



backup-servers through browse-networks 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. 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 security appliance is unavailable. When you configure backup servers, the security appliance pushes the server list to the client as the IPSec tunnel is established.

```
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 security appliance pushes a null server list.
keep-client-config	Specifies that the security appliance 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 security appliance 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 security appliance.

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
Group-policy	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Configure backup servers either on the client or on the primary security appliance. If you configure backup servers on the security appliance, 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. The **no banner** command removes all lines from the banner keyword specified (**exec**, **login**, or **motd**).

```
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 security appliance using Telnet.
motd	Configures the system to display a message-of-the-day banner when you first connect.
<i>text</i>	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:

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

Command History

Release	Modification
Preexisting	This command was preexisting.

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 security appliance. 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 security appliance 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 security appliance 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

This 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:
Think on These Things
```

This 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
Think on These Things and Enjoy Today
```

Related Commands

Command	Description
<code>clear configure banner</code>	Removes all banners.
<code>show running-config banner</code>	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. This option allows inheritance of a banner from another group policy. To prevent inheriting a banner, use the **banner none** 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 <i>banner_string</i>	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:

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

Command History

Release	Modification
7.0(1)	This command was introduced.

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 7.0(1).
```

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:

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

To view the currently allocated memory, enter the **show blocks queue history** command. If you reload the security appliance, 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

To specify which system image the system will use at next reload and which configuration file the system will use at startup, use the **boot** command in privileged EXEC mode. Use the **no** form of this command to restore the default value.

```
boot {config | system} url
```

```
no boot {config | system} url
```

Syntax Description

config	Specifies which configuration file to use when the system is loaded.
system	Specifies which system image file to use when the system is loaded.
<i>url</i>	Sets the context configuration URL. All remote URLs must be accessible from the admin context. See the following URL syntax: <ul style="list-style-type: none"> • disk0:<i>[/path/]filename</i> This option is only available for the ASA platform, and indicates the internal Flash card. You can also use flash instead of disk0; they are aliased. • disk1:<i>[/path/]filename</i> This option is only available for the ASA platform, and indicates the external Flash card. • flash:<i>[/path/]filename</i> • tftp:<i>[/user[:password]@]server[:port]/[/path/]filename</i>

Defaults

If the **boot config** command is not specified, the startup-config will be saved to a hidden location, and used only with commands that utilize it, such as the **show startup-config** command and the **copy startup-config** command.

For the **boot system** command, there are no defaults. If the BOOT environment variable is not configured, the system searches only the internal Flash for the first valid image to boot. If no valid image is found no system image will be loaded, and the system will boot loop until ROMMON or Monitor mode is broken into.

You can enter up to four **boot system** command entries, to specify different images to boot from in order, and the security appliance will boot the first valid image it finds.



Note

The PIX platform **boot system** command does not support loading an image using a TFTP location.

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
7.0(1)	This command was introduced.

Usage Guidelines

You set the CONFIG_FILE environment variable in the current running memory when you use the **boot config** command. This variable specifies which configuration file to load when the system boots.

**Note**

Only one **boot system tftp:** command may be configured, and it must be the first one configured. Subsequent multiple **boot system tftp:** commands will fail unless a **no boot system** command is issued.

When you use this global configuration command, you affect only the running configuration. Use the **write memory** or **copy** command to save the environment variable from your running configuration to your startup configuration. Note that saving the running configuration to the startup configuration will also overwrite the configured file with the running configuration, so change this variable and execute the **write memory** command before copying the new configuration file to the configured name.

The system stores and executes the boot system commands in the order in which you enter them in the configuration file. To execute the configuration when the reloads use the **write memory** command or **copy** command to save the environment variable from your running configuration to your startup configuration.

**Tip**

The ASDM image file is specified by the **asdm image** command.

Examples

The following example specifies that at startup the security appliance should load a configuration file called configuration.txt:

```
hostname(config)# boot config configuration.txt
```

Related Commands

Command	Description
asdm image	Specifies the ASDM software image.
show bootvar	Displays boot file and configuration properties.

border style

To customize the border of the WebVPN Home page that is displayed to authenticated WebVPN users, use the **border style** command from webvpn customization mode:

border style *value*

[**no**] **border style** *value*

To remove the command from the configuration and cause the value to be inherited, use the **no** form of the command.

Syntax Description

value The Cascading Style Sheet (CSS) parameters (maximum 256 characters).

Defaults

The default style of the border is background-color:#669999;color:white.

Command Modes

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

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

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The **style** option is expressed as any valid Cascading Style Sheet (CSS) parameters. Describing these parameters is beyond the scope of this document. For more information about CSS parameters, consult CSS specifications at the World Wide Web Consortium (W3C) website at www.w3.org. Appendix F of the CSS 2.1 Specification contains a convenient list of CSS parameters, and is available at www.w3.org/TR/CSS21/propidx.html.

Here are some tips for making the most common changes to the WebVPN pages—the page colors:

- You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.
- RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.
- HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.



Note

To easily customize the WebVPN pages, we recommend that you use ASDM, which has convenient features for configuring style elements, including color swatches and preview capabilities.

Examples

The following example customizes the background color of the border to the RGB color #66FFFF, a shade of green:

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# border style background-color:66FFFF
```

Related Commands

Command	Description
application-access	Customizes the Application Access box of the WebVPN Home page.
browse-networks	Customizes the Browse Networks box of the WebVPN Home page.
web-bookmarks	Customizes the Web Bookmarks title or links on the WebVPN Home page.
file-bookmarks	Customizes the File Bookmarks title or links on the WebVPN Home page.

browse-networks

To customize the Browse Networks box of the WebVPN Home page that is displayed to authenticated WebVPN users, use the **browse-networks** command from webvpn customization mode:

```
browse-networks { title | message | dropdown } { text | style } value
```

```
[no] browse-networks { title | message | dropdown } { text | style } value
```

To remove the command from the configuration and cause the value to be inherited, use the **no** form of the command.

Syntax Description

title	Specifies you are changing the title.
message	Specifies you are changing the message displayed under the title.
dropdown	Specifies you are changing the drop-down box.
text	Specifies you are changing the text.
style	Specifies you are changing the style.
<i>value</i>	The actual text to display (maximum 256 characters), or Cascading Style Sheet (CSS) parameters (maximum 256 characters).

Defaults

The default title text is “Browse Networks”.

The default title style is:

```
background-color:#99CCCC;color:black;font-weight:bold;text-transform:uppercase
```

The default message text is “Enter Network Path”.

The default message style is:

```
background-color:#99CCCC;color:maroon;font-size:smaller.
```

The default dropdown text is “File Folder Bookmarks”.

The default dropdown style is:

```
border:1px solid black;font-weight:bold;color:black;font-size:80%.
```

Command Modes

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

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

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The **style** option is expressed as any valid Cascading Style Sheet (CSS) parameters. Describing these parameters is beyond the scope of this document. For more information about CSS parameters, consult CSS specifications at the World Wide Web Consortium (W3C) website at www.w3.org. Appendix F of the CSS 2.1 Specification contains a convenient list of CSS parameters, and is available at www.w3.org/TR/CSS21/propidx.html.

Here are some tips for making the most common changes to the WebVPN pages—the page colors:

- You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.
- RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.
- HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

**Note**

To easily customize the WebVPN pages, we recommend that you use ASDM, which has convenient features for configuring style elements, including color swatches and preview capabilities.

Examples

The following example changes the title to “Browse Corporate Networks”, and the text within the style to blue:

```
F1-asal(config)# webvpn
F1-asal(config-webvpn)# customization cisco
F1-asal(config-webvpn-custom)# browse-networks title text Browse Corporate Networks
F1-asal(config-webvpn-custom)# browse-networks title style color:blue
```

Related Commands

Command	Description
application-access	Customizes the Application Access box of the WebVPN Home page.
file-bookmarks	Customizes the File Bookmarks title or links on the WebVPN Home page.
web-applications	Customizes the Web Application box of the WebVPN Home page.
web-bookmarks	Customizes the Web Bookmarks title or links on the WebVPN Home page.