

CiscoWorks VMS 2.2

概要

課題

ネットワーク管理における主な課題の1つは、変化し続けるネットワークのニーズに適応可能な柔軟性を持つソリューションを構築することです。ネットワークの利用目的にかかわらず、基本的なネットワーク管理機能を備えたアプリケーションを導入することには十分な意義がありますが、それと同時にネットワーク環境についても考慮する必要があります。そのためには、目的に適ったネットワーク管理ツールを用意することが重要です。たとえば、QoS レベルの管理に焦点をあてたツールは、サーバファームのトポロジ管理には、必ずしも適切であるとは言えません。

ネットワーク セキュリティの発展と強化

ネットワークを企業の戦略的資産として考えた場合、ネットワーク管理が企業の成功にとって重要な要因であることは明白です。e- コマース、B2B 取引、VoIP など、従来型データ ネットワークの商用利用が進化するにつれて、安全なネットワーク接続に対するニーズがますます高まっています。その結果、Virtual Private Network (VPN) が普及し、ネットワーク セキュリティに対する意識が急速に高まりつつあります。

本書の目的

対象読者

本書では、CiscoWorks VPN/Security Management Solution (VMS) を効率よく展開する方法について説明します。本書のトピックは次のとおりです。1) サーバ、インストール、およびオペレーティングシステムの要件、2) 基本トポロジ、3) 監視基準、4) デバイスの設定に関する注意事項。本書では、クイック スタート ガイドおよびユーザ マニュアルの内容を補い、次のような疑問に回答します。1) このパッケージにはどのような製品が含まれ、それらの利用目的は何か。2) 何台のサーバが必要か。3) このアプリケーションでは、どのようなデバイスを管理できるか。4) VMS サーバ自体のセキュリティはどの程度まで強化できるか。これらの疑問に答える形で、さまざまな Cisco® セキュリティ テクノロジーの管理に関する基本的なベスト プラクティスを示します。

本書に含まれない内容

本書は、ユーザ ガイド（または、他の製品ドキュメント）に置き換わる性質の文書ではありません。また、本製品のさまざまな特徴や機能に関する全般的な詳細には触れていません。

対象読者

本書は、ネットワーク セキュリティ、VPN、ファイアウォール、および侵入検知に関する知識をすでにお持ちで、それらの概念とツールの基本を理解されている方を対象としています。本書では、本稼動環境で VMS を展開する最善の方法について説明します。



VMS 2.2 の全般的概要

機能

CiscoWorks VMS は、VPN およびセキュリティ管理用の包括的なソリューションを提供する統合ツールセットです。VMS には、企業の VPN、ファイアウォール、ネットワークベース / ホストベース侵入検知システムおよび侵入防止システム (IDS/IPS) の設定、監視、トラブルシューティングを行うための機能があります。VMS には、セキュリティ専用ハードウェアの展開、監視、および管理を支援する主要な機能が含まれています。また、運用管理サポート、ソフトウェア配布、設定アーカイブ、変更監査、シスコセキュリティインフラストラクチャの各種要素のログ管理といった機能もあります。VMS は、規模の大小を問わず、VPN およびセキュリティ展開のニーズを満たすスケーラブルなソリューションです。

VMS 2.2 コンポーネント (順不同)

CiscoWorks VMS 2.2 は、インストール可能な複数のソフトウェア コンポーネントで構成されているので、柔軟な展開が可能です。表 1 に、各種 VMS モジュールとそれぞれの機能を示します。

表 1 : VMS 2.2 モジュール¹

VMS モジュールとバージョン	プラットフォーム	使用目的
Common Services 2.2 (CiscoView 5.5 付属)	Windows Solaris	管理センターおよび CiscoWorks Resource Manager Essentials (RME) に共通するソフトウェアとサービスを提供します。 CiscoView には、デバイス シャーシの物理的状態の表示機能と、基本的なステータス監視機能があります。
Management Center for Firewalls 1.1.3	Windows	Cisco PIX [®] Firewall および Cisco Catalyst [®] Firewall Service Module を設定するために使用します。
Auto Update Server 1.1	Windows Solaris	アップデート サーバから設定を取得します。
Management Center for VPN Routers 1.1.1	Windows	Cisco IOS [®] ルータおよび Cisco Catalyst VPN Service Module の VPN 機能およびファイアウォール機能を設定するために使用します。
Management Center for IDS Sensor 1.2 (または 1.1)	Windows (1.2) Solaris (1.1)	ネットワーク ベース IDS センサーおよび Cisco Catalyst IDS Service Module を設定するために使用します。
Monitoring Center for Security 1.2 (または 1.1)	Windows (1.2) Solaris (1.1)	ネットワーク / ホストベース IDS のイベント、Cisco IOS ソフトウェア、および Cisco PIX syslog を監視します。
Management Center for Cisco Security Agent 4.0	Windows	重要なサーバを保護するようにホストベース IPS を設定します。
Cisco Security Agent 4.0	Windows Solaris	保護対象のサーバにインストールされるエージェントです。
VPN Monitor 1.2.1	Windows Solaris	IP Security (IPSec) ベースの Site-to-Site VPN およびリモート アクセス VPN を監視します。



表 1：VMS 2.2 モジュール¹

VMS モジュールとバージョン	プラットフォーム	使用目的
Resource Manager Essentials (RME) 3.5	Windows Solaris	ソフトウェア配布、変更監査、syslog 分析などの運用管理機能を提供します。

1. CCO の Software Center を参照して、VMS に新しいモジュールが追加されていないかどうかを確認してください。

これらのコンポーネントは、次の 3 つのカテゴリに分類されます。1) コア資産管理アプリケーション、2) セキュリティ監視アプリケーション、3) セキュリティ設定アプリケーション。このセクションでは、これらの製品カテゴリに関連する基本的機能の一部について詳しく説明します。

コア資産管理アプリケーション

1. Resource Manager Essentials (RME)

Resource Manager Essentials は、インベントリ、設定、変更監査、syslog などの、日常のネットワーク管理を支援する基本的なネットワーク管理ツールです。また、RME には、VPN 管理機能が追加されました。これにより、VPN 環境固有のデバイス設定、ソフトウェア イメージおよび syslog レポートの作成が可能になりました。

2. CiscoView (Common Service 内部に組み込まれるオプション インストール)

CiscoView は、さまざまなシスコ インターネットワーキング製品の動的ステータス、監視情報、および設定情報を表示する Web ベースのデバイス管理アプリケーションです。CiscoView には、デバイス シャーシの物理的状态が表示され、モジュールおよびポートが色分けされるので、ステータスを一目で把握することができます。監視機能では、パフォーマンスなどの統計情報が表示されます。また、設定機能では、デバイスにさまざまな変更を加えることができます。

セキュリティ監視アプリケーション

1. VPN Monitor

VPN Monitor は、VPN デバイスおよびトンネルのステータスを監視するアプリケーションです。このアプリケーションは、Cisco IOS Software シリーズ VPN ルータや Cisco VPN 3000 シリーズ コンセントレータなどの VPN 対応デバイスの統計情報を収集して、保存し、レポートします。VPN Monitor は、Layer 2 Tunneling Protocol (L2TP)、Point-to-Point Tunneling Protocol (PPTP)、および IPSec を含む複数のトンネリング プロトコルをサポートし、2 種類の VPN (Site-to-Site およびリモート アクセス) をサポートしています。



2. Monitoring Center for Security

Monitoring Center for Security (または Security Monitor) は、IDS イベントに加え、各種シスコ デバイスからの SYSLOG メッセージを監視します。その中には、ネットワーク IDS センサー アプライアンス、Cisco Catalyst 6500 シリーズ IDS モジュール、Cisco IOS Software IDS メッセージ、Cisco PIX Firewall の syslog メッセージ、Catalyst 6500 Firewall Service Module の syslog メッセージ、Cisco Security Agent のイベントなどが含まれます。

セキュリティ設定アプリケーション

1. CiscoWorks Common Services

CiscoWorks Common Services Software には、Web サーバ、汎用データベース、ポーリング エンジンなど、管理サーバの基本的コンポーネントが含まれています。このソフトウェアは、VMS バンドルに含まれる管理センター ツールを利用するための前提条件となっているため、この CD を最初にインストールしてください。

2. Management Center for VPN Routers (Router MC)

Router MC は、Cisco IOS VPN ルータ用に設計された VPN/Cisco IOS Firewall 機能セットおよび展開ツールです。Router MC は、Common Services 上にインストールされる Web ベースのアプリケーションです。

3. CiscoWorks Management Center for Firewalls (Firewall MC)

Firewall MC は、Cisco PIX ファイアウォールおよび Cisco Catalyst スイッチ ファイアウォール サービス モジュール用に設計された包括的なファイアウォール/アクセスルール ポリシー設定ツールです。新しいファイアウォールを設定できるだけでなく、既存のファイアウォールまたは設定ファイルから設定をインポートすることもできます。また、Firewall MC には、設定およびステータスの変更を参照しながら、ネットワークに加えられた変更を制御できる強力なツールも用意されています。Firewall MC は、Common Services 上にインストールされる Web ベースのアプリケーションです。

4. CiscoWorks Auto Update Server Software (AUS)

AUS は、デバイス設定ファイルおよびソフトウェア イメージ (ファイアウォール イメージおよび Cisco PIX Device Manager [PDM] イメージ) の保存およびアップグレードに使用されるツールです。ファイアウォール デバイスは、定期的に AUS と通信して、設定およびソフトウェアのアップデートがないかどうかを確認します。この仕組みにより、ファイアウォール デバイスは、常に最新状態に保たれます。特に、リモートの PIX Firewall デバイスが動的アドレスを使用していたり、ネットワーク アドレス変換 (NAT) デバイスの背後にある場合は、AUS を使用するとたいへん便利です。AUS は、Common Services 上にインストールされる Web ベースのアプリケーションです。



5. Management Center for IDS Sensors (IDS MC)

IDS MC は、シスコのネットワーク IDS センサー アプライアンス、および Catalyst スイッチの Cisco IDS サービス モジュール用に設計された IDS 設定 / 展開ツールです。IDS MC は、Common Services の上にインストールされる Web ベースのアプリケーションです。

6. Management Center for Cisco Security Agent (Cisco Security Agent MC)

Cisco Security Agent MC は、ホスト ベース IDS ソリューション (Cisco Security Agent) 用に設計された設定 / 展開ツールであり、IDS MC および Security Monitor の機能を補完します。Cisco Security Agent MC は、Common Services 上にインストールされる Web ベースのアプリケーションです。

7. Cisco Security Agent

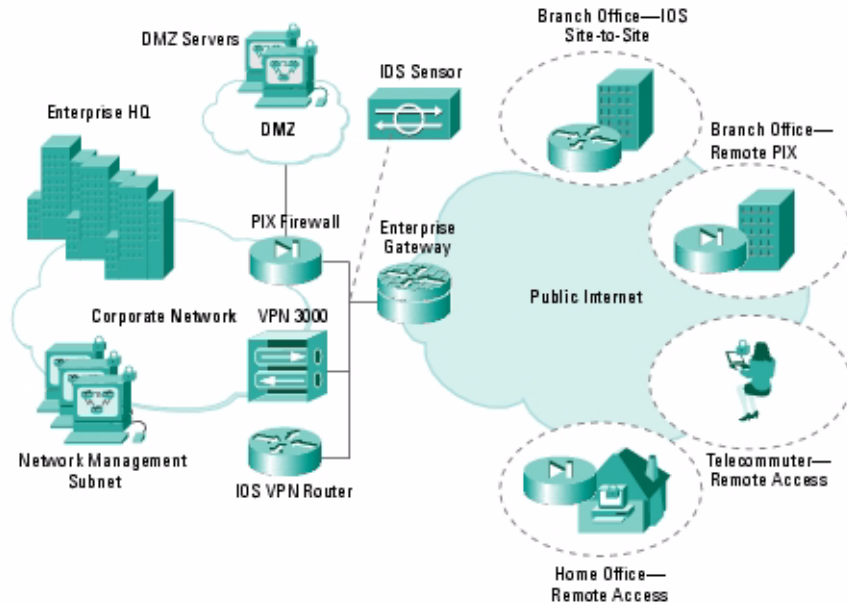
Cisco Security Agent は、オペレーティング システムに統合され、重要なサーバおよびホストを保護する、ホスト IDS/IPS アプリケーションです。Cisco Security Agent は、カーネルへのシステム コールを代行受信して、攻撃を識別し、リソースへのアクセスと不正なトランザクションを防止することによって、ホストを保護します。

基本トポロジ

CiscoWorks VMS の最善な展開方法を説明するために、基本ネットワーク トポロジ (図 1) を使用して、VPN およびネットワーク セキュリティのさまざまな側面を示します。このトポロジはお客様の環境と必ずしも一致しませんが、安全なネットワークの全体像としてとらえることができます。この基本トポロジを参考にして、お客様のトポロジに最も適したコンポーネントを選択し、お客様の環境で VMS を展開する最善の方法を把握してください。



図 1：基本セキュリティトポロジ



関係するインフラストラクチャ

- 企業ゲートウェイ：Cisco IOS Firewall Feature Set を搭載した Cisco IOS ルータです。このデバイスの主な目的は、ゲートウェイルーティング機能と最前線での基本的ファイアウォール機能を実行することです。
- PIX Firewall：Cisco PIX Firewall は、企業ネットワークに対して包括的なファイアウォール機能を提供します。これらのデバイスをネットワークアクセスポイントへ戦略的に配置することで、企業ネットワークのリソースが保護されます。
- Cisco 800、1700、2600、3600、7100 または 7200 シリーズルータ：シスコルータは、Site-to-Site VPN の終端ポイントとして機能します。ハブ/スポーク型 VPN トポロジの場合は、ハイエンドの VPN ルータがハブとして機能し、小規模/中規模のルータがスポークとして機能します。
- VPN 3000：VPN 3000 シリーズ コンセントレータは、スケーラビリティに優れたリモートアクセス VPN 終端ポイントとして機能します。このトポロジでは、コンセントレータによって、さまざまなリモートアクセス環境、VPN クライアントソフトウェア、およびトンネリングプロトコル (IPSec、L2TP、PPTP など) との VPN 接続が終端されます。
- Cisco VPN リモートアクセスクライアントソフトウェア：リモートアクセスユーザは、このソフトウェアを使用して、企業ネットワークに VPN 経由で接続できます。
- ネットワークIDSセンサー：このデバイスは、ネットワークセグメントに設置されて受動的にトラフィックを「リスニング」し、一般的な攻撃のシグニチャのデータベースと照合します。IDS のイベント情報は、監視ステーションに転送されます。
- シスコホストベースIDS/IPSセキュリティエージェント：このソフトウェアは、重要なネットワークサーバ上だけでなく、ホームオフィスPCやモバイルラップトップ上にも常駐し、各ホストを侵入や攻撃から守ります。イベントは、中央の監視コンソールに転送されます。



- ネットワーク管理サブネット：このサブネットは、ネットワーク管理サーバ専用のネットワーク セグメントです。VMS のコンポーネントはこのサブネットに存在し、インフラストラクチャのさまざまな部分を管理します。VMS サーバはすべて、Cisco Security Agent により保護されています。
- DMZ サーバ：このサブネットは、一般公開されているネットワーク サーバ専用のネットワーク セグメントです。通常は、電子メールサーバ、Web サーバ、FTP サーバなどが含まれ、この場合は、CiscoWorks Auto Update Server Software も含まれます。DMZ サーバはすべて、Cisco Security Agent により保護されています。

次は、この基本トポロジの中で、VMS によって管理されるインフラストラクチャの各要素について説明します。VMS に含まれるネットワーク管理アプリケーションでは、他のデバイス（Cisco Catalyst スイッチなど）も管理することができますが、VMS で中心的に管理する必要があるコンポーネントは以下のとおりです。

•企業本部

-このセクションには、ネットワーク管理サーバ、内部ファイアウォール、VPN 終端ポイント（ハブルータおよびVPN コンセントレータ）、IDS センサーが含まれます。ネットワークのDMZ部分へのアクセスは、内部ファイアウォールによって制御されます。また、一般公開サーバも含まれません。

•リモートアクセスサイト

-このトポロジのリモートアクセスサイトには、リモートPIXファイアウォール、リモートCisco IOS VPN ルータ、およびリモートVPNクライアントが含まれます。これらのインフラストラクチャ要素は、リモートサイトにおけるVPN終端およびファイアウォールアクセスポリシーに関連する処理を実行します。

VMS の OS サポート およびシステム要件

VMS は、（1台または複数台の）ネットワーク管理サーバ上に常駐する一連のツールで構成されています。このセクションでは、VMS のコンポーネントを実行するためにあらかじめインストールしておく必要があるソフトウェアについて説明します。最初に、OS のサポートについて説明します。VMS バンドルに含まれるほとんどのアプリケーションでサポートされている OS は、Windows 2000 Professional または Server です。表 2 および表 3 を参照してください。

表 2：VMS 2.2 モジュールでサポートされている OS

VMS モジュール	Windows サポート	Solaris サポート
Common Services		
Management Center for Firewalls		
Auto Update Server		
Management Center for VPN Routers		



表 2： VMS 2.2 モジュールでサポートされている OS

VMS モジュール	Windows サポート	Solaris サポート
Management Center for IDS Sensor		
Monitoring Center for Security		
Management Center for CSA		
Resource Manager Essentials		
VPN Monitor		

表 3： VMS サーバのハードウェアおよび OS の最小要件

Windows	
ハードウェア	1 GHz 以上の Pentium CPU を搭載した IBM PC 互換機 1 GB のメモリ 9 GB の空きハード ディスク容量 ¹ CD-ROM ドライブ 16 ビット カラー対応のビデオ カードとカラー モニタ 10/100 BaseT 以上のネットワーク接続
オペレーティング システム	Windows 2000 Professional Windows 2000 Server ² Windows Advanced Server ² Service Pack 3 以降 NTFS ファイル システム 2 GB の仮想メモリ
Solaris	
ハードウェア	440 MHz 以上の CPU を搭載した Sun UltraSPARC 60MP、または Sun UltraSPARC III (Sun Blade 2000 Workstation または Sun Fire 280R Server) CD-ROM ドライブ 16 ビット カラー対応のビデオ カードとカラー モニタ 10/100 BaseT 以上のネットワーク接続
オペレーティング システム	Sun Solaris 2.8 フル インストール 必要なパッチ： 108528-13 108527-15

1. 実際に必要となるハード ドライブ容量は、インストールする VMS コンポーネントの数と、管理および監視するデバイスの数によって異なります。
2. Windows 2000 Server および Windows Advanced Server の場合は、ターミナル サービスをリモート管理モードに設定し、インストール中はオフにしておく必要があります。



VMS サーバの安全確保

ハードウェアおよびソフトウェアの基本的要件について説明したので、このセクションでは、サーバ自体を管理できるように設定する方法について説明します。セキュリティ上の原則として、ホストの安全確保するには、システム内のすべてのコンポーネントに注意を払う必要があります。最新のパッチや修正プログラムなどを適用して、すべてのシステムを最新状態に保ってください。VMS を使用する場合は、必ず Windows 2000 および Solaris の最新パッチとホットフィックスを適用してセキュリティを確保する必要があります。管理サーバとして使用するサーバに関して確認する必要がある項目のチェックリストを以下に示します。

1. Windows

- オペレーティングシステムは、専用のパーティションにインストールしてください。
- プライマリ ドメイン コントローラ (PDC) またはバックアップ ドメイン コントローラ (BDC) には VMS をインストールしないでください。
- 推測されにくいパスワードを使用してください。
- ネットワーク共有は作成しないでください。
- 不要なアカウントは無効にしてください。
- レジストリのセキュリティを設定してください。
- すべてのホットフィックスとセキュリティ パッチを適用してください。
- 使用しないサービスや不要なサービスは無効にしてください (Windows の実行に最低限必要なサービスは、Domain Name System [DNS] Client、Event Log、Plug and Play、Protected Storage、および Security Accounts Manager です。Microsoft の Internet Information Server [IIS] は、インストールしないでください)。
- Internet Protocol (TCP/IP) 以外のすべてのネットワーク プロトコルを無効にしてください。
- システムのセキュリティを定期的に監視してください。
- サーバへの物理的接触を制限してください。
- 可能な場合は、リモート アクセス ツールやリモート管理ツールをサーバにインストールしないでください。
- ウィルス スキャン アプリケーションを定期的にサーバ上で実行してください。

2. Solaris

- 推測されにくいパスワードを使用してください。
- Network Infrastructure Solutions (NIS/NIS+) サーバおよび DNS サーバをインストールしないでください。
- サーバへの物理的接触を制限してください。
- 不要なアカウントは無効にしてください。



3. Cisco Security Agent による VMS サーバの保護 (Windows のみ)

Windows ベースの VMS サーバを使用する場合は、Cisco Security Agent などのホスト IDS/IPS ソリューションを使用して、サーバを保護することをお勧めします。Cisco Security Agent は、動作ベースのホスト IPS です。このソリューションは、悪意のあるアプリケーションや、想定外のアプリケーションがシステム内で実行されることを防止するだけでなく、バッファ オーバフローなどの攻撃も防ぐことができるため、インバウンドおよびアウトバウンドのネットワーク接続とサービスを制御するファイアウォールとして機能します。

VMS には、Windows ベースの VMS サーバを保護するために、3 つの Cisco Security Agent が付属し、VMS サーバをロックするように設計されたデフォルトのグループ ポリシーが含まれています。これら 3 つの Cisco Security Agent は、VMS 設定サーバ、VMS 監視サーバ、および VMS 自動アップデート サーバの保護を目的としています。サーバを 1 台しか設置しない場合は、必要となるエージェントも 1 つだけになります。4 台以上のサーバを保護する必要がある場合は、シスコから Cisco Security Agent ライセンスを追加購入する必要があります。

VMS サーバのデフォルト グループは、CiscoWorks VMS System グループです。サーバを完全に保護するために、このグループには次のポリシーが含まれています (表 4)。

表 4：サーバを完全に保護するための VMS サーバ デフォルト グループ ポリシー

ポリシー	説明
CiscoWorks Base Security Module	CiscoWorks を実行するすべてのシステムに適用される基本ポリシー (17 個のルールが付属)
CiscoWorks VMS Module	CiscoWorks VMS 製品コンポーネントを実行するサーバに適用されるポリシー モジュール (30 個のルールが付属)
Required Windows System Module	重要な Windows 機能を許可するポリシー モジュール (12 個のルールが付属)

ここでは、これら 3 つのポリシーに関連付けられている 59 個すべてのルールについては説明しません。次のパラグラフでは、Cisco VMS Module ポリシーのルール 214 によって VMS サーバがどのように保護されるかについて説明します。

Apache などの VMS デーモンは、Network Access Control Rule 214 によって、リモート接続の受け入れを許可されています。クライアントからの User Datagram Protocol (UDP) 接続および TCP 接続を受け入れることが許可されているのは、「CiscoWorks VMS network daemons」というアプリケーション クラス (apache.exe、crmlog.exe、crmrsh.exe などのネットワーク デーモン実行可能ファイルを含む事前定義済みのアプリケーション クラス) のみです。



規模および展開に関する考慮事項

VMS バンドルのソフトウェア要件だけでなく、ハードウェア要件についても考慮する必要があります。また、このソリューションに含まれる各種アプリケーションの展開方法を決定することも重要な課題です。インストール可能なソフトウェアアプリケーションが 11 種類あるため、展開するアプリケーションの組み合わせは数多く存在します。

最小要件も重要な考慮事項ですが、推奨されるシステムの仕様はネットワークおよび構成の規模によって異なります。このセクションでは、小規模、中規模、および大規模な構成について検討します。最初に考慮する必要がある事項はスケーラビリティです。何台のデバイスが小規模、中規模、大規模の各構成に該当するのでしょうか。

規模

スケーラビリティの基準は、VMS に含まれるアプリケーションごとに異なります。表 5 に、各アプリケーションの理論上の最大値を示します。

表 5： 規模に関する VMS アプリケーションの理論上の上限

VMS モジュール	スケーラビリティの基準 (テスト済みの最大数 ¹)
IDS MC	IDS センサー x 300
Security Monitor	500 イベント / 秒 ²
Firewall MC	PIX ファイアウォール x 1000
AUS	PIX ファイアウォール x 1000
Router MC	ルータ x 1000
CSA MC	Cisco Security Agent x 5000
RME	デバイス 5000 台分のインベントリ、デバイス 1000 台分のアベイラビリティ
VPN Monitor	ダッシュボード上のデバイス x 30 (ソフトウェア自体の上限)

1. これらの理論上の上限は、各ツールを実際に使用してテストされた上限です。これらの数値は、適度なパフォーマンスおよびユーザ側の体感速度を確保するためのガイドラインとして提示されています。これらの基準を超えることも可能ですが、お勧めしません。

2. 毎秒 500 を超えるセキュリティイベントが長時間にわたって発生する場合は、より多くのイベントを処理できるパートナーベンダーの監視製品の導入をご検討ください。

これらの数値の大半は、ソフトウェア自体に課せられた上限ではなく、ソフトウェアテストに基づく上限値です。たとえば、Router MC を使用している場合、1001 台目のデバイスを追加することは可能ですが、サポートの観点からは推奨されていません。



また、VMS に関して推奨されている最小限のハードウェアシステム仕様は、バンドルに含まれるアプリケーション 1 種類のためのテストおよびパフォーマンス統計に基づいて提示されていることに注意してください。たとえば、IDS MC を使用して 300 台のセンサー（理論上の最大数）を管理する場合、同じサーバ上で他のアプリケーションを使用することはお勧めしません。複数の VMS アプリケーションを使用して多数のデバイスを管理する場合は、別々のサーバに分けてインストールすることを強くお勧めします。

次に、多くのリソースを消費するバンドルアプリケーションについて検討します。構成の規模に応じて、表 6 ~ 8 を参照してください。

表 6：小規模構成の基準（制限付き VMS ライセンス モデルを反映）

VMS モジュール	スケーラビリティの基準（最大）
IDS MC	IDS センサー x 20
Security Monitor	200 イベント / 秒
Firewall MC	PIX ファイアウォール x 20
AUS	PIX ファイアウォール x 20
Router MC	ルータ x 20
CSA MC	Cisco Security Agent x 5000

表 7：中規模構成の基準¹

VMS モジュール	スケーラビリティの基準（最大）
IDS MC	IDS センサー x 100
Security Monitor	300 イベント / 秒
Firewall MC	PIX ファイアウォール x 100
AUS	PIX ファイアウォール x 100
Router MC	ルータ x 100
CSA MC	Cisco Security Agent x 5000

1. この構成は、大部分の VMS ユーザの基準を反映しています。

表 8：大規模構成（スケーラビリティに関する理論上の最大基準を反映）

VMS モジュール	スケーラビリティの基準（最大）
IDS MC	IDS センサー x 300
Security Monitor	500 イベント / 秒



表 8：大規模構成（スケーラビリティに関する理論上の最大基準を反映）

VMS モジュール	スケーラビリティの基準（最大）
Firewall MC	PIX ファイアウォール x 1000
AUS	PIX ファイアウォール x 1000
Router MC	ルータ x 1000
CSA MC	Cisco Security Agent x 5000

サーバのサイズ

上記の要素に基づき、各構成で推奨されるサーバのサイズをより詳細に検討します。これらの仕様は個々のアプリケーションの最小要件であり、多くの環境の要件はこれらを超えている場合があります。原則として、パフォーマンスに多大な影響を与える基準を1つでも選択する必要がある場合は、RAMの容量を増やしてください。また、各アプリケーションの上限にも注意してください。前述した理論上の上限に近づいている場合は、VMSサーバの処理能力の増強を検討してください。たとえば、P4 2.2 GHz CPU および 4GB の RAM を搭載したサーバで VMS アプリケーションを実行しても、無駄な投資にはなりません。一般的なガイドラインを表9に示します。

表 9：VMS 構成に使用するサーバの（最小）推奨値

構成	小規模	中規模	大規模
CPU	PIII 1 GHz	P4 1.7 GHz	P4 2.5 GHz
RAM	1 GB	1.5 GB	2 GB
仮想メモリ	2 GB	3 GB	4 GB
ハードディスク容量	9 GB	20 GB	40 GB

サーバの展開：一般的な原則

アプリケーションの互換性の観点から、次の原則に従う必要があります。

- Common Services を最初にインストールする必要があります。
- 他のすべてのアプリケーションは、Common Services 上にインストールする必要があります。





VMS では、これらの条件が満たされている限り、非常に柔軟な展開が可能です。たとえば、すべてのコンポーネントを1台のサーバにインストールして実行することもできれば、各コンポーネントをそれぞれの専用サーバにインストールすることもできます。ただし、これらは極端な例なのであまり現実的ではありません。実際の展開方法は、次のような要因に基づいて決定されます。







































1. 実際にどのアプリケーションが必要か。

VMS は機能豊富な包括的管理ソリューションですが、必ずしもすべてのツールを使用する必要はない場合があります。まず確認すべきことは、「実際にどのアプリケーションが必要か」という点です。これを確認すれば、必要なモジュールのみを選んでインストールすることができます。図 2 に、複数の管理オプションを 1 台のサーバにインストールする場合のインストール順序を示します。

図 2 : VMS モジュールのインストールマトリクス (() 内のコンポーネントはオプション)

Legend				
	Manage VPN/FW Router		Manage IDS Sensor	
	Manage PIX Firewall		Manage Security Agent	

Management Options				Installation
				Common Services, Router MC, (RME), (VPN Monitor)
				Common Services, Firewall MC, AUS
				Common Services, IDS MC
				Common Services, CSA MC
				Common Services, IDS MC, CSA MC
				Common Services, Router MC, Firewall MC, (RME), (VPN Monitor)
				Common Services, Router MC, IDS MC, CSA MC, (RME), (VPN Monitor)
				Common Services, Firewall MC, IDS MC
				ALL



注：この表は、基本的なガイドラインのみを示しています。VMSに含まれるすべてのツールおよびすべての組み合わせは網羅されていません。インストールの順序が関係するツールのみが挙げられています。

- インストール オプション 1：VPN の管理では、VPN Monitor によって監視コンポーネントが処理されます。監視が必要な場合は、VPN Monitor をインストールする必要があります。
- インストール オプション 2：ファイアウォールの管理では、PIX Firewall の設定およびソフトウェアの展開に自動アップデート機能を活用したい場合にのみ、AUS が必要になります。
- インストール オプション 3：ネットワーク / ホストベース IDS の管理では、これらすべてのコンポーネントからのイベントを監視するために Security Monitor が必要になります。ただし、他のセキュリティ情報管理アプリケーションを使用する場合は除きます。

2. 各アプリケーションで何台のデバイスを管理するか。

いずれかのアプリケーションが理論上の上限に近づいている場合は、そのアプリケーションを専用のサーバ上で実行することをお勧めします。多数のデバイスを管理する場合、リソースおよびタスクの配分という観点から見て、貴重な CPU リソースを他のアプリケーションと共有させない方がよいことは明白です。

たとえば、すでにインストールされている Firewall MC のインスタンスで 800 台の PIX ファイアウォールを管理していて、600 のルータ スポークから構成されるハブ / スポーク型 VPN 環境をさらに展開する場合は、これらのアプリケーションをそれぞれの専用サーバに分離することをお勧めします。

3. 何人の管理者がこれらのアプリケーションを使用するか。

複数の管理者が存在する環境では、別の VMS 展開オプションを検討することにも意義があります。VMS には目的の異なるアプリケーションが数多く含まれているため、それぞれのセキュリティ管理者が別々のアプリケーションを使用する場合があります。このような場合は、各アプリケーションを専用サーバにインストールして分離することをお勧めします。この方法を取れば、設定ファイルの生成のように、大量のリソースを消費するタスクによって 1 つのアプリケーションがビジー状態になったときでも、他のアプリケーションのパフォーマンスはまったく低下しません。

4. サーバの調達に関して、どのようなコスト上の制約があるか。

VMS を使用している組織に複数のサーバはありますか（または入手することが可能ですか）。場合によっては、サーバ 1 台分の予算しか確保できないこともあります。そのような場合は、最小システム要件を上回るハイエンドサーバを購入されることをお勧めします。これにより、パフォーマンスが向上するだけでなく、環境規模の成長にも対応できます。

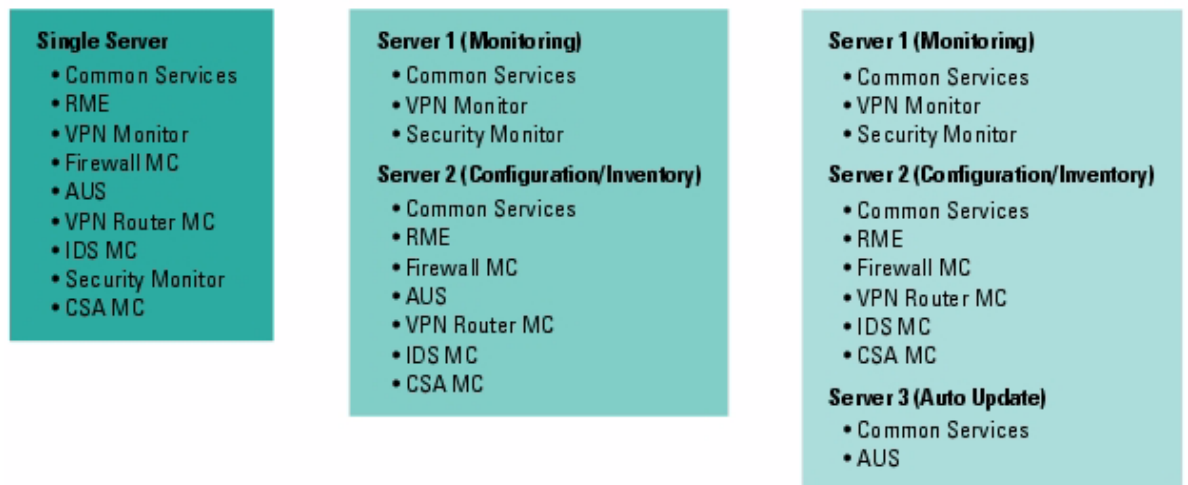


サーバの台数

根本的には、可能な限り多くのサーバを使用して、アプリケーションを合理的に分散するのが最善の方法です。スケーラビリティ、リソース割り当て、タスク配分、成長への対応といった観点からすると、管理不能な状態に陥らない限り、その数は多ければ多いほどよいと言えます。また、1台のサーバに複数のアプリケーションをインストールする場合は、各アプリケーションのハードウェア要件に十分な注意を払い、それに応じて調整する必要がありますことを念頭に置いてください。

次のセクションでは、基本的な展開オプションについて説明し、多くのユーザに関係する一般的なガイドラインを示します (図3)。これらは単なる推奨事項であり、必ずしもこのとおりにVMSを展開する必要はありません。

図3：サーバ展開オプション



オプション1：サーバ1台での展開

ネットワークセキュリティ管理者が1人だけの小規模なセキュリティ環境では、1台のサーバでの展開をお勧めします。この展開には、コストが安く、管理が容易であるという利点があります。

オプション2：サーバ2台 (設定と監視)

この展開オプションでは、機能ごとにVMSアプリケーションを分割します。一方のサーバは監視専用となり、もう一方のサーバは設定専用となります。

1. サーバ1：監視

この展開オプションの1台目のサーバは、監視専用サーバです。VPN Monitor を使用して IPsec MIB を監視し、Security Monitor を使用して PostOffice IDS、Remote Data Exchange Protocol (RDEP) IDS、Cisco Security Agent、PIX、Cisco IOS Syslog メッセージなどのイベント表示を統合します。このサーバで使用するアプリケーションは、次のとおりです。



- Common Services
- VPN Monitor
- Security Monitor

2. サーバ 2 : 設定およびインベントリ

このセキュリティ管理サーバでは、設定を支援するすべての VMS アプリケーションを組み合わせて使用します。VPN ルータ、PIX Firewall、IDS センサー、Cisco Security Agent など、インフラストラクチャの種類を問わず、このサーバの主要目的は設定です。関連するアプリケーションは、次のとおりです。

- Common Services
- RME
- Firewall MC
- AUS¹
- IDS MC
- CSA MC

オプション 3 : サーバ 3 台 (機能をさらに細分化)

AUS サーバはリモート ファイアウォールの管理を目的としているため、設定、OS、PDM のアップデートを確認するために多数のリモート デバイスが AUS に接続すると、大量のリソースが消費される可能性があります。AUS 単独で 1 台のサーバを使用できるように、ネットワークの DMZ に AUS を配置することをお勧めします。

1. サーバ 1 : 監視

- Common Services
- VPN Monitor
- Security Monitor

2. サーバ 2 : 設定 / インベントリ

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



3. サーバ 3 : 自動アップデート

- Common Services
- AUS

オプション 4 : サーバ 3 台 (セキュリティ アプリケーション機能) (図 3 には表示なし)

4 番目の展開オプションでは、管理の対象となるセキュリティテクノロジー (またはインフラストラクチャ) ごとに、VMS アプリケーションを分割します。1 台目のサーバは VPN を処理し、通常は Cisco IOS Software ベースの VPN ルータを扱います。2 台目のサーバには、Cisco PIX Firewall を管理するためのアプリケーションをインストールします。最後に、3 台目のサーバは、IDS (ネットワークベース IDS およびホストベース IDS) の管理と監視を行うための専用サーバになります。

1. サーバ 1 : VPN

- Common Services
- RME
- VPN Monitor
- Router MC

2. サーバ 2 : ファイアウォール

- Common Services
- Firewall MC
- AUS

3. サーバ 3 : IDS

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

オプション 5 : サーバ 4 台 (管理機能をさらに細分化) (図 3 には表示なし)

さらに展開を分割すると、機能がより細分化され、スケーラビリティが向上します。このオプションの最も大きな違いは、AUS 専用のサーバを使用する点です。AUS は、ネットワークの別のサブネットに配置されます。

1. サーバ 1 : 設定

- Common Services
- Firewall MC



- Router MC
- IDS MC
- CSA MC

2. サーバ 2 : インベントリ

- Common Services
- RME

3. サーバ 3 : 監視

- Common Services
- VPN Monitor
- Security Monitor

4. サーバ 4 : リモート管理 (DMZ に配置)

- Common Services
- AUS

これらは単なる推奨事項です。使用可能な組み合わせおよび展開オプションは非常に多いため、それぞれ個別に検討する必要があります。また、VMS に含まれるすべてのアプリケーションを使用する必要がないケースも少なくありません。

VMS の応用

インストールの観点からの VMS コンポーネントの展開方法が明確になったので、次は、機能的な観点からこれらのアプリケーションを展開する方法について説明します。このセクションでは、次の 3 つの基本的質問について検討します。

1. 各アプリケーションにはどのような管理機能があるか
2. どのデバイスを管理できるか
3. どのタイプのサービスを有効にする必要があるか

最初の質問に答えるには、各製品の機能を詳細に検討する必要があります。これにより、VMS の各コンポーネントを使用してセキュリティ管理のどの側面を管理できるか、または管理する必要があるかを明確にすることができます。また、2 番目の質問に答えることによって、各コンポーネントアプリケーションでサポートされているデバイスの違いから生じる混乱を解消することができます。最後に、3 番目の質問では、各アプリケーション



ンが管理対象のデバイスとどのように通信するかを検討します。使用される通信プロトコルを検討することで、VMS の展開を成功させるために必要な事項のリストをまとめることができます。議論をわかりやすくするために、製品またはサーバごとに、各質問を検討します。

注： シスコのネットワーク インフラストラクチャのコンポーネントは、非常に多岐にわたります。ここでは、セキュリティに関する議論が中心となるため、次の 5 種類のオブジェクトのみに焦点を当てます。Cisco IOS ルータ、PIX ファイアウォール、VPN コンセントレータ、IDS センサー、およびホストベース Security Agent。これは、VMS が他の要素を管理できないということを意味するのではなく、単に、これらが特に注意を要するデバイスであるということ意味しているにすぎません。

管理サブネットについて (アウトバンド管理)

多くのネットワークでは、隔離された管理用サブネットを設計するのが望ましいと言えます。これはアウトバンド管理と呼ばれ、管理ステーションが管理対象のネットワーク要素から分離されたサブネット上にある状況を指します。セキュリティのレベルが高くなり、ネットワーク内部の機能区分が明確になるため、この方法は多くのネットワーク管理者にとって魅力的です。

ただし、すべてのネットワーク管理ツールと同様に、VMS は管理対象デバイスへのネットワーク アクセスを必要とします。したがって、完全に隔離された管理サブネットを構築するのは確かに望ましいことですが、ネットワークの他の部分に IP 接続できなければまったく意味がありません。そのような環境で VMS を展開する場合は、この点を注意深く検討する必要があります。

CiscoView (Common Service 内部に含まれる)

1. どのような管理機能があるか

CiscoView を使用すると、Web ベースでの視覚的なデバイス管理が可能になります。CiscoView では、コンピュータの画面上にデバイスがグラフィック表示されます。このツールでは、デバイスのステータスをリアルタイムで監視でき、場合によっては、それらのデバイスの設定を変更することもできます。CiscoView は、VMS の中で、トラブルシューティング ツールに位置づけられます。ネットワーク内で問題が発生し、その問題が 1 つのデバイスまたはインターフェイスのレベルにまで絞り込まれた場合は、CiscoView を使用してそのデバイスに関連する統計情報を参照し、問題を解決する設定変数を検討することができます。

2. どのデバイスを管理できるか

CiscoView は、大半の Cisco IOS ルータ、Cisco Catalyst スイッチ、VPN 3000 コンセントレータ、および PIX 501、506 シリーズ ファイアウォールをサポートしています。



3. どのサービスを有効にする必要があるか (アプリケーション プロトコルの要件)

CiscoView の機能は、Simple Network Management Protocol (SNMP) の get/set 操作 (UDP ポート 161) に全面的に依存しています。CiscoView サーバからデバイスにアクセスするには、SNMP トラフィックを有効にする必要があります。また、管理対象となるデバイス側でも、SNMP がサポートされている必要があります。Cisco IOS Software デバイスは、(監視も設定も) get および set の操作を両方サポートでき、read および write コミュニティ スtring が別々に設定されているため、きめ細かく管理することができます。VPN 3000 シリーズ コンセントレータおよび PIX ファイアウォールは、SNMP の read 操作しかサポートしていないため、CiscoView を使用してこれらのデバイスを監視することはできますが、設定を変更することはできません。

RME

1. どのような管理機能があるか

RME の機能に関する説明は、それだけで独立した文書になります。全体として (セキュリティという観点からすると)、このアプリケーションは、基本的なネットワーク管理機能の操作と管理を目的としています。このツールには次の機能があります。

- インベントリ管理：インフラストラクチャ内のデバイスを常時監視します
- 設定管理：ネットワーク デバイスの設定を管理します
- 変更監査管理：ネットワーク内で発生した変更 (設定、その他) を常時監視します
- ソフトウェア イメージ管理：ソフトウェア バージョンの維持を容易にします
- Syslog 管理：ネットワーク デバイスから syslog メッセージを受信して分析します

このリストが示すように、RME の機能には、セキュリティ インフラストラクチャ管理の範囲を超えた利点があります。ただし、本書では、この環境に関係する利点のみに焦点を当てています。特に重要な点は、RME が設定レポート、ソフトウェア イメージアップグレード分析、および VPN 関連インフラストラクチャ / 環境に固有の syslog レポートを作成できるという事実です。

2. どのデバイスを管理できるか















RME は、Cisco IOS ルータ、VPN 3000 コンセントレータ、および PIX シリーズ 506、515、520、525 ファイアウォールをサポートしています。ただし、コンセントレータに関しては、RME による設定管理がサポートされておらず、ソフトウェア イメージ管理も一部の機能に限定されています。また、PIX ファイアウォールに関しては、RME による syslog 管理が一部の機能に限定されています。再び基本トポロジの図 (図 1) を参照すると、IDS Sensor を例外として、基本的にネットワークのすべての側面が RME によって管理されることがわかります。このため、RME は「コア」管理アプリケーションと呼ばれます。



3. どのサービスを有効にする必要があるか (アプリケーション プロトコルの要件)

RME は複数のプロトコルを使用してデバイスを管理します。代表的なプロトコルには、SNMP、Telnet、TFTP、Syslog があります。RME にはさまざまなサブコンポーネントがあり、管理対象となるデバイスが異なるため、このツールに関するアプリケーション プロトコルの要件を表 10 にまとめます。

表 10 : CiscoView と RME のプロトコル要件

アプリケーション	トラフィック フロー	サービス	TCP/UDP ポート番号
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 TFTP ICMP	TCP 23 UDP 161 N/A
Syslog Analyzer	 → 	Syslog	UDP 514



このマトリクスを参考にして、RME の管理対象デバイスから適切な情報が提供されるように設定されているかどうかを確認してください。SNMP の read コミュニティ スtring の設定が必要です (該当する場合は write も)。ログイン パスワードが設定された Telnet サービスを有効にする必要があります。また、syslog メッセージを RME サーバへ送信するように各デバイスを設定する必要があります。

Common Services

1. どのような管理機能があるか

Common Services は、一連のクライアント アプリケーション (各種 Management Center) に共通のサービスおよび管理機能を提供するサーバ環境です。これらのサービスおよび機能には、次のものが含まれます。

- データの保存および管理
- Web インフラストラクチャ
- セッション管理
- ユーザ認証およびアクセス権限管理
- 複数のクライアント アプリケーションの共用環境

サーバに Common Services がインストールされていないと、Management Center、Security Monitor、AUS などはインストールできません。これらのアプリケーションは Common Services に統合され、Common Services が提供するサービスと機能を使用します。

2. どのデバイスを管理できるか

Common Services はサーバ環境を提供するだけなので、特定のネットワーク デバイスを直接的には管理しません。通常は、Common Services 上にインストールされたアプリケーションによって管理が行われます。

3. どのサービスを有効にする必要があるか (アプリケーション プロトコルの要件)

Common Services は、VMS Management Center アプリケーションの Web インフラストラクチャの役割を担っています。したがってアプリケーション プロトコルという観点では、Web クライアントから Web サーバへの接続を維持することが重要になります。通常は、事前に割り当てられた次のポート番号を経由する HTTP トラフィックおよび HTTPS トラフィックがこれに該当します。

- TCP 1741 : CW デスクトップ ログイン セッション用の HTTP ポート
- TCP 1742 : CW デスクトップ ログイン セッション用の HTTPS ポート
- TCP 443 : すべての MC および AUS ユーザの Web セッション用の HTTPS ポート
- TCP 1751 : AUS OS および PDM イメージ ダウンロード用の HTTP ポート

Common Services で使用される TCP および UDP ポート番号の完全なリストについては、製品マニュアル『*Installing CiscoWorks Common Services on Windows 2000*』を参照してください。



Management Center for VPN Routers

1. どのような管理機能があるか

Router MC は、ハブ/スポーク型トポロジにおいて、複数の Cisco IOS Software デバイス間の VPN 接続を確立して管理するために用意された、便利な管理インターフェイスです。また、Router MC は、Cisco IOS Software デバイ스에搭載された PIX Firewall 機能セットをサポートしています (Cisco Catalyst 6000 シリーズスイッチは除く)。Router MC を使用すれば、大規模な Site-to-Site VPN においても、接続、セキュリティ、パフォーマンスなどの重要なパラメータを、すばやく簡単に調整できます。また、Router MC には、マウスで操作できる Web ベースのインターフェイスと、VPN 作成用の事前定義済みコンポーネントが用意されているので、シンプルな小規模 VPN をすばやく設定することができます。Router MC は、ハブ/スポーク型 VPN の設定だけでなく、専用回線接続を VPN 接続に切り替えたり、まだルータがネットワーク上に設置されていない状態で VPN 構成を作成することができます。

2. どのデバイスを管理できるか

Router MC は、Cisco IOS ルータおよび Catalyst スイッチに搭載された VPN Service Module によって構成される VPN を管理するために使用します。通常、このアプリケーションでは、ハードウェアプラットフォームの処理能力は重要な問題となりません。このアプリケーションで重要となるのは、Cisco IOS Software のバージョンと、サポートされている機能セットのみです。原則として、ルータは IPsec、Secure Shell Protocol (SSH)、および名前付きアクセスリストをサポートしている必要があります。表 11 に、Router MC でテスト済みの Cisco IOS Software バージョンを示します。

表 11： Router MC でサポートされる Cisco IOS Software バージョン

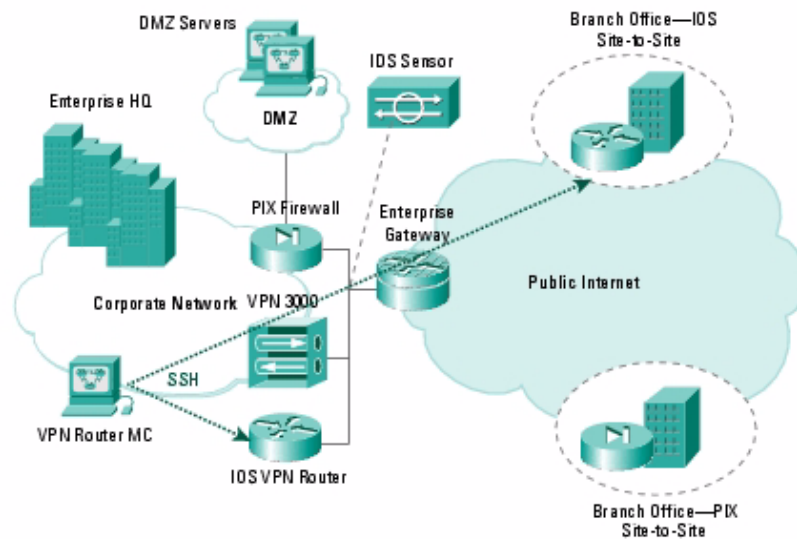
Cisco IOS ソフトウェア プラットフォーム	最小限の Cisco IOS ソフトウェア バージョン
7100、7200 (ハブ)	12.1(9)E
7400 (ハブ)	12.1(9)YE
3620/40/60 (ハブ)	12.2
71xx/72xx/74xx (スポーク)	12.1(9)E
XM 2600/10/11/20/21/22/50/51/91 および 3620/40/60	12.2
1710/20/21/50/51/60 (スポーク)	12.2
803、806、831、826、827 (スポーク)	12.2
3725、3745	12.2
VPN Service Module を搭載した Catalyst 6500	12.2(9)Y01



3. どのサービスを有効にする必要があるか (アプリケーション プロトコルの要件)

Router MC は、SSH (TCP ポート 22) を使用して Cisco IOS ルータを設定します。Router MC に初めてデバイスをインポートする際には、SSH セッションが確立されます。以後、デバイスへ設定をプッシュする際には、このセッションが SSH によって暗号化されます。図 4 に、Router MC が前述の基本トポロジの中でどのように応用されるかを図示します。

図 4 : Router MC の応用



Management Center for Firewalls

1. どのような管理機能があるか

Firewall MC では、新しいファイアウォールを設定したり、既存のファイアウォールの設定または設定ファイルをインポートする機能があり、PIX Firewall および Catalyst Switch Firewall Service Module を管理できます。ファイアウォールデバイスの設定、アクセスルール、変換ルールなどを設定できます。設定を変更したら、ネットワーク上のファイアウォールに展開することができます。また、Firewall MC には、設定およびステータスの変更を参照しながら、ネットワークに加えられた変更を制御できる強力なツールも用意されています。

2. どのデバイスを管理できるか

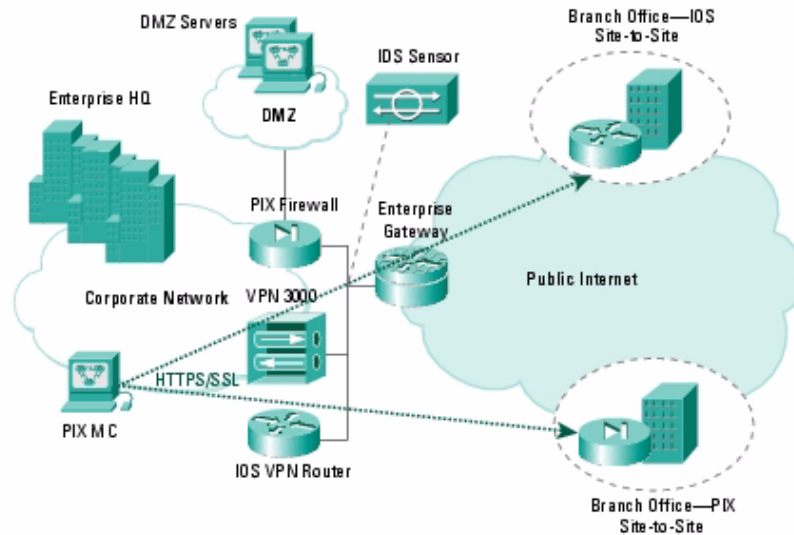
Firewall MC は、ネットワーク内に展開された PIX ファイアウォールおよびファイアウォール サービス モジュールを管理するために使用します。この中には、すべての PIX プラットフォームが含まれます (501、506E、515E、525、535、および Catalyst Firewall Service Module)。Firewall MC は、PIX OS バージョン 6.3 のほとんどのコマンドセットをサポートしています。



3. どのサービスを有効にする必要があるか (アプリケーション プロトコルの要件)

Firewall MC は、暗号化セッションを使用して、PIX Firewall デバイスおよびファイアウォール サービス モジュールを管理します。使用されるプロトコルは SSL (または HTTPS) で、この接続に割り当てられるポート番号は TCP ポート 443 です。したがって、Firewall MC を使用して適正にデバイスを管理するには、(管理インターフェイスから) PIX Firewall に対して TCP 443 の使用を許可する必要があります。図 5 に、Firewall MC が前述の基本トポロジの中でどのように応用されるかを図示します。

図 5 : Firewall MC の応用



Auto Update Server

1. どのような管理機能があるか

AUS には、PIX ファイアウォールの設定およびソフトウェアイメージを保管する機能があります。自動アップデートモードで動作しているファイアウォールは、定期的に AUS にアクセスして、ソフトウェアイメージ、設定、および PDM のバージョンをアップグレードし、デバイスの情報とステータスを AUS に渡します。また、AUS を使用すると、Dynamic Host Configuration Protocol (DHCP; ダイナミック ホスト コンフィギュレーション プロトコル) を使用してアドレスを取得するデバイスや、NAT の背後にあるデバイスの管理が容易になります。AUS にはこのような管理機能があるため、リモート サイトの PIX ファイアウォールから直接アクセスできる一般公開 DMZ に AUS を展開するのが一般的です。



2. どのデバイスを管理できるか

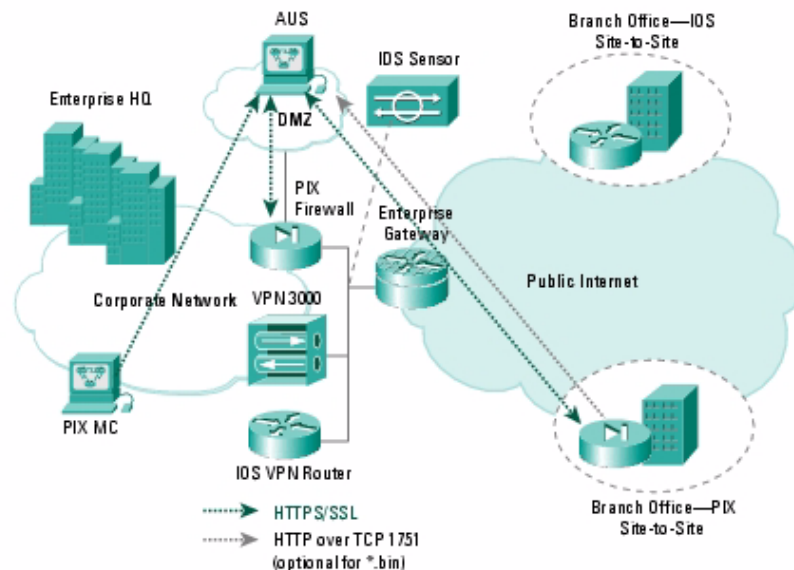
Firewall MC は、ネットワーク内に展開されたファイアウォールを管理するために使用します。この中には、すべての PIX プラットフォームが含まれます (501、506E、515E、525、535、および Catalyst Firewall Service Module)。AUS を利用するには、ファイアウォール側で OS バージョン 6.2 以降が実行されている必要があります (自動アップデート機能が必要なため)。

3. どのサービスを有効にする必要があるか (アプリケーション プロトコルの要件)

AUS は、前述のトポロジに含まれる 2 種類の要素と通信します。1 つ目の要素は、Firewall MC サーバです。これら 2 つのアプリケーションが同じシステムにインストールされている場合は、通信アーキテクチャについて何も注意する必要はありませんが、これらが別々のサーバにインストールされている場合は、SSL を使用して設定ファイルが Firewall MC から AUS にプッシュされるため、注意が必要になります。したがって、TCP 443 を AUS システムに対して開放する必要があります。

2 つ目の要素は、AUS と PIX Firewall の間の実際の通信です。この動作では、双方向の通信が行われ、いずれも SSL が使用されます。したがって、PIX Firewall から AUS への接続に対して TCP 443 を開放するだけでなく、逆方向の接続にも TCP 443 を開放する必要があります。バイナリ イメージの転送 (PIX および PDM ソフトウェア) には、標準の HTTP (TCP 1751) が使用されます (オプションで、SSL に変更することもできます)。図 6 に、AUS が前述の基本トポロジの中でどのように応用されるかを図示します。

図 6 : AUS の応用





Management Center for IDS

1. どのような管理機能があるか

IDS MC は、Cisco IDS センサーの設定を管理します。Web ベースの画面を通じて、センサーのあらゆる設定を管理できます。個々のセンサー、または設定が同じセンサーのグループを管理することができます。センサーの設定データは、データベースに保存されます。また、IDS MC には、シスコの Web サイトからアップデートアーカイブをダウンロードし、シグニチャアップデートを適切なセンサーに配布して、シグニチャのアップデートを実行する機能もあります。

Monitoring Center for Security (Security Monitor) は、このアプリケーションと密接な関係がありますが、完全に別個の製品です。Security Monitor には、ネットワークデバイスのイベントを収集、表示、集計し、相互に関連付け、レポートする機能があります。これについては、次のセクションで説明します。

2. どのデバイスを管理できるか

IDS MC は、Cisco IDS アプライアンス センサーおよび Catalyst 6500 用の Cisco IDS Module を管理します。このアプリケーションに必要な IDS ソフトウェアは、プラットフォームによって異なります (表 12)。

表 12 : IDS MC で必要とされる IDS センサー ソフトウェア

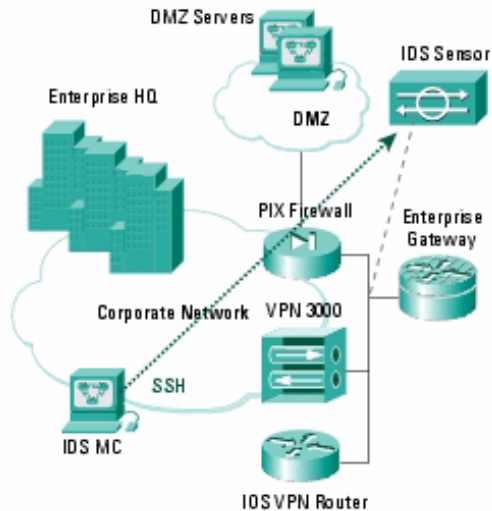
IDS センサー プラットフォーム	最小ソフトウェア要件
3.x Cisco IDS アプライアンス センサー	3.0.1
4.x Cisco IDS アプライアンス センサー	4.0.1
Catalyst 6000 IDS Module (IDSM-1)	3.0.5
Catalyst 6500 IDS Module (IDSM-2)	4.0.1

3. どのサービスを有効にする必要があるか (アプリケーション プロトコルの要件)

IDS MC は、密接に関連する 2 種類のプロトコルを使用して、IDS センサーを管理します。まず、SSH を使用して、センサーへの安全なリモート ログインを行います。次に、Secure Copy Protocol (SCP) を使用して、実際のセンサー設定ファイルの転送を暗号化します。SCP では、データの転送に SSH が使用されるため、センサーに対しては TCP 22 を開放するだけで済みます。図 7 に、IDS MC が前述の基本トポロジの中でどのように応用されるかを図示します。



図 7 : IDS MC の応用



Security Monitor

1. どのような管理機能があるか

Security Monitor は、次のデバイスのイベントをリアルタイムで収集、表示、集計し、相互に関連付け、通知する Web ベースのインターフェイスです。

- Cisco Intrusion Detection System Sensor (3.x および 4.x)
- Catalyst スイッチに搭載された Cisco IDS Service Module (IDSM-1 および IDSM-2)
- IDS ソフトウェアを実行している Cisco IOS ルータ
- Cisco Security Agent (Cisco Security Agent MC から転送)
- PIX Firewall
- Catalyst スイッチに搭載された Cisco Firewall Service Module

Security Monitor のイベントは、カスタマイズ可能なイベント ビューア上に表示されます。また、Security Monitor では、基本的なイベント関連付けルールを作成して、イベントを整理できます。リアルタイムで通知を発行するようにこれらのルールを設定することもできます。

2. どのデバイスを管理できるか

Security Monitor は、次のソフトウェア要件を満たす 5 つのソースからセキュリティ イベントを受信できます (表 13)。



表 13 : Security Monitor デバイスのソフトウェア要件

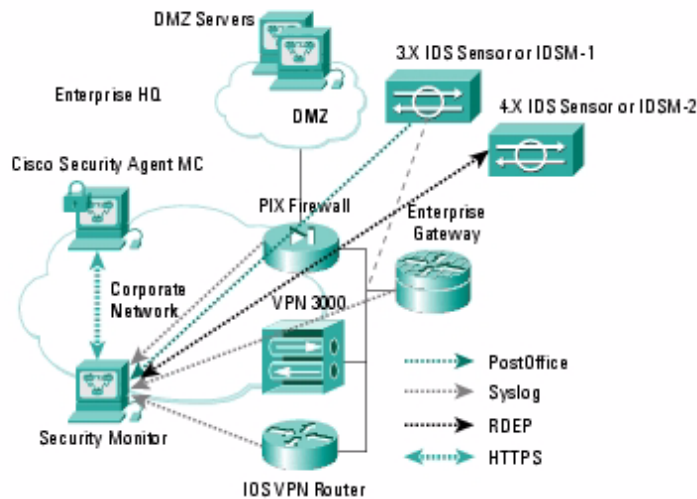
セキュリティ イベント ソース	最小ソフトウェア要件
3.x Cisco IDS アプライアンス センサー	3.0.1
4.x Cisco IDS アプライアンス センサー	4.0.1
Catalyst 6500 IDS Module (IDSM-1)	3.0.5
Catalyst 6500 IDS Module (IDSM-2)	4.0.1
Cisco IOS ルータ	IDS 機能セット (ip audit) 付き Cisco IOS Software
PIX Firewall	syslog をサポートするすべてのバージョン
Catalyst 6500 Firewall Module	6.3
Cisco Security Agent MC	4.0

3. どのサービスを有効にする必要があるか (アプリケーション プロトコルの要件)

Security Monitor には、非常に多くのデータ入力があるため、アプリケーションのプロトコル要件を個別に検討する必要があります。ソース デバイスが 3.x アプライアンス センサーおよび IDSM-1 IDS サービス モジュールの場合、Security Monitor は PostOffice プロトコルを使用してイベントを受信します。ソース デバイスが 4.x アプライアンス センサーおよび IDSM-2 IDS サービス モジュールの場合、Security Monitor は、(HTTPS ベースの) RDEP を使用してイベントをプルします。ソース デバイスが Cisco Security Agent の場合、Security Monitor は、HTTPS を使用して Cisco Security Agent MC からイベントをプルします。その他のデータ ソース (Cisco IOS Software、PIX Firewall、および Firewall Service Module) の場合、イベントは syslog を通じて Security Monitor に送信されます。したがって、Security Monitor サーバへの PostOffice (UDP 45000)、RDEP (TCP 443)、HTTPS (TCP 443)、および syslog (UDP 514) を許可する必要があります。図 8 に、Security Monitor が前述の基本トポロジの中でどのように応用されるかを図示します。



図 8 : Security Monitor の応用



VPN Monitor

1. どのような管理機能があるか

VPN Monitor の目的は、企業のヘッドエンド VPN デバイス、つまりハブ/スポーク型 VPN トポロジの「ハブ」についての監視統計情報を提供することです。前述の基本トポロジでは、Cisco 7x00 シリーズ ルータと Cisco VPN 3000 コンセントレータがこれに相当します。したがって、VPN Monitor サーバからこれらのデバイスへ適切に接続できるようにする必要があります。このアプリケーションは、VPN の統計情報をグラフおよび表の形式で表示します。また、(ユーザによる設定が可能) VPN 関連のしきい値を超えた場合に、視覚的な通知を提供するツールとしても使用できます。ネットワーク管理者は、VPN Monitor を使用して、暗号化トラフィック統計、セキュアハンドシェイク ネゴシエーション、パケットリレーなどの基準を参照し、VPN の稼動状況を全体的に把握できます。

2. どのデバイスを管理できるか

VPN Monitor は、必要な IPSec MIB に対応した Cisco IOS ルータ、および Cisco VPN 3000 コンセントレータをサポートしています。現在、このアプリケーションは、Cisco 1700、2600、3600、7100、および 7200 シリーズ ルータをサポートしています。ソフトウェア イメージ バージョンの要件は、次のとおりです。

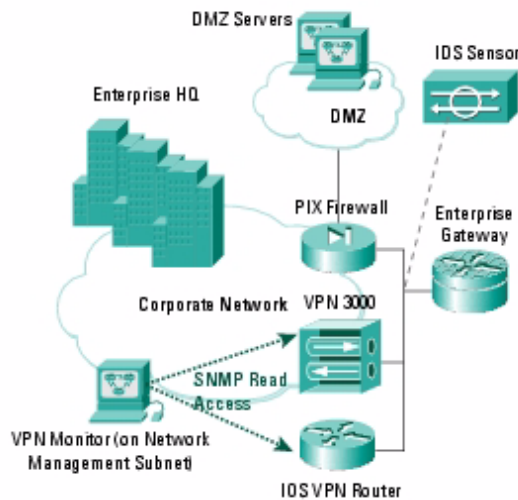
- Cisco 1700、2600、または 3600 シリーズ IOS ルータ : 12.2(4)T 以降
- Cisco 7100 または 7200 シリーズ IOS ルータ : 12.1(5a)E 以降
- VPN 3000 シリーズ コンセントレータ : 2.5.2f 以降



3. どのサービスを有効にする必要があるか (アプリケーション プロトコルの要件)

CiscoView と同様に、VPN Monitor を機能させるには SNMP (UDP ポート 161) を開放する必要があります。VPN Monitor サーバは、定期的にデバイスをポーリングして IPsec MIB 情報を取得します。これは純粋な監視ツールなので、この 2 種類のデバイスについて考慮する必要があるのは、SNMP get 操作のみです。これは、VPN Monitor で管理するネットワークデバイスについて SNMP read コミュニティストリングを設定する作業に対応しています。図 9 に、VPN Monitor が前述の基本トポロジの中でどのように応用されるかを図示します。

図 9 : VPN Monitor の応用



注： 上記の要件が満たされていれば、リモート VPN デバイス上で VPN Monitor を使用することも可能ですが、この方法は次の 2 つの理由から実用的ではありません。1) この監視方法ではスケーラビリティが低くなる。2) 多くの場合は、トンネルの両側ではなく、片側からのみ VPN 関連基準を参照するだけで十分である。

Cisco Security Agent MC

1. どのような管理機能があるか

Cisco Security Agent MC は、IDS MC および Security Monitor に組み込まれたネットワーク ベース IDS 管理機能を補完する製品です。これにより、VMS は侵入検知を管理するための真に包括的なソリューションとなります。Cisco Security Agent の目的は、個々のホストシステムを侵入から保護することです。このエージェントはホスト自体に常駐し、OS カーネルへのシステム コールを検査して、事前定義済みのルールおよびポリシーと照合します。イベントは、中央の Cisco Security Agent Management Center にレポートされます。Cisco



Security Agent Management Center では、管理対象のエージェントから受信した情報が統合されます。Cisco Security Agent では、ルールとの一致が検出された場合に、その操作を阻止するか、ユーザにプロンプトを出すかを選択することができます。また、それと同時に、リアルタイムで通知が発行されます。

この保護モデルでは、ユーザによる設定作業なしに、SQL (Structured Query Language) Slammer 攻撃や WebDAV 攻撃など、既知の脅威を緩和できることが実証されています。したがって、重要なネットワーク ホストでは、お客様の判断に基づいて、Cisco Security Agent を使用することが特に重要です。前述の基本トポロジでは、VMS ソリューションを形成するすべてのネットワーク管理サーバに Cisco HIDS エージェント コードをインストールすることをお勧めします。これにより、重要なネットワーク管理システムを保護することができます。また、リモートのデスクトップとラップトップに加え、すべての DMZ サーバにも Cisco Security Agent をインストールすることをお勧めします。これらのサーバまたはデスクトップからは、Cisco Security Agent MC にセキュリティ イベントがレポートされます。その情報は Security Monitor に転送することができます。

2. どのデバイスを管理できるか

Cisco Security Agent は、シスコのネットワーク デバイスとは直接対話しませんが、インストールされた Cisco Security Agent キットを使用してネットワーク ホストとは対話します。現在保護できる OS バージョンは次のとおりです。

サーバエージェントによる保護

- Windows NT v4.0 Server
- Windows NT Enterprise Server (SP 5 以降)
- Windows 2000 Server
- Windows 2000 Advanced Server
- Solaris 2.8 (64 ビット カーネル)

デスクトップエージェントによる保護

- Windows NT 4 Workstation (SP5 以降)
- Windows 2000 Professional
- Windows XP Professional

製品ドキュメントを参照して、Cisco Security Agent ソフトウェアの最新オプションを確認することをお勧めします。



3. どのサービスを有効にする必要があるか (アプリケーション プロトコルの要件)

Cisco Security Agent を適切に機能させるには、Management Center と通信できるようにする必要があります。エージェントは Management Center にセキュリティ イベントをレポートします。また、Management Center ではエージェント用のポリシー設定を変更することができ、エージェントは Management Center から定期的に最新のポリシーを取得します。この通信は、標準の HTTP および HTTPS を使用して実行されます。図 10 に、Cisco Security Agent Management Center が前述の基本トポロジの中でどのように応用されるかを図示します。

図 10 : Cisco Security Agent MC および Agents の応用



まとめ

VMS の各種コンポーネントを展開する場所を決定し、各コンポーネントで管理するネットワーク インフラストラクチャの要素を区別することが重要です。表 14 に、このセクションで説明した情報と、それぞれのアプリケーションを適切に機能させるために有効にする必要がある管理プロトコルをまとめます。

表 14 : VMS コンポーネントの一覧

アプリケーション	プロトコル	TCP/UDP ポート番号
CiscoView	SNMP	UDP 161
RME	SNMP, Telnet, TFTP, Syslog	UDP 161, TCP 23, UDP 69, UDP 514
Firewall MC	HTTPS (SSL)	TCP 443 ¹
AUS	HTTP, HTTPS, CNS	TCP 1751, TCP 443, TCP 11011
Router MC	SSH	TCP 22
VPN Monitor	SNMP	UDP 161
IDS MC	SSH, SCP	TCP 22
Security Monitor	PostOffice, RDEP, HTTPS	UDP 45000, TCP 443
Cisco Security Agent MC	HTTP, HTTPS	TCP 80, TCP 443

1. このポート番号はカスタマイズできます。TCP 443 は、デフォルト値です。



注意事項と解決方法

VMS を展開する際には、各アプリケーションで必要とされるサービスを把握しておくことが重要になります。これらについては、前のセクションで説明されています。状況によっては、2種類のアプリケーションが同じアクセス方式で特定のデバイスと通信する場合があります（たとえば、CiscoView と VPN Monitor は、どちらも SNMP を使用して管理情報を取得します）。また、一部の VMS アプリケーションではセキュリティに重点が置かれているため、デバイスへのアクセスを共有することにより、競合が発生する可能性があります。このセクションでは、この文書に記載されている展開ガイドラインから逸脱する場合の重要な考慮事項について説明します。

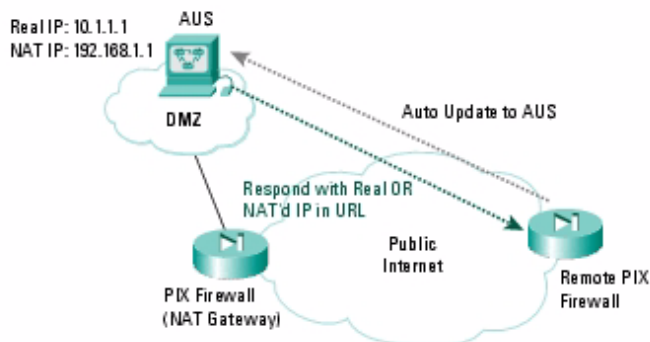
NAT に関する考慮事項

NAT はさまざまなトポロジで使用されています。NAT はセキュリティおよびアドレス空間を確保する上で便利な機能ですが、管理ツールと併用すると問題が発生する場合があります。このセクションでは、NAT を使用しているネットワーク環境に VMS を展開する場合の注意事項と問題点について説明します。

•NAT と AUS

AUS アプリケーションを使用していて、サーバが NAT ゲートウェイの背後にある場合は、管理対象となる PIX ファイアウォールに対して特に注意する必要があります。AUS サーバと通信するリモート PIX があると仮定します。このデバイスは、（リアルアドレスではなく）NAT アドレスにアクセスします。AUS は、更新された設定またはソフトウェアイメージをダウンロードするための URL を通知する際に、NAT アドレスを使用します。反対に、AUS が NAT ゲートウェイの背後にない場合は、リアルアドレスを通知するように設定することができます。管理対象となるすべての PIX ファイアウォールに対して NAT アドレスとリアルアドレスのどちらを使用するかを決定する必要があります。1つの AUS インストール内で、これら2つ（NAT と非 NAT）を併用することはできません（図 11）。

図 11 : NAT と AUS



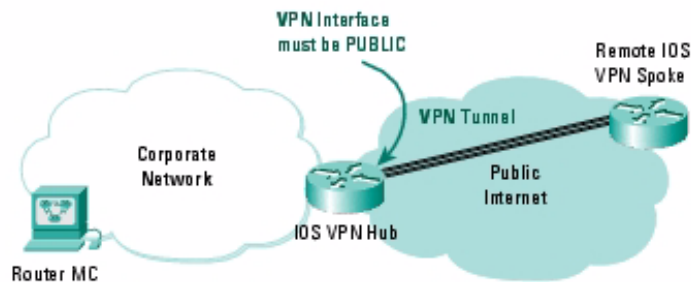


内部および外部の PIX ファイアウォールを両方管理する必要がある場合は、AUS を 2 コピー インストールすることをお勧めします。1 つは、外部ファイアウォール用として NAT アドレスを使用し、もう一つは内部ファイアウォール用としてリアル IP アドレスを使用します。NAT の設定は、AUS の Admin タブで変更できます。

•NAT と Router MC (ハブ側)

Router MC を使用してハブ / スポーク型の VPN 環境を構築する場合は、ハブ ルータの VPN インターフェイスに注意する必要があります。製品の設計上、このインターフェイスでは NAT 処理を行えません。VPN 終端インターフェイスは、パブリック アドレスを持つ IP サブネットになっている必要があります。このインターフェイスのアドレスが NAT 処理されている場合、ピアの観点からも NAT 処理されたアドレスを割り当てる必要がありますが、Router MC アプリケーションでは、IP アドレスではなく、インターフェイスを基準として割り当てることしかできません。したがって、ピアのステートメントが不正確になります。Router MC と互換性を持つ VPN トポロジを構築する方法については、図 12 を参照してください (ハブ ルータを NAT デバイスの背後に配置することはできませんが、ハブ ルータの IP を NAT 処理しないでください)。

図 12 : NAT と Router MC



•NAT と Router MC (スポーク側)

NAT と VPN スポーク デバイスに関しても、展開上の注意事項があります。現行バージョンの Router MC は、スポークの IP アドレスが NAT 処理されている状況をサポートしていないため、Router MC では、リアル IP アドレスを使用してスポーク デバイス (VPN ピア) を管理する必要があります (スポーク ルータを NAT デバイスの背後に配置することはできませんが、スポーク ルータの IP を NAT 処理しないでください)。

複数の Syslog デーモン

VMS バンドルに含まれるアプリケーションには、さまざまなソースから syslog メッセージを受信できるものがあります。OS のサポートが変更されたことにより、これらのアプリケーションすべてを 1 台のサーバにインストールすることが可能になりました。その場合は、これらすべての syslog デーモンの互換性をどのように確保するかを検討する必要があります。



最初に、syslog メッセージを受信できるアプリケーションと、syslog メッセージのソース デバイスを確認します (表 15)。

表 15 : VMS の Syslog サーバ アプリケーションの一覧

VMS モジュール	Syslog ソース
RME	Cisco IOS Software、PIX、VPN3K
Security Monitor	Cisco IOS Software、PIX、Firewall Service Module

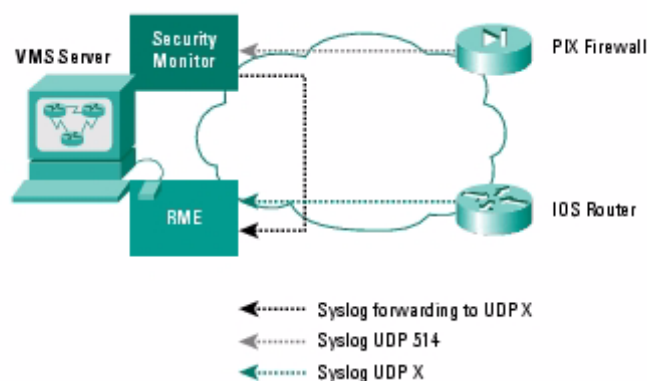
デフォルトでは、これらすべてのアプリケーションが UDP ポート 514 でリスニングを行います。これらのアプリケーションが別々のサーバに分散されている場合は、(複数のソースに syslog メッセージを送信するだけなので) まったく問題は起きません。しかし、これらすべてのアプリケーションが 1 つのシステム上にインストールされている場合、すべての syslog デーモンを利用するとどうなるでしょうか。

Security Monitor を使用すると、2 つの方法でこの問題を緩和することができます。1 つは、syslog メッセージのリスニングを行うポート番号を設定する方法です。デフォルトは UDP 514 ですが、この設定は変更できます。また、同じシステムまたは別のシステム上の他のポートに syslog メッセージを転送するように Security Monitor を設定することもできます。PIX ファイアウォールは同じホストの異なるポート番号に syslog メッセージを送信できるという点も重要です。その場合は、次の方法で syslog 機能を最適化することができます。

- Cisco IOS Software から、RME 宛てに syslog を送信する (UDP X)
- PIX から、Security Monitor 宛てに syslog を送信する (UDP 514)
- Security Monitor から、RME に syslog を転送する (ポート X)

図 13 に、この統合方法を図示します。

図 13 : VMS での Syslog の統合





このシナリオでは、最低 2 台のサーバを使用して、3 つのツールすべてを利用するのが理想的です。一方のシステムでは Security Monitor を実行し、もう一方のシステムでは RME を実行します。

Cisco Security Agent の初期展開

VMS バンドルの主要コンポーネントの 1 つは、ホストレベルで侵入検知 / 防止を管理する機能です。VMS の管理サーバはきわめて重要なので、それらのシステムには Cisco Security Agent ソフトウェアをインストールすることをお勧めします。また、VMS バンドルの Cisco Security Agent MC には、デフォルトのポリシーグループ「VMS server」が含まれています。

エージェントキットを初めて展開する際には、「テストモード」でエージェントを配置することをお勧めします。テストモードでは、すべてのルール違反がログに記録されますが、実際の対処は行われません。最初の数週間ほど「テストモード」で通常どおりに使用すれば、このテスト期間中に発生したイベントに基づいて、基本的なポリシーを作成することができます。

アウトバンド管理

多くのネットワークでは、隔離された管理用サブネットを設計するのが望ましいと言えます。これはアウトバンド管理と呼ばれ、管理ステーションが管理対象のネットワーク要素から分離されたサブネット上にある状況を指します。セキュリティのレベルが高くなり、ネットワーク内部の機能区分が明確になるため、この方法は多くのネットワーク管理者にとって魅力的です。

ただし、すべてのネットワーク管理ツールと同様に、VMS は管理対象デバイスへのネットワークアクセスを必要とします。したがって、完全に隔離された管理サブネットを構築するのは一見望ましいことですが、ネットワークの他の部分に IP 接続できなければまったく意味がありません。そのような環境で VMS を展開する場合は、この点を注意深く検討する必要があります。

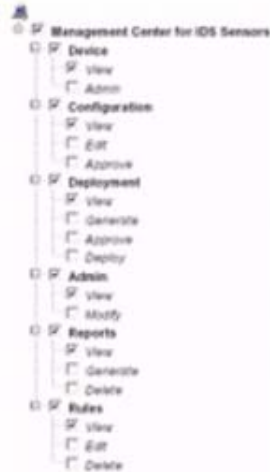
ACS との統合によるロールベース アクセス コントロール

CiscoWorks VMS には、7 種類のユーザロール (HelpDesk、Approver、Network Operator、Network Admin、System Admin、Export Data、Developer) が組み込まれており、各ユーザには 1 つまたは複数のロールを割り当てることができます。これらのロールでは、GUI で実行できる操作の権限が固定されています。

より緻密で柔軟なロールベース アクセス コントロール (RBAC) を可能するには、VMS と ACS を組み合わせ、各ユーザに許可する操作を細かく制御する必要があります。たとえば、ACS の「Read Only」ユーザロールは、図 14 のように設定することができます (写真は ACS の画面)。



図 14 : ACS での Read Only ユーザ ロールの設定



結論と要約

VPN とセキュリティの進化

近年、ネットワークセキュリティ関連のニーズが急速に高まりつつあります。特に、境界ネットワークセキュリティ、パブリック インフラストラクチャを介した安全なトランザクション、およびエンドシステムでの広範囲なセキュリティという3つの分野におけるニーズが顕著です。その結果、このような環境に対処するための管理方式を進化させる必要が生じ、CiscoWorks VPN/Security Management Solution (VMS) が導入されました。

CiscoWorks VMS は、Cisco IOS VPN ルータ、Cisco VPN Service Module、Cisco PIX Firewall、Cisco Firewall Service Module、Cisco Network IDS Sensor、Cisco Network IDS Service Module、ホストベースの Cisco Security Agent など、セキュリティ専用ハードウェアの管理を支援するアプリケーションで構成されています。VMS は、VPN の展開、監視、境界セキュリティポリシーの作成、侵入検知の管理など、さまざまな課題に対処できます。本書では、このソリューションの各種コンポーネント、その役割、および複数のコンポーネントを連携させるための設定方法を説明することで、VMS を展開するための基本的なガイドラインを提示しています。本書は、VMS をネットワーク管理計画に組み込む方法、および VMS によって付加される価値を明確に理解できるように構成されています。

他のダイナミックな環境と同様に、ネットワークセキュリティに関連するニーズとテクノロジーは常に進化しています。VMS は、ネットワーク管理という観点から今後も進化し続け、この環境に固有の側面を管理するための包括的なツールを提供し続けていきます。

1 AUS の主な目的は、リモートの PIX ファイアウォールに設定およびソフトウェアのアップデートを提供することです。したがって、組織の DMZ 内に AUS を配置することをお勧めします。その場合は、AUS 専用のサーバを使用することをお勧めします。

©2004 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、および Cisco ロゴは米国およびその他の国における Cisco Systems, Inc. の商標または登録商標です。
この文書で説明した商品、サービスはすべて、それぞれの所有者の商標、サービスマーク、登録商標、登録サービスマークです。
この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ株式会社

URL: <http://www.cisco.com/jp/>

問合せ URL: <http://www.cisco.com/jp/service/contactcenter/>

〒107-0052 東京都港区赤坂 2-14-27 国際新赤坂ビル東館

TEL.03-6670-2992

電話でのお問合せは、以下の時間帯で受け付けております。

平日 10:00 ~ 12:00 および 13:00 ~ 17:00

お問い合わせ先