CHAPTER 4

backup-servers through bridge-group Commands

backup-servers

To configure backup servers, use the **backup-servers** command in group-policy configuration mode. To remove a backup server, use the **no** form of this command.

backup-servers {*server1 server2. . . . server10* | **clear-client-config** | **keep-client-config**}

no backup-servers [*server1 server2. . . . server10* | **clear-client-config** | **keep-client-config**]

Syntax Description

clear-client-config	Specifies that the client uses no backup servers. The FWSM pushes a null server list.
keep-client-config	Specifies that the FWSM sends no backup server information to the client. The client uses its own backup server list, if configured.
server1 server 2.... server10	Provides a space delimited, priority-ordered list of servers for the VPN client to use when the primary FWSM is unavailable. Identifies servers by IP address or hostname. The list can be 500 characters long, but can contain only 10 entries.

Defaults

Backup servers do not exist until you configure them, either on the client or on the primary FWSM.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Group-policy configuration	•	•	•	•	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

To remove the backup-servers attribute from the running configuration, use the **no** form of this command without arguments. This enables inheritance of a value for backup-servers from another group policy.

IPSec backup servers let a VPN client connect to the central site when the primary FWSM is unavailable. When you configure backup servers, the FWSM pushes the server list to the client as the IPSec tunnel is established.

Configure backup servers either on the client or on the primary FWSM. If you configure backup servers on the FWSM, it pushes the backup server policy to the clients in the group, replacing the backup server list on the client if one is configured.

Note If you are using hostnames, it is wise to have backup DNS and WINS servers on a separate network from that of the primary DNS and WINS servers. Otherwise, if clients behind a hardware client obtain DNS and WINS information from the hardware client via DHCP, and the connection to the primary server is lost, and the backup servers have different DNS and WINS information, clients cannot be updated until the DHCP lease expires. Further, if you use hostnames and the DNS server is unavailable, significant delays can occur.

Examples

The following example shows how to configure backup servers with IP addresses 10.10.10.1 and 192.168.10.14, for the group policy named "FirstGroup":

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# backup-servers 10.10.10.1 192.168.10.14
```

banner

To configure the session, login, or message-of-the-day banner, use the **banner** command in global configuration mode. To remove all lines from the banner keyword specified (**exec**, **login**, or **motd**), use the **no** form of the command.

banner {**exec** | **login** | **motd** *text*}

[no] banner {**exec** | **login** | **motd** [*text*]}

Syntax Description

exec	Configures the system to display a banner before displaying the enable prompt.
login	Configures the system to display a banner before the password login prompt when accessing the FWSM using Telnet.
motd	Configures the system to display a message-of-the-day banner.
text	Line of message text to display.

Defaults

The default is no login, session, or message-of-the-day banner.

Command Modes

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

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

Command History

Release	Modification
2.2(1)	This command was introduced.

Usage Guidelines

The **banner** command configures a banner to display for the keyword specified. The *text* string consists of all characters following the first white space (space) until the end of the line (carriage return or line feed [LF]). Spaces in the text are preserved. However, you cannot enter tabs through the CLI.

Subsequent *text* entries are added to the end of an existing banner unless the banner is cleared first.

Note The tokens $(domain) and $(hostname) are replaced with the hostname and domain name of the FWSM. When you enter a $(system) token in a context configuration, the context uses the banner configured in the system configuration.

Multiple lines in a banner are handled by entering a new banner command for each line that you wish to add. Each line is then appended to the end of the existing banner. There is no limit on the length of a banner other than RAM and Flash limits.

When accessing the FWSM through Telnet or SSH, the session closes if there is not enough system memory available to process the banner messages or if a TCP write error occurs. Only the exec and motd banners support access to the FWSM through SSH. The login banner does not support SSH.

To replace a banner, use the **no banner** command before adding the new lines.

Use the **no banner** {**exec | login | motd**} command to remove all the lines for the banner keyword specified.

The **no banner** command does not selectively delete text strings, so any *text* that you enter at the end of the **no banner** command is ignored.

Examples

The following example shows how to configure the **exec**, **login**, and **motd** banners:

```
hostname(config)# banner motd Think on These Things
hostname(config)# banner exec Enter your password carefully
hostname(config)# banner login Enter your password to log in
hostname(config)# show running-config banner
exec:
Enter your password carefully

login:
Enter your password to log in

motd:
```

The following example shows how to add a second line to the **motd** banner:

```
hostname(config)# banner motd and Enjoy Today
hostname(config)# show running-config banner motd
```

Related Commands

Command	Description
clear configure banner	Removes all banners.
show running-config banner	Displays all banners.

banner (group-policy)

To display a banner, or welcome text, on remote clients when they connect, use the **banner** command in group-policy configuration mode. To delete a banner, use the **no** form of this command.

banner {**value** *banner_string* | **none**}

no banner

Note If you configure multiple banners under a VPN group-policy, and you delete any one of the banners, all banners will be deleted.

Syntax Description

none	Sets a banner with a null value, thereby disallowing a banner. Prevents inheriting a banner from a default or specified group policy.
value *banner_string*	Constitutes the banner text. Maximum string size is 500 characters. Use the “\n” sequence to insert a carriage return.

Defaults

There is no default banner.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-policy configuration	•	—	•	—	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

The **no** form of this command allows inheritance of a banner from another group policy. To prevent inheriting a banner, use the **banner none** command.

Examples

The following example shows how to create a banner for the group policy named “FirstGroup”:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# banner value Welcome to Cisco Systems
```

bgp router-id

To specify a router ID for BGP routing process on the FWSM, use the **bgp router-id** command in router configuration mode. To restore the default router ID, use the **no** form of this command.

bgp router-id *ip-addr*

no bgp router-id *ip-addr*

Syntax Description

ip-addr	An IP address. The router ID is entered in IP address format. Any valid IP address can be used, even an address that is not locally configured on the FWSM.

Defaults

The router ID is set to the highest IP address configured on the FWSM.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context[1]	System
Router configuration	•	—	•	•	—

[1] This command is only available in the admin context.

Command History

Release	Modification
3.2(1)	This command was introduced.

Usage Guidelines

Use the **bgp router-id** command to configure a fixed router ID for a local BGP routing process. Enter the router ID in IP address format. You can use any valid IP address, even an address that is not locally configured on the FWSM. Changing the router ID causes peering sessions to automatically reset.

In multiple context mode, this command is only available in the admin context. The admin context must be in routed mode. The BGP stub routing configuration entered in the admin context applies to all contexts configured on the device; you cannot configure BGP stub routing on a per-context basis.

Examples

The following example shows a BGP routing configuration with the router ID of the FWSM set to 192.168.1.1:

```
hostname(config)# router bgp 800
hostname(config-router)# bgp router-id 192.168.1.1
hostname(config-router)# neighbor 10.1.1.1 remote-as 800
hostname(config-router)# neighbor 10.1.1.1 password bQ2$f78t
hostname(config-router)# network 192.168.1.0 mask 255.255.255.0
hostname(config-router)# network 10.1.1.0 mask 255.255.255.0
```

Related Commands

Command	Description
router bgp	Creates a BGP routing process and enters router configuration mode for that process.
show running-config router	Displays the **router** commands in the running configuration.

blocks

To allocate additional memory to block diagnostics (displayed by the **show blocks** command), use the **blocks** command in privileged EXEC mode. To set the value back to the default, use the **no** form of this command. The amount of memory allocated will be at most 150 KB but never more than 50% of free memory. Optionally, you can specify the memory size manually.

blocks queue history enable [*memory_size*]

no blocks queue history enable [*memory_size*]

Syntax Description

memory_size	(Optional) Sets the memory size for block diagnostics in Bytes, instead of applying the dynamic value. If this value is greater than free memory, an error message displays and the value is not accepted. If this value is greater than 50% of free memory, a warning message displays, but the value is accepted.

Defaults

The default memory assigned to track block diagnostics is 2136 Bytes.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	Support for this command was introduced.

Usage Guidelines

To view the currently allocated memory, enter the **show blocks queue history** command.

If you reload the FWSM, the memory allocation returns to the default.

Examples

The following example increases the memory size for block diagnostics:

```
hostname# blocks queue history enable
```

The following example increases the memory size to 3000 Bytes:

```
hostname# blocks queue history enable 3000
```

The following example attempts to increase the memory size to 3000 Bytes, but the value is more than free memory:

```
hostname# blocks queue history enable 3000
```

```
ERROR: memory size exceeds current free memory
```

The following example increases the memory size to 3000 Bytes, but the value is more than 50% of free memory:

```
hostname# blocks queue history enable 3000
WARNING: memory size exceeds 50% of current free memory
```

Related Commands

Command	Description
clear blocks	Clears the system buffer statistics.
show blocks	Shows the system buffer utilization.

boot device (IOS)

By default, the FWSM boots from the **cf:4** application partition. However, you can choose to boot from the **cf:5** application partition or into the **cf:1** maintenance partition. To change the default boot partition, enter the **boot device** command in global configuration mode. To restore the defualt, use the **no** form of this command.

boot device module *mod_num* **cf:***n*

no boot device module *mod_num* [**cf:***n*]

Syntax Description

cf:*n*	Sets the boot partition. Application partitions include **cf:4** (the default) and **cf:5**. The maintenance partition is **cf:1**.
module *mod_num*	Specifies the module number. Use the **show module** command to view installed modules and their numbers.

Defaults

The default boot partition is cf:4.

Command Modes

Global configuration.

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

To set the boot partition, enter the **set boot device cf:***n* [*mod_num*] command:

```
Router# set boot device cf:n [mod_num]
```

Examples

The following example shows how to set the boot partition to the maintenance partition:

```
Router(config)# boot device module 1 cf:1
```

Related Commands

Command	Description
hw-module module reset	Resets the module.
set boot device	Sets the boot partition.
show module	Shows all installed modules.

bridge-group

To assign an interface to a bridge group in transparent firewall mode, use the **bridge-group** command in interface configuration mode. To unassign an interface, use the **no** form of this command. A transparent firewall connects the same network on its inside and outside interfaces. Each pair of interfaces belongs to a bridge group.

bridge-group *number*

no bridge-group *number*

Syntax Description

number	Specifies an integer between 1 and 100.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

You can configure up to eight bridge groups of two interfaces each. You can only assign two interfaces to a bridge group. You cannot assign the same interface to more than one bridge group.

Assign a management IP address to the bridge group using the **interface bvi** command and then the **ip address** command.

Each bridge group connects to a separate network. Bridge group traffic is isolated from other bridge groups; traffic is not routed to another bridge group within the FWSM, and traffic must exit the FWSM before it is routed by an external router back to another bridge group in the FWSM.

You might want to use more than one bridge group if you do not want the overhead of security contexts, or want to maximize your use of security contexts. Although the bridging functions are separate for each bridge group, many other functions are shared between all bridge groups. For example, all bridge groups share a syslog server or AAA server configuration. For complete security policy separation, use security contexts with one bridge group in each context.

Examples

The following example assigns VLAN 100 to bridge group 1:

```
hostname(config)# interface vlan 100
hostname(config-if)# bridge-group 1
```

Related Commands

Command	Description
interface bvi	Enters the interface configuration mode for a bridge group so you can set the management IP address.
interface	Configures an interface.
ip address	Sets the management IP address for a bridge group.
nameif	Sets the interface name.
security-level	Sets the interface security level.