



activation-key through auto-update timeout Commands

activation-key

To change the activation key on the FWSM and check the activation key running on the FWSM against the activation key that is stored as a hidden file in the Flash partition of the FWSM, use the **activation-key** command in global configuration mode.

activation-key [*activation-key-four-tuple*| *activation-key-five-tuple*]

Syntax Description

<i>activation-key-four-tuple</i>	Sets the activation key; see the “Usage Guidelines” section for formatting guidelines.
<i>activation-key-five-tuple</i>	Sets the activation key; see the “Usage Guidelines” section for formatting guidelines.

Defaults

This command has no default settings.

Command Modes

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

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

Command History

Release	Modification
2.2(1)	Support for this command was introduced.

Usage Guidelines

Enter the *activation-key-four-tuple* as a four-element hexadecimal string with one space between each element, or *activation-key-five-tuple* as a five-element hexadecimal string with one space between each element as follows:

```
0xe02888da 0x4ba7bed6 0xf1c123ae 0xffd8624e
```

The leading 0x specifier is optional; all values are assumed to be hexadecimal.

The key is not stored in the configuration file. The key is tied to the serial number.

Examples

This example shows how to change the activation key on the FWSM:

```
hostname(config)# activation-key 0xe02888da 0x4ba7bed6 0xf1c123ae 0xffd8624e
```

Related Commands

Command	Description
show activation-key	Displays the activation key.

address-pool

To specify a list of address pools for allocating addresses to remote clients, use the **address-pool** command in tunnel-group general-attributes configuration mode. To eliminate address pools, use the **no** form of this command.

address-pool [(*interface name*)] *address_pool1* [...*address_pool6*]

no address-pool [(*interface name*)] *address_pool1* [...*address_pool6*]

Syntax Description

<i>address_pool</i>	Specifies the name of the address pool configured with the ip local pool command. You can specify up to 6 local address pools.
<i>interface name</i>	(Optional) Specifies the interface to be used for the address pool.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

You can enter multiples of each of these commands, one per interface. If an interface is not specified, then the command specifies the default for all interfaces that are not explicitly referenced.

Examples

The following example entered in config-general configuration mode, specifies a list of address pools for allocating addresses to remote clients for an IPSec remote-access tunnel group xyz:

```
hostname(config)# tunnel-group xyz
hostname(config)# tunnel-group xyz general
hostname(config-general)# address-pool (inside) addrpool1 addrpool2 addrpool3
hostname(config-general)#
```

Related Commands

Command	Description
ip local pool	Configures IP address pools to be used for VPN remote-access tunnels.
clear configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group.
tunnel-group-map default-group	Associates the certificate map entries created using the crypto ca certificate map command with tunnel groups.

admin-context

To set the admin context for the system configuration, use the **admin-context** command in global configuration mode. The system configuration does not include any network interfaces or network settings for itself; rather, when the system needs to access network resources (such as downloading the FWSM software or allowing remote management for an administrator), it uses one of the contexts that is designated as the admin context.

admin-context *name*

Syntax Description

<i>name</i>	<p>Sets the name as a string up to 32 characters long. If you have not defined any contexts yet, then first specify the admin context name with this command. Then, the first context you add using the context command must be the specified admin context name.</p> <p>This name is case sensitive, so you can have two contexts named “customerA” and “CustomerA,” for example. You can use letters, digits, or hyphens, but you cannot start or end the name with a hyphen.</p> <p>“System” or “Null” (in upper or lower case letters) are reserved names, and cannot be used.</p>
-------------	---

Defaults

For a new FWSM in multiple context mode, the admin context is called “admin.”

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	N/A	N/A	—	—	•

Command History

Release	Modification
2.2(1)	This command was introduced.

Usage Guidelines

You can set any context to be the admin context, as long as the context configuration resides on the internal Flash memory.

You cannot remove the current admin context, unless you remove all contexts using the **clear configure context** command.

Examples

The following example sets the admin context to be “administrator”:

```
hostname(config)# admin-context administrator
```

Related Commands	Command	Description
	clear configure context	Removes all contexts from the system configuration.
	context	Configures a context in the system configuration and enters context configuration mode.
	show admin-context	Shows the current admin context name.

alias

To manually translate an address and perform DNS reply modification, use the **alias** command in global configuration mode. To remove an **alias** command, use the **no** form of this command. This command functionality has been replaced by outside NAT commands, including the **nat** and **static** commands with the **dns** keyword. We recommend that you use outside NAT instead of the **alias** command.

```
alias interface_name mapped_ip real_ip [netmask]
```

```
[no] alias interface_name mapped_ip real_ip [netmask]
```

Syntax Description

<i>interface_name</i>	Specifies the ingress interface name for traffic destined for the mapped IP address (or the egress interface name for traffic from the mapped IP address).
<i>mapped_ip</i>	Specifies the IP address to which you want to translate the real IP address.
<i>real_ip</i>	Specifies the real IP address.
<i>netmask</i>	(Optional) Specifies the subnet mask for both IP addresses. Enter 255.255.255.255 for a host mask.

Defaults

This command has no default settings.

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

You can also use this command to perform address translation on a destination address. For example, if a host sends a packet to 209.165.201.1, you can use the **alias** command to redirect traffic to another address, such as 209.165.201.30.



Note

If the **alias** command is used for DNS rewrite and not for other address translation, disable **proxy-arp** on the alias-enabled interface. Use the **sysopt noproxyarp** command to prevent the FWSM from pulling traffic toward itself via **proxy-arp** for generic NAT processing.

After changing or removing an **alias** command, use the **clear xlate** command.

You must have an A (address) record in the DNS zone file for the “dnat” address in the **alias** command.

The **alias** command has two uses that can be summarized in the following ways:

- If the FWSM gets a packet that is destined for the *mapped_ip*, you can configure the **alias** command to send it to the *real_ip*.
- If the FWSM gets a DNS packet that is returned to the FWSM destined for *real_ip*, you can configure the **alias** command to alter the DNS packet to change the destination network address to *mapped_ip*.

The **alias** command automatically interacts with the DNS servers on your network to ensure that domain name access to the aliased IP address is handled transparently.

You can specify a net alias by using network addresses for the *real_ip* and *mapped_ip* IP addresses. For example, the **alias 192.168.201.0 209.165.201.0 255.255.255.224** command creates aliases for each IP address between 209.165.201.1 and 209.165.201.30.

To access an **alias** *mapped_ip* address with **static** and **access-list** commands, specify the *mapped_ip* address in the **access-list** command as the address from which traffic is permitted as follows:

```
hostname(config)# alias (inside) 192.168.201.1 209.165.201.1 255.255.255.255
hostname(config)# static (inside,outside) 209.165.201.1 192.168.201.1 netmask
255.255.255.255
hostname(config)# access-list acl_out permit tcp host 192.168.201.1 host 209.165.201.1 eq
ftp-data
hostname(config)# access-group acl_out in interface outside
```

An alias is specified with the inside address 192.168.201.1 mapping to the destination address 209.165.201.1.

When the inside network client 209.165.201.2 connects to example.com, the DNS response from an external DNS server to the internal client's query would be altered by the FWSM to be 192.168.201.29. If the FWSM uses 209.165.200.225 through 209.165.200.254 as the global pool IP addresses, the packet goes to the FWSM with SRC=209.165.201.2 and DST=192.168.201.29. The FWSM translates the address to SRC=209.165.200.254 and DST=209.165.201.29 on the outside.

Examples

This example shows that the inside network contains the IP address 209.165.201.29, which on the Internet belongs to example.com. When inside clients try to access example.com, the packets do not go to the FWSM because the client assumes that the 209.165.201.29 is on the local inside network.

To correct this, use the **alias** command as follows:

```
hostname(config)# alias (inside) 192.168.201.0 209.165.201.0 255.255.255.224

hostname(config)# show running-config alias
alias 192.168.201.0 209.165.201.0 255.255.255.224
```

This example shows a web server that is on the inside at 10.1.1.11 and the **static** command that was created at 209.165.201.11. The source host is on the outside with address 209.165.201.7. A DNS server on the outside has a record for www.example.com as follows:

```
dns-server# www.example.com. IN A 209.165.201.11
```

You must include the period at the end of the www.example.com. domain name.

This example shows how to use the **alias** command:

```
hostname(config)# alias 10.1.1.11 209.165.201.11 255.255.255.255
```

The FWSM changes the name server replies to 10.1.1.11 for inside clients to directly connect to the web server.

To provide access you also need the following commands:

```

hostname(config)# static (inside,outside) 209.165.201.11 10.1.1.11

hostname(config)# access-list acl_grp permit tcp host 209.165.201.7 host 209.165.201.11 eq telnet
hostname(config)# access-list acl_grp permit tcp host 209.165.201.11 eq telnet host 209.165.201.7

```

Related Commands

Command	Description
access-list extended	Creates an access list.
clear configure alias	Removes all alias commands from the configuration.
show running-config alias	Displays the overlapping addresses with dual NAT commands in the configuration.
static	Configures a one-to-one address translation rule by mapping a local IP address to a global IP address, or a local port to a global port.

allocate-acl-partition

To assign a context to a memory partition, use the **allocate-acl-partition** command in context configuration mode. To remove the assignment, use the **no** form of this command.

allocate-acl-partition *partition_number*

no allocate-acl-partition *partition_number*

Syntax Description

partition_number Specifies the partition number as an integer from 0 to the number of partitions available, minus 1. The default is 12 partitions, so the range is 0 to 11. See the **resource acl-partition** command to configure the number of memory partitions.

Defaults

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
Context configuration	N/A	N/A	—	—	•

Command History

Release	Modification
2.3(1)	This command was introduced.

Usage Guidelines

In multiple context mode, the FWSM partitions the memory allocated to rule configuration, and assigns each context to a partition. By default, a context belongs to one of 12 partitions that offers a maximum of 12,130 rules, including ACEs, AAA rules, and others. The FWSM assigns contexts to the partitions in the order they are loaded at startup. For example, if you have 12 contexts, each context is assigned to its own partition, and can use 12,130 rules. If you add one more context, then context number 1 and the new context number 13 are both assigned to partition 1, and can use 12,130 rules divided between them; the other 11 contexts continue to use 12,130 rules each. If you delete contexts, the partition membership does not shift, so you might have some unequal distribution until you reboot, at which time the contexts are evenly distributed.



Note

Rules are used up on a first come, first served basis, so one context might use more rules than another context.

Alternatively, you can manually assign a context to a partition with the **allocate-acl-partition** command. You can also reduce the number of partitions to better match the number of contexts you have with the **resource acl-partition** command.

When you assign a context to a partition, then the partition becomes *exclusive*. An exclusive partition only includes contexts that you specifically assign to it. Partitions that do not have contexts specifically assigned to them are non-exclusive and contexts are allocated to them in a round-robin fashion.

**Note**

If you assign contexts to all partitions, then they are all exclusive. If you later add a context that is not assigned to a partition, however, then it is assigned to partition 0 by default.

Examples

The following example assigns context test to partition 0:

```
hostname# context test
hostname(config-ctx)# allocate-acl-partition 0
```

Related Commands

Command	Description
context	Configures a security context.
resource acl-partition	Determines the number of memory partitions for multiple context mode.
show resource acl-partition	Shows the contexts assigned to each memory partition and the number of rules used.

allocate-interface

To allocate interfaces to a security context, use the **allocate-interface** command in context configuration mode. To remove an interface from a context, use the **no** form of this command.

allocate-interface *vlan*number[-*vlan*number] [*map_name*[-*map_name*]] [**visible** | **invisible**]

no allocate-interface *vlan*number[-*vlan*number]

Syntax Description

invisible	(Default) Allows context users to only see the mapped name (if configured) in the show interface command.
<i>map_name</i>	(Optional) Sets a mapped name. The <i>map_name</i> is an alphanumeric alias for the interface that can be used within the context instead of the VLAN ID. If you do not specify a mapped name, the VLAN ID is used within the context. For security purposes, you might not want the context administrator to know which interfaces are being used by the context. A mapped name must start with a letter, end with a letter or digit, and have as interior characters only letters, digits, or an underscore. For example, you can use the following names: <code>int0</code> <code>inta</code> <code>int_0</code> You can specify a range of mapped names. See the “ Usage Guidelines ” section for more information about ranges.
visible	(Optional) Allows context users to see physical interface properties in the show interface command even if you set a mapped name.
<i>vlan</i> number	Sets the VLAN number, typically from 2 to 1000 and from 1025 to 4094 (see the switch documentation for supported VLANs). To view all interfaces currently configured on the FWSM, enter the show running-config interface command or the show interface command. You can only allocate an interface that exists in the system configuration. By default, all VLANs assigned to the FWSM by the switch are added to the system configuration. You can also add VLANs manually to the system configuration, but you need to assign them from the switch if you want them to pass traffic.

Defaults

The VLAN ID is invisible in the **show interface** command output by default if you set a mapped name.

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
Context configuration	N/A	N/A	—	—	•

Command History

Release	Modification
2.2(1)	This command was introduced.

Usage Guidelines

You can enter this command multiple times to specify different ranges. To change the mapped name or visible setting, reenter the command for a given VLAN ID, and set the new values; you do not need to enter the **no allocate-interface** command and start over. If you remove the **allocate-interface** command, the FWSM removes any interface-related configuration in the context.

You can assign the same interfaces to multiple contexts in routed mode, if desired. Transparent mode does not allow shared interfaces.

If you specify a range of VLAN IDs, you can specify a matching range of mapped names. Follow these guidelines for ranges:

- The mapped name must consist of an alphabetic portion followed by a numeric portion. The alphabetic portion of the mapped name must match for both ends of the range. For example, enter the following range:

```
int0-int10
```

- The numeric portion of the mapped name must include the same quantity of numbers as the **vlanx-vlany** statement. For example, both ranges include 100 interfaces:

```
vlan100-vlan199 int1-int100
```

If you enter **vlan100-vlan199 int1-int15** or **vlan100-vlan199 happy1-sad5**, for example, the command fails.

Examples

The following example shows VLANs 100, 200, and 300 through 305 assigned to the context. The mapped names are int1 through int8.

```
hostname(config-ctx) # allocate-interface vlan100 int1
hostname(config-ctx) # allocate-interface vlan200 int2
hostname(config-ctx) # allocate-interface vlan300-vlan305 int3-int8
```

Related Commands

Command	Description
context	Creates a security context in the system configuration and enters context configuration mode.
interface	Configures an interface and enters interface configuration mode.

Command	Description
show context	Shows a list of contexts (system execution space) or information about the current context.
show interface	Displays the runtime status and statistics of interfaces.

area

To create an OSPF area, use the **area** command in router configuration mode. To remove the area, use the **no** form of this command.

```
area area_id
```

```
no area area_id
```

Syntax Description

<i>area_id</i>	The ID of the area being created. You can specify the identifier as either a decimal number or an IP address. Valid decimal values range from 0 to 4294967295.
----------------	--

Defaults

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 configuration	•	—	•	—	—

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

The area that you create does not have any parameters set. Use the related area commands to set the area parameters.

Examples

The following example shows how to create an OSPF area with an area ID of 1:

```
hostname(config-router)# area 1
hostname(config-router)#
```

Related Commands

Command	Description
area authentication	Enables authentication for the OSPF area.
area nssa	Defines the area as a not-so-stubby area.
area stub	Defines the area as a stub area.

Command	Description
router ospf	Enters router configuration mode.
show running-config router	Displays the commands in the global router configuration.

area authentication

To enable authentication for an OSPF area, use the **area authentication** command in router configuration mode. To disable area authentication, use the **no** form of this command.

```
area area_id authentication [message-digest]
```

```
no area area_id authentication [message-digest]
```

Syntax Description

<i>area_id</i>	The identifier of the area on which authentication is to be enabled. You can specify the identifier as either a decimal number or an IP address. Valid decimal values range from 0 to 4294967295.
message-digest	(Optional) Enables Message Digest 5 (MD5) authentication on the area specified by the <i>area_id</i> .

Defaults

Area authentication 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
Router configuration	•	—	•	—	—

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

If the specified OSPF area does not exist, it is created when this command is entered. Entering the **area authentication** command without the **message-digest** keyword enables simple password authentication. Including the **message-digest** keyword enables MD5 authentication.

Examples

The following example shows how to enable MD5 authentication for area 1:

```
hostname(config-router)# area 1 authentication message-digest
hostname(config-router)#
```

Related Commands

Command	Description
router ospf	Enters router configuration mode.
show running-config router	Displays the commands in the global router configuration.

area default-cost

To specify a cost for the default summary route sent into a stub or NSSA, use the **area default-cost** command in router configuration mode. To restore the default cost value, use the **no** form of this command.

```
area area_id default-cost cost
```

```
no area area_id default-cost
```

Syntax Description

<i>area_id</i>	The identifier of the stub or NSSA whose default cost is being changed. You can specify the identifier as either a decimal number or an IP address. Valid decimal values range from 0 to 4294967295.
<i>cost</i>	Specifies the cost for the default summary route that is used for a stub or NSSA. Valid values range from 0 to 65535.

Defaults

The default value of *cost* is 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
Router configuration	•	—	•	—	—

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

If the specified area has not been previously defined using the **area** command, this command creates the area with the specified parameters.

Examples

The following example show how to specify a default cost for summary route sent into a stub or NSSA:

```
hostname(config-router)# area 1 default-cost 5
hostname(config-router)#
```

Related Commands

Command	Description
area nssa	Defines the area as a not-so-stubby area.
area stub	Defines the area as a stub area.

Command	Description
router ospf	Enters router configuration mode.
show running-config router	Displays the commands in the global router configuration.

area filter-list prefix

To filter prefixes advertised in type 3 LSAs between OSPF areas of an ABR, use the **area filter-list prefix** command in router configuration mode. To change or cancel the filter, use the **no** form of this command.

```
area area_id filter-list prefix list_name {in | out}
```

```
no area area_id filter-list prefix list_name {in | out}
```

Syntax Description

<i>area_id</i>	Identifier of the area for which filtering is configured. You can specify the identifier as either a decimal number or an IP address. Valid decimal values range from 0 to 4294967295.
in	Applies the configured prefix list to prefixes advertised inbound to the specified area.
<i>list_name</i>	Specifies the name of a prefix list.
out	Applies the configured prefix list to prefixes advertised outbound from the specified area.

Defaults

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 configuration	•	—	•	—	—

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

If the specified area has not been previously defined using the **area** command, this command creates the area with the specified parameters.

Only type 3 LSAs can be filtered. If an ASBR is configured in the private network, then it will send type 5 LSAs (describing private networks) which are flooded to the entire AS including the public areas.

Examples

The following example filters prefixes that are sent from all other areas to area 1:

```
hostname(config-router)# area 1 filter-list prefix-list AREA_1 in
hostname(config-router)#
```

Related Commands

Command	Description
router ospf	Enters router configuration mode.
show running-config router	Displays the commands in the global router configuration.

area nssa

To configure an area as an NSSA, use the **area nssa** command in router configuration mode. To remove the NSSA designation from the area, use the **no** form of this command.

```
area area_id nssa [no-redistribution] [default-information-originate [metric-type {1 | 2}]
[metric value]] [no-summary]
```

```
no area area_id nssa [no-redistribution] [default-information-originate [metric-type {1 | 2}]
[metric value]] [no-summary]
```

Syntax Description

area_id	Identifier of the area being designated as an NSSA. You can specify the identifier as either a decimal number or an IP address. Valid decimal values range from 0 to 4294967295.
default-information-originate	Used to generate a Type 7 default into the NSSA area. This keyword only takes effect on an NSSA ABR or an NSSA ASBR.
metric metric_value	(Optional) Specifies the OSPF default metric value. Valid values range from 0 to 16777214.
metric-type {1 2}	(Optional) the OSPF metric type for default routes. Valid values are the following: <ul style="list-style-type: none"> 1—type 1 2—type 2. The default value is 2.
no-redistribution	(Optional) Used when the router is an NSSA ABR and you want the redistribute command to import routes only into the normal areas, but not into the NSSA area.
no-summary	(Optional) Allows an area to be a not-so-stubby area but not have summary routes injected into it.

Defaults

The defaults are as follows:

- No NSSA area is defined.
- The **metric-type** is 2.

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 configuration	•	—	•	—	—

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

If the specified area has not been previously defined using the **area** command, this command creates the area with the specified parameters.

If you configure one option for an area, and later specify another option, both options are set. For example, entering the following two command separately results in a single command with both options set in the configuration:

```
area 1 nssa no-redistribution
area area_id nssa default-information-originate
```

Examples

The following example shows how setting two options separately results in a single command in the configuration:

```
hostname(config-router)# area 1 nssa no-redistribution
hostname(config-router)# area 1 nssa default-information-originate
hostname(config-router)# exit
hostname(config-router)# show running-config router ospf 1
router ospf 1
  area 1 nssa no-redistribution default-information-originate
```

Related Commands

Command	Description
area stub	Defines the area as a stub area.
router ospf	Enters router configuration mode.
show running-config router	Displays the commands in the global router configuration.

area range

To consolidate and summarize routes at an area boundary, use the **area range** command in router configuration mode. To disable this function, use the **no** form of this command.

```
area area_id range address mask [advertise | not-advertise]
```

```
no area area_id range address mask [advertise | not-advertise]
```

Syntax Description

<i>address</i>	IP address of the subnet range.
advertise	(Optional) Sets the address range status to advertise and generates type 3 summary link-state advertisements (LSAs).
<i>area_id</i>	Identifier of the area for which the range is configured. You can specify the identifier as either a decimal number or an IP address. Valid decimal values range from 0 to 4294967295.
<i>mask</i>	IP address subnet mask.
not-advertise	(Optional) Sets the address range status to DoNotAdvertise. The type 3 summary LSA is suppressed, and the component networks remain hidden from other networks.

Defaults

The address range status is set to advertise.

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 configuration	•	—	•	—	—

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

If the specified area has not been previously defined using the **area** command, this command creates the area with the specified parameters.

The **area range** command is used only with ABRs. It is used to consolidate or summarize routes for an area. The result is that a single summary route is advertised to other areas by the ABR. Routing information is condensed at area boundaries. External to the area, a single route is advertised for each address range. This behavior is called *route summarization*. You can configure multiple **area range** commands for an area. Thus, OSPF can summarize addresses for many different sets of address ranges.

The **no area area_id range ip_address netmask not-advertise** command removes only the **not-advertise** optional keyword.

Examples

The following example specifies one summary route to be advertised by the ABR to other areas for all subnets on network 10.0.0.0 and for all hosts on network 192.168.110.0:

```
hostname(config-router)# area 10.0.0.0 range 10.0.0.0 255.0.0.0
hostname(config-router)# area 0 range 192.168.110.0 255.255.255.0
hostname(config-router)#
```

Related Commands

Command	Description
router ospf	Enters router configuration mode.
show running-config router	Displays the commands in the global router configuration.

area stub

To define an area as a stub area, use the **area stub** command in router configuration mode. To remove the stub area function, use the **no** form of this command.

```
area area_id [no-summary]
```

```
no area area_id [no-summary]
```

Syntax Description

<i>area_id</i>	Identifier for the stub area. You can specify the identifier as either a decimal number or an IP address. Valid decimal values range from 0 to 4294967295.
no-summary	Prevents an ABR from sending summary link advertisements into the stub area.

Defaults

The default behaviors are as follows:

- No stub areas are defined.
- Summary link advertisements are sent into the stub area.

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 configuration	•	—	•	—	—

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

The command is used only on an ABR attached to a stub or NSSA.

There are two stub area router configuration commands: the **area stub** and **area default-cost** commands. In all routers and access servers attached to the stub area, the area should be configured as a stub area using the **area stub** command. Use the **area default-cost** command only on an ABR attached to the stub area. The **area default-cost** command provides the metric for the summary default route generated by the ABR into the stub area.

Examples

The following example configures the specified area as a stub area:

```
hostname(config-router)# area 1 stub
hostname(config-router)#
```

Related Commands

Command	Description
area default-cost	Specifies a cost for the default summary route sent into a stub or NSSA
area nssa	Defines the area as a not-so-stubby area.
router ospf	Enters router configuration mode.
show running-config router	Displays the commands in the global router configuration.

area virtual-link

To define an OSPF virtual link, use the **area virtual-link** command in router configuration mode. To reset the options or remove the virtual link, use the **no** form of this command.

```
area area_id virtual-link router_id [authentication [message-digest | null]] [hello-interval
seconds] [retransmit-interval seconds] [transmit-delay seconds] [dead-interval seconds]
[[authentication-key key] | [message-digest-key key_id md5 key]]
```

```
no area area_id virtual-link router_id [authentication [message-digest | null]] [hello-interval
seconds] [retransmit-interval seconds] [transmit-delay seconds] [dead-interval seconds]
[[authentication-key key] | [message-digest-key key_id md5 key]]
```

Syntax Description

area_id	Area ID of the transit area for the virtual link. You can specify the identifier as either a decimal number or an IP address. Valid decimal values range from 0 to 4294967295.
authentication	(Optional) Specifies the authentication type.
authentication-key <i>key</i>	(Optional) Specifies an OSPF authentication password for use by neighboring routing devices.
dead-interval <i>seconds</i>	(Optional) Specifies the interval before declaring a neighboring routing device is down if no hello packets are received; valid values are from 1 to 65535 seconds.
hello-interval <i>seconds</i>	(Optional) Specifies the interval between hello packets sent on the interface; valid values are from 1 to 65535 seconds.
md5 <i>key</i>	(Optional) Specifies an alphanumeric key up to 16 bytes.
message-digest	(Optional) Specifies that message digest authentication is used.
message-digest-key <i>key_id</i>	(Optional) Enables the Message Digest 5 (MD5) authentication and specifies the numerical authentication key ID number; valid values are from 1 to 255.
null	(Optional) Specifies that no authentication is used. Overrides password or message digest authentication if configured for the OSPF area.
retransmit-interval <i>seconds</i>	(Optional) Specifies the time between LSA retransmissions for adjacent routers belonging to the interface; valid values are from 1 to 65535 seconds.
<i>router_id</i>	The router ID associated with the virtual link neighbor. The router ID is internally derived by each router from the interface IP addresses. This value must be entered in the format of an IP address. There is no default.
transmit-delay <i>seconds</i>	(Optional) Specifies the delay time between when OSPF receives a topology change and when it starts a shortest path first (SPF) calculation in seconds from 0 to 65535. The default is 5 seconds.

Defaults

The defaults are as follows:

- *area_id*: No area ID is predefined.
- *router_id*: No router ID is predefined.
- **hello-interval** *seconds*: 10 seconds.
- **retransmit-interval** *seconds*: 5 seconds.

- **transmit-delay** *seconds*: 1 second.
- **dead-interval** *seconds*: 40 seconds.
- **authentication-key** *key*: No key is predefined.
- **message-digest-key** *key_id md5 key*: No key is predefined.

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 configuration	•	—	•	—	—

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

In OSPF, all areas must be connected to a backbone area. If the connection to the backbone is lost, it can be repaired by establishing a virtual link.

The smaller the hello interval, the faster topological changes are detected, but more routing traffic ensues.

The setting of the retransmit interval should be conservative, or needless retransmissions occur. The value should be larger for serial lines and virtual links.

The transmit delay value should take into account the transmission and propagation delays for the interface.

The specified authentication key is used only when authentication is enabled for the backbone with the **area area_id authentication** command.

The two authentication schemes, simple text and MD5 authentication, are mutually exclusive. You can specify one or the other or neither. Any keywords and arguments you specify after **authentication-key key** or **message-digest-key key_id md5 key** are ignored. Therefore, specify any optional arguments before such a keyword-argument combination.

If the authentication type is not specified for an interface, the interface uses the authentication type specified for the area. If no authentication type has been specified for the area, the area default is null authentication.



Note

Each virtual link neighbor must include the transit area ID and the corresponding virtual link neighbor router ID for a virtual link to be properly configured. Use the **show ospf** command to see the router ID.

To remove an option from a virtual link, use the **no** form of the command with the option that you want removed. To remove the virtual link, use the **no area area_id virtual-link** command.

Examples

The following example establishes a virtual link with MD5 authentication:

```
hostname(config-router)# area 10.0.0.0 virtual-link 10.3.4.5 message-digest-key 3 md5  
sa5721bk47
```

Related Commands

Command	Description
area authentication	Enables authentication for an OSPF area.
router ospf	Enters router configuration mode.
show ospf	Displays general information about the OSPF routing processes.
show running-config router	Displays the commands in the global router configuration.

arp

To add a static ARP entry to the ARP table, use the **arp** command in global configuration mode. To remove the static entry, use the **no** form of this command. A static ARP entry maps a MAC address to an IP address and identifies the interface through which the host is reached. Static ARP entries do not time out, and might help you solve a networking problem. In transparent firewall mode, the static ARP table is used with ARP inspection (see the **arp-inspection** command).

```
arp interface_name ip_address mac_address [alias]
```

```
no arp interface_name ip_address mac_address
```

Syntax Description

alias	(Optional) Enables proxy ARP for this mapping. If the FWSM receives an ARP request for the specified IP address, then it responds with the FWSM MAC address. When the FWSM receives traffic destined for the host belonging to the IP address, the FWSM forwards the traffic to the host MAC address that you specify in this command. This keyword is useful if you have devices that do not perform ARP, for example. In transparent firewall mode, this keyword is ignored; the FWSM does not perform proxy ARP.
<i>interface_name</i>	The interface attached to the host network.
<i>ip_address</i>	The host IP address.
<i>mac_address</i>	The host MAC address.

Defaults

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	•	•	•	•	—

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

Although hosts identify a packet destination by an IP address, the actual delivery of the packet on Ethernet relies on the Ethernet MAC address. When a router or host wants to deliver a packet on a directly connected network, it sends an ARP request asking for the MAC address associated with the IP address, and then delivers the packet to the MAC address according to the ARP response. The host or router keeps an ARP table so it does not have to send ARP requests for every packet it needs to deliver.

The ARP table is dynamically updated whenever ARP responses are sent on the network, and if an entry is not used for a period of time, it times out. If an entry is incorrect (for example, the MAC address changes for a given IP address), the entry times out before it can be updated.

**Note**

In transparent firewall mode, dynamic ARP entries are used for traffic to and from the FWSM, such as management traffic.

Examples

The following example creates a static ARP entry for 10.1.1.1 with the MAC address 0009.7cbe.2100 on the outside interface:

```
hostname(config)# arp outside 10.1.1.1 0009.7cbe.2100
```

Related Commands

Command	Description
arp timeout	Sets the time before the FWSM rebuilds the ARP table.
arp-inspection	For transparent firewall mode, inspects ARP packets to prevent ARP spoofing.
show arp	Shows the ARP table.
show arp statistics	Shows ARP statistics.
show running-config arp	Shows the current configuration of the ARP timeout.

arp timeout

To set the time before the FWSM rebuilds the ARP table, use the **arp timeout** command in global configuration mode. To restore the default timeout, use the **no** form of this command. Rebuilding the ARP table automatically updates new host information and removes old host information. You might want to reduce the timeout because the host information changes frequently.

arp timeout *seconds*

no arp timeout *seconds*

Syntax Description	<i>seconds</i>	The number of seconds between ARP table rebuilds, from 60 to 4294967.
---------------------------	----------------	---

Defaults	The default value is 14,400 seconds (4 hours).
-----------------	--

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	•	•	•	•	—

Command History	Release	Modification
	1.1(1)	This command was introduced.

Examples	The following example changes the ARP timeout to 5000 seconds:
-----------------	--

```
hostname(config)# arp timeout 5000
```

Related Commands	Command	Description
	arp	Adds a static ARP entry.
	arp-inspection	For transparent firewall mode, inspects ARP packets to prevent ARP spoofing.
	show arp statistics	Shows ARP statistics.
	show running-config arp timeout	Shows the current configuration of the ARP timeout.

arp-inspection

To enable ARP inspection for transparent firewall mode, use the **arp-inspection** command in global configuration mode. To disable ARP inspection, use the **no** form of this command. ARP inspection checks all ARP packets against static ARP entries (see the **arp** command) and blocks mismatched packets. This feature prevents ARP spoofing.

arp-inspection *interface_name* **enable** [**flood** | **no-flood**]

no arp-inspection *interface_name* **enable**

Syntax Description

enable	Enables ARP inspection.
flood	(Default) Specifies that packets that do not match any element of a static ARP entry are flooded out all interfaces except the originating interface. If there is a mismatch between the MAC address, the IP address, or the interface, then the FWSM drops the packet.
<i>interface_name</i>	The interface on which you want to enable ARP inspection.
no-flood	(Optional) Specifies that packets that do not exactly match a static ARP entry are dropped.

Defaults

By default, ARP inspection is disabled on all interfaces; all ARP packets are allowed through the FWSM. When you enable ARP inspection, the default is to flood non-matching ARP packets.

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	—	•	•	•	—

Command History

Release	Modification
2.2(1)	This command was introduced.

Usage Guidelines

Configure static ARP entries using the **arp** command before you enable ARP inspection.

When you enable ARP inspection, the FWSM compares the MAC address, IP address, and source interface in all ARP packets to static entries in the ARP table, and takes the following actions:

- If the IP address, MAC address, and source interface match an ARP entry, the packet is passed through.
- If there is a mismatch between the MAC address, the IP address, or the interface, then the FWSM drops the packet.

- If the ARP packet does not match any entries in the static ARP table, then you can set the FWSM to either forward the packet out all interfaces (flood), or to drop the packet.

ARP inspection prevents malicious users from impersonating other hosts or routers (known as ARP spoofing). ARP spoofing can enable a “man-in-the-middle” attack. For example, a host sends an ARP request to the gateway router; the gateway router responds with the gateway router MAC address. The attacker, however, sends another ARP response to the host with the attacker MAC address instead of the router MAC address. The attacker can now intercept all the host traffic before forwarding it on to the router.

ARP inspection ensures that an attacker cannot send an ARP response with the attacker MAC address, so long as the correct MAC address and the associated IP address are in the static ARP table.

**Note**

In transparent firewall mode, dynamic ARP entries are used for traffic to and from the FWSM, such as management traffic.

Examples

The following example enables ARP inspection on the outside interface and sets the FWSM to drop any ARP packets that do not match the static ARP entry:

```
hostname(config)# arp outside 209.165.200.225 0009.7cbe.2100
hostname(config)# arp-inspection outside enable no-flood
```

Related Commands

Command	Description
arp	Adds a static ARP entry.
clear configure arp-inspection	Clears the ARP inspection configuration.
firewall transparent	Sets the firewall mode to transparent.
show arp statistics	Shows ARP statistics.
show running-config arp	Shows the current configuration of the ARP timeout.

asdm disconnect

To terminate an active ASDM session, use the **asdm disconnect** command in privileged EXEC mode.

asdm disconnect *session*

Syntax Description

<i>session</i>	The session ID of the active ASDM session to be terminated. You can display the session IDs of all active ASDM sessions using the show asdm sessions command.
----------------	--

Defaults

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
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
1.1(1)	This command was introduced (as the pdm disconnect command).
3.1(1)	This command was changed from the pdm disconnect command to the asdm disconnect command.

Usage Guidelines

Use the **show asdm sessions** command to display a list of active ASDM sessions and their associated session IDs. Use the **asdm disconnect** command to terminate a specific session.

When you terminate an ASDM session, any remaining active ASDM sessions keep their associated session ID. For example, if there are three active ASDM sessions with the session IDs of 0, 1, and 2, and you terminate session 1, the remaining active ASDM sessions keep the session IDs 0 and 2. The next new ASDM session in this example would be assigned a session ID of 1, and any new sessions after that would begin with the session ID 3.

Examples

The following example terminates an ASDM session with a session ID of 0. The **show asdm sessions** commands display the active ASDM sessions before and after the **asdm disconnect** command is entered.

```
hostname# show asdm sessions
0 192.168.1.1
1 192.168.1.2
hostname# asdm disconnect 0
hostname# show asdm sessions
1 192.168.1.2
```

Related Commands

Command	Description
show asdm sessions	Displays a list of active ASDM sessions and their associated session ID.

asdm disconnect log_session

To terminate an active ASDM logging session, use the **asdm disconnect log_session** command in privileged EXEC mode.

asdm disconnect log_session *session*

Syntax Description

session The session ID of the active ASDM logging session to be terminated. You can display the session IDs of all active ASDM sessions using the **show asdm log_sessions** command.

Defaults

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
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

Use the **show asdm log_sessions** command to display a list of active ASDM logging sessions and their associated session IDs. Use the **asdm disconnect log_session** command to terminate a specific logging session.

Each active ASDM session has one or more associated ASDM logging sessions. ASDM uses the logging session to retrieve syslog messages from FWSM. Terminating a log session may have an adverse effect on the active ASDM session. To terminate an unwanted ASDM session, and the associated log sessions, use the **asdm disconnect** command.



Note

Because each ASDM session has at least one ASDM logging session, the output for the **show asdm sessions** and **show asdm log_sessions** may appear to be the same.

When you terminate an ASDM logging session, any remaining active ASDM logging sessions keep their associated session ID. For example, if there are three active ASDM logging sessions with the session IDs of 0, 1, and 2, and you terminate session 1, the remaining active ASDM logging sessions keep the session IDs 0 and 2. The next new ASDM logging session in this example would be assigned a session ID of 1, and any new logging sessions after that would begin with the session ID 3.

Examples

The following example terminates an ASDM session with a session ID of 0. The **show asdm log_sessions** commands display the active ASDM sessions before and after the **asdm disconnect log_sessions** command is entered.

```
hostname# show asdm log_sessions
0 192.168.1.1
1 192.168.1.2
hostname# asdm disconnect 0
hostname# show asdm log_sessions
1 192.168.1.2
```

Related Commands

Command	Description
show asdm log_sessions	Displays a list of active ASDM logging sessions and their associated session ID.

asdm group



Caution

Do not manually configure this command. ASDM adds **asdm group** commands to the running configuration and uses them for internal purposes. This command is included in the documentation for informational purposes only.

```
asdm group real_grp_name real_if_name
```

```
asdm group ref_grp_name ref_if_name reference real_grp_name
```

Syntax Description

<i>real_grp_name</i>	The name of an ASDM object group.
<i>real_if_name</i>	The name of the interface to which the specified object group is associated.
<i>ref_grp_name</i>	The name of an object group that contains translated IP addresses of the object group specified by the <i>real_grp_name</i> argument.
<i>ref_if_name</i>	The name of the interface from which the destination IP address of inbound traffic is translated.

Defaults

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	•	•	•	•	—

Command History

Release	Modification
1.1(1)	This command was introduced (as the pdm group command).
3.1(1)	This command was changed from the pdm group command to the asdm group command.

Usage Guidelines

Do not manually configure or remove this command.

asdm history enable

To enable ASDM history tracking, use the **asdm history enable** command in global configuration mode. To disable ASDM history tracking, use the **no** form of this command.

asdm history enable

no asdm history enable

Syntax Description This command has no arguments or keywords.

Defaults 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	•	•	•	•	•

Command History	Release	Modification
	1.1(1)	This command was introduced (as the pdm history enable command).
	3.1(1)	This command was changed from the pdm history enable command to the asdm history enable command.

Usage Guidelines The information obtained by enabling ASDM history tracking is stored in the ASDM history buffer. You can view this information using the **show asdm history** command. The history information is used by ASDM for device monitoring.

Examples The following example enables ASDM history tracking:

```
hostname(config)# asdm history enable
hostname(config)#
```

Related Commands	Command	Description
	show asdm history	Displays the contents of the ASDM history buffer.

asdm location



Caution

Do not manually configure this command. ASDM adds **asdm location** commands to the running configuration and uses them for internal communication. This command is included in the documentation for informational purposes only.

```
asdm location ip_addr netmask if_name
```

```
asdm location ipv6_addr/prefix if_name
```

Syntax Description

<i>ip_addr</i>	IP address used internally by ASDM to define the network topology.
<i>netmask</i>	The subnet mask for <i>ip_addr</i> .
<i>if_name</i>	The name of the interface through which ASDM is accessed.
<i>ipv6_addr/prefix</i>	The IPv6 address and prefix used internally by ASDM to define the network topology.

Defaults

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	•	•	•	•	—

Command History

Release	Modification
1.1(1)	This command was introduced (as the pdm location command).
3.1(1)	This command was changed from the pdm location command to the asdm location command.

Usage Guidelines

Do not manually configure or remove this command.

asr-group

To specify an asymmetrical routing interface group ID, use the **asr-group** command in interface configuration mode. To remove the ID, use the **no** form of this command.

asr-group *group_id*

no asr-group *group_id*

Syntax Description

group_id The asymmetric routing group ID. Valid values are from 1 to 32.

Defaults

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	•	•	•	•	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

In some situations, return traffic for a session may be routed through a different interface than it originated from. In failover configurations, return traffic for a connection that originated on one unit may return through the peer unit. This most commonly occurs when two interfaces on a single FWSM, or two FWSMs in a failover pair, are connected to different service providers and the outbound connection does not use a NAT address. By default, FWSM drops the return traffic because there is no connection information for the traffic.

You can prevent the return traffic from being dropped using the **asr-group** command on interfaces where this is likely to occur. When an interface configured with the **asr-group** command receives a packet for which it has no session information, it checks the session information for the other interfaces that are in the same group.



Note

In failover configurations, you must enable Stateful Failover for session information to be passed from the standby unit or failover group to the active unit or failover group.

If it does not find a match, the packet is dropped. If it finds a match, then one of the following actions occurs:

- If the incoming traffic originated on a peer unit in a failover configuration, some or all of the layer 2 header is rewritten and the packet is redirected to the other unit. This redirection continues as long as the session is active.
- If the incoming traffic originated on a different interface on the same unit, some or all of the layer 2 header is rewritten and the packet is reinjected into the stream.

**Note**

Using the **asr-group** command to configure asymmetric routing support is more secure than using the **static** command with the **nailed** option.

You can view ASR statistics using the **show interface detail** command. These statistics include the number of ASR packets sent, received, and dropped on an interface.

Examples

The following example assigns the selected interfaces to the asymmetric routing group 1.

Context ctx1 configuration:

```
hostname/ctx1(config)# interface Vlan101
hostname/ctx1(config-if)# nameif outside
hostname/ctx1(config-if)# ip address 192.168.1.11 255.255.255.0 standby 192.168.1.21
hostname/ctx1(config-if)# asr-group 1
```

Context ctx2 configuration:

```
hostname/ctx2(config)# interface Vlan102
hostname/ctx2(config-if)# nameif outside
hostname/ctx2(config-if)# ip address 192.168.1.31 255.255.255.0 standby 192.168.1.41
hostname/ctx2(config-if)# asr-group 1
```

Related Commands

Command	Description
interface	Enters interface configuration mode.
show interface	Displays interface statistics.

authentication-port

To specify the port number used for RADIUS authentication for this host, use the **authentication-port** command in AAA-server host mode. To remove the authentication port specification, use the **no** form of this command. This command specifies the destination TCP/UDP port number of the remote RADIUS server hosts to which you want to assign authentication functions.

authentication-port *port*

no authentication-port

Syntax Description

port A port number, in the range 1-65535, for RADIUS authentication.

Defaults

By default, the device listens for RADIUS on port 1645 (in compliance with RFC 2058). If the port is not specified, the RADIUS authentication default port number (1645) 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
AAA-server host	•	•	•	•	—

Command History

Release	Modification
3.1(1)	This command was introduced, replacing the aaa-server radius-authport command.

Usage Guidelines

If your RADIUS authentication server uses a port other than 1645, you must configure the FWSM for the appropriate port prior to starting the RADIUS service with the **aaa-server** command.



Tip

RFC 2138 introduced a change to the standard port for RADIUS authentication, to port 1812.

This command is valid only for server groups that are configured for RADIUS.

Examples

The following example configures a RADIUS AAA server named “svrgrp1” on host “1.2.3.4”, sets a timeout of 9 seconds, sets a retry-interval of 7 seconds, and configures authentication port 1650.

```
hostname(config)# aaa-server svrgrp1 protocol radius
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry-interval 7
hostname(config-aaa-server-host)# authentication-port 1650
```

Related Commands	Command	Description
	aaa authentication	Enables or disables LOCAL, TACACS+, or RADIUS user authentication, on a server designated by the aaa-server command, or ASDM user authentication.
	aaa-server host	Enters AAA server host configuration mode, so that you can configure AAA server parameters that are host-specific.
	clear configure aaa-server	Removes all AAA command statements from the configuration.
	show running-config aaa-server	Displays AAA server statistics for all AAA servers, for a particular server group, for a particular server within a particular group, or for a particular protocol.

authentication-server-group

To specify the aaa-server group to use for user authentication, use the **authentication-server-group** command in tunnel-group general-attributes mode. To return this command to the default, use the **no** form of this command.

authentication-server-group [(*interface name*)] *server group* [**LOCAL** | **NONE**]

no authentication-server-group [(*interface name*)] *server group*

Syntax Description

<i>interface name</i>	(Optional) Specifies the interface the IPsec tunnel terminates.
LOCAL	(Optional) Specifies authentication to be performed against the local user database if all of the servers in the server group have been deactivated due to communication failures. If the server group name is either LOCAL or NONE , do not use the LOCAL keyword here.
NONE	(Optional) Specifies the server group name as none. To indicate that authentication is not required, use the NONE keyword as the server group name.
<i>server group</i>	Specifies the name of the aaa-server group, which defaults to LOCAL .

Defaults

The default setting for this command is **LOCAL**.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

You can apply this attribute to the IPsec remote access tunnel-group type only:

Examples

The following example entered in config-general configuration mode, configures an authentication server group named aaa-server456 for an IPsec remote-access tunnel group named remotegrp:

```
hostname(config)# tunnel-group remotegrp type ipsec_ra
hostname(config)# tunnel-group remotegrp general
hostname(config-general)# authentication-server-group aaa-server456
hostname(config-general)#
```

Related Commands

Command	Description
aaa-server host	Configures AAA-server parameters.
clear configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group.
tunnel-group-map default-group	Associates the certificate map entries created using the crypto ca certificate map command with tunnel groups.

authorization-dn-attributes

To specify what part of the subject DN field to use as the username for authorization, use the **authorization-dn-attributes** command in tunnel-group ipsec-attributes configuration mode. To return this command to the default, use the **no** form of this command.

[no] authorization-dn-attributes {*primary-attr* [*secondary-attr*] | **use-entire-name**}

Syntax Description

<i>primary-attr</i>	Specifies the attribute to use in deriving a name for an authorization query from a certificate.
<i>secondary-attr</i>	(Optional) Specifies an additional attribute to use in deriving a name for an authorization query from a certificate, if the primary attribute does not exist.
use-entire-name	Specifies that the FWSM should use the entire subject DN (RFC 1779) to derive the name.

Defaults

The default value for the primary attribute is Common Name.

The default value for the secondary attribute is Organization Unit.

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 ipsec-attributes configuration	•	•	•	•	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

You can apply this attribute to IPSec remote access tunnel type only.

Primary and secondary attributes include the following:

Attribute	Definition
CN	Common Name: the name of a person, system, or other entity
OU	Organizational Unit: the subgroup within the organization (O)
O	Organization: the name of the company, institution, agency, association or other entity
L	Locality: the city or town where the organization is located
SP	State/Province: the state or province where the organization is located

Attribute	Definition
C	Country: the two-letter country abbreviation. These codes conform to ISO 3166 country abbreviations.
EA	E-mail address
T	Title
N	Name
GN	Given Name
SN	Surname
I	Initials
GENQ	Generational Qualifier
DNQ	Domain Name Qualifier
UID	User Identifier

Examples

The following example entered in config-ipsec configuration mode, creates a remote access tunnel group (ipsec_ra) named remotegrp, specifies IPsec group attributes and defines the Common Name to be used as the username for authorization:

```
hostname(config)# tunnel-group remotegrp type ipsec_ra
hostname(config)# tunnel-group remotegrp ipsec-attributes
hostname(config-ipsec)# authorization-dn-attributes CN
hostname(config-ipsec)#
```

Related Commands

Command	Description
clear configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the indicated certificate map entry.
tunnel-group-map default-group	Associates the certificate map entries created using the crypto ca certificate map command with tunnel groups.

authorization-required

To require users to authorize successfully to connect, use the **authorization-required** command in tunnel-group ipsec-attributes configuration mode. To return this command to the default, use the **no** form of this command.

[no] authorization-required

Defaults

The default setting of this command 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
Tunnel-group general attributes configuration	•	•	•	•	—

Syntax Description

This command has no arguments or keywords.

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

You can apply this attribute to IPSec remote-access tunnel-group type only.

Examples

The following example entered in config-ipsec configuration mode, requires authorization based on the complete DN for users connecting through a remote-access tunnel group named remotegrp. The first command configures the tunnel-group type as ipsec_ra (IPSec remote access) for the remote group named remotegrp. The second command enters ipsec-attributes mode for the specified tunnel group, and the last command specifies authorization required for the named tunnel group:

```
hostname(config)# tunnel-group remotegrp type ipsec_ra
hostname(config)# tunnel-group remotegrp ipsec-attributes
hostname(config-ipsec)# authorization-required
hostname(config-ipsec)#
```

Related Commands

Command	Description
clear configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the indicated certificate map entry.
tunnel-group-map default-group	Associates the certificate map entries created using the crypto ca certificate map command with tunnel groups.

authorization-server-group

To specify the aaa-server group for user authorization, use the **authorization-server-group** command in tunnel-group general-attributes mode. To return this command to the default, use the **no** form of this command.

authorization-server-group *server group*

no authorization-server-group

Syntax Description

server group Specifies the name of the aaa-server group, which defaults to **none**.

Defaults

The default setting for this command is **no authorization-server-group**.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

You can apply this attribute only to IPSec remote access tunnel-group types.

When VPN Authorization is defined as LOCAL, the attributes configured in the default group policy DfltGrpPolicy are enforced.

Examples

The following example entered in config-general configuration mode, configures an authorization server group named “aaa-server78” for an IPSec remote-access tunnel group named “remotegrp”:

```
hostname(config)# tunnel-group remotegrp type ipsec-ra
hostname(config)# tunnel-group remotegrp general
hostname(config-general)# authorization-server-group aaa-server78
hostname(config-general)#
```

Related Commands

Command	Description
aaa-server host	Configures AAA-server parameters.
clear configure tunnel-group	Clears all configured tunnel groups.

Command	Description
show running-config tunnel-group	Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group.
tunnel-group-map default-group	Associates the certificate map entries created using the crypto ca certificate map command with tunnel groups.

auth-prompt

To specify or change the AAA challenge text for through-the-FWSM user sessions, use the **auth-prompt** command in global configuration mode. To remove the authentication challenge text, use the **no** form of this command.

auth-prompt {**prompt** | **accept** | **reject**} *string*

no auth-prompt {**prompt** | **accept** | **reject**}

Syntax Description

accept	If a user authentication via Telnet is accepted, display the prompt <i>string</i> .
prompt	The AAA challenge prompt string follows this keyword.
reject	If a user authentication via Telnet is rejected, display the prompt <i>string</i> .
<i>string</i>	A string of up to 235 alphanumeric characters or 31 words, limited by whichever maximum is first reached. Special characters, spaces, and punctuation characters are permitted. Entering a question mark or pressing the Enter key ends the string. (The question mark appears in the string.)

Defaults

If you do not specify an authentication prompt, the prompt users see when they log in depends on the protocol they use:

- Users who log in using HTTP see the following prompt: `HTTP Authentication`.
- Users who log in using FTP see the following prompt: `FTP Authentication`.
- Users who log in using Telnet see no prompt.

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	•	•	—	—	•

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

The **auth-prompt** command lets you specify the AAA challenge text for HTTP, FTP, and Telnet access through the FWSM when requiring user authentication from TACACS+ or RADIUS servers. This text is primarily for cosmetic purposes and displays above the username and password prompts that users view when logging in.

If the user authentication occurs from Telnet, you can use the **accept** and **reject** options to display different status prompts to indicate that the authentication attempt is accepted or rejected by the AAA server.

If the AAA server authenticates the user, the FWSM displays the **auth-prompt accept** text, if specified, to the user; otherwise it displays the **reject** text, if specified. Authentication of HTTP and FTP sessions displays only the challenge text at the prompt. The **accept** and **reject** text are not displayed.

**Note**

Customizing the login prompt causes the FWSM to use MSCHAPv2 for the user password. Please check for MSCHAPv2 compatibility with your RADIUS server and back-end database before enabling this feature.

Microsoft Internet Explorer displays up to 37 characters in an authentication prompt. Netscape Navigator displays up to 120 characters, and Telnet and FTP display up to 235 characters in an authentication prompt.

Examples

The following example sets the authentication prompt to the string “Please enter your username and password.”:

```
hostname(config)# auth-prompt prompt Please enter your username and password
```

After this string is added to the configuration, users see the following:

```
Please enter your username and password
User Name:
Password:
```

For Telnet users, you can also provide separate messages to display when the FWSM accepts or rejects the authentication attempt; for example:

```
hostname(config)# auth-prompt reject Authentication failed. Try again.
hostname(config)# auth-prompt accept Authentication succeeded.
```

The following example sets the authentication prompt for a successful authentication to the string, “You are OK.”

```
hostname(config)# auth-prompt accept You are OK.
```

After successfully authenticating, the user sees the following message:

```
You are OK.
```

Related Commands

Command	Description
clear configure auth-prompt	Removes the previously specified authentication prompt challenge text and reverts to the default value, if any.
show running-config auth-prompt	Displays the current authentication prompt challenge text.

auto-update device-id

To configure the FWSM device ID for use with an Auto Update Server, use the **auto-update device-id** command in global configuration mode. To remove the device ID, use the **no** form of this command.

```
auto-update device-id [hardware-serial | hostname | ipaddress [if_name] |
  mac-address [if_name] | string text]
```

```
no auto-update device-id [hardware-serial | hostname | ipaddress [if_name] |
  mac-address [if_name] | string text]
```

Syntax Description

hardware-serial	Uses the hardware serial number of the FWSM to uniquely identify the device.
hostname	Uses the hostname of the FWSM to uniquely identify the device.
ipaddress [if_name]	Uses the IP address of the FWSM to uniquely identify the FWSM. By default, the FWSM uses the interface used to communicate with the Auto Update Server. If you want to use a different IP address, specify the <i>if_name</i> .
mac-address [if_name]	Uses the MAC address of the FWSM to uniquely identify the FWSM. By default, the FWSM uses the MAC address of the interface used to communicate with the Auto Update Server. If you want to use a different MAC address, specify the <i>if_name</i> .
string text	Specifies the text string to uniquely identify the device to the Auto Update Server.

Defaults

The default ID is the hostname.

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	•	•	•	—	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

The following example sets the device ID to the serial number:

```
hostname(config)# auto-update device-id hardware-serial
```

Related Commands

auto-update poll-period	Sets how often the FWSM checks for updates from an Auto Update Server.
auto-update server	Identifies the Auto Update Server.
auto-update timeout	Stops traffic from passing through the FWSM if the Auto Update Server is not contacted within the timeout period.
clear configure auto-update	Clears the Auto Update Server configuration
show running-config auto-update	Shows the Auto Update Server configuration.

auto-update poll-period

To configure how often the FWSM checks for updates from an Auto Update Server, use the **auto-update poll-period** command in global configuration mode. To reset the parameters to the defaults, use the **no** form of this command.

auto-update poll-period *poll_period* [*retry_count* [*retry_period*]]

no auto-update poll-period *poll_period* [*retry_count* [*retry_period*]]

Syntax Description

<i>poll_period</i>	Specifies how often, in minutes, to poll an Auto Update Server, between 1 and 35791. The default is 720 minutes (12 hours).
<i>retry_count</i>	Specifies how many times to try reconnecting to the Auto Update Server if the first attempt fails. The default is 0.
<i>retry_period</i>	Specifies how long to wait, in minutes, between connection attempts, between 1 and 35791. The default is 5 minutes.

Defaults

The default poll period is 720 minutes (12 hours).

The default number of times to try reconnecting to the Auto Update Server if the first attempt fails is 0.

The default period to wait between connection attempts is 5 minutes.

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	•	•	•	—	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

The following example sets the poll period to 360 minutes, the retries to 1, and the retry period to 3 minutes:

```
hostname(config)# auto-update poll-period 360 1 3
```

Related Commands

auto-update device-id	Sets the FWSM device ID for use with an Auto Update Server.
auto-update server	Identifies the Auto Update Server.

auto-update timeout	Stops traffic from passing through the FWSM if the Auto Update Server is not contacted within the timeout period.
clear configure auto-update	Clears the Auto Update Server configuration
show running-config auto-update	Shows the Auto Update Server configuration.

auto-update server

To identify the Auto Update Server, use the **auto-update server** command in global configuration mode. To remove the server, use the **no** form of this command. The FWSM periodically contacts the Auto Update Server for any configuration, operating system, and ASDM updates.

auto-update server *url* [*verify-certificate*]

no auto-update server *url* [*verify-certificate*]

Syntax Description

<i>url</i>	Specifies the location of the Auto Update Server using the following syntax: http[s]:[[user:password@]location [:port]] / pathname
<i>verify_certificate</i>	Verifies the certificate returned by the Auto Update Server.

Defaults

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	•	•	•	—	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

Only one server can be configured.

Examples

The following example sets the Auto Update Server URL:

```
hostname(config)# auto-update server http://10.1.1.1:1741/
```

Related Commands

auto-update device-id	Sets the FWSM device ID for use with an Auto Update Server.
auto-update poll-period	Sets how often the FWSM checks for updates from an Auto Update Server.
auto-update timeout	Stops traffic from passing through the FWSM if the Auto Update Server is not contacted within the timeout period.

clear configure auto-update	Clears the Auto Update Server configuration
show running-config auto-update	Shows the Auto Update Server configuration.

auto-update timeout

To set a timeout period in which to contact the Auto Update Server, use the **auto-update timeout** command in global configuration mode. If the Auto Update Server has not been contacted for the timeout period, the FWSM stops all traffic through the FWSM. Set a timeout to ensure that the FWSM has the most recent image and configuration. To remove the timeout, use the **no** form of this command.

auto-update timeout *period*

no auto-update timeout [*period*]

Syntax Description	<i>period</i>	Specifies the timeout period in minutes between 1 and 35791. The default is 0, which means there is no timeout. You cannot set the timeout to 0; use the no form of the command to reset it to 0.
---------------------------	---------------	--

Defaults The default timeout is 0, which sets the FWSM to never time out.

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	•	•	•	—	—

Command History	Release	Modification
	3.1(1)	This command was introduced.

Usage Guidelines A timeout condition is reported with system log message 201008.

Examples The following example sets the timeout to 24 hours:

```
hostname(config)# auto-update timeout 1440
```

Related Commands	auto-update device-id	Sets the FWSM device ID for use with an Auto Update Server.
	auto-update poll-period	Sets how often the FWSM checks for updates from an Auto Update Server.
	auto-update server	Identifies the Auto Update Server.

clear configure auto-update	Clears the Auto Update Server configuration
show running-config auto-update	Shows the Auto Update Server configuration.
