

Migrating to the Cisco ASA Services Module from the FWSM

Contents

- [Information About the Migration, page 1](#)
- [Migrating the FWSM Configuration to the ASA SM, page 2](#)
- [Unsupported Runtime Commands, page 4](#)
- [Configuration Migration Reference, page 7](#)
- [Related Documentation, page 17](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 17](#)

Information About the Migration

This guide describes how to convert Cisco FWSM configurations to Cisco ASA SM 8.5 configurations. This document also provides details about the differences between Cisco FWSM and Cisco ASA SM behavior.

Although the ASA SM shares a common software foundation with the FWSM, you cannot directly use a FWSM configuration on an ASA SM.

Differences between the platforms, such as the use of specific commands, prevent FWSM configurations from being used unmodified on the ASA SM.



Warning

After running Migration Tool, you cannot paste the migrated configuration directly at the CLI prompt on the ASA SM; you must copy the configuration over the network to the startup configuration and reload the ASA SM so that it can perform additional migrations at startup.

In particular, the NAT feature on the ASA SM is redesigned for increased flexibility and functionality compared to FWSM. On the ASA SM, you can configure NAT using auto NAT, where you configure NAT as part of the attributes of a network object, and manual NAT, where you can configure more advanced NAT options.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2011 Cisco Systems, Inc. All rights reserved.

On the ASA SM, all NAT and NAT-related commands are redesigned. The following commands were introduced or modified: **nat** (in global and object network configuration mode), **show nat**, **show nat pool**, **show xlate**, **show running-config nat**. The following commands were removed: **global**, **static**, **nat-control**, **alias**.

For a description of the differences in NAT matching for statics between FWSM and ASA SM, see [Migration Due to Default Behavior Differences, page 7](#).

For detailed information about the NAT feature changes on the ASA SM, see “NAT Migration” in *Cisco ASA 5500 Migration Guide for Version 8.3*.

Migrating the FWSM Configuration to the ASA SM

Migrating the FWSM configuration to the ASA SM occurs by perform two steps:

Step 1: [Running the Migration Tool](#)

Step 2: [Applying the Migrated Configuration to the ASA SM](#)

You must perform the migration from the FWSM to the ASA SM using these two steps because the Migration Tool does not make all the necessary command syntax changes when you run the Migration Tool. Because of this fact, you cannot open the migrated configuration file, enter the **select all** command and copy the configuration, and then paste the configuration to the command line of the ASA SM.

You must copy the migrated configuration file to the startup configuration of the ASA SM. When the ASA SM is subsequently restarted, the startup configuration is parsed upon startup. The ASA SM image takes the NAT, ACL, and other commands that have been deprecated or changed from the FWSM and translates the commands into the commands that the ASA SM accepts.

Running the Migration Tool

The Migration Tool includes a Windows and Macintosh application to perform the FWSM configuration migration.

Prerequisites

The ASA SM must be in a known state. The blade cannot have a configuration running on it. If it has been configured, execute the **write erase** command to clear the configuration on the service module.


To convert the FWSM configuration to an ASA SM configuration, perform the following steps:

-
- Step 1** From the Cisco software download site, locate the file `fwsml_migration_mac.zip` or `fwsml_migration_win.zip` and save it to a Windows or Macintosh client. Decompress the ZIP file and extract the corresponding file for the system on which you plan to run the conversion application—`fwsml_migration.exe` or `fwsml_migration.app`.
 - Step 2** From the FWSM that you are migrating to an ASA SM, copy all the configuration files, which includes each configuration file for all contexts and the system context file, to the directory in which you extracted the Migration Tool application.

For single mode, copy the running configuration file. For multi-mode, copy the following configuration files:

- The system space configuration
- The admin context

- Any user context of interest

- Step 3** Double click the `fwsd_migration.exe` or `fwsd_migration.app` file to start the Migration Tool. The FWSM Configuration Migration dialog box appears along with a command window, which will display the progress and status of the conversion.
- Step 4** Select the radio button appropriate for your conversion:
- **Single File**—select this option when you are converting the configuration file for the FWSM running in single-context mode.
 - **Directory**—select this option when you are converting multiple files for the FWSM that ran in multiple-context mode. Each context has an associated configuration file and the FWSM has a system context file.
- Step 5** Under the option you selected (Single File or Directory), enter information for the file or files to convert:
- **Input File field**—enter the path and file name for the configuration file for the single-context FWSM or click **Browse** to locate the file on your local system.
 - **Input Directory**—enter the path to the directory containing all the multi-context configuration files and the system context file or click **Browse** to locate the directory on your local system.
- Step 6** Under the option you selected (Single File or Directory), enter the conversion output information:
- **Output File field**—enter the path and file name for that the Migration Tool will use to create the converted configuration file for the single-context FWSM.
 - **Output Directory**—enter the path to the directory that the Migration Tool will place the converted multi-context configuration files and the system context file or click **Browse** to locate the directory on your local system.
- Step 7** In the ASA SM Boot Image field, enter the location of the ASA SM boot image in the following format:
drive:/boot-file-path
- The boot image value must include one of the following options:
- **disk0:***/path and filename on disk0*
 - **disk1:***/path and filename on disk1*
 - **flash:***/path and filename on flash*
 - URL beginning with tftp prefix
- The value you enter in this field defines the image you want the ASA SM to boot up with when it completes the final migration.
-  **Note** You must write the boot image value to memory by issuing the **write memory** command on the ASA SM. Issuing the **write memory** command saves the boot image value you specify for the boot image to the **BOOT** variable in the configuration file. After writing the value to memory, verify that the boot variable was written to memory by entering the **show bootvar** command. See *Cisco ASA 5500 Series Command Reference*, 8.5 for the ASA SM.
- Step 8** In the Log Location field, enter the path and file name for the log file that the Migration Tool will use to log the status information from the conversion or click **Browse** to locate the file on your local system.
- Step 9** Click **Convert** to start the conversion.
- Status information appears in the command window. Once the conversion successfully completes, a Success dialog box appears.

Step 10 Click **OK** to end the conversion.

What to Do Next

[Applying the Migrated Configuration to the ASA SM, page 4](#)

Applying the Migrated Configuration to the ASA SM

Prerequisites

- You must have migrated your FWSM configuration by using the Migration Tool. See [Running the Migration Tool, page 2](#).
- Configure an interface on the ASA SM to allow file transfer using TFTP, SSH, or HTTP.

Step 1 Copy the migrated files to the ASA SM via TFTP, SSH, or HTTP.



Note If necessary, add an interface configuration to allow file transfer using TFTP, SSH, or HTTP.

- If working in single mode, copy the migrated configuration to the startup-config file.
- If working in multiple mode, copy the system configuration to the startup-config and all context configuration files (such as, the Admin context) to disk0:.



Note The context files must be placed on disk0: in the path the system configuration points to for each context. If the system configuration has the configuration URL for a context as “config-url disk0:/context/ctx1.cfg” then the file for that context needs to be placed in that context directory path.



Note You cannot paste the migrated configuration directly at the CLI prompt on the ASA SM; you must copy the configuration over the network to the startup configuration and then reload the ASA SM so that it can perform additional migrations at startup. You cannot copy and paste the configuration because of the complexities of converting certain features, such as converting the FWSM NAT feature to the NAT feature on the ASA SM, which uses Object NAT and Twice NAT.

Step 2 Reload the ASA SM when you are migrating a single mode FWSM image.

On startup, final configuration modifications will be conducted by the ASA SM image.



Note When you upload multi-mode FWSM contexts, reloading the ASA SM is not necessary after applying each multi-mode context.

Unsupported Runtime Commands

This section contains the following topics:

- [Unsupported Debug Commands, page 5](#)
- [Unsupported Clear Commands, page 5](#)
- [Unsupported Show Commands, page 6](#)

Unsupported Debug Commands

The following **debug** commands are supported on the FWSM but not on the ASA SM.

- [show | no] debug ip bgp
- [show | no] debug resource partition
- [show | no] debug pc-lu
- [show | no] debug ssl
- [show | no] debug npc
- [show | no] debug route-np
- [show | no] debug aging
- [show | no] debug session
- [show | no] debug RM-NP-counter
- [show | no] debug control-plane
- [show | no] debug route-monitor
- [show | no] debug acl optimization
- [show | no] debug route-inject

Unsupported Clear Commands

The following **clear** commands are supported on the FWSM but not on the ASA SM.

- clear dispatch stats all
- clear ip bgp
- clear route-monitor statistics
- clear route statistics
- clear np *number_item* keyword
- clear np all stats
- clear npc statistics
- clear service-acceleration
- clear configure resource rule
- clear configure resource partition
- clear configure ftp-map
- clear configure gtp-map
- clear configure mgcp-map
- clear configure h225-map

- clear configure xlate-bypass
- clear configure rip
- clear configure route-monitor
- clear configure router bgp
- clear configure control-point tcp-normalizer
- clear configure route-inject

Unsupported Show Commands

The following **show** commands are supported on the FWSM but not on the ASA SM.

- show running-config all ftp-map
- show running-config all gtp-map
- show running-config all mgcp-map
- show running-config all h225-map
- show running-config all xlate-bypass
- show running-config all rip
- show running-config all route-monitor
- show running-config all control-point tcp-normalizer
- show running-config all route-inject
- show resource rule
- show resource acl-partition
- show resource partition
- show flashfs
- show conn np
- show asr
- show pcdebug
- show pc conn
- show nic
- show np *keyword*
- show np *number_item keywords*
- show cpu threshold
- show dispatch table
- show dispatch statistics
- show pc xlate
- show pc local-host
- show ip bgp
- show route-monitor
- show npc *keywords*

- show service-acceleration statistics
- show route-inject

Configuration Migration Reference

This section contains the following topics:

- [Migration Due to Default Behavior Differences, page 7](#)
- [Migration Due to Unsupported Features in ASA SM, page 8](#)
- [Migration Due to CLI Differences, page 9](#)
- [Default Value and Value Range Differences, page 15](#)
- [SNMP Differences, page 17](#)

Migration Due to Default Behavior Differences

The major default behavior differences between FWSM and ASA SM are as follows.

Implicit Deny

By default, when the interfaces on the FWSM are configured without assigning any access list or access group commands, the FWSM drops all traffic that enters those interfaces. To allow any traffic to enter the FWSM, you must attach an inbound access list to an interface.

By default, when the interfaces on the ASA SM are configured without assigning any access list or access group commands, the ASA SM allows traffic to pass from a higher security interface (assume the inside security level is 100) to a lower security interface (assume the outside security level is 0). The inverse is not true. The ASA SM does not allow traffic to pass from the outside to inside interface.

Therefore, the Migration Tool was created to assume that this type of FWSM configuration required that traffic be blocked no matter the direction. To maintain parity, the Migration Tool adds an explicit ACL (deny ip any any) on all the interfaces to deny traffic. Additionally, on ASA SM, the last statement of any access list is an implicit deny ip any any. IOS device use this same behavior.

See the following examples:

Example 1

```
no access-list/groups on any interface
```

Traffic from the inside to the outside is permitted.

Traffic from the outside to the inside is denied.

Example 2

```
access-list INSIDE permit ip 192.168.1.0 255.255.0 any
access-group INSIDE in interface inside
```

Traffic from the inside to the outside, source IP 192.168.1.10, is permitted.

Traffic from the inside to the outside, source IP 192.168.2.1, is denied (hits implicit).

Implicit ICMP Deny

By default, FWSM is configured to set an implicit ICMP deny to the interface. The ASA SM is configured to set an implicit permit.

When you run the Migration Tool, it adds icmp deny statements on all interfaces.

NAT Matching for Statics

By default, FWSM is configured to use best match for static NAT and static PAT (regular and policy). When overlapping IP addresses occur in the static statements, a warning is displayed but the overlapping IP addresses are supported. The order of the static commands does not matter; the static statement that best matches the real address is used.

In the ASA SM, IP addresses are matched against static NAT and static PAT rules based on the order the rules appear in the configuration.

The Migration Tool is unable to preserve the behavior of the FWSM; therefore, if you have overlapping NAT rules, you should look at your migrated configuration to ensure it matches your address translation requirements.

Migration Due to Unsupported Features in ASA SM

The following FWSM features are not supported in ASA SM.

IPSec in Multimode (Management only)

On the FWSM, IPSec is supported for management purposes in multimode.

The ASA SM does not provide support for IPSec in multimode. IPSec (both in single and multimode) is not supported. When you run the Migration Tool, it removes any VPN related commands and informs you that IPSec is not supported.

Asymmetric Routing

When asymmetric routing was introduced in ASA SM, it was not affected by the active/active restriction.

On the ASA SM, asymmetric routing is only supported in active/active mode.

The Migration Tool removes the commands if not in active/active mode and informs the user.

BGP Stub Routing

CLI commands:

router bgp

bgp router-id

neighbor remote-as

neighbor password

network

This is a feature in FWSM that supports BGP stub routing.

ASA SM does not support this feature.

The Migration Tool removes the BGP related commands and informs the user.

Failover Preemption for Active/Standby Failover

CLI command:

[no] failover preempt

This is a feature in FWSM that can be configured in an Active/Standby failover scenario. When this feature is configured, the Primary unit always becomes Active after a certain time in the following cases:

- When the primary unit fails and the secondary becomes active
- When the secondary unit boots before the primary unit and the secondary unit is active

ASA SM does not support this feature.

The Migration Tool removes the command and informs the user.

Route Health Injection

CLI commands:

route-inject

redistribute nat

redistribute connected

redistribute static

This is a feature on FWSM that installs connected, static, NAT pool routes configured on the FWSM into MSFC on a per context basis. MSFC can then redistribute the routes.

ASA SM does not support this feature.

DHCP Relay Interface Specific Servers

CLI:

interface vlan *vlan_id*

dhcprelay server *ip_address*

FWSM added this feature in 3.2(1). With this feature, interface specific DHCP servers can be configured. “dhcprelay server” CLI could be configured in global mode and it was also added to be in interface specific mode.

ASA SM does not support this feature.

The Migration Tool converts the commands from interface specific to global and informs the user.

Stateful Failover Uauth Table Replication

FWSM supports replicating the Uauth Table to the failover peer when stateful failover is configured.

ASA SM does not support this feature.

The Migration Tool adds an INFO message when stateful failover is configured.

Migration Due to CLI Differences

The following table lists the differences between CLI commands for FWSM and ASA SM:

Table 1 *FWSM vs. ASA SM Configuration CLI differences*

Feature	FWSM Commands	Behavior in ASA SM
Connection timeouts for all protocols	set connection timeout idle	The idle keyword is not supported on ASA SM. ASA SM has the tcp keyword, which is used to close TCP connections after a certain time. Running the Migration Tool converts the idle keyword to the tcp keyword.
Connection rate limit	set connection conn-rate-limit	The command is not supported on the ASA SM. The Migration Tool removes the command from the configuration.
AAA authentication challenge	aaa authentication challenge disable	The command is not supported on the ASA SM. The Migration Tool removes the command from the configuration.
AAA authentication clear conn	aaa authentication clear-conn	The command is not supported on the ASA SM. The Migration Tool removes the command from the configuration.
Virtual SSH	virtual ssh	The command is not supported on the ASA SM. The Migration Tool removes the command from the configuration.
Interactive password prompts with Radius for authentication	auth-prompt reject [invalid-credentials expired-pwd]	The ASA SM supports the command but not the new options. The Migration Tool removes the command when the new options are present.
DHCP relay trusted interface (option 82)	dhcrelay information trusted dhcrelay information trust-all	The command is not supported on the ASA SM. The Migration Tool removes the command from the configuration.
http-map	port-misuse	The command is not supported on the ASA SM. The Migration Tool removes the command from the configuration.
	logging deny conn-queue-full	The command is not supported on the ASA SM. The Migration Tool removes the command from the configuration.

Table 1 FWSM vs. ASA SM Configuration CLI differences

Feature	FWSM Commands	Behavior in ASA SM
EtherType Access lists and denying IPv4 and ARPs	On the FWSM, in transparent firewall mode with “deny all” ether type access-list, both IPv4 and ARP cannot be denied with FWSM.	On the ASA SM, in transparent firewall mode with “deny all” ether type access-list, all the ether types including IPv4 and ARP are denied. The Migration Tool adds permit statements for IPv4 and ARP ether types.
Direct Login or Logout using Virtual HTTP for User Authentication	virtual http <i>ip_address</i> [host <i>hostname</i>]	On the ASA SM, the virtual http command exists but has different behavior for this command. ASA SM supports the login aspect of direct authentication but not logout. ASA SM does support the cascading authentication with the virtual http command. You can configure this feature on ASA SM by using the aaa authentication listener http command.
Route Monitoring	Route-monitor	ASA SM supports the same feature using the sla monitor command. ASA SM supports more options with the command than FWSM. The Migration Tool removes the FWSM command and adds information in the tool log about the sla monitor command, which you can use to achieve similar functionality.
Application Inspection	ftp-map gtp-map h225-map http-map mgcp-map snmp-map sip-map	ASA SM supports the Application Inspection map commands. Running the Migration Tool converts the map commands to policy-map match commands used by the ASA SM.

Table 1 *FWSM vs. ASA SM Configuration CLI differences*

Feature	FWSM Commands	Behavior in ASA SM
RIP	rip	ASA SM supports single line RIP configuration. Running the Migration Tool converts the configuration to the RIP configuration used by the ASA SM when the command is present in the startup configuration.
TCP Normalizer	control-point tcp-normalizer	FWSM supports a limited TCP Normalizer. This can be enabled or disabled using a configuration setting. ASA SM does not include a setting to disable the TCP normalizer. The Migration Tool removes the command from the configuration.
Rule limits	resource acl-partition resource partition size rule allocate-acl-partition access-list commit resource rule	Due to Hard NPs, FWSM has fixed rule limits and commands to support the limits. ASA SM does not have fixed rule limits so it does not support the commands to allow fixed rule limits. The Migration Tool removes the commands from the configuration.
Xlates for all traffic	xlate-bypass	FWSM creates xlates for all traffic (including to the device traffic). ASA SM does not create xlates for all traffic and, therefore, does not support the command. The Migration Tool removes the command from the configuration.
ACL optimization	access-list optimization enable	ASA SM does not support this command. The Migration Tool removes the command from the configuration.

Table 1 *FWSM vs. ASA SM Configuration CLI differences*

Feature	FWSM Commands	Behavior in ASA SM
	sysopt uauth allow-http-cache	<p>ASA SM does not support this command.</p> <p>The Migration Tool removes the command from the configuration.</p>
	sysopt np completion-unit	<p>ASA SM does not support this command.</p> <p>The Migration Tool removes the command from the configuration.</p>
	sysopt connection tcp sack-permitted	<p>FWSM uses the no form of the command to clear the SACK permitted option exchanged during the TCP 3-way handshake. The SACK option is enabled by default.</p> <p>ASA SM implements this feature using the tcp-options selective-ack clear/allow command under tcp-map. By default, ASA SM allows the SACK option.</p> <p>The Migration Tool converts the no form of the command to the ASA SM tcp-options command.</p>
	sysopt connection tcp window-scale	<p>FWSM uses the no form of the command to clear the Window-scale TCP option. The option is allowed by default.</p> <p>ASA SM implements this feature using tcp-options window-scale {clear/allow} command under tcp-map. The default is to allow the window-scale option.</p> <p>The Migration Tool converts the no form of the command to the ASA SM tcp-options command.</p>

Table 1 *FWSM vs. ASA SM Configuration CLI differences*

Feature	FWSM Commands	Behavior in ASA SM
SNMP Trap commands	snmp-server enable traps entity redun-switchover snmp-server enable traps entity alarm-asserted snmp-server enable traps entity alarm-cleared snmp-server enable traps resource snmp-server enable traps resource limit-reached snmp-server enable traps resource rate-limit-reached	ASA SM does not support these SNMP traps and, therefore, does not support these commands. The Migration Tool removes the commands from the configuration.
Service Reset	service reset no-connection	ASA SM achieves the same behavior using the service reset inbound command. The Migration Tool converts the FWSM command to the service reset inbound command used by ASA SM.
	aaa schedule round-robin	ASA SM does not support this command. The Migration Tool removes the command from the configuration.
	aaa authentication {ftp telnet http https} challenge disable	ASA SM does not support the challenge disable command or the ftp option. The Migration Tool removes the command from the configuration.

Table 1 FWSM vs. ASA SM Configuration CLI differences

Feature	FWSM Commands	Behavior in ASA SM
Resource Limits	limit-resource rate fixups <i>value</i> limit-resource rate <i>resource value%</i> limit-resource Mac-addresses <i>value value%</i> limit-resource IPSec <i>value value%</i>	<p>ASA SM does not have upper limits on resources and, therefore, does not support % rate limit for resources. ASA SM does not support limiting MAC addresses and IPSec tunnels.</p> <p>The Migration Tool converts limit-resource rate fixups <i>value</i> to limit-resource rate inspects <i>value</i>, removes limit-resource rate <i>resource value%</i>, removes limit-resource Mac-addresses <i>value value%</i>, removes limit-resource IPSec <i>value value%</i>.</p>
URL-Server commands	url-server [<i>if_name</i>] vendor websense host <i>local_ip</i> protocol udp context-name url-server [<i>if_name</i>] vendor websense host <i>local_ip</i> protocol tcp connections <i>num_conns</i>	<p>ASA SM does not support the context-name keyword. ASA SM requires the protocol keyword followed by TCP for configuring the number of simultaneous connections.</p> <p>The Migration Tool removes the context-name keyword from the command. If the connections keyword is found without the protocol keyword, the Migration Tool adds the protocol keyword.</p>

Default Value and Value Range Differences

The following table lists the differences in default values and value ranges between the FWSM and the ASA SM. These differences in default values and value ranges do not affect the migration to ASA SM from FWSM.

Table 2 **Default Values/Value Range Differences**

FWSM Values	ASA SM Values
Minimum failover poll time in milliseconds is 500 CLI: failover polltime msec	Minimum failover poll time in milliseconds is 200 CLI: failover polltime msec
Minimum poll interval for interfaces is 3 seconds. CLI: failover polltime interface	Minimum poll interval for interfaces is 1 second. ASA SM supports milliseconds and the minimum millisecond interval is 500. CLI: failover polltime interval failover polltime interval msec
Minimum Failover Unit poll time is 500 milliseconds CLI: failover polltime unit msec	Minimum Failover Unit poll time is 200 milliseconds CLI: failover polltime unit msec
Resource limits. Conns – 999,900 Conns/Sec – 102,400 Fixups/Sec – 10,000 Hosts – 256K Syslogs/sec – 30,000 Xlates – 256K	ASA SM does not have resource limits for all the resources that are mentioned in the FWSM column.
SIP Disconnect Timeout Minimum – 1 minute Maximum – 10 minutes CLI: timeout sip-disconnect	SIP Disconnect Timeout Minimum – 1 second Maximum – 1193 minutes CLI: timeout sip-disconnect
SIP Invite Timeout Maximum – 30 minutes CLI: timeout sip-invite	SIP Invite Timeout Maximum – 1193 minutes CLI: timeout sip-invite
Xlate Timeout Minimum – 30 seconds CLI: timeout xlate	Xlate Timeout Minimum – 1 minute CLI: timeout xlate Note The Migration Tool converts the xlate timeout command that has values between 30 seconds to 59 seconds to 1 minute.

SNMP Differences

The following FWSM MIBs are not supported by ASA SM:

```
CISCO-ENTITY-ALARM-MIB.my
CISCO-ENTITY-REDUNDANCY-MIB.my
CISCO-ENTITY-REDUNDANCY-TC-MIB.my
CISCO-NAT-EXT-MIB.my
TCP-MIB.my
UDP-MIB.my
```

The following FWSM SNMP traps are not supported by ASA SM.

```
ceAlarmAsserted: CISCO-ENTITY-ALARM-MIB.my
ceRedunEventSwitchover: CISCO-ENTITY-REDUNDANCY-MIB.my
clrResourceRateLimitReached: CISCO-L4L7MODULE-RESOURCE-LIMIT-MIB.my
```

Related Documentation

For additional information about the FWSM, go to the following URL:

http://www.cisco.com/en/US/products/hw/modules/ps2706/ps4452/tsd_products_support_model_home.html

For additional information about the ASA SM, go to the following URL:

<http://www.cisco.com/go/asadocs>

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

This document is to be used in conjunction with the documents listed in the “Related Documentation” section.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

©2010 Cisco Systems, Inc. All rights reserved.
