



DEPLOYMENT GUIDE

CISCOWORKS VMS 2.3

INTRODUCTION

The Challenge

One of the major challenges of network management is to create a solution that is flexible enough to adapt to the changing needs of your network. While it makes sense to have applications that provide basic network management functionality regardless of the function, the network environment must also be considered. To do this successfully, it is better to have a focused set of tools for management. For example, a tool that focuses on managing quality of service (QoS) levels is probably not going to be very good at managing a server farm topology.

Growth and Enhancements in Network Security

When we look at the network as a strategic asset to the enterprise, network management clearly becomes an important factor in the success of the company. When we consider the evolution of business applications running across the traditional data network including e-commerce, business-to-business transactions, and voice over IP (VoIP), the need to provide secure network connections grows. As a result, we have witnessed a proliferation in virtual private networks (VPNs) and an enhanced awareness of network security.

PAPER OBJECTIVE

This paper provides guidance on how to effectively deploy CiscoWorks VPN/Security Management Solution (VMS). Covered topics include: server, installation and operating system requirements, reference topology, metrics to monitor, and device configuration considerations. It supplements the quick start guide and user manual, and addresses such questions as: Which products are included and what are they used for? How many servers will I need? What devices can I manage with this application? How can I harden VMS server itself? By answering these questions, we can provide some basic best practices for managing specific Cisco® security technologies.

What It Does NOT Do

This paper is not intended to replace user guides (or other product documentation). It does not go into comprehensive detail about the various features or capabilities of the products.

Intended Audience

This paper is intended for audiences that are already familiar with network security, VPNs, firewalls, and intrusion detection, and have a basic understanding of these concepts and tools. It explains how best to deploy VMS in a production environment.

HIGH-LEVEL OVERVIEW OF VMS 2.3

What Does It Do?

CiscoWorks VMS is a set of integrated tools that provide a comprehensive solution for VPN and security management. VMS features are positioned to configure, monitor, and troubleshoot enterprise VPNs, firewalls, and network- and host-based intrusion detection and prevention systems (IDS/IPS). VMS provides key features to assist customers in the deployment, monitoring, and management of their security-specific hardware. It also provides the operational management support, software distribution, configuration archive, change-audit, and logging management for different

elements of a Cisco security infrastructure. VMS provides a scalable solution that addresses the needs of small- to large-scale VPN and security deployments.

VMS 2.3 COMPONENTS

CiscoWorks VMS 2.3 consists of installable software components for flexible deployment options. Table 1 lists the different VMS modules and what they do.

Table 1. VMS 2.3 Modules*

VMS Module & Versions	Platform	Usage
Common Services 2.2	Windows Solaris	Provides a set of common software and services for VMS components and CiscoWorks Resource Manager Essentials (RME)
CiscoView 5.5		CiscoView provides physical graphical view of device chassis and basic status monitoring
Management Center for Firewalls 1.3.3 (FWMC)	Windows Solaris	Configures Cisco PIX® firewalls and Cisco Catalyst® Firewall Service Modules
Auto Update Server 1.3 (AUS)	Windows Solaris	Permits configurations, PIXOS and PDM files to be pulled from update server
Management Center for VPN Routers 1.3.1 (RouterMC)	Windows Solaris	Configures VPN and firewall feature set on Cisco IOS® routers and Cisco Catalyst VPN Service Modules
Management Center for IDS Sensors 2.0 (IDSMC)	Windows Solaris	Configures and updates network-based IDS sensors and Cisco Catalyst IDS Service Modules
Monitoring Center for Security 2.0.2 (SECMON)	Windows Solaris	Monitors network and host-based IDS events, Cisco IOS Software, and Cisco PIX syslog
Monitor Center for Performance 2.0.2	Windows Solaris	Monitors and troubleshoots the health and performance of enterprise network security services (remote-access VPN, site-to-site VPN, firewall, web server load-balancing, and proxied SSL).
Management Center for Cisco Security Agent 4.5 (CSAMC) Note: 4.5 will be available on CCO shortly after the release of VMS 2.3, while officially the version in VMS 2.3 is 4.0.3. We have decided to include directly 4.5 in this guide, since it is going to be released shortly after the VMS2.3 bundle.	Windows	Configures host-based IPS to protect critical servers

VMS Module & Versions	Platform	Usage
Cisco Security Agent 4.5 (CSA)	Windows	The agents installed on the servers to be protected
	Solaris	
	Linux	
Resource Manager Essentials 3.5 (RME)	Windows	Provides operational management, such as software distribution, change audit, syslog analysis
	Solaris	

* Users should check the Software Center on CCO to see if any new modules have been added into VMS.

These components can be divided into distinct categories: core asset management applications, security monitoring applications, and security configuration applications. This section details some of the basic features associated with each of these product categories.

Foundation Software, Common Components, Required Installation

1. CiscoWorks Common Services

CiscoWorks Common Services includes basic components of the management server such as the web server, common database, polling engine, and so forth. **Install this CD first**, because it is a prerequisite for the management center tools in the VMS bundle. Common Services can be thought of as like an “operating system” for CiscoWorks applications.

Core Asset Management Applications

1. Resource Manager Essentials (RME)

Resource Manager Essentials provides the basic network management tools for day-to-day network management including inventory, configuration, change audit, and syslog. RME also provides additional VPN management capabilities. Network administrators will now be able to produce device configuration, software image, and syslog reports specific for VPN environments.

2. CiscoView (an optional install located within Common Services)

CiscoView is a web-based device management application that provides dynamic status, monitoring, and configuration information for the broad range of Cisco internetworking products. CiscoView displays a physical view of a device chassis with color-coded modules and ports for at-a-glance status. Monitoring capabilities display performance and other statistics, and configuration allows comprehensive changes to devices.

Security Monitoring Applications

1. Monitoring Center for Security (SECMON) a.k.a. “Security Monitor”

SECMON monitors the IDS events as well as SYSLOG messages from various Cisco devices. These include network IDS sensor appliances, Cisco Catalyst 6500 Series IDS modules, Network Modules for routers (NM-IDS), Cisco IOS Software IDS messages (including the new IPS IDS feature for the routers), Cisco PIX Firewall syslog messages, Catalyst 6500 Firewall Service Module syslog messages, Cisco Security Agent events and events coming from another Security Monitor server.

2. Monitoring Center for Performance (MCP)

MCP is a browser-based tool that monitors and troubleshoots the health and performance of enterprise network security services. Performance Monitor replaces the VPN Monitor 1.2 application. Supported service types are remote-access VPN, site-to-site VPN, firewall, web server load-balancing, and SSL accelerators.

Security Configuration Applications

1. Management Center for VPN Routers (Router MC)

Router MC is a VPN and Cisco IOS Firewall feature set configuration and deployment tool for Cisco IOS VPN routers. Router MC is a web-based application installed on top of Common Services.

2. CiscoWorks Management Center for Firewalls (FWMC)

Firewall MC is a complete firewall and access rule policy configuration tool for Cisco PIX firewalls and firewall service modules in Cisco Catalyst switches. You can configure new firewalls as well as import configurations from existing firewalls or configuration files. Firewall MC also provides a powerful tool for controlling changes made to your network, showing configuration and status changes. Firewall MC is a web-based application installed on top of Common Services.

3. CiscoWorks Auto Update Server Software (AUS)

AUS is a tool used to store and upgrade device configuration files and software images (firewall image and Cisco PIX Device Manager [PDM] image). Firewall devices periodically contact the AUS to request configuration and software updates. In this way, firewall devices are actively kept up to date. AUS is particularly useful for scaled deployments of PIX firewalls when the remote PIX Firewall devices are dynamically addressed or behind a Network Address Translation (NAT) device. AUS is a web-based application installed on top of Common Services.

4. Management Center for IDS Sensors (IDSMC)

IDS MC is an IDS configuration and deployment tool for Cisco network IDS sensor appliances, Cisco IDS service modules in Catalyst switches (IDSM) and routers (NM_IDS) and IPS IDS. IDS MC is a web-based application installed on top of Common Services.

5. Management Center for Cisco Security Agent (CSAMC)

Working as a complementary technology to IDS MC and Security Monitor, the Cisco Security Agent MC is a configuration and deployment tool for the host-based IDS solution, Cisco Security Agent. Cisco Security Agent MC is a web-based application installed on top of Common Services.

6. Cisco Security Agent (CSA)

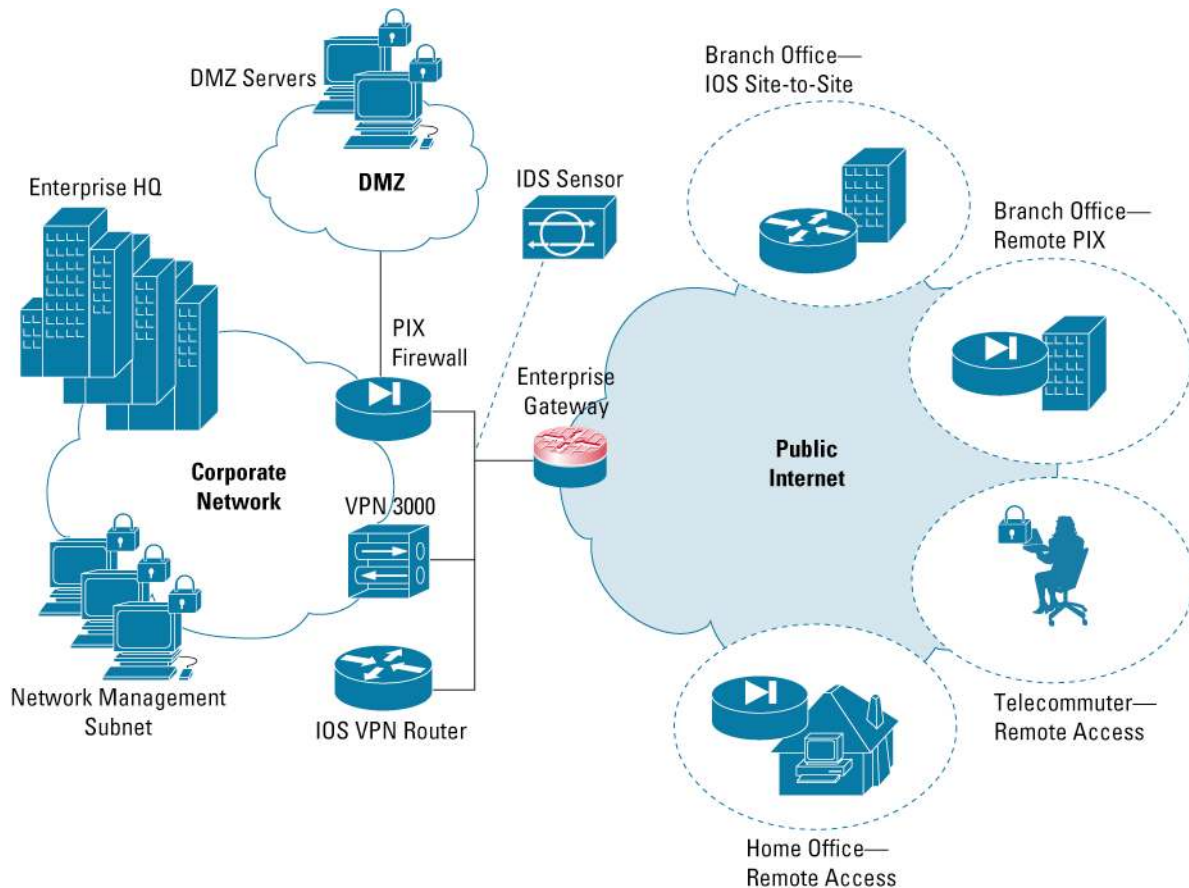
A Cisco host IDS/IPS application, Cisco Security Agent protects critical servers and hosts by integrating with the operating system.

By intercepting system calls to the kernel, Cisco Security Agent can protect your hosts by identifying attacks and preventing access to resources and unauthorized transactions.

REFERENCE TOPOLOGY

A reference network topology that shows the different aspects of VPN and network security (Figure 1) is provided to describe how best to deploy CiscoWorks VMS. Although it is not identical to most customer environments, it does serve to provide a holistic view of a secured network. By using this reference topology, you can select the components that best represent your topology and understand how best to deploy VMS in your environment.

Figure 1. Reference Security Topology



The Infrastructure Involved

- *Enterprise Gateway*—This is a Cisco IOS Router with the Cisco IOS Firewall Feature Set. The main purpose of this device is to perform gateway routing and basic frontline firewall functionality.
- *PIX Firewall*—The Cisco PIX Firewall provides the comprehensive firewall functionality for this enterprise network. Corporate network resources are protected by this firewall by strategically placing these devices at network access points.
- *Cisco 800, 1700, 2600, 3600, 7100 or 7200 Series routers*—Cisco routers act as site-to-site VPN termination points. In a hub-and-spoke VPN topology, the high-end VPN routers act as hubs and the small- to medium-sized routers act as spokes.
- *VPN 3000*—The VPN 3000 Series Concentrator provides scalable remote access VPN termination. In this topology the concentrator terminates VPN connections with a variety of remote access environments, VPN client software, and tunneling protocols (IPSec, L2TP, PPTP).
- *Cisco VPN remote access client software*—This software allows remote access users to connect to the corporate network through VPNs.
- *Network IDS Sensor*—This device sits on a network segment and passively “listens” to the traffic, inspecting it against a database of common attack signatures. It forwards IDS event information to the monitoring station.
- *Cisco host-based IDS/IPS security agents*—This software sits on critical network servers as well as home office PCs and mobile laptops to protect individual hosts from intrusion and attacks. Events are forwarded to a central monitoring console.
- *Network management subnet*—This subnet represents a dedicated network segment for the network management servers. The components of VMS reside in this subnet to manage the different pieces of the infrastructure. All VMS servers are secured by Cisco Security Agents.
- *DMZ Servers*—This subnet represents a dedicated network segment for publicly accessible network servers. Generally, this includes e-mail, Web, FTP servers, and in our case includes CiscoWorks Auto Update Server Software. All DMZ servers are secured by Cisco Security Agents.

Within these reference topologies, we now focus on several pieces of the infrastructure that VMS manages. Note that the network management applications within VMS can manage other devices (such as Cisco Catalyst switches), but the following are the components that should be the focal point of VMS. These components include:

- Enterprise HQ
 - This section includes the network management servers, internal firewalls, VPN termination points (both hub routers and VPN concentrators), and IDS sensors. Access to the DMZ portion of the network is controlled by internal firewalls and also has publicly accessible servers.
- Remote Access Sites
 - The remote access sites in our topology contain the remote PIX firewalls, remote Cisco IOS VPN routers, and remote VPN clients. These pieces of the infrastructure are responsible for VPN termination and firewall access policy at the remote site.

OS SUPPORT AND SYSTEM REQUIREMENTS FOR VMS

VMS is composed of a series of tools that reside on a network management server (or servers). This section discusses the prerequisite software you need to install in order to run the components within VMS. Primarily, this refers to OS support. For almost every application in the VMS bundle, the supported OS is Windows 2000 Server or Advanced Server. This is summarized in Tables 2 and 3.

Table 2. Supported OS for VMS 2.3 Modules

VMS Module	Windows Support	Solaris Support
Common Services	X	X
Management Center for Firewalls	X	X
Auto Update Server	X	X
Management Center for VPN Routers	X	X
Management Center for IDS Sensor	X	X
Monitoring Center for Security	X	X
Management Center for CSA	X	
Resource Manager Essentials	X	X
Monitor Center for Performances	X	X

Table 3. Minimum Hardware and OS Requirement for VMS Server

Windows	
Hardware	IBM PC compatible with 1GHz or faster Pentium CPU 1 GB memory 9 GB free hard drive space* CD-ROM drive Color monitor with video card capable of 16-bit colors 10/100 BaseT or faster network connection
Operating System	Windows 2000 Server** Windows Advanced Server** Service Pack 4 NTFS file system 2 GB virtual memory
Solaris	
Hardware	Sun UltraSPARC 60MP with 440 MHz or faster CPU or Sun UltraSPARC III (Sun Blade 2000 Workstation or Sun Fire 280R Server) CD-ROM drive Color monitor with video card capable of 16-bit colors 10/100 BaseT or faster network connection
Operating System	Sun Solaris 2.8 full installation Required patches: 108528-13 108527-15

* The actual amount of hard drive space required depends on the number of VMS components you are installing and the number of devices you are managing and monitoring.

** Terminal Services in application mode cannot be installed on the server while installing VMS 2.3. Instead it can be on the server at installation time if in other modes, but it has to be disabled during installation.

Note: If Virus Scan is turned on, the installation can be longer due to the Virus scan operations. We recommend that Virus Scan be turned off for a faster installation.

Server Sizing

Based on these factors, the recommend server sizing for each of these configurations should be more closely examined. Note that these specifications are minimum requirements for individual applications and are frequently exceeded in many deployments. The general rule is: If you must choose one metric that will have the greatest affect on performance, increase the amount of RAM. It is also necessary to pay attention to the scale limits of each application. If you are approaching some of those theoretical limits, consider increasing the horsepower of your VMS server(s). For example, it is not unreasonable to see a P4 2.2 GHz CPU with 4 GB of RAM running VMS applications. See Table 4 for a general guideline.

Table 4. Server Recommendations (Minimum) for VMS Configurations

Configuration	Small	Medium	Large	Extra Large
CPU	P4 1 GHz	P4 2.5 GHz	Xeon 2 GHz	Dual/Quad Xeon,
RAM	1 GB	2 GB	2+ GB	2-8 GB RAM
Virtual Memory	2 GB	3 GB	4 GB	4 GB
Hard Disk Space	9 GB	20 GB	40 GB with SCSI Hard Drive	40 GB with SCSI RAID 5

Server Deployment—General Rules

In terms of application compatibility, there are several rules to follow:









































- Common Services must be installed first
- All other applications must be installed on top of Common Services

Given these conditions, VMS can have extremely flexible deployments. All of the components can be installed and run on a single server—or, each component can be installed on its own individual server. In general, both extreme is not recommended and the deployment will generally depend on a number of factors:

1. Which applications do you actually need?

Although VMS provides a rich, comprehensive management solution, it is possible that not every component will be used. The first question that should be asked is: which applications will I use? Once this has been answered, you can choose to install only the modules that are needed. Figure 2 provides a table that defines the installation order based upon the different management options, when they are installed on a single server.

Figure 2. VMS Module Installation Matrix (components included in () are optional)

Legend							
	Managed VPN/FW Router		Managed Firewall		Managed IDS		Managed Security Agent
Management Option				Installation			
				Common Services, Router MC, (RME), MCP			
				Common Services, Firewall MC, AUS, MCP			
				Common Services, IDS MC, (SecMon)			
				Common Services, CSA MC			
				Common Services, IDSMC, CSAMC, (Secmon)			
				Common Services, Router MC, Firewall MC, (RME), MCP			
				Common Services, Router MC, IDSMC, CSAMC, (SecMon), (RME), MCP			
				Common Services, IDSMC, FMC, MCP, (SecMon)			
				ALL			

Note: This table provides basic guidelines. Obviously, not all combinations and tools within VMS are covered—only those with installation order dependencies.

- Installation option 1: For VPN management, the monitoring component is handled by Monitoring Center for Performance. If monitoring is necessary, MCP needs to be installed.
- Installation option 2: For firewall management, AUS is only necessary if you want to take advantage of the auto-update feature for PIX Firewall configuration and software deployment.
- Installation option 3: For network and host-based IDS management, Security Monitor is necessary to monitor the events from all these components unless you plan to use other security information-management applications. Is always good practice to install Security Monitor on a separate server than the configuration server.

2. How many devices will each application manage?

If one of the applications you are using is approaching its theoretical scale limits (Table 5), it is a good idea to dedicate a server to that application. For obvious reasons of resource allocation and task distribution, it is best not to have other applications using valuable CPU resources if you are trying to manage a large number of devices.

For example, if you have an instance of Firewall MC installed that is managing 800 PIX firewalls, and you are also trying to roll out a hub-and-spoke VPN deployment across 600 router spokes, it is recommended to break these applications apart onto dedicated servers.

3. How many administrators will be using these applications?

In some multi-administrator environments, it makes sense to explore different deployment options for VMS. Since there are several VMS components involved, and each has a very distinct purpose, it is possible that there will be different security administrators using different applications. In this case, consider splitting these applications onto dedicated servers. This way, if one application is busy with a resource-intensive task such as generating configuration files, the second application will not suffer any degradation in performance.

4. What cost restrictions exist in terms of server procurement?

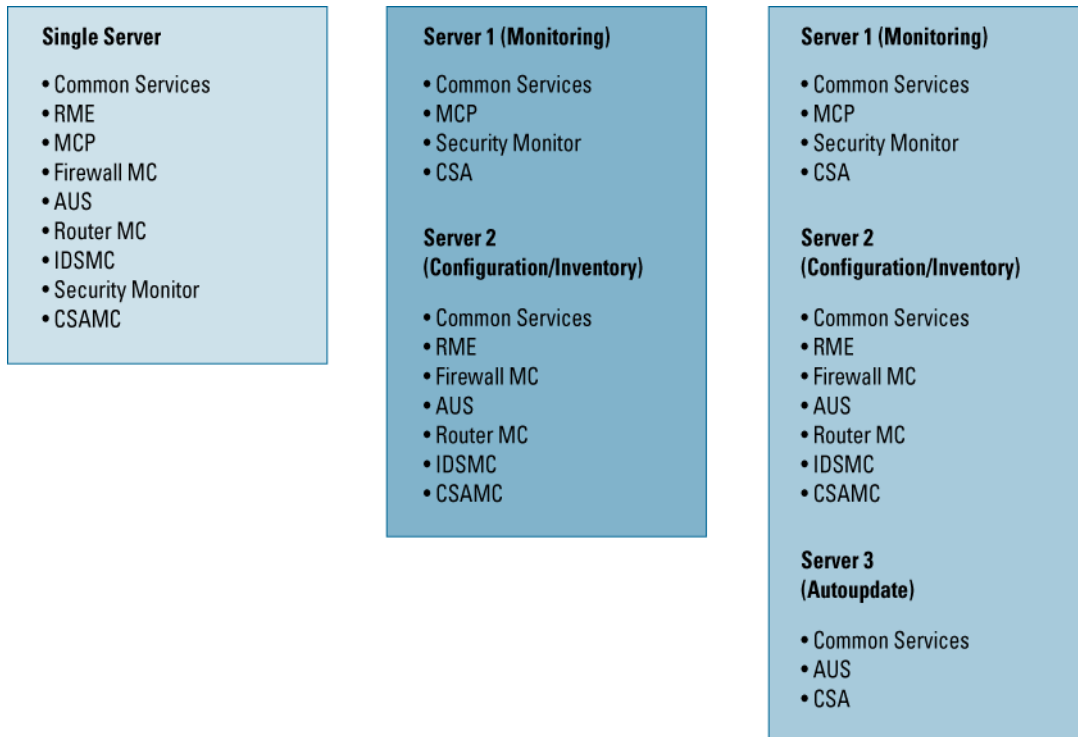
Does the organization using VMS have (or have the ability to get) multiple servers? In some cases, there may only be enough in the budget for one server. If this is the case, then it is always better to acquire a high-end server that exceeds the minimum system requirements. This allows room for growth, as well as improved performance.

More is Better

Ultimately, it is best to use multiple servers and split the applications across them in a way that makes sense, if at all possible. Generally, for better scalability, resource allocation, task distribution, and room for growth, more is better as long as it doesn't become cumbersome and unmanageable. Also keep in mind that, should you decide to combine multiple applications onto a single server, you will need to pay special attention to the hardware requirements of each application and adjust accordingly.

The following section discusses some basic deployment options and provides some general guidelines that cover most user scenarios (Figure 3). Keep in mind that these are simply recommendations and do not necessarily indicate that VMS must be deployed in this manner.

Figure 3. Server Deployment Options



Option 1—Single Server Deployment

For small-scale security environments with a single network security administrator, we recommend a single-server deployment. This has the benefit of low cost to the organization as well as ease of administration.

Option 2—2 Servers: Configuration and Monitoring

This deployment option breaks down the VMS applications across function: One server is dedicated for monitoring and the second server is dedicated for configuration.

1. Server 1: Monitoring

The first server in this deployment option is dedicated for monitoring. MCP is used for IPsec MIB monitoring and performance monitoring for Firewalls, while Security Monitor is used for consolidated event viewing of PostOffice IDS, Remote Data Exchange Protocol (RDEP) IDS, Cisco Security Agent, PIX, and Cisco IOS Syslog messages. The applications for this server are:

- Common Services
- MCP
- Security Monitor
- CSA (to protect the VMS server)

2. Server 2: Configuration and Inventory

This security management server is used to combine all of the VMS applications that assist in configuration. Regardless if the infrastructure is VPN router, PIX Firewall, IDS sensor, or Cisco Security Agent, this server's primary function is configuration. The relevant applications are:

- Common Services
- RME
- Firewall MC
- AUS*
- Router MC
- IDS MC
- CSA MC

Option 3—3 Servers: Recommended for most environments

Since AUS server is intended to manage to remote firewalls, it can be resource consumptive when many remote devices are contacting AUS for configuration, or OS and PDM updates. Also, AUS should be positioned on the DMZ of the network, so AUS could use one server by itself.

1. Server 1: Monitoring

- Common Services
- MCP
- Security Monitor
- CSA for protection

2. Server 2: Configuration/Inventory

- Common Services
- RME
- Firewall MC
- Router MC
- IDSMC
- CSA MC

3. Server 3: Auto Update

- Common Services
- AUS
- CSA for protection

* The primary purpose of AUS is to provide configuration and software updates to remote PIX firewalls. As such, it is frequently recommended to place the AUS within the organization's DMZ. If this is the case, we recommend using a dedicated server for AUS.

Option 4—3 Servers: Security Application Function (Not shown in Figure 3)

The fourth deployment option centers around splitting up the VMS application according to the security technology (or infrastructure) managed. The first server deals with VPNs, which generally covers Cisco IOS Software-based VPN routers. The second server contains the applications used to manage Cisco PIX firewalls. Finally, the third server is dedicated to the management and monitoring of IDS—both network-based and host-based IDS.

1. Server 1: VPN

- Common Services
- RME
- MCP
- Router MC
- CSA for protection

2. Server 2: Firewall

- Common Services
- Firewall MC
- AUS
- CSA for protection

3. Server 3: IDS

- Common Services
- IDS MC
- Security Monitor
- CSA MC

Option 5—4 Servers: Granular Management Control (Not Shown in Figure 3)

For even more granularity and scalability benefits, we recommend you further divide your deployment. The most important difference with this option is the use of a dedicated server for AUS since it is placed within a different subnet of the network.

1. Server 1: Configuration

- Common Services
- Firewall MC
- Router MC
- IDS MC
- CSA MC

2. Server 2: Inventory

- Common Services
- RME
- CSA for protection

3. Server 3: Monitoring

- Common Services
- MCP
- Security Monitor
- CSA for protection

4. Server 4: Remote Management (placed in DMZ)

- Common Services
- AUS
- CSA for protection

Keep in mind that these are only recommendations. There are numerous combinations and deployment options available and each case should be considered on an individual basis. There will also be many cases where customers don't want to use all of the possible applications within VMS.

SCALING AND DEPLOYMENT CONSIDERATION

It is necessary to be aware of the hardware requirements for the VMS bundle as well as the software. There is also the inherent challenge of deciding how best to deploy the different applications in the solution. Since we have eleven installable software applications, there are numerous combinations in which to deploy them.

Keeping the minimum requirements in mind, the difference in recommended system specifications based upon different sized networks and configurations must also be examined. We will discuss three different sized configurations: small, medium, and large. The first consideration is scalability, or how many devices equate to a small, medium, or large configuration (see Table 6, 7 and 8).

Scaling

Each application within VMS has a different scalability metric. Table 5 provides the theoretical maximum for each application.

Table 5. Theoretical Scale Limits for VMS Applications

VMS Module	Scalability Metric (tested up to*)
IDS MC	300 IDS sensors or IOS IPS
Security Monitor	50 events/sec** (500ev/sec for burst)
Firewall MC	1000 PIX firewalls & FWSM (is suggested not to generate or deploy for more than 300 devices at the same time in case of simple config, i.e. 501. If the configuration is medium to complex the performances will be lower, therefore is suggested to deploy in a smaller number of devices at the time)
AUS	1000 PIX firewalls
Router MC	1000 routers
CSA MC	100.000 Cisco Security Agents
RME	5000 devices inventory, 1000 devices availability

VMS Module	Scalability Metric (tested up to*)
MCP	1000 devices (1000 Routers & 4000 tunnels with 25 min polling cycle, if the Routers/Tunnels are reduced then the polling cycle is reduced also. For 1000 pix a 25 min polling cycle is needed and if the number of device is less then the polling cycle also is reduced. Polling cycle is the time taken to poll all the devices in MCP).

* The theoretical scale limits are the limits the tools have been tested to. The numbers are stated as a guideline to guarantee reasonable performance and user experience. Although possible, it is not recommended to exceed these metrics.

** The volume of security events can arrive up to 500 per second only for a limited period of time, it is recommended that users consider a monitoring product from a partner-vendor that can handle higher event volumes.

In general, these are not software-imposed limits, but rather the scale limitations based on software testing. For example, if you are using Router MC and want to add device number 1001, the software will still allow you to do so, but from a support standpoint it is not recommended.

Also note that the specifications for the minimum hardware requirements for VMS are provided based upon testing and performance statistics for just ONE (not all) of the applications in the bundle. For example, if you are using IDS MC to manage 300 sensors (the theoretical maximum), we do NOT recommend to use any other application on that server. If you plan to heavily use more than one application within VMS, it is highly recommended to put them on separate servers.

Now we will consider some of the resource-intensive applications within the bundle. The configurations are grouped as shown in Tables 6–8.

Table 6. Small Configuration Metrics (reflects restricted VMS license model)

VMS Module	Scalability Metric (up to)
IDS MC	20 IDS sensors
Security Monitor	20 events per second sustained
Firewall MC	20 PIX firewalls
AUS	20 PIX firewalls
Router MC	20 routers
CSA MC	500 Cisco Security Agents
MCP	40 devices

Table 7. Medium Configuration Metrics*

VMS Module	Scalability Metric (up to)
IDS MC	100 IDS sensors
Security Monitor	30 events per second sustained
Firewall MC	100 PIX firewalls
AUS	100 PIX firewalls

VMS Module	Scalability Metric (up to)
Router MC	100 routers
CSA MC	5000 Cisco Security Agents
MCP	200 devices

* This configuration is designed to represent the majority of the VMS customer base.

Table 8. Large Configuration (reflects the theoretical maximum scalability metrics)

VMS Module	Scalability Metric (up to)
IDS MC	300 IDS sensors
Security Monitor	50 events per second sustained
Firewall MC	1000 PIX firewalls
AUS	1000 PIX firewalls
Router MC	1000 routers
CSA MC	100,000 Cisco Security Agents
MCP	1000 devices

Scaling SecMon

SecMon has a maximum rate of 50 ev/sec for a sustained period of time, and can reach 500ev/sec on a burst time of 5 minutes max. If you expect the event rate to be greater than this, it is suggested that you consider using other vendor/partner monitoring tools.

Those numbers are not strict, but can vary depending on the server used, the I/O speed of the computer and other parameters.

Scaling IDSMC

When generating or deploying a configuration for a router, keep in mind that it takes 24 secs on average per router to generate a configuration and 30 secs on average per router to deploy a configuration.

Scaling FWMC

The complexity of the configuration files will determine the number of devices Firewall MC can effectively manage for generation of configuration files and deployment at the same time.

Firewall MC was successfully tested with 1000 devices containing simple configurations (501s) however, medium to complex files will increase the generate and deploy times and reduce the number of devices the MC can effectively provision. For example for a mix of simple and complex configurations for ~310 devices when a global setting or rule is changed the direct deploy to all devices takes ~8hrs.

Scaling MCP

For MCP the suggested polling rate is 30 minutes. In case of small deployment can be decreased in time, but for high number of devices is suggested not to define a polling time lower than 30 minutes. For example for 1000 Routers & 4000 tunnels a polling cycle of 25 min is needed, if the Routers/Tunnels are reduced then the polling cycle is reduced also.

For 1000 pix a 25 min polling cycle is needed and if the number of devices is less than that the polling cycle also is reduced.

Polling cycle is the time taken to poll all the devices in MCP.

Scaling CSA MC

In CSAMC version 4.5, it will be possible to use a remote database (or cluster of databases), allowing us to scale up to 100 000 agents.

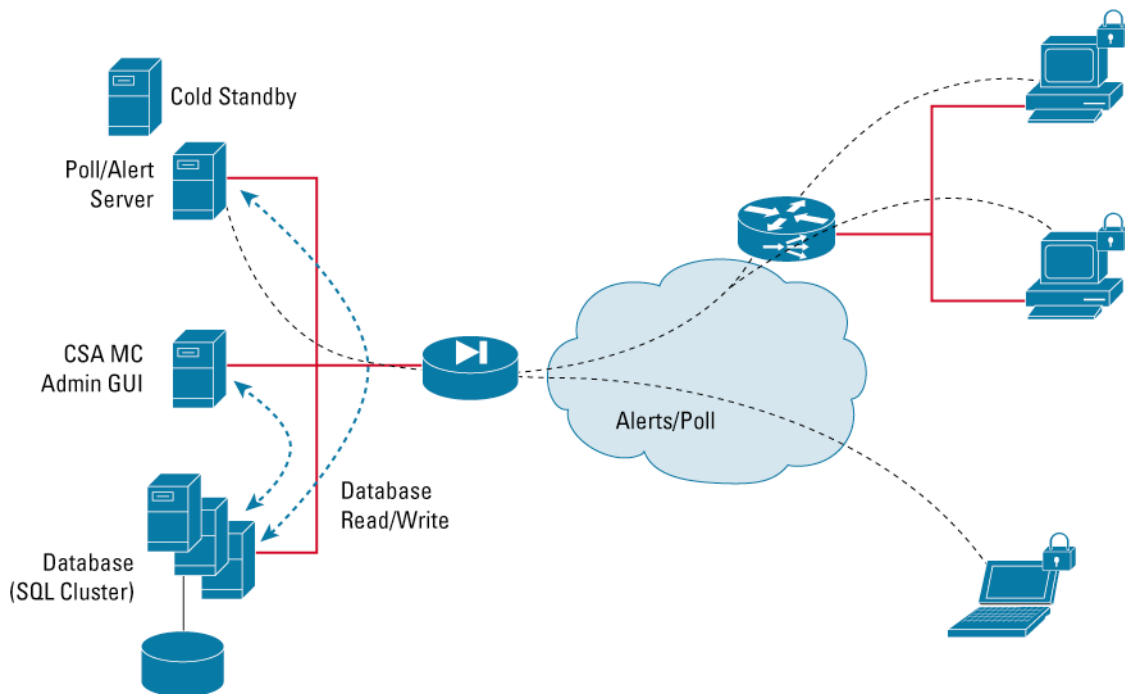
The suggested configuration, depending on the number of supported agents, is as follows

- **500 Agents or less:** If your need is for a small number of agents, we suggest to install a local database using the Microsoft SQL Server Desktop Engine included on the same system.
- **From 500 to 5000 agents:** In this case we suggest to keep using a local database but switch to a Microsoft SQL Server 2000 that has 2 GB limit. In this case the license has to be separate and the SQL server must be installed before the CSAMC. In this case it is still possible to have a remote database to have even better performance.
- **From 5000 to 10000 agents:** Use of a remote database is recommended for such a large number of agents. We also recommend use of two servers, one for configuration, and the other for polling. In this case one can be used for configuration and one for polling. This would allow, in case of an attack, to have the configuration server free and able to deploy changes faster in order to mitigate the attack.

For more information on how to install a remote database, please refer to the “CSAMC installation guide”.

The image shows the architecture in case of a remote database:

Figure 4. CSAMC Architecture in Case of Remote Database Installation



Secure the VMS Server

Now that the basic hardware and software requirements are defined, it is time to examine how to configure the servers themselves to be ready for management. As a general security axiom, to secure hosts, pay careful attention to each of the components within the systems. Keep all systems up-to-date with the latest patches, fixes, and so forth. For VMS, you must make sure that you have the latest Windows 2000 and Solaris patches and hot fixes for security. Below is a detailed checklist of items to consider making sure your servers are ready to be used as management servers:

1. Windows

- Install the operating system on its own partition.
- Do not install VMS on primary domain controller (PDC) or backup domain controller (BDC).
- Use strong passwords.
- Avoid creating network shares.
- Disable unnecessary accounts.
- Secure the registry.
- Apply all hot fixes and security patches.
- Disable unused and unneeded services (at a minimum, Windows requires the following services to run: Domain Name System (DNS) client, event log, plug and play, protected storage, and security accounts manager. Do not install Microsoft's Internet Information Server [IIS].)
- Disable all network protocols except Internet Protocol and Transmission Control Protocol (TCP/IP).
- Monitor the security of your system regularly.
- Limit physical access to your server.
- If possible, do not install remote access or administration tools on the server.
- Periodically run a virus scanning application on the server.

2. Solaris

- Use strong passwords
- Do not install Network Infrastructure Solutions (NIS/NIS+) and DNS servers
- Limit physical access to the server
- Disable unnecessary accounts

3. Use Cisco Security Agent to protect your VMS server (Windows only)

It is a good idea to actively protect your Windows-based VMS server with a host IDS/IPS solution like Cisco Security Agent. Cisco Security Agent is a behavior-based host IPS. It stops not only the malicious or unexpected application from executing in the system, but also stops exploits like buffer overflows, and can work as a firewall to control inbound and outbound network connections and services.

Three Cisco Security Agents are shipped with VMS to protect the Windows-based VMS servers, including default group policies specifically designed to lock down VMS servers. The three Cisco Security Agents are intended to protect VMS configuration server, VMS monitoring server, and VMS auto-update server. If your deployment only has one server installed, then only one agent is required. If you have more than three servers to protect, more Cisco Security Agent licenses need to be purchased from Cisco.

The default Agent used is called "CiscoWorks VMS System", which consists of the following 5 modules (Table 9).

Table 9. VMS Server Default Group Policies to Completely Secure the Server

Policies	Description
----------	-------------

CiscoWorks Base Security Module	Base policy for all systems running CiscoWorks (5 rules attached)
CiscoWorks VMS Module	Module for servers running CiscoWorks VMS product components (22 rules attached)
CiscoWorks Restrictive Security Module	Module for systems running only the VMS bundle (2 rules attached)
CiscoWorks Application Classification Module	Module classifying CiscoWorks applications (6 rules attached)
CiscoWorks CSAMC SQL Server Module	Module for SQL Server on the CSA MC system (3 rules attached)

The 38 rules associated with these three policies cannot all be explained here. For more details please, refer to the CSAMC User guide.

VMS APPLIED

Now that we have determined how to deploy the components of VMS from an installation perspective, we need to take a look at how these applications should be deployed from a functional standpoint. Three basic questions will be addressed in this section:

1. What is the management function of each application?
2. What devices can I manage?
3. What types of services do I need to enable?

The first question requires a detailed look into the capabilities of each product. Then this information is used to determine what aspects of your security management can and should be managed by each of the components within VMS. The second question will clarify confusion surrounding the variances in devices supported by the component applications. Finally, the last question looks at how each application touches the device(s) that it manages. By examining the communication protocols being used, we can compile a list of requirements that ensures a successful deployment of VMS. For the sake of clarity, we will examine each of the questions on a product/server basis.

Note: The components of a Cisco network infrastructure are diverse and varied. However, for the purposes of a discussion surrounding security, we are only focusing on five classes of objects: Cisco IOS routers, PIX firewalls, VPN concentrators, IDS sensors, and host-based Security Agents. This does not imply that VMS is not able to manage other elements, simply that these are the pieces that require special attention.

A Word About Management Subnets (Out-of-Band Management)

In many networks, it is desirable to design a separate management subnet. This is commonly referred to as out-of-band management and describes a situation where your management stations reside on an isolated subnet separate from the network elements that they are trying to manage. This is attractive to many network administrators due to the inherent higher level of security and clear functional division within their network.

As is the case with all network management tools, however, VMS requires network access to the devices that it is trying to manage. So when making this decision, consider that, while it might be desirable to have a completely isolated management subnet, it will do you no good unless there is IP connectivity to the rest of the network. This must be carefully planned out when deploying VMS in such an environment.

CiscoView (delivered within Common Service)

1. What is the management function?

CiscoView provides graphical web-based device management. Users of CiscoView are able to see a graphical representation on their computer screen. This tool allows you to monitor real-time device status, and in certain cases make configuration changes to those devices. From a VMS perspective, CiscoView is positioned as a troubleshooting tool. If there is a problem within the network and that problem has been isolated to a single device or interface, then CiscoView can be used to look at the statistics associated with that device and consider potential configuration variable(s) to solve the problem.

2. What devices does it manage?

CiscoView provides support for the majority of Cisco IOS routers, Cisco Catalyst switches, VPN 3000 concentrators, and the PIX family.

3. Which services do I need to enable? (Application protocol requirements)

CiscoView relies entirely on Simple Network Management Protocol (SNMP) get/set operations (UDP port 161) for its functionality. From the CiscoView server to the device, you need to enable SNMP traffic. Furthermore, the devices that you are managing must be configured to support SNMP. Cisco IOS Software devices can support both get and set operations (for both monitoring and configuration), so both read and write community strings are configured separately to provide this level of granularity. For the VPN 3000 concentrators and the PIX firewalls, only SNMP read operations are supported, so while you can monitor these devices, configuration using CiscoView is not possible.

RME

1. What is the management function?

A description of the functions of RME would take an entire paper by itself. In general (and from a security perspective), the purpose of this application is for basic network management operations and administration. This tool provides:

- Inventory management to keep track of the devices in your infrastructure
- Configuration management to manage the configurations of your network devices
- Change audit control to keep track of any changes (configuration or otherwise) occurring in the network
- Software image management to facilitate the maintenance of software versions
- Syslog management to receive and analyze syslog messages sourced from the network devices

As this list shows, RME functionality provides benefit beyond the scope of security infrastructure management. In our case, however, we focus on the benefits that it provides to our environment. Of special interest is the fact that RME can generate configuration reports, software image upgrade analysis, and syslog reports specific to VPN-related infrastructure and environments.








2. What devices does it manage?

RME provides support for Cisco IOS routers, VPN 3000 concentrators and PIX Series. The caveats are that for the concentrators, RME does NOT support configuration management and only provides limited support for software image management. For PIX firewalls, RME provides limited support for syslog management. If you refer back to the diagram of our reference topology (Figure 1), you will see that this essentially covers all aspects of our network with the exception of the IDS sensor. For this reason, RME is frequently referred to as our “core” management application.

3. Which services do I need to enable? Application protocol requirements

RME depends on several protocols to manage its devices. These include SNMP, Telnet, TFTP, and Syslog, among others. Because the subcomponents of RME are so varied, along with the different devices, the application protocol requirements for this tool are summarized in Table 10.

Table 10. CiscoView and RME Protocol Requirements

Application	Traffic Flow	Service(s)	TCP/UDP Port Number
CiscoView		SNMP	UDP 161
Inventory Manager		SNMP	UDP 161
Configuration Manager		Telnet TFTP SNMP	TCP 23 UDP 69 UDP 161
Software Image Manager		Telnet TFTP SNMP	TCP 23 UDP 69 UDP 161
Change Audit Services		Syslog	UDP 514
Availability Manager		Telnet SNMP ICMP	TCP 23 UDP 161 N/A
Syslog Analyzer		Syslog	UDP 514

Based on this matrix, it is important to make sure that the devices you are managing with RME are configured to provide the proper information. SNMP read (and write where applicable) community strings need to be configured. The Telnet service along with a login password needs to be enabled. Finally, the devices need to be configured to point their syslog messages at the RME server.

Common Services

1. What is the management function?

Common Services is a server environment that provides a common set of services and management functions to a suite of client applications—the Management Centers. These services and functions include the following:

- Data storage and management
- A web infrastructure
- Session management

- User authentication and permission management
- Common environment for multiple client applications

You must install Common Services on your server before you can install any of the Management Centers, Security Monitor, or AUS. These applications integrate with Common Services and use the services and management functions provided by Common Services.

2. What devices does it manage?

Since Common Services simply provides the server environment, it does not directly manage any particular network devices. The management is typically handled by the applications that sit on top of Common Services.

3. Which services do I need to enable? (Application protocol requirements)

Common Services is responsible for the web infrastructure of the VMS Management Center applications, so in terms of application protocols, it is important to maintain the connection from the web client to the web server. Typically, this will be HTTP and HTTPS traffic through pre-assigned port numbers:

- TCP 1741—HTTP port for CW desktop login session
- TCP 1742—HTTPS port for CW desktop login session
- TCP 443—HTTPS port for all MCs and AUS user web session
- TCP 1751—HTTP port for AUS OS and PDM image download

For a comprehensive list of TCP and UDP port numbers used by Common Services, consult the product documentation, *Installing CiscoWorks Common Services on Windows 2000*.

Management Center for VPN Routers

1. What is the management function?

The purpose of Router MC is to provide an easy management interface to set up and maintain VPN connections between multiple supported Cisco IOS Software devices in a hub-and-spoke topology. Router MC also provides configuration support for the PIX Firewall feature set on Cisco IOS Software devices, except Cisco Catalyst 6000 Series switches. Router MC allows network managers to quickly and easily provision all critical connectivity, security, and performance parameters for a site-to-site, large-scale VPN. Utilizing a point-and-click web-based interface and preconfigured components for VPN creation, Router MC also allows the quick configuration of smaller, simpler VPNs. In addition to configuring hub-and-spoke VPNs, Router MC also lets you replace leased-line connections with VPN connections, or prepare VPN configurations for routers not yet on the network

2. What devices does it manage?

Router MC is used to manage VPNs across Cisco IOS routers and VPN Service Modules in Catalyst switches. In general, the application is hardware-platform agnostic. It only cares about the version of Cisco IOS Software and the supported feature set. The basic rule is that the routers have to support IPSec, Secure Shell Protocol (SSH), and named access lists. Table 11 lists the Cisco IOS Software versions that have been tested with Router MC.

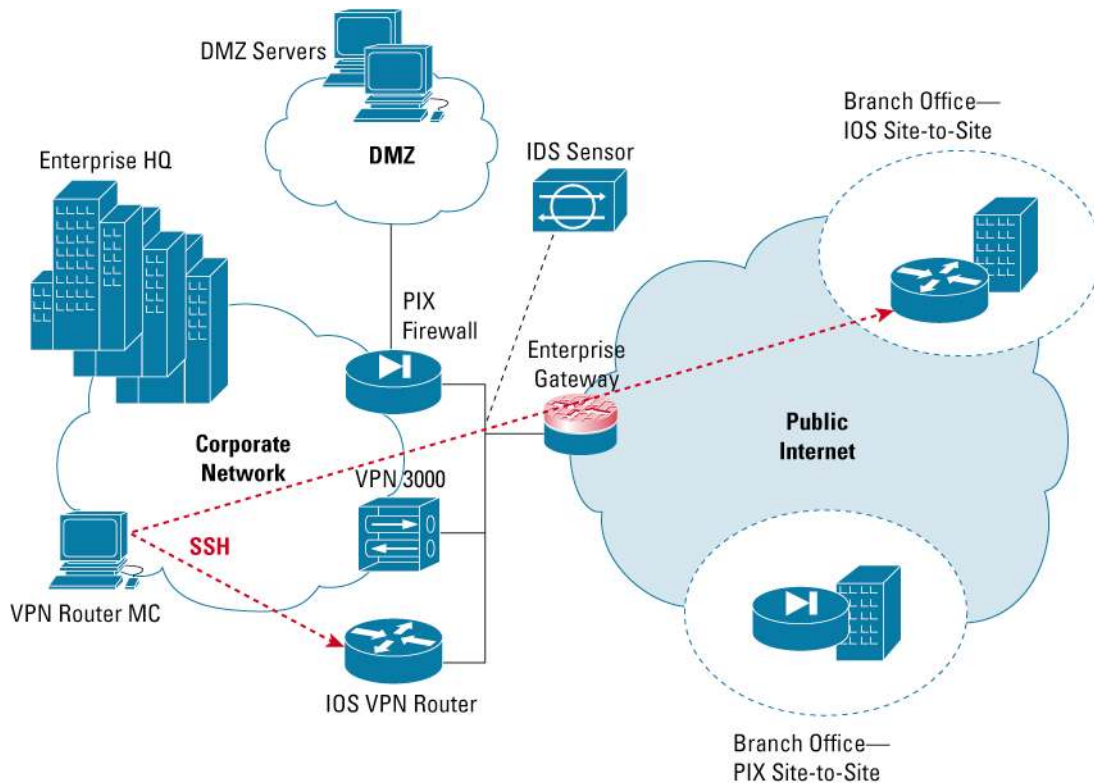
Table 11. Supported Cisco IOS Software Versions in Router MC

Cisco IOS Software Platform	Minimum Cisco IOS Software Version
7100, 7200 (Hub)	12.1(9)E
7400 (Hub)	12.1(9)YE
3620/40/60 (Hub)	12.2
71xx/72xx/74xx (Spoke)	12.1(9)E
XM 2600/10/11/20/21/22/50/51/91 and 3620/40/60	12.2
1710/20/21/50/51/60 (Spoke)	12.2
803, 806, 831, 826, 827 (Spoke)	12.2
3725, 3745	12.2
Catalyst 6500 with VPN Service Module	12.2(9)YO1

3. Which services do I need to enable? Application protocol requirements

Router MC uses SSH (TCP port 22) to configure the Cisco IOS routers. The SSH session is established when devices are initially imported into Router MC. Then, when configurations are pushed out to the devices, this session is also encrypted using SSH. Figure 5 provides an illustration of how Router MC is applied to our reference topology.

Figure 5. Router MC Applied



Management Center for Firewalls

1. What is the management function?

Firewall MC is a policy tool that enables you to manage your PIX Firewalls and Catalyst Switch Firewall Service Modules by configuring new firewalls and importing configurations from existing firewalls or configuration files. You can configure firewall device settings, access rules, and translations rules. These configuration changes can then be deployed to the firewalls on your network. Firewall MC also provides a powerful tool for controlling changes made to your network, showing configuration and status changes.

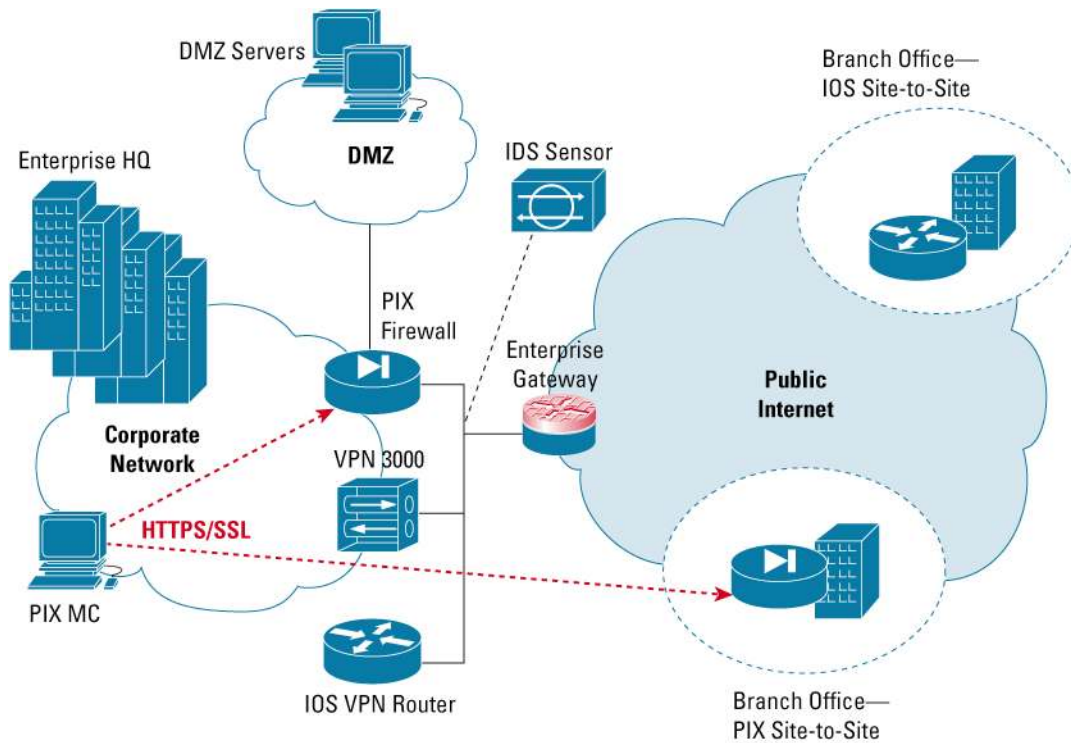
2. What devices does it manage?

Firewall MC is used to manage the PIX firewalls and firewall service modules deployed throughout your network. These include all the PIX platforms: 501, 506E, 515E, 525, and 535, and the Catalyst Firewall Service Module. Supported versions are PIX 6.0.x up to 6.3.4 and FWSM from 1.1.x up to 2.3.1.

3. Which services do I need to enable? (Application protocol requirements)

Firewall MC uses an encrypted session to manage its PIX Firewall devices and service modules. The protocol that it uses is SSL (or HTTPS) and the port number assigned for this connection is TCP port 443. Therefore, it is necessary to permit TCP 443 to a PIX Firewall (from the management interface) in order for Firewall MC to properly manage the device. Figure 6 provides an illustration of how Firewall MC is applied to our reference topology.

Figure 6. Firewall MC Applied



Auto Update Server

1. What is the management function?

AUS is responsible for storing configurations and software images for PIX firewalls. Firewalls operating in auto-update mode periodically contact AUS to upgrade software images, configurations, and versions of PDM, and to pass device information and status to AUS. Using AUS also facilitates managing devices that obtain their addresses through Dynamic Host Configuration Protocol (DHCP) or that sit behind NAT boundaries. Typically, because of this management function, the AUS is deployed in a publicly accessible DMZ which the remote site PIX firewalls can contact directly.

2. What devices does it manage?

Firewall MC is used to manage the firewalls deployed throughout your network. These include all the PIX platforms: 501, 506E, 515E, 525, and 535, and Catalyst Firewall Service Modules. AUS requires the firewalls to be running OS version 6.2 or later because it requires the Auto Update feature.

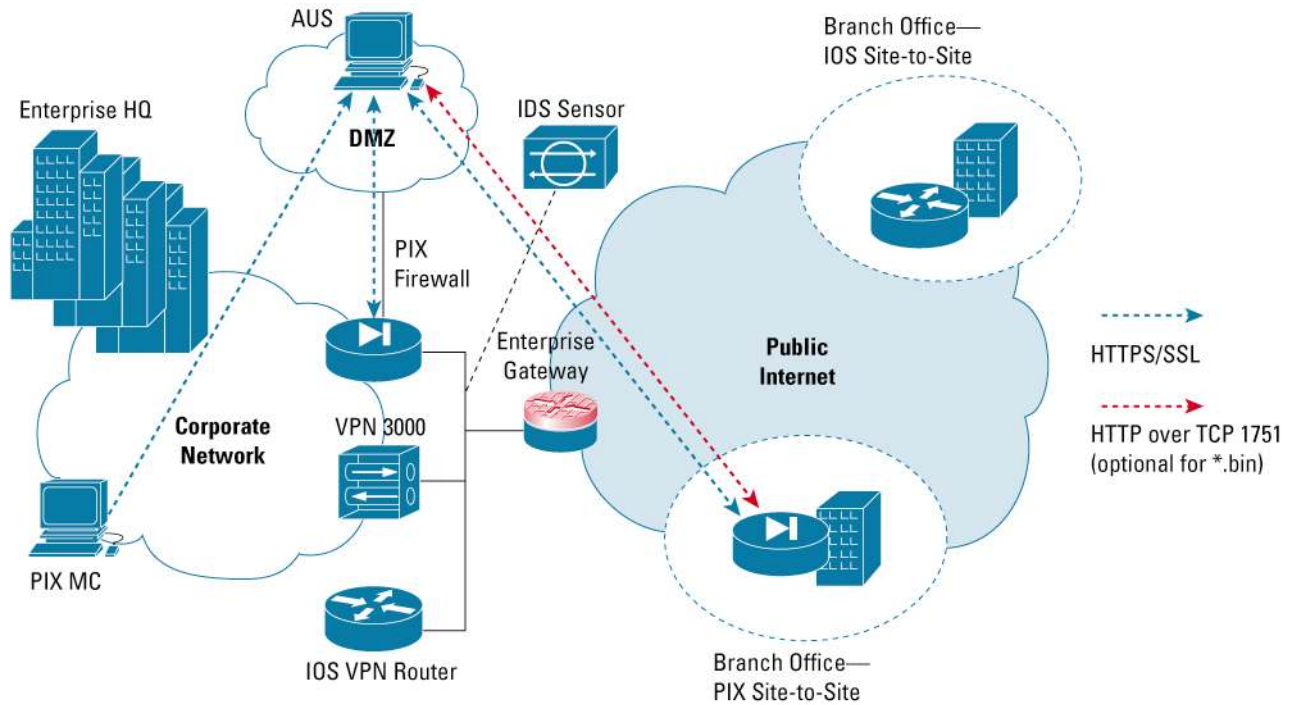
3. Which services do I need to enable? (Application protocol requirements)

AUS talks to two different pieces in our topology diagram. The first piece it talks to is the Firewall MC server. If these two applications are installed on the same system, you do not need to worry about the communication architecture. However, if they are installed on different servers, then you should be aware that the Firewall MC will push configuration files to AUS using SSL. Therefore, it is necessary to open up TCP 443 to the AUS system.

The second piece is the actual communication between the AUS and the PIX Firewall itself. In this scenario, there is two-way communication and both occur through SSL. Therefore, it is not only necessary to open up TCP 443 to the AUS from the PIX Firewall, but also vice versa. For

transfer of binary images (PIX and PDM software), this will be transferred using standard HTTP over TCP 1751 (this can optionally be changed to SSL). Figure 7 illustrates how AUS is applied to our reference topology.

Figure 7. AUS Applied



Management Center for IDS

1. What is the management function?

IDS MC manages configurations for Cisco IDS sensors. Through a series of web-based screens, you can manage all aspects of sensor configuration. You can manage individual sensors or a group of sensors having a common configuration. The sensor configuration data resides in a database. IDS MC can also perform signature updates by downloading the update archives from the Cisco Web location and then distributing these signature updates to the appropriate sensors.

A separate but closely related product, Monitoring Center for Security (Security Monitor), provides event collection, viewing, aggregation, correlation, and reporting capability for network devices. This is covered in the next section.

2. What devices does it manage?

IDS MC manages the Cisco IDS appliance sensors, the Cisco IDS Module for the Catalyst 6500 and for the Routers (NM-IDS) and the IPS IDS feature on the routers. The IDS software required for the application is determined by the platform (Table 12).

Table 12. Required IDS Sensor Software for IDS MC

IDS Sensor Platform	Minimum Required Software
3.x Cisco IDS Appliance Sensor	3.0.1
4.x Cisco IDS Appliance Sensor	4.0.1
IPS IDS for 800, 1700, 2600, 2691, 3600, 3725, 3745, 7200	12.3(8)T4
Catalyst 6000 IDS Module (IDSM-1)	3.0.5
Catalyst 6500 IDS Module (IDSM-2)	4.0.1
Module for 2600XM, 3660, and 3700 Series Routers (NM-IDS)	4.0.1

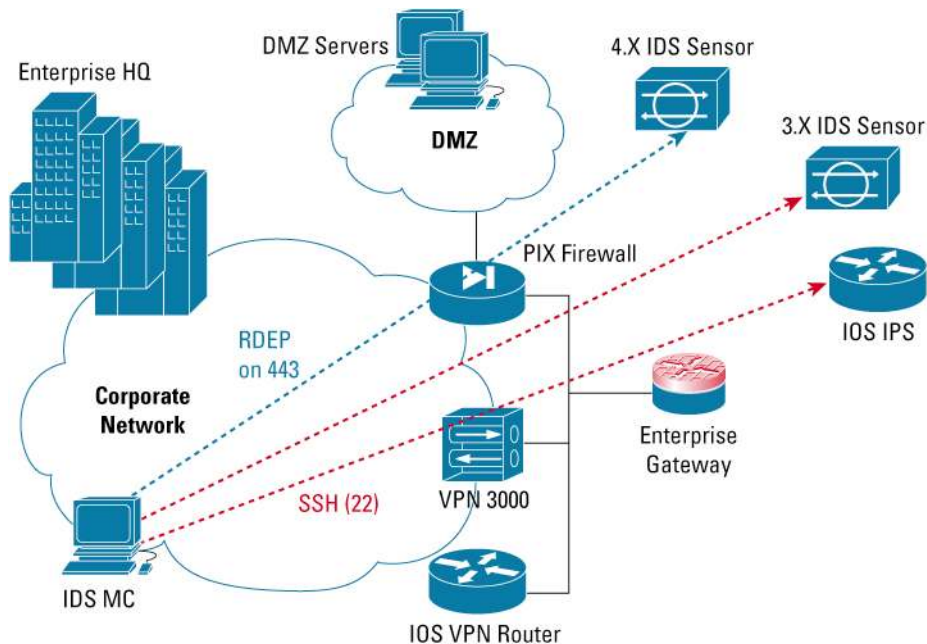
3. Which services do I need to enable? Application protocol requirements

IDS MC uses two protocols to manage the IDS

- **RDEP** is used for 4.x sensor for import and deployment of the configuration. RDEP uses port 443
- **SSH** for IOS IDS and 3.x sensors. SSH uses port 22 to connect to the device.

Figure 8 illustrates how IDS MC is applied to our reference topology.

Figure 8. IDS MC Applied



Security Monitor

1. What is the management function?

The Security Monitor provides a web-based real-time interface for event collection, viewing, aggregation, correlation, and notification for the following devices:

- Cisco Intrusion Detection System Sensors (both 3.x and 4.x)
- Cisco IDS Service Modules on Catalyst switches (both IDSM-1 and IDSM-2)
- Cisco IDS Service Module on Routers
- Cisco IOS Router running IDS software
- Cisco Security Agents (forwarded by Cisco Security Agent MC)
- PIX Firewall
- Cisco Firewall Service Modules on Catalyst switches
- Another Security Monitor server.

The Security Monitor events are displayed on a customizable event viewer. Security Monitor also allows you to write some basic event correlation rules to consolidate events. These rules can also be set up to provide real-time notifications.

2. What devices does it manage?

Security Monitor can receive security events from five sources with the following software requirements (Table 13).

Table 13. Required Software for Security Monitor Devices

Security Event Source	Minimum Software Required
3.x Cisco IDS Appliance Sensor	3.0.1
4.x Cisco IDS Appliance Sensor	4.0.1
IDS Module for Routers (NM-IDS)	4.0.1
Catalyst 6500 IDS Module (IDSM-1)	3.0.5
Catalyst 6500 IDS Module (IDSM-2)	4.0.1
Cisco IOS Router	Cisco IOS Software with IDS features set
PIX Firewall	Any version that supports syslog
Catalyst 6500 Firewall Module	1.x or 2.x
Cisco Security Agent MC	4.0
Security Monitor	SecMon 2.0

3. Which services do I need to enable? Application protocol requirements

Since the Security Monitor has so many data inputs, it is necessary to consider each of these individually in terms of application protocol requirements.

For 3.x sensor appliance and IDSM-1 IDS service module, Security Monitor uses PostOffice protocol to receive events from devices.

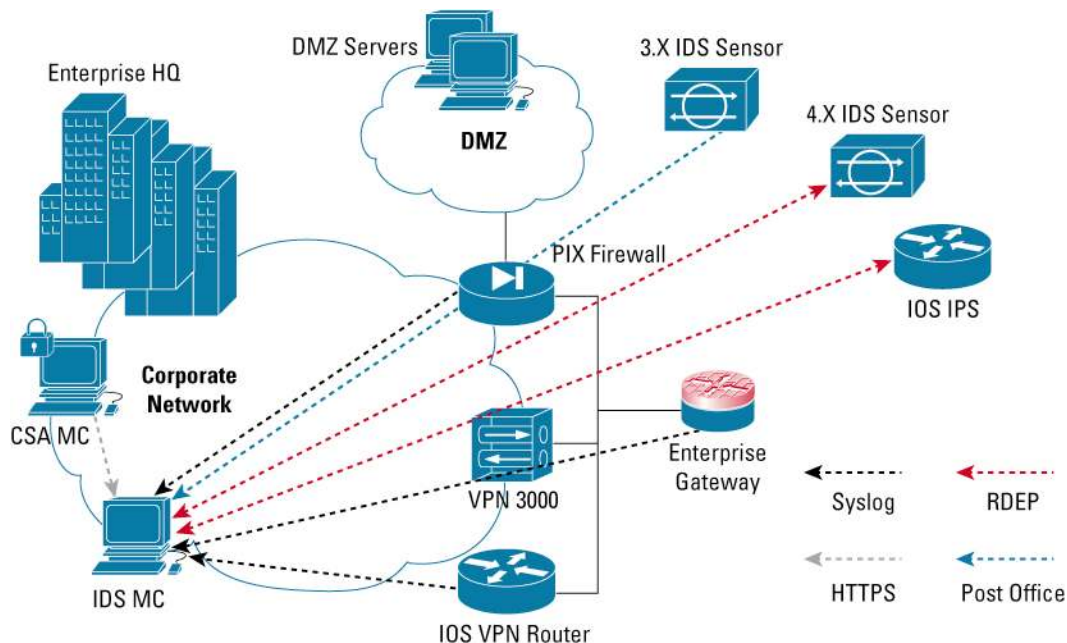
For 4.x sensor appliance, IDSM-2, IDS service module Security Monitor uses RDEP, which based on HTTPS, to pull events from devices, while for IOS IPS and other SecMon servers, Security Monitor uses SDEE.

For Cisco Security Agent, Security Monitor use HTTPS to pull events from Cisco Security Agent MC.

For the other data sources (PIX firewalls, and Firewall Service Module), the events are sent to Security Monitor through syslog.

This means you must allow PostOffice (UDP 45000) and syslog (UDP 514) to the Security Monitor server, while RDEP (TCP 443), HTTPS (TCP 443) from Security Monitor to the devices. Figure 9 illustrates how Security Monitor is applied to our reference topology.

Figure 9. Security Monitor Applied



Monitor Center for Performance

1. What is the management function?

Monitoring Center for Performance 2.0.1 (Performance Monitor) is a browser-based tool that monitors and troubleshoots the health and performance of enterprise network security services. Performance Monitor replaces the VPN Monitor 1.2 application. Supported service types are remote-access VPN, site-to-site VPN, firewall, web server load-balancing, and proxied SSL. It enables you to increase service availability by isolating, analyzing, and troubleshooting significant events in your network as they occur. Performance Monitor does not require expertise with IPSec or other security technologies.

2. What devices does it manage?

Supported service types are remote-access VPN, site-to-site VPN, firewall, web server load-balancing, and proxied SSL.

Table 14. Supported Services and Required Software for MCP

Series	Supported Devices	Software Versions	Supported Services
Cisco VPN Routers	7100 and 7200 series	IOS 12.1(8)E, (12.2(8)T8, 12.3(5b), and later	Site-to-Site VPN
	7400 series	IOS 12.2(15)B, 12.2(9)YE, 12.3(4)T2, and later	Site-to-Site VPN
	3700 series	IOS 12.2(13)T, 12.3(5b), and later	Site-to-Site VPN
	800 series	IOS 12.2(13)T, 12.3(2)T, and later	Site-to-Site VPN
	1700 series	IOS 12.2(13)T, 12.3(5b), and later	Site-to-Site VPN
	2600 and 3600 series	IOS 12.2(13)T, 12.3(5)A, and later	Site-to-Site VPN
Cisco Catalyst 6500 Switches	Firewall Service Module	1.1(1), 1.1(2), and 1.1(3) with IOS 12.2(14)SY, 12.1(13)E, and later on SUP 2 12.2(17b)SXA, 12.2(14)SX1, and later on SUP 720	Firewall
	VPN Service Module	12.2(14)SY, 12.2(9)YO1, and later on SUP 2 12.2(17b)SXA and later on SUP 720	Site-to-Site VPN
	SSL Service Module	1.1(1), 1.2 with IOS 12.1(13)E, and later on SUP 2 12.2(14)SX1 and later on SUP 720	SSL
	Content Switching Module (Load Balancing)	3.1, 3.2 with IOS 12.1(13)E and later 12.2(14)SX1 and later on SUP 720	Load Balancing
Cisco PIX Firewall	PIX 501, PIX 506E, PIX 515, PIX 515E, PIX 525, PIX 535	PIX 6.0 and later	Firewall
Cisco VPN Concentrators	3000 series	3.0 and 4.1 and later	Remote Access VPN

3. Which services do I need to enable? (Application protocol requirements)

MCP requires mostly SNMP (UDP port 162) and HTTPS to function. The MCP server will periodically poll the devices to retrieve the IPsec MIB information, while for firewalls some of the information are also retrieved using HTTPS connections to the PDM code.

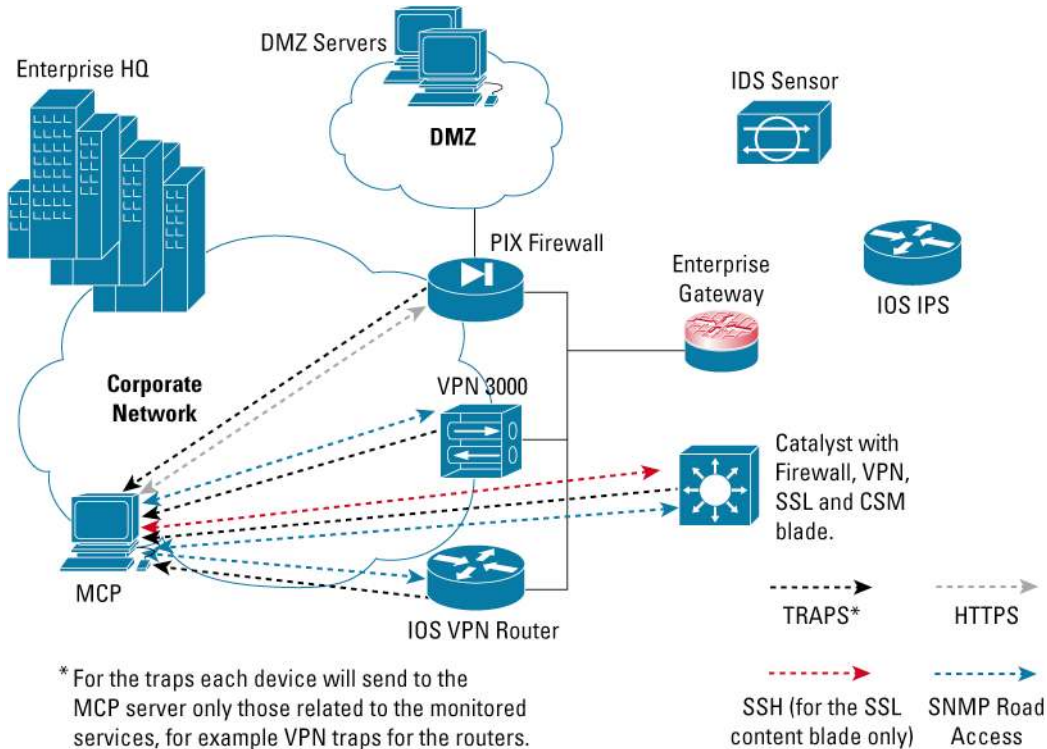
MCP supports different devices and for each of them different services need to be enabled; here is a list of them:

- **VPN 3000 Concentrators:** enable SNMP, HTTPS(for user logout feature), XML interface(to get cluster detail), syslogs (for user login details)
- **VPN Router:** Enable SNMP and VPN related traps
- **Catalyst 6500 + CSM module:** enable SNMP and CSM related traps

- **Catalyst 6500 + VPN module:** enable SNMP and VPN related traps
- **PIX and Catalyst 6500 + FW module:** enable SNMP, HTTPS server and HTTPS access and syslogs
- **Catalyst 6500 + SSL:** enable SSH access

Figure 10 illustrates how VPN Monitor is applied to our reference topology.

Figure 10. MCP Applied



Note: Given these requirements, it is possible to use MCP on a remote VPN device. However, this may not be entirely practical for two reasons: First, this type of monitoring does not scale as well. Second, in most cases it is sufficient to view the VPN metrics from one end of the tunnel (and not both).

Cisco Security Agent MC

1. What is the management function?

The Cisco Security Agent MC is a product that complements the network-based IDS management provided in IDS MC and Security Monitor and gives VMS a truly comprehensive solution to manage intrusion detection. The purpose of Cisco Security Agent is to protect individual host systems from intrusion. The agent sits on the host itself and examines system calls to the OS kernel, comparing these to a database of predefined rules and policies. Events are reported back to a central Cisco Security Agent Management Center, which consolidates the information from the agents it is managing. If a rule match is found, Cisco Security Agent has the ability to either prevent the operation or prompt the user for permission, and at the same time shoot off a real-time notification.

This model of protection has been proven to mitigate well-known threats such as Sasser, Bagle, Blaster, MyDoom and many other exploits without the need of any user configuration. As such, the Cisco Security Agent is especially important to use on your important network hosts—which is at your discretion. In our reference topology, we recommend installing the Cisco Security Agent code on all the network management

servers that comprise the VMS solution, thus protecting your important network management systems. And we recommend installing Cisco Security Agent on all the DMZ servers as well as remote desktops and laptops. These servers or desktops will report security events back to the Cisco Security Agent MC, which can then be forward to Security Monitor.

2. What devices does it manage?

The Cisco Security Agent does not directly interact with Cisco network devices; however, it does interact with network hosts using the Cisco Security Agent kit installed. At present, the following OS versions are protected:

- Windows 2003
- Windows XP (SP0 pr SP1)
- Windows 2000 Professional, Server, Advanced Server (SP 0, 1, 2 or 3)
- Windows 2003
- Windows NT Workstation, Server or Enterprise Server (SP5 or higher)
- Solaris 2.8 (64-bit kernel)
- RedHat Enterprise Linux 3.0

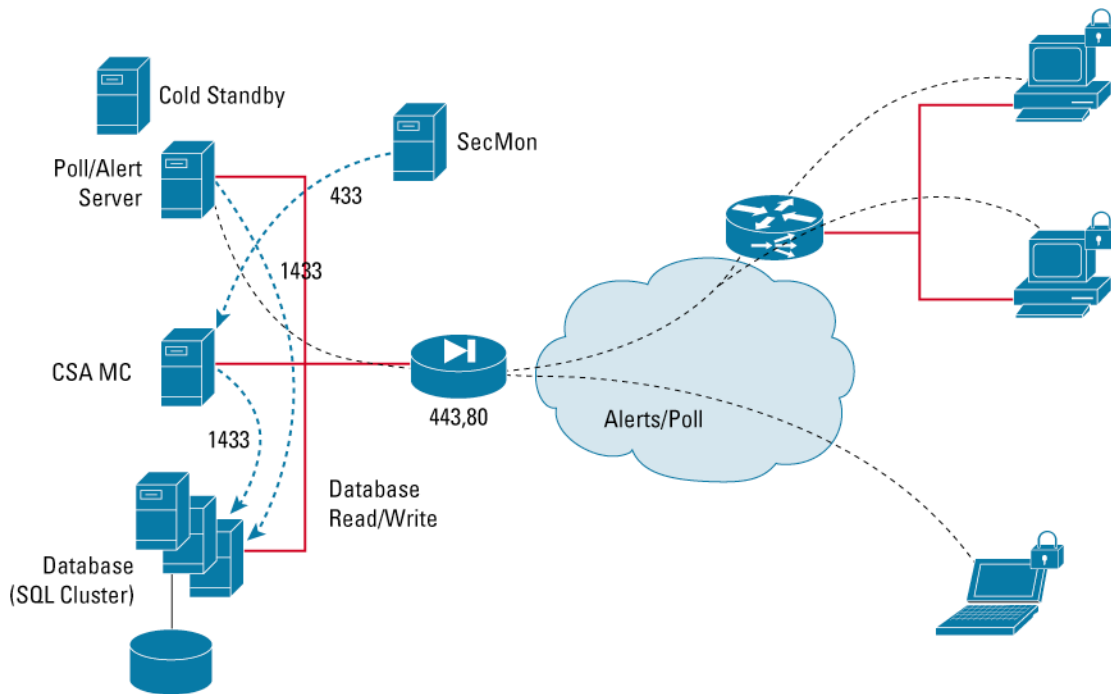
It is recommended that you consult the product documentation to verify the current available option of the Cisco Security Agent software.

3. Which services do I need to enable? Application protocol requirements.

For Cisco Security Agent to work properly, the agents must be able to communicate with the Management Center. This is necessary so that the agents can report security events to the Management Center, and just as importantly, so that the Management Center can make policy configuration changes for the agents and agents will periodically get the latest policies from the Management Center. This communication is accomplished through standard HTTP and HTTPS. Figure 11 illustrates how the Cisco Security Agent Management Center is applied to our reference topology.

Monitor Center for Cisco Security Agent now has the capability to install the database in a remote cluster in order to have a better scalability and allow the support for up to 100,000 devices. If this is done, the communication between the VMS server and the server with the database will be over ODBC to SQL server, and the database listener port will be 1433.

Figure 11. Cisco Security Agent MC and Agents Applied



Putting It All Together

Clearly, it is important to determine where to deploy the various components of VMS, and distinguish what elements of the network infrastructure each piece manages. Table 15 summarizes the information presented in this section along with the associated management protocols that must be enabled in order for the applications to function properly.

Table 15. Summary of VMS Components Applied

Application	Protocols	TCP/UPD Port Numbers
CiscoView	SNMP	UDP 161
RME	SNMP, Telnet, TFTP, Syslog	UDP 161, TCP 23, UDP 69, UDP 514
Firewall MC	HTTPS (SSL)	TCP 443*
AUS	HTTP, HTTPS, CNS	TCP 1751, TCP 443, TCP 11011
Router MC	SSH	TCP 22
IDS MC	SSH, SCP	TCP 22, TCP 443, TCP 69 (tftp) is required on Solaris
Security Monitor	PostOffice, RDEP, HTTPS	UDP 45000, TCP 443, Syslog 514, TCP 69 (tftp) is required on Solaris
MCP	HTTPS, SNMP	TCP 443, UDP 161
Cisco Security Agent MC	HTTP, HTTPS, ODBC	TCP 80, TCP 443, TCP 1433

* This port number is customizable. TCP 443 is the default value.

CAVEATS AND GOTCHAS

When deploying VMS, it is important to realize the specific services required by each individual application. These are outlined in the previous section. In certain instances, two different applications may require the same type of access to a particular device (for example, CiscoView and VPN Monitor both use SNMP to retrieve the management information). Additionally, because some of the applications within VMS have a security focus, sharing access to a device can be a potentially contentious situation. This section outlines important considerations should you deviate from the deployment guidelines provided in this document.

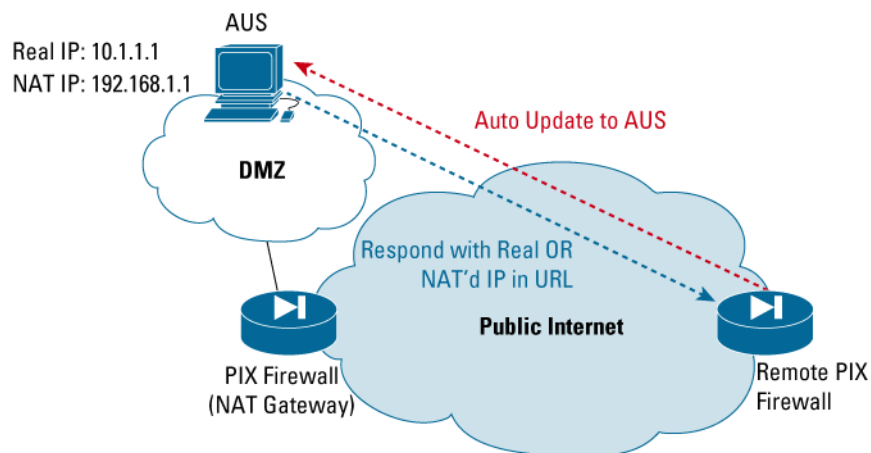
Considerations with NAT

NAT is used in many topologies. Although this is a great feature for security and address space conservation, it can create some problems with management tools. This section discusses some of the caveats and issues you may run into when you deploy VMS into a network environment with NAT.

- NAT and AUS

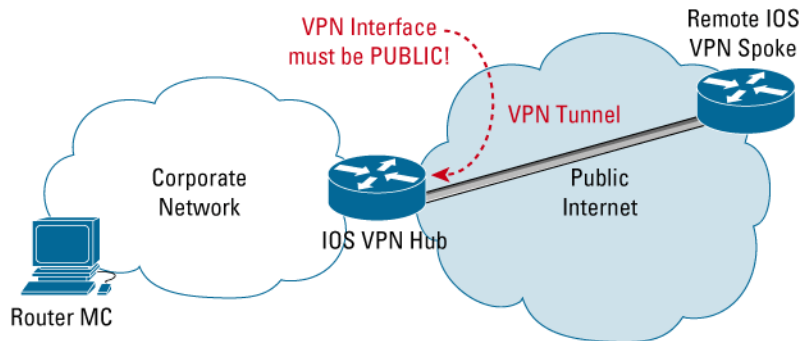
- If you are using the AUS application and the server is sitting behind a NAT gateway, then you have to pay special attention to the PIX firewalls that you are managing. Consider a remote PIX that contacts the AUS server. It will actually contact the NAT address (not the real address). When the AUS responds with the proper URL to download the updated configuration or software image, it will use the NAT address. Conversely, if the AUS is NOT behind a NAT gateway, you could configure it to provide its real address. You need to decide whether to use the NAT address or the real address for ALL the PIX firewalls you are managing—and you cannot mix the two (NAT and non-NAT) within a single installation of AUS (Figure 12).

Figure 12. NAT and AUS



- If you have instances in which you need to manage PIX firewalls (both internal and external), it is recommended to install two copies of AUS—one for the external firewalls that will use the NAT address and one for the internal firewalls that will use the real IP address. The NAT setting is configured under the Admin tab in AUS.
- NAT and Router MC (Hub Side)
 - If you are using Router MC to set up a hub-and-spoke VPN environment, you must be careful about the hub router VPN interface. Because of the way the product is designed, this interface address cannot be NATed. The VPN termination interface must be a publicly addressable IP subnet. This is because, if the interface address is NATed, then from the perspective of the peer, you would need to assign it the NATed address. However, the Router MC application only allows you to assign by interface and not IP address—so the peer statements will be incorrect. Refer to Figure 13 to see how the VPN topology must be built for compatibility with Router MC. (You can put the hub router behind a NAT device, but the hub router's IP must not be NATed).

Figure 13. NAT and Router MC



- NAT and Router MC (Spoke Side)
 - There is also a deployment caveat with NAT and VPN spoke devices. Router MC needs to manage the spoke devices (VPN peers) with their real IP address because the current version of Router MC does not support the situation where the spoke’s IP address is NATed. (You can put the spoke router behind a NAT device, but the spoke router’s IP must not be NATed.)
- NAT and IDS MC (IDSMC server behind NAT)
 - In this case the user have to specify the IP address that the device has to use to contact the MC. This can be done at import time: while is the import wizard, in the “Enter sensor information” page, you have to enter the IP address that the sensor has to use to contact the MC in the “NAT address to MC” field at the bottom of the page.
- NAT and IDS MC (Sensor behind NAT)
 - In this case, the only action needed is to specify the public address for the sensor at import time

Multiple Syslog Daemons

Several applications within the VMS bundle can receive syslog messages from various sources. With our modified OS support, we can also install all of these applications on a single server. In this scenario, we need to determine how to make all of these syslog daemons compatible.

First, let’s take a look at which applications can receive syslog messages and from which devices (Table 16):

Table 16. Summary of Syslog Server Applications in VMS

VMS Module	Syslog Source
RME	Cisco IOS Software, PIX, VPN3K
Security Monitor	Cisco IOS Software, PIX, Firewall Service Module
MCP	Cisco Firewalls and FWSM, Cisco VPN 3K

By default, all of these applications listen on UDP port 514. This is not a problem if these applications are split across different servers—you would simply send syslog messages to multiple sources. However, what happens when all of these applications are installed on a single system AND the customer wants to take advantage of all three syslog daemons?

There are two ways Security Monitor can alleviate this problem. First, you can configure the port number it should listen to for syslog messages. It is UDP 514 by default, but that can be changed. You can also set up Security Monitor to forward the syslog messages to another port on that same system or other systems. The other important factor is that PIX firewalls can send syslog messages to the same host, but different port numbers. In this situation, here is what you could do to maximize the syslog functionality:

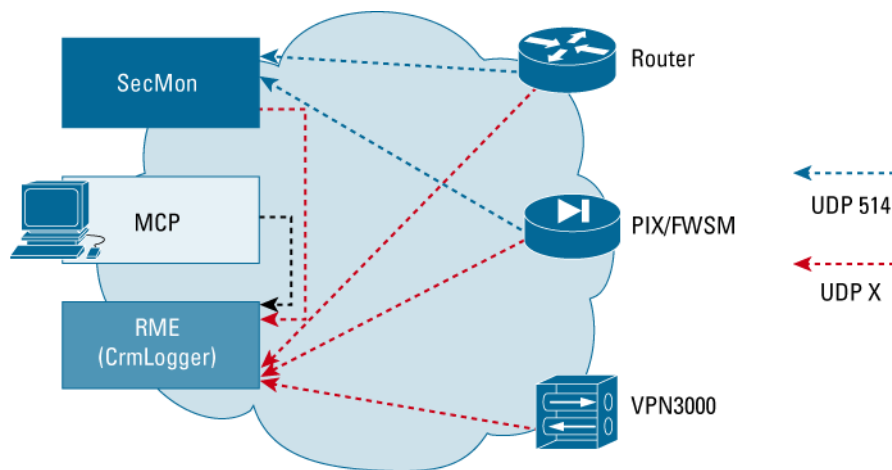
- From Cisco IOS Software, send syslog to RME at UDP X
- From PIX, send syslog to Security Monitor at UDP 514 and to MCP port Y
- From Security Monitor, forward syslog to RME at port X

The port on which syslog is received is not important to MCP as it is simply reading the messages from the crmlogger file. On installation, SecMon records the port on which crmlogger is listening and automatically forwards messages to this file.

MCP is simply reading the file and filtering the messages it is interested into.

See Figure 14 to visualize this consolidation.

Figure 14. Syslog Consolidations in VMS



Ideally, if you have at least two servers in this scenario then you can take advantage of all three tools. The first box would be running Security Monitor while the second system would be running RME.

Cisco Security Agent Initial Deployment

A major component of the VMS bundle is the ability to manage intrusion detection and prevention on a host level. The management servers for VMS should definitely be considered critical, and we recommend that you install the Cisco Security Agent software on these systems. A default policy group “VMS server” is also included in the Cisco Security Agent MC of VMS bundle.

When initially deploying the agent kits, we recommend putting the agent in “Testing Mode,” which only logs any rule violation without actually taking any action. Use “Testing Mode” for the first several weeks of regular use so you can develop baseline policies based on the events received during the testing period.

Out-of-Band Management

In many networks, it is desirable to design a separate management subnet. This is commonly referred to as out-of-band management and describes a situation where your management stations reside on an isolated subnet separate from the network elements that they are trying to manage. This is attractive to many network administrators due to the inherent higher level of security and clear functional division within their network.

As is the case with all network management tools, however, VMS requires network access to the devices that it is trying to manage. So when making this decision, consider that, while it seem desirable to have a completely isolated management subnet, it will do you no good unless there is IP connectivity to the rest of the network. This must be carefully planned out when deploying VMS in such an environment.

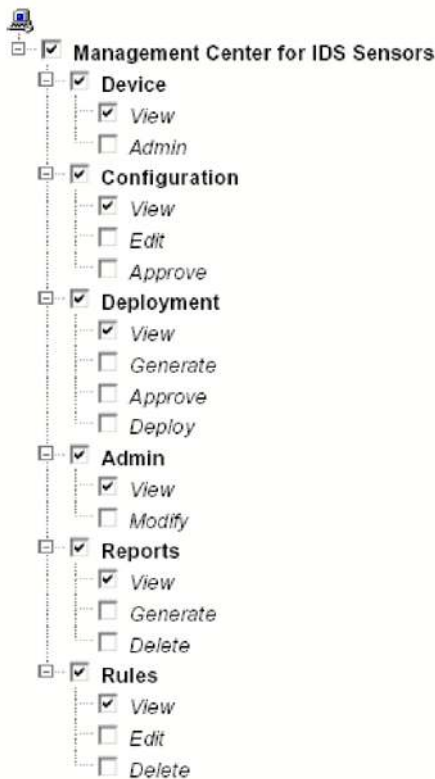
ACS integration for Role-Based Access Control

CiscoWorks VMS has seven built-in user roles (HelpDesk, Approver, Network Operator, Network Admin, System Admin, Export Data, and Developer) and users can have one or multiple roles. Those roles have fixed permission for what the user can do in the GUI.

To implement fine granular and flexible Role-Based Access Control (RBAC), ACS must be used together with VMS to control what the user can exactly do in a very detailed fashion. For example, a Read Only user role in ACS can be configured as shown in Figure 15 (picture taken from ACS).

Note: The VMS components supporting RBAC with ACS are IDSMC, Router MC, FWMC and AUS. Security Monitor and CSAMC cannot integrate with ACS.

Figure 15. Configuration of a Read Only User Role in ACS



VMS 2.X APPLICATION NOTES

1. Slow installation

If Virus Scan is turned on, the installation can be longer due to the Virus scan operations. We recommend that Virus Scan be turned off for a faster installation.

2. Installing VMS2.3 and ACLM n the same server

When ACLM (ACL Manager) is installed over the Common Services 2.2 for VMS, it can no longer communicate with JRM and therefore you can't do any job deployment. Hence it is necessary to install the ACLM "update 1".

3. Installing VMS2.3 and Campus Manager on the same Solaris server

For the following bug CSCsa50466 VMS and Campus manager have problems if they are installed on the same Solaris server. The problem does not exist in case of Windows installation.

First of all before upgrading apply all the latest IDU to the server.

CSCsa50466: Campus Manager unusable on Solaris if VMS 2.3 CS installed.

The workaround is the following:

Apply jrm and corba patch and follow the following steps for setting the proper java.library.path and to locate .so files)

Go to /opt/CSCOpX/objects/dmgt and open the 'dmgtd.conf' file look if you see the following entry in the file.

```
ANIServer y EDS,ANIDbEngine /opt/CSCOpX/campus/jre/bin/java -
Xbootclasspath:/opt/CSCOpX/www/classpath/vbjorb.jar:/opt/CSCOpX/campus/jre/lib/rt.jar:/
opt/CSCOpX/campus/jre/lib/i18n.jar -Xminf0.1 -Xmaxf0.1 -Djava.class.path=/opt/CSCOpX/
campus/
www/classpath/jndi.jar:/opt/CSCOpX/campus/www/classpath/providerutil.jar:/opt/CSCOpX/
campus/www/classpath/dns.jar:/opt/CSCOpX/campus/lib/classpath:/opt/CSCOpX/campus/www/
classpath:/opt/CSCOpX/lib/classpath:/opt/CSCOpX/www/classpath:/opt/CSCOpX/lib/classpath/
servlet.jar -Dvbroker.orb.gcTimeout=90 -Xrs -Xmx512m com.cisco.nm.ani.server.frontend.
AniMain
```

Modify the previous entry with the following:

```
ANIServer y EDS,ANIDbEngine /opt/CSCOpX/campus/jre/bin/java -Xbootclasspath:/opt/CSCOpX/
www/classpath/vbjorb.jar:/opt/CSCOpX/campus/jre/lib/rt.jar:/opt/CSCOpX/campus/jre/lib/
i18n.jar -Xminf0.1 -Xmaxf0.1 -Djava.class.path=/opt/CSCOpX/campus/www/classpath/jndi.jar:/
opt/CSCOpX/campus/www/classpath/providerutil.jar:/opt/CSCOpX/campus/www/classpath/
dns.jar:/opt/CSCOpX/campus/lib/classpath:/opt/CSCOpX/campus/www/classpath:/opt/CSCOpX/
lib/classpath:/opt/CSCOpX/www/classpath:/opt/CSCOpX/lib/classpath/servlet.jar -
Djava.library.path=/opt/CSCOpX/lib:/opt/CSCOpX/campus/lib:/opt/CSCOpX/MDC/lib -
Dvbroker.orb.gcTimeout=90 -Xrs -Xmx512m com.cisco.nm.ani.server.frontend.AniMain
```

Restart the daemons after editing dmgtd.conf file. It is recommended to take a backup of dmgtd.conf file before editing.

4. Configuring Client Java (JRE) and Multiple JRE Versions

On Windows platforms VMS requires Internet Explorer 6.0 with Service Pack 1. VMS also requires that **Cookies** and **JavaScript** be enabled. In addition, your client must have the correct JRE installed, currently JRE 1.4.1_02.

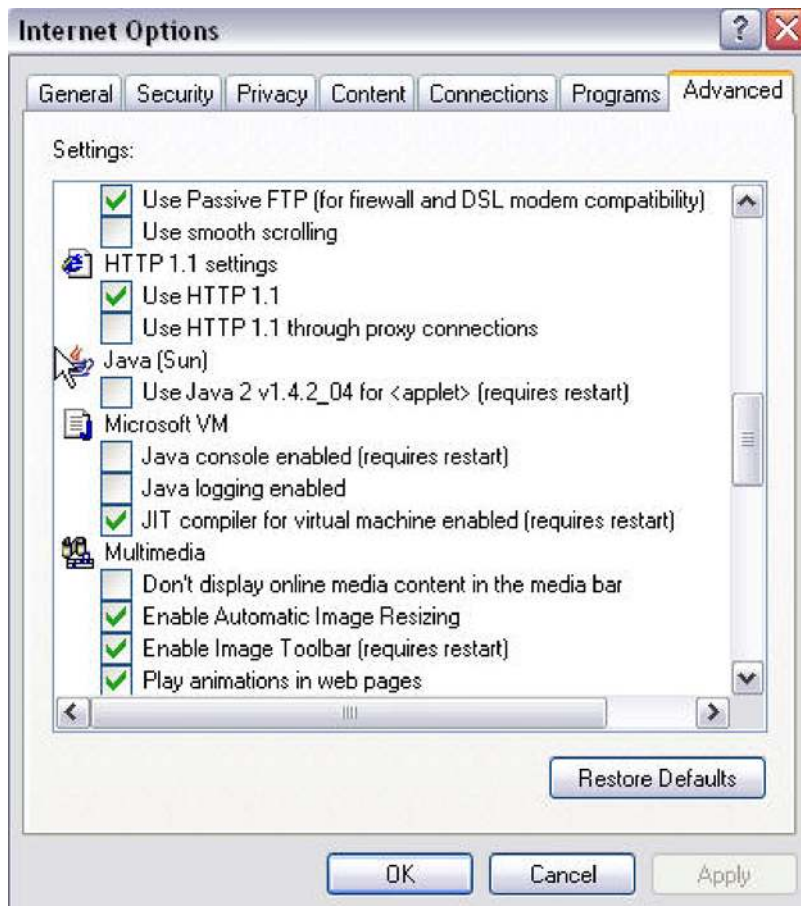
There are two cases that frequently cause problems:

- 1) The browser is inadvertently forced to use an incompatible JRE
- 2) Multiple JREs are installed but not working or configured correctly. We realize that other management products, including those from Cisco, require other JRE versions.

To prevent issues with your JRE we suggest taking two actions:

- 1) Uncheck the “Use JRE...” in your Internet Explorer

In Internet Explorer, go to: Tools -> Internet Options -> Advanced and see what JRE version under the “Java (Sun)” section. Uncheck the “Use Java 2 v1.4.2_04 <applet> (requires restart)” configuration in your browser. This will force the browser to look for other JRE versions that are installed. If the necessary needed JRE is not installed, VMS will then prompt you to install it directly from the VMS server.



2) Use Sun Java Web Start to properly handle multiple JREs on a single system with paths and environmental variables set correctly for each.

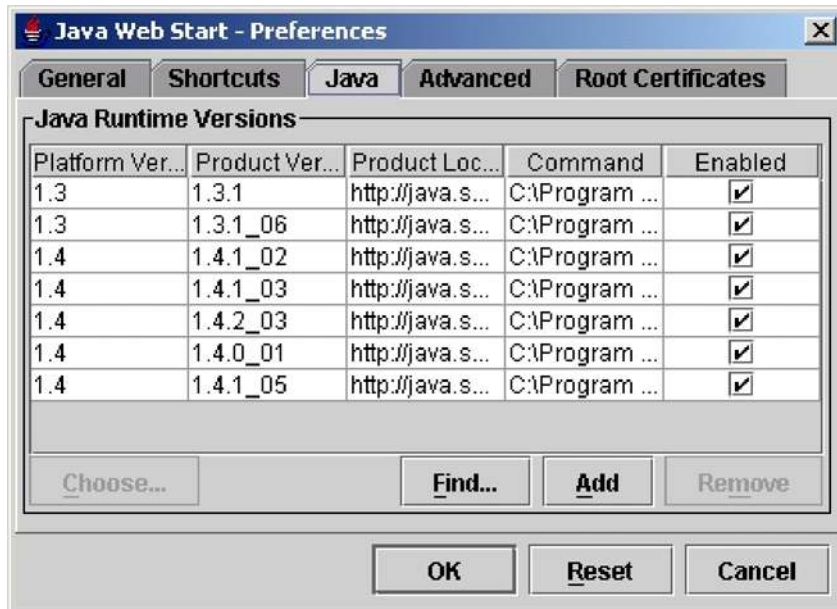
In the event you require more than one JRE version to be installed on your client PC we recommend using Java Web Start. Otherwise, you may encounter problems resulting from your browser using a corrupt version or the wrong version of JRE.

Java WebStart can be downloaded from the following site:

<http://java.sun.com/cgi-bin/javawebstart-platform.sh>

The README (<http://java.sun.com/products/javawebstart/docs/readme.html>) contains comprehensive instructions on downloading, installing, and using Java Web Start.

With Java Web Start users do not need to manually update applications because each time they launch an application, it is transparently updated from the Web, therefore the different JRE version installed on the computer are transparent to the user. As you can see from the picture below, Java Web Start lists all installed JRE versions. Java WebStart can be utilized to manage which version of JRE is used with the appropriate webpage.



CONCLUSIONS

Evolution of VPNs and Security

In the recent past, we have seen huge growth in the need for network security, specifically in three areas: perimeter network security, secured transactions over public infrastructure, and pervasive security on end systems. This growth has made it necessary to evolve how a management scheme handles this environment, which has resulted in the introduction of the CiscoWorks VPN/Security Management Solution (VMS).

The CiscoWorks VMS provides customers with applications to assist in the management of their security-specific hardware such as Cisco IOS VPN routers, Cisco VPN Service Modules, Cisco PIX firewalls, Cisco Firewall Service Modules, Cisco Network IDS Sensors, Cisco Network IDS Service Modules, and host-based Cisco Security Agents. VMS addresses the challenges of VPN deployment, monitoring, development of perimeter security policies, and management of intrusion detection. This paper provides some basic deployment guidelines for VMS by outlining the different

components of the solution, what they do, and how they can be configured to work together. It is intended that, after reading this document, the reader should clearly understand how VMS fits into their network management scheme and the value that it adds.

As with any dynamic environment, the needs and technologies around network security are constantly evolving. From a network management perspective, VMS will continue to evolve to provide a comprehensive set of tools to manage the unique aspects of this environment.



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.
168 Robinson Road
#28-01 Capital Tower
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 Website at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • 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

Copyright © 2005 Cisco Systems, Inc. All rights reserved. Catalyst, Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and PIX are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0501R) 204192.bd_ETMG_LF_1.05

