage Guidelines

The **traceroute** command prints the result of each probe sent. Every line of output corresponds to a TTL value in increasing order. The following are the output symbols printed by the **traceroute** command:

Output Symbol	Description
*	No response was received for the probe within the timeout period.
U	No route to the destination.
nn msec	For each node, the round-trip time (in milliseconds) for the specified number of probes.
!N.	ICMP network unreachable. For ICMPv6, address is out of scope.
!H	ICMP host unreachable.
!P	ICMP protocol unreachable. For ICMPv6, port not reachable.
!A	ICMP administratively prohibited.
?	Unknown ICMP error.

Examples

The following example shows traceroute output that results when a destination IP address has been specified:

```
ciscoasa# traceroute 209.165.200.225
Tracing the route to 209.165.200.225
 1  10.83.194.1 0 msec 10 msec 0 msec
 2  10.83.193.65 0 msec 0 msec 0 msec
 3  10.88.193.101 0 msec 10 msec 0 msec
 4  10.88.193.97 0 msec 0 msec 10 msec
 5  10.88.239.9 0 msec 10 msec 0 msec
 6  10.88.238.65 10 msec 10 msec 0 msec
 7 172.16.7.221 70 msec 70 msec 80 msec
 8 209.165.200.225 70 msec 70 msec 70 msec
ciscoasa/admin(config)# traceroute 2002::130
```

```
Type escape sequence to abort.
Tracing the route to 2002::130
 1  5000::2 0 msec 0 msec 0 msec
2  2002::130 10 msec 0 msec 0 msec
```

Related Commands

Command	Description
capture	Captures packet information, including trace packets.
show capture	Displays the capture configuration when no options are specified.
packet-tracer	Enables packet tracing capabilities.

track rtr

To track the reachability of an SLA operation, use the **track rtr** command in global configuration mode. To remove the SLA tracking, use the **no** form of this command.

track *track-id* **rtr** *sla-id* **reachability**
no track *track-id* **rtr** *sla-id* **reachability**

Syntax Description

reachability	Specifies that the reachability of the object is being tracked.
sla-id	The ID of the SLA used by the tracking entry.
track-id	Creates a tracking entry object ID. Valid values are from 1 to 500.

Command Default

SLA tracking is disabled.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

The **track rtr** command creates a tracking entry object ID and specifies the SLA used by that tracking entry.

Every SLA operation maintains an operation return-code value, which is interpreted by the tracking process. The return code may be OK, Over Threshold, or several other return codes. Table 2-1 displays the reachability state of an object with respect to these return codes.

Table 1: SLA Tracking Return Codes

Tracking	Return Code	Track State
Reachability	OK or Over Threshold	Up
	Any other code	Down

Examples

The following example configures an SLA operation with an ID of 123 and creates a tracking entry with the ID of 1 to track the reachability of the SLA:

```
ciscoasa(config)# sla monitor 123
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside

ciscoasa(config-sla-monitor-echo)# timeout 1000
ciscoasa(config-sla-monitor-echo)# frequency 3
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
```

Related Commands

Command	Description
route	Configures a static route.
sla monitor	Defines an SLA monitoring operation.

traffic-forward

To direct traffic to a module and bypass access control and other processing, use the **traffic-forward** command in interface configuration mode. To disable traffic-forwarding, use the **no** form of this command.

traffic-forward *module_type***monitor-only**
no traffic-forward *module_type* **monitor-only**

Syntax Description

module_type The type of module. Supported modules are:

- **sfr**—ASA FirePOWER module.
- **cxsc**—ASA CX module.

monitor-only Sets the module to monitor-only mode. In monitor-only mode, the module can process traffic, but then drops the traffic. Usage differs by module type:

- ASA FirePOWER—Use this command to configure passive mode. You can use this mode for production purposes.
- ASA CX—This is strictly a demonstration mode. You cannot use the traffic-forwarding interface or the device for production purposes.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
9.1(2)	This command was added.
9.2(1)	The **sfr** keyword was added.
9.3(2)	Support for production use with the **sfr** keyword was added.

Usage Guidelines

This command is an alternative to using the service policy **sfr** or **cxsc** commands with the **monitor-only** keyword to redirect traffic to the module. With service policies, the traffic is still subject to ASA processing, such as access rules and TCP normalization, that can result in dropped traffic. Additionally, the ASA simply sends a copy of the traffic to the module, and eventually transmits the traffic according to its own policies.

The **traffic-forward** command, on the other hand, bypasses ASA processing completely and simply forwards the traffic to the module. The module then inspects traffic, makes policy decisions, and generates events, showing you what it would have done to the traffic if it was operating in inline mode. Although the module operates on a copy of the traffic, the ASA itself drops the traffic immediately regardless of ASA or module policy decisions. The module acts as a black hole.

Connect the traffic-forwarded interface to a SPAN port on a switch in your network.

Traffic-forwarding interface configuration has these restrictions:

- You cannot configure both monitor-only mode and normal inline mode at the same time on the ASA. Only one type of security policy is allowed.
- The ASA must be in single context transparent mode.
- Traffic-forwarding interfaces must be physical interfaces, not VLANs or BVIs. The physical interface also cannot have any VLANs associated with it.
- Traffic-forwarding interfaces cannot be used for ASA traffic; you cannot name them or configure them for ASA features, including failover or management-only.

Examples

The following example makes GigabitEthernet 0/5 a traffic-forwarding interface:

```
interface gigabitethernet 0/5
  no nameif
  traffic-forward sfr monitor-only
  no shutdown
```

Related Commands

Command	Description
interface	Enters interface configuration mode.
cxsc	Service policy command that redirects traffic to an ASA CX module.
sfr	Service policy command that redirects traffic to an ASA FirePOWER module.

traffic-non-sip

To allow non-SIP traffic using the well-known SIP signaling port, use the **traffic-non-sip** command in parameters configuration mode. Parameters configuration mode is accessible from policy map configuration mode. To disable this feature, use the **no** form of this command.

traffic-non-sip
no traffic-non-sip

Syntax Description

This command has no arguments or keywords.

Command Default

Beginning with 9.16, this command is disabled by default. In previous releases, it is enabled by default.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was added.
9.16(1)	The default setting was changed to disabled.

Examples

The following example shows how to allow non-SIP traffic using the well-known SIP signaling port in a SIP inspection policy map:

```
ciscoasa(config)# policy-map type inspect sip sip_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# traffic-non-sip
```

Related Commands

Command	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.

transfer-encoding

To restrict HTTP traffic by specifying a transfer encoding type, use the **transfer-encoding** command in HTTP map configuration mode, which is accessible using the **http-map** command. To disable this feature, use the **no** form of this command.

transfer-encoding type { **chunked | compress | deflate | gzip | identity | default** } **action** { **allow | reset | drop** } [**log**]
no transfer-encoding type { **chunked | compress | deflate | gzip | identity | default** } **action** { **allow | reset | drop** } [**log**]

Syntax Description

action	Specifies the action taken when a connection using the specified transfer encoding type is detected.
allow	Allows the message.
chunked	Identifies the transfer encoding type in which the message body is transferred as a series of chunks.
compress	Identifies the transfer encoding type in which the message body is transferred using UNIX file compression.
default	Specifies the default action taken by the ASA when the traffic contains a supported request method that is not on a configured list.
deflate	Identifies the transfer encoding type in which the message body is transferred using zlib format (RFC 1950) and deflate compression (RFC 1951).
drop	Closes the connection.
gzip	Identifies the transfer encoding type in which the message body is transferred using GNU zip (RFC 1952).
identity	Identifies connections in which the message body is no transfer encoding is performed.
log	(Optional) Generates a syslog.
reset	Sends a TCP reset message to client and server.
type	Specifies the type of transfer encoding to be controlled through HTTP application inspection.

Command Default

This command is disabled by default. When the command is enabled and a supported transfer encoding type is not specified, the default action is to allow the connection without logging. To change the default action, use the **default** keyword and specify a different default action.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
HTTP map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

When you enable the **transfer-encoding** command, the ASA applies the specified action to HTTP connections for each supported and configured transfer encoding type.

The ASA applies the **default** action to all traffic that does *not* match the transfer encoding types on the configured list. The preconfigured **default** action is to **allow** connections without logging.

For example, given the preconfigured default action, if you specify one or more encoding types with the action of **drop** and **log**, the ASA drops connections containing the configured encoding types, logs each connection, and allows all connections for the other supported encoding types.

If you want to configure a more restrictive policy, change the default action to **drop** (or **reset**) and **log** (if you want to log the event). Then configure each permitted encoding type with the **allow** action.

Enter the **transfer-encoding** command once for each setting you wish to apply. You use one instance of the **transfer-encoding** command to change the default action and one instance to add each encoding type to the list of configured transfer encoding types.

When you use the **no** form of this command to remove an application category from the list of configured application types, any characters in the command line after the application category keyword are ignored.

Examples

The following example provides a permissive policy, using the preconfigured default, which allows all supported application types that are not specifically prohibited.

```
ciscoasa(config)# http-map inbound_http
ciscoasa(config-http-map)# transfer-encoding gzip drop log
ciscoasa(config-http-map)#
```

In this case, only connections using GNU zip are dropped and the event is logged.

The following example provides a restrictive policy, with the default action changed to reset the connection and to log the event for any encoding type that is not specifically allowed.

```
ciscoasa(config)# http-map inbound_http
ciscoasa(config-http-map)# port-misuse default action reset log
ciscoasa(config-http-map)# port-misuse identity allow
ciscoasa(config-http-map)#
```

In this case, only connections using no transfer encoding are allowed. When HTTP traffic for the other supported encoding types is received, the ASA resets the connection and creates a syslog entry.

Related Commands

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

trustpoint (saml idp)

To configure a trustpoint that contains the certificates for idp authentication or sp authentication, use the **trustpoint** command in saml idp configuration mode. You can access the saml idp configuration mode by first entering the **webvpn** command. To remove the trustpoint, use the **no** form of this command.

trustpoint idp *trustpoint-name* [*trustpoint-name2*]
no trustpoint idp *trustpoint-name* [*trustpoint-name2*]

trustpoint sp *trustpoint-name*
no trustpoint sp *trustpoint-name*

Syntax Description

trustpoint-name	Specifies the name of the trustpoint to use.
trustpoint-name2	Specifies the name of the second trustpoint to use.
sp	The trustpoint contains the ASA (SP)'s certificate for IdP to verify ASA's signature or encrypt SAML assertion.
idp	The trustpoint contains the IdP certificate for ASA to verify SAML assertions.

Command Default

No default behavior or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Saml idp configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.5(2)	This command was added.
9.20(3)	*trustpoint_name2* variable was added.

Usage Guidelines

A trustpoint represents a Certificate Authority identity, based on a CA-issued certificate that can be relied upon as being valid without the need for validation testing, especially a public-key certificate used to provide the first public key in a certification path.

You can configure two trustpoints for a SAML IdP on a device. This feature allows you to gracefully transition to a new Identity Provider (IdP) certificate without any loss of service. You do not need to open a maintenance window to simultaneously update all ASAs and the IdP with the same certificate. When the new IdP certificate is enabled on the IdP, the device automatically detects the new certificate. You can safely delete the original trustpoint after the transition.

Related Commands

Command	Description
saml idp	Creates a configuration for a third-party Idp, and puts you in saml-idp mode so you can configure SAML attributes.

trustpoint (sso server) (Deprecated)

Note The last supported release for this command was Version 9.5(1).

To specify the name of a trustpoint that identifies the certificate to be sent to the SAML POST-type SSO server, use the **trustpoint** command in sso server mode. To eliminate a trustpoint specification, use the **no** form of this command.

trustpoint *trustpoint-name*
no trustpoint *trustpoint-name*

Syntax Description

trustpoint-name	Specifies the name of the trustpoint to use.

Command Default

No default behavior or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Config webvpn sso saml	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command is added.
9.5(2)	This command was deprecated due to support for SAML 2.0.

Usage Guidelines

Single sign-on support, available only for WebVPN, lets users access different secure services on different servers without entering a username and password more than once. The ASA currently supports the SAML POST-type SSO server and the SiteMinder-type of SSO server.

This command applies only to SAML-type SSO Servers.

A trustpoint represents a Certificate Authority identity, based on a CA-issued certificate that can be relied upon as being valid without the need for validation testing, especially a public-key certificate used to provide the first public key in a certification path.

Examples

The following example enters config-webvpn-sso-saml mode and names a trustpoint for identifying the certificate to be sent to the SAML POST type SSO Server:

```
ciscoasa(config-webvpn)# sso server
ciscoasa(config-webvpn-sso-saml)# trustpoint mytrustpoint
```

Related Commands

Command	Description
crypto ca trustpoint	Manages trustpoint information.
show webvpn sso server	Displays the operating statistics for all SSO servers configured on the security device.
sso server	Creates, names, and specifies type for an SSO server.

trust-verification-server

To identify Trust Verification Services servers, which enable Cisco Unified IP Phones to authenticate application servers during HTTPS establishment, use the **trust-verification-server** command in parameters configuration mode for SIP inspection. Parameters configuration mode is accessible from policy map configuration mode. To disable this feature, use the **no** form of this command.

trust-verification-server { **ip** *address* | **port** *number* }
no trust-verification-server { **ip** *address* | **port** *number* }

Syntax Description

ip *address*	Specifies the IP address of the Trust Verification Services server. You can enter the command with this argument up to four times in a SIP inspection policy map. SIP inspection opens pinholes to each server for each registered phone, and the phone decides which to use. Configure the Trust Verification Services server on the Cisco Unified Communications Manager (CUCM) server.
port *number*	Specifies the port number used by the server. The allowed port range is 1026 to 32768.

Command Default

The default port is 2445.

Command Modes

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

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

Command History

Release	Modification
9.3(2)	This command was added.

Examples

The following example shows how to configure four Trust Verification Services servers in a SIP inspection policy map:

```
ciscoasa(config)# policy-map type inspect sip sip_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# trust-verification-server ip 10.1.1.1

ciscoasa(config-pmap-p)# trust-verification-server ip 10.1.1.2

ciscoasa(config-pmap-p)# trust-verification-server ip 10.1.1.3

ciscoasa(config-pmap-p)# trust-verification-server ip 10.1.1.4
```

```
ciscoasa(config-pmap-p)# trust-verification-server port 2445
```

Related Commands

Command	Description
policy-map type inspect	Creates an inspection policy map.
show running-config policy-map	Display all current policy map configurations.

tsig enforced

To require a TSIG resource record to be present, use the **tsig enforced** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

tsig enforced action { **drop** [**log**] | **log** }
no tsig enforced [**action** { **drop** [**log**] | **log** }]

Syntax Description

drop	Drops the packet if TSIG is not present.
log	Generates a system message log.

Command Default

This command is disabled by default.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This command enables monitoring and enforcement of TSIG presence in DNS transactions.

Examples

The following example shows how to enable TSIG enforcement in a DNS inspection policy map:

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# tsig enforced action log
```

Related Commands

Command	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.

Command	Description
show running-config policy-map	Display all current policy map configurations.

ttl-evasion-protection

To enable Time-To-Live (TTL) evasion protection, use the **ttl-evasion-protection** command in tcp-map configuration mode. To disable the feature, use the **no** form of this command.

ttl-evasion-protection
no ttl-evasion-protection

Syntax Description

This command has no arguments or keywords.

Command Default

TTL evasion protection offered is enabled by default.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tcp-map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **tcp-map** command is used along with the Modular Policy Framework infrastructure. Define the class of traffic using the **class-map** command and customize the TCP inspection with **tcp-map** commands. Apply the new TCP map using the **policy-map** command. Activate TCP inspection with **service-policy** commands.

Use the **tcp-map** command to enter tcp-map configuration mode. Use the **ttl-evasion-protection** command in tcp-map configuration mode to prevent attacks that attempt to evade security policy. With TTL evasion protect, the maximum TTL for a connection is determined by the TTL in the initial packet. The TTL for subsequent packets can decrease, but it cannot increase. The system will reset the TTL to the lowest previously-seen TTL for that connection.

For instance, an attacker can send a packet that passes policy with a very short TTL. When the TTL goes to zero, a router between the ASA and the endpoint drops the packet. It is at this point that the attacker can send a malicious packet with a long TTL that appears to the ASA to be a retransmission and is passed. To the endpoint host, however, it is the first packet that has been received by the attacker. In this case, an attacker is able to succeed without security preventing the attack. Enabling this feature prevents such attacks.

Examples

The following example shows how to disable TTL evasion protection on flows from network 10.0.0.0 to 20.0.0.0:

```
ciscoasa(config)# access-list TCP1 extended permit tcp 10.0.0.0 255.0.0.0 20.0.0.0 255.0.0.0
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# no
```

```
 ttl-evasion-protection
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match access-list TCP1
ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
ciscoasa(config-pmap)# set connection advanced-options tmap
ciscoasa(config)# service-policy pmap global
```

Related Commands

Command	Description
class	Specifies a class map to use for traffic classification.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
set connection	Configures connection values.
tcp-map	Creates a TCP map and allows access to tcp-map configuration mode.

tunnel destination

To specify the IP address (IPv4 or IPv6) of the VTI tunnel's destination, use the tunnel destination command in the interface configuration mode. Use the no form of this command to remove the VTI tunnel's destination IP address.

tunnel destination { *IP address* | *hostname* }
no tunnel destination { *IP address* | *hostname* }

Syntax Description

IP address	Specifies the IP address (IPv4 or IPv6) of the VTI tunnel's destination.
hostname	Specifies the hostname of the VTI tunnel's destination.

Command Default

No default behavior or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• No	• Yes	• No	—

Command History

Release	Modification
9.7(1)	We introduced this command.
9.16(1)	We introduced support for IPv6 addresses.

Usage Guidelines

This command is available in the interface configuration mode after using the **interface tunnel** command in the Global Configuration mode.

Examples

The following example specifies the IP address of the VTI tunnel's destination:

```
ciscoasa(config)# interface tunnel 10
ciscoasa(config-if)# tunnel destination 10.2.2.3
```

Related Commands

Command	Description
interface tunnel	Creates a new VTI tunnel interface.
tunnel source interface	Specifies the source interface to create a VTI tunnel.

Command	Description
tunnel mode	Specifies that IPsec is used for tunnel protection.
tunnel protection ipsec	Specifies the IPsec profile that will be used for tunnel protection.

tunnel mode

To specify the tunnel protection mode for a VTI tunnel, use the tunnel mode command in the interface configuration mode. A tunnel can use IPSec over IPv4 or IPv6. Use the no form of this command to remove VTI tunnel protection.

tunnel mode ipsec { **ipv4** | **ipv6** }
no tunnel mode ipsec { **ipv4** | **ipv6** }

Syntax Description

ipsec	Specifies that the tunnel will use IPsec as the tunnel protection standard.
ipv4	Specifies that the tunnel will use IPsec over IPv4.
ipv6	Specifies that the tunnel will use IPsec over IPv6.

Command Default

No default behavior or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• No	• Yes	—	—

Command History

Release	Modification
9.7(1)	We introduced this command.
9.16(1)	We introduced IPSec over IPv6.

Usage Guidelines

This command is available in the interface configuration mode after using the **interface tunnel** command in the Global Configuration mode.

Examples

The following example specifies IPsec as the protection mode:

```
ciscoasa(config)# interface tunnel 10
ciscoasa(config-if)# tunnel mode ipsec ipv4
```

Related Commands

Command	Description
interface tunnel	Creates a new VTI tunnel interface.

Command	Description
tunnel source interface	Specifies the source interface to create a VTI tunnel.
tunnel destination	Specifies the IP address of the VTI tunnel's destination.
tunnel protection ipsec	Specifies the IPsec profile that will be used for tunnel protection.

tunnel protection ipsec

To specify the IPsec profile for the VTI tunnel, use the **tunnel protection ipsec** command in the interface configuration mode. Use the no form of this command to remove the IPsec profile for the tunnel.

tunnel protection ipsec { **profile** *IPsec_profile_name* | **policy** *acl_name* }
no tunnel protection ipsec *IPsec_profile_name*
no tunnel protection ipsec policy *acl_name*

Syntax Description

IPsec_profile_name	Specifies the name of the IPsec profile.
acl_name	Specifies the name of the ACL.

Command Default

No default behavior or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• No	• Yes	• No	—

Command History

Release	Modification
9.19(1)	Support for configuring specific traffic selectors using ACL for a static VTI.
9.7(1)	We introduced this command.

Usage Guidelines

This command is available in the interface configuration mode after using the **interface tunnel** command in the Global Configuration mode.

The IKEv1 policy is attached to the IPsec profile when using the **tunnel protection ipsec profile** command.

The **tunnel protection ipsec policy** command is an optional command. If an ACL isn't attached to a static VTI, by default any-any traffic selector is chosen for the VTI tunnel.

Examples

In the following example, profile12 is the IPsec profile:

```
ciscoasa(config)# interface tunnel 10
ciscoasa(config-if)# tunnel protection ipsec profile profile12
```

Examples

The following shows how to configure specific traffic selectors using acl10 for a static VTI (Tunnel10):

```
ciscoasa(config)# interface tunnel 10
ciscoasa(config-if)# tunnel protection ipsec policy acl10
```

Related Commands

Command	Description
interface tunnel	Creates a new VTI tunnel interface.
tunnel source interface	Specifies the source interface to create a VTI tunnel.
tunnel destination	Specifies the IP address of the VTI tunnel's destination.
tunnel mode	Specifies the tunnel protection mode for a VTI tunnel.

tunnel source interface

To specify the source interface for the VTI tunnel, use the tunnel source interface command in the interface configuration mode. Use the no form of this command to remove the VTI tunnel's source interface.

tunnel source interface *interface_name*
tunnel source interface *interface_name* **ipv6** *ipv6_address*
no tunnel source interface *interface_name*
no tunnel source interface *interface_name* **ipv6** *ipv6_address*

Syntax Description

interface_name	Specifies the source interface to be used to create the VTI tunnel. If the source interface is an IPv6 address, prefix ipv6 to the address.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
9.7(1)	We introduced this command.
9.16(1)	We introduced support for IPv6 addresses.

Usage Guidelines

This command is available in the interface configuration mode after using the **interface tunnel**command in the Global Configuration mode. The IP address is taken from the selected interface.

Examples

The following example specifies the source interface of the VTI tunnel:

```
ciscoasa(config)# interface tunnel 10
ciscoasa(config-if)# tunnel source interface outside
```

Related Commands

Command	Description
interface tunnel	Creates a new VTI tunnel interface.
tunnel destination	Specifies the IP address of the VTI tunnel's destination.
tunnel mode	Specifies that IPsec is used for tunnel protection.

Command	Description
tunnel protection ipsec	Specifies the IPsec profile that will be used for tunnel protection.

tunnel-group

To create and manage the database of connection-specific records for IPsec and WebVPN tunnels, use the **tunnel-group** command in global configuration mode. To remove a tunnel group, use the **no** form of this command.

tunnel-group *name* **type** *type*
no tunnel-group *name*

Syntax Description

name Specifies the name of the tunnel group. This can be any string you choose. If the name is an IP address, it is usually the IP address of the peer.

type Specifies the type of tunnel group:

- remote-access—Allows a user to connect using either IPsec remote access or WebVPN (portal or tunnel client).
- ipsec-l2l—Specifies IPsec LAN-to-LAN, which allows two sites or LANs to connect securely across a public network like the Internet.

Note The following tunnel-group types are deprecated in Release 8.0(2):ipsec-ra—IPsec remote access webvpn—WebVPN. The ASA converts these to the remote-access type.

Command Default

No default behavior or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	See Note.	• Yes	• Yes	—

Note The tunnel-group command is available in transparent firewall mode to allow configuration of a LAN-to-LAN tunnel group, but not a remote-access group or a WebVPN group. All the **tunnel-group** commands that are available for LAN-to-LAN are also available in transparent firewall mode.

Command History

Release	Modification
7.0(1)	This command was added.
7.1(1)	The webvpn type was added.
8.0(2)	The remote-access type was added and the ipsec-ra and webvpn types were deprecated.

Release	Modification
8.3(1)	The *name argument was modified to accept IPv6 addresses.*
9.0(1)	Support for multiple context mode was added.
9.15(1)	The external-browser option is deprecated in the config-tunnel-webvpn mode.
9.17(1)	WebAuthN support was added using AnyConnect external browser. The external-browser option is added in the config-tunnel-webvpn mode.

Usage Guidelines

SSL VPN users (both AnyConnect and clientless) can choose which tunnel group to access using these different methods:

- group-url
- group-alias
- certificate maps, if using certificates

This command and subcommands configures the ASA to allow users to select a group via a drop-down menu when they log in to the webvpn service. The groups that appear in the menu are either aliases or URLs of real connection profiles (tunnel groups) configured on the ASA.

The ASA has the following default tunnel groups:

- DefaultRAGroup, the default IPsec remote-access tunnel group
- DefaultL2LGroup, the default IPsec LAN-to-LAN tunnel group
- DefaultWEBVPNGroup, the default WebVPN tunnel group.

You can change these groups, but not delete them. The ASA uses these groups to configure default tunnel parameters for remote access and LAN-to-LAN tunnel groups when there is no specific tunnel group identified during tunnel negotiation.

After entering the **tunnel-group** command, you enter the appropriate following commands to configure specific attributes for a particular tunnel group. Each of these commands enters a configuration mode for configuring tunnel-group attributes.

- **tunnel-group general-attributes**
- tunnel-group ipsec-attributes
- tunnel-group webvpn-attributes
- tunnel-group ppp-attributes

For LAN-to-LAN connections, the ASA attempts to select a tunnel group for a connection by matching the peer address specified in the crypto map to a tunnel group of the same name. Therefore, for IPv6 peers, you should configure the tunnel group name as the IPv6 address of the peer. You can specify the tunnel group name in short or long notation. The CLI reduces the name to the shortest notation. For example, if you enter this tunnel group command:

```
ciscoasa(config)# tunnel-group 2001:0db8:0000:0000:0000:0000:1428:57ab type ipsec-l2l
```

The tunnel group appears in the configuration as:

```
tunnel-group 2001:0db8::1428:57ab type ipsec-l2l
```

Examples

The following examples are entered in global configuration mode. The first configures a remote access tunnel group. The group name is group1.

```
ciscoasa(config)# tunnel-group group1 type remote-access
ciscoasa(config)#
```

The following example shows the tunnel-group command configuring the webvpn tunnel group named “group1”. You enter this command in global configuration mode:

```
ciscoasa(config)# tunnel-group group1 type webvpn
ciscoasa(config)#
```

Related Commands

Command	Description
clear configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group.
tunnel-group general-attributes	Enters the config-general mode for configuring general tunnel-group attributes
tunnel-group ipsec-attributes	Enters the config-ipsec mode for configuring IPsec tunnel-group attributes.
tunnel-group ppp-attributes	Enters the config-ppp mode for configuring PPP settings for L2TP connections.
tunnel-group webvpn-attributes	Enters the config-webvpn mode for configuring WebVPN tunnel-group attributes.

tunnel-group general-attributes

To enter the general-attribute configuration mode, use the **tunnel-group general-attributes** command in global configuration mode. This mode is used to configure settings that are common to all supported tunneling protocols.

To remove all general attributes, use the **no** form of this command.

tunnel-group *name* **general-attributes**
no tunnel-group *name* **general-attributes**

Syntax Description

general-attributes	Specifies attributes for this tunnel-group.
name	Specifies the name of the tunnel-group.

Command Default

No default behavior or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group general-attributes configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
7.1(1)	Various attributes from other tunnel-group types migrated to the general tunnel-group attributes list, and the prompt for tunnel-group general-attributes mode changed.
9.0(1)	Support for multiple context mode was added.

Examples

The following example entered in global configuration mode, creates a remote-access tunnel group for a remote-access connection using the IP address of the LAN-to-LAN peer, then enters general-attributes configuration mode for configuring tunnel-group general attributes. The name of the tunnel group is 209.165.200.225.

```
ciscoasa(config)# tunnel-group 209.165.200.225 type remote-access
ciscoasa(config)# tunnel-group 209.165.200.225 general-attributes
ciscoasa(config-tunnel-general)#
```

The following example entered in global configuration mode, creates a tunnel group named" remotegrp" for an IPsec remote access connection, and then enters general configuration mode for configuring general attributes for the tunnel group named "remotegrp":

```
ciscoasa(config)# tunnel-group remotegrp type ipsec_ra
ciscoasa(config)# tunnel-group remotegrp general
ciscoasa(config-tunnel-general)
```

Related Commands

Command	Description
clear configure tunnel-group	Clears the entire tunnel-group database or just the specified tunnel-group.
show running-config tunnel-group	Displays the currently running tunnel-group configuration for a specified tunnel group or for all tunnel groups.
tunnel-group	Creates and manages the database of connection-specific records for IPsec and WebVPN tunnels.

tunnel-group ipsec-attributes

To enter the ipsec-attribute configuration mode, use the **tunnel-group ipsec-attributes** command in global configuration mode. This mode is used to configure settings that are specific to the IPsec tunneling protocol.

To remove all IPsec attributes, use the **no** form of this command.

tunnel-group *name* **ipsec-attributes**
no tunnel-group *name* **ipsec-attributes**

Syntax Description

ipsec-attributes	Specifies attributes for this tunnel-group.
name	Specifies the name of the tunnel-group.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.
7.1(1)	Various IPsec tunnel-group attributes migrated to the general tunnel-group attributes list, and the prompt for tunnel-group ipsec-attributes mode changed.
9.0(1)	Support for multiple context mode was added.

Examples

The following example entered in global configuration, creates a tunnel group for the IPsec remote-access tunnel group named remotegrp, and then specifies IPsec group attributes:

```
ciscoasa(config)# tunnel-group remotegrp type ipsec_ra
ciscoasa(config)# tunnel-group remotegrp ipsec-attributes
ciscoasa(config-tunnel-ipsec)
```

Related Commands

Command	Description
clear configure tunnel-group	Clears the entire tunnel-group database or just the specified tunnel-group.

Command	Description
show running-config tunnel-group	Displays the currently running tunnel-group configuration for a specified tunnel group or for all tunnel groups.
tunnel-group	Creates and manages the database of connection-specific records for IPsec and WebVPN tunnels.

tunnel-group-list enable

To enable the tunnel-groups defined in tunnel-group group-alias, use the **tunnel-group-list enable** command:

tunnel-group-list enable

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

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

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

Usage Guidelines

This command is used in conjunction with the tunnel-group group-alias and group-url commands for clientless and AnyConnect VPN client sessions. It enables the feature so that the tunnel-group drop-down is displayed on the login page. The group-alias is a text string such as employees, engineering, or consultants defined by the ASA administrator to display to end users.

Command History

Release	Modification
7.0(1)	This command was added.

Examples

```
ciscoasa# configure
 terminal
ciscoasa(config)# tunnel-group ExampleGroup1 webvpn-att
ciscoasa(config-tunnel-webvpn)# group-alias Group1 enable
ciscoasa(config-tunnel-webvpn)# exit
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# tunnel-group-list enable
```

Related Commands

Command	Description
tunnel-group	Creates a VPN connection profile or accesses the database of VPN connection profiles.
group-alias	Configures an alias for a connection profile (tunnel group).
group-url	Matches the URL or IP address specified by the VPN endpoint to the connection profile.

Command	Description
show running-config tunnel-group	Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group.

tunnel-group-map

When the adaptive security appliance receives an IPsec connection request with client certificate authentication, it assigns a connection profile to the connection according to a policy you configure.

That policy can be to use rules you configure, use the certificate OU field, use the IKE identity (i.e. hostname, IP address, key ID), the client's IP address, or a default connection profile to assign the connection profile. For SSL connections, the adaptive security appliance only uses the rules you configure to assign the connection profile.

The **tunnel-group-map** command assigns a connection profile to the connection based on rules you configure by associating an existing map name with a connection profile.

Use the **no** form of this command to disassociate a connection profile with a map name. The no form of the command does not delete the map name, just its association with a connection profile.

This is the syntax of the command:

tunnel-group-map [*mapname*] [*rule-index*] [*connection-profile*]
no tunnel-group-map [*mapname*] [*rule-index*]

Note

- You create the certificate map name with this command:crypto ca certificate map [mapname] [rule-index]
- A "tunnel group" is old terminology for what we now call a "connection profile." Think of the tunnel-group-map command as creating a connection profile map.

Syntax Description

mapname	Required. Identifies the name of the existing certificate map.
rule-index	Required. Identifies the rule-index associated with the mapname. The rule-index parameter was defined using the **crypto ca certificate map** command. The values are 1 to 65535.
connection-profile	Designates the connection profile name for this certificate map list.

Command Default

If a tunnel-group-map is not defined, and the ASA receives an IPsec connection request with client certificate authentication, the ASA assigns a connection profile by trying to match the certificate authentication request to one of these policies, in this order:

Certificate ou field—Determines connection profile based on the value of the organizational unit (OU) field in the subject distinguished name (DN).

IKE identity—Determines the connection profile based on the content of the phase1 IKE ID.

peer-ipDetermines the connection profile based on the established client IP address.

Default Connection Profile—If the ASA does not match the previous three policies, it assigns the default connection profile. The default profile is DefaultRAGroup. The default connection profile would otherwise be configured using the tunnel-group-map default-group command.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

The map name you specify must already exist before you can associate it with a connection profile. You create a map name using the **crypto ca certificate map** command. Refer to the documentation on the **crypto ca certificate map** command for more information.

Once you have associated map names with connection profiles, you need to enable the tunnel-group-map to use the rules you have configured rather than the default polices described earlier. To do this you must run the tunnel-group-map enable rules command in global configuration mode.

Examples

The following example associates the map name SalesGroup, with rule index 10, to the SalesConnectionProfile connection profile.

```
ciscoasa(config)# tunnel-group-map SalesGroup 10 SalesConnectionProfile
ciscoasa(config)#
```

Related Commands

Command	Description
crypto ca certificate map [map name]	Enters ca certificate map configuration mode and you can use it to create a certificate map name.
tunnel-group-map enable	Enables certificate-based IKE sessions based on established rules.
tunnel-group-map default-group	Designates an existing tunnel-group name as the default tunnel group.

tunnel-group-map default-group

The tunnel-group-map default-group command specifies the default tunnel-group to use if the name could not be determined using other configured methods.

Use the **no** form of this command to eliminate a tunnel-group-map.

tunnel-group-map [*rule-index*] **default-group** *tunnel-group-name*
no tunnel-group-map

Syntax Description

default-group *tunnel-group-name*	Specifies a default tunnel group to use when the name cannot be derived by other configured methods. The *tunnel-group name* must already exist.
rule index	Optional. Refers to parameters specified by the **crypto ca certificate map** command. The values are 1 to 65535.

Command Default

The default value for the **tunnel-group-map default-group** is DefaultRAGroup.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

The tunnel-group-map commands configure the policy and rules by which certificate-based IKE sessions are mapped to tunnel groups. To associate the certificate map entries, created using the **crypto ca certificate map** command, with tunnel groups, use the **tunnel-group-map** command in global configuration mode. You can invoke this command multiple times as long as each invocation is unique and you do not reference a map index more than once.

The **crypto ca certificate map** command maintains a prioritized list of certificate mapping rules. There can be only one map. But this map can have up to 65535 rules. Refer to the documentation on the **crypto ca certificate map** command for more information.

The processing that derives the tunnel-group name from the certificate ignores entries in the certificate map that are not associated with a tunnel group (any map rule not identified by this command).

Examples

The following example entered in global configuration mode, specifies a default tunnel group to use when the name cannot be derived by other configured methods. The name of the tunnel group to use is group1:

```
ciscoasa(config)# tunnel-group-map default-group group1
ciscoasa(config)#
```

Related Commands

Command	Description
crypto ca certificate map	Enters crypto ca certificate map configuration mode.
subject-name (crypto ca certificate map)	Identifies the DN from the CA certificate that is to be compared to the rule entry string.
tunnel-group-map enable	Configures the policy and rules by which certificate-based IKE sessions are mapped to tunnel groups

tunnel-group-map enable

The **tunnel-group-map enable** command configures the policy and rules by which certificate-based IKE sessions are mapped to tunnel groups. Use the **no** form of this command to restore the default values.

tunnel-group-map [*rule-index*] **enable** *policy*
no tunnel-group-map enable [*rule-index*]

Syntax Description

policy	Specifies the policy for deriving the tunnel group name from the certificate. *Policy* can be one of the following: **ike-id**—Indicates that if a tunnel-group is not determined based on a rule lookup or taken from the ou, then the certificate-based IKE sessions are mapped to a tunnel group based on the content of the phase1 IKE ID. **ou**—Indicates that if a tunnel-group is not determined based on a rule lookup, then use the value of the organizational unit (OU) in the subject distinguished name (DN). **peer-ip**—Indicates that if a tunnel-group is not determined based on a rule lookup or taken from the ou or ike-id methods, then use the established peer IP address. **rules**—Indicates that the certificate-based IKE sessions are mapped to a tunnel group based on the certificate map associations configured by this command.
rule index	(Optional) Refers to parameters specified by the **crypto ca certificate map** command. The values are 1 to 65535.

Command Default

The default values for the **tunnel-group-map** command are **enable ou** and **default-group** set to DefaultRAGroup.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

The **crypto ca certificate map** command maintains a prioritized list of certificate mapping rules. There can be only one map. But this map can have up to 65535 rules. Refer to the documentation on the **crypto ca certificate map** command for more information.

Examples

The following example enables mapping of certificate-based IKE sessions to a tunnel group based on the content of the phase1 IKE ID:

```
ciscoasa(config)# tunnel-group-map enable ike-id
ciscoasa(config)#
```

The following example enables mapping of certificate-based IKE sessions to a tunnel group based on the established IP address of the peer:

```
ciscoasa(config)# tunnel-group-map enable peer-ip
ciscoasa(config)#
```

The following example enables mapping of certificate-based IKE sessions based on the organizational unit (OU) in the subject distinguished name (DN):

```
ciscoasa(config)# tunnel-group-map enable ou
ciscoasa(config)#
```

The following example enables mapping of certificate-based IKE sessions based on established rules:

```
ciscoasa(config)# tunnel-group-map enable rules
ciscoasa(config)#
```

Related Commands

Command	Description
crypto ca certificate map	Enters CA certificate map mode.
subject-name (crypto ca certificate map)	Identifies the DN from the CA certificate that is to be compared to the rule entry string.
tunnel-group-map default-group	Designates an existing tunnel-group name as the default tunnel group.

tunnel-group ppp-attributes

To enter the ppp-attributes configuration mode and configure PPP settings that are used by L2TP over IPsec connections, use the **tunnel-group ppp-attributes** command in global configuration mode.

To remove all PPP attributes, use the **no** form of this command.

tunnel-group *name* **ppp-attributes**
no tunnel-group *name* **ppp-attributes**

Syntax Description

name	Specifies the name of the tunnel-group.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

PPP settings are used by the Layer 2 Tunneling Protocol (L2TP), a VPN tunneling protocol which allows remote clients to use the dialup telephone service public IP network to securely communicate with private corporate network servers. L2TP is based on the client/server model and uses PPP over UDP (port 1701) to tunnel the data. All of the tunnel-group ppp commands are available for the PPPoE tunnel-group type.

Examples

The following example creates the tunnel group *telecommuters* and enters ppp-attributes configuration mode:

```
ciscoasa(config)# tunnel-group telecommuters type pppoe
ciscoasa(config)# tunnel-group telecommuters ppp-attributes
ciscoasa(tunnel-group-ppp)#
```

Related Commands

Command	Description
clear configure tunnel-group	Clears the entire tunnel-group database or just the specified tunnel-group.

Command	Description
show running-config tunnel-group	Displays the currently running tunnel-group configuration for a specified tunnel group or for all tunnel groups.
tunnel-group	Creates and manages the database of connection-specific records for IPsec and WebVPN tunnels.

tunnel-group-preference

To change the VPN preference to a connection profile with a group URL that matches the one specified by the endpoint, use the **tunnel-group-preference** command in webvpn configuration mode. To remove the command from the configuration, use the **no** form.

tunnel-group-preference group-url
no tunnel-group-preference group-url

Syntax Description

This command has no arguments or keywords.

Command Default

By default, if the ASA matches a certificate field value specified in a connection profile to the field value of the certificate used by the endpoint, the ASA assigns that profile to the VPN connection. This command overrides the default behavior.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Config-webvpn	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.2(5)/8.4(2)	This command was added.

Usage Guidelines

This command changes the preference of a connection profile during the connection profile selection process. It lets you rely on the group URL preference used by many older ASA software releases. If the endpoint specifies a group URL that is not present in a connection profile, but it specifies a certificate value that matches that of a connection profile, the ASA assigns that connection profile to the VPN session.

Although you enter this command in webvpn configuration mode, it changes the connection profile selection preference for all clientless and AnyConnect VPN connections negotiated by the ASA.

Examples

The following example changes the preference of a connection profile during the connection profile selection process:

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# tunnel-group-preference group-url
ciscoasa(config-webvpn)#
```

Related Commands

Command	Description
tunnel-group	Creates a VPN connection profile or accesses the database of VPN connection profiles.
group-url	Matches the URL or IP address specified by the VPN endpoint to the connection profile.
show running-config tunnel-group	Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group.

tunnel-group webvpn-attributes

To enter the webvpn-attribute configuration mode, use the **tunnel-group webvpn-attributes** command in global configuration mode. This mode configures settings that are common to WebVPN tunneling.

To remove all WebVPN attributes, use the **no** form of this command.

tunnel-group *name* **webvpn-attributes**
no tunnel-group *name* **webvpn-attributes**

Syntax Description

name	Specifies the name of the tunnel-group. **Note** Ensure that the tunnel group name does not contain the following special characters: &, ", or <.
webvpn-attributes	Specifies WebVPN attributes for this tunnel-group.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.1(1)	This command was added.
9.0(1)	Support for multiple context mode was added.
9.8(1)	Changed the pre-fill-username and secondary-pre-fill-username value from clientless to client.

Usage Guidelines

In addition to the general attributes, you can also configure the following attributes specific to WebVPN connections in webvpn-attribute mode:

- authentication
- customization
- dns-group
- group-alias
- group-url

- without-csd

The pre-fill-username and secondary-pre-fill-username attributes are used to extract a username from a certificate for use in authentication and authorization. The values are client or clientless.

Examples

The following example entered in global configuration mode, creates a tunnel group for a WebVPN connection using the IP address of the LAN-to-LAN peer, then enters webvpn-configuration mode for configuring WebVPN attributes. The name of the tunnel group is 209.165.200.225.

```
ciscoasa(config)# tunnel-group 209.165.200.225 type webvpn
ciscoasa(config)# tunnel-group 209.165.200.225 webvpn-attributes
ciscoasa(config-tunnel-webvpn)#
```

The following example entered in global configuration mode, creates a tunnel group named" remotegrp" for a WebVPN connection, and then enters webvpn configuration mode for configuring WebVPN attributes for the tunnel group named "remotegrp":

```
ciscoasa(config)# tunnel-group remotegrp type webvpn
ciscoasa(config)# tunnel-group remotegrp webvpn-attributes
ciscoasa(config-tunnel-webvpn)#
```

Related Commands

Command	Description
clear configure tunnel-group	Clears the entire tunnel-group database or just the specified tunnel-group.
show running-config tunnel-group	Displays the currently running tunnel-group configuration for a specified tunnel group or for all tunnel groups.
tunnel-group	Creates and manages the database of connection-specific records for IPsec and WebVPN tunnels.

tunnel-limit

To specify the maximum number of active GTP tunnels allowed, use the **tunnel limit** command in policy map parameters configuration mode. Use the **no** form of this command to set the tunnel limit back to its default.

tunnel-limit *max_tunnels*
no tunnel-limit *max_tunnels*

Syntax Description

max_tunnels	The maximum number of tunnels allowed. This is equivalent to the number of PDP contexts or endpoints.

Command Default

The default tunnel limit is 500.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

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

Examples

The following example specifies a maximum of 10,000 tunnels for GTP traffic:

```
ciscoasa(config)# policy-map type inspect gtp gtp-policy
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# tunnel-limit 10000
```

Related Commands

Commands	Description
clear service-policy inspect gtp	Clears global GTP statistics.
inspect gtp	Applies a specific GTP map to use for application inspection.
show service-policy inspect gtp	Displays the GTP configuration.

tx-ring-limit

To specify the depth of the priority queues, use the **tx-ring-limit** command in priority-queue mode. To remove this specification, use the **no** form of this command.

Note This command is not supported on ASA 5580 Ten Gigabit Ethernet interfaces, the ASA 5512-X through ASA 5555-X Management interface, or the ASA Services Module. (Ten Gigabit Ethernet interfaces are supported for priority queues on the ASA 5585-X.)

tx-ring-limit *number-of-packets*
no tx-ring-limit *number-of-packets*

Syntax Description

number-of-packets	Specifies the maximum number of low-latency or normal priority packets allowed into the Ethernet transmit driver before the driver pushes back to the queues on the interface to let them buffer packets until the congestion clears. The range 3 through 511.

Command Default

The default is 511.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Priority-queue	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The ASA allows two classes of traffic: low-latency queuing (LLQ) for higher priority, latency sensitive traffic (such as voice and video) and best-effort, the default, for all other traffic. The ASA recognizes priority traffic and enforces appropriate Quality of Service (QoS) policies. You can configure the size and depth of the priority queue to fine-tune the traffic flow.

You must use the **priority-queue** command to create the priority queue for an interface before priority queuing takes effect. You can apply one **priority-queue** command to any interface that can be defined by the **nameif** command.

The **priority-queue** command enters priority-queue mode, as shown by the prompt. In priority-queue mode, you can configure the maximum number of packets allowed in the transmit queue at any given time (**tx-ring-limit** command) and the number of packets of either type (priority or best-effort) allowed to be buffered before dropping packets (**queue-limit** command).

The tx-ring-limit and the queue-limit that you specify affect both the higher priority low-latency queue and the best-effort queue. The tx-ring-limit is the number of either type of packets allowed into the driver before the driver pushes back to the queues sitting in front of the interface to let them buffer packets until the congestion clears. In general, you can adjust these two parameters to optimize the flow of low-latency traffic.

Because queues are not of infinite size, they can fill and overflow. When a queue is full, any additional packets cannot get into the queue and are dropped. This is *tail drop* . To avoid having the queue fill up, you can use the **queue-limit** command to increase the queue buffer size.

Note The upper limit of the range of values for the **queue-limit** and **tx-ring-limit** commands is determined dynamically at run time. To view this limit, enter **help** or **?** on the command line. The key determinant is the memory needed to support the queues and the memory available on the device.

On ASA Model 5505 (only), configuring priority-queue on one interface overwrites the same configuration on all other interfaces. That is, only the last applied configuration is present on all interfaces. Further, if the priority-queue configuration is removed from one interface, it is removed from all interfaces.

To work around this issue, configure the priority-queue command on only one interface. If different interfaces need different settings for the queue-limit and/or tx-ring-limit commands, use the largest of all queue-limits and smallest of all tx-ring-limits on any one interface.

Examples

The following example configures a priority queue for the interface named test, specifying a queue limit of 2048 packets and a transmit queue limit of 256 packets.

```
ciscoasa(config)# priority-queue test
ciscoasa(priority-queue)# queue-limit 2048
ciscoasa(priority-queue)# tx-ring-limit 256
```

Related Commands

Command	Description
clear configure priority-queue	Removes the current priority queue configuration on the named interface.
priority-queue	Configures priority queuing on an interface.
queue-limit	Specifies the maximum number of packets that can be enqueued to a priority queue before it drops data.
show priority-queue statistics	Shows the priority-queue statistics for the named interface.
show running-config priority-queue	Shows the current priority queue configuration. If you specify the **all** keyword, this command displays all the current **priority-queue**, **queue-limit**, and **tx-ring-limit** command configuration values.

type echo

To configure the SLA operation as an echo response time probe operation, use the **type echo** command in SLA monitor configuration mode. To remove the type from the SLA configuration, use the **no** form of this command.

type echo protocol ipIcmpEcho *target* **interface** *if-name*
no type echoprotocol ipIcmpEcho *target* **interface** *if-name*

Syntax Description

interface *if-name*	Specifies the interface name, as specified by the **nameif** command, of the interface used to send the echo request packets. The interface source address is used as the source address in the echo request packets.
protocol	The protocol keyword. The only value supported is **ipIcmpEcho**, which specifies using an IP/ICMP echo request for the echo operation.
target	The IP address or host name of the object being monitored.

Command Default

No default behaviors or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Sla monitor configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

The default size of the payload of the ICMP packets is 28 bytes, creating a total ICMP packet size of 64 bytes. The payload size can be changed using the **request-data-size** command.

Examples

The following example configures an SLA operation with an ID of 123 that uses an ICMP echo request/response time probe operation. It creates a tracking entry with the ID of 1 to track the reachability of the SLA. The frequency of the SLA operation is set to 10 seconds, the threshold to 2500 milliseconds, and the timeout value us set to 4000 milliseconds.

```
ciscoasa(config)# sla monitor 123
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside

ciscoasa(config-sla-monitor-echo)# threshold 2500
ciscoasa(config-sla-monitor-echo)# timeout 4000
```

```
ciscoasa(config-sla-monitor-echo)# frequency 10
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
```

Related Commands

Command	Description
num-packets	Specifies the number of request packets to send during an SLA operation.
request-data-size	Specifies the size of the payload for the SLA operation request packet.
sla monitor	Defines an SLA monitoring operation.