CHAPTER 61

Managing Routers

Note From version 4.17, though Cisco Security Manager continues to support IOS features/functionality, it does not support any bug fixes or enhancements.

Cisco Security Manager supports the management and configuration of security features and other platform-specific features on Cisco IOS access security routers. You configure these features in the form of policies, each of which defines a different aspect of the configuration of the router. For a detailed explanation of the policy paradigm used by Security Manager, see Chapter 5, "Managing Policies".

You can discover the configurations that are already defined on Cisco IOS routers. The discovery process imports the device configuration into Security Manager as policies and policy objects that you can then manage as required. For more information, see Discovering Router Policies, page 61-3.

Note Security Manager supports Cisco IOS Software Releases 12.3 and later. However, a limited number of policies are supported for routers running Cisco IOS Software Release 12.1 or 12.2. See Configuring Routers Running IOS Software Releases 12.1 and 12.2, page 61-3.

By right-clicking a policy type in one of the policy selectors, you can assign a policy to a single router, share the policy among multiple routers, or unassign the policy from the device.

The following topics describe how to configure platform policies and interface policies on Cisco IOS routers:

- Interface polices:
  - Basic Interface Settings on Cisco IOS Routers, page 62-1
  - Advanced Interface Settings on Cisco IOS Routers, page 62-13
  - IPS Module Interface Settings on Cisco IOS Routers, page 62-22
  - CEF Interface Settings on Cisco IOS Routers, page 62-25
  - Dialer Interfaces on Cisco IOS Routers, page 62-28
  - ADSL on Cisco IOS Routers, page 62-34
  - SHDSL on Cisco IOS Routers, page 62-41
  - PVCs on Cisco IOS Routers, page 62-47
  - PPP on Cisco IOS Routers, page 62-71
- Device administration policies:
  - AAA on Cisco IOS Routers, page 63-2

  - User Accounts and Device Credentials on Cisco IOS Routers, page 63-14
  - Bridging on Cisco IOS Routers, page 63-18
  - Time Zone Settings on Cisco IOS Routers, page 63-22
  - CPU Utilization Settings on Cisco IOS Routers, page 63-25
  - HTTP and HTTPS on Cisco IOS Routers, page 63-28
  - Line Access on Cisco IOS Routers, page 63-35
  - Optional SSH Settings on Cisco IOS Routers, page 63-63
  - SNMP on Cisco IOS Routers, page 63-66
  - DNS on Cisco IOS Routers, page 63-74
  - Hostnames and Domain Names on Cisco IOS Routers, page 63-77
  - Memory Settings on Cisco IOS Routers, page 63-78
  - Secure Device Provisioning on Cisco IOS Routers, page 63-81
  - DHCP on Cisco IOS Routers, page 63-87
  - NTP on Cisco IOS Routers, page 63-96
- Identity policies:
  - 802.1x on Cisco IOS Routers, page 64-1
  - Network Admission Control on Cisco IOS Routers, page 64-8
- Logging policies:
  - Logging on Cisco IOS Routers, page 65-1
- Quality of Service:
  - Quality of Service on Cisco IOS Routers, page 66-1
- Routing policies:
  - BGP Routing on Cisco IOS Routers, page 67-1
  - EIGRP Routing on Cisco IOS Routers, page 67-8
  - OSPF Routing on Cisco IOS Routers, page 67-19
  - RIP Routing on Cisco IOS Routers, page 67-42
  - Static Routing on Cisco IOS Routers, page 67-50

Note The settings on the Policy Management page of the Security Manager Administration window determine which router platform policies can be managed with Security Manager. Any policy type that you do not select in this window does not appear on the configuration pages of Security Manager.

Configuring Routers Running IOS Software Releases 12.1 and 12.2

Note From version 4.17, though Cisco Security Manager continues to support IOS features/functionality, it does not support any bug fixes or enhancements.

Security Manager provides limited support for routers running Cisco IOS Software Releases 12.1 and 12.2 (with the exception of the ASR 1000 Series, which supports more features). You can configure the following policies on these routers:

- Access Rules (Layer 3 only). See Chapter 16, "Managing Firewall Access Rules".
- Access Rule Settings. See Chapter 16, "Managing Firewall Access Rules".
- Interfaces. See Basic Interface Settings on Cisco IOS Routers, page 62-1.
- FlexConfigs. See Chapter 7, "Managing FlexConfigs".

All other policies require Cisco IOS Software Release 12.3 or later. For more information about supported devices, see *Supported Devices and Software Versions for Cisco Security Manager*.

Discovering Router Policies

You can discover the configurations of your Cisco IOS routers and import these configurations as policies into Security Manager. This makes it possible to add existing devices and manage them with Security Manager without having to manually configure each device policy by policy. For more information, see Adding Devices to the Device Inventory, page 3-6.

You can discover all Cisco IOS commands that can be configured with Security Manager. Discovery ignores unsupported commands, which means that they are left intact on the device even after subsequent deployments. Additionally, in cases where Security Manager can discover the command, but not all the subcommands and keywords related to that command, the unsupported elements are ignored and left intact on the device.

You can also rediscover the configurations of devices that you are already managing with Security Manager at any time. Be aware, however, that performing rediscovery overwrites the policies that you have defined in Security Manager, and is therefore not generally recommended. For more information, see Discovering Policies on Devices Already in Security Manager, page 5-15.

Note We recommend that you perform deployment immediately after you discover the policies on a Cisco IOS router, *before* you make any changes to policies or unassign policies from the device. Otherwise, the changes that you configure in Security Manager might not be deployed to the device.

Note If a policy that is not configured in Security Manager was configured on the device using an out-of-band method (such as the CLI) between the time of the first discovery and rediscovery, we recommend that you perform deployment immediately after rediscovery.

Related Topics

- Understanding Policies, page 5-1

- Discovering Policies, page 5-12
- Working with Deployment and the Configuration Archive, page 8-25