VPN Network Management Tools

This chapter discusses select Cisco VPN network management software. Each section discusses the particular environments in which the network management tool is applicable.

This chapter includes the following sections:

- Cisco Secure Policy Manager, page 5-1
- Cisco VPN/Security Management Solution, page 5-2
- IPSec MIB and Third Party Monitoring Applications, page 5-3
- Cisco VPN Device Manager, page 5-3

Cisco Secure Policy Manager

Cisco Secure Policy Manager (CSPM) should be used for multi-device, multi-platform VPN, firewall, and IDS (Intrusion Detection System) configuration.

CSPM is a multi-device policy-based management tool for Cisco security products, including PIX Firewalls, the Cisco IOS firewall feature set, Cisco 7200 series router, and Intrusion Detection System (IDS) Sensors. CSPM allows these security devices to be configured and managed with an easy-to-use graphical user interface (GUI). CSPM simplifies the configuration of complex VPN and security devices by creating each device configuration file after the security policies have been defined. CSPM also distributes each device configuration in a secure fashion with IPSec. CSPM allows security devices to be configured from a central location. CSPM also provides other management services including monitoring, notification, and reporting.

CSPM increases the scalability of VPN and security networks by centralizing the management of all devices within a network. CSPM facilitates the deployment of remote VPN devices and firewalls including colocated DSL and Cable Modem users. IPSec templates are included in CSPM for both meshed and hub-and-spoke networks. CSPM adds value in any security networking environment by simplifying small security networks, multi-site enterprise deployments and large service provider environments by centralizing and abstracting the management of security networks.

See the *Cisco Secure Policy Manager* for more information.
Cisco VPN/Security Management Solution

The Cisco VPN/Security Management Solution should be used to implement comprehensive, multi-device VPN configuration and monitoring, firewall configuration, and infrastructure management.

The Cisco VPN/Security Management Solution provides key functionality to assist customers who are deploying Cisco 7200 series routers and who require monitoring of remote access and site-to-site VPNs, based upon IPSec, L2TP, and PPTP. The solution also provides key features for deployment and management of perimeter security using the Cisco PIX Firewall.

Note

The term ‘Cisco 7200 series router’ in this Guide implies that an Integrated Service Adaptor (ISA) or a VAM (VAM, VAM2, or VAM2+) is installed in the Cisco 7200 series router.

The following modules are included in the Cisco VPN/Security Management Solution. Together, these modules provide essential VPN and security management capabilities:

- Cisco Secure Policy Manager Lite (CSPM-Lite)—Provides policies for defining VPN policies on Cisco 7200 series routers and PIX Firewalls. CSPM also defines security policies on Cisco PIX Firewalls, and reporting and notifying of intrusions when Cisco Intrusion Detection Sensors technology is deployed.

- Cisco VPN Monitor is a web-based management tool that allows network administrators to collect, store, and report information on L2TP, PPTP remote access, and IPSec-based site-to-site VPNs configured on the Cisco 7200 series routers, Cisco 3600 series routers, Cisco 2600 series routers, Cisco 1700 series routers, Cisco 800 series routers, and Cisco VPN 3000 Concentrator Series. Multiple devices can be viewed from an easy-to-use dashboard configured on a web browser. After the dashboard is configured, Cisco VPN Monitor continuously collects data from the devices it manages over a rolling seven-day window. Operational status, performance, and security information can be viewed at a glance, providing status information on IPsec VPN implementations.

Note

The Cisco VPN Monitor does not support PIX Firewalls. For information on monitoring PIX Firewalls, see the PIX Firewall System Management documentation.

- Resource Manager Essentials (RME)—Provides the operational management features required by enterprises. RME features include software distribution, change audit and authorization, device inventory and credentials management and Syslog analysis for problem solving and notification of VPN and security operational problems.

- CiscoWorks2000 Inventory Services (CD Two) — Cisco VPN/Security Management Solution provides an installation option for customers who want to install only the inventory administration tools of RME. Inventory Services tracks the network devices, and reports hardware and software characteristics, and provides device credentials management.

- CiscoView—Provides administrators with browser access to real-time device status, and operational and configuration functions. CiscoView is the most widely used Cisco graphical device management application and is now web-based.

- CiscoWorks2000 Management Server (CD-One)—Provides the common database, web, and desktop services used to integrate with other Cisco and third-party tools.

See the following websites for further information:

- Update for CiscoWorks VPN/Security Management Solution 2.1
- CiscoWorks VPN/Security Management Solution
IPSec MIB and Third Party Monitoring Applications

The IPSec MIB feature allows users to configure and monitor their IPSec MIB tunnel tables and their trap notifications using Simple Network Management Protocol (SNMP). IPSec MIB can increase the performance of your Cisco VPN, as trap notifications can be sent only once and are discarded as soon as they are sent. This reduces traffic and creates lower overhead on your network. This feature allows users to specify the desired size of a tunnel history table or a tunnel failure table. The history table archives attribute and statistic information about the tunnel; the failure table archives tunnel failure reasons along with the time failure occurred. A failure history table can be used as a simple method to distinguish between a normal and an abnormal tunnel termination. That is, if a tunnel entry in the tunnel history table has no associated failure record, the tunnel must have terminated normally. However, a tunnel history table does not accompany every failure table because every failure does not correspond to a tunnel. Thus, supported setup failures are recorded in the failure table, but an associated history table is not recorded because a tunnel was never set up.

This feature also allows a router to send IPSec trap notifications, which are MIB related, to a random or specified host. A trap notification may be sent when a particular event, such as an error, occurs.

Note

The traps are not supported in the current version of the MIB. They only pertain to the Cisco IOS-specific IPSec MIB.

The IPSec MIB feature is used in conjunction with an SNMP agent, which is based on Version 1 of the SNMP protocol. The SNMP agent implements the IPSec MIB subsystem, which implements the MIBs referred to in the "Supported Standards, MIBs, and RFCs" section of this feature module. By allowing the user to adjust tunnel tables and enable IPSec trap notifications, the IPSec MIB feature provides enhancements to the SNMP agent process.

See IPSec—SNMP Support for more information on IPSec MIB.

Cisco VPN Device Manager

This section provides an overview of Cisco VPN Device Manager (VDM). VDM is a wizard-based GUI application that allows simplified VPN configuration of the device on which it resides.

This section includes the following topics:

- VDM Overview
- Installing and Running VDM
- Using VDM to Configure VPNs
- Using VDM to Monitor VPNs
- Using VDM to Troubleshoot Connectivity
- Related Documents
VDM Overview

VDM enables network administrators to manage and configure site-to-site VPNs on a single IOS VPN device from a web browser, and view the effects of their changes in real time. VDM implements a wizard-based GUI to simplify the process of configuring site-to-site VPNs using the IPSec protocol.

VDM software is installed directly on Cisco VPN devices. It is designed for use and compatibility with other device manager products.

Note

VDM supports site-to-site VPNs but not remote-client access VPNs.

Figure 5-1 shows the VDM Home Page page under the System menu. This is the first window to appear after you launch VDM and is the starting point for all other VDM activities.

The following other options are also available from the System menu:

- IOS Config—displays device Cisco IOS configuration information
- Log—displays messages about VDM activity

Figure 5-1  VDM Home Page

<table>
<thead>
<tr>
<th>Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Application menu bar</td>
</tr>
<tr>
<td>2</td>
<td>Application-specific primary menu bar</td>
</tr>
<tr>
<td>3</td>
<td>Application-specific secondary menu bar</td>
</tr>
<tr>
<td>4</td>
<td>Application status bar</td>
</tr>
<tr>
<td>between 3 and 4</td>
<td>Application content area</td>
</tr>
</tbody>
</table>
Using a browser, you can log into a Cisco device and use VDM to efficiently configure VPNs on it. You can set particular tunneling, encryption, and other VPN options, which can then be applied to the interfaces facing peer devices. Use VDM to conveniently troubleshoot specific problems and perform configuration updates and changes.

Cisco IOS Commands

You must configure some Cisco IOS CLI commands before VDM becomes fully operational. Details about these commands can be found in the Cisco IOS feature document *VPN Device Manager*.

Benefits

This section contains information about the following benefits of using VDM:

- Configuration Wizards
- Single Device Configuration
- Monitoring Functions
- Convenient Navigation
- No Client Installation

Configuration Wizards

Browser-based VDM wizards help you perform ordinarily complex setup operations including:

- Step-by-step instructional panes for simplified VPN configuration, such as peer-to-peer setup.
- Tunneling and encryption support using transform sets, key lifetimes, IKE policies, security association (SA) lifetime, authentication policies, error reports, and performance monitoring.

Single Device Configuration

VDM configures only the device from which it is launched. It does not read or write configuration information to or from other devices.

Monitoring Functions

Monitored data in graphs and charts contains basic device information, a VPN report card, top-ten lists, and detailed views of user-specified tunnels that monitor duration, errors, and throughput.

Convenient Navigation

The following navigation methods ensure that you can conveniently identify your current location within each wizard:

- Cascading highlighted menu tabs at the top of the GUI.
- A step-by-step tasks list in each wizard's left frame contains a highlighted bar which moves down the list as you progress through that wizard.

No Client Installation

VDM is distributed in the following two components:

- Crypto-enabled Cisco IOS image containing the necessary VPN subsystems.
- File to be installed on the Cisco IOS Flash memory file system.
Installing and Running VDM

You can install the VDM client on your Cisco device in the following ways:

- Order the device with VDM installed (if the device is ordered new).
- Install a Cisco IOS version that VDM supports and upload the VDM client to the device Flash memory.

VDM supports crypto-enabled IOS images. See *VPN Device Manager - Release and Installation Notes* for further information on obtaining the correct Cisco IOS image.

To simplify its use, VDM starts as a GUI into a web-browser home page that is run from the managed device (VPN device on which VDM is installed) at connection time. VDM is a Java application that uses continuous XML data exchange to update the appropriate part of the VDM GUI.

The VDM GUI contains step-by-step configuration wizards for common VPN setups, interfaces, and policies and protocols, including:

- IPSec tunnels
- Pre-shared keys and Internet Key Exchange (IKE) policies

---
**Note**

VDM does not work with RSA-encrypted nonces. (Nonces are random numbers or keys that are generated once and not reused.)
Using VDM to Configure VPNs

VDM configuration wizards make it easier to perform ordinarily complex setup operations and configure VPN connections.

Table 5-1 describes the following VDM browser-based configuration wizards:

<table>
<thead>
<tr>
<th>Wizard</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificates</td>
<td>Starts the Certificates wizard, which allows you to enroll the device with a certificate authority and use digital certificates for authenticating peers.</td>
</tr>
<tr>
<td>Connections</td>
<td>Starts the Connections wizard, which creates VPN protected connections for selected traffic between selected local and remote hosts and subnets.</td>
</tr>
<tr>
<td>IKE</td>
<td>Starts the IKE wizard, which allows you to create IKE policies that determine how IKE establishes SAs with peers.</td>
</tr>
<tr>
<td>Peer Keys</td>
<td>Starts the Peer Keys wizard, which assigns and edits pre-shared keys, used to authenticate peers.</td>
</tr>
<tr>
<td>Transforms</td>
<td>Starts the Transforms wizard, which creates transform sets to authenticate, encrypt, and compress VPN traffic.</td>
</tr>
<tr>
<td>VLANs</td>
<td>Starts the VLANs wizard, which allows you to create access and interface VLANs on the device.</td>
</tr>
</tbody>
</table>

These configuration wizards contain:

- Simple step-by-step instructions for configuring simple VPNs.
- Tunneling and encryption support using transforms sets, key lifetimes, IKE policies, SA lifetime, authentication policies, error reports, and performance monitoring.

The wizard navigation buttons within the VDM Configure menu allow for flexible multi-directional navigation. The wizard configuration action buttons within the same menu allow you to create or modify your VPN settings conveniently.
Figure 5-3 shows the **Connections** page for the VDM Connections wizard. This wizard allows you to add, edit, or remove VPN connections. The **Select a Connection** list displays existing connections.

The **Connection Description** list provides the following details about the selected connection:

- IP addresses of peers
- Local and remote hosts and subnets
- Protocols
- Transforms
- The interface VLAN that acts as the inside interface to a IPSec VPN Acceleration Serviced Module (only on devices that contain this module)
- Interface(s) to which the connection is applied

---

**Figure 5-3  VDM Connections Wizard Overview Page**

![Connections wizard overview](image.png)
Figure 5-4 shows the **Certificates** page for the VDM Certificates wizard. This wizard allows you to enroll a certificate identity with the Certificate Authority (CA) by using the Certificate Enrollment wizard, as well as add, edit, and remove existing certificate identities.

The **Select a Certificate Identity** list displays existing certificate identities. The **Certificate Identity Description** list provides the following details about the selected certificate identity, such as:

- Enrolled URL
- Proxy host and port
- Retry specifics

![VDM Certificates Wizard Overview Page](image)
Figure 5-5 shows the IKE Overview page for the VDM IKE wizard. This wizard allows you to add, edit, or remove IKE policies.

The Select a Policy list displays existing user-configured policies, as well as one global and one default IKE policy. The Policy Description list provides the following details about the policy selected:

- Encryption and hash algorithms
- Authentication method
- SA specifics

Figure 5-5  VDM IKE Wizard Overview Page

Using VDM to Monitor VPNs

VDM monitors general system statistics and VPN-specific information such as tunnel throughput and errors. You can configure VPNs in parallel, while monitoring is automatically updated based upon a selected polling interval. The graphing capability allows you to compare such parameters as traffic volume, tunnel counts, and system utilization.
Figure 5-6 shows the VDM Charts page with the CPU Utilization chart selected. You can generate many charts from this page based on your charting object and charting object attribute selections.

The left list displays all objects with attributes that can be charted, such as CPU, IKE, IPSec, and a variety of interfaces. The right list displays all object attributes associated with a selected object.

You must first select an object attribute to generate a chart. For example, under the IPSec object, you have a choice of the following three different object attributes:

- Tunnels
- Total throughput
- Total crypto throughput

Available object attributes vary according to the selected object. For example, chartable object attributes for the Interface object include the following:

- In and out packets
- Dropped packets
- Octets
- Errors

You can customize charts to display both historical and real-time data from periods as short as 10 minutes to as much as 5 days.

Figure 5-6  VDM Charts Page with CPU Utilization Chart
Figure 5-7 shows the **VDM Report Card** page, which displays information about the following activity on the device:

- Total throughput
- Crypto throughput and failures
- IKE and IPSec Tunnels
- Replayed Packets

**Figure 5-7  VDM Report Card Page**
Figure 5-8 shows the **VDM Top-Ten Lists** page, which displays details about IKE and IPSec tunnels by duration, errors, and traffic volume. You can select any of these reports from the drop-down list.

A top-ten list is a list of 10 tunnels on the device that rank highest when measured by particular criteria. For example, you can view a list of the 10 IKE tunnels on the device that have the highest traffic volume.

Each top-ten list displays information about the following:

- Monitored tunnels
- Tunnel source devices
- Peers
- Transmitted packets and bytes
- SA details

**Figure 5-8  VDM Top-Ten Lists Page**
Using VDM to Troubleshoot Connectivity

VDM allows you to test device connectivity using two different methods—traceroute or ping. Figure 5-9 shows the VDM Test Connectivity page executing the ping command. These options function the same way as executing these commands from the CLI.

Figure 5-9  VDM Test Connectivity Page

Related Documents

Further information on VDM can be found in the following related documents:

- **VPN Device Manager** Cisco IOS feature document
- **Installation and Release Notes for VPN Device Manager**
- **VPN Device Manager Online Help**

For additional information, see the Cisco VPN Device Manager (VDM).