pr - pz

pre-fill-username

To enable extracting a username from a client certificate for use in authentication and authorization, use the **pre-fill-username** command in tunnel-group webvpn-attributes mode. To remove the attribute from the configuration, use the **no** form of this command.

pre-fill-username { **client** | **clientless** }
no pre-fill-username

Syntax Description

client	Enables this feature for AnyConnect VPN client connections. Use the **client** keyword in 9.8(1)+.
ssl-client	
clientless	Enables this feature for clientless connections.

Command Default

No default value or 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
Tunnel-group webvpn-attributes configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(4)	This command was added.
9.8(1)	The **ssl-client** keyword was changed to **client**.

Usage Guidelines

The **pre-fill-username** command enables the use of a username extracted from the certificate field specified in the **username-from-certificate** command as the username for username/password authentication and authorization. To use this pre-fill username from certificate feature, you must configure both commands.

To enable this feature, you must also configure the **username-from-certificate** command in tunnel-group general-attributes mode.

Examples

The following example, entered in global configuration mode, creates an IPsec remote access tunnel group named remotegrp and specifies that the name for an authentication or authorization query for an SSL VPN client must be derived from a digital certificate:

```
ciscoasa(config)# tunnel-group remotegrp type ipsec_ra
ciscoasa(config)# tunnel-group remotegrp webvpn-attributes
ciscoasa(config-tunnel-webvpn)# pre-fill-username client
ciscoasa(config-tunnel-webvpn)#
```

Related Commands

Command	Description
pre-fill-username	Enables the pre-fill username feature.
show running-config tunnel-group	Shows the indicated tunnel-group configuration.
tunnel-group general-attributes	Specifies the general attributes for the named tunnel-group.
username-from-certificate	Specifies the field in a certificate to use as the username for authorization.

preempt

To cause the failover group to become active on the preferred unit, use the **preempt** command in failover group configuration mode. To remove the preemption, use the **no** form of this command.

preempt [*delay*]
no preempt [*delay*]

Syntax Description

seconds The wait time, in seconds, before the peer is preempted. Valid values are from 1 to 1200 seconds.

Command Default

By default, there is no delay.

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
Failover group configuration	• Yes	• Yes	—	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Earlier software versions allowed "simultaneous" boot up so that the failover groups did not require the **preempt** command to become active on the preferred unit. However, this functionality has now changed so that both failover groups become active on the first unit to boot up.

Usage Guidelines

Assigning a **primary** or **secondary** preference to a failover group specifies which unit the failover group becomes active on when you set the **preempt** command. Both failover groups become active on the first unit that boots up (even if it seems like they boot simultaneously, one unit becomes active first), despite the **primary** or **secondary** setting for the group. When the other unit comes online, any failover groups that have the second unit as a priority do not become active on the second unit unless the failover group is configured with the **preempt** command or is manually forced to the other unit with the **no failover active** command. If the failover group is configured with the **preempt** command, the failover group automatically becomes active on the designated unit.

Note If Stateful Failover is enabled, the preemption is delayed until the connections are replicated from the unit on which the failover group is currently active.

Examples

The following example configures failover group 1 with the primary unit as the higher priority and failover group 2 with the secondary unit as the higher priority. Both failover groups are configured

with the **preempt** command with a wait time of 100 seconds, so the groups will automatically become active on their preferred unit 100 seconds after the units become available.

```
ciscoasa(config)# failover group 1

ciscoasa(config-fover-group)# primary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# exit
ciscoasa(config)# failover group 2
ciscoasa(config-fover-group)# secondary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# mac-address e1 0000.a000.a011 0000.a000.a012

ciscoasa(config-fover-group)# exit
ciscoasa(config)#
```

Related Commands

Command	Description
failover group	Defines a failover group for Active/Active failover.
primary	Gives the primary unit in a failover pair priority for the failover group being configured.
secondary	Gives the secondary unit in a failover pair priority for the failover group being configured.

prefix-list

The OSPFv2, EIGRP and BGP protocols all use the **prefix-list** command in global configuration mode. To remove a prefix list entry, use the **no** form of this command.

prefix-list*prefix-list-name* [**seq***seq_num*] { **permit** | **deny** } *network*/*len* [**ge***min_value*] [**le***max_value*]
no prefix-list *prefix-list-name* [**seq** *seq_num*] { **permit** | **deny** } *network* / *len* [**ge** *min_value*] [**le** *max_value*]

Syntax Description

/	A required separator between the *network* and *len* values.
deny	Denies access for a matching condition.
ge *min_value*	(Optional) Specifies the minimum prefix length to be matched. The value of the *min_value* argument must be greater than the value of the *len* argument and less than or equal to the *max_value* argument, if present.
le *max_value*	(Optional) Specifies the maximum prefix length to be matched. The value of the *max_value* argument must be greater than or equal to the value of the *min_value* argument, if present, or greater than the value of the *len* argument if the *min_value* argument is not present.
len	The length of the network mask. Valid values are from 0 to 32.
network	The network address.
permit	Permits access for a matching condition.
prefix-list-name	The name of the prefix list. The prefix-list name cannot contain spaces.
seq *seq_num*	(Optional) Applies the specified sequence number to the prefix list being created.

Command Default

If you do not specify a sequence number, the first entry in a prefix list is assigned a sequence number of 5, and the sequence number for each subsequent entry is increased by 5.

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.

Release	Modification
9.2(1)	Support for BGP was added.

Usage Guidelines

The **prefix-list** commands are ABR type 3 LSA filtering commands. ABR type 3 LSA filtering extends the capability of an ABR that is running OSPF to filter type 3 LSAs between different OSPF areas. Once a prefix list is configured, only the specified prefixes are sent from one area to another area. All other prefixes are restricted to their OSPF area. You can apply this type of area filtering to traffic going into or coming out of an OSPF area, or to both the incoming and outgoing traffic for that area.

When multiple entries of a prefix list match a given prefix, the entry with the lowest sequence number is used. The ASA begins the search at the top of the prefix list, with the entry with the lowest sequence number. Once a mach is made, the ASA does not go through the rest of the list. For efficiency, you may want to put the most common matches or denials near the top of the list by manually assigning them a lower sequence number.

By default, the sequence numbers are automatically generated. They can be suppressed with the **no prefix-list sequence-number** command. Sequence numbers are generated in increments of 5. The first sequence number generated in a prefix list would be 5. The next entry in that list would have a sequence number of 10, and so on. If you specify a value for an entry, and then do not specify values for subsequent entries, the generated sequence numbers are increased from the specified value in increments of 5. For example, if you specify that the first entry in the prefix list has a sequence number of 3, and then add two more entries without specifying a sequence number for the additional entries, the automatically generated sequence numbers for those two entries would be 8 and 13.

You can use the **ge** and **le** keywords to specify the range of the prefix length to be matched for prefixes that are more specific than the *network*/*len* argument. Exact match is assumed when neither the **ge** or **le** keywords are specified. The range is from *min_value* to 32 if only the **ge** keyword is specified.The range is from *len* to *max_value* if only the **le** keyword is specified.

The value of the *min_value* and *max_value* arguments must satisfy the following condition:

len < *min_value* <= *max_value* <= 32

Use the **no** form of the command to remove specific entries from the prefix list. Use the **clear configure prefix-list** command to remove a prefix list. The clear **configure prefix-list** command also removes the associated **prefix-list description** command, if any, from the configuration.

Examples

The following example denies the default route 0.0.0.0/0:

```
ciscoasa(config)# prefix-list abc deny 0.0.0.0/0
```

The following example permits the prefix10.0.0.0/8:

```
ciscoasa(config)# prefix-list abc permit 10.0.0.0/8
```

The following example shows how to accept a mask length of up to 24 bits in routes with the prefix 192/8:

```
ciscoasa(config)# prefix-list abc permit 192.168.0.0/8 le 24
```

The following example shows how to deny mask lengths greater than 25 bits in routes with a prefix of 192/8:

```
ciscoasa(config)# prefix-list abc deny 192.168.0.0/8 ge 25
```

The following example shows how to permit mask lengths from 8 to 24 bits in all address space:

```
ciscoasa(config)# prefix-list abc permit 0.0.0.0/0 ge 8 le 24
```

The following example shows how to deny mask lengths greater than 25 bits in all address space:

```
ciscoasa(config)# prefix-list abc deny 0.0.0.0/0 ge 25
```

The following example shows how to deny all routes with a prefix of 10/8:

```
ciscoasa(config)# prefix-list abc deny 10.0.0.0/8 le 32
```

The following example shows how to deny all masks with a length greater than 25 bits for routes with a prefix of 192.168.1/24:

```
ciscoasa(config)# prefix-list abc deny 192.168.1.0/24 ge 25
```

The following example shows how to permit all routes with a prefix of 0/0:

```
ciscoasa(config)# prefix-list abc permit 0.0.0.0/0 le 32
```

Related Commands

Command	Description
clear configure prefix-list	Removes the **prefix-list** commands from the running configuration.
prefix-list description	Lets you to enter a description for a prefix list.
prefix-list sequence-number	Enables prefix list sequence numbering.
show running-config prefix-list	Displays the **prefix-list** commands in the running configuration.

prefix-list description

To add a description to a prefix list, use the **prefix-list description** command in global configuration mode. To remove a prefix list description, use the **no** form of this command.

prefix-list*prefix-list-name***description***text*
no prefix-list *prefix-list-name* **description** [*text*]

Syntax Description

prefix-list-name	The name of a prefix list.
text	The text of the prefix list description. You can enter a maximum of 80 characters.

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	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

You can enter **prefix-list** and **prefix-list description** commands in any order for a particular prefix list name; you do not need to create the prefix list before entering a prefix list description. The **prefix-list description** command will always appear on the line before the associated prefix list in the configuration, no matter what order you enter the commands.

If you enter a **prefix-list description** command for a prefix list entry that already has a description, the new description replaces the original description.

You do not need to enter the text description when using the **no** form of this command.

Examples

The following example adds a description for a prefix list named MyPrefixList. The **show running-config prefix-list** command shows that although the prefix list description has been added to the running configuration, the prefix-list itself has not been configured.

```
ciscoasa(config)# prefix-list MyPrefixList description A sample prefix list description
ciscoasa(config)# show running-config prefix-list
!
prefix-list MyPrefixList description A sample prefix list description
!
```

Related Commands

Command	Description
clear configure prefix-list	Removes the **prefix-list** commands from the running configuration.
prefix-list	Defines a prefix list for ABR type 3 LSA filtering.
show running-config prefix-list	Displays the **prefix-list** commands in the running configuration.

prefix-list sequence-number

To enable prefix list sequence numbering, use the **prefix-list sequence-number** command in global configuration mode. To disable prefix list sequence numbering, use the **no** form of this command.

prefix-list sequence-number

Syntax Description

This command has no arguments or keywords.

Command Default

Prefix list sequence numbering 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
Global Configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Only the **no** form of this command appears in the configuration. When the **no** form of this command is in the configuration, the sequence numbers, including the manually configured ones, are removed from the **prefix-list** commands in the configuration and new prefix lists entries are not assigned a sequence number.

When prefix list sequence numbering is enabled, all prefix list entries are assigned sequence numbers using the default numbering method (starting with 5 and incrementing each number by 5). If a sequence number was manually assigned to a prefix list entry before numbering was disabled, the manually assigned number is restored. Sequence numbers that are manually assigned while automatic numbering is disabled are also restored, even though they are not displayed while numbering is disabled.

Examples

The following example disables prefix list sequence numbering:

```
ciscoasa(config)# no prefix-list sequence-number
```

Related Commands

Command	Description
prefix-list	Defines a prefix list for ABR type 3 LSA filtering.
show running-config prefix-list	Displays the **prefix-list** commands in the running configuration.

prf

To specify the pseudo-random function (PRF) in an IKEv2 security association (SA) for AnyConnect IPsec connections, use the prf command in IKEv2 policy configuration mode. To remove the command and use the default setting, use the no form of this command:

prf { **md5** | **sha** | **sha256** | **sha384** | **sha512** }
no prf { **md5** | **sha** | **sha256** | **sha384** | **sha512** }

Syntax Description

md5	Specifies the MD5 algorithm.
sha	(Default) Specifies the Secure Hash Algorithm SHA 1.
sha256	Specifies the Secure Hash Algorithm SHA 2 with the 256-bit digest.
sha384	Specifies the Secure Hash Algorithm SHA 2 with the 384-bit digest.
sha512	Specifies the Secure Hash Algorithm SHA 2 with the 512-bit digest.

Command Default

The default is **sha** (SHA 1).

Usage Guidelines

An IKEv2 SA is a key used in phase 1 to enable IKEv2 peers to communicate securely in phase 2. After entering the crypto ikev2 policy command, use the **prf** command to select the pseudo-random function used for the construction of keying material for all of the cryptographic algorithms used in the SA.

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
8.4(1)	This command was added.
8.4(2)	The sha256, sha384, and sha512 keywords were added for SHA 2 support.

Examples

The following example enters IKEv2 policy configuration mode and sets the PRF to MD5:

```
ciscoasa(config)# crypto ikev2 policy 1
ciscoasa(config-ikev2-policy)# prf md5
```

Related Commands

Command	Description
encryption	Specifies the encryption algorithm in an IKEv2 SA for AnyConnect IPsec connections.
group	Specifies the Diffie-Hellman group in an IKEv2 SA for AnyConnect IPsec connections.
integrity	Specifies the ESP integrity algorithm in an IKEv2 SA for AnyConnect IPsec connections.
lifetime	Specifies the SA lifetime for the IKEv2 SA for AnyConnect IPsec connections.

primary

To set the preferred unit for a failover group when using the **preempt** command, use the **primary** command in failover group configuration mode. To restore the default value, use the **no** form of this command.

primary
no primary

Syntax Description

This command has no arguments or keywords.

Command Default

If **primary** or **secondary** is not specified for a failover group, the failover group defaults to **primary**.

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
Failover group configuration	• Yes	• Yes	—	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Earlier software versions allowed "simultaneous" boot up so that the failover groups did not require the **preempt** command to become active on the preferred unit. However, this functionality has now changed so that both failover groups become active on the first unit to boot up.

Usage Guidelines

Assigning a **primary** or **secondary** preference to a failover group specifies which unit the failover group becomes active on when you set the **preempt** command. Both failover groups become active on the first unit that boots up (even if it seems like they boot simultaneously, one unit becomes active first), despite the **primary** or **secondary** setting for the group. When the other unit comes online, any failover groups that have the second unit as a priority do not become active on the second unit unless the failover group is configured with the **preempt** command or is manually forced to the other unit with the **no failover active** command. If the failover group is configured with the **preempt** command, the failover group automatically becomes active on the designated unit.

Examples

The following example configures failover group 1 with the primary unit as the higher priority and failover group 2 with the secondary unit as the higher priority. Both failover groups are configured with the **preempt** command, so the groups will automatically become active on their preferred unit as the units become available.

```
ciscoasa(config)# failover group 1

ciscoasa(config-fover-group)# primary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# exit
```

```
ciscoasa(config)# failover group 2
ciscoasa(config-fover-group)# secondary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# mac-address e1 0000.a000.a011 0000.a000.a012

ciscoasa(config-fover-group)# exit
ciscoasa(config)#
```

Related Commands

Command	Description
failover group	Defines a failover group for Active/Active failover.
preempt	Forces the failover group to become active on its preferred unit when the unit becomes available.
secondary	Gives the secondary unit a higher priority than the primary unit.

priority (class)

To enable QoS priority queuing, use the **priority** command in class configuration mode. For critical traffic that cannot tolerate latency, such as voice over IP (VoIP), you can identify traffic for low latency queuing (LLQ) so that it is always transmitted at a minimum rate. To remove the priority requirement, use the **no** form of this command.

Note This command is not supported on the ASA Services Module.

priority
no priority

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or variables.

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
Class configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

LLQ priority queuing lets you prioritize certain traffic flows (such as latency-sensitive traffic like voice and video) ahead of other traffic.

The ASA supports two types of priority queuing:

- Standard priority queuing—Standard priority queuing uses an LLQ priority queue on an interface (see the **priority-queue** command), while all other traffic goes into the "best effort" queue. 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 called *tail drop* .To avoid having the queue fill up, you can increase the queue buffer size. You can also fine-tune the maximum number of packets allowed into the transmit queue. These options let you control the latency and robustness of the priority queuing. Packets in the LLQ queue are always transmitted before packets in the best effort queue.
- Hierarchical priority queuing—Hierarchical priority queuing is used on interfaces on which you enable a traffic shaping queue (the **shape** command). A subset of the shaped traffic can be prioritized. The standard priority queue is not used. See the following guidelines about hierarchical priority queuing:

- Priority packets are always queued at the head of the shape queue so they are always transmitted ahead of other non-priority queued packets.
- Priority packets are never dropped from the shape queue unless the sustained rate of priority traffic exceeds the shape rate.
- For IPsec-encrypted packets, you can only match traffic based on the DSCP or precedence setting.
- IPsec-over-TCP is not supported for priority traffic classification.

Configuring QoS with Modular Policy Framework

To enable priority queuing, use the Modular Policy Framework. You can use standard priority queuing or hierarchical priority queuing.

For standard priority queuing, perform the following tasks:

1.class-map—Identify the traffic on which you want to perform priority queuing.

2.policy-map—Identify the actions associated with each class map.

- **a.class**—Identify the class map on which you want to perform actions.
- **b.priority**—Enable priority queuing for the class map.

3.service-policy—Assigns the policy map to an interface or globally.

For hierarchical priority-queuing, perform the following tasks:

1.class-map—Identify the traffic on which you want to perform priority queuing.

2.policy-map (for priority queuing)—Identify the actions associated with each class map.

- **a.class**—Identify the class map on which you want to perform actions.
- **b.priority**—Enable priority queuing for the class map. You can only include the priority command in this policy map if you want to use is hierarchically.

3.policy-map (for traffic shaping)—Identify the actions associated with the **class-default** class map.

- **a.class class-default**—Identify the **class-default** class map on which you want to perform actions.
- **b.shape**—Apply traffic shaping to the class map.
- **c.service-policy**—Call the priority queuing policy map in which you configured the **priority** command so you can apply priority queuing to a subset of shaped traffic.

4.service-policy—Assigns the policy map to an interface or globally.

Examples

The following is an example of the **priority** command in policy-map configuration mode:

```
ciscoasa(config)# policy-map localpolicy1
ciscoasa(config-pmap)# class firstclass
ciscoasa(config-pmap-c)# priority
ciscoasa(config-pmap-c)# class class-default
ciscoasa(config-pmap-c)#
```

Related Commands

class	Specifies a class map to use for traffic classification.

clear configure policy-map	Remove all policy-map configuration, except that if a policy-map is in use in a service-policy command, that policy-map is not removed.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
show running-config policy-map	Display all current policy-map configurations.

priority (cluster group)

To set the priority of this unit for master unit elections in an ASA cluster, use the **priority** command in cluster group configuration mode. To remove the priority, use the **no** form of this command.

priority *priority_number*
no priority [*priority_number*]

Syntax Description

priority_number	Sets the priority of this unit for master unit elections, between 1 and 100, where 1 is the highest priority.

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
Cluster group configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Members of the cluster communicate over the cluster control link to elect a master unit, as follows:

1. When you enable clustering for a unit (or when it first starts up with clustering already enabled), it broadcasts an election request every 3 seconds.

2. Any other units with a higher priority respond to the election request; the priority is set between 1 and 100, where 1 is the highest priority.

3. If after 45 seconds, a unit does not receive a response from another unit with a higher priority, then it becomes master.

Note If multiple units tie for the highest priority, the cluster unit name, and then the serial number is used to determine the master.

4. If a unit later joins the cluster with a higher priority, it does not automatically become the master unit; the existing master unit always remains as the master unless it stops responding, at which point a new master unit is elected.

Note You can manually force a unit to become the master using the **cluster master unit** command. For centralized features, if you force a master unit change, then all connections are dropped, and you have to re-establish the connections on the new master unit. See the configuration guide for a list of centralized features.

Examples

The following example sets the priority to 1 (the highest):

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# priority 1
```

Related Commands

Command	Description
clacp system-mac	When using spanned EtherChannels, the ASA uses cLACP to negotiate the EtherChannel with the neighbor switch.
cluster group	Names the cluster and enters cluster configuration mode.
cluster-interface	Specifies the cluster control link interface.
cluster interface-mode	Sets the cluster interface mode.
conn-rebalance	Enables conn ection rebalancing.
console-replicate	Enables console replication from slave units to the master unit.
enable (cluster group)	Enables clustering.
health-check	Enables the cluster health check feature, which includes unit health monitoring and interface health monitoring.
key	Sets an authentication key for control traffic on the cluster control link.
local-unit	Names the cluster member.
mtu cluster-interface	Specifies the ma ximum transmission unit for the cluster control link interface.
priority (cluster group)	Sets the priority of this unit for master unit elections.

priority (vpn load balancing)

To set the priority of the local device participating in the virtual load-balancing cluster, use the **priority** command in VPN load-balancing mode. To revert to the default priority specification, use the **no** form of this command.

priority *priority*
no priority

Syntax Description

priority	The priority, in the range of 1 to 10, that you want to assign to this device.

Command Default

The default priority depends on the model number of the device:

Model Number	Default Priority
5520	5
5540	7

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
VPN load-balancing	—	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

You must first use the **vpn load-balancing** command to enter VPN load-balancing mode.

This command sets the priority of the local device participating in the virtual load-balancing cluster.

The priority must be an integer in the range of 1 (lowest) to 10 (highest).

The priority is used in the master-election process as one way to determine which of the devices in a VPN load-balancing cluster becomes the master or primary device for the cluster. See CLI configuration guide for details about the master-election process.

The **no** form of the command reverts the priority specification to the default value.

Examples

The following is an example of a VPN load-balancing command sequence that includes a **priority** command that sets the priority of the current device to 9:

```
ciscoasa(config)# interface GigabitEthernet 0/1
ciscoasa(config-if)# ip address 209.165.202.159 255.255.255.0
ciscoasa(config)# nameif test
ciscoasa(config)# interface GigabitEthernet 0/2
ciscoasa(config-if)# ip address 209.165.201.30 255.255.255.0
ciscoasa(config)# nameif foo
ciscoasa(config)# vpn load-balancing
ciscoasa(config-load-balancing)# priority 9
ciscoasa(config-load-balancing)# interface lbpublic test
ciscoasa(config-load-balancing)# interface lbprivate foo
ciscoasa(config-load-balancing)# cluster ip address 209.165.202.224
ciscoasa(config-load-balancing)# participate
```

Related Commands

Command	Description
vpn load-balancing	Enter VPN load-balancing mode.

priority-queue

To create a standard priority queue on an interface for use with the **priority** command, use the **priority-queue** command in global configuration mode. To remove the queue, use the **no** form of this command.

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

priority-queue *interface-name*
no priority-queue *interface-name*

Syntax Description

interface-name	Specifies the name of the physical interface on which you want to enable the priority queue, or for the ASA 5505 or ASASM, the name of the VLAN interface.

Command Default

By default, priority queuing 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
7.0(1)	This command was added.
8.2(3)/8.4(1)	Support for Ten Gigabit Ethernet interfaces was added for the ASA 5585-X.

Usage Guidelines

LLQ priority queuing lets you prioritize certain traffic flows (such as latency-sensitive traffic like voice and video) ahead of other traffic.

The ASA supports two types of priority queuing:

- Standard priority queuing—Standard priority queuing uses an LLQ priority queue on an interface that yopu create using the **priority-queue** command, while all other traffic goes into the “best effort” queue. 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 called *tail drop* . To avoid having the queue fill up, you can increase the queue buffer size (the **queue-limit** command). You can also fine-tune the maximum number of packets allowed into the transmit queue (the **tx-ring-limit** command). These options

let you control the latency and robustness of the priority queuing. Packets in the LLQ queue are always transmitted before packets in the best effort queue.

- Hierarchical priority queuing—Hierarchical priority queuing is used on interfaces on which you enable a traffic shaping queue. A subset of the shaped traffic can be prioritized. The standard priority queue is not used.

Note On the ASA 5505 only, configuring a priority queue on one interface overwrites the same configuration on all other interfaces; only the last applied configuration is present on all interfaces. Also, 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 (CSCsi13132).

Examples

The following example configures a priority queue for the interface named test, specifying a queue limit of 30,000 packets and a transmit queue limit of 256 packets.

```
ciscoasa(config)# priority-queue test
ciscoasa(priority-queue)# queue-limit 30000
ciscoasa(priority-queue)# tx-ring-limit 256
ciscoasa(priority-queue)#
```

Related Commands

Command	Description
queue-limit	Specifies the maximum number of packets that can be enqueued to a priority queue before it drops data.
tx-ring-limit	Sets the maximum number of packets that can be queued at any given time in the Ethernet transmit driver.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
clear configure priority-queue	Removes the current priority queue configuration.
show running-config [all] 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 configuration values.

privilege

To configure command privilege levels for use with command authorization (local, RADIUS, and LDAP (mapped) only), use the **privilege** command in global configuration mode. To disallow the configuration, use the **no** form of this command.

privilege [**show** | **clear** | **configure**] **level** *level* [**mode** *cli_mode*] **command** *command*
no privilege [**show** | **clear** | **configure**] **level** *level* [**mode** *cli_mode*] **command** *command*

Syntax Description

clear	(Optional) Sets the privilege only for the clear form of the command. If you do not use the **clear**, **show**, or **configure** keywords, all forms of the command are affected.
command *command*	Specifies the command you are configuring. You can only configure the privilege level of the *main* command. For example, you can configure the level of all **aaa** commands, but not the level of the **aaa authentication** command and the **aaa authorization** command separately.
configure	(Optional) Sets the privilege only for the configure form of the command. The configure form of the command is typically the form that causes a configuration change, either as the unmodified command (without the **show** or **clear** prefix) or as the **no** form. If you do not use the **clear**, **show**, or **configure** keywords, all forms of the command are affected.
level *level*	Specifies the privilege level; valid values are from 0 to 15. Lower privilege level numbers are lower privilege levels.
mode *cli_mode*	(Optional) If a command can be entered in multiple CLI modes, such as user EXEC/privileged EXEC mode, global configuration mode, or a command configuration mode, then you can set the privilege level for these modes separately. If you do not specify the mode, then all versions of the command use the same level. See the following modes: • **exec**—Specifies both user EXEC mode and privileged EXEC mode. • **configure**—Specifies global configuration mode, accessed using the **configure terminal** command. • *command_config_mode* —Specifies a command configuration mode, accessed using the command name in global or another command configuration mode. For example, the **mac-address** command can be entered in both global and interface configuration mode. The mode keyword lets you set the level separately for each mode. You cannot use this command to set the level for a command
show	(Optional) Sets the privilege only for the show form of the command. If you do not use the **clear**, **show**, or **configure** keywords, all forms of the command are affected.

Command Default

By default, the following commands are assigned to privilege level 0. All other commands are at level 15.

- **show checksum**
- **show curpriv**
- **enable**

- **help**
- **show history**
- **login**
- **logout**
- **pager**
- **show pager**
- **clear pager**
- **quit**
- **show version**

If you move any configure mode commands to a lower level than 15, be sure to move the **configure** command to that level as well, otherwise, the user will not be able to enter configuration mode.

To view all privilege levels, see the **show running-config all privilege all** 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	• Yes	—

Command History

Release	Modification
8.0(2)	Support for RADIUS users with Cisco VSA CVPN3000-Privilege-Level was added. LDAP users are supported if you map the LDAP attribute to the CVPN3000-Privilege-Level using the **ldap map-attributes** command.

Usage Guidelines

The **privilege** command lets you set privilege levels for ASA commands when you configure the **aaa authorization command LOCAL** command. Even though the command uses the **LOCAL** keyword, this keyword enables local, RADIUS, and LDAP (mapped) authorization.

Examples

For example, the **filter** command has the following forms:

- **filter** (represented by the **configure** option)
- **show running-config filter**
- **clear configure filter**

You can set the privilege level separately for each form, or set the same privilege level for all forms by omitting this option. For example, set each form separately as follows:

```
ciscoasa(config)# privilege
 show
 level
 5
 command
 filter
ciscoasa(config)# privilege
 clear
 level
 10
 command
 filter
ciscoasa(config)# privilege
 cmd
 level
 10
 command
 filter
```

Alternatively, you can set all filter commands to the same level:

```
ciscoasa(config)# privilege
 level
 5
 command
 filter
```

The **show privilege** command separates the forms in the display.

The following example shows the use of the **mode** keyword. The **enable** command must be entered from user EXEC mode, while the **enable password** command, which is accessible in configuration mode, requires the highest privilege level.

```
ciscoasa(config)# privilege cmd level 0 mode exec command enable
ciscoasa(config)# privilege cmd level 15 mode configure command enable
ciscoasa(config)# privilege show level 15 mode configure command enable
```

The following example shows the **mac-address** command in two modes, and different levels for show, clear, and cmd versions :

```
ciscoasa(config)# privilege cmd level 10 mode configure command mac-address
ciscoasa(config)# privilege cmd level 15 mode interface command mac-address
ciscoasa(config)# privilege clear level 10 mode configure command mac-address
ciscoasa(config)# privilege clear level 15 mode interface command mac-address
ciscoasa(config)# privilege show level 2 mode configure command mac-address
ciscoasa(config)# privilege show level 2 mode interface command mac-address
```

Related Commands

Command	Description
clear configure privilege	Removes privilege command statements from the configuration.
show curpriv	Displays current privilege level.
show running-config privilege	Displays privilege levels for commands.

profile

To create or edit a call-home profile, use the **profile** command in call-home configuration mode. To remove one or all of the configured call-home profiles, use the **no** form of this command specifying one or all of the profiles. You can access the call-home configuration mode by first entering the **call-home** command.

profile *profile-name*
no profile { *profile-name* | **all** }

Syntax Description

profile-name	Name of the profile, up to 20 characters long.
all	Includes all configured profiles.

Command Default

A default profile, **Cisco TAC**, has been provided. The default profile has a predefined set of groups (diagnostic, environment, inventory, configuration, and telemetry) to monitor and predefined destination e-mail and HTTPS URLs. The default profile is created automatically when you initially configure Smart Call Home. The destination e-mail is callhome@cisco.com and the destination URL is https://tools.cisco.com/its/service/oddce/services/DDCEService.

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
call-home configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
8.2(1)	We introduced this command.
8.2(2)	Added the keyword all.
9.3(2)	We added the **License** profile for Smart Software Licensing.
9.6(2)	Introduced the reference-identity option for **destination address http**.

Usage Guidelines

The following commands are used in profile configuration mode.

Enable or Disable a Profile

To enable a call-home profile, use the **active** command in call-home-profile configuration mode. To disable a call-home profile, use the **no active** command in call-home-profile configuration mode. You can access the call-home-profile configuration mode by first entering the **call-home** then **profile** command. The default is enabled.

active

no active

Set Profile Commands to Default

To set the call home profile settings to their default values use the default command in call-home-profile configuration mode. You can access the call-home-profile configuration mode by first entering the **call-home** then **profile** commands. You can also reset call-home configuration mode settings from this mode. Use command help, **default ?**, to determine and reset all call-home profile and general settings.

default {**activedestinationemail-subjectsubscribe-to-alert-group**}

Destination Type, Address and Settings

To set the destination address, reference identity, message format, and transport method for the Smart Call Home message receiver, use the **destination** command in call-home-profile configuration mode. To remove the destination parameters, or reset them to default, use the **no destination** or **default** command.

The default message format is XM, the default message size is 5MB (0 means unlimited), and the default transport method is e-mail. You must specify a previously configured reference identity. This is used to validate the call-home server's certificate when connecting. It applies to http destinations only.

destination address {**e-mail** *e-mail-address***http** *http-url*}
no destination address {**e-mailhttp** [**all**]}
destination address http *http-url* **reference-identity** *ref-id-name*
no destination address http *http-url* **reference-identity** *ref-id-name*
destination address {**e-mail** *e-mail-address***http** *http-url*} **msg-format** {**short-textlong-textxml**}
no destination address {**e-mail** *e-mail-address***http** *http-url*} **msg-format** {**short-textlong-textxml**}
destination message-size-limit *max-size*
no destination message-size-limit *max-size*
destination preferred-msg-format {**short-textlong-textxml**}
no destination preferred-msg-format {**short-textlong-textxml**}
destination transport-method {**e-mailhttp**}
no destination transport-method {**e-mailhttp**}

Configure E-mail Subject

To set a prefix or suffix on the email subject for call-home email, use the **email-subject** command in call-home-profile configuration mode. To clear these fields use the **no email-subject** command. You can access the call-home-profile configuration mode by first entering the **call-home** then **profile** command.

email-subject {**appendprepend**} *chars*
no email-subject {**appendprepend**} *chars*

Subscribe to an alert group

To subscribe to an alert group use the s**ubscribe-to-alert-group** command in call-home-profile configuration mode. To clear these subscriptions use the no s**ubscribe-to-alert-group** command. You can access the call-home-profile configuration mode by first entering the **call-home** then **profile** command.

- [no] subscribe-to-alert-group alert-group-name [severity {catastrophic | disaster | emergencies | alert | critical | errors | warning | notifications | informational | debugging}]—Subscribes to events of a group with a specified severity level.alert-group-name: Syslog, diagnostic, environment, or threat are valid values.
- [no] subscribe-to-alert-group syslog [{severity {catastrophic | disaster | emergencies | alert | critical | errors | warning | notifications | informational | debugging} | message start [-end]}]—Subscribes to syslogs

with a severity level or message ID.start-[end]: One syslog message ID or a range of syslog message IDs.

Note Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debugging** only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Also, use it during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood of increasing the processing overhead that will affect system use.

- [no] subscribe-to-alert-group inventory [periodic {daily | monthly day_of_month | weekly day_of_week [hh:mm]]—Subscribes to inventory events.day_of_month: Day of the month, 1-31.day_of_week: Day of the week (Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday).hh, mm: Hours and minutes of a day, in 24-hour time.
- [no] subscribe-to-alert-group configuration [export full | minimum] [periodic {daily | monthly day_of_month | weekly day_of_week [hh:mm]]—Subscribes to configuration events.full: Configuration to export the running configuration, startup configuration, feature list, number of elements in an access list, and the context name in multimode.minimum: Configuration to export-only feature list, number of elements in an access list, and the context name in multimode.day_of_month: Day of the month, 1-31.day_of_week: Day of the week (Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday).hh, mm: Hours and minutes of a day, in 24-hour time.
- [no] subscribe-to-alert-group telemetry periodic {hourly | daily | monthly day_of_month | weekly day_of_week [hh:mm]—Subscribes to telemetry periodic events.day_of_month: Day of the month, 1-31.day_of_week: Day of the week (Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday).hh, mm: Hours and minutes of a day, in 24-hour time.
- [no] subscribe-to-alert-group snapshot periodic {interval minutes | hourly [mm] | daily | monthly day_of_month |weekly day_of_week [hh:mm]}—Subscribes to snapshot periodic events.minutes: The interval in minutes.day_of_month: Day of the month, 1-31.day_of_week: Day of the week (Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday).hh, mm: Hours and minutes of a day, in 24-hour time.

Related Commands

Command	Description
call-home	Puts the user into call home configuration mode
show call-home	Displays Call Home configuration information.
reference-identity	Configures a reference identity object.

prompt

To customize the CLI prompt, use the prompt command in global configuration mode. To revert to the default prompt, use the no form of this command.

prompt { [**hostname**] [**context**] [**domain**] [**slot**] [**state**] [**priority**] [**cluster-unit**]
no prompt [**hostname**] [**context**] [**domain**] [**slot**] [**state**] [**priority**] [**cluster-unit**]

Syntax Description

cluster-unit	Displays the cluster unit name. Each unit in a cluster can have a unique name.
context	(Multiple mode only) Displays the current context.
domain	Displays the domain name.
hostname	Displays the hostname.
priority	Displays the failover priority as pri (primary) or sec (secondary). Set the priority using the **failover lan unit** command.
state	Displays the traffic-passing state or role of the unit. For failover, the following values are displayed for the **state** keyword: • act—Failover is enabled, and the unit is actively passing traffic. • stby— Failover is enabled, and the unit is not passing traffic and is in a standby, failed, or other non-active state. • actNoFailover—Failover is not enabled, and the unit is actively passing traffic. • stbyNoFailover—Failover is not enabled, and the unit is not passing traffic. This might happen when there is an interface failure above the threshold on the standby unit. For clustering, the following values are displayed for the **state** keyword: • control node • data node For example, if you set **prompt hostname cluster-unit state**, then in the prompt "ciscoasa/cl2/data node>", the hostname is ciscoasa, the unit name is cl2, and the state name is data node.

Command Default

The default prompt is the hostname. In multiple context mode, the hostname is followed by the current context name (*hostname* /*context*).

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
7.2(1)	This command was added.
9.0(1)	The **cluster-unit** option was added. The **state** keyword was updated for clustering.
9.19(1)	For clustering, the **state** display was changed from **master** and **slave** to **control node** and **data node**.

Usage Guidelines

The order in which you enter the keywords determines the order of the elements in the prompt, which are separated by a slash (/).

In multiple context mode, you can view the extended prompt when you log in to the system execution space or the admin context. Within a non-admin context, you only see the default prompt, which is the hostname and the context name.

The ability to add information to a prompt allows you to see at-a-glance which ASA you are logged into when you have multiple modules. During a failover, this feature is useful when both ASAs have the same hostname.

Examples

The following example shows all available elements in the prompt available for failover:

```
ciscoasa(config)# prompt hostname context slot state priority
```

The prompt changes to the following string:

```
ciscoasa/admin/pri/act(config)#
```

Related Commands

Command	Description
clear configure prompt	Clears the configured prompt.
show running-config prompt	Displays the configured prompt.

propagate sgt

To enable propagation of a security group tag (called **sgt**) on an interface, use the **propagate sgt** command in cts manual interface configuration mode. To disable propagation of a security group tag (called **sgt**) on an interface, use the **no** form of this command.

propagate sgt
no propagate sgt

Syntax Description

This command has no arguments or keywords.

Command Default

Propagation 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
Cts manual interface configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.3(1)	This command was added.

Usage Guidelines

This command enables and disables the propagation of a security group tag in CTS Layer 2 SGT Imposition.

Restrictions

- Supported only on physical interfaces, VLAN interfaces, port channel interfaces, and redundant interfaces.
- Not supported on logical interfaces or virtual interfaces, such as BVI, TVI, and VNI.

Examples

The following example enables an interface for Layer 2 SGT imposition and indicates that the SGT is not being propagated:

```
ciscoasa(config)# interface gi0/0
ciscoasa(config-if)# cts manual

ciscoasa(config-if-cts-manual)# no propagate sgt
```

Related Commands

Command	Description
cts manual	Enables Layer 2 SGT Imposition and enters cts manual interface configuration mode.

Command	Description
policy static sgt	Applies a policy to a manually configured CTS link.

protocol

To specify the protocol and encryption types for an IPsec proposal for IKEv2 connections, use the **protocol** command from IPsec proposal configuration mode. To remove the protocol and encryption types, use the no form of the command:

protocol esp { **encryption** { **des** | **3des** | **aes** | **aes-192** | **aes-256** | **aes-gcm** | **aes-gcm-192** | **aes-gcm-256** | **aes-gmac** | **aes-gmac-192** | **aes-gmac-256** | **null** } | **integrity** { **md5** | **sha-1** | **sha-256** | **sha-384** | **sha-512** | **null** }
no protocol esp { **encryption** { **des** | **3des** | **aes** | **aes-192** | **aes-256** | **aes-gcm** | **aes-gcm-192** | **aes-gcm-256** | **aes-gmac** | **aes-gmac-192** | **aes-gmac-256** | **null** } | **integrity** { **md5** | **sha-1** | **sha-256** | **sha-384** | **sha-512** | **null** }

Syntax Description

esp	Specifies the Encapsulating Security Payload (ESP) IPsec protocol (currently the only supported protocol for IPsec).
des	Specifies 56-bit DES-CBC encryption for ESP.
3des	(Default) Specifies the triple DES encryption algorithm for ESP.
aes	Specifies AES with a 128-bit key encryption for ESP.
aes-192	Specifies AES with a 192-bit key encryption for ESP.
aes-256	Specifies AES with a 256-bit key encryption for ESP.
aes-gcm	Specifies which AES-GCM or AES-GMAC algorithm to use.
aes-gcm-192	Specifies which AES-GCM or AES-GMAC algorithm to use.
aes-gcm-256	Specifies which AES-GCM or AES-GMAC algorithm to use.
aes-gmac	Specifies which AES-GCM or AES-GMAC algorithm to use.
aes-gmac-192	Specifies which AES-GCM or AES-GMAC algorithm to use.
aes-gmac-256	Specifies which AES-GCM or AES-GMAC algorithm to use.
null	Does not use encryption for ESP.
integrity	Specifies the integrity algorithm for the IPsec protocol.
md5	Specifies the md5 algorithm for the ESP integrity protection.
sha-1	(Default) Specifies the Secure Hash Algorithm (SHA) SHA-1, defined in the U.S. Federal Information Processing Standard (FIPS), for ESP integrity protection.
sha-256	Specifies which algorithm to use as an IPsec integrity algorithm.
sha-384	Specifies which algorithm to use as an IPsec integrity algorithm.
sha-512	Specifies which algorithm to use as an IPsec integrity algorithm.

null	Choose if AES-GCM/GMAC is configured as the encryption algorithm.

Command Default

The default settings for an IPsec proposal are the encryption type 3DES and the integrity type SHA-1.

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
IPsec proposal configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.4(1)	This command was added.
9.0(1)	Support for AES-GCM or AES-GMAC algorithm was added. The ability to choose an algorithm to use as an IPsec integrity algorithm was added.

Usage Guidelines

IKEv2 IPsec proposals can have multiple encryption and integrity types. Use this command to specify the types, which allows the peer to pick and choose as desired.

You must choose the null integrity algorithm if AES-GMC/GMAC is configured as the encryption algorithm.

Examples

The following example creates the IPsec proposal proposal_1, configures the ESP encryption types DES and 3DES, and specifies the crypto algorithms MD5 and SHA-1 for integrity protection:

```
ciscoasa(config)# crypto ipsec ikev2 ipsec-proposal proposal_1
ciscoasa(config-ipsec-proposal)# protocol ESP encryption des 3des
ciscoasa(config-ipsec-proposal)# protocol ESP integrity md5 sha-1
```

Related Commands

Command	Description
crypto ikev2 enable	Enables ISAKMP IKEv2 negotiation on the interface on which the IPsec peer communicates.
crypto ipsec ikev2 ipsec-proposal	Creates an IPsec proposal and enters IPsec proposal configuration mode where you specify multiple encryption and integrity types for the proposal.
show running-config ipsec	Displays the configuration of all transform sets.
crypto map set transform-set	Specifies the transform sets to use in a crypto map entry.
crypto dynamic-map set transform-set	Specifies the transform sets to use in a dynamic crypto map entry.
show running-config crypto map	Displays the crypto map configuration.

Command	Description
show running-config crypto dynamic-map	Displays the dynamic crypto map configuration.

protocol-enforcement

To enable the domain name, label length, and format check, including compression and looped pointer check, use the **protocol-enforcement** command in parameters configuration mode. To disable protocol enforcement, use the **no** form of this command.

protocol-enforcement
no protocol-enforcement

Syntax Description

This command has no arguments or keywords.

Command Default

Protocol enforcement is enabled by default. This feature can be enabled when **inspect dns** is configured even if a **policy-map type inspect dns** is not defined. To disable, **no protocol-enforcement** must explicitly be stated in the policy map configuration. If **inspect dns** is not configured, NAT rewrite is not performed.

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

Under certain conditions, protocol enforcement is performed even if the command is disabled. This occurs when parsing a DNS resource record is required for other purposes, such as DNS resource record classification, NAT or TSIG check.

Examples

The following example shows how to enable protocol 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)# protocol-enforcement
```

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.

protocol http

To specify HTTP as a permitted distribution point protocol for retrieving a CRL, use the **protocol http** command in ca-crl configuration mode. To remove HTTP as the permitted method of CRL retrieval, use the **no** form of this command.

protocol http
no protocol http

Syntax Description

This command has no arguments or keywords.

Command Default

The default setting is to permit HTTP.

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
Ca-crl configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

If you use this command, be sure to assign HTTP rules to the public interface filter. Subject to permission, the content of the CRL distribution point determines the retrieval method (HTTP, LDAP, and/or SCEP).

Examples

The following example enters ca-crl configuration mode, and permits HTTP as a distribution point protocol for retrieving a CRL for trustpoint central:

```
ciscoasa(configure)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# protocol http
```

Related Commands

Command	Description
crl configure	Enters ca-crl configuration mode.
crypto ca trustpoint	Enters trustpoint configuration mode.
protocol ldap	Specifies LDAP as a retrieval method for CRLs.
protocol scep	Specifies SCEP as a retrieval method for CRLs.

protocol ldap

To specify LDAP as a distribution point protocol for retrieving a CRL, use the **protocol ldap** command in ca-crl configuration mode. Subject to permission, the content of the CRL distribution point determines the retrieval method (HTTP, LDAP, and/or SCEP).

To remove the LDAP protocol as the permitted method of CRL retrieval, use the **no** form of this command.

protocol ldap
no protocol ldap

Syntax Description

This command has no arguments or keywords.

Command Default

The default setting is to permit LDAP.

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
crl configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example enters ca-crl configuration mode, and permits LDAP as a distribution point protocol for retrieving a CRL for trustpoint central:

```
ciscoasa(configure)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# protocol ldap
```

Related Commands

Command	Description
crl configure	Enters ca-crl configuration mode.
crypto ca trustpoint	Enters trustpoint configuration mode.
protocol http	Specifies HTTP as a retrieval method for CRLs
protocol scep	Specifies SCEP as a retrieval method for CRLs

protocol-object

To add a protocol object to a protocol object group, use the protocol-object command in protocol configuration mode. To remove port objects, use the **no** form of this command.

protocol-object *protocol*
no protocol-object *protocol*

Syntax Description

protocol	Protocol name or number.

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
Protocol configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **protocol-object** command is used with the **object-group** command to define a protocol object in protocol configuration mode.

You can specify an IP protocol name or number using the *protocol* argument. The udp protocol number is 17, the tcp protocol number is 6, and the egp protocol number is 47.

Examples

The following example shows how to define protocol objects:

```
ciscoasa(config)# object-group protocol proto_grp_1
ciscoasa(config-protocol)# protocol-object udp
ciscoasa(config-protocol)# protocol-object tcp
ciscoasa(config-protocol)# exit
ciscoasa(config)# object-group protocol proto_grp
ciscoasa(config-protocol)# protocol-object tcp
ciscoasa(config-protocol)# group-object proto_grp_1
ciscoasa(config-protocol)# exit
ciscoasa(config)#
```

Related Commands

Command	Description
clear configure object-group	Removes all the object group commands from the configuration.

Command	Description
group-object	Adds network object groups.
network-object	Adds a network object to a network object group.
object-group	Defines object groups to optimize your configuration.
show running-config object-group	Displays the current object groups.

protocol scep

To specify SCEP as a distribution point protocol for retrieving a CRL, use the **protocol scep** command in crl configure mode. Subject to permission, the content of the CRL distribution point determines the retrieval method (HTTP, LDAP, and/or SCEP).

To remove the SCEP protocol as the permitted method of CRL retrieval, use the **no** form of this command.

protocol scep
no protocol scep

Syntax Description

This command has no arguments or keywords.

Command Default

The default setting is to permit SCEP.

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
Crl configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example enters ca-crl configuration mode, and permits SCEP as a distribution point protocol for retrieving a CRL for trustpoint central:

```
ciscoasa(configure)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# protocol scep
ciscoasa(ca-crl)#
```

Related Commands

Command	Description
crl configure	Enters ca-crl configuration mode.
crypto ca trustpoint	Enters trustpoint configuration mode.
protocol http	Specifies HTTP as a retrieval method for CRLs.
protocol ldap	Specifies LDAP as a retrieval method for CRLs.

protocol shutdown

To disable the IS-IS protocol so that it cannot form any adjacency on any interface and will clear the IS-IS LSP database, use the **protocol shutdown** command in router isis configuration mode. To reenable the IS-IS protocol, use the **no** form of this command

protocol shutdown
no protocol shutdown

Syntax Description

This command has no arguments or keywords.

Command Default

This command has 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
Router isis configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(1)	This command was added.

Usage Guidelines

This command allows you to disable the IS-IS protocol for a specific routing instance without removing any existing IS-IS configurations parameters. When you enter the **protocol shutdown** command, the IS-IS protocol continues to run on the ASA, and you can use the current IS-IS configuration, but IS-IS does not form any adjacencies on any interface, and it also clears the IS-IS LSP database.

If you want to disable the IS-IS protocol for a specific interface, use the **isis protocol shutdown** command.

Examples

The following example disables the IS-IS protocol for a specific routing instance:

```
ciscoasa(config)# router isis
ciscoasa(config-router)# protocol shutdown
```

Related Commands

protocol-violation

To define actions when a protocol violation occurs with HTTP and NetBIOS inspection, use the **protocol-violation** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

protocol-violation action [**drop** [**log**] | **log**]
no protocol-violation action [**drop** [**log**] | **log**]

Syntax Description

drop	Specifies to drop packets that do not conform to the protocol.
log	Specifies to log the protocol violations.

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
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This command can be configured in an HTTP or NetBIOS policy map. A syslog is issued when the HTTP or NetBIOS parser cannot detect a valid HTTP or NetBIOS message in the first few bytes of the message. This occurs, for instance, when a chunked encoding is malformed and the message cannot be parsed.

Examples

The following example shows how to set up an action for protocol violation in a policy map:

```
ciscoasa(config)# policy-map type inspect http http_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# protocol-violation action drop
```

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.

proxy-auth

To flag the tunnel group as a specific proxy authentication tunnel group, use the **proxy-auth** command in webvpn configuration mode.

proxy-auth [**sdi**]

Syntax Description

sdi	Parses RADIUS/TACACS SDI proxy messages into native SDI directives.

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	—	—

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

Use the **proxy-auth** command for enabling the parsing of aaa-server proxy authentication text messages into native protocol directives.

proxy-auth_map sdi

To map RADIUS challenge messages returned from a RADIUS proxy server to native SDI messages, use the **proxy-auth_map sdi** command in aaa-server configuration mode.

proxy-auth_map sdi [**sdi_message**] [**radius_challenge_message**]

Syntax Description

radius_challenge_message	Specifies the RADIUS challenge messages that are used to map specific SDI messages, which can any of the following: • new-pin-meth—New PIN Method, [default] Do you want to enter your own pin • new-pin-reenter—Reenter new PIN, [default] Reenter PIN: • new-pin-req—New PIN requested, [default] Enter your new Alpha-Numerical PIN • new-pin-sup—New PIN supplied, [default] Please remember your new PIN • new-pin-sys-ok—New PIN accepted, [default] New PIN Accepted • next-ccode-and-reauth—Reauthenticate on token change, [default] new PIN with the next card code • next-code—Provide the tokencode without PIN, [default] Enter Next PASSCODE • ready-for-sys-pin—Accept system generated PIN, [default] ACCEPT A SYSTEM GENERATED PIN
sdi_message	Specifies the native SDI messages.

Command Default

The default mapping on the ASA corresponds to default settings on the Cisco ACS (including the system administration, configuration, and RSA SecureID prompts), which also synchronizes with default settings on the RSA Authentication Manager.

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
Aaa-server configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

To enable parsing and mapping of RADIUS challenge messages from a RADIUS proxy, you must enable the **proxy-auth** command in tunnel-group configuration mode. Then default mapping values are used. You can change the default mapping values using the **proxy-auth_map** command.

A remote user connects to the ASA with the Secure Client and tries to authenticate using an RSA SecurID token. The ASA can be configured to use a RADIUS proxy server which in turn, communicates with the SDI server about that authentication.

During authentication, the RADIUS server presents access challenge messages to the ASA. Within these challenge messages are reply messages containing text from the SDI server. The message text is different when the ASA is communicating directly with an SDI server than when the ASA is communicating through the RADIUS proxy.

Therefore, to appear as a native SDI server to the Secure Client, the ASA must interpret the messages from the RADIUS server. Also, because the SDI messages are configurable on the SDI server, the message text on the ASA must match (in whole or in part) the message text on the SDI server. Otherwise, the prompts displayed to the remote client user may not be appropriate for the action required during authentication. The Secure Client might fail to respond, and authentication might fail.

Related Commands

Command	Description
proxy-auth	Enables parsing and mapping of RADIUS challenge messages from a RADIUS proxy.

proxy-bypass

To configure the ASA to perform minimal content rewriting, and to specify the types of content to rewrite—external links and/or XML—use the **proxy-bypass** command in webvpn configuration mode. To disable proxy bypass, use the **no** form of the command.

proxy-bypass interface *interface name* { **port** *port number* | **path-mask** *path mask* } **target** *url* [**rewrite** { **link** | **xml** | **none**] }
no proxy-bypass interface *interface name* { **port** *port number* | **path-mask** *path mask* } **target** *url* [**rewrite** { **link** | **xml** | **none**] }

Syntax Description

host	Identifies the host to forward traffic to. Use either the host IP address or a hostname.
interface	Identifies the ASA interface for proxy bypass.
interface name	Specifies an ASA interface by name.
link	Specifies rewriting of absolute external links.
none	Specifies no rewriting.
path-mask	Specifies the pattern to match.
path-mask	Specifies a pattern to match that can contain a regular expression. You can use the following wildcards: * — Matches everything. You cannot use this wildcard by itself. It must accompany an alphanumeric string. ? —Matches any single character. [!seq] — Matches any character not in sequence. [seq] — Matches any character in sequence. Maximum 128 bytes.
port	Identifies the port reserved for proxy bypass.
port number	Specifies a high numbered port reserved for proxy bypass. The port range is 20000-21000. You can use a port for one proxy bypass rule only.
rewrite	(Optional) Specifies the additional rules for rewriting: none or a combination of XML and links.
target	Identifies the remote server to forward the traffic to.
url	Enter the URL in the format **http(s)://***fully_qualified_domain_name*[:*port*]. Maximum 128 bytes. The port for HTTP is 80 and for HTTPS it is 443, unless you specify another port.
xml	Specifies rewriting XML content.

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	—	—

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

Use proxy bypass for applications and web resources that work better with minimum content rewriting. The proxy-bypass command determines how to treat specific web applications that travel through the ASA.

You can use this command multiple times. The order in which you configure entries is unimportant. The interface and path mask or interface and port uniquely identify a proxy bypass rule.

If you configure proxy bypass using ports rather than path masks, depending on your network configuration, you might need to change your firewall configuration to allow these ports access to the ASA. Use path masks to avoid this restriction. Be aware, however, that path masks can change, so you might need to use multiple pathmask statements to exhaust the possibilities.

A path is everything in a URL after the .com or .org or other types of domain name. For example, in the URL www.example.com/hrbenefits, *hrbenefits* is the path. Similarly, for the URL www.example.com/hrinsurance, *hrinsurance* is the path. If you want to use proxy bypass for all hr sites, you can avoid using the command multiple times by using the * wildcard as follows: /hr*.

Examples

The following example shows how to configure the ASA to use port 20001 for proxy bypass over the webvpn interface, using HTTP and its default port 80, to forward traffic to example.com and to rewrite XML content.

```
ciscoasa
(config)#
 webvpn
ciscoasa
(config-webvpn)#
 proxy-bypass interface webvpn port 20001 target http://example.com rewrite xml
```

The next example shows how to configure the ASA to use the path mask mypath/* for proxy bypass on the outside interface, using HTTP and its default port 443 to forward traffic to example.com, and to rewrite XML and link content.

```
ciscoasa
(config)#
 webvpn
ciscoasa
(config-webvpn)#
 proxy-bypass interface outside path-mask /mypath/* target https://example.com rewrite
xml,link
```

Related Commands

Command	Description
apcf	Specifies nonstandard rules to use for a particular application.
rewrite	Determines whether traffic travels through the ASA.

proxy-ldc-issuer

To issue TLS proxy local dynamic certificates, use the proxy-ldc-issuer command in crypto ca trustpoint configuration mode. To remove the configuration, use the **no** form of this command.

proxy-ldc-issuer
no proxy-ldc-issuer

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
Crypto ca trustpoint configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

Use the proxy-ldc-issuer command to issue TLS proxy local dynamic certificates. The proxy-ldc-issuer command grants a crypto trustpoint the role as local CA to issue the LDC and can be accessed from crypto ca trustpoint configuration mode.

The proxy-ldc-issuer command defines the local CA role for the trustpoint to issue dynamic certificates for TLS proxy. This command can only be configured under a trustpoint with “enrollment self.”

Examples

The following example shows how to create an internal local CA to sign the LDC for phones. This local CA is created as a regular self-signed trustpoint with proxy-ldc-issuer enabled.

```
ciscoasa(config)# crypto ca trustpoint ldc_server
ciscoasa(config-ca-trustpoint)# enrollment self
ciscoasa(config-ca-trustpoint)# proxy-ldc-issuer
ciscoasa(config-ca-trustpoint)# fqdn my _ldc_ca.example.com
ciscoasa(config-ca-trustpoint)# subject-name cn=FW_LDC_SIGNER_172_23_45_200
ciscoasa(config-ca-trustpoint)# keypair ldc_signer_key
ciscoasa(config)# crypto ca enroll ldc_server
```

Related Commands

Commands	Description
ctl-provider	Defines a CTL provider instance and enters provider configuration mode.

Commands	Description
server trust-point	Specifies the proxy trustpoint certificate to be presented during the TLS handshake.
show tls-proxy	Shows the TLS proxies.
tls-proxy	Defines a TLS proxy instance and sets the maximum sessions.

proxy paired

To set the VNI interface to paired proxy mode for the ASA virtual on Azure for the Azure Gateway Load Balancer (GWLB), use the **proxy paired** command in interface configuration mode. To remove the proxy, use the **no** form of this command.

proxy paired
no proxy paired

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
9.19(1)	This command was added.

Usage Guidelines

In an Azure service chain, ASA virtuals act as a transparent gateway that can intercept packets between the internet and the customer service. The ASA virtual defines an external interface and an internal interface on a single NIC by utilizing VXLAN segments in a paired proxy.

Examples

The following example configures the VNI 1 interface for Azure GWLB:

```
ciscoasa(config)# interface vni 1
ciscoasa(config-if)# proxy paired
ciscoasa(config-if)# internal-segment-id 1000
ciscoasa(config-if)# external-segment-id 1001
ciscoasa(config-if)# internal-port 101
ciscoasa(config-if)# external-port 102
ciscoasa(config-if)# vtep-nve 1
ciscoasa(config-if)# nameif vxlan1000
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
ciscoasa(config-if)# security-level 50
```

Related Commands

Command	Description
debug vxlan	Debugs VXLAN traffic.

Command	Description
encapsulation vxlan	Sets the NVE instance to VXLAN encapsulation.
external-port	Sets the external VXLAN port.
external-segment-id	Specifies the VXLAN external segment ID for a VNI interface.
inspect vxlan	Enforces compliance with the standard VXLAN header format.
interface vni	Creates the VNI interface for VXLAN tagging.
internal-port	Sets the internal VXLAN port.
internal-segment-id	Specifies the VXLAN internal segment ID for a VNI interface.
nve	Specifies the Network Virtualization Endpoint instance.
peer ip	Manually specifies the peer VTEP IP address.
show interface vni	Shows the parameters, status and statistics of a VNI interface, status of its bridged interface (if configured), and NVE interface it is associated with.
show nve	Shows the parameters, status and statistics of a NVE interface, status of its carrier interface (source interface), IP address of the carrier interface, VNIs that use this NVE as the VXLAN VTEP, and peer VTEP IP addresses associated with this NVE interface.
source-interface	Specifies the VTEP source interface.
vtep-nve	Associates a VNI interface with the VTEP source interface.
vxlan port	Sets the VXLAN UDP port. By default, the VTEP source interface accepts VXLAN traffic to UDP port 4789.

proxy-server (Deprecated)

To configure an HTTP proxy for the Phone Proxy feature that is written into the IP phone's configuration file under the <proxyServerURL> tag, use the **proxy-server** command in phone-proxy configuration mode. To remove the HTTP proxy configuration from the Phone Proxy, use the **no** form of this command.

proxy-server address *ip_address* [*listen_port*] **interface** *ifc*
no proxy-server address *ip_address* [*listen_port*] **interface** *ifc*

Syntax Description

interface *ifc*	Specifies the interface on which the HTTP proxy resides on the ASA.
ip_address	Specifies the IP address of the HTTP proxy.
listen_port	Specifies the listening port of the HTTP proxy. If not specified, the default will be 8080.

Command Default

If the listen port is not specified, the port is configured to be 8080 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
Phone-proxy configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(4)	The command was added.
9.4(1)	This command was deprecated along with all **phone-proxy** mode commands.

Usage Guidelines

Setting the proxy server configuration option for the Phone Proxy allows for an HTTP proxy on the DMZ or external network in which all the IP phone URLs are directed to the proxy server for services on the phones. This setting accommodates nonsecure HTTP traffic, which is not allowed back into the corporate network.

The *ip_address* you enter should be the global IP address based on where the IP phone and HTTP proxy server is located.

If the proxy server is located in a DMZ and the IP phones are located outside the network, the ASA does a lookup to see if there is a NAT rule and uses the global IP address to write into the configuration file.

You can enter a hostname in the *ip_address* argument when that hostname can be resolved to an IP address by the ASA (for example, DNS lookup is configured) because the ASA will resolve the hostname to an IP address.

By default, the Phone URL Parameters configured under the Enterprise Parameters use an FQDN in the URLs. The parameters might need to be changed to use an IP address if the DNS lookup for the HTTP proxy does not resolve the FQDNs.

To make sure the proxy server URL was written correctly to the IP phones configuration files, check the URL on an IP phone under Settings > Device Configuration > HTTP configuration >Proxy Server URL.

The Phone Proxy does not inspect this HTTP traffic to the proxy server.

If the ASA is in the path of the IP phone and the HTTP proxy server, use existing debugging techniques (such as syslogs and captures) to troubleshoot the proxy server.

You can configure only one proxy server while the Phone Proxy is in use; however, if the IP phones have already downloaded their configuration files after you have configured the proxy server, you must restart the IP phones so that they get the configuration file with the proxy server's address in the file.

Examples

The following example shows the use of the **proxy-server** command to configure the HTTP proxy server for the Phone Proxy:

```
ciscoasa(config-phone-proxy)# proxy-server 192.168.1.2 interface inside
```

Related Commands

Command	Description
phone-proxy	Configures the Phone Proxy instance.

proxy single-arm

To enable single-arm proxy for a VXLAN VNI interface, use the **proxy single-arm** command in interface configuration mode. To disable the proxy, use the **no** form of this command.

proxy single-arm
no proxy single-arm

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
Interface configuration	• Yes	• —	• Yes	• —	—

Command History

Release	Modification
9.17(1)	We added this command.

Usage Guidelines

The AWS Gateway Load Balancer combines a transparent network gateway and a load balancer that distributes traffic and scales virtual appliances on demand. The ASA virtual supports the Gateway Load Balancer centralized control plane with a distributed data plane (Gateway Load Balancer endpoint). This use case requires you to configure the VNI interface as a single-arm proxy. Be sure to also enable **same-security-traffic permit intra-interface** to allow traffic to u-turn out the VTEP source interface.

Examples

The following example configures the VNI interface as a single-arm proxy:

```
ciscoasa(config)# interface vni 1
ciscoasa(config-if)# vtep-nve 1
ciscoasa(config-if)# nameif geneve1000
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0 standby 192.168.1.2
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# proxy single-arm
ciscoasa(config)# same-security-traffic permit intra-interface
```

Related Commands

Command	Description
debug vxlan	Debugs VXLAN traffic.

Command	Description
encapsulation geneve	Sets the NVE instance to Geneve encapsulation.
interface vni	Creates the VNI interface for VXLAN tagging.
nve	Specifies the Network Virtualization Endpoint instance.
nve-only	Specifies that the VXLAN source interface is NVE-only.
show interface vni	Shows the parameters, status and statistics of a VNI interface, status of its bridged interface (if configured), and NVE interface it is associated with.
show nve	Shows the parameters, status and statistics of a NVE interface, status of its carrier interface (source interface), IP address of the carrier interface, VNIs that use this NVE as the VXLAN VTEP, and peer VTEP IP addresses associated with this NVE interface.
source-interface	Specifies the VTEP source interface.
vtep-nve	Associates a VNI interface with the VTEP source interface.

ptp domain

To specify the domain number of all PTP ports on the ISA 3000, use the **ptp domain** command in privileged EXEC or global configuration mode. The domain number ranges from 0 to 255; the default value is 0. Packets received on a domain different from the configured domain will be treated like regular multicast packets and will not undergo any PTP processing. To reset the domain number to 0, the default value, use the **no** form of this command.

ptp domain *domain_num*
no ptp domain

Note This command is only available on the Cisco ISA 3000 appliance.

Syntax Description

domain *domain_num*	Specifies the domain number for all PTP-enabled ports on the ISA 3000.

Command Default

The default **ptp domain** number 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
Privileged EXEC	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.7(1)	This command was added.

Usage Guidelines

The **ptp domain** command is also available in global configuration mode.

Examples

The following example shows the use of the **ptp domain** command to set the PTP domain number to 127:

```
ciscoasa# ptp domain 127
```

Related Commands

Command	Description
show ptp port	Displays PTP interface/port information.

ptp enable

To enable PTP on an interface on the ISA 3000, use the **ptp enable** command in interface configuration mode. The mode in which PTP will be enabled is specified with the **ptp mode** command. To disable PTP on an interface, use the **no** form of this command. PTP packets coming into and going out of the interface will then be treated like regular multicast packets.

ptp enable
no ptp enable

Note This command is only available on the Cisco ISA 3000 appliance.

Syntax Description

This command has no arguments or keywords.

Command Default

PTP is enabled on all ISA 3000 interfaces in transparent mode by default. In routed mode, you must add the necessary configuration to ensure that the PTP packets are allowed to flow through the device.

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	• Yes	—	—

Command History

Release	Modification
9.7(1)	This command was added.

Usage Guidelines

This command is entered in interface configuration mode only.

This command is allowed only on physical interfaces. It is not allowed on sub-interfaces, other virtual interfaces, or the management interface.

PTP flows on VLAN sub-interfaces are supported, assuming the appropriate PTP configuration is present on the parent interface.

If PTP is not enabled in any mode, this command will be accepted, but will have no effect. A warning will be issued.

Related Commands

Command	Description
show ptp clock	Displays PTP clock properties.

ptp mode

To specify the PTP clock mode on the ISA 3000, use the **ptp mode** command in privileged EXEC or global configuration mode. To disable PTP on all interfaces, use the **no** form of this command.

ptp mode e2etransparent
no ptp mode

Note This command is only available on the Cisco ISA 3000 appliance.

Syntax Description

e2etranparent	Enables End to End Transparent mode on all PTP-enabled interfaces on the ISA 3000.

Command Default

End to End Transparent mode 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
Privileged EXEC	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.7(1)	This command was added.

Usage Guidelines

When End to End Transparent mode is disabled, all PTP packets are treated like any other multicast packets. This is equivalent to forward mode.

The **ptp mode** command is also available in global configuration mode.

Examples

The following example shows the use of the **ptp mode** command to set the PTP clock mode to End to End Transparent:

```
ciscoasa# ptp mode e2etranparent
```

Related Commands

Command	Description
show ptp internal-info	Displays PTP statistics and counter information.

public-key

To specify the DNSCrypt provider public key for certificate verification required by Cisco Umbrella, use the **public-key** command in Umbrella configuration mode. Use the **no** form of this command to remove the key and use the default key.

public-key *dnscrypt_key*
no public-key [*dnscrypt_key*]

Syntax Description

dnscrypt_key	The public key used by the Cisco Umbella server for DNSCrypt. This key is relevant only if you enable dnscrypt in the DNS inspection policy map used for Cisco Umbrella. The key is a 32-byte hexadecimal value. Enter the hex value in ASCII with a colon separator for every 2 bytes. The key is 79 bytes long. Obtain this key from Cisco Umbrella.

Command Default

The default key is used.

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

If you intend to enable DNSCrypt in the DNS inspection policy map, you can optionally configure the DNSCrypt provider public key for certificate verification. If you do not configure the key, the default currently distributed public key is used for validation.

Configuring a key is necessary only if Cisco Umbrella changes the public key it uses for DNSCrypt encryption.

Examples

The following example configures a public key for use with Cisco Umbrella. The example also shows how to enable DNSCrypt in the default DNS inspection policy map, which is used in global DNS inspection.

```
ciscoasa(config)# umbrella-global

ciscoasa(config-umbrella)# public-key
B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:CA43:FB79

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
ciscoasa(config)# policy-map type inspect dns preset_dns_map

ciscoasa(config-pmap)# parameters

ciscoasa(config-pmap-p)# umbrella

ciscoasa(config-pmap-p)# dnscrypt
```

Related Commands

Commands	Description
dnscrypt	Enables DNScrypt encryption for the connection between the device and Cisco Umbrella.
inspect dns	Enables DNS inspection.
policy-map type inspect dns	Creates a DNS inspection policy map.
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.
token	Identifies the API token that is needed to register with Cisco Umbrella.
umbrella-global	Configures the Cisco Umbrella global parameters.

publish-crl

To allow other ASAs to validate the revocation status of certificates issued by the local CA, use the **publish-crl** command in ca-server configuration mode to allow downloading of the CRL directly from and interface on the ASA. To make the CRL unavailable for downloading, use the **no** form of this command.

[**no**] **publish-crl interface** *interface* [**port** *portnumber*]

Syntax Description

interface *interface*	Specifies the *nameif* used for the interface, such as gigabitethernet0/1. See the interface command for details.
port *portnumber*	(Optional) Specifies the port on which the interface device expects to download the CRL. Port numbers can be in the range of 1-65535.

Command Default

The default **publish-crl** status is **no publish**. TCP port 80 is the default for HTTP.

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
Ca-server configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

The CRL is inaccessible by default. You must enable access to the CRL file on the interface and port required.

TCP port 80 is the HTTP default port number. If you configure a non-default port (other than port 80), be sure the **cdp-url** configuration includes the new port number so other devices know to access this specific port.

The CRL Distribution Point (CDP) is the location of the CRL on the local CA ASA. The URL you configure with the **cdp-url** command is embedded into any issued certificates. If you do not configure a specific location for the CDP, the default CDP URL is: http://hostname.domain/+CSCOCA+/asa_ca.crl.

An HTTP redirect and a CRL download request are handled by the same HTTP listener, if Clientless SSL VPN is enabled on the same interface. The listener checks for the incoming URL and if it matches the one configured with the **cdp-url** command, the CRL file downloads. If the URL does not match the **cdp-url** command, the connection is redirected to HTTPS (if HTTP redirect is enabled).

Examples

The **publish-crl** command example, entered in ca-server configuration mode, enables port 70 of the outside interface for CRL download:

```
ciscoasa(config)# crypto ca server
```

```
ciscoasa (config-ca-server)#publish-crl outside 70
ciscoasa(config-ca-server)#
```

Related Commands

Command	Description
cdp-url	Specifies a particular location for the automatically generated CRL.
show interface	Displays the runtime status and statistics of interfaces.

pwd

To display the current working directory, use the **pwd** command in privileged EXEC mode.

pwd

Syntax Description

This command has no arguments or keywords.

Command Default

The root directory (/) is the 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
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0	This command was added.

Usage Guidelines

This command is similar in functionality to the **dir** command.

Examples

The following example shows how to display the current working directory:

```
ciscoasa# pwd
disk0:/
ciscoasa# pwd
flash:
```

Related Commands

Command	Description
cd	Changes the current working directory to the one specified.
dir	Displays the directory contents.
more	Displays the contents of a file.