

Cisco Secure PIX[®] Firewall バージョン6.0

概要

業界をリードするCisco Secure PIX[®] Firewall シリーズは、今日のネットワーク利用者に対し、比類のないセキュリティ、信頼性、およびパフォーマンスを提供します。これは、完全にステータフルのファイアウォール保護、およびIPsec (IP Security) VPN (仮想プライベートネットワーク)機能を実現するハードウェアとソフトウェアの統合パッケージであり、外部の侵入から内部ネットワークを厳重に保護します。一般的に使われているプロキシサーバはCPUに負荷が集中して、通信におけるボトルネックになることがあります。これに対してSecure PIX Firewallは、UNIXで実装されておらず、安全かつリアルタイムな組み込みシステムを使用しています。従来の柔軟性とスケーラビリティに加え、幅広い種類のプラットフォームや機能を選択できることから、PIXは顧客のあらゆる要件を満たします。

Cisco Secure PIX Firewall専用オペレーティングシステムの最新リリースであるバージョン6.0は、新たに改善されたPIXの機能、パフォーマンス、およびセキュリティに加え、数々の新機能を提供します。

PIX Device Manager

Cisco PIX Device Manager (PDM) は、ブラウザベースの設定ツールです。このツールを使用すると、PIX Firewallのコマンドラインインタフェース (CLI) についての深い知識がなくても、PIX Firewallのセットアップ、構成、監視を行うことができます。

VPN Client サポートの追加

Cisco VPN Client バージョン 3.0 (統合 VPN Client フレームワーク)

実装と運用の簡単なCisco VPN Clientを使用すると、顧客は安全なエンドツーエンドの暗号化トンネルを構築できます。クライアントは、展開する前に設定しておくことで導入が用意になり、初期ログイン時にユーザーが実行しなければならないことはほとんどありません。VPNのアクセスポリシーと構成はCisco Secure PIX Firewallから

ダウンロードされ、接続が確立された時点でクライアントに送られます。このように、高度なスケーラビリティの実現に加え、展開と管理を簡略化できます。Cisco VPN Clientは、Windows 95/98/Me/NT 4.0/2000に対応しています。

レイヤ2 トンネリングプロトコルのサポート

Cisco Secure PIX Firewallには、Windows 2000 OSに組み込まれたレイヤ2 トンネリングプロトコル (L2TP) クライアントによって開始されたVPNトンネルを終端する機能があります。L2TPにより、リモートクライアントは公衆IPネットワークを使用して、企業の専用線ネットワークと安全に通信できるようになります。また、L2TPでは認証が可能なので、IPsecと併用することで、暗号化された安全なトンネルをクライアントに提供できます。

音声拡張

Skinny プロトコルのサポート

Cisco Secure PIX Firewallのアプリケーションの処理方法が拡張され、Cisco IP PhoneでのVoIP 通話シグナリングに使用されるSCCP (Skinny Client Control Protocol) が新たにサポートされます。この機能は、メディアセッション、およびネットワークアドレス変換 (NAT) 組み込みのIPアドレスに対し、動的に「穴」を空けます。SCCPはIPテレフォニーをサポートし、H.323環境と共存可能です。アプリケーションレイヤでは、すべてのSCCPシグナリングとメディアパッケージがPIX Firewallを通過し、H.323端末と相互運用できることが保証されます。

SIP (Session Initiation Protocol) による拡張

IETF (Internet Engineering Task Force) の規定するSIP (Session Initiation Protocol) は、呼設定セッション、特に2者間音声会議 (「通話」) を実現します。SIPはSDP (Session Description Protocol) と協調して動作し、呼設定に先がけて呼を定義します。SIPを使用することで、Cisco Secure PIX FirewallはVoIP (Voice-over-IP) およびVoIpを使用するあらゆるプロキシサーバをサポートできます。本バージョンでの拡張機能は以下のとおりです。

- UDP (User Datagram Protocol) シグナリングおよび TCP (Transmission Control Protocol) シグナリングメッセージに対するアドレス変換
- 複数の通話区間 (コールレグ) をサポート
- SIP プロキシのサポート
- 外線からの接続を新しいシグナリング接続によって終端、自動転送、保留、通話転送できるようにするための初期接続での UDP サポート

バージョン 6.0 の新規機能

動的な排除

この機能により、Cisco Secure PIX Firewall に Cisco IDS センサを組み合わせると、新規接続を遮断し、あらゆる既存接続からのパケットを禁止することで、攻撃ホストに動的に対処できます。Cisco Secure IDS デバイスは、トラフィックの送信元に悪意があると判断すると、PIX Firewall に対し、この送信元からのトラフィックを排除するよう指示します。排除 (shun) コマンドは、攻撃を受けるインタフェースに対し、特定の期間に渡るブロック機能を適用します。Cisco Secure IDS マスタユニットによりこのブロック機能が解除されない限り、攻撃ホストの IP アドレスを含むパケットは破棄および記録されます。この IP ソースアドレスからのあらゆるトラフィックは、PIX Firewall 上の通過を禁止され、残りの接続はすべてタイムアウトされます。排除コマンドのブロック機能は、指定のホストアドレスによる接続が現在アクティブかどうかに関わらず適用されます。排除関連の統計は、show コマンド、syslog メッセージ、および PIX Device Manager (PDM) によるモニタリングによって参照できます。

PAT によるポートのリダイレクション

Cisco Secure PIX Firewall バージョン 6.0 は、静的な PAT (Port Address Translation) 機能を新たに提供します。これは、1 つのグローバルアドレスを介して、複数の受信 (インバウンド) TCP または UDP サービスを異なる内部ホストへ送信する機能です。このグローバルアドレスには、一意のアドレス、共有発信 (アウトバウンド) PAT、または外部インタフェースとの共有アドレスのいずれかを使用できます。

HTTP セッションのステートフルな共有

Cisco Secure PIX Firewall は、冗長ホットスタンバイユニットの実装によって、高度な可用性を実現します。このフェイルオーバーオプションは、ステートフルな自動同期により、複数の同時接続を維持します。この機能により、システム障害が発生した場合であってもセッションが維持され、経路切り替えがネットワークユーザーにとっては完全

に透過的となることが保証されます。PIX Firewall バージョン 6.0 には、HTTP (ポート 80) セッションを維持する機能が追加されました。

CPU 稼働状態

本バージョンには、PIX 上の CPU 負荷を監視する機能が新たに加えられました。show コマンドと PDM モニタリングを使用すると、5 秒間、1 分間、および 5 分間の CPU 稼働状態の統計を表示できます。

アクセス制御リストの syslog メッセージにポート番号を表示

syslog メッセージには、アクセス制御リスト (ACL) によって拒否されたパケットに含まれる TCP/UDP ポート番号が追加されるようになりました。

10 種類のイーサネットインタフェース

組み込みシステムの利点を損なうことなく必要に応じたプラットフォームの拡張を可能にするため、Cisco Secure PIX Firewall シリーズは 1 ポートまたは 4 ポート 10/100 ファーストイーサネット NIC、およびギガビットイーサネット NIC をサポートします。バージョン 6.0 の PIX ソフトウェアを使用すると、制限なしのライセンスによる Cisco Secure PIX Firewall 535 では、最大 10 種類のイーサネットインタフェースをサポートできます。制限付きライセンス製品では、最大 8 種類のイーサネットインタフェースのサポートが可能です。

技術仕様

互換性

VPN Client : Cisco Secure VPN Client バージョン 1.1、または Cisco VPN 3000 Client バージョン 2.5 以上いずれのクライアントも Windows 95、Windows 98、および Windows NT 4.0 に対応

システム要件

ハードウェアプラットフォーム : Cisco Secure PIX Firewall 506、515、520、525、または 535
ランダムアクセスメモリ : 32 MB
フラッシュメモリ : 16 MB (PIX 506 に 8 MB 必要)

発注情報

PIX-CONN-VER= PIX Software Upgrade (サポート対象外のお客様用)



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/go/cnac/>

〒100-0005 東京都千代田区丸の内 3-2-3 富士ビルディング

TEL.03-5645-8856 FAX.03-5641-3523

お問い合わせ先