



backup interface through browse-networks Commands

backup interface

For models with a built-in switch, such as the ASA 5505, use the **backup interface** command in interface configuration mode to identify a VLAN interface as a backup interface, for example, to an ISP. To restore normal operation, use the **no** form of this command.

```

backup interface vlan number

no backup interface vlan number
    
```

Syntax Description	<i>vlan number</i>	Specifies the VLAN ID of the backup interface.
--------------------	--------------------	--

Defaults	By default, the backup interface 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
Interface configuration	•	—	•	—	—

Command History	Release	Modification
	7.2(1)	This command was introduced.
	7.2(2)	The Security Plus license no longer limits the number of VLAN interfaces to 3 for normal traffic, 1 for a backup interface, and 1 for failover; you can now configure up to 20 interfaces without any other limitations. Therefore ,the backup interface command is not required to enable more than 3 interfaces.

Usage Guidelines

This command can be entered in the interface configuration mode for a VLAN interface only. This command blocks all through traffic on the identified backup interface unless the default route through the primary interface goes down.

When you configure Easy VPN with the **backup interface** command, if the backup interface becomes the primary, then the ASA moves the VPN rules to the new primary interface. See the **show interface** command to view the state of the backup interface.

Be sure to configure default routes on both the primary and backup interfaces so that the backup interface can be used when the primary fails. For example, you can configure two default routes: one for the primary interface with a lower administrative distance, and one for the backup interface with a higher distance. See the **dhcp client route distance** command to override the administrative distance for default routes acquired from a DHCP server. To configure dual ISP support, see the **sla monitor** and **track rtr** commands for more information.

You cannot configure a backup interface when the **management-only** command is already configured on the interface.

Examples

The following example configures four VLAN interfaces. The backup-isp interface only allows through traffic when the primary interface is down. The **route** commands create default routes for the primary and backup interfaces, with the backup route at a lower administrative distance.

```
hostname(config)# interface vlan 100
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# backup interface vlan 400
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 200
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.2.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 300
hostname(config-if)# nameif dmz
hostname(config-if)# security-level 50
hostname(config-if)# ip address 10.3.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 400
hostname(config-if)# nameif backup-isp
hostname(config-if)# security-level 50
hostname(config-if)# ip address 10.1.2.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config)# interface ethernet 0/0
hostname(config-if)# switchport access vlan 100
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/1
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/2
hostname(config-if)# switchport access vlan 300
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/3
hostname(config-if)# switchport access vlan 400
hostname(config-if)# no shutdown

hostname(config-if)# route outside 0 0 10.1.1.2 1
hostname(config)# route backup-isp 0 0 10.1.2.2 2
```

Related Commands

Command	Description
forward interface	Restricts an interface from initiating traffic to another interface.
interface vlan	Creates a VLAN interface and enters interface configuration mode.
dhcp client route distance	Overrides the administrative distance for default routes acquired from a DHCP server.
sla monitor	Creates an SLA monitoring operation for static route tracking.
track rtr	Tracks the state of an SLA monitoring operation.

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 ASA pushes a null server list.
keep-client-config	Specifies that the ASA sends no backup server information to the client. The client uses its own backup server list, if configured.
<i>server1 server 2.... server10</i>	Provides a space delimited, priority-ordered list of servers for the VPN client to use when the primary ASA 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 ASA.

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 configuration	•	—	•	—	—

Command History

Release	Modification
7.0(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 ASA is unavailable. When you configure backup servers, the ASA pushes the server list to the client as the IPsec tunnel is established.

Configure backup servers either on the client or on the primary ASA. If you configure backup servers on the ASA, 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, 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. In addition, 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 ASDM, 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 this command.

```

banner { asdm | exec | login | motd text }

[no] banner { asdm | exec | login | motd [text] }
    
```

Syntax Description

asdm	Configures the system to display a banner after you successfully log in to ASDM. The user is prompted to either continue to complete login, or to disconnect. This option lets you require users to accept the terms of a written policy before connecting.
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 ASA using Telnet or a serial console.
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 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
7.2(4)/8.0(3)	The asdm keyword was added.
9.0(1)	The banner login command supports serial console connections.

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 ASA. 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 want to add. Each line is then appended to the end of the existing banner.

**Note**

The maximum length of the authorization prompt for banners is 235 characters or 31 words, whichever limitation is reached first.

When accessing the ASA 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 ASA through SSH. The login banner does not support SSHv1 clients or SSH clients that do not pass the username as part of the initial connection.

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 **asdm**, **exec**, **login**, and **motd** banners:

```
hostname(config)# banner asdm You successfully logged in to ASDM
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
asdm:
You successfully logged in to ASDM

exec:
Enter your password carefully

login:
Enter your password to log in

motd:
Think on These Things
```

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
Think on These Things and Enjoy Today
```

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 are 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 configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

To prevent inheriting a banner, use the **banner none** command.

The IPsec VPN client supports full HTML for the banner. However, the clientless portal and the AnyConnect client support partial HTML. To ensure the banner displays correctly to remote users, follow these guidelines:

- For IPsec client users, use the /n tag.
- For AnyConnect client users, use the
 tag.
- For clientless users, use the
 tag.

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.
```

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.

blocks queue history enable [*memory_size*]

no blocks queue history enable [*memory_size*]

Syntax Description

<i>memory_size</i>	(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 appears and the value is not accepted. If this value is greater than 50% of free memory, a warning message appears, 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
Privileged EXEC	•	•	•	—	•

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 ASA, the memory allocation returns to the default.

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.

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 the available 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 the 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 usage.

boot

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

```
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 image file to use when the system is loaded.
<i>url</i>	<p>Sets the location of the image or configuration. In multiple context mode, all remote URLs must be accessible from the admin context. See the following URL syntax:</p> <ul style="list-style-type: none"> disk0:/[path/]filename For the ASA, this URL indicates the internal flash memory. You can also use flash instead of disk0; they are aliased. disk1:/[path/]filename For the ASA, this URL indicates the external flash memory card. This option is not available for the ASA Services Module. flash:/[path/]filename This URL indicates the internal flash memory. tftp://[user[:password]@]server[:port]/[path/]filename[;int=interface_name] Specify the interface name if you want to override the route to the server address. This option is available for the boot system command for the ASA 5500 series only; the boot config command requires the startup configuration to be on the flash memory. Only one boot system tftp: command can be configured, and it must be the first one configured.

Defaults

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

For the **boot system** command, there are no defaults. If you do not specify a location, the ASA searches only the internal flash memory for the first valid image to boot. If no valid image is found, no system image will be loaded, and the ASA will boot loop until you break into the ROMMON or Monitor mode.

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

When you save this command to the startup configuration using the **write memory** command, you also save the settings to the BOOT and CONFIG_FILE environment variables, which the ASA uses to determine the startup configuration and software image to boot when it restarts.

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

If you want to use a startup configuration file at the new location that is different from the current running configuration, then be sure to copy the startup configuration file to the new location after you save the running configuration. Otherwise, the running configuration will overwrite the new startup configuration when you save it.

**Tip**

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

Examples

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

```
hostname(config)# boot config disk0:/configuration.txt
```

Related Commands

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

border style

To customize the border of the WebVPN Home page that is displayed to authenticated WebVPN users, use the **border style** command in customization configuration mode. To remove the command from the configuration and cause the value to be inherited, use the **no** form of this command.

border style *value*
no border style *value*

Syntax Description	<i>value</i>	Specifies the Cascading Style Sheet (CSS) parameters to use. The maximum number of characters allowed is 256.
--------------------	--------------	---

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
Customization configuration	•	—	•	—	—

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:

```
hostname(config)# webvpn
hostname(config-webvpn)# customization cisco
hostname(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.

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 interfaces. Up to four interfaces can belong to a bridge group.

- bridge-group** *number*
- no bridge-group** *number*

Syntax Description	<i>number</i>	Specifies an integer between 1 and 100.
--------------------	---------------	---

Command Default	No default behavior or values.
-----------------	--------------------------------

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

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

Command History	Release	Modification
	8.4(1)	We introduced this command.

Usage Guidelines

You can configure up to eight bridge groups of four interfaces each. You can only assign four 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 ASA, and traffic must exit the ASA before it is routed by an external router back to another bridge group in the ASA.

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 GigabitEthernet 1/1 to bridge group 1:

```
hostname(config)# interface gigabitethernet 1/1
```



```
hostname(config-if) # bridge-group 1
```

Related Commands

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

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 in webvpn customization configuration mode. To remove the command from the configuration and cause the value to be inherited, use the **no** form of this command.

```

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

Syntax Description

dropdown	Specifies a change to the drop-down list.
<i>message</i>	Specifies youa change to the message displayed under the title.
style	Specifies a change to the style.
text	Specifies a change to the text.
title	Specifies a change to the title.
<i>value</i>	Indicates the actual text to display. The maximum number of characters allowed is 256. This value applies to Cascading Style Sheet (CSS) parameters also.

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 configuration	•	—	•	—	—

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.

