Miercom

Lab Testing Summary Report

December 2004
Report 041206

Product Category:

Router Configuration Software

Vendor Tested:

Cisco Systems

Product Tested:

Cisco Router and Security Device Manager v2.0

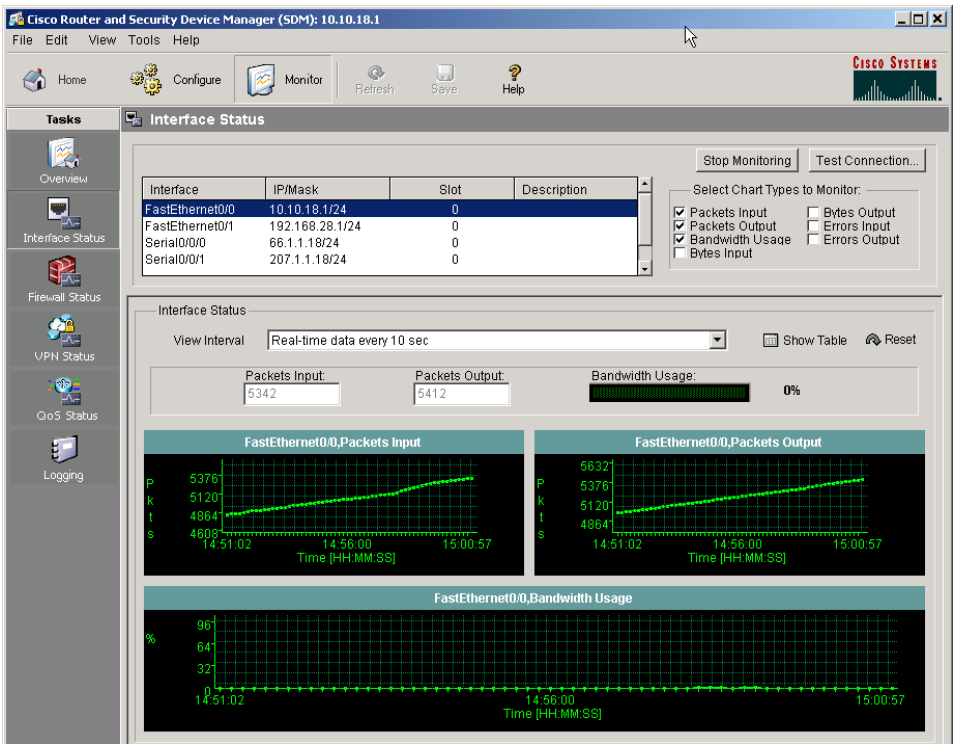
Miercom PERFORMANCE VERIFIED™

Key findings and conclusions:

- **Wizard-based tools greatly simplify complex security and configuration tasks: VPNs, IPS, QoS, Firewall and ACL settings**
- **Built-in intelligence in SDM uses the integration of WAN, routing, VPN, NAT, and Firewall technologies in the Cisco routers to avoid potential configuration problems**
- **Cisco SDM significantly reduces the technical and command line (CLI) expertise required to configure Cisco routers**
- **GUI-based configuration, monitoring and troubleshooting; features excellent on-line help**

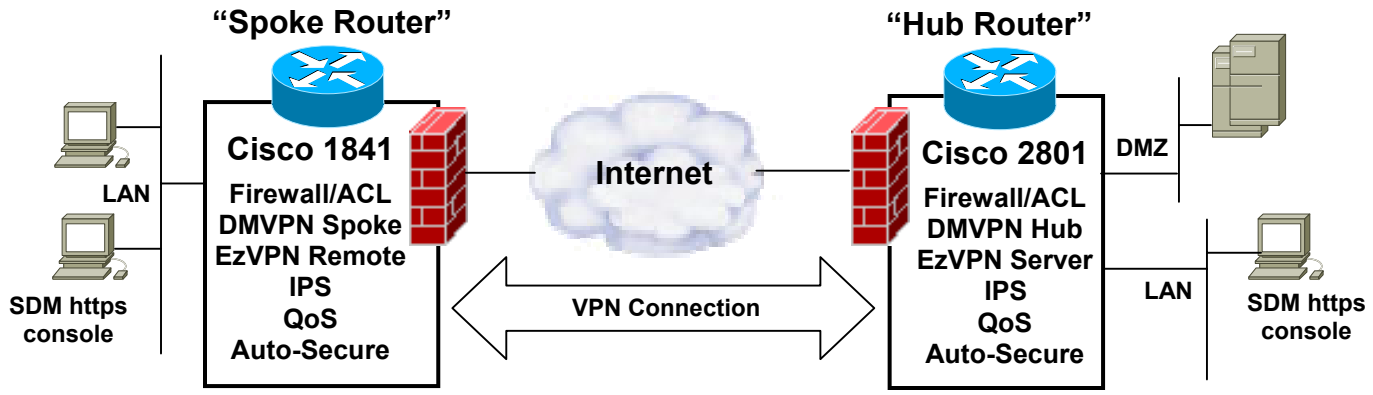
Cisco Systems engaged Miercom to independently assess the features and wizards of the Cisco Router and Security Device Manager (SDM) v2.0. This is a free software tool, which loads and runs on Cisco low-end to mid-range routers. On many current models, SDM comes factory installed.

Cisco's SDM product has evolved over the last few years into a fully capable router management application that not only provides a GUI



Monitoring traffic load and statistics can be done with SDM's Graphical User Interface. The user selects which interface and which statistics to monitor for that interface. Graphs are automatically updated.

Test Bed Setup



About the testing … Two routers were setup in the lab to demonstrate the initial configuration and subsequent configuration editing capabilities of SDM (v2.0). The test bed modeled a Hub Router Site and a Spoke Router Site interconnected by a simulated IP WAN/Internet link. We used the same test-bed set-up to exercise the configuration of two types of secure WAN connections: a DMVPN (Dynamic Multipoint VPN) connection and an "Easy VPN" WAN connection. Both the Cisco 1841 and Cisco 2801 routers were running IOS version 12.3(8)T5 with SDM v2.0. The SDM version we tested was pre-installed on these routers. The laptop we used for the SDM console was updated with a new Java 2 Runtime Environment (J2RE, SE v1.4.2).

interface for router security set-up and management, but also provides a GUI for complete router management – from initially putting the router in service, to managing the router over the long term. With SDM you're very likely to never have to type a single IOS CLI command. SDM involves only GUI screens, with plenty of help.

The SDM product is designed to work with routers in the Cisco 830, 1700, 1800, 2600XM, 2800, 3600, 3800, 7200 series and the 7301. The minimum IOS version varies by platform, but in most cases support starts at around version 12.2(13)T.

Router Deployment (Out of the box)

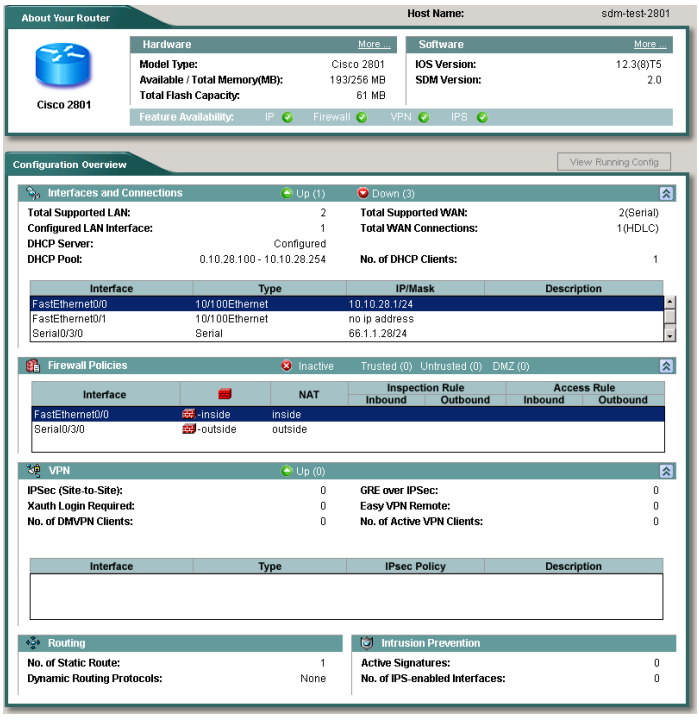
The test bed started with both the Cisco 1841 Router and the Cisco 2801 Router as factory shipped, with factory default initial configurations. The SDM Quick-Start Guide, a pamphlet shipped with the routers, was used. This provided very clear step-by-step instructions to connect our laptop as an SDM console (via https). The SDM console was connected to the router using the default (factory set) IP address.

SDM automatically uses SSHv2 for communication between the router and the PC. The initial connection wizard prompts you to enter basic router configuration like the router name, username, password, etc.

On finishing the Startup Wizard, SDM notifies us that the new configuration is being delivered to the router.

Interfaces and Connections

After finishing with the Startup Wizard and the user reconnects, SDM presents its "home" screen. The SDM home page has an intuitive dashboard view of all vital router services, hardware and software inventory. For additional



configuration updates, the home screen presents a task bar (down the left side of the screen) to the user. The user can select any one of the main tasks to be configured. These include: Interfaces and Connections, Firewalls/ACLs, VPN, Security Audit, Routing, NAT, IPS, QoS, and Additional Tasks. If the user selects a task item that has not yet been configured, SDM will invoke a Wizard to automatically guide the user through a set of screens, with questions and input fields, prompting the user for the necessary configuration information. After the Wizard has initially configured the facility, the user will be presented with an edit session, showing all the currently configured parameters.

For old-fashioned technical experts, we note that SDM does allow configuration changes to be made via the CLI. Where existing configurations, not generated by SDM, are used, SDM will make every attempt to read and interpret this configuration information and display it within the SDM user interface. SDM has some built-in facilities for working with the text-based (CLI-style) configuration files. For instance, there is a point-and-click facility to extract the configuration file from the router. This is well integrated with the SDM facility – you simply select the file name on your laptop to receive the configuration file and click "OK".

You can also set as one of your "preferences" the option to view Cisco IOS command lines being delivered to router. When this preference is set, the command lines are displayed as the last step in an update before the lines are delivered to the router.

Real-time network and router monitor

The SDM Monitor facility allows the network administrator to view a wide variety of key parameters both graphically and in tabular format. The Overview display gives a quick look at the router's overall status, showing bar-graphs for the current CPU and memory utilizations, the current count of Firewall attempts denied, VPN connections, application-level traffic analysis mapped to QoS policies and counts of event log severity levels.

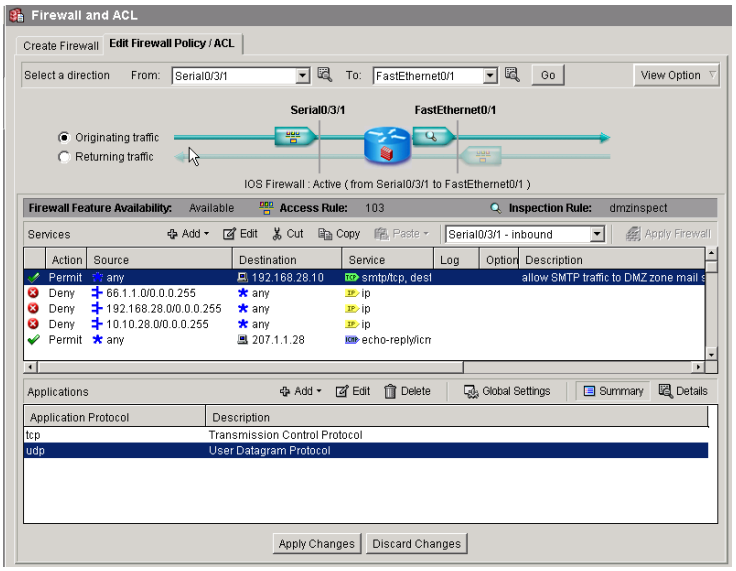
The monitoring screen shown on page 1 is an example of SDM's display on selecting "Interface Status." The display allows the user to specify a specific interface and display graphically various statistics on that interface, like bandwidth utilization or errors.

In addition to data displayed in the overview, the Monitor can also display more details about Firewall Status, VPN Status and QoS Status. In addition, details concerning the Event Log entries can also be displayed.

Firewall and ACLs

A key strength of SDM is its graphical interface for setting up Firewall Policies and the associated ACLs. Even for Cisco network pros, completely configuring Firewall policies across all interfaces is grueling and very tedious. SDM provides well thought-out interfaces to configure Firewall policies at a high level – and then SDM automatically generates the many configuration commands. The user is asked which interfaces are "inside" and "outside", and then can select a "default" policy or customize one.

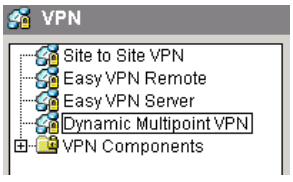
The Firewall/ACL policy editor is very powerful – giving a high-level view of each policy based on traffic flow. At the top of the screen you set the interfaces the Firewall is protecting, and below that you indicate whether the traffic is originating or returning on that interface. SDM then displays all the applicable ACLs in the window below. Then, any of these ACLs can be edited or new ones added.



VPN configuration

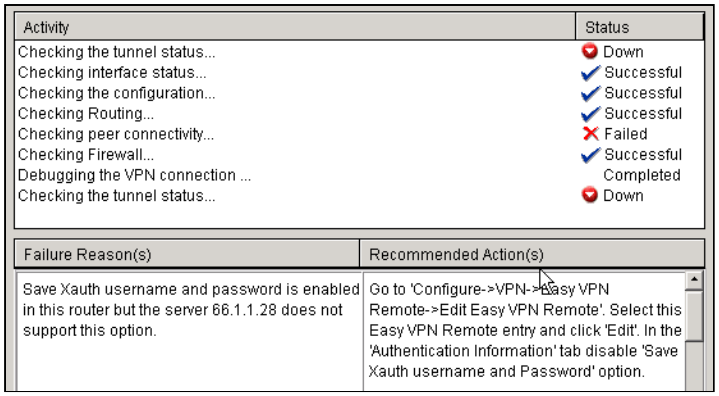
SDM offers wizard-based configuration of a wide variety of IPSec VPN topologies (hub, spoke, full mesh, dynamic site-to-site, dynamic routing based, etc.) and advanced security features like digital certificates. To help select the best technology, SDM offers graphical views of the VPN topologies and their use scenarios.

SDM has special features to assist in the setup and debug of VPN connections between Cisco routers. We used the configuration wizards to setup an Easy VPN Server (with Split Tunneling) and an Easy VPN Client. We also setup DMVPN (Dynamic Multipoint VPN) configurations (Hub and Spoke, as well as Fully Meshed, are supported). SDM guides you through DMVPN configuration with a multipoint GRE tunnel, pre-shared keys, IKE policies, IPSec transform set, and dynamic routing protocols. VPN wizards in SDM automatically picked the right set of default configuration values based on the hardware and software capabilities of the router. These wizards have built-in intelligence to determine the necessary firewall policies automatically to allow the IPSec traffic.



Troubleshooting

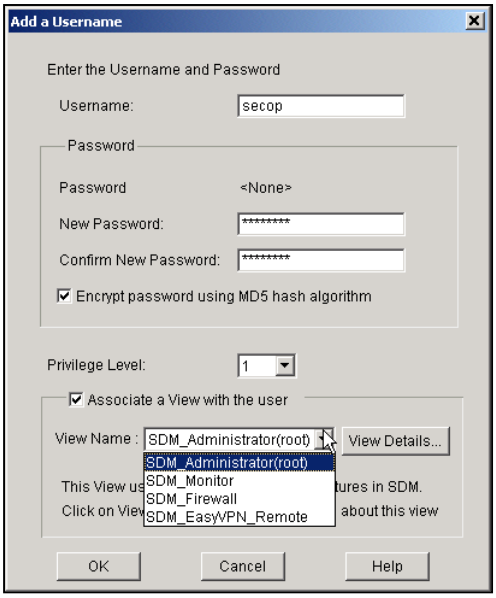
During our configuration of Easy VPN between the routers, the connection did not work successfully the first time. It turned out we had a configuration mismatch between the Easy VPN Server on the 2801, and the Easy VPN Client on the 1841. The troubleshooting facility, directly accessible from the link status display screen, showed that the link was down. The troubleshooting wizard ran automatically through a set of steps (see below) checking all aspects of the link, and correctly identified the problem. This feature can be a great time saver for network or security operators because it takes advantage of the integration of WAN access, routing, firewall, and VPNs to diagnose and recover from many VPN connection problems, from WAN link problems to IPSec remote peer configuration issues.



SDM's built-in intelligence (above) methodically checks the "Status" of the link, determines the "Failure Reasons" and provides "Recommended Actions".

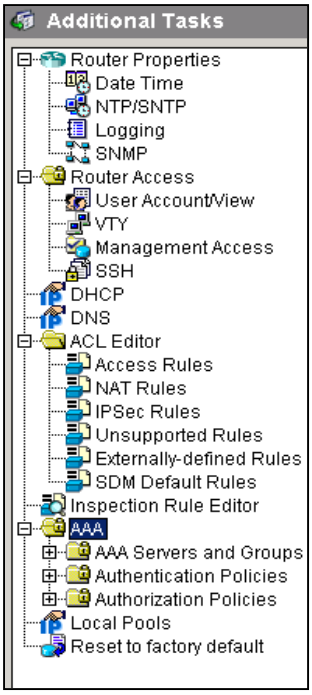
Role-based user access

Users can be defined to SDM with certain privileges and access profiles (views). This can be used to restrict the access of less experienced users. In SDM, the configuration capabilities outside the user's access profile appear "grayed-out". SDM ships with several predefined access profiles, like "Read-only" and "Firewall" views, which can benefit customers who need to restrict router configuration access.



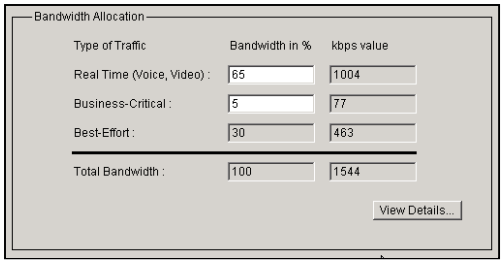
Additional Tasks

SDM groups a number of remaining router configuration items under the "Additional Tasks" button. These configuration tasks are presented here to allow the user to handle the configuration of remaining facilities, like SNMP, NTP, Router Management Access and others. The directory tree structure of these configuration items (see figure to the right) provides quick and easy access to the facilities that still need to be configured or modified.



QoS and NBAR

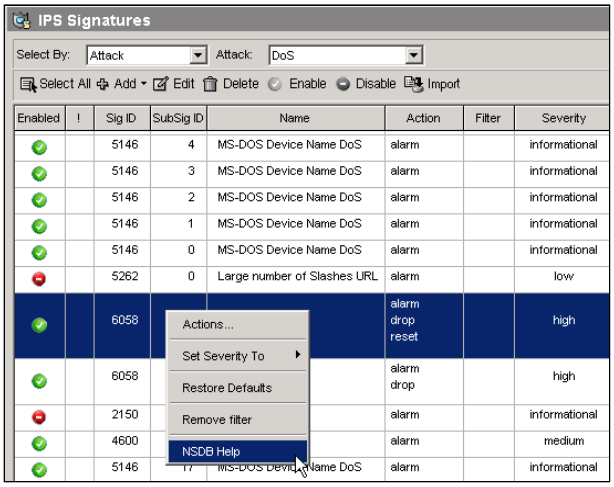
If your router needs to prioritize voice, video or other business critical traffic over WAN or VPN connections, you can select the "Quality of Service" task button. QoS can be used to enforce security practices and policies by prioritizing critical traffic like VoIP, routing protocols, SQL, and others over volumes of general web or email traffic. SDM's QoS setup wizard, carefully walks the user though the initial QoS policy setup with plenty of helpful explanations along the way. After you select the interface to apply the QoS policy, the wizard offers a spreadsheet-like input table where you can select the percentage of available bandwidth per QoS class (real time and business critical, best effort traffic is allocated to whatever bandwidth is remaining). We also used SDM to fine-tune the QoS policy for a couple of custom-created applications.



The NBAR (Network-Based Application Recognition) discovery feature tracks the bandwidth usage by application and is usually run on interfaces with QoS applied.

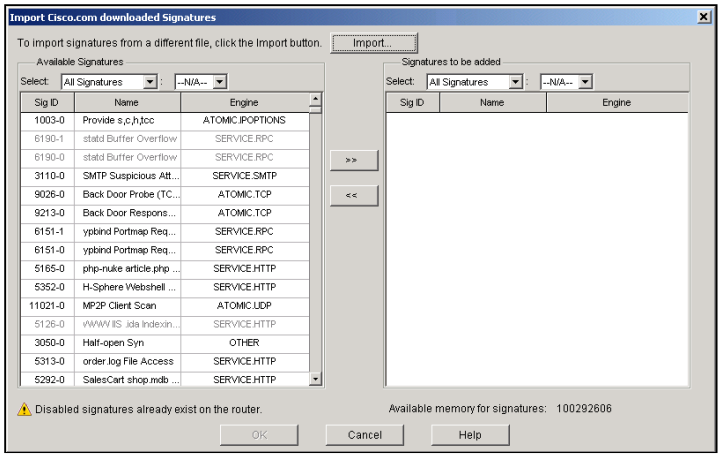
Intrusion Prevention System

The Cisco IOS IPS (Intrusion Prevention System) can be fully configured and maintained with SDM. IOS IPS is special software that runs on the router, that provides in-line, real-time protection against network attacks, looking for DoS, virus and worm packets. We downloaded 758 signatures from the Cisco Secure Software website. The signatures are pre-assigned as "enabled" or "disabled" and also a recommended "action" and "severity". The user can accept these or edit any of the signatures by category and attack type so that they can quickly apply mass configuration changes (like drop packet and alarm) for all the selected signatures.



For any signature, a user can directly access Cisco's Network Security Database (NSDB) on the web to determine if the signature is applicable to their particular network environment or change parameters such as the "severity", or "actions".

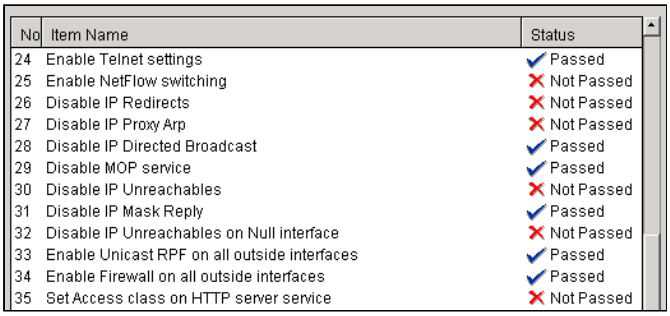
New signatures can be downloaded from the Cisco Website. Once the new signature file is downloaded, the user can decide how to apply it. SDM builds a display showing which signatures are already loaded ("grayed-out") and those available to be loaded. Cisco routers in a large enterprise network can be configured to pick the latest signature files from a centrally located TFTP or HTTP server.



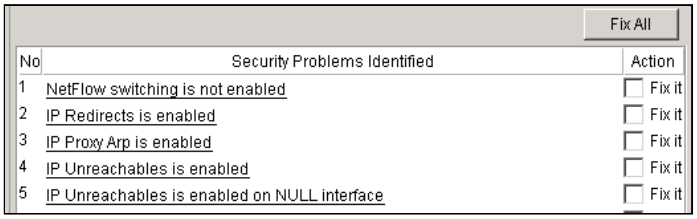
Security Audit

SDM includes a feature called "One-Step Lockdown", that can automatically enable router security based on a set of default configuration parameters. This is a one-keystroke function that configures the overall security parameters of the router and disables certain system processes and services, eliminating potential network security threats.

After configuring your firewalls and VPNs you can run the "Security Audit" task. This assesses all the security-related configuration parameters and checks them against Cisco recommendations for assuring a secure network. The audit incorporates recommendations from NSA, ICSA Labs and the Cisco TAC. Each potential exposure is highlighted and the user can select any of these and simply tell SDM to "Fix it", and the configuration will be updated.

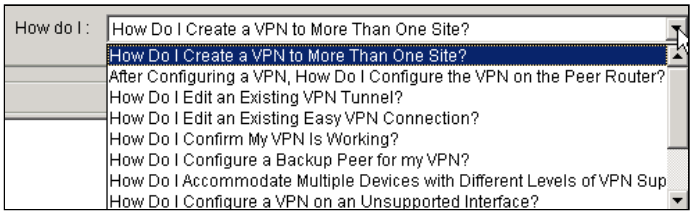


Below is a portion of the display screen where the user can select the Security Problem that he would like to fix. The user clicks the checkbox on the right, or clicks "Fix All" at the top. The "Fix All" button allows non-expert users to auto-secure the router with a single click.



Help

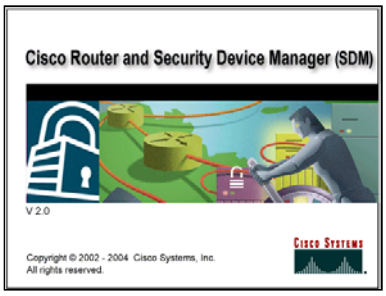
To help less experienced staff handle router configurations, detailed explanations are provided on SDM's wizard screens, prompting the user for input. Context sensitive help for all screens is also provided. All the help is located in the SDM module residing on the router; you don't need to have Web access to view help pages. In addition, there is also a "How Do I" Q&A facility at the bottom of many screens.



Miercom Performance Verified

Based on Miercom's examination of SDM's Features and Wizards, as described herein, Miercom hereby attests to these findings:

- Wizard-based tools greatly simplify complex security and configuration tasks: e.g., VPNs, IPS, Firewall and ACL settings
- Built-in intelligence in SDM uses the integration of WAN, routing, VPN, NAT, and Firewall technologies in the Cisco routers to avoid potential configuration problems
- Cisco Router and Security Device Manager significantly reduces technical expertise required to configure Cisco routers
- Virtually eliminates the need to know Cisco's command structure
- GUI-based configuration, monitoring and troubleshooting, features excellent on-line help and tutorials
- Software tool works with broad range of Cisco routers, and Cisco IOS releases



Cisco Router and
Security Device Manager

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

About Miercom's Product Testing Services…

With hundreds of its product-comparison analyses published over the years in such leading network trade periodicals as *Business Communications Review* and *Network World*, Miercom's reputation as the leading, independent product test center is unquestioned. Founded in 1988, the company has pioneered the comparative assessment of networking hardware and software, having developed methodologies for testing products from SAN switches to VoIP gateways and IP PBX's. Miercom's private test services include competitive product analyses, as well as individual product evaluations. Products submitted for review are typically evaluated under the "Net**WORKS** As Advertised™" program, in which networking-related products must endure a comprehensive, independent assessment of the products' usability and performance. Products that meet the appropriate criteria and performance levels receive the "Net**WORKS** As Advertised™" award and Miercom Labs' testimonial endorsement.

379 Princeton-Hightstown Rd., East Windsor, NJ 08512
609-490-0200 ● fax 609-490-0610 ● www.miercom.com

Report 041206