

CiscoWorks **VPN/Security Management** Solution

Version 2.2

CiscoWorks VPN/Security Management Solution (VMS) is the flagship integrated security management solution from Cisco, and is an integral part of the SAFE Blueprint from Cisco for network security.

CiscoWorks VMS protects the productivity of enterprises, by combining Web-based tools for configuring, monitoring, and troubleshooting enterprise VPNs, firewalls, and network and host-based intrusion detection systems (IDS). CiscoWorks VMS delivers the industry's first robust and scalable foundation and feature set that addresses the needs of small and large-scale VPN and security deployments.

Today's business challenges and resulting security deployments require more scalability than merely supporting a large number of devices. Many customers have limited staffing, yet are asked to manage a myriad of security devices. These customers must manage the security and network infrastructure; frequently update many remote devices; implement change control and auditing when multiple organizations are involved in defining and deploying policies; enhance security without adding more headcount; or roll out remote access VPNs to all employees and monitor the VPN service.

CiscoWorks VMS enables customers to deploy security infrastructures from a small to large environment, using the following multifaceted scalability features:

- **Complete SAFE Blueprint Coverage**

To completely manage a SAFE environment, a network management solution must manage SAFE infrastructure components, support features based upon an appliance or Cisco IOS® Software, and support a range of management functions. CiscoWorks VMS is uniquely able to scale across SAFE Blueprint components, including firewalls, VPNs, and network- and host-based IDSs. CiscoWorks VMS also takes advantage of Cisco Secure Access Control Server (ACS) by using a common ACS logon. CiscoWorks VMS can manage a feature set through an appliance, for example, the Cisco PIX® Firewall, or through the Cisco IOS Software. Scalable management also involves more than configuring devices. CiscoWorks VMS provides the complete range of management with features to configure, monitor, and troubleshoot the network.

- **Scalable Foundation**

CiscoWorks VMS implements a foundation with a consistent user experience, which makes it easier to scale management to many devices. CiscoWorks VMS provides users with a consistent GUI, workflow, ACS logon, roles definition, platforms, database engine, installation, and more. An industry-leading feature of this foundation is the Auto Update feature, which allows numerous devices to be



updated easily and quickly. Auto Update enables devices, even remote and dynamically addressed devices, to periodically "call home" to an update server and "pull" the most current security configurations or Cisco PIX operating system. Auto Update is required to effectively scale remote office firewall deployments across intermittent links or dynamic addresses. Prior policy updating methods relied on a "push" model. Although this model works for known devices, it does not work for remote devices with unknown addresses or devices that are not always active. Without Auto Update a more manual process is required to update each remote device. The Auto Update feature provides a dramatic scalability improvement for organizations that want to deploy devices with many remote and local locations. In addition to easier and faster policy updates, Auto Update also provides consistent policy deployments.

- **Enterprise Operational Integration**

CiscoWorks VMS enables organizations to easily integrate management into their operations. One operational need is to replicate policies to multiple locations. The Smart Rules hierarchy addresses this need, by enabling administrators to define device groups and implement policy inheritance. For example, an administrator can define a device group for the New York sales office and deploy that same policy to all other sales offices quickly and consistently. The Command and Control Workflow feature provides change control and auditing, and is particularly important for customers who have separate groups for network and security operations. The solution includes processes for generating, approving, and deploying configurations. This can help security operations to define and approve new policies. Network operations can later deploy the new policies during their regular maintenance window. An audit of the changes can be maintained.

- **Centralized Role-Based Access Control (RBAC)**

Role-based access control enables organizations to scale access privileges. CiscoWorks VMS conveniently uses a common ACS logon for users, administrators, devices, and applications. CiscoWorks VMS enables different groups to have different access rights across different devices and applications.

- **Integrated Infrastructure Management**

Scalability requires that multiple components be managed, not just firewalls, but also VPNs, network- and host-based IDSs, routers, and switches. CiscoWorks VMS not only manages the security infrastructure, but also manages the network infrastructure. Customers benefit from being able to manage these components from one solution. Integrated monitoring is also required to see the larger picture. CiscoWorks VMS provides integrated monitoring of Cisco PIX and Cisco IOS syslogs, and events from network and host-based IDSs, along with event correlation.

CiscoWorks VMS Functions

CiscoWorks VMS is launched from the CiscoWorks dashboard and is organized into several functional areas:

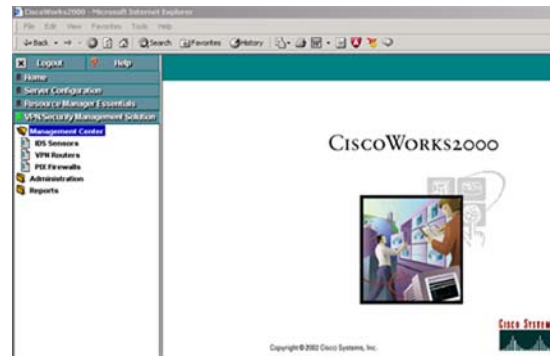
- Firewall management
- Auto Update Server
- IDS management, network and host-based
- VPN router management
- Security monitoring
- VPN monitoring
- Operational management

These functional areas supply multifaceted scalability by offering features such as a consistent user experience, auto update, command and control workflow, and role-based access control.



Figure 1 shows CiscoWorks VMS displayed as a "drawer" in the CiscoWorks dashboard.

Figure 1



Firewall Management

CiscoWorks VMS enables the large-scale deployment of Cisco PIX firewalls, by providing the following features:

- Smart Rules hierarchy and inheritance
- User-defined device and customer groups including nesting
- Global role-based access with administrative privileges per device and customer groups with other CiscoWorks products and Cisco Secure ACS
- Mandatory and default device settings inheritance
- Workflow deployment to device, directory, or Auto Update Server
- Look and feel of Cisco PIX Device Manager but with scalability to thousands of PIX firewalls
- Integration with other CiscoWorks network management software
- Complete SAFE Blueprint coverage for centralized management of Cisco PIX firewalls, including access control, VPN, IDS, and authentication, authorization, and accounting (AAA)

Smart Rules is an innovative feature that allows common information including access rules and settings to be inherited for all firewalls in a device or customer group. Smart Rules allows a user to define common rules once, which results in reduced configuration time, fewer administrative errors, and higher device scalability. Using Smart Rules, a user can configure a common rule such as allowing all HTTP traffic once and can apply this rule globally to all firewalls. Smart Rules can also be defined on a device or customer group basis. For specific information on the firewall management functionality of VMS, refer to: <http://www.cisco.com/en/US/products/sw/cscowork/ps3992/index.html>

Auto Update Server for Firewall Management

CiscoWorks VMS introduces the industry's first firewall Auto Update Server that allows users to implement a "pull" model for security and Cisco PIX operating system management. Auto Update Server permits remote firewall networks with unprecedented scalability. The Auto Update Server allows Cisco PIX firewalls to both periodically and automatically contact the update server for any security configuration, Cisco PIX Operating System, and PIX Device Manager (PDM) updates. The Auto Update Server supports the following features:

- Security management of remote Cisco PIX firewalls that use Dynamic Host Control Protocol (DHCP)
- Automated Cisco PIX OS distribution to groups of Cisco PIX firewalls

Cisco Systems, Inc.

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.



- Automated Cisco PDM updates to remote firewalls
- Configuration verification at periodic intervals
- Automated replacement of inaccurate or tampered configurations
- New firewalls configured at "boot time"

The Auto Update Server is an indispensable component of any large-scale remote Cisco PIX firewall deployment. Auto Update Server is an easy-to-use solution to automatically update all remote or local firewalls with new operating system releases. Cisco is the industry's first vendor to provide this pull model of security policy and operating system management. For specific information on the Auto Update Server component of VMS, refer to: <http://www.cisco.com/en/US/products/sw/cscowork/ps3993/index.html>

Network-Based IDS Management

Administrators can use CiscoWorks VMS to configure network and switch IDS sensors. Many sensors can be quickly configured using group profiles. Additionally, a more powerful signature management feature is included to increase the accuracy and specificity of detection. Some prominent features are:

- Easy-to-use Web-based interface
- Wizards that lead users through common management tasks
- Access to the Network Security Database (NSDB), which provides meaningful information about alarms for users without IDS security expertise
- Ability to define a hierarchy of sensors containing groups and subgroups, and the ability to configure multiple sensors concurrently using group profiles
- Support for several hundred sensor deployments from each console
- Use of a robust relational database to store a high volume of data

For specific information on the network-based IDS management functionality of VMS, refer to:

<http://www.cisco.com/en/US/products/sw/cscowork/ps3990/index.html>

Host-Based IDS Management

CiscoWorks VMS provides threat protection for server and desktop computing systems, also known as "endpoints." VMS goes beyond conventional endpoint security solutions by identifying and preventing malicious behavior before it can occur, thereby removing potential known and unknown security risks that threaten enterprise networks and applications. Because CiscoWorks VMS analyzes behavior rather than relying on signature matching, its solution provides robust protection with reduced operational costs. Features of host-based IDS management include:

- Aggregates and extends multiple endpoint security functions by providing host intrusion prevention, distributed firewall, malicious mobile code protection, operating system integrity assurance, and audit log consolidation all within a single agent.
- Provides preventive protection against entire classes of attacks including port scans, buffer overflows, Trojan horses, malformed packets, and e-mail worms.
- Offers "zero update" prevention for known and unknown attacks
- Provides industry-leading protection for UNIX and Windows servers and Windows desktops allowing customers to patch systems on their own schedules.



- Open and extensible architecture offers the capability to define and enforce security according to corporate policy.
- Scalable to thousands of agents per manager to support large enterprise deployments.

For specific information on the host-based IDS management functionality of VMS, refer to: the Management Center for Cisco Security Agents Datasheet.

VPN Router Management

CiscoWorks VMS includes functions for the setup and maintenance of large deployments of VPN connections and provides users with a point-and-click interface for setting up and deploying connections. This application is intended for scalable configuration of site-to-site VPN connections in a hub-and-spoke topology for centralized, multidevice configuration and deployment of Internet Key Exchange (IKE) and IP Security (IPsec) tunneling policies on VPN routers.

Major features include:

- Wizard-based interface for the creation of IKE and VPN tunneling policies.
- Hierarchical inheritance and Smart Rules hierarchy to reflect the organizational and common setup of devices and simplified device management
- IKE-KA (IKE Keepalive) or generic routing encapsulation (GRE) with Open Shortest Path First (OSPF) and Enhanced Interior Gateway Routing Protocol (EIGRP) for failover routing scenarios.
- Centralized role-based access control model allows for centralized management of users and accounts.

For specific information on the VPN router management functionality of VMS, refer to: <http://www.cisco.com/en/US/products/sw/cscowork/ps3994/index.html>

Security Monitoring

CiscoWorks VMS provides integrated monitoring to reduce the number of security monitoring consoles, reduce the number of events to monitor, and provide a broader view of security status.

- Integrated monitoring is used to capture, store, view, correlate, and report on events from many of the devices in the SAFE Blueprint such as Cisco network IDSs, switch IDSs, host IDSs, firewalls, and routers.
- Event correlation is used to identify attacks that are not easily recognizable from a single event. A flexible notification scheme and automated responses to critical events also aid in quick action.
- The event viewer can read both real-time and historical events.
- Events are color-coded and administrators can quickly isolate problems. Administrators can also define thresholds and time periods when rules can be triggered to provide notification.
- On-demand and scheduled reports facilitate ongoing monitoring.

For specific information on the security monitoring component of VMS, refer to: <http://www.cisco.com/en/US/products/sw/cscowork/ps3991/index.html>



VPN Monitoring

CiscoWorks VMS offers a Web-based management tool that allows network administrators to collect, store, and view information on IPsec VPN connections for remote-access or site-to-site VPN terminations. Multiple devices can be viewed from an easy-to-use dashboard that is configured using a Web browser. This dashboard provides the following capabilities:

- Provides data on system resources related to real-time memory usage, percent CPU usage per device, and active tunnel and active sessions. This data simplifies the identification of devices with potential performance problems and devices with the highest usage.
- Enables viewing of current and long-term packet rates and packet dropped percentage which can aid in determining where excess capacity can be tapped or quickly identify bottlenecks and device throughput problems.
- Enables identification of the devices with the most persistent problems through the event log; key device and VPN statistics are evaluated against a set of global and device-specific thresholds, and exceptions are recorded in the event log.
- Provides graphing of important common metrics. Device performance comparisons provide a global view of short-term trends in VPN performance, enabling administrators to identify problem areas before they become critical failures.

For specific information on the VPN monitoring component of VMS, refer to: <http://www.cisco.com/en/US/products/sw/cscowork/ps2326/index.html>

Operational Management

CiscoWorks VMS provides the operational management for the network, allowing network managers to perform the following:

- Quickly build a complete network inventory
- Manage device credentials information
- Monitor and report on hardware, software, configuration, and inventory changes
- Manage and deploy configuration changes and software image updates to multiple devices
- Monitor and troubleshoot critical LAN and WAN resources
- Quickly identify devices that can be used for VPNs, if upgraded with the appropriate Cisco IOS Software
- Discover which VPN devices have hardware encryption modules
- Graphically compare configurations of VPN devices
- Isolate IPsec-related problems by running customized Syslog reports

For specific information on the operational management functionality of VMS, refer to: <http://www.cisco.com/en/US/products/sw/cscowork/ps2073/index.html>

Server Specifications (Minimum requirements)

Server Hardware

- PC-compatible computer with 1 GHz or faster Pentium processor
- Sun UltraSPARC 60 MP with 440 MHz or faster processor
- Sun UltraSPARCIII (Sun Blade 2000 Workstation or Sun Fire 280R Workgroup Server)



- CD-ROM drive
- 100BASE-T or faster connection
- 1 GB RAM
- 9 GB available disk drive space
- 2 GB virtual memory
- Color monitor with video card capable of 16-bit color

Server Operating System

CiscoWorks VMS requires the following operating systems:

- Windows 2000 Professional, Server, and Advanced Server (Service Pack 3)

Note: Support for Advanced Server requires that Terminal Services be turned off.

Sun Solaris 2.8 with patches:

109742 has been replaced by 108528-13

109322 has been replaced by 108827-15

109279 has been replaced by 108528-13

108991 has been replaced by 108827-15

Java Requirements

Sun Java plug-in 1.3.1-b24

Client Requirements

Hardware

- PC-compatible computer with 300 MHz or faster Pentium processor
- Solaris SPARCstation or Sun Ultra 10

Client Operating System

- Windows 2000 Server or Professional Edition with Service Pack 3, or Windows XP SP1 with Microsoft VM.
- Solaris 2.8

Client Browser

- Internet Explorer 6.0 Service Pack 1, on Windows operating systems
- Netscape Navigator 4.79, on Windows 2000 Server or Professional Edition with Service Pack 3, or Windows XP; Netscape Navigator 4.76 on Solaris 2.8

The CiscoWorks Management Center for Firewalls, and CiscoWorks Management Center for VPN Routers, are supported on Internet Explorer 6.0, but not on Netscape Navigator. In addition to supporting Internet Explorer The Management Center for IDS and the Monitoring Center for Security are also supported on Netscape Navigator.

Service and Support

CiscoWorks products are eligible for coverage under the Cisco Software Application Service (SAS) program. This service program offers customers contract-based 24-hour access to the Cisco Technical Assistance Center (TAC), full Cisco.com privileges, and software maintenance updates. A SAS contract ensures that customers have easy access to the information and services needed to stay current with newly supported device packages, patches, and minor updates. For further information about service and support offerings, contact your local sales office.

Ordering Information

CiscoWorks VMS is available for purchase through regular Cisco sales and distribution channels worldwide. CiscoWorks VMS includes all the necessary components needed for an independent installation on a Microsoft Windows or Sun Solaris workstation.

For More Information

For more information, go to <http://www.cisco.com/warp/public/cc/pd/wr2k/vpmnso/prodlit/> or send e-mail to cisoworks@cisco.com



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 6317 7777
Fax: +65 6317 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 Web site 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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Catalyst, Cisco, Cisco Systems, Cisco IOS, the Cisco Systems logo, Cisco Unity, and EtherSwitch are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0303R) 203051/ETMG 04/03