

CiscoWorks VPN Monitor 1.2

Enterprises have recognized the dramatic benefits of virtual private networks (VPNs) using IP Security (IPSec) to reduce costs and secure their networks. Now, as IPSec VPNs become business critical, enterprises need strong management tools to monitor the health of IPSec tunnels and central-site VPN devices.

Introduction

Once a VPN has been deployed, network administrators must be able to monitor the health of the tunnels and VPN devices to ensure optimal VPN services. They need the following information:

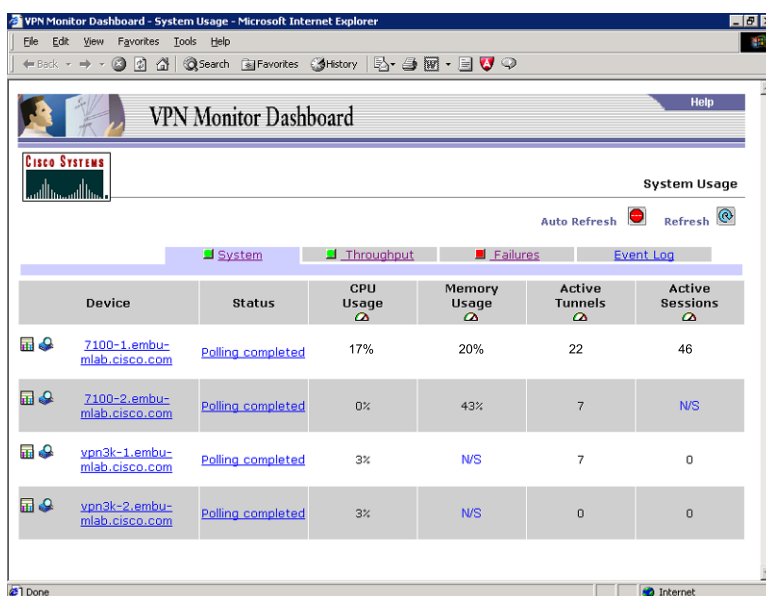
- Number of operational tunnels
- Throughput of individual tunnels
- Status of security negotiations and sessions
- VPN device performance status
- Performance threshold violations

Network managers can generate special reports on VPN-related problems to provide visibility on Internet Key Exchange (IKE), encryption, encapsulation, and certificate problems. Network managers need ongoing reports on current VPN activity, outages, VPN failures, signs of impending failures, and activity history.

CiscoWorks VPN Monitor is 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. CiscoWorks VPN Monitor manages VPNs that are configured on Cisco VPN 3000 concentrators, and Cisco 1700, 2600, 3600, 7100, 7200, or 7400 Series routers. Multiple devices can be viewed from an easy-to-use dashboard configured on a Web browser. After the dashboard is configured, CiscoWorks 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.

The dashboard allows network administrators to drill down to further analyze each device's performance and its current IPSec connections. Administrators

Figure 1
CiscoWorks
VPN Monitor
Dashboard





can use this drill-down capability to view device CPU and memory performance, tunnel throughput, failure events, threshold violations, and active tunnels on a device. Data collected from VPN devices can also be viewed in detailed graphs that display important parameters related to VPN operation.

CiscoWorks VPN Monitor supports the commonly deployed VPN tunneling protocols, including the IETF Layer 2 Tunneling Protocol (L2TP), Point-to-Point Tunneling Protocol (PPTP), and IPsec.

Features and Benefits

Flexible Monitoring

CiscoWorks VPN Monitor's configuration flexibility allows network administrators to set polling and graphing intervals to best reflect the network performance of the network and the graphical user interface of CiscoWorks VPN Monitor. The types of monitoring range from the percent utilization of a CPU, to the throughput of a VPN concentrator or router, to the number of users with established connections. Other variables that can be tracked include:

- System resources—average and maximum memory available and CPU utilization percentage per device
- Traffic throughput—average and maximum of encrypted traffic
- Statistics—number of sites that are online, number of sessions established, number of IKE and session failures, and number of current security errors

The dashboard can also provide troubleshooting information. Auto-refreshing Web-based status reports provide detailed information on conditions such as the number of session failures or IKE failures by peer. You can set warnings and alerts based on user-defined threshold values.

Multidevice Comparison

CiscoWorks VPN Monitor provides a convenient way to view important statistics of multiple VPN termination devices in a single dashboard. This capability enables administrators to quickly correct for devices with the highest CPU or memory usage. The multidevice view gives the administrator an aggregated summary of active VPN tunnels and sessions.

Supported Cisco Devices

- Cisco VPN 3000 concentrators with the 2.5.2f software image or later
- Cisco 7100, 7200, or 7400 Series routers with Cisco IOS® Software Release 12.1.(5a)E or later
- Cisco 1700, 2600, and 3600 Series routers with Cisco IOS Software Release 12.2(4)T or later

System Requirements

For comprehensive hardware and operating requirements, see the CiscoWorks VMS Overview at <http://www.cisco.com/go/vms>

Ordering Information

CiscoWorks VPN Monitor is available exclusively as part of the CiscoWorks VPN/Security Management Solution (VMS).

Detailed ordering information is available in the VMS product bulletin at <http://www.cisco.com/warp/public/cc/pd/wr2k/vpmnso/prodlit/>.



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 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