

Cisco IOSソフトウェア Firewall フィーチャセット



ビジネストランザクションの安全性を確保するためにネットワークセキュリティがますます重要になるなかで、企業はネットワークの設計と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性を感じています。そのためには、ネットワークの重要なコンポーネントの1つとして、セキュリティポリシーを実施することが最も効果的です。

Cisco IOS®ソフトウェアは、インターネットバックボーンルータの80パーセント以上に搭載されており、ネットワークインフラストラクチャの最も基本的なコンポーネントとなっています。Cisco IOSソフトウェアベースのセキュリティは、エンドツーエンドのインターネット、イントラネット、およびリモートアクセスネットワークセキュリティに最適なソリューションを提供します。

Cisco Secure製品であるCisco IOS Firewall フィーチャセットは、Cisco IOSソフトウェアのセキュリティに特化したオプションです。Cisco IOS Firewallを使用すれば、すべてのネットワーク境界に対する強力なファイアウォール機能および侵入検出機能が統合され、既存のCisco IOSセキュリティ機能が拡張されます。また、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、動的なユーザーごとの認証および権限付与、ネットワーク攻撃からの防御、Javaブロッキング、リアルタイムのアラートなど、最新のセキュリティ機能を搭載しており、認証、暗号化、フェールオーバーなど、既存のCisco IOSセキュリティソリューションを柔軟に実現します。またCisco IOS IPSecソフトウェアや、L2TP(Layer 2 Tunneling Protocol)およびQoS(Quality of Service)などのCisco IOSソフトウェアのテクノロジーとCisco IOS Firewallを組み合わせることに

よって、完全に統合されたバーチャルプライベートネットワーク(VPN)ソリューションが提供されます。

ルータベースのファイアウォール機能

Cisco IOSソフトウェアを搭載したルータは、多様な用途に利用されています。Cisco IOS Firewallでは、リモートおよびブランチオフィスに対するインターネット接続の安全性を確保するだけでなく、イントラネットやエクストラネットの接続についても高度なセキュリティとポリシーを実行します。

Cisco IOS Firewallは、セキュリティポリシーの実施によってマルチプロトコルルーティングを統合し、管理者がCiscoルータをファイアウォールとして設定するための最適な選択肢となります。Cisco IOS Firewallを使用すると、顧客は帯域幅、LAN/WAN密度、およびマルチサービス要件といった条件に基づいてルータのプラットフォームを選択でき、そのなかで高度なセキュリティを得ることができます。さまざまなセキュリティ環境に対して適切なCiscoルータを選択するには、次の一般的なガイドラインを参考にしてください。

- 小規模/ホームオフィス: Cisco 800、uBR900シリーズ、1600、および1720ルータシリーズ
- ブランチおよびエクストラネット環境: Cisco 2500、2600、および3600ルータシリーズ
- VPN および WAN 集約ポイントなどの高スループット環境: Cisco 7100、7200、7500、およびRSM(Route Switch Module)ルータシリーズ

主な利点

Cisco IOS Firewallは、Cisco IOSソフトウェアとのシームレスな相互運用性を備え、次のような有用性や利点を提供します。



- 柔軟性 --- Cisco ルータにインストールするため、オールインワンのスケーラブルな Cisco IOS Firewall ソリューションが実現され、マルチプロトコルルーティング、境界セキュリティ、侵入検出、VPN 機能、およびユーザーごとの認証および権限付与が実行できます。
- 投資保護 --- ファイアウォール機能をマルチプロトコル ルータに統合することで、新しいプラットフォームについてのトレーニングコストを削減でき、既存のルータ投資が活用されます。
- VPN サポート --- Cisco IOS の暗号化および QoS VPN 機能を組み合わせて Cisco IOS Firewall を展開することで、公衆ネットワークに対して極めて安全で低価格の伝送が実現され、ミッションクリティカルなアプリケーショントラフィックの優先度の高い配信が可能になります。
- スケーラブルな展開 --- 多様なルータプラットフォームに使用できるため、ネットワークの帯域幅およびパフォーマンス要件に合わせて Cisco IOS Firewall を拡張できます。
- 簡単な管理 --- Cisco ConfigMaker ソフトウェアを使用することで、ネットワーク管理者は、ネットワークの中央コンソールから Cisco IOS のセキュリティ機能 (Cisco IOS Firewall、NAT [Network Address Translation]、Cisco IPSec など) を設定することができます。

Cisco IOS Firewall は、Cisco 800、uBR900、1400、1600、1700、2500、2600、3600、7100、7200、および 7500 ルータシリーズに搭載することができます。Catalyst® 5000 スイッチでも利用可能で、統合マルチサービス (データ/音声/ビデオ/ダイヤル) や、ダイヤルアップ接続に対する高度なセキュリティ機能も提供します。また、7x00、7500、および RSM シリーズについては、大企業およびサービスプロバイダーの顧客宅内機器 (CPE) 向けに、インターネットゲートウェイにおける統合型ルーティングおよびセキュリティなどの機能もあります。

最新リリースの新機能 (Cisco IOS Firewall ソフトウェア 12.1(4)T)

HTTP についての認証プロキシアカウント

アカウントリングは、ユーザーの行動を追跡するための方法です。通常、アカウントリング情報は、ユーザーアクションとアクション期間から構成されています。アカウントリング情報は、アカウントリングサーバに送信され、そこにレコード形式で保存されます。システム管理者は、セキュリティ、課金、あるいはリソース管理計画などにアカウントリング情報を使用します。アカウントリングサーバは、課金とセキュリティ監査に必要なだけの情報を持った、スタートレコードとストップレコードを提供します。認証プロキシに AAA (Authentication, Authorization, and Accounting) を追加することによって、認証プロキシサービスでのユーザーの行動を監視できるようになります。

ファイアウォールの実装

認証プロキシキャッシュと、それに関連するダイナミック ACL (アクセス制御リスト) が作成されると、認証プロキシは、認証されたホストについてのアカウント情報の追跡を開始します。このイベントについてのデータは、AAA によって保存されます。このとき、アカウントリングの「スタート」オプションが有効になっていれば、「スタートレコード」と呼ばれるアカウントリングレコードが作成されます。またファイアウォールには、このデータを表示するためのコマンドがあります。認証プロキシキャッシュが期限超過になったり削除されたりすると、アカウントリング情報にデータ (期限切れといった情報) が追加され、「ストップレコード」がサーバに送信されます。この時点で、情報は AAA から削除されます。

Cisco IOS Firewall の主な機能

Cisco IOS Firewall では、Cisco ルータの柔軟性およびセキュリティを向上して、ネットワークに対する統合ファイアウォール機能を提供します。Cisco IOS Firewall の主な機能を表 1 に示します。



表1: Cisco IOS Firewallの概要

機能	説明
コンテキストベースアクセス制御(CBAC)	<ul style="list-style-type: none"> 企業の専用ネットワークとインターネット間などの境界部におけるトラフィックに対して、安全なアプリケーションごとにアクセス制御を設定できます。
不正侵入検出	<ul style="list-style-type: none"> 最もよくある攻撃や情報収集のための不正侵入検出用のシグニチャを広範囲に網羅したファイルを用意し、リアルタイムのモニタリング、インターセプト、およびネットワークの誤使用に対する応答を提供します。
認証プロキシ	<ul style="list-style-type: none"> LAN ベースおよびダイヤルイン通信に対して、ユーザーごとの動的な認証および権限付与、業界標準のTACACS+およびRADIUS認証プロトコルによるユーザー認証を提供します。ネットワーク管理者がユーザーごとに個別のセキュリティポリシーを設定できます。
サービス拒否の検出と防止	<ul style="list-style-type: none"> 一般的な攻撃からルータリソースを保護します。パケットヘッダを検査し、不審なパケットを廃棄します。
動的ポートマッピング	<ul style="list-style-type: none"> ネットワーク管理者は、非標準ポートで CBAC をサポートしたアプリケーションを実行できます。
Javaアプレットブロッキング	<ul style="list-style-type: none"> 発生源が不明な悪意のあるJavaアプレットを防止します。
VPN、IPSec暗号化、およびQoSサポート	<ul style="list-style-type: none"> Cisco IOSソフトウェア暗号化、トンネリング、および安全なVPN用のQoS機能が提供されます。 強力な境界セキュリティ、高度な帯域幅管理、不正侵入検出、およびサービスレベル検証を統合する際に、スケーラブルな暗号化トンネルをルータに提供します。 相互運用性に対する標準準拠
リアルタイムアラート	<ul style="list-style-type: none"> サービス拒否への攻撃やその他の事前定義された条件に対してアラートを出します。アプリケーションごと、機能ごとに設定可能です。
監査追跡	<ul style="list-style-type: none"> トランザクションの詳細(タイムスタンプ、送信元ホスト、宛先ホスト、ポート、所要時間、および合計転送バイト数など)を詳細レポートに記録します。アプリケーションごと、機能ごとに設定可能です。
イベントロギング	<ul style="list-style-type: none"> コンソール端末や syslog サーバへのシステムエラーメッセージ出力のロギングや、重大度レベルの設定、他のパラメータの記録などによって、管理者が潜在的なセキュリティ違反や標準に合っていない他のアクティビティをリアルタイムに追跡することができます。
ファイアウォール管理	<ul style="list-style-type: none"> Cisco 1600、1720、2500、2600、および3600ルータでは、ウィザードベースのネットワーク構成ツールを使って、ネットワーク設計、アドレッシング、およびCisco IOS Firewallセキュリティポリシーを構成できます。また、NATおよびIPSec構成もサポートされています。
Cisco IOSソフトウェアとの統合	<ul style="list-style-type: none"> Cisco IOS機能との相互運用性を備え、ネットワークにおけるセキュリティポリシー実施を統合します。
基本および高度なトラフィックフィルタリング	<ul style="list-style-type: none"> 標準および拡張アクセス制御リスト(ACL) --- 特定のネットワークセグメントにアクセス制御を適用し、どのトラフィックがネットワークセグメントを通過するかを定義します。 ロック&キーダイナミック ACL では、ファイアウォールによってユーザーID(ユーザー名/パスワード)に対する一時アクセス権が付与されます。
ポリシーベースのマルチインタフェースサポート	<ul style="list-style-type: none"> セキュリティポリシーに基づいて決定された IP アドレスおよびインタフェースによって、ユーザーアクセスを制御する機能を提供します。
冗長性/フェールオーバー	<ul style="list-style-type: none"> 障害が発生した場合に、自動的にバックアップルータにトラフィックの経路を指定します。
ネットワークアドレス変換	<ul style="list-style-type: none"> 拡張されたセキュリティ機能によって、外部から内部ネットワークが見えないようにします。
時間指定によるアクセスリスト	<ul style="list-style-type: none"> 時間帯および曜日ごとによるセキュリティポリシーを定義します。
ピアルータ認証	<ul style="list-style-type: none"> ルータが承認された送信元からの信頼できるルーティング情報を確実に受信できるようにします。
メールサーバに対する攻撃の検出と防御を改良	<ul style="list-style-type: none"> 新しい侵入検出では、SMTPを利用した攻撃を考慮した設計になっています。



コンテキストベースアクセス管理 (CBAC)

Cisco IOS Firewall CBACエンジンでは、ネットワーク境界に対して安全なアプリケーションごとのアクセス制御を提供します。CBACでは、送信元および宛先アドレスを調べることで、ファイル転送プロトコル (FTP) および電子メールトラフィックなど、既知のポートを使用するTCPおよびUDPアプリケーションに対するセキュリティが拡張されます。CBACを使用すると、ネットワーク管理者は統合された1つのソリューションの一部として、ファイアウォールインテリジェンスを実装することができます。

たとえば、インターネットアプリケーション、マルチメディアアプリケーション、またはOracleデータベースを実行するエクストラネットパートナーとのセッションを構築するために、ネットワークを解放して弱点を作り出す必要はありません。CBACでは、現在の基本的なアプリケーショントラフィックを安全に実行するだけでなく、マルチメディアやビデオ会議といった高度なアプリケーションをルータを経由しても安全に実行することができます。

ネットワークセキュリティに対する CBAC の影響

CBACは、標準TCPおよびUDPインターネットアプリケーション、マルチメディアアプリケーション (H.323および他のビデオアプリケーションを含む)、およびOracleデータベースを含む、IPトラフィックに対するアプリケーションごとの制御機能です。CBACではTCPおよびUDPパケットが調査され、その“状態”または接続ステータスが追跡されます。

TCPは、コネクション指向のプロトコルです。データを転送する前に「3ウェイハンドシェイク」と呼ばれる手順によって宛先との接続がネゴシエートされます。このハンドシェイクプロセスによって有効なTCP接続およびエラーのない伝送が可能になります。接続を設定する際に、TCPはパケットヘッダで簡単に識別できる複数の状態 フェーズ を通過します。標準および拡張ACLではパケットヘッダから状態を読み込み、リンクでトラフィックが許可されるかを判断します。

アプリケーションステータス情報のパケット全体を読み込むことで、CBACではACL機能に検出インテリジェンスを追加します。この情報を使用して、応答トラフィックを信頼できるネットワークに許可する、一時的なセッション固有のACLエントリがCBACで作成されます。この一時的なACLでは、ファイアウォールのドアが効率的に開かれます。セッションがタイムアウトまたは終了するとACLエントリは削除され、追加トラフィックに対してドアが閉じられます。標準および拡張ACLでは一時ACLエントリは作成されないため、管理者はこれまで情報アクセス要件に対してセキュリティリスクを強制的に付加する必要がありました。リターントラフィックに対して複数のチャネルから選択する拡張アプリケーションでは、標準または拡張ACLを使用して簡単に安全性を確保することはできませんでした。

CBACは、ファイアウォールによってセッションを許可するかを決定する際にアプリケーションタイプを説明し、リターントラフィックの複数チャネルから選択されるかを決定するため、現在のACLのみのソリューションよりも安全です。CBACより以前は、ファイアウォールのドアを開けたままにする永続的なACLを記述する方法によってのみ、管理者は拡張アプリケーショントラフィックを許可できたため、ほとんどの管理者はこのようなアプリケーショントラフィックをすべて拒否していました。CBACを使用すると、必要に応じてファイアウォールを開き、それ以外のときは閉じることで、マルチメディアおよび他のアプリケーショントラフィックを安全に許可することができます。たとえば、CBACがMicrosoft NetMeetingを許可するように構成されている場合は、内部ユーザーが接続を開始すると、ファイアウォールでリターントラフィックが許可されます。ただし、外部のNetMeeting送信元で内部ユーザーとの接続が開始された場合、CBACではエントリが拒否され、パケットが廃棄されます。

不正侵入検出

侵入検出システム (IDS) は、内部や外部の攻撃からネットワークを保護することで、ファイアウォールを上回るレベルの保護を提供します。セキュリティポリシーに違反したり悪意のあるネットワークアクティビティを表すパケットおよびフローを適切に処理することで、Cisco IOS Firewall IDSテクノロジーは境界ファイアウォール保護を強化します。

Cisco IOS Firewall侵入検出機能は、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をより見やすくするのに最も適しています。ネットワーク管理者は、ネットワークに対する強固な保護を活用することで、内部または外部ホストからの攻撃に自動的に対応することができます。

検出と応答

Cisco IOS Firewall IDSでは、ネットワークトラフィックの誤使用のパターンを検出するシグニチャを使用して、最も一般的な59種類の攻撃を識別します。Cisco IOS Firewallの新しいリリースに含まれる侵入検出シグニチャは、侵入検出シグニチャのさまざまな面から選択されました。IDSシグニチャは、セキュリティの重大な違反、最も一般的なネットワーク攻撃、および情報収集スキャンを表します。

Cisco IOS Firewallはインライン侵入検出センサーとして機能し、パケットおよびセッションがルータを介して流れるのを監視し、シグニチャに一致するものをスキャンします。不審なアクティビティが検出されると、ネットワークセキュリティが損なわれる前に対応し、Cisco IOS syslogによってイベントが記録されます。ネットワーク管理者は、さまざまな脅威に対して適切な対応が選択されるように、IDSシステムを構成することができます。セッション内のパケットがシグニチャと一致した場合、IDSシステムを次のように構成することができます。



- syslogサーバまたはCisco Secure Intrusion Detection System (旧名称: NetRanger) Director (集中管理 インタフェース) にアラームを送信する
- パケットを廃棄する
- TCP接続をリセットする

シスコでは、不正な反応があった場合に個別のシグニチャを無効にできるように、柔軟性を念頭においてCisco IOS FirewallのIOS®ソフトウェアベースの侵入検出機能を開発しました。また、ネットワークセキュリティポリシーをサポートするCBACセキュリティエンジンのファイアウォールおよび侵入検出機能の両方を有効にした方がいい場合、これらの機能はそれぞれ異なるルーティングフェースで個別に有効になります。Cisco IOSソフトウェアベースの侵入検出は、Cisco IOS Firewallに含まれる機能で、Cisco uBR900、1720、2600、3600、7100、7200、7500、およびCatalyst 5000用RSMルータシリーズで使用できます。Cisco IOS Firewallを含むすべてのプラットフォームでは、最も一般的な5つのSMTP攻撃が検出されます。

Cisco IOS Firewall と Cisco Secure IDS

すでにCisco Secure IDS (Intrusion Detection System) を使用している場合には、既存のIDSシステムを補完する、Cisco IOSソフトウェアベースのIDSシグニチャを導入することができます。これにより、NetRangerセンサーをサポートできない領域にIDSを展開することができます。Cisco IOS IDSシグニチャは、他のCisco IOS Firewall機能とともに、または別個に展開することができます。

侵入検出を備えたCisco IOS Firewallは、Cisco Secure IDS Directorの画面にアイコンとして表示され、ネットワーク全体にわたってすべての侵入検出センサーが統一して表示されます。Cisco IOS Firewall侵入検出機能には、Cisco IOS syslogに加えて、Cisco Secure IDS Directorコンソールへのロギングを許可する拡張レポート機能があります。

認証プロキシ

ネットワーク管理者は、Cisco IOS Firewallが装備しているLANベースの動的なユーザーごとの認証および権限付与を使用して、ユーザーごとに固有のセキュリティポリシーを作成することができます。以前は、ユーザーの固定IPアドレスによってユーザーIDおよび関連する認可アクセスが判断されていたが、または個別のセキュリティポリシーをユーザーグループまたはサブネット全体に適用する必要がありました。現在は、Cisco IOSソフトウェア認証、権限付与、および課金管理 (AAA) サービスを使用して、TACACS+またはRADIUS認証サーバからルータにユーザーごとのポリシーを動的にダウンロードすることができます。

ユーザーが、ネットワークにログインするかまたはHTTPによってインターネットにログオンすることで、特定のアクセスプロファイルが自動的にダウンロードされます。必要に応じて、適切な動的個別アクセス特権が使用可能になり、複数のユーザーに適用される一般的なポリシーに対してネットワークが保護されます。認証および権限付与は、エ

クストラネット、イントラネット、およびインターネットで安全な受信または送信に使用されるルーティングフェースに適用されます。

サービス拒否の検出と防止

拡張されたサービス拒否の検出と保護では、TCP接続のパケットシーケンス番号を調べることで、SYN (synchronize/start) あふれ、ポートスキャン、およびパケット導入などの一般的な攻撃モードに対してネットワークが防御されます。番号が予期しない範囲にある場合は、ルータによって不審なパケットが廃棄されます。ルータで通常とは異なる高速の新しい接続が検出されると、アラートメッセージが発行され、システムリソースが消耗しないように、半分開いたTCP接続状態テーブルが廃棄されます。

Cisco IOS Firewallが攻撃の可能性を検出すると、送信元または宛先アドレスおよびポートの組に基づいてユーザーアクセスを追跡します。また、トランザクションの詳細を調べて、監査追跡を作成します。

動的ポートマッピング

柔軟なアプリケーションごとのポートマッピングを使用すると、CBACをサポートするアプリケーションを非標準ポートで実行することができます。この機能によって、ネットワーク管理者は、ネットワークの個別のニーズに合わせて、特定のアプリケーションおよびサービスに対するアクセス制御をカスタマイズできます。

Java アプレットブロッキング

インターネットで使用できるJavaアプレットの普及によって、ネットワーク管理者にとって悪意のあるアプレットからネットワークを保護することが主な関心事になりました。Javaブロッキング機能は、アーカイブに埋め込まれていない、またはファイルに圧縮されていないJavaアプレットへのアクセスをフィルタしたり、完全に拒否したりするように構成できます。

VPN、IPSec 暗号化、および QoS サポート

Cisco IPSec テクノロジーと組み合わせることで、Cisco IOS Firewallによる統合VPN機能が提供されます。VPNは、公衆回線 (インターネットなど) に安全なデータ転送を提供し、リモートユーザー、ブランチオフィス、およびエクストラネットの電気通信および管理コストを削減し、QoSおよび信頼性を拡張できるよう急速に開発されています。

Cisco IOS Firewallは、Cisco IOSソフトウェア暗号化、トンネリング、および安全なVPNに対するQoS機能とともに動作します。ネットワークレイヤの暗号化機能によって、転送の際にネットワークにおけるデータの盗聴や改ざんが回避されます。Cisco IOS Firewallでは、56ビット (DES) および 168 ビット (3DES) の両方の標準IPSec (Internet Protocol Security) をサポートしており、信用できないネットワークを経由したプライベートなデータ通信を可能にします。



最大限の相互運用性のために、Cisco IOS ソフトウェアでは、汎用ルーティングカプセル化 (GRE)、レイヤ2 転送 (L2F)、およびレイヤ2 伝送プロトコル (L2TP) とともに機能する、複数のトンネリングプロトコル標準がサポートされます。QoS機能によってトラフィックの分類、輻輳の管理、および必要に応じてアプリケーションの優先付けが行われます。

シスコのVPN対応のプラットフォーム (Cisco uBR900、1720、2600、3600、および7100 ルータシリーズ) に Cisco IOS Firewall を搭載すると、既存のネットワークをVPN (仮想プライベートネットワーク) に拡張できます。シスコでは、VPNソリューションは公衆ネットワーク設備に対して安全な暗号化トンネルを上回る機能を提供する必要があると考えています。また、データをタイムリーかつ確実に配信し、企業から公衆ネットワークに入る際に強固な境界セキュリティを提供する必要もあります。Cisco IOS Firewall は、7100ルータシリーズなどと組み合わせることで、たとえば強力な境界セキュリティ、高度な帯域幅管理、不正侵入検出、およびサービスレベル検証を統合する際に、スケーラブルな暗号化トンネルを提供します。

Cisco IOS Firewall 認証プロキシ機能では、ユーザー認証およびCisco VPNクライアントソフトウェアに対する認証も提供されます。

構成可能なリアルタイムアラート、監査追跡、およびイベントロギング

リアルタイムアラートでは、不審なアクティビティが検出されたときに中央管理コンソールにsyslogエラーメッセージが送信され、ネットワーク管理者が侵入にただちに対応できるようにします。拡張監査追跡機能を利用すれば、syslogを使用してすべてのトランザクション、タイムスタンプ、送信元ホスト、宛先ホスト、使用されたポート、セッション所要時間、および拡張セッションベースレポートの合計転送バイト数が追跡されます。

Cisco IOS Firewall アラートおよび監査追跡機能は、より柔軟なレポートおよびエラー追跡を可能にするよう構成することができます。構成可能な監査追跡機能では、特定のCBACをサポートするアプリケーションおよびJavaブロックのモジュラ追跡をサポートしています。また、さまざまなサードパーティレポートツールによって、リアルタイムアラートおよび監査追跡機能の両方がサポートされています。

ネットワークイベントが発生すると、Cisco IOS ソフトウェアsyslog機能によってロギングホストにアラートが送られます。これにより、コンソール端末やsyslogサーバへのシステムエラーメッセージ出力のロギングや、重大度レベルの設定、他のパラメータの記録などによって、管理者が潜在的なセキュリティ違反や標準に合っていない他のアクティビティをリアルタイムに追跡することができます。

ファイアウォール管理

セキュリティポリシーの実装にCisco IOS Firewallを使用すれば、中央からGUIベースで高速かつ効率的に管理できます。Cisco ConfigMaker 2.1およびそれ以降のバージョンには、セキュリティウィザードが用意されており、Cisco IOS Firewallのセキュリティポリシーを素早く構成できるようになっています。ここでは、NATおよびIPSec構成もサポートされています。

ConfigMakerは、Microsoft Windows 95、Windows 98、およびWindows NT 4.0のウィザードベースの使いやすいソフトウェアツールで、Ciscoルータ、スイッチ、ハブ、などのネットワークデバイスから構成される小規模ネットワークを1つのPCから設定するために使用するものです。Cisco 800、1600、1720、2500、2600、および3600ルータシリーズに使用することができます。

Cisco IOS ソフトウェアとの統合

Cisco IOS Firewallは、Cisco IOSソフトウェアによってネットワークに統合されるセキュリティソリューションです。強固なセキュリティポリシーでは、境界制御やファイアウォール設定および管理を超える機能が必要とされます。セキュリティポリシーの実施は、ネットワーク自体の本質的なコンポーネントである必要があります。Cisco IOSソフトウェアは、グローバルセキュリティポリシーを実装するのに最も適した手段です。シスコのエンドツーエンドソリューションを導入することで、管理者はネットワークの拡張に合わせてセキュリティポリシーを強化することができます。

また、Cisco IOS Firewallは、NAT、VPNトンネリングプロトコル、CEF (Cisco Express Forwarding)、AAA 拡張、暗号化テクノロジ、およびCisco IOS IPSecを含む、Cisco IOSソフトウェア機能と完全に相互運用性があります。

Cisco IOS Firewall の対象

- 強力なセキュリティ、侵入検出、ユーザーごとの認証と権限付与、VPN機能、およびマルチプロトコルルーティングを組み合わせた、1つにまとまったソリューションを必要とする顧客
- すべてのネットワーク境界、特にブランチオフィス、イントラネット、およびエクストラネットにわたって境界セキュリティを拡張する、コスト効率のよい方法に関心がある顧客
- 統合されたファイアウォールおよび侵入検出機能を備えた、コスト効率のよいルータを探している中小規模の企業
- 管理型サービスのためのルータ / ファイアウォールパッケージとして展開を考えるサービスプロバイダー
- ネットワークセグメント間 (組織と信用度の低いパートナーサイト間など) にさらにセキュリティを必要とする顧客
- さらにセキュリティが要求されるイントラネット接続を使用する組織

- 企業のオフィスまたはインターネットに接続するブランチオフィスサイト
- 個別のファイアウォールプラットフォームを必要としない、Cisco IOSに精通した顧客
- 奥行きのある防御環境を構築するために、ネットワークインフラストラクチャ全体にファイアウォール保護を実装しようと考えている顧客

サポートについて

シスコシステムズでは、業界をリードするネットワークソリューションだけでなく、ローカルおよび広域ネットワークを管理するシステム管理者をサポートする、世界トップクラスのエンドツーエンドサポートソリューションも提供しています。シスコのサポート製品は、投資を保護して効果を最大化するための高度なカスタムサービスの他にも、導入、メンテナンス、およびマーケティングに対するサポートを提供します。Cisco IOS Firewallの最新版は、シスコのWebサイト「Cisco Connection Online (CCO)」からいつでも入手することができます。

発注情報

Cisco IOS Firewallは、Cisco 800、uBR900シリーズ、1600、1720、2500、2600、3600、7100、7200、7500、およびRSMJレータシリーズのソフトウェアイメージオプションとして購入できます。Cisco Webサイトからソフトウェアイメージをダウンロードするか、またはCD-ROMでご請求ください。製品価格について詳細は、シスコ製品の販売店にお問い合わせください。

©2001 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/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