Cisco IOS Commands for ASASM

clear diagnostics loopback

To clear the online diagnostic test configuration, use the clear diagnostic **loopback** command in privileged EXEC mode.

clear diagnostics loopback

Syntax Description

This command has no arguments or keywords

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Usage Guidelines

The **clear diagnostics loopback** command clears the online diagnostic test configuration.

Examples

The following is sample output from the **clear diagnostics loopback** command:

```
ciscoasa#
clear diagnostics loopback
Port  Test  Pkts-received    Failures
0  0  0    0
1  0  0    0
```

Related Commands

Command	Description
show diagnostics loopback	Shows the information related to the PC loopback test, the number of tests run, the number of loopback packets received, and the number of failures detected.

firewall autostate

To enable autostate messaging, use the **firewall autostate** command in global configuration mode. To disable autostate, use the **no** form of this command.

firewall autostate
no firewall autostate

Syntax Description

This command has no arguments or keywords.

Command Default

By default, autostate is disabled.

Command Modes

Global configuration

Usage Guidelines

Autostate messaging lets the ASA quickly detect that a switch interface has failed or has come up. The supervisor engine can send autostate messages to the ASA about the status of physical interfaces associated with ASA VLANs. For example, when all physical interfaces associated with a VLAN go down, the autostate message tells the ASA that the VLAN is down. This information lets the ASA declare the VLAN as down, bypassing the interface monitoring tests normally required for determining which side suffered a link failure. Autostate messaging provides a dramatic improvement in the time the ASA takes to detect a link failure (a few milliseconds as compared to up to 45 seconds without autostate support).

The switch supervisor sends an autostate message to the ASA when:

- The last interface belonging to a VLAN goes down.
- The first interface belonging to a VLAN comes up.

Examples

The following example enables autostate messaging:

```
Router(config)# firewall autostate
```

Related Commands

Command	Description
show firewall autostate	Shows the setting of the autostate feature.

firewall module

To assign firewall groups to the ASA, enter the **firewall module** command in global configuration mode. To remove the groups, use the **no** form of this command.

firewall module *module_number* **vlan-group** *firewall_group*
no firewall module *module_number* **vlan-group** *firewall_group*

Syntax Description

module_number	Specifies the module number. Use the **show module** command to view installed modules and their numbers.
vlan-group *firewall_group*	Specifies one or more group numbers as defined by the **firewall vlan-group** command: • A single number (*n*) • A range (*n-x*) Separate numbers or ranges by commas. For example, enter the following numbers: `5,7-10`

Command Default

No default behavior or values.

Command Modes

Global configuration

Usage Guidelines

- You can assign up to 16 firewall VLAN groups to each ASASM. (You can create more than 16 VLAN groups in Cisco IOS software, but only 16 can be assigned per ASASM.) See the **firewall vlan-group** command to create a group. For example, you can assign all the VLANs to one group; or you can create an inside group and an outside group; or you can create a group for each customer.
- There is no limit on the number of VLANs per group, but the ASASM can only use VLANs up to the ASASM system limit (see the ASASM licensing documentation for more information).
- You cannot assign the same VLAN to multiple firewall groups.
- You can assign a single firewall group to multiple ASASMs. VLANs that you want to assign to multiple ASASMs, for example, can reside in a separate group from VLANs that are unique to each ASASM.
- If you are using ASASM failover within the same switch chassis, do not assign the VLAN(s) that you are reserving for failover and stateful communications to a switch port. However, if you are using failover between chassis, you must include the VLANs in the trunk port between the chassis.
- If you do not add the VLANs to the switch before you assign them to the ASASM, the VLANs are stored in the supervisor engine database and are sent to the ASASM as soon as they are added to the switch.
- You can configure a VLAN in the ASASM configuration before it has been assigned on the switch. Note that when the switch sends the VLAN to the ASASM, the VLAN defaults to be administratively up on the ASASM, regardless of whether the you shut them down in the ASASM configuration. You need to shut them down again in this case.

Examples

The following example shows how to create three firewall VLAN groups: one for each ASA, and one that includes VLANs assigned to both ASAs.

```
Router(config)# firewall vlan-group 50 55-57
Router(config)# firewall vlan-group 51 70-85
Router(config)# firewall vlan-group 52 100
Router(config)# firewall module 5 vlan-group 50,52
Router(config)# firewall module 8 vlan-group 51,52
```

The following is sample output from the show firewall vlan-group command:

```
Router# show firewall vlan-group
Group vlans
----- ------
   50 55-57
   51 70-85
   52 100
```

The following is sample output from the show firewall module command, which shows all VLAN groups:

```
Router# show firewall module
Module Vlan-groups
  5    50,52
  8    51,52
```

Related Commands

Command	Description
firewall vlan-group	Assigns VLANs to a VLAN group.
show firewall module vlan-group	Shows the VLAN groups and the VLANs assigned to them.
show module	Shows all installed modules.

firewall multiple-vlan-interfaces

To allow you to add more than one SVI to the ASA, use the **firewall multiple-vlan-interfaces** command in global configuration mode. To disable this feature, use the **no** form of this command.

firewall multiple-vlan-interfaces
no firewall multiple-vlan-interfaces

Syntax Description

This command has no arguments or keywords.

Command Default

By default, multiple SVIs are not allowed.

Command Modes

Global configuration

Usage Guidelines

A VLAN defined on the MSFC is called a switched virtual interface. If you assign the VLAN used for the SVI to the ASA, then the MSFC routes between the ASA and other Layer 3 VLANs. For security reasons, by default, only one SVI can exist between the MSFC and the ASA. For example, if you misconfigure the system with multiple SVIs, you could accidentally allow traffic to pass around the ASA by assigning both the inside and outside VLANs to the MSFC.

However, you might need to bypass the ASA in some network scenarios. For example, if you have an IPX host on the same Ethernet segment as IP hosts, you will need multiple SVIs. Because the ASA in routed firewall mode only handles IP traffic and drops other protocol traffic like IPX (transparent firewall mode can optionally allow non-IP traffic), you might want to bypass the ASA for IPX traffic. Make sure to configure the MSFC with an access list that allows only IPX traffic to pass on the VLAN.

For transparent firewalls in multiple context mode, you need to use multiple SVIs because each context requires a unique VLAN on its outside interface. You might also choose to use multiple SVIs in routed mode so you do not have to share a single VLAN for the outside interface.

Examples

The following example shows a typical configuration with multiple SVIs:

```
Router(config)# firewall vlan-group 50 55-57
Router(config)# firewall vlan-group 51 70-85
Router(config)# firewall module 8 vlan-group 50-51
Router(config)# firewall multiple-vlan-interfaces
Router(config)# interface vlan 55
Router(config-if)# ip address 10.1.1.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# interface vlan 56
Router(config-if)# ip address 10.1.2.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# end
Router#
```

The following is sample output from the show interface command:

```
Router# show interface vlan 55
Vlan55 is up, line protocol is up
  Hardware is EtherSVI, address is 0008.20de.45ca (bia 0008.20de.45ca)
  Internet address is 55.1.1.1/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
   reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
ARP type:ARPA, ARP Timeout 04:00:00
Last input never, output 00:00:08, output hang never
Last clearing of "show interface" counters never
Input queue:0/75/0/0 (size/max/drops/flushes); Total output drops:0
Queueing strategy:fifo
Output queue :0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
L2 Switched:ucast:196 pkt, 13328 bytes - mcast:4 pkt, 256 bytes
L3 in Switched:ucast:0 pkt, 0 bytes - mcast:0 pkt, 0 bytes mcast
L3 out Switched:ucast:0 pkt, 0 bytes
   0 packets input, 0 bytes, 0 no buffer
   Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
   4 packets output, 256 bytes, 0 underruns
   0 output errors, 0 interface resets
   0 output buffer failures, 0 output buffers swapped out
```

Related Commands

Command	Description
firewall module	Assigns a VLAN group to the ASA.
firewall vlan-group	Defines a VLAN group.

firewall vlan-group

To assign VLANs to a firewall group, enter the **firewall vlan-group** command in global configuration mode. To remove the VLANs, use the **no** form of this command.

firewall [**switch** { **1** | **2** }] **vlan-group** *firewall_group vlan_range*
no firewall [**switch** { **1** | **2** }] **vlan-group** *firewall_group vlan_range*

Syntax Description

firewall_group	Specifies the group ID as an integer.
vlan_range	Specifies the VLANs assigned to the group. The *vlan_range* value can be one or more VLANs (2 to 1000 and from 1025 to 4094) identified in one of the following ways: • A single number (*n*) • A range (*n*-*x*) Separate numbers or ranges by commas. For example, enter the following numbers: `5,7-10,13,45-100` **Note** Routed ports and WAN ports consume internal VLANs, so it is possible that VLANs in the 1020-1100 range might already be in use.
switch {**1**|**2**}	(Optional) For VSS configurations, specifies the switch number.

Command Default

No default behavior or values.

Command Modes

Global configuration.

Usage Guidelines

- You can assign up to 16 firewall VLAN groups to each ASASM using the **firewall module** command. (You can create more than 16 VLAN groups in Cisco IOS software, but only 16 can be assigned per ASASM.) For example, you can assign all the VLANs to one group; or you can create an inside group and an outside group; or you can create a group for each customer.
- There is no limit on the number of VLANs per group, but the ASASM can only use VLANs up to the ASASM system limit (see the ASASM licensing documentation for more information).
- You cannot assign the same VLAN to multiple firewall groups.
- You can assign a single firewall group to multiple ASASMs. VLANs that you want to assign to multiple ASASMs, for example, can reside in a separate group from VLANs that are unique to each ASASM.
- Use VLAN IDs 2 to 1000 and from 1025 to 4094.
- Routed ports and WAN ports consume internal VLANs, so it is possible that VLANs in the 1020-1100 range might already be in use.
- You cannot use reserved VLANs.
- You cannot use VLAN 1.

- If you are using ASASM failover within the same switch chassis, do not assign the VLAN(s) that you are reserving for failover and stateful communications to a switch port. However, if you are using failover between chassis, you must include the VLANs in the trunk port between the chassis.
- If you do not add the VLANs to the switch before you assign them to the ASASM, the VLANs are stored in the supervisor engine database and are sent to the ASASM as soon as they are added to the switch.
- You can configure a VLAN in the ASASM configuration before it has been assigned on the switch. Note that when the switch sends the VLAN to the ASASM, the VLAN defaults to be administratively up on the ASASM, regardless of whether the you shut them down in the ASASM configuration. You need to shut them down again in this case.

Examples

The following example shows how to create three firewall VLAN groups: one for each ASA, and one that includes VLANs assigned to both ASAs.

```
Router(config)# firewall vlan-group 50 55-57
Router(config)# firewall vlan-group 51 70-85
Router(config)# firewall vlan-group 52 100
Router(config)# firewall module 5 vlan-group 50,52
Router(config)# firewall module 8 vlan-group 51,52
```

The following is sample output from the show firewall vlan-group command:

```
Router# show firewall vlan-group
Group vlans
----- ------
   50 55-57
   51 70-85
   52 100
```

The following is sample output from the show firewall module command, which shows all VLAN groups:

```
Router# show firewall module
Module Vlan-groups
  5    50,52
  8    51,52
```

Related Commands

Command	Description
firewall module	Assigns a VLAN group to an ASA.
show firewall vlan-group	Shows the VLAN groups and the VLANs assigned to them.
show module	Shows all installed modules.

service-module session

To gain console access to the ASASM from the switch CLI, enter the **service-module session** command in privileged EXEC mode.

service-module session [**switch** { **1 | 2** }] **slot** *number*

Syntax Description

slot *number*	Specifies the slot number of the ASASM. To view the module slot numbers, enter the **show module** command at the switch prompt.
switch {**1** | **2**}	(Optional) For VSS configurations, specifies the switch number.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Usage Guidelines

Using the **service-module session** command, you create a virtual console connection to the ASASM, with all the benefits and limitations of an actual console connection.

Benefits include:

- The connection is persistent across reloads and does not time out.
- You can stay connected through ASASM reloads and view startup messages.
- You can access ROMMON if the ASASM cannot load the image.

Limitations include:

- The connection is slow (9600 baud).
- You can only have one console connection active at a time.

Note Because of the persistence of the connection, if you do not properly log out of the ASASM, the connection may exist longer than intended. If someone else wants to log in, they will need to kill the existing connection. See the CLI configuration guide for more information.

Examples

The following example shows how to gain console access to an ASASM in slot 3:

```
Router# service-module session slot 3
ciscoasa>
```

Related Commands

Commands	Description
session	Telnets to the ASASM over the backplane.

session

To Telnet from the switch CLI to the ASASM over the backplane, use the **session** command in privileged EXEC mode.

session [**switch** { **1** | **2** }] **slot** *number* **processor 1**

Syntax Description

processor 1	Specifies the processor number, which is always 1.
slot *number*	Specifies the slot number. To view the module slot numbers, enter the **show module** command at the switch prompt.
switch {**1** | **2**}	(Optional) For VSS configurations, specifies the switch number.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Usage Guidelines

Using the **session** command, you create a Telnet connection to the ASASM.

Benefits include:

- You can have multiple sessions to the ASASM at the same time.
- The Telnet session is a fast connection.

Limitations include:

- The Telnet session is terminated when the ASASM reloads, and can time out.
- You cannot access the ASASM until it completely loads; you cannot access ROMMON.

Note The **session** *slot* **processor 0** command, which is supported on other services modules, is not supported on the ASASM; the ASASM does not have a processor 0.

You are prompted for the login password. Enter the login password to the ASASM. By default, the password is **cisco**.

You access user EXEC mode.

Examples

The following example Telnets to an ASASM in processor 1:

```
Router# session slot number processor 1
ciscoasa passwd: cisco
ciscoasa>
```

Related Commands

Command	Description
service-module session	Obtains console access to the ASASM from the switch CLI.

show boot device

To view the default boot partition, use the **show boot device** command.

show boot device [*mod_num*]

Syntax Description

mod_num	(Optional) Specifies the module number. Use the **show module** command to view installed modules and their numbers.

Command Default

The default boot partition is cf:4.

Command Modes

Privileged EXEC.

Examples

The following is sample output from the **show boot device** command that shows the boot partitions for each installed ASA on Cisco IOS software:

```
Router# show boot device
[mod:1 ]:
[mod:2 ]:
[mod:3 ]:
[mod:4 ]: cf:4
[mod:5 ]: cf:4
[mod:6 ]:
[mod:7 ]: cf:4
[mod:8 ]:
[mod:9 ]:
```

Related Commands

Command	Description
boot device (IOS)	Sets the default boot partition.
show module (IOS)	Shows all installed modules.

show diagnostic loopback

To display information related to the PC loopback test, including the number of tests run, the number of loopback packets received, and the number of failures detected, use the **show diagnostics loopback** command in privileged EXEC mode.

show diagnostics loopback

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		Secuity Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
12.2(18)SXF5	This command was added.

Usage Guidelines

The **show diagnostics loopback command provides** information related to the PC loopback test, including the number of tests run, the number of loopback packets received, and the number of failures detected.

Examples

The following is sample output from the **show diagnostics loopback** command:

```
ciscoasa#
show diagnostics loopback
Port  Test  Pkts-received    Failures
0  447  447    0
1  447  447    0
```

Related Commands

Command	Description
clear diagnostics loopback	Clears the online diagnostic test configuration.
firewall autostate	Enables the autostate feature.

show firewall autostate

To view the setting of the autostate feature, use the **show firewall autostate** command in privileged EXEC mode.

show firewall autostate

Syntax Description

This command has no arguments or keywords.

Command Default

By default, autostate is disabled.

Command Modes

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

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

Usage Guidelines

Autostate messaging in Cisco IOS software allows the ASA to quickly detect that a switch interface has failed or come up. The switch supervisor sends an autostate message to the ASA when:

- The last interface belonging to a VLAN goes down.
- The first interface belonging to a VLAN comes up.

Related Commands

Command	Description
clear diagnostics loopback	Clears the online diagnostic test configuration.
firewall autostate	Enables the autostate feature.

show firewall module

To view the VLAN groups assigned to each ASA, enter the **show firewall module** command in privileged EXEC mode.

show firewall [**switch** { **1** | **2** }] **module** [*module_number*]

Syntax Description

module_number	(Optional) Specifies the module number. Use the **show module** command to view installed modules and their numbers.
switch { **1** | **2** }	(Optional) For VSS configurations, specifies the switch number.

Command Default

No default behavior or values.

Command Modes

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

Command Modes

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

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

Examples

The following is sample output from the show firewall module command, which shows all VLAN groups:

```
Router# show firewall module
Module Vlan-groups
  5    50,52
  8    51,52
```

Related Commands

Command	Description
firewall module	Assigns a VLAN group to an ASA.
firewall vlan-group	Assigns VLANs to a VLAN group.
show firewall module vlan-group	Shows the VLAN groups and the VLANs assigned to them.
show module	Shows all installed modules.

show firewall module state

To view the state of each ASA, enter the **show firewall module state** command in privileged EXEC mode.

show firewall [**switch** { **1 | 2** }] **module** [*module_number*] **state**

Syntax Description

module_number	(Optional) Specifies the module number.
switch { **1** | **2** }	(Optional) For VSS configurations, specifies the switch 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		Secuity Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	•	•	•	•	•

Examples

The following is sample output from the show firewall module state command:

```
Router# show firewall module 11 state
Firewall module 11:
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: 3,6,7,20-24,40,59,85,87-89,99-115,150,188-191,200,250,
     501-505,913,972
Pruning VLANs Enabled: 2-1001
Vlans allowed on trunk:
Vlans allowed and active in management domain:
Vlans in spanning tree forwarding state and not pruned:
```

Related Commands

Command	Description
firewall module	Assigns a VLAN group to an ASA.
firewall vlan-group	Assigns VLANs to a VLAN group.
show firewall module vlan-group	Shows the VLAN groups and the VLANs assigned to them.

Command	Description
show module	Shows all installed modules.

show firewall module traffic

To view the traffic flowing through each ASA, enter the **show firewall module traffic** command in privileged EXEC mode.

show firewall [**switch** { **1 | 2** }] **module** [*module_number*] **traffic**

Syntax Description

module_number	(Optional) Specifies the module number.
switch { **1** | **2** }	(Optional) For VSS configurations, specifies the switch 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		Secuity Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	•	•	•	•	•

Examples

The following is sample output from the show firewall module traffic command:

```
Router# show firewall module 11 traffic
Firewall module 11:
Specified interface is up line protocol is up (connected)
  Hardware is EtherChannel, address is 0014.1cd5.bef6 (bia 0014.1cd5.bef6)
  MTU 1500 bytes, BW 6000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Full-duplex, 1000Mb/s, media type is unknown
  input flow-control is on, output flow-control is on
  Members in this channel: Gi11/1 Gi11/2 Gi11/3 Gi11/4 Gi11/5 Gi11/6
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 10000 bits/sec, 17 packets/sec
     8709 packets input, 845553 bytes, 0 no buffer
     Received 745 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     18652077 packets output, 1480488712 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

Related Commands

Command	Description
firewall module	Assigns a VLAN group to an ASA.
firewall vlan-group	Assigns VLANs to a VLAN group.
show firewall module vlan-group	Shows the VLAN groups and the VLANs assigned to them.
show module	Shows all installed modules.

show firewall module version

To view the software version number of the ASA Services Module, enter the **show firewall module version** command in privileged EXEC mode.

show firewall [**switch** { **1** | **2** }] **module** [*module_number*] **version**

Syntax Description

module_number	(Optional) Specifies the module number.
switch {**1** | **2**}	(Optional) For VSS configurations, specifies the switch 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		Secuity Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Examples

The following is sample output from the show firewall module version command:

```
Router# show firewall switch 1 module 2 version
ASA Service Module 2:
Sw Version: 100.7(8)19
```

Related Commands

Command	Description
firewall module	Assigns a VLAN group to an ASA.
firewall vlan-group	Creates a group of VLANs.
show module	Shows all installed modules.

show firewall module vlan-group

To view VLAN groups that can be assigned to the ASA, enter the**show firewall module vlan-group** command in privileged EXEC mode.

show firewall [**switch** { **1** | **2** }] **module** [*module_number*] **vlan-group** [*firewall_group*]

Syntax Description

firewall_group	(Optional) Specifies the group ID.
module_number	(Optional) Specifies the module number.
switch {**1** | **2**}	(Optional) For VSS configurations, specifies the switch 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		Secuity Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	•	•	•	•	•

Examples

The following is sample output from the show firewall module vlan-group command:

```
Router# show firewall module vlan-group
Group vlans
----- ------
   50 55-57
   51 70-85
   52 100
```

Related Commands

Command	Description
firewall module	Assigns a VLAN group to an ASA.
firewall vlan-group	Creates a group of VLANs.
show module	Shows all installed modules.

show firewall multiple-vlan-interfaces

To show the state of multiple firewall VLAN interfaces for the ASASM, enter the **show firewall multiple-vlan-interfaces** command in privileged EXEC mode.

show firewall multiple-vlan-interfaces

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		Secuity Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	•	•	•	•	•

Examples

The following is sample output from the show firewall multiple-vlan-interfaces command:

```
Router# show firewall multiple-vlan-interfaces
Multiple firewall vlan interfaces feature is enabled
```

Related Commands

Command	Description
firewall module	Assigns a VLAN group to an ASA.
firewall vlan-group	Creates a group of VLANs.
show module	Shows all installed modules.

show module

To verify that the switch acknowledges the ASASM and has brought it online, use the **show module** command in privileged EXEC mode.

show module [**switch** { **1 | 2** }] [*mod-num* | **all**]

Syntax Description

all	(Optional) Specifies all the modules.
mod_num	(Optional) Specifies the module number.
switch { **1** | **2** }	(Optional) For VSS configurations, specifies the switch 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		Secuity Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	•	•	•	•	•

Examples

The following is sample output from the show module command:

```
Router# show module
Mod Ports Card Type                                Model              Serial No.
--- ----- ------------------------------------- ------------------- -----------
 2    3  ASA Service Module                     WS-SVC-ASA-SM1     SAD143502E8
 4    3  ASA Service Module                     WS-SVC-ASA-SM1     SAD135101Z9
 5    5  Supervisor Engine 720 10GE (Active)    VS-S720-10G        SAL12426KB1
 6   16  CEF720 16 port 10GE                    WS-X6716-10GE      SAL1442WZD1
Mod MAC addresses                       Hw     Fw           Sw           Status
--- ---------------------------------- ------ ------------ ------------ -------
 2  0022.bdd4.016f to 0022.bdd4.017e   0.201 12.2(2010080 12.2(2010121 Ok
 4  0022.bdd3.f64e to 0022.bdd3.f655   0.109 12.2(2010080 12.2(2010121 PwrDown
 5  0019.e8bb.7b0c to 0019.e8bb.7b13   2.0   8.5(2)       12.2(2010121 Ok
 6  f866.f220.5760 to f866.f220.576f   1.0   12.2(18r)S1  12.2(2010121 Ok
Mod  Sub-Module                  Model              Serial       Hw     Status
---- -------------------------- ------------------ ----------- ------- -------
2/0 ASA Application Processor   SVC-APP-PROC-1     SAD1436015D  0.202  Other
4/0 ASA Application Processor   SVC-APP-INT-1      SAD141002AK  0.106  PwrDown
 5  Policy Feature Card 3       VS-F6K-PFC3C       SAL12437BM2  1.0    Ok
 5  MSFC3 Daughterboard         VS-F6K-MSFC3       SAL12426DE3  1.0    Ok
 6  Distributed Forwarding Card WS-F6700-DFC3C     SAL1443XRDC  1.4    Ok
Base PID:
Mod  Model            Serial No.
---- -----------      ----------
 2 WS-SVC-APP-HW-1    SAD143502E8
 4 TRIFECTA           SAD135101Z9
Mod  Online Diag Status
---- -------------------
 2  Pass
2/0 Not Applicable
 4  Not Applicable
4/0 Not Applicable
 5  Pass
 6  Pass
```

Related Commands

Command	Description
firewall module	Assigns a VLAN group to an ASA.
firewall vlan-group	Creates a group of VLANs.