Using the Cisco Security Conversion Tool

This document describes how to install and use the Cisco Security Conversion Tool (Cisco SCT) Version 1.1(1). Cisco SCT converts a single Check Point 4.x, NG, NGX, or Provider-1 device configuration to a single configuration file for Cisco ASA/PIX Version 7.0 or higher, or FWSM Version 2.3 or 3.1. Cisco SCT is compatible with the Cisco security appliance CLI, ASDM, and Cisco Security Manager Version 3.0.

This document includes the following sections:

- Introduction, page 1
- What Does Cisco SCT Convert?, page 3
- Getting Started, page 4
- Running Cisco SCT, page 7
- Using the Configuration File with a Cisco Security Appliance, page 10
- Check Point Conversion Guidelines, page 19

Introduction

The process of migrating a Check Point firewall to a Cisco security appliance includes four phases:

- Phase 1—Identification of Requirements
- Phase 2—Performing the Firewall Conversion
- Phase 3—Pre-Implementation Planning
- Phase 4—Implementation

Cisco SCT helps you to complete Phase 2 more quickly and efficiently. Without Cisco SCT, migration from Check Point to Cisco can be a laborious process, taking many weeks for each device. Cisco SCT makes the process much easier.

However, the conversion is *only* for the firewall rules and related configuration and not for the entire configuration.

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

To complete a successful migration, you must also complete the other phases, but the required processes and procedures are beyond the scope of this document. For information about identifying your requirements, pre-implementation planning, and implementation, contact your Cisco TAC or account representative.

Cisco SCT runs as a Windows executable on Windows 2000 or XP. Cisco SCT automatically converts Check Point configurations to ASA 7.0 or higher, FWSM 3.1, and FWSM 2.3. Cisco SCT does not require a live device. Cisco SCT takes input from the Check Point 4.x, NG Firewall-1, NGX, and Provider-1 files:

- <objects>.C
- rulebases.fws (optional)
- <rules>.W
- Interfaces and route information

Cisco SCT generates the CLIs related to the firewall rules and ignores everything else. After installing Cisco SCT (see the "Running Cisco SCT" section on page 7, perform the following steps:

Step 1 Get the necessary files from the Check Point device.

See the "Required Check Point Files" section on page 4.

Step 2 Run Cisco SCT to generate the CLIs.

See the "Running Cisco SCT" section on page 7.

Step 3 Copy the CLIs to the ASA/PIX/FWSM.

See the "Using the Configuration File with a Cisco Security Appliance" section on page 10.

Step 4 Complete the migration by manually converting the Check Point configuration that is skipped by Cisco SCT.

If converting the Check Point firewall configuration to an unsupported Cisco security appliance, such as FWSM 2.1 or PIX Firewall 6.3, you can still use Cisco SCT to convert the firewall rules (ACLs) and manually convert the other areas of the configuration. However, FWSM Version 2.x code and pre-PIX Version 7.0 code does not support disabled rules. These will need to be manually removed from the output of Cisco SCT.

To perform a complete firewall conversion, you must complete the following four sections of the Check Point firewall configuration into Cisco security appliance syntax:

- Basic hardware configuration (interfaces, IP Addresses, routing table)

  The basic hardware configuration is typically easy to convert manually. Cisco SCT needs this information to provide the seed routing table.

- Firewall policy (rule set)

  Converting the firewall policy is time-consuming and error-prone. A manual conversion that requires weeks can be completed in minutes with far fewer errors using Cisco SCT. However, you still need to review the Cisco SCT errors and warnings to ensure that no issues were encountered.

- NAT policy

  Converting NAT policies can be easy. However, Check Point supports some NAT features that Cisco does not. In these cases, you must determine the workaround on a case-by-case basis using the errors and warnings that are generated by Cisco SCT.

- Advanced firewall features

Cisco SCT does convert administrative access or other advanced firewall features.

What Does Cisco SCT Convert?

Cisco SCT converts the following Check Point policy constructs:.

- Check Point Network objects to corresponding Cisco security appliance name or object-group network commands
- Check Point Network Group objects to Cisco security appliance **object-group network** commands
- Check Point Service Group objects into Cisco security appliance **object-group service** commands
- Check Point Rules into Cisco security appliance **access-list** and **access-group** commands
- Check Point NAT Rules into Cisco security appliance **nat/global** and **static** commands
- Network/service objects
- Access lists (rules) including references to network object groups, service object groups, time range, and log
- Access group CLI to apply an ACL to an interface
- Network address translation, including static NAT, dynamic NAT, NAT 0, no NAT control
- Network object groups including nested network object groups
- Service object groups including nested service object groups
- name CLI
- Interface configuration
- Static routes

Cisco SCT also generates the corresponding **interface** and **route** commands.

Cisco SCT generates CLIs that will work on an ASA or PIX 515/515E/525/535 running ASA/PIX Version 7.0 or higher, FWSM Version 2.3, and FWSM Version 3.1.

Not all the options for every Check Point construct are converted. The following are the exceptions:

- Actions: Only Accept or Drop/Reject are converted. Other actions are ignored.

  Only the **accept** and **drop/reject** actions are converted. The **UserAuth**, **ClientAuth**, and **SessionAuth** actions are ignored.
- Track: User Auth, Client Auth, and Session Auth are not supported.

  Only the **Log** option is converted. The **Account**, **Alert**, **SnmpTrap**, and **Mail** options are ignored
- Time range
- IP range for the source or destination address
- Negated rule
- Use of clustering
- When converting supernetting rules that span multiple interfaces, Cisco SCT will convert them to use only one interface.

Getting Started

This section describes how to get started with Cisco SCT and includes the following topics:

- Hardware and Software Requirements, page 4
- Required Check Point Files, page 4
- Creating the Routing and Interface File for the Nokia IPSO or Check Point SecurePlatform, page 5
- Running Cisco SCT, page 7

Hardware and Software Requirements

The follow source platforms are required:

- Cisco SCT supports Check Point 4.x, NG, NGX, and Provider-1.

Cisco SCT supports the following Cisco firewall destination platforms:

- Cisco Adaptive Security Appliances (ASA) running Version 7.0 or later
- Cisco PIX Firewalls running Version 7.0 or later
- FWSM 2.3 with limitations regarding NAT conversion
- FWSM 3.1

Note Cisco SCT Release 1.0 does not support Cisco IOS firewalls or Cisco PIX Firewalls running Version 6.x.

Cisco SCT requires Windows 2000 or XP with Java VM 1.4.2 or later.

Installing Cisco SCT

This section describes the procedure for installing Cisco SCT.

Step 1 Make sure you have the latest Java Runtime available in the PC.

If not, download and install the Java from http://java.sun.com/downloads/index.html Supported versions are Java 1.4.2 and 1.5 (also called 5.0).

Step 2 Download the latest installation file from Cisco.com at https://upload.cisco.com/cgi-bin/swc/fileexg/main.cgi?CONTYPES=sct

Step 3 Run the installer file.

Required Check Point Files

Cisco SCT requires the following information from the Check Point configuration for conversion to a Cisco security appliance configuration file:

- objects.C (Check Point 4.x) or objects_5_0.C (Check Point NG/NGX). This file contains the object definition for the firewall.
- <rule>.W (default Standard.W) This file contains the policy or rule definition for the firewall.

- rulebases.fws or rulebases_5_0.fws (optional). This file is stored in the management system and contains the rule comments.
- Routes and interface information (route.cfg) from the Nokia IPSO platform (see "Creating the Routing and Interface File for the Nokia IPSO or Check Point SecurePlatform" section on page 5) or in a specific format for other platforms (see the "Creating the Routing and Interface File for Other Check Point Platforms" section on page 6.)

Finding the Check Point Files

Find the Check Point files in the **conf** directory in the Check Point Firewall directory. The Check Point Firewall directory is defined by the FWDIR environment variable.

Creating the Routing and Interface File for the Nokia IPSO or Check Point SecurePlatform

If you are running a Nokia (IPSO) platform, you can obtain the required routing and interface information by entering the following command:

```
firewall[admin]# uname -a;fw ver;netstat -nr;ifconfig -a
```

However, Cisco SCT does not know the interfaces that are inside, outside, dmz, and so forth, or the interfaces that are unused. For this reason, please edit the interface information in the Cisco SCT Interface screen to appropriate values.

The following is typical output from preceding command on a Nokia IPSO platform:

```
IPSO  ...<snip>
This is Check Point VPN-1(TM) & FireWall-1(R) Version 4.1 <snip>
This is Check Point VPN-1(TM) & FireWall-1(R) Version 4.1 <snip>

Routing tables

IPv4:
Destination        Gateway            Flags     Refs     Use        Netif Expire
default            10.1.1.1           CU          0        0     eth-s1p3c0
0.0.0.0                               CU          0        0
10.1.1/24                             CGUX        0        0     eth-s1p1c0
...
<snip>
....
224/4                                 RCU         0        0
224.0.0.1                             CDU         0        0
224.0.0.18                            CDU         0        0
240/4                                 BCU         0        0
255.255.255.255                       RCGU        0        0

IPv6:
Destination        Gateway            Flags     Refs     Use        Netif Expire
default                               RCU         1        0
::/96                                 CU          0        0
::                                    CU          0        0
::1                ::1                CG          0        0
::ffff:0:0/96                         CU          0        0
ff00::/8                              RCU         0        0
ff02::1                               CDU         0        0
eth-s1p1c0:  lname eth-s1p1c0
```

```
flags=e7<UP,PHYS_AVAIL,LINK_AVAIL,BROADCAST,MULTICAST,AUTOLINK>
        inet mtu 1500 11.1.1.1/24 broadcast 10.83.1.255
        phys eth-s1p1 flags=4133<UP,LINK,BROADCAST,MULTICAST,PRESENT>
        ether <snip> speed 100M full duplex
....
<snip>
```

Make sure your output looks like this. Otherwise, Cisco SCT will not convert the file correctly.

Creating the Routing and Interface File for Other Check Point Platforms

If you are using a Check Point platform other than Nokia IPSO, you must manually create the routes.cfg file, which contains the routes and interface information in a format that can be processed by Cisco SCT. The following is the required format:

```
#INTERFACE|<interace-ip>|<subnet-mask>|<original-FW1-interface>|<pix-hwname>|<pix-logical-
name>|<pix-security-level

INTERFACE|20.1.1.1|255.255.255.248|eth-s0|ethernet0|outside|0
INTERFACE|10.1.1.1|255.255.255.248|eth-s1|ethernet1|inside|100
#ROUTE|<network>|<mask>|<gateway-addr>
ROUTE|100.1.1.0|255.255.255.0|10.1.1.254
ROUTE|0.0.0.0|0.0.0.0|20.1.1.254
```

Make sure that the last entry is the default route.

You can use the **netstat** command to get the information required to create the route.cfg file when using a non-Nokia platform. There are codes in the output that tell you if it is a directly connected interface, a host route, a network route, and so forth. The output varies depending on the platform.

The following sample output indicates that the IP address of the qfe0 interface is 10.10.10.2:

```
10.10.10.0         10.10.10.2          U        1    347     qfe0
```

In the following output, two IP Addresses are assigned to interface qfe5. The secondary IP address is indicated by a colon and a number following the interface name (qfe5:1). Secondary IP addressing is not supported on Cisco firewalls and these entries must be manually converted before including them in the route.cfg file.

```
10.10.12.0          10.10.12.4           U        1 262673  qfe5
20.10.12.0          20.10.12.103         U        1      0  qfe5:1
```

If the secondary IP address (assigned to qfe5:1 in this example) has an IP address on the same IP network as qfe5 then this is probably a shared Check Point cluster IP Address. You only need be alarmed if there are virtual interfaces residing on differing IP subnets.

In the following example a route exists to the 10.0.0.0 network. But what is the correct mask? 255.0.0.0?

```
10.0.0.0             10.116.130.1          UG       162060382
```

In this example, there is a host route to 10.15.1.2 with a network mask of 255.255.255.255. Notice the flag of UGH.

```
10.15.1.2         10.10.10.2           UGH      1      0
```

Running Cisco SCT

After completing the installation of Cisco SCT, an option is added to the Start menu. Select **Start > Programs > Cisco Security Conversion Tool > Cisco Security Conversion Tool**. The system displays the Welcome to Cisco Security Conversion Tool Wizard.

Identifying the Check Point Firewall Files

To identify the Check Point Firewall files that you want to convert, use the following options on the Welcome to Cisco Security Conversion Tool Wizard screen.

You can run Cisco SCT in a demonstration mode by checking **Demo** check box.

Check Point Firewall Files:

- Object definition file—This file contains the object definition for the Check Point Firewall. The file name is objects.C (Check Point 4.x) or objects_5_0.C (Check Point NG/NGX).
- Policy and Rule Definition File—This file contains the policy or rule definition for the Check Point Firewall. The file name is <rule>.W (default Standard.W)
- (Optional) FWS file—This file is stored in the management system and contains the rule comments. The file name is rulebases.fws or rulebases_5_0.fws.

Specifying Interface and Route Information

To specify the interface and route information required for conversion of the Check Point configuration, type the pathname and file name of the route information file or click **Browse** and select the file from the window that appears.

To provide the routes and interface information to the conversion tool, use the following methods:

If you're running Nokia IPSO or Check Point SecurePlatform platforms, follow the procedure described in “Creating the Routing and Interface File for the Nokia IPSO or Check Point SecurePlatform” section on page 5.

For all other Check Point platforms, the required format is described in the “Creating the Routing and Interface File for Other Check Point Platforms” section on page 6.

After completing the first wizard screen, click **Next**. The system displays the second wizard screen, where you can specify the target Cisco platform, identify the address format, and optimize configuration files.

Specify the Output Configuration Parameters

To specify the target Cisco firewall platforms, select one of the following options from the Output Configuration Parameters.

- ASA platform running Version 7.0 or higher
- PIX platform running Version 7.0 or higher
- FWSM platform running Version 2.3 software
- FWSM platform running Version 3.1

Identify the Address Format Used in Access Lists

To identify the address format to be used in the converted Cisco security appliance access list commands, choose one of the following options:

- Generate names command use names in access list
- Generate description as part of name commands
- Generate object-group command use object-group in access-list commands
- Use IP addresses in the access list

Optimizing Configuration Files

To optimize the output configuration file, use the following options:

- Create object groups if more than one item exists in a cell.
- Display rules similar to Check Point GUI, if using Cisco Security Manager—Generates object-group commands that display in Cisco Security Manager in a way that is analogous to the display in Check Point.

Note To use keyboard shortcuts instead of a mouse, press **Alt-+***shortcut key*. The shortcut keys are underlined on each page of the Wizard.

The first option generates object group names when more than one item exists in a cell in the source CheckPoint configuration.

The second option generates **object-group** commands that will be displayed in the rule table similar to Check Point. A Check Point rule can specify multiple source or destination addresses. To get this behavior, Cisco SCT converts this rule into a network object group using a special name. CSM recognizes this special name and displays the elements in the object group in a single row just like in Check Point.

Specifying Output Options

To specify the location and name of the output file, use the following options (which are prepopulated by default):

- Directory—Enter the absolute path to where you want the output file stored. The default is C:\Program Files\Cisco Systems\SCT\output.
- Config File Name—Enter the name you want for the output file. The default is device-config.cfg.

Configuring Interfaces on the Cisco Device

The third wizard screen lets you configure the interfaces on the Cisco device. You can set the security level, interface name, Checkpoint interface name, IP address and subnet mask for each interface on your security appliance.

Select **Edit** to enable and change the properties of each interface.

Generating the Configuration Listing

After completing the wizard screens, the system displays the **Summary Page**. This screen lists the input files that will be used during the conversion process. Click **Back** to change any of the input information, or click **Finish** to begin the conversion process.

When you click **Finish** on this screen, the system displays a summary of the conversion, as well as statistics about what has been produced from the conversion.

The Summary Page displays general conversion statistics.

To view details regarding the conversion, click the **Conversion Report** button. The system displays the report in your browser, but you may need to disable pop-up blocking to view it.

Conversion Report

To view details regarding the conversion, click the **Conversion Report** button. The system displays the report in your browser, but you may need to disable pop-up blocking to view it.

The Conversion Report tab lists each Check Point rule in numerical order and shows the Cisco security appliance commands that have been automatically generated from the Check Point rules. Messages are displayed describing any elements that could not be completely converted and that require manual conversion. The message may be informational, warning, or error messages.

The first few lines of the Conversion Report shows the following information:

- Date and time the conversion was completed
- Input files
- Options enabled
- General messages regarding NAT conversion

The rest of the Conversion Report is divided into the following sections, which you can jump to using the links at the top of the screen:

- Messages—Error messages that indicate problems or exceptions that occurred during conversion.
- Interface—The Cisco security appliance interface configuration
- Route—Lists the static routes generated from the Check Point routing information provided.
- Name—Lists the host names with the associated IP addresses that are used in the Cisco security appliance configuration.
- Network Object Group—Lists the network object group definitions
- Service Object Group—Lists the service object group definitions
- NAT—Contains the NAT rules for the Cisco security appliance. This section contains a command to disable NAT control, which allows traffic to flow without explicit NAT rules. NAT control is a Cisco security appliance option that prevents traffic flow until specific NAT rules are defined.
- Access Rules—Lists the Cisco security appliance access lists, with each access control entry (ACE) on a separate line.

Original Check Point Rules

To view the original Check Point configuration, click the **Original Check Point Policy** tab.

This window displays each Check Point rule with each element listed a separate column. Table 1 summarizes the contents of each column.

Table 1 Check Point Policy Elements

Column Heading	Description
Rule	The numerical order of the Check Point rule.
Source	The source object, such as an address or host name, to which the rule applies.
Destination	The destination object, such as an address or host name, to which the rule applies.
Services	The specific services to which the rule applies.
Action	The action taken on traffic that matches the rule criteria. Only the **accept** and **drop/reject** actions are converted. The **UserAuth**, **ClientAuth**, and **SessionAuth** actions are ignored.
Track	The methods used to monitor traffic that matches the rule criteria. Only the **Log** option is converted. The **Account**, **Alert**, **SnmpTrap**, and **Mail** options are ignored
Time	The time range during which the rule is in effect.
Install on	The Check Point devices on which the rule should be applied.
Comment	Text description of the rule.

Note Rules that were disabled in Check Point are shown in red type. In the Cisco security configuration, rules that were disabled in Check Point are converted to access lists ending with the **inactive** option, which disables the access list on the Cisco security appliance.

ASA/PIX/FWSM Configuration File

To view the Cisco security appliance configuration file, click the **Cisco Device Config** tab. The system displays the configuration in your browser.

This screen provides the actual configuration listing that you need to configure to the Cisco security appliance. For information about different ways to do this, see the "Using the Configuration File with a Cisco Security Appliance" section on page 10.

Using the Configuration File with a Cisco Security Appliance

This section describes how to use the converted configuration file with a Cisco security appliance. It includes the following topics:

- Backing up the System Configuration From the Command Line, page 11
- Downloading Configuration Files From the Command Line, page 11

Note It is not recommended that you copy and paste your configuration into a terminal session on the Cisco security appliance, because some long lines may truncate and be misread because of a line wrap. Additionally, the terminal session buffer may not be big enough for cutting and pasting large configuration files.

Backing up the System Configuration From the Command Line

If the Cisco security appliance has a working configuration that you want to keep, back it up before proceeding.

In single context mode, or from the system configuration in multiple mode, you can back up the startup configuration, running configuration, or any configuration file in Flash memory.

Enter one of the following commands for the appropriate backup server:

- To copy to a TFTP server, enter the following command:

  ```
  hostname# copy {startup-config | running-config | flashmem:/[path/]filename}
  tftp://server[/path]/filename
  ```

  where *flashmem is* **flash**, **disk0**, **or disk1**. The **flash** keyword represents the internal Flash memory on the PIX 500 series security appliance. You can enter **flash** or **disk0** for the internal Flash memory on the ASA 5500 series adaptive security appliance or FWSM. The **disk1** keyword represents the external Flash memory on the ASA.

- To copy to an FTP server, enter the following command:

  ```
  hostname# copy {startup-config | running-config | flashmem:/[path/]filename}
  ftp://[user[:password]@]server[/path]/filename[;type=xx]
  ```

In multiple context mode, from within a context, you can perform the following backups:

- To copy the running configuration to the startup configuration server (connected to the admin context), enter the following command:

  ```
  hostname/contexta# copy running-config startup-config
  ```

- To copy the running configuration to a TFTP server connected to the context network, enter the following command:

  ```
  hostname/contexta# copy running-config tftp:/server[/path]/filename
  ```

Downloading Configuration Files From the Command Line

This section describes how to download the startup and running configuration files and context configuration files from a TFTP server. This section includes the following topics:

- Copying the Cisco Security Appliance Configuration to a Server, page 12
- Downloading a Text File to the Startup or Running Configuration, page 12
- Configuring the File to Boot as the Startup Configuration, page 13
- Copying the Startup Configuration to the Running Configuration, page 13

Copying the Cisco Security Appliance Configuration to a Server

To upload the Cisco security appliance configuration from Cisco SCT to a TFTP, HTTP, or FTP server, perform the following steps:

Step 1 Click on the **Cisco Security Application Configuration** tab on Cisco SCT.

Step 2 Use the mouse or press **Shift+Down Arrow** to select the entire configuration listing.

Step 3 Select **Edit** > **Copy** of press **Ctrl+C** to copy the configuration listing into the clipboard.

Step 4 Open a text editor, such as Notepad and paste the configuration listing into the Notepad window.

Select **Edit** > **Paste** or press **Ctrl+V**.

Step 5 Save the file with an appropriate file name to the correct directory on the server.

Make sure you save the file to a directory on a server to which the security appliance is connected and has read access.

Note It is not recommended that you copy and paste your configuration into a terminal session on the Cisco security appliance, because some long lines may truncate and be misread because of a line wrap. Additionally, the terminal session buffer may not be big enough for cutting and pasting large configuration files.

Downloading a Text File to the Startup or Running Configuration

You can download a text file from the following server types:

- TFTP
- FTP
- HTTP
- HTTPS

Make sure you have network access to the server:

- For single context mode, configure any interface, its IP address, and any static routes required to reach the server.
- For multiple context mode, add the admin context and configure interfaces, IP addresses, and routing to provide network access.

To check connectivity, use the **ping** command.

To copy the startup configuration or running configuration from the server to the security appliance, enter one of the following commands for the appropriate download server.

Note When you copy a configuration to the running configuration, you merge the two configurations. A merge adds any new commands from the new configuration to the running configuration. If the configurations are the same, no changes occur. If commands conflict or if commands affect the running of the context, then the effect of the merge depends on the command. You might get errors, or you might have unexpected results.

- To copy from a TFTP server, enter the following command:

  hostname# **copy tftp://***server*[**/***path*]**/***filename* {**startup-config** | **running-config**}

- To copy from an FTP server, enter the following command:

  hostname# **copy ftp://**[*user*[**:***password*]**@**]*server*[**/***path*]**/***filename* {**startup-config** | **running-config**}

  You can use ASCII or binary for configuration files.

- To copy from an HTTP or HTTPS server, enter the following command:

  hostname# **copy http**[**s**]**://**[*user*[**:***password*]**@**]*server*[**:***port*][**/***path*]**/***filename* {**startup-config** | **running-config**}

For example, to copy the configuration from a TFTP server, enter the following command:

hostname# **copy tftp://209.165.200.226/configs/startup.cfg startup-config**

To copy the configuration from an FTP server, enter the following command:

hostname# **copy ftp://admin:letmein@209.165.200.227/configs/startup.cfg;type=an startup-config**

To copy the configuration from an HTTP server, enter the following command:

hostname# **copy http://209.165.200.228/configs/startup.cfg startup-config**

Configuring the File to Boot as the Startup Configuration

By default, the security appliance boots from a startup configuration that is a hidden file. For PIX/ASA Version 7.0 and higher, you can alternatively set any configuration to be the startup configuration by entering the following command:

hostname(config)# **boot config** {**flash:/** | **disk0:/** | **disk1:/**}[*path***/**]*filename*

The **flash:/** keyword represents the internal Flash memory on the PIX 500 series security appliance. You can enter **flash:/** or **disk0:/** for the internal Flash memory on the ASA 5500 series adaptive security appliance. The **disk1:/** keyword represents the external Flash memory on the ASA.

Copying the Startup Configuration to the Running Configuration

Copy a new startup configuration to the running configuration using one of these options:

- To merge the startup configuration with the current running configuration, enter the following command:

  hostname(config)# **copy startup-config running-config**

- To load the startup configuration and discard the running configuration, restart the security appliance by entering the following command:

  hostname# **reload**

  Alternatively, you can use the following commands to load the startup configuration and discard the running configuration without requiring a reboot:

  hostname/contexta(config)# **clear configure all**
  hostname/contexta(config)# **copy startup-config running-config**

Using the Configuration File with Cisco Security Manager

The following sections provide information about using Cisco SCT with Cisco Security Manger. If you are not working with Cisco Security Manager you may safely ignore this section. This section includes the following topics:

- Applying the Configuration File with Cisco Security Manager, page 14
- Copying and Sharing Policies with Cisco Security Manager, page 16

Applying the Configuration File with Cisco Security Manager

When you add a device to Cisco Security Manager, you bring in a range of identifying information for the device, such as DNS name, IP address, and the software release. To use a configuration file with Cisco Security Manager, make sure this information is correct in the configuration file that was converted by Cisco SCT.

After you add the device, it appears in the Cisco Security Manager device inventory. You can then copy or clone the configuration policy to other devices in the network. When you clone the policy, a single copy of the configuration file is used for all the associated devices. Any changes made to that file are applied to all devices that use the cloned policy.

Step 1 Click the **Device View** button in the toolbar. The Devices page appears.

Step 2 Click the **Add** button in the Device selector. The New Device - Choose Method wizard page appears with four options.

Step 3 Select **Add Device(s) from Configuration File**, then click **Next**.

Step 4 Select the device type for the new device:

a. Select the top-level device type folder to display the supported device families.

b. Select the device family folder to display the supported device types.

c. Select the device type.

Note If you do not know the device type, select the device family folder as described in step b. Through discovery, Cisco Security Manager automatically selects the appropriate device type for the new device.

System object IDs for that device type are displayed in the SysObjectId field.

Step 5 Enter the full path to the directory containing the device configuration files in the Configuration Files field, or click **Browse** to navigate to the directory and locate the configuration file.

Step 6 From the Discover field, select one of the discovery options:

- Policies and Inventory—When selected, discovers policies and interfaces. This is the default option.

  When policy discovery is initiated, the system analyzes the configuration on the device, then imports the configured service and platform policies into Cisco Security Manager to be managed. When inventory discovery is initiated, the system analyzes the interfaces on the device and then imports them into Cisco Security Manager to be managed. If the device is a composite device, all the service modules in that device are discovered.

  If you select this option, the following policies are displayed:

  - Platform Settings—Also called platform-specific policy domains. Platform-specific policy domains exist on firewall devices and Cisco IOS routers. These domains contain policies that configure features that are specific to the selected platform.

    This is the default option. If you do not want these discovered, deselect this check box.
  - Firewall Policies—Also called firewall services. Firewall services include policies, such as access rules, inspection rules, AAA rules, web filter rules, and transparent rules.

    This is the default option. If you do not want these discovered, deselect this check box.
- Inventory Only—When selected, discovers interfaces. If the device is a composite device, all the service modules in that device are discovered.
- No Discovery—When selected, Cisco Security Manager does not initiate discovery.

Step 7 Select the **Security Context of Unmanaged Parent** check box to manage a security context, whose parent (PIX Firewall, ASA, or FWSM) is not managed by Cisco Security Manager.

You can partition a PIX Firewall, ASA, or FWSM into multiple virtual firewalls, also known as security contexts. Each context is an independent system, with its own configuration and policies. You can manage these standalone contexts in Cisco Security Manager, even though the parent (PIX Firewall, ASA, or FWSM) is not managed by Cisco Security Manager.

Note This field is active only if the device you selected in the Device selector is a firewall device, such as PIX Firewall, ASA, or FWSM and that firewall device supports virtual context.

Step 8 Do one of the following:

- Click **Finish**. The system performs device validation tasks.

  If the data you entered is incorrect, the system generates error messages and displays the wizard page where the error occurs with a red error icon corresponding to it. Otherwise, the Task Status page appears, displaying the status of the device import and discovery.

  Do one of the following in the Task Status page:
  - Click **Abort** to end device import and discovery. This button is enabled during device import and discovery.
  - Click **Close** to close this page. This button is enabled after device import and discovery are completed.
- Click **Next** to continue. The Device Grouping wizard page appears.

Step 9 Do one of the following:

- Click **Finish**. The system performs device validation tasks.

  If the data you entered is incorrect, the system generates error messages and displays the wizard page where the error occurs with a red error icon corresponding to it. Otherwise, the Task Status page appears, displaying the status of the device import and discovery.

  Do one of the following in the Task Status page:
  - Click **Abort** to end device import and discovery. This button is enabled during device import and discovery.
  - Click **Close** to close this page. This button is enabled after device import and discovery are completed.
- Click **Next** to continue.

Step 10 (Optional) Assign the device to a group.

Note If you add the device without specifying the information in the Device Grouping tab, that device is added to the ALL folder in the Device selector. You can then manage that device directly from the ALL folder.

Step 11 Click **Finish**. The system performs device validation tasks.

If the data you entered is incorrect, the system generates error messages and displays the wizard page where the error occurs with a red error icon corresponding to it. Otherwise, the Task Status page appears, displaying the status of the device import and discovery.

Step 12 Do one of the following in the Task Status page:

- Click **Abort** to end device import and discovery. This button is enabled during device import and discovery.
- Click **Close** to close this page. This button is enabled after device import and discovery are completed.

Copying and Sharing Policies with Cisco Security Manager

This section describes how to use Cisco Security Manager to copy policies from one device to another or to share a single policy among multiple devices. It includes the following topics:

- Configuring Local Policies in Device View, page 16
- Copying Policies Between Devices, page 17
- Working with Shared Policies in Device View, page 17

Configuring Local Policies in Device View

Use Device view to configure local platform and service policies on individual firewall devices and Cisco IOS routers. Each policy defines a particular configuration task the device can perform. Local policies are unnamed and are particular to the individual device on which they have been defined. Any changes that you make to a local policy do not affect other devices that Cisco Security Manager is managing.

When you configure a policy, a lock is placed on that policy to prevent other users from making changes to the same policy at the same time. After configuring a policy, you must deploy the changes to the device in order to make them active on that device.

Step 1 In Device view, select a device from the Device selector, then select a policy for that device from the Device Policies selector. The details of the policy appear in the work area.

Step 2 Click **Save** to save your changes to the server.

If this is the first time you are configuring this policy on this particular device, the icon next to the selected policy changes to indicates that the policy is configured and assigned locally to the device.

Copying Policies Between Devices

Cisco Security Manager enables you to streamline device configuration by copying multiple policies, or even a complete set of policies, from one device to others of the same type. This makes it easy, for example, to quickly configure a new firewall device with the same policies configured on an existing firewall device.

When copying policies between devices, those policies that are local on the source device are copied locally to the target device. Those policies that are shared policies assigned to the source device are assigned as shared policies to the target device as well.

Tip Use the Clone Device feature to create a new device of the same type that shares the same configuration and properties (including device operating system version, credentials, and grouping attributes) as the source device.

Step 1 In Device view, select a device from the Device selector.

Step 2 Do one of the following:

- Select **Policy > Copy Policies Between Devices**.
- Right-click a device in the Device selector, then select **Copy Policies Between Devices**.

The Copy Policies wizard is displayed.

Step 3 On the Select Source Device page, select the source device from which to copy policies, then click **Next**. The Select Target Devices page is displayed.

Note If you selected a device before selecting the Copy Policies Between Devices command, you are automatically brought to the second page of the wizard. You can click **Back** to return to the first page to select a different device.

Step 4 Select the target devices to which you want to copy policies from the source device, then click **Next**. The Select Policies page is displayed.

Step 5 (Optional) By default, all policy types that have been configured on the source device (local and shared) are selected for copying. If you do not want to copy some policies, deselect the check box next to those policies.

Note When copying policies between firewall devices, copying the interfaces policy automatically copies the failover policy and vice-versa.

Step 6 Click **Finish**. The selected policies are copied from the source device to the target device.

Working with Shared Policies in Device View

Sharing policies makes it possible to configure multiple devices with common policies, which provides greater consistency in your policy definitions and streamlines your management efforts. Any changes to a shared policy affect all the devices and VPN topologies to which the policy is assigned. This makes it easy, for example, to update all of your Cisco IOS routers with new quality of service policies by updating the shared Quality of Service policy assigned to these devices.

When working in Device view, you can convert a local policy (such as a policy created during device discovery) to a shared policy. You can then assign the shared policy to as many devices as you want, and you can change these assignments at any time. In addition, you can take a shared policy and convert it back to a local policy for a particular device. You can use this action to create a special configuration that affects only that device. Other devices assigned the shared policy continue to use the shared policy as before.

Note As an alternative to converting local policies, you can create new shared policies from scratch in Policy view. After creating the shared policy and assigning it to devices in Policy view, you can return to Device view and perform additional operations on the policy, as described in the sections that follow.

Shared policies can also be created and managed at the network level using Policy view.

As your network grows, you might decide to convert a local policy into a shared policy that you can assign to multiple devices. Sharing a policy provides a streamlined management approach that ensures that all devices assigned to the policy are configured in a consistent manner. For example, if you configure a set of firewall inspection rules on a particular device, sharing that device's inspection rules policy makes it possible to assign that policy to other devices, eliminating the need to configure each device individually. In addition, having a shared policy enables you to update the configurations of each assigned device at one time, saving time and promoting greater consistency across your set of managed devices.

When you share a policy, you must name the policy. (Local policies do not have names, because they are associated with only a single device.) This enables you to identify this policy when managing shared policies in Policy view.

Step 1 In Device view, select a device from the Device selector, then select a local policy for that device from the Device Policies selector. The details of the policy appear in the work area.

Step 2 Do one of the following:

- Select **Policy > Share Policy**.
- Right-click the local policy, then select **Share Policy**.

The Share Policy dialog box is displayed.

Step 3 Enter a name for the shared policy. Policy names can contain up to 255 characters, including spaces and special characters.

Step 4 Click **OK** to save the policy as a shared policy.

In the Device Policies selector, the icon next to the selected policy type changes to show that the policy is now a shared policy.

Additionally, a header is added to the work area above the policy definition details. This header contains several important pieces of information: the name of the policy (and its inheritance, if applicable) and the number of devices to which the policy is assigned (including the selected device), as well as user privilege and lock indicators, where applicable. Links contained in the header can be used as follows:

- Click the link in the policy name to select a different shared policy to assign to the selected device.
- Click the link in the number of assigned devices to edit the list of devices to which the policy is assigned.

Check Point Conversion Guidelines

This section provides guidelines to follow for a successful conversion from a Check Point firewall to a Cisco security appliance. It includes the following topics:

- General Guidelines and Issues, page 19
- Routing Guidelines and Issues, page 19
- Converting Network Objects, page 20
- Converting to Multiple Security Contexts, page 21
- Network Management Guidelines, page 22

General Guidelines and Issues

The following are general guidelines and issues that apply to converting a Check Point firewall configuration to a Cisco security appliance:

- Cisco enforces firewall rules on an interface-specific basis. However, Check Point enforces firewall rules globally, meaning without regard to the interfaces through which the data passes. This does not lend itself well to the Cisco architecture.

  As a result, after the conversion some rules will require manual pruning. For example, if a Check Point firewall allows any host to access a particular device then that rule will be applied to every interface on a Cisco security appliance by Cisco SCT.

  Often, it is the intent of the firewall administrator to allow Internet access to a particular host and not necessarily allow DMZ or Inside access to that host. Although the conversion tool provides the exact same effective policy as the original Check Point firewall configuration, most administrators will want to manually prune these rules from some of the interfaces of the Cisco security appliance.
- Disconnect the Check Point firewall interfaces from the network before connecting the Cisco firewalls interfaces to the same network. This will avoid ARP collisions that might occur if both firewalls have interfaces on the same network (or VLAN). Check Point firewalls experiencing ARP collisions may hang and require a hard reset. If you preconfigure and predeploy the Cisco firewall, ensure that the interfaces are not assigned to the same network as any Check Point firewall until you are ready to replace the Check Point device.
- Audit and cleanup firewall rules either before or after, but not in the middle of a firewall migration. Making major changes during a firewall migration introduces unnecessary variables and risks.
- Enable the Check Point counter-spoofing feature in production before converting to a Cisco device. Resolve any issues that arise before conversion. Issues that arise when the counter-spoofing feature is enabled indicate underlying problems in the existing firewall or network configuration.

Routing Guidelines and Issues

The following guidelines apply to the conversion of routing and interface configuration from a Check Point firewall to a Cisco security appliance:

- Successful pings through a Check Point firewall may give a false confirmation of connectivity. Because ICMP is a connectionless protocol, it may pass through the standby firewall and successful responses pass back through the primary firewall. For example, an outside router may be

misconfigured with a static route with a next-hop-address of the standby firewall instead of the active firewall. When performing a ping, successful replies may be received but any TCP or UDP connections will be dropped.

Note There are frequently implicit Check Point rules which allow icmp traffic. Cisco firewalls do not implicitly allow icmp traffic.

- Extended pings from a router can source a router interface that is *not* the nearest interface to the destination device.
- Avoid using Policy Based-Routing (PBR). Note that multicast traffic and PBR typically do not mix well. Also, PBR does not support high availability very well. PBR is really just complicated static routing.
- Avoid asymmetric routing across disparate firewall interfaces: Check Point firewalls are very tolerant of network issues resulting in asymmetric routing because Check Point enforces firewall policy globally, across all interfaces. However, a Cisco firewall will not tolerate asymmetric routing. Asymmetric routing is often caused by multi-VLAN, multi-homed servers. The following are some specific notes regarding this scenario:
  - Servers that have multiple Ethernet interfaces connected to more than one IP subnet or VLAN can create an issue where traffic with the source IP address of one server interface is forwarded out a second server interface—frequently due to a default route. For example, a server connected to VLAN 10 and 20 with a default gateway on VLAN 10 may receive traffic on VLAN 10 with a source IP address from the server interface on VLAN 20. Check Point firewalls tolerate this scenario.
  - If the Check Point firewall has the anti-spoofing or counter-spoofing feature enabled, this scenario should not occur or have a negative impact during the migration from Check Point to Cisco.
- Secondary IP addressing is not supported on Cisco security appliances.
- Avoid sharing interfaces across multiple firewall (security) contexts, except for a shared management interface. Many problems are associated with sharing interfaces across multiple security contexts. Although many of these problems can be avoided with a carefully designed deployment, overlapping static NAT translations remain a problem in this scenario. Misconfiguration of a static NAT translation on one security context can negatively impact another security context.

  For all supported Cisco platforms except FWSM Version 2.3, the requirement to configure certain static NAT statements is not necessary if you have **no nat-control** configured. However, if you deploy a shared interface across multiple security contexts, then you will not be able to take advantage of this enhancement.

Converting Network Objects

The following guidelines apply to the conversion of network objects from a Check Point firewall configuration to a Cisco security appliance:

- Check Point administrators use network objects extensively. These objects are defined from a strict functional perspective without consideration of where the members of the object reside. Cisco SCT clones network objects with members connected through multiple interfaces. This is required because some device management applications, such as PDM, require that every object be defined in relation to an interface.

For example, a Check Point network object, "network-x," includes the definition for three networks, each of which may exist on three different firewall interfaces. In this case, three network objects are created by Cisco SCT after conversion.

- Define objects from a functional and interface perspective. For example, if you have SMTP servers off two DMZ subnetworks, then define two objects: SMTP-Server-DMZ1 and SMTP-Servers-DMZ2. This is important if you are using a device manager such as PDM or ASDM to manage your Cisco security appliance.
- Avoid the use of the **name** command. Define network objects instead. If you use names as an option with the current version of Cisco SCT then the description of the objects to be converted will be lost.
- If you must use the **name** command, then append the network mask, in significant bit notation, to the name of the object. For example, change the name of name george 10.10.10.0 with an expected network mask of 255.255.255.0 to name george-24 10.10.10.0. This lets you verify that the correct network mask is used with the named object.
- Do not use nested object groups if you are using PDM or ASDM, because PDM and ASDM do not support nested object groups. A nested object is an object with members that are network objects.
- Mixed use of network objects and **name** commands may result in a named object having the exact same name as a network object. Besides being confusing, this may result in an inconsistent network mask application, which in turn may result in too broad or too narrow application of a rule.
- If you have a large number of objects, some objects may not appear correctly in PDM/ASDM. That is, they may not appear under an interface or appear as an unknown object. Further, the objects may not appear in the correct order.

Converting to Multiple Security Contexts

The following guidelines apply to the conversion of a Check Point firewall configuration to a Cisco security appliance with multiple security contexts.

To split a single Check Point firewall configuration into multiple virtual firewalls (security contexts), perform the following steps:

Step 1 Create a test firewall system.

Step 2 Remove all the rules that do not apply to the virtual firewall that you wish to deploy.

Step 3 Capture the .W file and run it through Cisco SCT.

Step 4 If the output includes multiple interfaces, take the first output of the routing table in the converted Cisco configuration to generate a manual routing table.

It is important that you create or edit the route.cfg table to accurately reflect the interfaces which need to be converted and the relevant routes that that security context should contain.

Step 5 Run it through Cisco SCT again but with the config.ini file pointing to the manual routing table.

- Do not pre-deploy a firewall with the monitoring (for failover) of interfaces enabled. This is especially important for virtual firewalls as some security contexts may already be deployed in production. The impact is that the primary firewall may initiate failover procedures and become the standby firewall. If nothing else, it is alarming when you begin the firewall implementation to find that the secondary firewall is active.

- Place a router (**msfc interface**) between security contexts. Do not directly daisy-chain security contexts where one firewalls interface is directly connected to another firewall interface.
- Use relevant interface names in the system configuration and individual security contexts. This will help prevent confusion as to the purpose of any VLAN regardless of what portion of the configuration is being reviewed.

  For example, the following interface configuration might be used in the system configuration:

  ```
  allocate-interface vlan101 vlan101-outside
  ```

  In the security context, the following configuration might be used:

  ```
  nameif vlan101-outside outside security
  ```

  When looking at the system configuration, you can tell that VLAN 101 corresponds to the outside interface of the relevant context. When looking at the relevant context, you can see that VLAN 101 is tied to the outside of the context. Basically, the **allocate-interface** and **nameif** commands provide the "cabling" for your virtual firewall. By following a consistent naming convention, you are doing a good job of labeling your cables, as it were.

Network Management Guidelines

The following guidelines address network management issues that arise when converting a Check Point firewall configuration to a Cisco security appliance:

- A shared management interface for security contexts is recommended but not required. Typically, there should not be any static NAT commands for the management interface as the management interface should not be a transit interface for any production traffic. A benefit of using a shared interface for the management network, when converting to FWSM, is the default PVLAN behavior of the FWSM. The FWSM does not allow one security context to communicate with another security context.
- If you are using a device management GUI, such as PDM or ASDM, and you use a shared interface for the management network of multiple security contexts, exclude any security context that supports VPN access for firewall administrators. The FWSM has a default PVLAN behavior. A remote administrator will not be able to remotely administer a firewall context using a device management GUI. This is not an issue if a centralized management server such as Cisco Works VPN Management Solution (VMS) or Cisco Security Manager is used.
- When possible, use VMS or CSM to manage firewalls and security contexts because these tools support nested objects, software configuration version control, and they can automatically audit firewalls to help prevent unauthorized changes in the configuration.
- Protect management servers behind a standalone security appliance, such as a Cisco ASA. The benefits include IPS, firewall, and SSL Proxy VPN access. SSL VPN access allows secure remote access to the management network. Additionally, SSL Proxy VPN allows administrators access to web applications and email.
- Specific VMS best practices should be considered when installing the VMS application. Following Cisco AS best practice will result in a robust and responsive VMS application.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:

http://www.cisco.com/univercd/home/home.htm

The Product Documentation DVD is created and released regularly. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

http://www.cisco.com/go/marketplace/docstore

Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

http://www.cisco.com/go/marketplace/docstore

If you do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Technical Support & Documentation site area by entering your comments in the feedback form available in every online document.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to do the following:

- Report security vulnerabilities in Cisco products
- Obtain assistance with security incidents that involve Cisco products
- Register to receive security information from Cisco

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For emergencies only—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.
- For nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked encryption key or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT to find other means of encrypting the data before sending any sensitive material.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive Cisco Product Alerts and Cisco Field Notices by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. (To register as a Cisco.com user, go to this URL: http://tools.cisco.com/RPF/register/register.do) Registered users can access the tool at this URL: http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the **Cisco Product Identification Tool** to locate your product serial number before submitting a request for service online or by phone. You can access this tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This tool offers three search options: by product ID or model name; by tree view; or, for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Tip Displaying and Searching on Cisco.com

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing F5.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. On the Cisco.com home page, click the **Advanced Search** link under the Search box

and then click the **Technical Support & Documentation** radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411
Australia: 1 800 805 227
EMEA: +32 2 704 55 55
USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The Cisco Online Subscription Center is the website where you can sign up for a variety of Cisco e-mail newsletters and other communications. Create a profile and then select the subscriptions that you would like to receive. To visit the Cisco Online Subscription Center, go to this URL:

  http://www.cisco.com/offer/subscribe

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco channel product offerings. To order and find out more about the *Cisco Product Quick Reference Guide*, go to this URL:

  http://www.cisco.com/go/guide

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- Cisco Press publishes a wide range of general networking, training, and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website where networking professionals share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- "What's New in Cisco Documentation" is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of "What's New in Cisco Documentation" at this URL:

  http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html