Application Note

Cisco Router and Security Device Manager **Role-Based Access**

Introduction

This document gives an example of how to restrict user access to a set of operational commands and configuration capabilities.

Role-Based CLI Access

The Role-Based CLI Access feature of Cisco IOS® Software allows the network administrator to define "views," which are a set of operational commands and configuration capabilities that provide selective or partial access to Cisco IOS EXEC and configuration (config) mode commands. Views restrict user access to Cisco IOS command-line interface (CLI) and configuration information; that is, a view can define what commands are accepted and what configuration information is visible. Thus, network administrators can exercise better control over access to Cisco Systems® networking devices.

Role-Based Access Supported by Cisco Router and Security Device Manger

The Cisco® Router and Security Device Manager (SDM) can create and delete four predefined views for Cisco SDM users: SDM_Administrator(root), SDM_Monitor, SDM_Firewall, and SDM_EasyVPN_Remote.

- SDM_Administrator(root)—A user associated to this view type has complete access to the Cisco SDM, and can perform all operations supported by the Cisco SDM.
- SDM_Monitor—A user associated to this view type can monitor all the features supported by the Cisco SDM, but cannot deliver configurations using the Cisco SDM. The user can navigate the various areas of Cisco SDM, such as the Interfaces and Connections, Firewall, and VPN features. However, the user interface components in these areas are disabled.
- SDM_Firewall—A user associated to this view type can use the Cisco SDM Firewall and Monitor features. The user can configure firewalls and access control lists (ACLs) using the Firewall wizard, Firewall Policy View, Inspect Rule Editor, and the ACL Editor. The user can associate or disassociate ACLs and Inspect rules from Interfaces and Connections; user interface components in other areas are disabled for this user.
- SDM_EasyVPN_Remote—A user associated to this view type can use the Cisco SDM Easy VPN Remote features. The user can create Easy VPN Remote connections and edit them. User interface components in other areas are disabled for this user.

A user associated to a user-defined view (or the Cisco SDM predefined view called "none") can invoke the Cisco SDM if the user-defined view contains the minimal set of commands required by the Cisco SDM. However, the Cisco

SDM maps the view to the SDM_Monitor view based on the commands available in the user-defined view, and the Cisco SDM is launched as read-only mode.

Deployment Scenario

In this scenario, create a security operator to configure a firewall and monitor routers.

Sample Configuration

Prerequisites

Before creating a view, ensure the following prerequisites are met:

- The "enable" password must exist.
- Authentication, authorization, and accounting (AAA) dependency—If the router runs a Cisco IOS Software release prior to Release 12.3(11)T, AAA must be enabled and authentication and authorization must be properly configured.
- To configure a view, the user must access the root view, which is available only to privilege-level 15 users.

CLI View Configuration

The sample configuration includes the configuration of the view (View_Security) for security operators and new user (secOP) creation; the prerequisites configurations are not covered in this sample configuration.

The CLI View configuration requires extensive knowledge of the Cisco IOS CLIs used to configure access rules, inspection rules, and show commands to display firewall rules, firewall status, router configuration, and router status.

Cisco SDM Role-Based Access

Cisco SDM facilitates role-based access by providing four predefined views; each view is named with its main operational commands and configuration capabilities, so you can easily associate a user to a view.

Deployment Scenarios

This document demonstrates how to configure a user associated to a view, how to edit a user associated to a view. Two users have been configured to associated with views, sdmadmin is associated to SDM_Administrator(root) with privilege level 1, sdmvpn is associated to SDM_EasyVPN_Remote with privilege level 15.

The scenarios include adding new user account sdmOP associated to SDM_Firewall with privilege level 1, and editing sdmvpn to have privilege level 1.

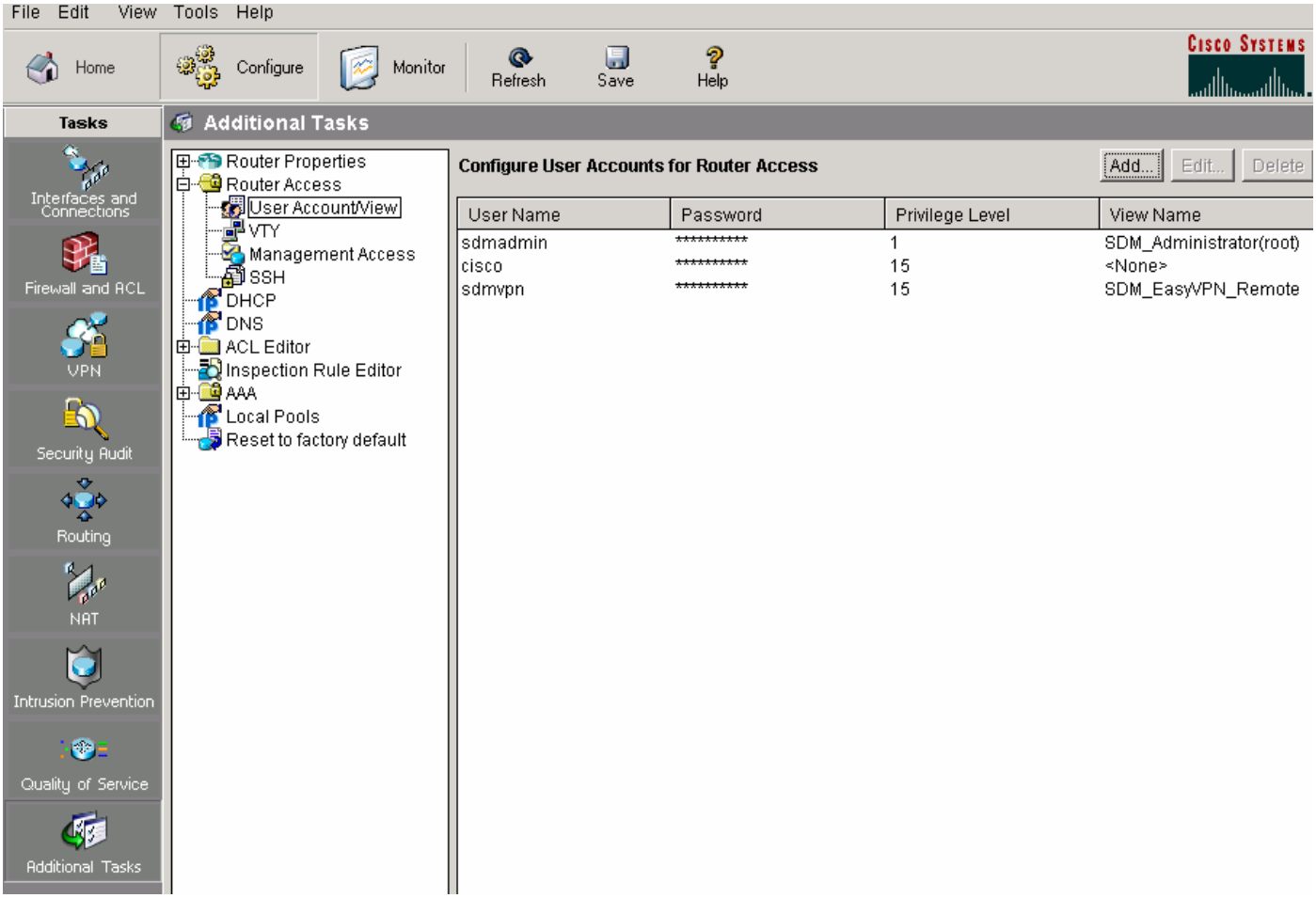
Configuring User Accounts and Associating the Users to Views

Launch the Cisco SDM as the privilege-level 15 user or a user associated to SDM_Administrator(root) to perform router access configuration[1]. In this scenario, log on as user sdmadmin.

At *Configure Mode*, select *Additional Tasks*, expand *Router Access*, and select *User Account/View* (Figure 1).

[1] If a user is not configured with a view, the Cisco SDM places the user in the privilege level. If a user is configured with a view as well as a privilege level in the user database, the view takes precedence over the privilege level.

Figure 1. Configure User Accounts for Router Access



Click *Add* to launch the *Add a Username* screen.

To configure a security operator (Figure 2), enter the following:

- The username is *secOP*.
- The password is *secOP123*.
- Check *Encrypt password using MD5 hash algorithm.*
- The privilege level is *1*.
- Check *Associate a view with the user.*
- The view name is *SDM_Firewall.*
- (Optional) Click *View Details…* to see the commands included in the view (Figure 3).
- Click *OK*.

Note: If you are associating a non-SDM_Administrator(root) view to any user for the first time, you will be prompted to enter the view password; in this scenario, the view password is *security123* (Figure 4). For associating the SDM_Administrator(root) to any user, the view password is requested only if the enable secret password is not configured on the router.

Figure 2. Add a Username

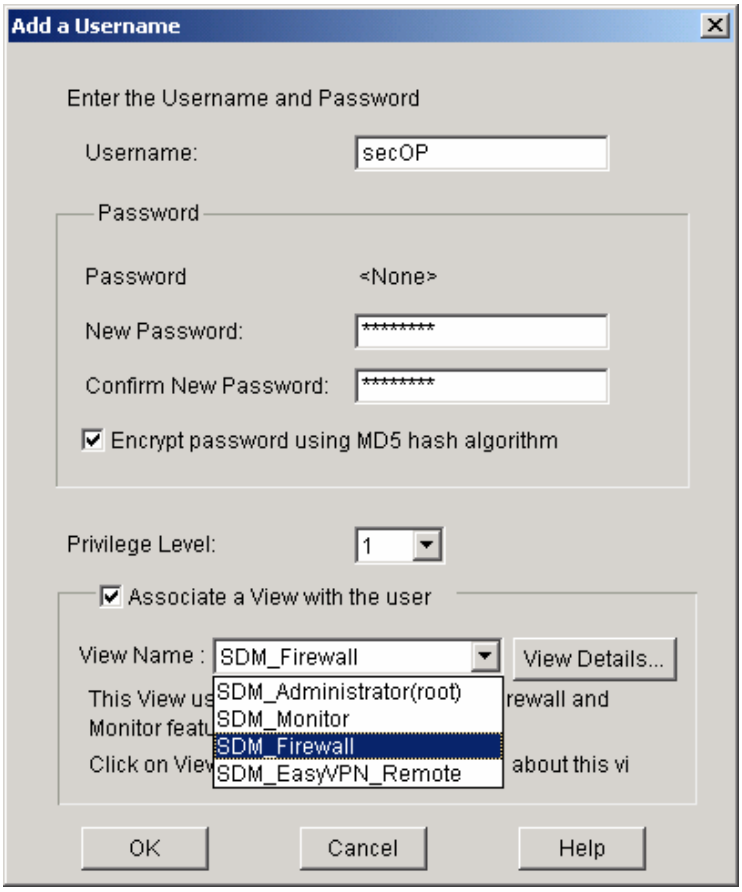


Figure 3. **View Details**

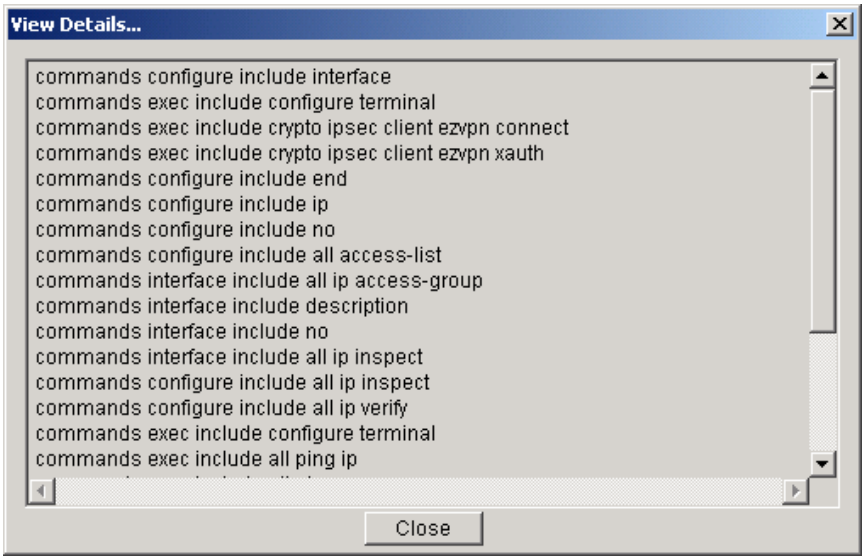
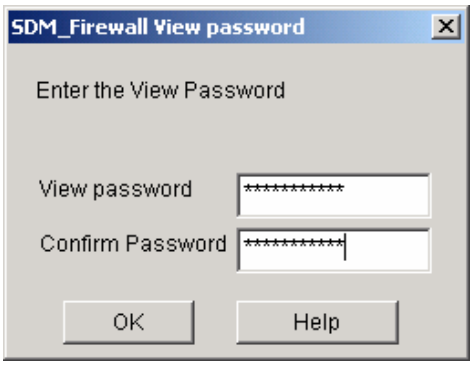


Figure 4. **View Password**

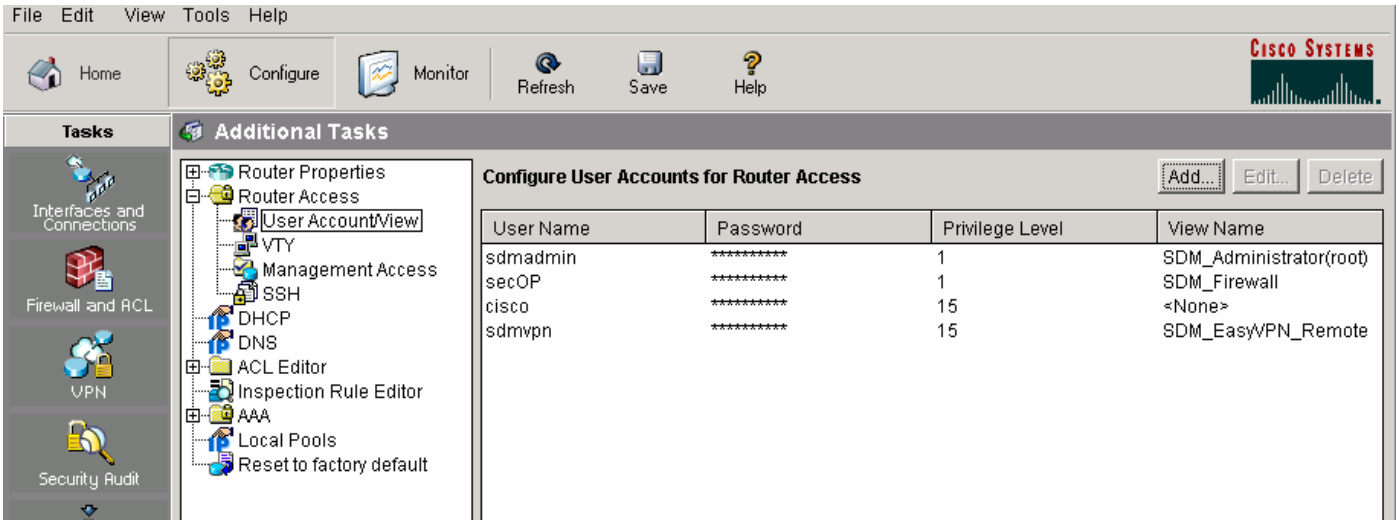


Click **OK** to deliver the configuration.

After finishing the task, go to *Configure Mode*, select *Additional Tasks*, expand *Router Access*, and select *User Account/View* (Figure 5).

The Cisco SDM creates a view, SDM_Firewall, and associates the new user, secOP, to the view.

Figure 5. User Account CLI View



Edit User Account

In this scenario, change the password and privilege level of user sdmvpn (Figure 6) from 15 to 1.

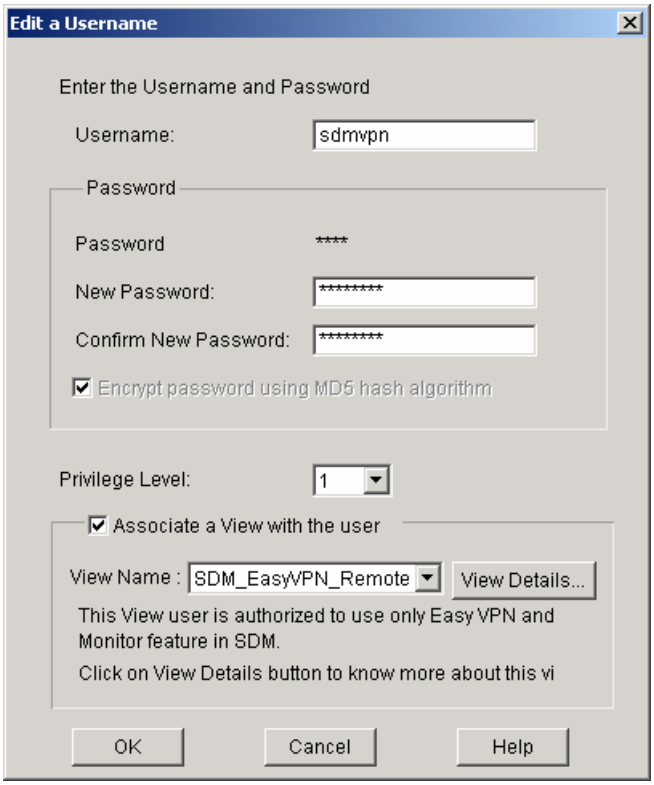
At *Configure Mode*, select *Additional Tasks*, expand *Router Access*, and select *User Account/View*.

To edit user *sdmvpn*, do the following:

- Select *sdmvpn.*
- Click *Edit;* the *Edit a Username* window pops up.
- The new password is *ilikesdm.*
- Enter *ilikesdm* again to confirm password.
- The privilege level is *1.*
- Click *OK.*

Note: If you are prompted with a Cisco SDM Warning message, look at the message, and click *Yes*.

Figure 6. Edit a Username



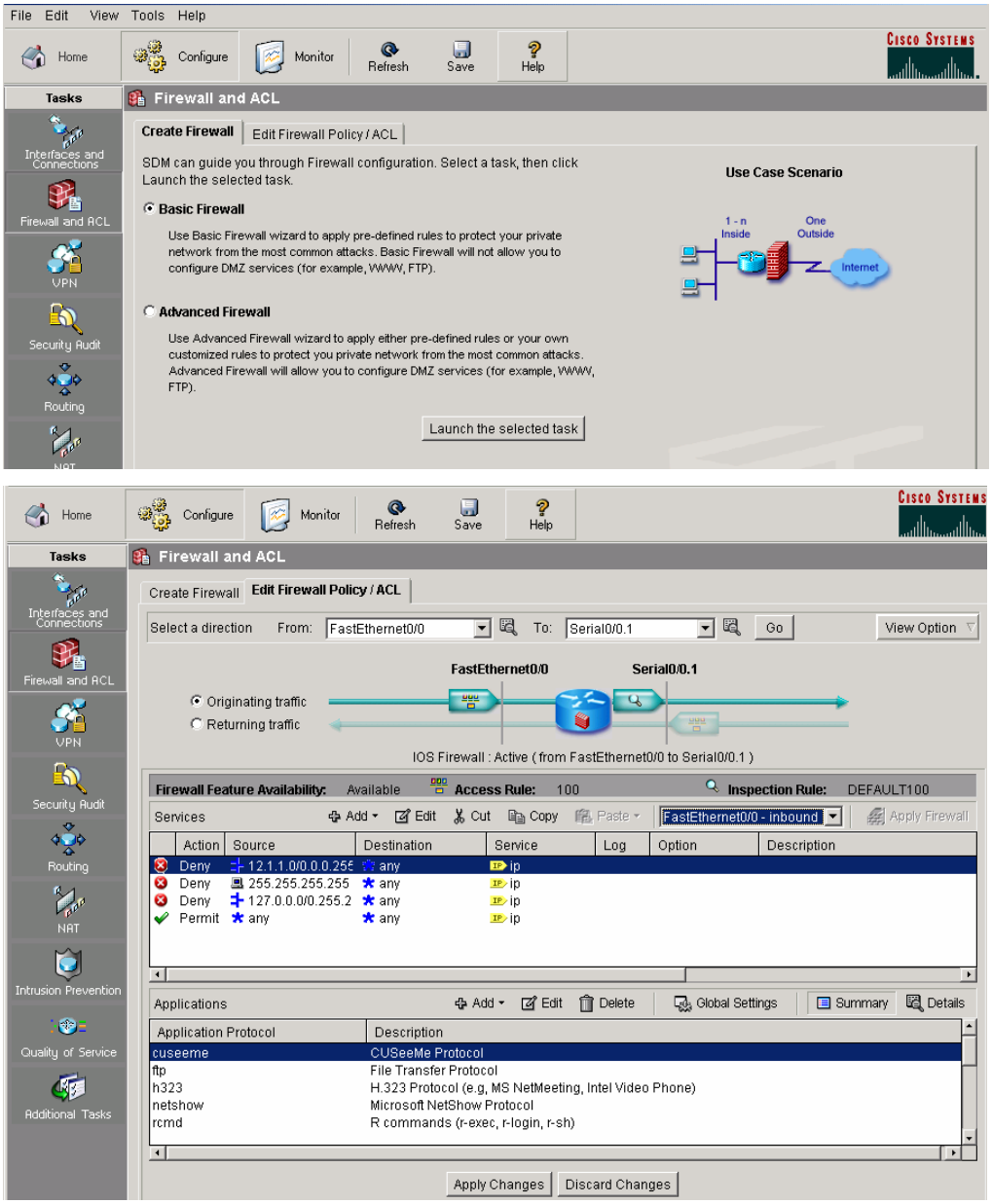
Verification

Log on as user *secOP*, who is allowed to configure firewall and monitor router configuration and status. On the bottom of the browser window, the status bar shows what view the user can access; in this scenario, you should see "Active View: see SDM_Firewall".

Configuration, Editing, and Monitoring

At the *Configure Mode/Firewall and ACL* screen, *Create Firewall* and *Edit Firewall Policy/ACL* (Figure 7) are enabled for secOP to configure a firewall.

Figure 7. Create Firewall and Edit Firewall Policy and ACL



At the *Configure Mode/Interfaces and Connections* screen, functions on *Create Connection* are disabled (Figure 8); all functions[2] are disabled (Figure 9) except Edit (Figure 10) on the *Edit Interface/Connection* screen [CORRECT?].

Figure 8. Create Connection

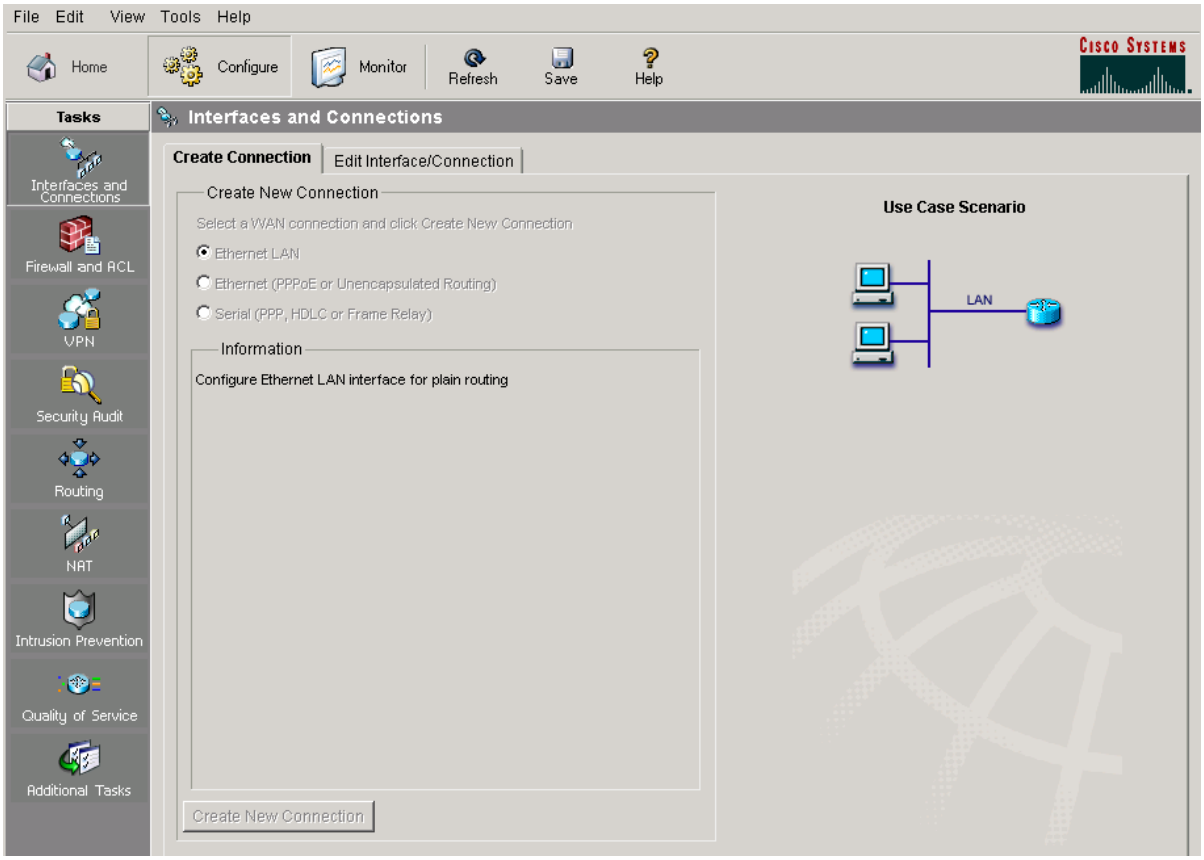
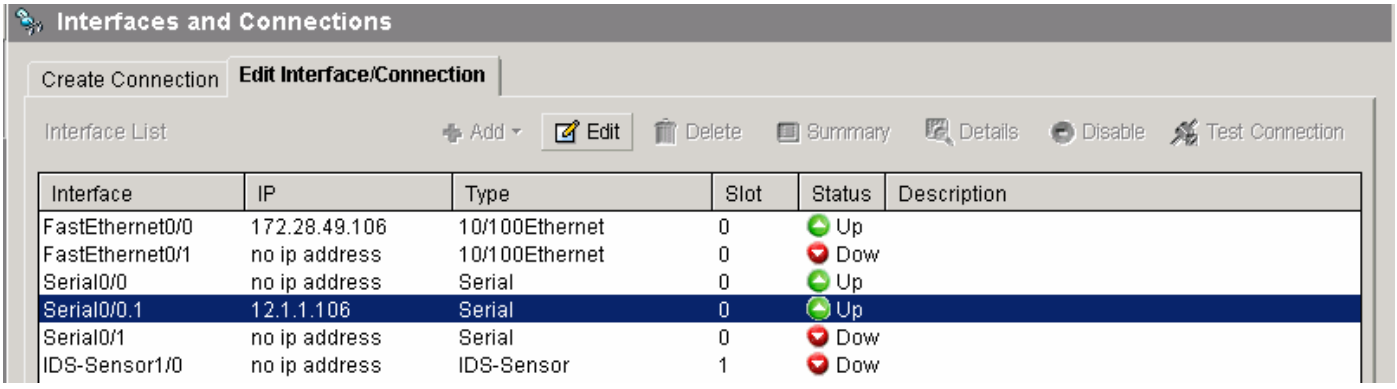


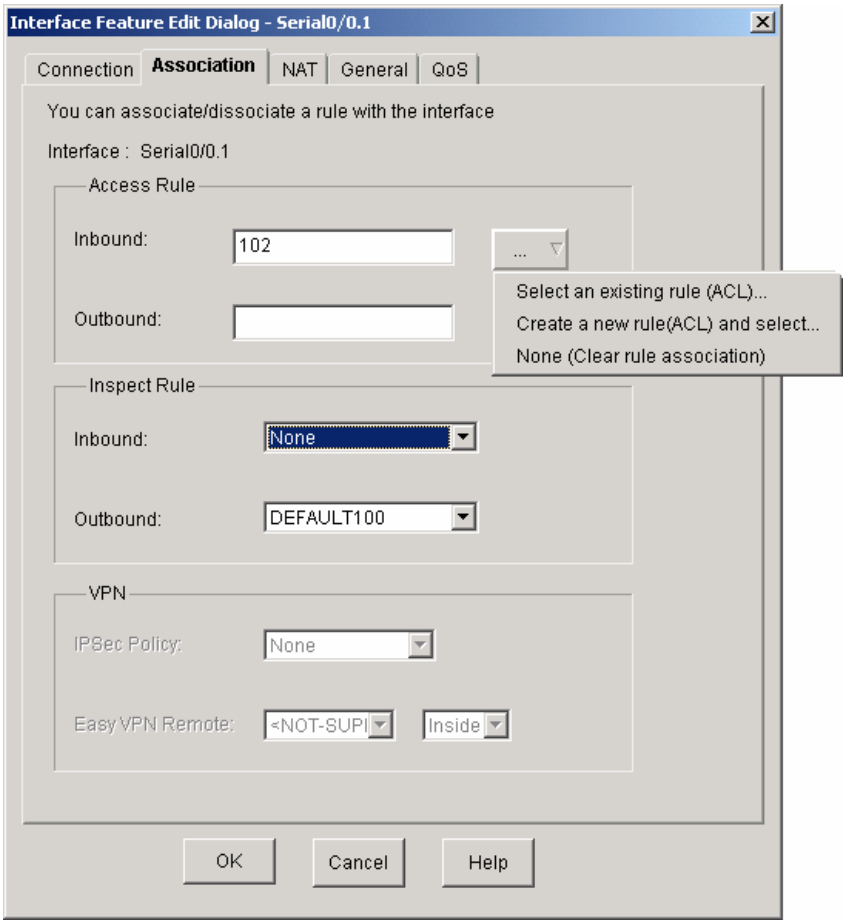
Figure 9. Edit Interface/Connection Screen



Users can associate and disassociate access rules and inspection rules to interfaces.

[2] The Edit button is not disabled; users can use it to display interface features; the interface editing capabilities are disabled.

Figure 10. Edit Interface/Connection -> Edit -> Association



In summary, by using the Cisco SDM, users can conduct the same Role-Based CLI Access configuration easily and quickly without a comprehensive knowledge of the Cisco IOS CLI.

References

- Role-based CLI access:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_7/gtclivws.pdf

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico• The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Printed in the USA