

Cisco Secure PIX Firewall ソフトウェア v5.2

世界最先端のCisco Secure PIX Firewall™ シリーズは、比類ないセキュリティ、信頼性、そしてパフォーマンスを今日のネットワークを使用するお客様に提供します。ハードウェア/ソフトウェア統合型のパッケージにより、完全なステートフルファイアウォール保護機能とIPSec (IP Security) VPN (仮想プライベートネットワーク) 機能を提供して、内部ネットワークを外部から厳重に保護します。

概要

Cisco Secure PIX Firewall は、CPU を大量に消費する一般的なフルタイムのプロキシサーバと異なり、非UNIXの安全なリアルタイムの組み込みシステムを使用します。実績ある柔軟性とスケラビリティ、そして広範なプラットフォーム/機能オプションを備えるPIXは、お客様のあらゆるニーズを満たします。

Cisco Secure PIX Firewall 専用オペレーティングシステム (OS) の最新リリースであるバージョン5.2は、最新のPIX機能、パフォーマンス、改善されたセキュリティ機能、そして新機能を提供します。

8つ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保持しながら必要なプラットフォームの拡張性を提供するために、Cisco Secure PIX Firewall シリーズは広範なネットワークインタフェースカード (NIC) をサポートしています。標準NICとして、1ポートまたは4ポートの10/100ファーストイーサネット・カード、ギガビットイーサネット・カード、4/16トークンリング・カード、およびデュアルアタッチ・マルチモードFDDIカードが用意されています。PIXソフトウェアバージョン5.2を使用すると、525-URなどのPIX Firewallで、最大8つのイーサネットインタフェースをサポートできます。

侵入検出機能

Cisco Secure PIX Firewallには、新たに侵入検出テクノロジーが装備されています。これは、あらゆるネットワーク境界、特にネットワークセグメントの間に追加セキュリティが必要とされるロケーションに最適です。また、イントラネット、エクストラネット、およびブランチオフィスのインターネット境界でさらに高いビジビリティ (可視性) を提供します。

PIX Firewallの侵入検出システム (IDS) は、ネットワークトラフィックの悪用パターンを検出するためのシグネチャを使って、53の一般的な攻撃を識別します。これらのシグネチャは、最も一般的なネットワーク攻撃や情報収集スキャンなどのセキュリティ違反を表します。

この機能を備えたPIXは、インライン侵入検出センサとして機能します。PIXはファイアウォールを通過するパケットやセッションを監視して、いずれかのIDSシグネチャと一致するかどうかについて、それぞれをスキャンします。不審なアクティビティが検出されると、PIXは直ちに対応します。この対応については、次のような設定ができます。

```
syslog サーバにアラームを送信する
パケットを廃棄する
TCP ( Transmission Control Protocol ) 接続をリセットする
```

柔軟性を念頭に置いて開発されたPIX IDSでは、検出されたインタフェースに応じてシグネチャへの対応を変えることができます。また、PIXでは、疑わしい現象が何度も検出された場合に、そのシグネチャだけを無効にすることもできます。

DHCP クライアント / サーバのサポート

PIX Firewallでは、DHCP (Dynamic Host Configuration Protocol) のサポートしています。DHCPとは、アドレスを要求しているクライアントに対してアドレスプールからTCP/IPアドレスを自動的に割り当てる方法です。DHCPによって静的なIPアドレスを手動で割り当てる必要がなくなります。PIXにDHCPクライアント/サーバ機能が実装されていることで、高価で煩雑な静的なIPアドレスの維持が必要なくなり、特にケーブルおよびDSL (デジタル加入者線) ブロードバンド環境への展開が大幅に簡素化されます。

DHCP クライアント

DHCPクライアントをサポートするPIXは、信頼できないインタフェースのIPアドレス、ネットマスク、およびオプションとしてDSLまたはケーブルISP（インターネットサービスプロバイダー）からのデフォルトルートを手動的に取得できます。この機能は、PIXがDSLまたはケーブルモデム/ルータに直接接続されている場合に最も有用です。

DHCP サーバ

PIXは、信頼できるネットワークに設置されているホストにDHCPサービスを提供することが可能となっており、動的アドレス指定が設定されているマシンに自動的にIPアドレスを割り当てることができます。

Cisco VPN 3000 Client

Cisco VPN 3000 Clientバージョン2.5を使用しているリモートアクセスVPNユーザーは、PIX Firewallを通して自社のネットワークに安全なアクセスを行うことができます。

Cisco Secure VPN Clientとは異なり、Cisco VPN 3000 Clientでは、ゲートウェイによってポリシー情報をVPN 3000 Clientにプッシュする必要があります。VPN 3000 Clientをサポートするために、PIX Firewall内のIKE（Internet Key Exchange）モード構成機能が拡張されて、DNS（ドメインネームシステム）、WINS、デフォルトドメイン、およびスプリットトンネルモード属性をVPN 3000 Clientにダウンロードできるようになっています。スプリットトンネルモードによって、PIX Firewallは、クリアテキスト形式またはIPSecトンネルによる暗号化形式で、ネットワークインタフェースにパケットを送ることができます。追加された新しいPIX Firewallコマンドを使用すると、クライアントポリシー属性を設定することで、VPNグループ名と関連付けられた所定グループのVPN 3000 Clientにダウンロードできるようになります。こうした新しいコマンドは、VPN 3000 Clientポリシーグループを構成するために追加されています。

VPN 3000 ClientがPIX Firewallを使ってISAKMPを開始すると、VPNグループ名と事前に分配されたキーがPIX Firewallに送信されます。そしてPIX Firewallは、グループ名を使って所定のVPN 3000 Client用に構成されたクライアントポリシー属性を調べ、該当するポリシー属性をIKEネゴシエーション時にクライアントにダウンロードします。

ユーザー名とグループによる Websense フィルタリング

PIX FirewallはWebsense Enterpriseソフトウェアと連携してURLをアクティブにフィルタリングすることで、ユーザーがアクセスできるWebサイトを制御します。PIX v5.2の新機能では、ホストとPIX Firewallの間でグループとユーザー名の認証を行うことができます。PIX Firewallがユーザー名のルックアップを実行し、次にWebsenseサーバがURLフィルタリングとユーザー名を記録します。Websense プロトコルバージョン4では、次の機能が拡張されています。

URLフィルタリングにより、PIX Firewallは、Websenseサーバで定義されたポリシーに対して、発信するURLリクエストをチェックできます。

ユーザー名ロギングは、Websenseサーバ上のユーザー名、グループ、およびドメイン名を追跡します。

ユーザー名ルックアップにより、PIX Firewallは、ユーザー認証テーブルを使ってホストのIPアドレスをユーザー名にマップできます。

Secure Shell

これまで、PIX Firewallをリモートで構成するには、Telnet接続を開始する必要がありました。この方法では、Telnetが提供するだけのセキュリティ、つまり下位層の暗号化（IPSecなど）やアプリケーションセキュリティ（リモートホストでのユーザー名/パスワード認証）が可能でした。今では、PIXはSSH（Secure Shell）バージョン1をサポートしています。SSHは、TCP/IPのような信頼性の高いトランスポート層の上で動作するアプリケーションで、強力な認証および暗号化機能を提供します。SSHは、ネットワークを通じた別のコンピュータへのログオン、リモートでのコマンドの実行、およびあるホストから別のホストへのファイルの移動をサポートします。

PIXでは、最大5台のSSHクライアントがPIX Firewallコンソールに同時にアクセスできます。PIX Firewallに対するSSH接続の開始を認可される特定のホストやネットワークを定義したり、接続解除するまでのセッションのアイドル時間を指定できます。SSHは、DES（データ暗号規格）または3DES（Triple DES）有効化キーでのみ使用できます。

Certificate Authority（認証局）サーバ

PIX Firewallは、EntrustおよびVerisignのCA（Certificate Authority）サーバのサポートに加えて、BaltimoreのUniCert Certificate Management SystemとMicrosoft Windows 2000 Advanced Serverもサポートしています。

CA（認証局）とは、身元を確認とデジタル証明書の発行を行う、信用できるサードパーティです。CAは、デジタル認証リクエストの管理と、参加しているIPSecネットワークピアに対する証明書の発行を行います。これらのサービスは、参加しているピアにキーの集中管理機能を提供し、IPSecネットワークデバイス（ピア）の管理を簡素化します。

TCP インターセプト

新しいTCPインターセプト機能により、PIXは、TCP SYN 攻撃を受けやすいシステムに拡張保護機能を提供します。オプションの初期接続制限に達した後、初期接続数がこのしきい値未満になるまでは、影響を受けるサーバの全SYNパウンドがインターセプト(傍受)されます。それぞれのSYNに対して、PIX Firewallは空のSYN/ACKセグメントを使ってサーバの代わりに応答します。PIX Firewallは、関連するステート情報を保持し、パケットをドロップして、クライアントの確認を待ちます。ACKが受信されると、クライアントのSYNセグメントのコピーがサーバに送信されて、PIX Firewallとサーバの間でTCPの3方向ハンドシェイクが実行されます。この3方向ハンドシェイクが完了した場合のみ、通常どおり接続が再開します。接続段階中にクライアントが応答しない場合は、PIX Firewallは指数関数的バックオフを使って必要なセグメントを再送信します。

ユニキャスト RPF (Reverse Path Forwarding)

IPプロトコルのIPスプーフィング(代理応答)には潜在的な危険性があるため、可能な場合はこのリスクを減らすための対策をとる必要があります。ユニキャストRPF(Reverse Path Forwarding)またはリバースルートルックアップ(逆経路調査)は、特定の環境でこうした操作を防ぐために効果的な方法です。ユニキャストRPFは、インタフェースへの着信パケットをふるいにかける入力機能です。PIX v5.2では、RFC 2267に記述されているネットワークの入口側(インGRESS)または出口側(イーグレス)フィルタリングを使ってIPスプーフィング攻撃から保護するインタフェースを指定できます。

インGRESSフィルタリング

インGRESSフィルタリングは、IP送信元アドレスの完全性について着信パケットをチェックします。着信パケットに送信元アドレスがないと、ルートが分からないため、そのパケットが送信元に戻るための最善のパスを使って到着したのかどうかは分かりません。ルーティングエンティティはすべてのネットワークに対するルートを維持することはできないため、このような事態はしばしば発生します。

イーグレスフィルタリング

イーグレスフィルタリングは、管理ドメイン外部のホストに宛てられたパケットが、実施するエンティティのローカルルーティングテーブル内のルートで検証できるIP送信元アドレスを持っていることを確認します。出て行くパケットが送信元に戻る際に最善リターンパスに到着しなければ、パケットは廃棄されてアクティビティが記録されます。イーグレスフィルタリングは、内部ユーザーがローカルドメイン外部のIP送信元アドレスを使って攻撃を開始するのを阻止します。ほとんどの攻撃ではIPスプーフィングを使って攻撃元ホストの身元を隠すため、イーグレスフィルタリングによって攻撃の出所の追跡作業がはるかに簡単になります。イーグレスフィルタリングを使用すると、これによってIP送信元アドレスは有効なネットワークアドレスプールから取得されるようになります。実施するエンティティにローカルのアドレスは、容易に追跡できます。

構成可能なフェイルオーバーポーリング

PIX Firewallのステートフルフェイルオーバーオプションは高い可用性を保証して、シングル障害ポイントをなくします。2つのPIX Firewallが並行して動作している場合に、1つに障害が発生すると、2番目のPIX Firewallがセキュリティオペレーションを自動的に維持します。デフォルトでは、2台のユニットがフェイルオーバー「hello」パケットを15秒ごとに互いに送信します。このデータはプライマリまたはセカンダリユニットのIDと他方のユニットの電源ステータスを提供し、2台のユニット間の様々なフェイルオーバー通信のリンクとして機能します。PIXソフトウェアv5.2では、フェイルオーバー「hello」パケットの間隔を設定できます。これには、3秒間(最小)から15秒間(最大)までの値を指定できます。ポーリング間隔が短いほど、PIX Firewallは速やかに障害を検出してフェイルオーバーを実行できます。

RADIUS グループアクセスリスト

PIX Firewallは、RADIUS認証サーバのユーザーグループ属性を受け付けるようになりました。PIX Firewallは、ユーザーを認証した後で、認証サーバから戻されたCisco Secureアクセスコントロールサーバ(ACS)のACL属性を使用して、所定ユーザーグループのアクセスリストを識別できます。たとえば、営業、マーケティング、エンジニアリングといった会社の各部門ごとにアクセスリストが存在する場合があります。一貫性を保つために、PIX FirewallはTACACS+にも同じ機能を提供します。

ICMP アクセスリスト

PIXは、ICMP(Internet Control Message Protocol)アクセスリストを使って、PIXで終端するICMPトラフィックを許可/拒否することができます。本質的には、インタフェースへのpingを有効/無効できるということです。pingを無効にすると、PIX Firewallは実質的にネットワーク上で検出不可能になります。

IP フラグメンテーション

次のIPフラグメンテーション(またはTeardrop)攻撃が検出された場合に、それを示すためのSyslogメッセージが追加されました。またPIXは、その同じIP IDの全パケットフラグメントを自動的に廃棄します。

PIX Firewallやその背後のシステムがIPフラグメンテーション攻撃を受けている場合、または、フラグメント攻撃を阻止するためにしきい値が設定されたことにより、PIX Firewallが処理できる以上のフラグメントを正当に受信している場合、有効なIPパケット(65535バイト)より長いことを自ら報告するフラグメントが到着した場合、これは、既知のバグを持つIPスタックを破壊するための攻撃、または破損したIPスタックからのパケットを意味する可能性があります。IPフラグメントが廃棄された場合に表示されます。

PAT IP アドレス共有

PIX ユーザーは、ポートアドレス変換 (PAT) のために、外部インタフェースについて単一のグローバル IP アドレスだけを持つ場合があります。これにより、DHCP が検索したアドレスを PAT で使用できるようになるため、これは DHCP の構成にとって重要な機能です。インタフェースで PAT を有効にすると、TCP、UDP (User Datagram Protocol) および ICMP サービスの損失はゼロになります。これらのサービスにより、Cisco Secure PIX Firewall の外部のインタフェースで終端することが可能になります。

SIP

IETF (Internet Engineering Task Force) で制定された SIP (Session Initiation Protocol) は、コール処理セッション、特に 2 人による音声カンファレンス (コール) を可能にします。SIP は、コール処理前のコールを定義する SDP (Session Description Protocol) と連携して動作します。Cisco Secure PIX Firewall は SIP を使って、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。SIP と SDP は、コールネゴシエーション用の H.245 および H.225 プロトコルを含む H.323 バージョン 2 プロトコルスイートの一部で、次の RFC で定義されています。

SIP: Session Initiation Protocol, RFC 2543

SDP: Session Description Protocol, RFC 2327

H.323 V2

H.323 は、LAN (ローカルエリアネットワーク) 上でのマルチメディアカンファレンスのために ITU (International Telecommunication Union) が定義したプロトコル群です。H.323 バージョン 2 によって、PIX Firewall に次の機能が追加されています。

Fast Connect または Fast Start プロシージャによるさらに迅速なコール設定

H.245 トンネリングによるリソースの節約、コールの同期化、および設定時間の短縮

コールのリダイレクション

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 以降。両方のクライアントとも Windows 95、Windows 98、および Windows NT version 4.0 で使用できます。

必要なシステム構成

ハードウェア	
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 では 8 MB が必要)

発注情報

製品番号	説明
PIX-CONN-VER=	サポート契約をしていないお客様に対する PIX ソフトウェアアップグレード

©2000 Cisco Systems, Inc. All rights reserved.

Cisco と Cisco Systems は商標です。Cisco のロゴは Cisco Systems, Inc. の登録商標です。

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。

本仕様は予告なしに変更される場合があります。



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/go/cnae/>

〒100-0005 東京都千代田区丸の内3-2-3 富士ビルディング

TEL 03-5219-6000 FAX 03-5219-6010

お問い合わせ先