


Cisco Firewall ファミリ： Cisco PIX Firewall と Cisco IOS Firewall フィーチャセット



セキュリティはもはや、単に特定の機能を可能にするためのテクノロジーではなく、ネットワーク デザインの必須要素となっています。ネットワークで重要なトランザクションやコミュニケーションのセキュリティを保護できるということを多くの企業が認識するようになって、この新しいパワフルで便利な手段は標準的なビジネス ツールとなっています。

ネットワークの完全性を保証するためには、インフラストラクチャ自体にセキュリティを組み込む必要があります。世界のネットワークの 80% 以上がシスコシステムズの機器を使って構築されている状況を考えると、シスコこそネットワークに組み込まれたセキュリティ提供者として最適な立場にあると言えるでしょう。

Cisco PIX[®] Firewall シリーズと Cisco IOS[®] Firewall フィーチャセットを含む Cisco Firewall ファミリは、ネットワーク境界で 1 カ所を保護するだけでなく、ネットワークの内在コンポーネントとしてセキュリティ ポリシーを実施します。専用の統合されたポリシー施行が可能な柔軟性により、広範囲な地域に分散したイントラネット、エクストラネット、およびインターネットを使ったコミュニケーションに対してセキュリティ ソリューションを提供します。

Cisco Firewall ファミリ

あらゆるニーズを満たすファイアウォール：
Cisco PIX Firewall と Cisco IOS Firewall

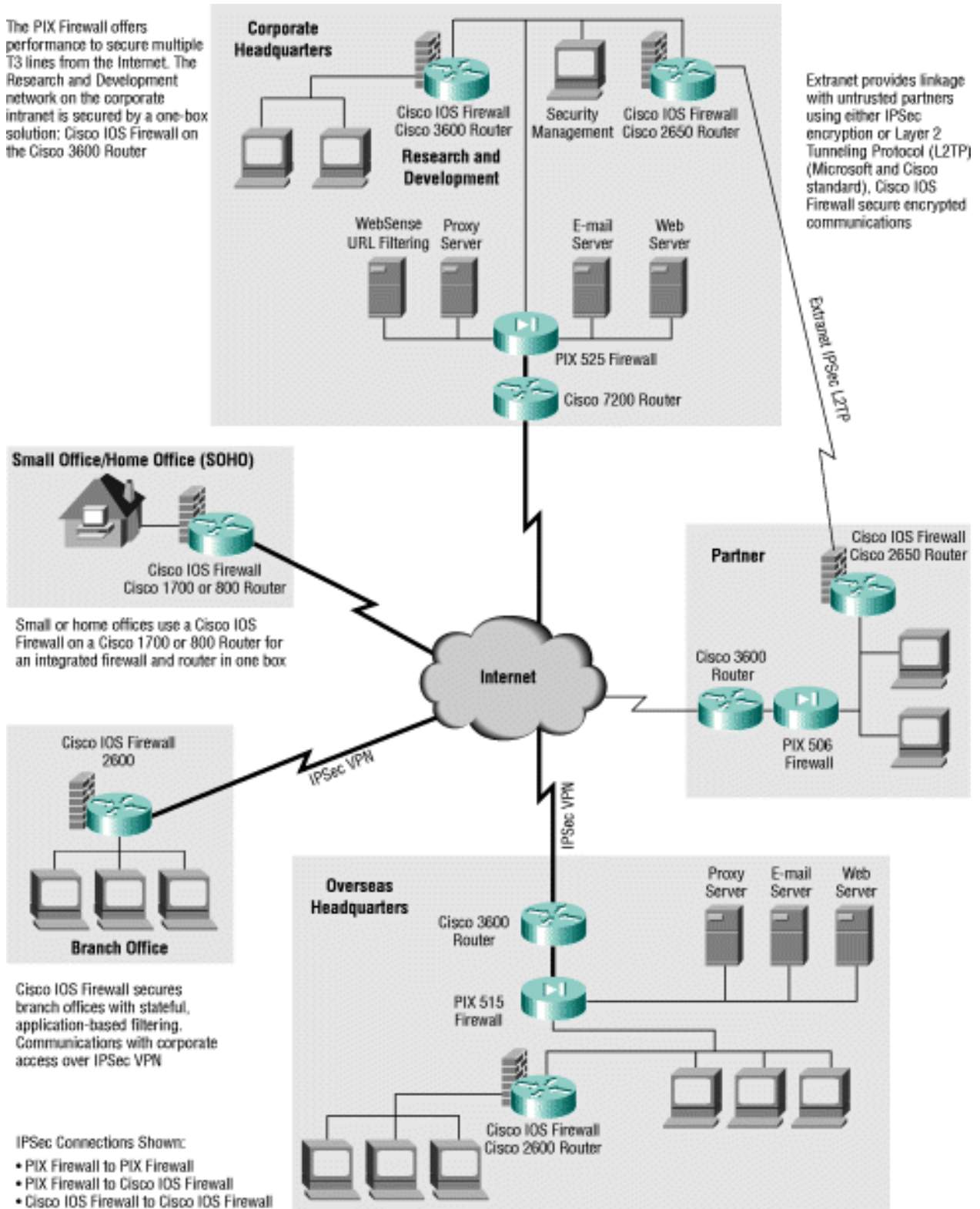
Cisco PIX Firewall は世界最先端のファイアウォール専用アプライアンスです。この製品は、ファイアウォール製品として最高レベルのセキュリティ 認定を取得しています。Cisco PIX Firewall は、優れたパフォーマンスと機能を備えたターンキーアプライアンスになっています。また、NetPartners WebSENSE URL 管理ソフトウェアなどのサードパーティのコンテンツソリューションを統合することで、業界をリードする Cisco PIX Firewall の機能がさらに強化さ

れています。Cisco PIX Firewall は、専用ファイアウォールアプライアンスを使って IP ベースのネットワークセキュリティを実現するための最善のソリューションです。Cisco PIX Firewall は IPsec (IP Security) と連携して、統合型の VPN (仮想プライベートネットワーク) ソリューションを提供します。

Cisco IOS Firewall は、強靭なファイアウォールと侵入探知テクノロジーを Cisco IOS ソフトウェアに統合します。Cisco IOS Firewall は、ステートフルなアプリケーションベースのフィルタリング機能、動的なユーザごとの認証と認可、そしてリアルタイムの警告機能を含めることで、既存の Cisco IOS ソフトウェアを拡張します。Cisco IOS Firewall は Cisco IOS IPsec ソフトウェアと連携して、統合 VPN ソリューションを実現します。広範な Cisco ルータで使用できる Cisco IOS Firewall は、マルチプロトコルルーティングをセキュリティポリシーの施行と統合するための最善のチョイスです。



図 1: Cisco PIX Firewall と Cisco IOS Firewall がエンタープライズ ネットワークのセキュリティを保護





Cisco PIX Firewall と Cisco IOS Firewall の最先端機能

Cisco PIX Firewall シリーズと Cisco IOS Firewall のいずれも、最先端のファイアウォール テクノロジーを組み込んでいます。表 1 は、双方のファイアウォールに共通の先進的な機能を要約しています。

表 1: Cisco PIX Firewall と Cisco IOS Firewall に共通の機能と利点

機能	利点
ステートフル パケットフィルタリング	データパケットを徹底的に検査し、クリティカルなアドレスとポート番号をルックアップテーブルに維持することで、強力なセキュリティ機能を提供
IPsec 仮想プライベート ネットワーク 標準ベース	インターネットを通して企業ネットワークへのセキュアなアクセスを可能にすることで、テレコミュニケーション費用を削減。DES または 3DES により、プライベート通信にデータを暗号化
LAN ベースおよびダイヤルイン通信に対してユーザごとに動的な認証と認可を実行	TACACS+ や RADIUS といった業界標準に対してユーザを認証
ネットワーク アドレス変換	社内ネットワークを外部から隠してセキュリティを強化
コンテンツ フィルタリング	悪意ある Java アプレットをブロック
管理	GUI ベースの管理機能により、ファイアウォールの管理とセキュリティポリシーの実施を中央ロケーションから行うことが可能。ホストにアクセスするトラフィックについて、プロトコルや Web サイト別の統計データおよび不正なアクセス試行の統計データをレポートツールが提供
冗長性/フェイルオーバー	障害が発生した場合は、トラフィックを自動的にバックアップ ユニットにルーティング
パブリック アプリケーション サーバの保護	Cisco PIX Firewall または Cisco IOS Firewall の追加インターフェイスを利用することで、Web、電子メール、FTP、または DNS といったパブリック アクセス可能なサーバのためのネットワークを隔離
Microsoft NetShow、White Pine CU-SeeMe、RealNetworks RealAudio および RealVideo、Xing StreamWorks、VDOnet VDO Live、Vxtreme WebTheater、VocalTec Internet Phone、Microsoft NetMeeting、Intel Internet Video Phone、White Pine Meeting Point といった多数のマルチメディアをサポート	各ユーザのワークステーションで時間をかけて再構成を行わなくても、ユーザは最新のメディアリッチなアプリケーションを使用することが可能
攻撃の探知と阻止	サービス拒否 (DoS) の探知と阻止により、syn フラッディング、ポートスキャン、およびパケット インジェクションからネットワークを防御
侵入探知システム (IDS)	IDS システムが一般的な攻撃シグネチャを識別し、ネットワーク トラフィックの悪用パターンを検出

どちらのファイアウォールも優れたセキュリティ ソリューションを提供しますが、環境やサイト独自の要件によっては、どちらかのファイアウォールのほうが適切な機能を提供する場合があります。表 2 は Cisco PIX Firewall を使用するほうが適切な環境を、表 3 は Cisco IOS Firewall を選択するほうがふさわしい環境を説明しています。多くの場合、最善のセキュリティ ソリューションは両方を併用することで実現します。

表 2: Cisco PIX Firewall の使用が適切な環境

ユーザの要件	Cisco PIX の利点
セキュリティ専用のデバイス	Cisco PIX Firewall は、ファイアウォール保護用に最適化された自身のハードウェアとオペレーティングシステムを装備する専用アプライアンスを提供
大規模な展開が可能	Cisco PIX Firewall シリーズには 506、515、525、および 535 という広範な選択肢が用意されており、大規模な展開に最適
高度なインターネットアクティビティ	Cisco PIX Firewall は、25 万以上の同時接続と 1.0Gbps 近くものスループットという業界をリードするパフォーマンスを提供し、マルチメディア プロトコル、暗号化、多数のユーザへの対応に理想的
認証と認可	Cisco PIX Firewall は、高速なカットスルー プロキシを使って RADIUS および TACACS+ 認証スキームと統合。ワイヤスピードでプロキシが提供されるというアプリケーション レベルの利点を提供
URL フィルタリング	Cisco PIX Firewall は NetPartners WebSENSE ソフトウェアと連携し、WebSENSE の大規模な URL フィルタリングデータベースを使ってインターネット サイトへのアクセスを管理することが可能



表 3: Cisco IOS Firewall の使用が適切な環境

ユーザの要件	Cisco IOS Firewall の利点
強力なセキュリティとマルチプロトコルルーティングを結合したワンボックスソリューション	Cisco IOS Firewall は、ステートフル パケット フィルタリング、侵入探知、ユーザごとの認証と認可、VPN 機能、およびマルチプロトコルルーティングといった包括的な統合セキュリティ ソリューションを 1 台の機器で実現
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を保護	Cisco IOS Firewall は、Cisco PIX Firewall のハイパフォーマンスを必要としないサイトにとって、経済的なソリューションを提供。Cisco IOS Firewall は、エクストラネット / イントラネット境界やブランチオフィス / リモートオフィスのインターネット接続のセキュリティを保護するための効果的で経済的なソリューションを実現
異なるパフォーマンス要件を持つ様々な Cisco IOS 環境で動作するスケーラビリティ	Cisco IOS Firewall は、ローエンドのルーティング プラットフォームからハイエンドモデルまで、必要なパフォーマンス レベルへのスケーラビリティを提供。Cisco IOS Firewall は、Cisco 800、1700、2600、3600、および 7000 シリーズルータにまで拡張可能
トレーニングと保守が簡単	Cisco IOS ソフトウェアの使用経験があれば、Cisco IOS Firewall のセットアップと管理にすでに精通しているため、容易に行うことが可能
先進的な QoS	Cisco IOS Firewall は Cisco IOS ソフトウェアを通してネットワークに統合し、Cisco IOS Firewall を実行する同じルータで先進的な Cisco IOS QoS 機能を使用することが可能

Cisco Firewall 管理ソリューション

Cisco PIX Device Manager (標準装備)

リリース 6.0 では、すべての Cisco PIX Firewall にブラウザ ベースの構成ツールである Cisco PIX Device Manager (PDM) が装備されています。PDM を使用すると、Cisco PIX Firewall CLI (コマンド行インターフェイス) を詳しく知らなくても、Cisco PIX Firewall をグラフィカルにセットアップ、構成、監視することができます。また、多種の情報を提供するリアルタイムの履歴レポート作成機能により、使用傾向、パフォーマンスのベースライン、およびセキュリティ イベントを的確に分析できます。

Cisco IOS Firewall 用の ConfigMaker (標準装備)

ConfigMaker は、使いやすいスタンドアロンの Windows GUI (グラフィカル ユーザインターフェイス) で、ユーザはこれを使用すると、コンソールポートに直接接続して、または Telnet を通してファイアウォール構成規則を実施できます。ConfigMaker は、Cisco Software Center から無料でご利用いただけます。

CiscoSecure Policy Manager (オプション)

CiscoSecure Policy Manager (CSPM) は、Windows NT ベースのソフトウェア ツールです。CSPM バージョン 2.3 は、シスコのセキュリティ ポリシー マネジメントの最新バージョンになります。これを使用すると、ネットワーク全体のセキュリティ ポリシーを中央ロケーションで定義、配信、施行、および監査することができます。CSPM によって、IOS Firewall を実行する Cisco ルータおよび Cisco PIX Firewall の複雑なネットワーク セキュリティ エLEMENTの管理タスクが簡素化されます。さらに、CSPM では Cisco IDS および Cisco IOS IPsec VPN の展開を管理することができ、管理者は中央の 1 つのツールでセキュリティ ポリシーをビジュアルに定義できます。

Cisco VMS (VPN/Security Management Solution) (オプション)

CiscoWorks VPN/Security Management Solution (VMS) は、ブラウザ ベースの包括的なアプリケーションで、VPN とファイアウォール接続を適切にセキュリティ保護して運用するという管理上の課題に対応します。VMS にはフルセットの監視および報告アプリケーションが含まれているほか、10 デバイス用の CSPM の “ 簡易 ” バージョンが装備されています (前述の CSPM を参照してください)。現在 VMS は、すべての Cisco PIX および 7100/7200 ルータのファイアウォール管理をサポートします。Cisco IOS ソフトウェアリリース 12.2(4)T 以降では、VMS は Cisco 1700、2600、および 3600 ルータをサポートできます。

サードパーティ パートナー (オプション)

Solsoft NP

Solsoft NP は、Cisco IOS Firewall と Cisco PIX Firewall をサポートする UNIX ベースの管理ツールです。マルチベンダー、マルチデバイスのスケーラブルな管理ソリューションである Solsoft NP を使用すると、中央ロケーションでセキュリティ ポリシーをビジュアルに定義、展開、施行、および監査することができます。詳細は、下記の URL を参照してください。

<http://www.solsoft.com>

まとめ

ビジネスの必須要素としてネットワークが急速に発展するにともない、ネットワークの周囲に防壁を築くことが必要になるばかりでなく、ネットワーク セキュリティの新しいアプローチも必要となってきます。このような環境では、ネットワークのセキュリティを保護するための最善の場所はネットワーク自身の中になります。Cisco Firewall 製品は、ネットワーク外部で単一の製品によるファイアウォール ソリューションを提供するのではなく、セキュリティポリシーの実施機能をネットワークの内在コンポーネントとして提供して標準ファイアウォール機能を実行します。

©2001 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。その他、記載されている会社名、製品名は各社の商標、登録商標または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