

シスコのサービス統合型ルータ：中堅・中小企業および大企業のブランチ オフィスにおける統合セキュリティの重要性

この 20 年の間に、ネットワークは閉じたインフラストラクチャから、ビジネス プロセスとアプリケーションを接続し自動化することによって、社員、パートナー、顧客、ベンダーとのより密接な連携を世界規模で可能にする統合システムへと進化しました。アプリケーションの Web 対応によって、生産性や収益性は大幅に向上しましたが、悪質な攻撃を受けるリスクも増大しています。

セキュリティ違反は、社内のネットワークに接続された PC やサーバなどのさまざまな場所で発生する可能性があります。また、ネットワークのエンドポイントは常に新種のワームやウイルスの危険にさらされています。こういった状況は、これらの危険に対処できるだけの IT リソースが十分そろっていない小規模オフィスやブランチ オフィスでは大きな問題になります。

シスコシステムズは、脅威の識別、防御、対処機能を大幅に向上させた自己防衛型ネットワークを構築することで、企業のセキュリティ攻撃問題に対応しています。進化するシスコの自己防衛型ネットワークの重要な基盤となるのが、次世代型のシスコ サービス統合型ルータです。このルータは、中堅・中小企業や大企業のブランチ オフィス向けに、セキュアなワイヤスピードのデータ、音声、映像、その他の高度なサービスを提供する業界初の製品です。

この資料では、変化を続けるセキュリティ環境と、Cisco 800 シリーズ ルータおよび Cisco ISR 1800/2800/3800 シリーズに組み込まれているセキュリティ機能を中心に説明します。また市場の動向が、小規模企業やブランチ オフィスにおけるサービス統合製品に対して需要の高まりを示す中で、ルータにセキュリティ機能を統合する重要性についても説明します。さらに、今日のセキュリティ上の課題だけでなく、将来の課題にも効果的に対処できるシスコ独自のシステム アプローチについても説明します。

この資料は、技術的な導入ガイドとして作成されたものではありません。シスコが 20 年来培ってきたルーティング技術にクラス最高レベルのネットワーク セキュリティ技術を融合させ、それによってネットワーク セキュリティを定義し直し、お客様にエンドツーエンドのネットワーク保護を提供しようとする取り組みについて説明することを目的としています。

今までにないネットワーク セキュリティ上の脅威

従来、社内外で発生する脅威は比較的動きが遅く、攻撃の緩和は今よりも容易でした。1980 年代に現れた最初のセキュリティ上の脅威（個人のコンピュータやネットワークに感染するブート ウイルス）は、感染が広がるのに数週間掛かりました。1990 年代に登場した第 2 世代型のセキュリティの脅威（マクロ ウイルス、E メール ウイルス、DoS 攻撃 [サービス拒絶攻撃]、一部のハッキング行為）は、数日で拡大しました。

今日の環境におけるネットワークのセキュリティ違反や破壊的な攻撃は、拡大の高速化と手口の巧妙化が驚くほどの勢いで進んでいます。インターネット ワーム、ウイルス、トロイの木馬をさまざまに組み合わせて構成された脅威は、世界中のあらゆる地域ネットワークに数分で拡大し、広範にわたる感染や被害をもたらします。

ネットワーク セキュリティ違反および攻撃がもたらす多額の損失

セキュリティ違反 1 件当たりの平均損失額

- 機密情報の漏洩/データ盗難： 1,136,409 米ドル (約 1 億 2500 万円)
- ダウンタイムによる損失およびウイルスによる被害： 61,729 米ドル (約 680 万円)
- データ ネットワークの破壊： 535,750 米ドル (約 5900 万円)
- 外部からのシステム侵入： 172,448 米ドル (約 1900 万円)
- DoS 攻撃： 108,107 米ドル (約 1200 万円)
- 内部者による不正アクセス： 1,008,050 米ドル (約 1 億 1100 万円)

出典：『CSI FBI Computer Crime & Security Survey 2004』

法規制によるセキュリティ対策義務の高まり

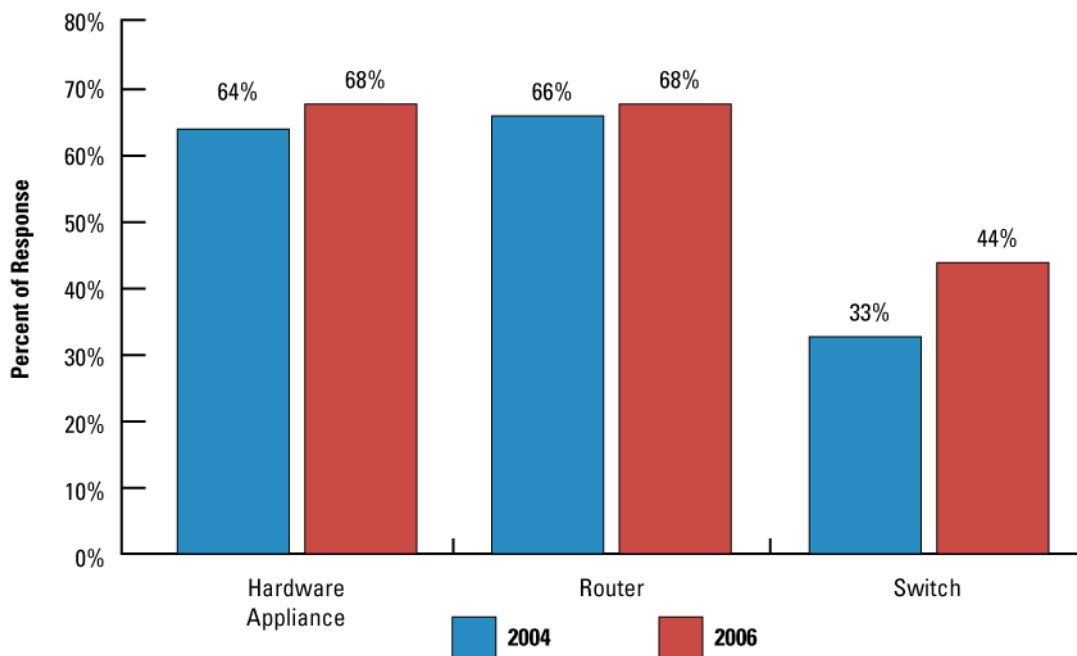
政府による規制や基準の増加も企業のネットワーク セキュリティ強化を促しています。これらの法規制は、プライバシー、国家安全保障、そして多くの場合は株式公開企業のアカウントビリティを強化するために制定されました。

これらの法規制には、ヘルスケア産業の Health Information and Patient Privacy Act (HIPPA)、金融サービス業界の Gramm Leach Bliley Act (GLBA; 米国金融制度改革法)、財務会計分野の Sarbanes-Oxley Act (SOX; 米国企業改革法) などがあります。欧州連合 (EU) のプライバシー規制 (Directive on Data Protection [データ保護条令]) では、EU 以外の国に個人情報を移送する場合、その国のプライバシー保護レベルが基準に達していることが必要となります。また、日本でも個人情報保護法、日本版 SOX 法や内部統制などの基準が設けられています。

セキュア ルータに対する需要の高まり

セキュリティやプライバシー保護に対する懸念が高まる中で、革新的なセキュリティ ソリューションを求める声が強くなっています。「Enemy at the Gates: The Evolution of Network Security」(Business Communication Review 誌、2004 年 12 月) という記事の中で、Infonetics Research 社の首席アナリストである Jeff Wilson 氏は次のように語っています。「セキュリティ アプライアンス市場には、多くの人々から大きな関心が寄せられていますが、ルータやスイッチによってセキュリティ機能が展開される範囲は見落とされがちです。インターネット接続が普及し、あらゆる規模の企業でネットワーク セキュリティの必要性が生じたことから、複数のセキュリティ テクノロジーを 1 つに統合した製品が登場しました。同じ理由から、ネットワーク製品メーカーはルータやスイッチにセキュリティ機能を統合した製品を市場に投入しています。」記事の中で引用されている Infonetics 社の調査によると、「セキュリティ アプライアンスとセキュア ルータの導入を予定している回答企業の割合はほぼ同数」です。

図 1 セキュリティ製品の導入予定



Infonetics Research 社のデータは、セキュア ルータの市場が急速に拡大しているという事実を裏付けています。Infonetics Research 社で企業の音声/データを担当するディレクティング アナリストの Matthias Machowinski 氏は、2004 年末のレポートでこのように述べています。「第 4 四半期のエンタープライズ向けルータによる収益の 12 パーセントはセキュア ルータの売り上げによるもので、第 3 四半期よりも 1 パーセント上昇しています。ルータの収益におけるセキュア ルータの割合は今後も増え続け、2008 年までにルータの総収益の 29 パーセントを占めるようになると私たちは見えています。」

進化するシスコのセキュリティ ソリューション

セキュリティ ソリューションは、常に変化するセキュリティ要件に対応して進化を続けています。シスコは、クラス最高レベルのセキュリティ ソリューションの提供を通じて、業界の主導的役割を担い続けています。

Synergy Research 社は、2005 年 3 月 14 日付けの Investors.com の「Hybrid Products Lead Security's Advance」と題する論説の中で、「昨年 (2004 年)、ネットワーク セキュリティ製品市場は 28% の成長を遂げて 40 億ドルを超える規模になりました。」と報告しています。Synergy 社のアナリストである Aaron Vance 氏は次のように語っています。「今年はやや急速な成長が見込まれ、ファイアウォールや VPN などのセキュリティ機能を組み合わせたハイブリッド製品が最大の牽引力になると思われます。この種のハイブリッド型セキュリティ製品の売り上げでは、ネットワーク機器のトップ メーカーであるシスコシステムズが首位に立っています。」

現在、シスコは出荷されるすべてのサービス統合型ルータのハードウェアにネットワーク セキュリティを組み込み、適切な Cisco IOS[®] ソフトウェア フィーチャ セットを使用してエンドツーエンドの保護を提供しています。シスコのサービス統合型ルータは、Cisco 7200 シリーズや 7301 アグリゲーション ルータと相互運用できるように設計されています。これらのルータはいずれも、Cisco IOS ソフトウェアの包括的な Advanced Security フィーチャ セットを使用します。

ルータにおける統合セキュリティ ソリューションの重要性

統合セキュリティは、シスコの自己防衛型ネットワークの基盤となる要素です。ルータの統合セキュリティ ソリューションには、シスコの優れたファイアウォール テクノロジーや Intrusion Prevention System (IPS; 侵入防御システム) テクノロジーが利用されており、Cisco IOS ソフトウェアの安定した機能や LAN/WAN 接続機能に、業界最高クラスのセキュリティ機能を融合しています。

Cisco IOS ソフトウェアのセキュリティをルータに直接統合すると、さまざまな利点が得られます。第 1 に、既存のネットワーク インフラストラクチャを有効に活用し、ハードウェアを追加しなくても Cisco IOS ソフトウェアを使ってルータに新しいセキュリティ機能を実現できます。これにより、ネットワークで使用するデバイスが少なくなるため、時間とコストが節約され、トレーニング コストおよび管理コストの抑制とともに全体的な総所有コスト (TCO) も削減されます。またルータのネットワーク モジュールは、既存のルータの Cisco SMARTnet[®] メンテナンス契約でもカバーされているため、管理がさらに簡素化されます。

第 2 に、ネットワークの任意の場所でファイアウォール、インライン型の侵入検知、VPN などのセキュリティ機能を柔軟に適用して、セキュリティ上の脅威に対する最適な防御を実現できます。シスコのルータベース、スイッチベース、アプライアンススペースの各種機能を組み合わせると、ネットワークのすべての場所でエンドツーエンドの保護を実現できます。

第 3 に、ルータはネットワークへの最初のエン트리 ポイントであるため、Cisco IOS ソフトウェアのセキュリティをルータに直接統合することで、ネットワークのゲートウェイを保護できます。Cisco IOS ソフトウェアのセキュリティは、データセンターのエン트리 ポイントである WAN アグリゲーション ルータにも統合されます。これにより、ネットワークのすべてのエン트리 ポイント (ネットワークの保護に適した論理上の場所) にクラス最高レベルのセキュリティ機能を導入することが可能になります。

ルータのセキュリティ機能はネットワークの最初のエン트리 ポイントを防御するだけでなく、ルータのインテリジェンスを利用して「信頼性の高い」トラフィック処理を行うことにより、高度なセキュリティ、Quality of Service (QoS; サービス品質)、ルーティング機能の統合を実現します。これにより、セキュリティ機能による情報の共有と脅威に対する迅速で正確な対応が可能になり、ネットワークのハイアベイラビリティが確保されます。統合セキュリティはルータそのものを保護すると同時に、Distributed DoS (DDoS; 分散型 DoS) 攻撃のようなネットワーク インフラストラクチャを直接ターゲットとする攻撃に対しても防御ラインを構築します。

単独機能を提供するセキュリティ ソリューションの多くは、ネットワークの特定の部分を保護するもので、シスコのセキュリティ ソリューションのように、インフラストラクチャ全体を保護できるセキュリティ ソリューションはほとんど存在しません。

システム アプローチ利用の重要性

Cisco 800 シリーズ、Cisco ISR 1800/2800/3800 シリーズ、Cisco 7200 シリーズに搭載されている統合セキュリティ機能の考察に移る前に、システム アプローチを利用することの重要性について説明します。

ブランチ オフィスにおけるハイ アベイラビリティ

シスコは、ブランチ オフィスのハイ アベイラビリティを維持するためにさまざまな機能を幅広く提供しています。シスコのアプローチは常時アクセス可能なネットワークを基本目標に設計されています。そのため、このアプローチをエンドツーエンドで利用することによって、企業の IT 部門は導入や管理が容易な自己防衛型ネットワーク アーキテクチャを実現できます。サービス統合型ルータでは、より多くのインターフェイスと機能を同時に利用することで、複数のセキュリティ、管理、統合といったサービスを優れたパフォーマンスで並行して実行できます。そのため、このアプローチはさらに強化されます。

シスコは、サービス統合型ルータを通じて、ブランチ オフィスのハイ アベイラビリティを実現し、将来にわたって利用可能な総合ソリューションを提供しています。このソリューションは、ネットワークの停止を最小限に抑え、重要な業務アプリケーションへの常時アクセスを確実に実現します。シスコでは、パフォーマンスを備えた新しいインフラストラクチャ サービスの統合に取り組んでいるため、企業はこれまで以上にインテリジェントで耐障害性に優れた信頼性の高いネットワークを構築できます。

パフォーマンス

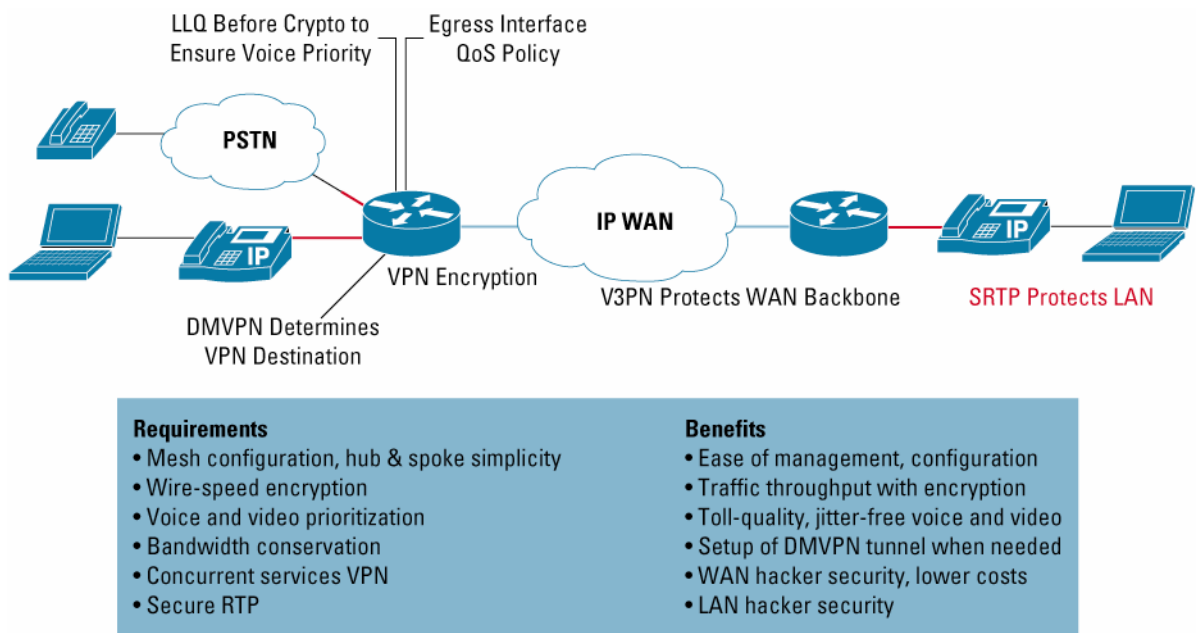
シスコのサービス統合型ルータは、システム アプローチを利用して、WAN で適切なラインレート パフォーマンスを提供できるように設計されています。音声やセキュリティなどのサービスを追加で利用する場合でも、対応する WAN インターフェイスの速度以下にパフォーマンスが低下することはありません。サービス統合型ルータは、適切な CPU 処理能力を利用して複数のサービスを同時に実行できるように最適化されており、VPN などの CPU 負荷の高いサービスは専用のアクセラレータにオフロードされます。

シスコは Mier Communications 社と提携して、新しいシスコ サービス統合型ルータのコンフィギュレーション、運用性、パフォーマンスに関する検証を独自に行いました。Miercom 社はこれらのシステムの詳細な検証に基づいて、大量のデータをやり取りしているブランチ オフィスに、重要性の高い高度なネットワーク サービス（ステートフルな Cisco IOS ファイアウォールと Network Address Translation [NAT; ネットワーク アドレス変換]、IPS、Voice over IP [VoIP]、アナログ電話サービスなど）を同時展開した場合のシステム パフォーマンスを証明しました。また、このテストでは、伝送負荷が大きい場合でも質の高い音声サービスを確保できることが確認されました。

インテリジェンス

システム アプローチは、シスコのサービス統合型ルータのような耐障害性に優れた単体のプラットフォームから始まりますが、「一体型」製品だけに限られる訳ではありません。システム アプローチでは、サービスの中にインテリジェントなサービスが組み込まれます。サービスは相互に連携することで、ダイナミック トンネリング対応の DMVPN（動的マルチポイント VPN）や、V³PN（Voice and Video Enabled VPN）といった優れた機能を発揮します（図 2 を参照）。

図 2 DMVPN および V³PN によるセキュアな高品質 IP テレフォニー



システム アプローチは、音声、セキュリティ、ルーティング、アプリケーション サービスを相互に連携させることによって、処理の自動化とインテリジェント化を実現します。その結果、ネットワークとアプリケーションにおけるセキュリティの幅広い展開、データ/音声/映像トラフィックに対応したより高度な QoS、非生産的な時間の短縮、ネットワーク リソースの活用化が実現します。

クラス最高レベルのソフトウェアとアプリケーションを単一のプラットフォームに統合することで、お客様は次のような利点を得ることができます。

- 基本的なサービスや高度なサービスの導入が迅速化する
- サービス管理に共通のツールとインターフェイスが利用できるため、運用が簡素化する
- ロックが必要な機器の数を最小限に抑えることで、ネットワークセキュリティが向上する
- 新しいアプリケーション用にデータ配信を高速化したりハードウェアを解放したりする際に、既存の、あるいは将来提供されるインターフェイスやネットワークモジュールを利用できる
- トラブルシューティングの迅速化、「スペア」管理の簡素化、スタッフ教育時間の短縮など、運用コスト削減につながるあらゆる要素が実現する
- バンドルパッケージとサービス契約の利用で資産コストが抑制される

シスコの新しいサービス統合型ルータの優れたセキュリティ機能

20年にわたるシスコの先進的な技術開発力をベースにした Cisco 800 シリーズ、Cisco 1812J、および Cisco ISR 1800/2800/3800 シリーズには、業界で最も幅広いセキュリティサービスが備わっています。データ、セキュリティ、音声を耐障害性に優れた単一システムにインテリジェントに統合することで、ミッションクリティカルなビジネスアプリケーションの迅速でスケーラブルな提供を可能にします。

たとえば、シスコのサービス統合型ルータは、ハードウェアベースの暗号化機能を標準で搭載しています。この内蔵されたハードウェアベースの暗号化アクセラレーションによって、VPN プロセスがオフロードされ、ルータの CPU に対する影響を最小限に抑えながら VPN のスループットを向上させます。VPN のスループットやスケーラビリティ（VPN トンネルの数など）の追加が必要な場合は、オプションの VPN 暗号化 Advanced Integration Module（AIM）を利用できます。

またサービス統合型ルータには、シスコの自己防衛型ネットワークが提案する信頼性およびアイデンティティ管理、ネットワークインフラストラクチャの保護、セキュアコネクティビティ、攻撃防御という4つの保護カテゴリを実装できます（図3を参照）。

図3 サービス統合型ルータと自己防衛型ネットワーク



信頼性およびアイデンティティ管理

信頼性およびアイデンティティ管理サービスを利用すると、NAC（ネットワーク アドミッション コントロール）、アイデンティティ サービス、Authentication, Authorization, Accounting（AAA; 認証、許可、アカウントリング）などのテクノロジーを使って、ネットワークのエンドポイントをインテリジェントに保護できます。

NAC

NAC はシスコが主導する業界コラボレーションです。NAC を利用すると、アクセスを許可する前にすべてのエンドポイントをネットワークのセキュリティ ポリシーに確実に適合させることができます。NAC では、ネットワークに接続するデバイスがネットワークにアクセスしようとする、これらが企業の最新のセキュリティ対策ポリシーや OS（オペレーティング システム）パッチ ポリシーに適合しているかどうかを確認することで、ウイルスやワームによる被害を最小限に抑えます。セキュリティ ポリシーに適合していない脆弱なホストは隔離され、パッチやセキュリティ保護が適用されるまで制限付きのネットワーク アクセスが付与されます。このようにして、脆弱なホストがワームやウイルスの感染源や感染対象になるのを防ぎます。

シスコの自己防衛型ネットワークを実現するための第一歩として、Cisco 800 シリーズ ルータ、Cisco 1812J ルータ、Cisco ISR 1800/2800/3800 シリーズ、Cisco 7200 シリーズ、および 7301 アグリゲーション ルータ上で NAC や Cisco IOS ソフトウェアの統合セキュリティ サービスを利用する場合は、Cisco IOS ソフトウェアの Advanced Security、Advanced IP Services、または Advanced Enterprise Services フィーチャ セットを使用します。

AAA

Cisco IOS ソフトウェアの AAA ネットワーク セキュリティ サービスは、ルータやアクセス サーバにアクセス制御を設定するための主要なフレームワークを提供します。AAA を利用すると、管理者は特定のサービスやインターフェイスに適用されるメソッド リストを使用して、回線単位（ユーザ単位）またはサービス単位（IP、Novell Internetwork Packet Exchange [IPX]、Virtual Private Dialup Network [VPDN]）で必要となる認証および許可のタイプをダイナミックに設定できます。

802.1X 標準

標準の 802.1X アプリケーションを利用すると、有効なアクセス証明書が要求されるため、保護された情報リソースへの不正アクセスが困難になります。また、ネットワーク管理者は、セキュリティ保護されていないワイヤレス アクセス ポイントをユーザが社内に持ち込めないようにすることができます。ユーザが持ち込む不正なワイヤレス アクセス ポイントは、簡単に導入できるワイヤレス LAN（WLAN）機器に関する大きな懸念の 1 つです。

USB ポート/着脱式証明書

Cisco 800 シリーズおよび Cisco ISR 1800/2800/3800 シリーズには、オンボードの USB 1.1 ポートが搭載されています。このポートを使うと、重要なセキュリティ機能やストレージ機能が利用できます。この機能は、セキュアな VPN 接続を確立するための着脱式証明書の保存、コンフィギュレーション ファイルの安全な配布、ファイルやコンフィギュレーション用の大容量フラッシュ ストレージに利用できます。

ネットワーク基盤の保護

Network Foundation Protection（NFP; ネットワーク基盤の保護）は、攻撃や脆弱性からネットワーク インフラストラクチャをネットワーク レベルで保護します。この機能には、コントロールプレーン ポリシング、AutoSecure、Network-Based Application Recognition（NBAR）などがあります。

コントロールプレーン ポリシング

非常に強固なソフトウェアやハードウェア アーキテクチャでも、意味のないトラフィックを大量に送りつけてネットワーク インフラストラクチャを麻痺させる悪質な DoS 攻撃に対しては脆弱です。Cisco IOS ソフトウェアには、制御パケットを偽装してネットワークの心臓部を狙うこの種の脅威を防御するために、コントロールプレーン プロセッサ宛のトラフィックのレートを制限するプログラム可能なポリシング機能が搭載されています。この機能は Control Plane Policing（CoPP; コントロールプレーン ポリシング）と呼ばれ、特定のトラフィック タイプを識別して制限するように設定できます。設定では、トラフィックを完全に制限したり、一定のスレッショールド レベルを超えた場合に制限したりすることができます。

AutoSecure

Cisco IOS ソフトウェアの機能の 1 つである AutoSecure は、ルータのセキュリティ設定を簡素化して、設定ミスリスクを軽減します。熟練したユーザ向けの対話モードでは、ルータのセキュリティ機能の制御を強化するために、セキュリティ設定とルータサービスのカスタマイズが要求されます。AutoSecure の非対話モードでは、International Computer Security Association (ICSA) が推奨するルータのセキュリティ機能が、シスコのデフォルト設定に基づいて自動で有効になります。コマンドを 1 回入力するだけで、ルータのセキュリティ ポスチャの設定と不要なシステム プロセスやサービスの無効化がただちに行われ、潜在的なネットワーク セキュリティの脅威を排除することができます。

NBAR

NBAR は Cisco IOS ソフトウェア内の分類エンジンで、詳細なステートフル パケット インспекションを使用して、Web ベースのプロトコルやその他の分類の困難なプロトコルを含む広範なアプリケーションを認識します。NBAR をセキュリティ コンテキストで使用すると、ペイロード シグニチャに基づいてワームを検出できます。アプリケーションが NBAR によって認識および分類されると、ネットワークはその特定のアプリケーションに対してサービスを起動できます。Cisco SDM には、NBAR を有効にする使いやすいウィザードが組み込まれています。また、アプリケーション トラフィックをグラフィカルに表示することもできます。

Cisco SDM

Cisco 800 シリーズ ルータ、Cisco ISR 1800/2800/3800 シリーズ、Cisco 7200 シリーズ ルータ、および Cisco 7301 アグリゲーション ルータには、Cisco SDM が出荷時にインストールされています。Cisco SDM は、シスコ ルータの導入や管理を行うための使いやすい Web ベース デバイス マネージャ (GUI) です。Cisco SDM では、迅速な導入とルータのロックダウンを行うスタートアップ ウィザードを使用して、ルータの設定とモニタリングを簡素化できます。また、Cisco SDM のスマート ウィザードを使用すると、セキュリティやルーティング機能の有効化、Technical Assistance Center (TAC) 推奨のルータ コンフィギュレーションの利用、テーマ別の教育コンテンツの利用が可能です。

セキュア コネクティビティ

セキュア コネクティビティでは、複数のタイプのトラフィックを統合して、セキュアでスケーラブルなネットワーク接続を実現します。具体的には、VPN トンネリングと暗号化、DMVPN、Easy VPN、V³PN、Virtual Tunneling Interface (VTI)、Multi-Virtual Route Forwarding (VRF)、Multiprotocol Label Switching (MPLS; マルチプロトコル ラベル スイッチング)、セキュア コンテキストなどです。

VPN トンネリングと暗号化

VPN は、最も急速な成長を遂げているネットワークの接続形態です。Cisco 800 シリーズ ルータ、Cisco 1812J ルータ、および Cisco ISR 1800/2800/3800 シリーズには、ハードウェアベースの VPN 暗号化アクセラレーションが内蔵されています。これによって IPSec 暗号化と VPN プロセスがオフロードされるため、ルータの CPU への影響が最小限に抑えられ、VPN のスループットが向上します。この機能は、AIM スロットを使用することなく、IPSec、AES、Digital Encryption Standard (DES)、Triple DES (3DES) 暗号化もサポートします。

VPN のスループットやスケーラビリティの追加が必要な企業では、オプションの VPN 暗号化 AIM が利用できます。これにより、VPN パフォーマンスの向上と、ルータの全体的な CPU 負荷の軽減が可能になります。オプションの AIM は、旧モデルと比較して最大 10 倍の暗号化パフォーマンスとトンネル スケーラビリティを提供します。

サービス統合型ルータでは、IPSec と Generic Routing Encapsulation (GRE; 総称ルーティング カプセル化) プロトコルを組み合わせた代替トンネリング技術も使用できます。GRE トンネリング技術を使用した IPSec は、シスコ独自のソリューションです。このソリューションは、VPN を介したダイナミック ルーティング プロトコルの送信を可能にするため、IPSec のみのソリューションよりもネットワークの耐障害性に優れています。GRE トンネルは、フェールオーバー メカニズムを提供するだけでなく、マルチキャスト パケット、ブロードキャスト パケット、非 IP プロトコルを暗号化する機能も備えています。

DMVPN

Cisco DMVPN を使うと、オンデマンドでスケーラブルなフルメッシュ VPN を利用して、遅延の短縮、帯域幅の節約、VPN 展開の簡素化を実現できます。DMVPN 機能は、IPSec とルーティングに関するシスコのノウハウをベースに開発されたもので、GRE トンネル、IPSec 暗号化、Next Hop Resolution Protocol (NHRP)、Open Shortest Path First (OSPF)、および Enhanced Interior Gateway Routing Protocol (EIGRP) を動的に設定することができます。

この VPN トンネルの動的設定に QoS や IP マルチキャストなどのテクノロジーを組み合わせると、音声や映像といった遅延の影響を受けやすいアプリケーションを最適化できます。また、DMVPN を使用すれば、新たにスポークを追加したり、スポークツースポーク接続をセットアップしたりするときに、ハブのコンフィギュレーションを変更する必要がないため、管理作業が容易になります。

セキュアな音声

シスコのサービス統合型アクセスルータ製品のメディア認証および暗号化機能を使用すると、Time Division Multiplexing (TDM; 時分割多重) またはアナログ音声ゲートウェイポートで終端する音声通話を盗聴から保護できます。この信頼性が高くスケーラブルな機能によって、LAN や WAN でのセキュアな IP コミュニケーション環境が実現します。

セキュアな Real-Time Transport Protocol (SRTP) を使用するメディア暗号化では、音声通話を暗号化することによって、音声ドメインに侵入またはアクセスした社内外のハッカーが通話内容を理解できないようにします。IETF RFC 3711 標準である SRTP は、特に音声パケット用に設計されたもので、AES 暗号化アルゴリズムをサポートします。SRTP を使用するメディア暗号化は、IPSec よりも優れた帯域幅利用効率を実現します。

Easy VPN

Easy VPN は、ハブアンドスポーク型の VPN トポロジをサポートするために設計された IPSec ソリューションで、少ない手間で高いスケーラビリティが得られます。Easy VPN を利用すると、Cisco ASA 5500 適応型セキュリティアプライアンスなどを使用した VPN ソリューションのプロビジョニングと管理を簡素化できます。多数の導入実績からもわかるように、Easy VPN では「ポリシープッシュ」テクノロジーを使用することで、豊富な機能とポリシー制御機能は維持しながら、コンフィギュレーションの簡素化を実現しています。

音声および映像に対応した IPSec

Cisco 800 シリーズルータ、Cisco 1812J ルータ、Cisco ISR 1800/2800/3800 シリーズ、Cisco 7200 シリーズ、および 7301 アグリゲーションルータは V³PN をサポートしています。V³PN は、セキュアな QoS 対応 IPSec ネットワーク上でデータ/音声/映像の統合に対応した VPN インフラストラクチャを提供します。V³PN を利用すると、音声および映像アプリケーションのパフォーマンスが、別の WAN リンク経由で伝送される場合と同様に、IP トランスポート上でも安全かつ効率的に実現します。シスコのサービス統合型ルータは、市販の多くの VPN デバイスとは異なり、マルチサービス IPSec VPN を実現する多様なネットワークトポロジとトラフィック要件に対応しています。V³PN のエンドツーエンドのネットワークアーキテクチャは、Cisco IOS ソフトウェア搭載のシスコのセキュリティ対応ルータを利用して音声トラフィックを保護します。

IPSec VPN を介して高品質の音声および映像配信を実現するには、トラフィックの暗号化だけでなく、最先端のマルチサービステクノロジーと IPSec VPN テクノロジーの融合が必要です。Cisco V³PN の利用を可能にする Cisco IOS ソフトウェアの主なテクノロジーには、マルチサービス重視型の QoS、多様なトラフィックのサポート、マルチサービスネットワークトポロジのサポート、拡張ネットワークフェールオーバー機能などがあります。

VTI (Virtual Tunneling Interface)

Cisco IPSec VTI (Virtual Tunneling Interface) は、異なるサイトのデバイスの間に IPSec ベースの VPN を設定できる新しいツールです。IPSec VTI トンネルは、共有 WAN 上での経路を指定し、新しいパケットヘッダーを使ってトラフィックをカプセル化することにより、指定の宛先への確実な配送を可能にします。トラフィックは一方のエンドポイントからしかトンネルに入らないため、このネットワークのプライバシーは維持されます。また、IPSec が提供する機密性保持機能(暗号化)によって、トラフィックは暗号化されます。

サービス プロバイダー向けのマルチ VRF と MPLS セキュア コンテキスト

マルチ VRF は、サイト間 IPsec VPN の拡張機能です。プロバイダー ネットワークを通じてトラフィックを伝送する場合、企業は当然セキュリティやプライバシーの確保を期待します。しかし、従来型の LAN ネットワークでは、トラフィックのセグメント化を適切に維持することが困難になってきています。複数のブランチ サイトにネットワークを展開する場合、これは特に重要なポイントです。マルチ VRF を利用すると、複数のセグメント間で簡潔かつ経済的にプライバシーを維持できます。

攻撃防御

攻撃防御サービスでは、ネットワーク サービスを利用して、ネットワーク攻撃や脅威に対する防御と対処を行います。この機能には、Cisco IOS ファイアウォールや Cisco IOS IPS などが含まれます。

Cisco IOS ファイアウォール

Cisco IOS ファイアウォールは、シスコ ルータで使用可能なステートフル インспекション ファイアウォール オプションです。このファイアウォールには、業界トップクラスの Cisco ASA 5500 適応型セキュリティ アプライアンスと同様のステートフル ファイアウォール テクノロジーが利用されており、Cisco IOS ソフトウェアの Advanced Security フィーチャ セット（またはさらに上位のフィーチャ セット）を搭載したすべてのサービス統合型ルータでサポートされています。Cisco IOS ファイアウォールは、セキュリティとルーティングを単体で実現するソリューションで、WAN への入り口の保護に最適です。通常、中央サイトでは、攻撃に備えてファイアウォールを配置しトラフィックも検査しますが、セキュリティ対策を講じる際にはリモート オフィスも考慮する必要があります。

Cisco IOS ファイアウォールの機能は、アプリケーション ファイアウォールのサポートを導入することで強化されています。Cisco IOS ファイアウォールで アプリケーション ファイアウォールを利用すると、非 HTTP トラフィックがブロックできるわけではありません。HTTP と推定されるトラフィックが本物の Web ブラウジングであり、ファイアウォール経由でアクセスしようとするインスタント メッセージングの類いではないことが確認できます。その結果、ネットワーク管理者は、ファイアウォールを通過するアプリケーションをより詳細に制御できるようになります。

Cisco IOS ファイアウォールを利用すると、ネットワーク境界部分のシングル ポイントを保護できるだけでなく、ネットワークそのものにセキュリティ ポリシーを実施する機能を組み込むことができます。セキュリティ ポリシーを専用で実施するにしても統合するにしても、柔軟性とコスト効率に優れたポリシー実施が可能です。そのため、エクストラネットとイントラネットの境界に対して、あるいはブランチ オフィスやリモート オフィスのインターネット接続に対してセキュリティ ソリューションを容易に実現できます。Cisco IOS ファイアウォールは Cisco IOS ソフトウェアによってネットワークに統合されるため、ユーザは同じルータで拡張 QoS 機能を利用できます。

Cisco IOS ソフトウェアは IPv6 ファイアウォールをサポートしているため、IPv4 と IPv6 の混在環境でも使用できます。また、IPv6 パケットのステートフルプロトコル インспекション（異常検出）を提供することで、IPv6 DoS 攻撃を軽減します。

トランスペアレント ファイアウォール

レイヤ 3 のステートフル ファイアウォールに加えて、Cisco 800 シリーズ ルータ、Cisco 1812J ルータ、Cisco ISR 1800/2800/3800 シリーズ、Cisco 7200 シリーズ、および 7301 アグリゲーション ルータは、トランスペアレント ファイアウォールをサポートします。これは、同一のルータ上で、レイヤ 2 接続に対してレイヤ 3 ファイアウォールを提供する機能です。トランスペアレント ファイアウォールは、サブインターフェイスと VLAN トランク、Spanning Tree Protocol (STP; スパニングツリー プロトコル)、すべての標準管理ツール、および対向のインターフェイス（双方向）に DHCP アドレスを割り当てる DHCP パススルーをサポートしています。この機能は、IP サブネット番号の変更やインターフェイス上の IP アドレスが必要ないため、既存のネットワークに容易に追加できます。

インライン型 IPS

シスコは、インライン型 IPS 機能搭載のルータを業界に先駆けて市場に投入しました。Cisco IOS IPS は、Cisco IOS ソフトウェアがネットワーク攻撃を効果的に軽減できるようにするインライン型のディープパケット インスペクションベース ソリューションです。侵入防御とイベント通知に使用される Cisco IOS IPS には、Cisco Intrusion Detection System (IDS; 侵入検知システム) センサ製品ファミリ (Cisco IDS 4200 シリーズ アプライアンス、Cisco Catalyst® 6500 IDS サービス モジュール、ネットワーク モジュールハードウェア IDS アプライアンスなど) のテクノロジーが活用されています。

Cisco IOS ソフトウェア IPS はインラインで動作するため、トラフィックの廃棄、アラームの送信、接続のリセットが実行でき、ルータはセキュリティ上の脅威に即座に対処してネットワークを保護できます。また、IPSec VPN、GRE、Cisco IOS ファイアウォールと連携して、ネットワーク (ブランチまたは中央サイト) のエントリ ポイントで復号化、トンネル終端、ファイアウォールによる保護、トラフィック検査を実行できます。これは業界初の機能です。Cisco IOS IPS を使うと、攻撃元に可能な限り近いところで攻撃トラフィックを防御できます。

Cisco 800 シリーズ ルータ、Cisco 1812J ルータ、および Cisco ISR 1800/2800/3800 シリーズのリリースに統合された Cisco IOS IPS では、Cisco IDS センサ アプライアンスと同様に、選択した IPS シグニチャのロードと有効化ができるため、Cisco IDS センサプラットフォームがサポートする 1200 を超えるシグニチャを利用できます。また、企業は新たに検出された脅威に対応するために、既存のシグニチャを変更したり、新しいシグニチャを作成したりすることができます。最大限の侵入防御を必要としている企業は、「最も可能性の高い」ワームや攻撃のシグニチャを含む、使いやすいシグニチャ ファイルを選択できます。ワームと攻撃に対するこの信頼性の高いシグニチャに一致するトラフィックは、廃棄されるように設定されます。Cisco SDM には、このシグニチャをプロビジョニングするためのわかりやすいユーザ インターフェイスが備わっています。これにより、ソフトウェア イメージを変更することなく Cisco.com から新しいシグニチャをアップロードし、そのシグニチャに対してルータを適切に設定することができます。

URL フィルタリング (オフボックス/オンボックス オプション)

シスコでは、Cisco IOS ファイアウォールをサポートする URL フィルタリングを提供しているため、Websense または N2H2 の URL フィルタリング製品のいずれかをシスコ セキュリティ ルータと組み合わせて利用できます。Websense の URL フィルタリング機能を使用すると、Cisco IOS ファイアウォールに Websense または N2H2 の URL フィルタリング ソフトウェアを連携させることで、企業のセキュリティ ポリシーに基づき指定の Web サイトへのアクセスを防止できます。Cisco IOS ファイアウォールは、Websense や N2H2 サーバと連携して、特定の URL を許可するか拒否 (ブロック) するかどうかを識別します。

拡張セキュリティ ネットワーク モジュール (Cisco ISR 2800/3800 シリーズのオプション)

IDS とコンテンツ セキュリティを実現する専用のハードウェアベース ソリューションを希望する企業は、Cisco ISR 2800/3800 シリーズに 2 種類のセキュリティ ネットワーク モジュールをオプションで追加することができます。

Cisco IDS ネットワーク モジュールを利用すると、他の IDS コンポーネントと相互に連携して、データや情報インフラストラクチャを効率的に保護する完全な IDS システムを実現できます。このモジュールには、IDS 専用の CPU と、1000 を超える IPS シグニチャを記録するための 20 GB ハード ドライブが搭載されています。Cisco Content Engine ネットワーク モジュールを利用すると、コンテンツ セキュリティ機能を備えたルータ統合型のコンテンツ配信システムを実現できます。また、インテリジェント キャッシングとコンテンツ ルーティングだけでなく、URL フィルタリング (Websense、SmartFilter) アプリケーション サーバとして動作することも可能です。

注目を集めるルータ統合サービス

企業規模の大小を問わず、ルータ統合サービスには強い関心が寄せられています。

Ann Taylor 社

Ann Taylor 社は、米国およびプエルトリコに 600 を超える店舗を持つ数十億ドル規模のアパレル会社です。同社は業務の拡大をサポートするために、既存のダイヤルアップ ネットワークを置き換えて、Web ベースの販売および在庫管理アプリケーション、迅速なクレジット決済を可能にするセキュアなトランザクション、将来店内に展開予定の音声/映像キオスクに対応できるようにすることを決めました。

Ann Taylor 社は新しいネットワークに VPN 機能を統合したシスコ ルータを導入し、導入先すべてにイントラネット、E メール、オンライン販売と注文処理システム、クレジット スイッチとカード決済システム、全社の在庫管理、販売実績アプリケーションを実現しました。

結果は大成功でした。新しい在庫管理システムにより、販売員は商品に関する正確な情報をリアルタイムで入手できるようになったため、商品管理が容易になりました。マネージャは書類やマニュアルの入手、販売データの確認、商品ディスプレイの変更が可能になりました。新しいシステムの導入によって、すべての拠点で売り上げが大幅に伸びました。

GST 社

34 か所のオフィスに 380 人の社員を抱える GST 社は、運送とロジスティックス ソリューションを提供しています。同社は既存のデータ ネットワークと音声ネットワークを統合することで、インターネット アクセスの拡大とコストの削減、ベンダーとネットワーク管理の簡素化、電話機の移設、追加、変更の手間とコストの削減を目指しました。

同社は、シスコのスイッチとルータを使用してデータ、VPN、セキュリティ、IP テレフォニーを統合しました。その結果、19 か所のオフィスに対して月 52,000 ドル掛かっていた経費が、3 年後には、34 か所のオフィスに対して月 57,000 ドルにまで削減されました。また、新たに 15 か所のオフィスがネットワークに追加されたため、リモートの社員も本社の社員と同じようにネットワークへアクセスできるようになりました。現在では、顧客が Web サイトを通じて直接オーダーを行ったり追跡したりできるようになっています。

専用のセキュリティ アプライアンスかサービス統合型ルータか

ファイアウォールを導入するお客様は、クラス最高レベルの専用の Cisco ASA 5500 適応型セキュリティ アプライアンスか、または Cisco IOS ファイアウォールかを選択できます。ルータ統合型の Cisco IOS ファイアウォール には、Cisco ASA 5500 適応型セキュリティ アプライアンスのテクノロジーにシスコが 20 年来培ってきたルーティングのノウハウが融合されています。

シスコは今後も、クラス最高レベルのセキュリティを組み込んだルータと専用のセキュリティ アプライアンスを提供していきます。これは、自社のネットワークのセキュリティ保護を考慮のお客様が、それぞれに最適なソリューションを選択できるようにするためです。統合型セキュリティとスタンドアロン型アプライアンスの境目はいまだに明確ではありませんが、お客様はさまざまな理由から、どちらか一方のセキュリティ ソリューションを選択したり組み合わせ使用したりしています。

小規模企業やブランチ オフィスに適した統合型セキュリティ

セキュリティ保護が必要なネットワークの場所を検討することは重要です。多くの企業では、エッジのアグリゲーション ルータにセキュリティを統合しています。ただし大企業では、ヘッドエンドをスタンドアロン型のアプライアンスで保護し、データセンターを Cisco Catalyst スイッチに搭載したファイアウォール サービス モジュール (FWSM) で保護することがあります。ネットワークのこのような場所ではより高いスループットが必要になるためです。また、こういった企業では、ブランチ オフィスにセキュリティ機能が統合されたルータを追加して、ネットワークのすべての場所を保護することもできます。

中堅・中小企業や大企業のブランチ オフィスは、大企業の本社と同様のさまざまなセキュリティ上の課題に直面しているばかりか、セキュリティ ソリューションを管理するローカルの IT スタッフがほとんど（または、まったく）いないことがほとんどです。IT スタッフが限られているため、数多くのデバイスの導入と管理が企業のサポート モデルになじまないことがあります。このような場合は、中央で管理できる単一のプラットフォームに複数のデバイスを統合することで、TCO を抑制しながら小規模なオフィスでのトラブルシューティングやメンテナンスを容易にすることができます。

Cisco 800 シリーズ ルータ、Cisco 1812J ルータ、および Cisco ISR 1800/2800/3800 シリーズは、中小企業や大企業のブランチ オフィスに最適な製品です。この製品が提供する機能豊富な統合ソリューションを利用すれば、リモート オフィス、モバイル ユーザ、パートナーのエクストラネットやプロバイダーが管理する Customer Premises Equipment (CPE; 顧客宅内機器) を接続することができます。シスコは、Cisco IOS ソフトウェアベースの VPN、ファイアウォール、IPS、また、オプションの拡張 VPN アクセラレーション、IDSや Content Engine ネットワーク モジュール (Cisco 2800/3800 シリーズ) を通じて、ブランチオフィス ルータ向けの堅牢性と適応性に優れたセキュリティ ソリューションを提供しています。

ある大手スーパーマーケット チェーンは、専用回線を使用して各店舗と本社を WAN で接続していました。このスーパーマーケットの本社に保管されている顧客データは非常に重要です。連邦法および州法によって、情報が漏洩した場合はすべての顧客に通知することが義務付けられているためです。店舗で発生する悪質な攻撃からネットワークを保護するために、このスーパーマーケット チェーンは既存のルータに Cisco IOS ファイアウォールを追加することにしました。

企業の好み

ネットワーク統合型セキュリティまたは専用セキュリティ ソリューションのいずれを使用するかという選択には、既存のインフラストラクチャの活用、導入および運用アーキテクチャ、特定の機能の違いといったユーザの好みが反映されることがあります。企業の中には、「ルータはルータとして使用し、スイッチはスイッチとして使用する」シンプルな構成を好むところもあります。また、セキュリティや VPN の専任管理チームを持っている企業では、管理上の問題から、セキュリティや VPN のインフラストラクチャをネットワーク インフラストラクチャから分離することが望まれる場合もあります。

将来必要になるコストの評価

既存のルータやスイッチに Cisco IOS ソフトウェアのセキュリティ イメージや VPN モジュールを追加してセキュリティ対策に活用することは、コスト効率に優れた方法であり、インフラストラクチャの寿命を延ばすことにもなります。既存の資産を最大限に有効活用できると同時に、未成熟なデバイスを導入したことが原因で発生する可能性のあるコストや業務の中断を大幅に減らすことができるからです。計画的なダウンタイムおよび予期しないダウンタイムに伴うコストは、将来必要になるコストを評価する上で最も重要な要素です。

ネットワークを将来のマルチメディア統合型構成に対応するようにサービス統合機能を強化すると、ネットワークの全体的な柔軟性と可用性も向上します。このような機能を備えることによって、企業は迅速な対応による機会損失の回避、新サービスの導入に要する時間の短縮、頻繁に行われる無用なデバイス アップグレードの解消、拡張性の向上による TCO の削減を実現することもできます。

機能の違い

Cisco IOS ファイアウォールには Cisco ASA 5500 適応型セキュリティ アプライアンスのテクノロジーが統合されているため、2つのセキュリティ ソリューションの機能はかなり似通ってきています。ただしシスコでは、サービス統合型ルータに新しいテクノロジーを組み込む前に、セキュリティ アプライアンスを使用して、そのテクノロジーの改良と検証を行うことにしています。通常、最新のセキュリティ機能は、Cisco IOS ファイアウォールのオプションとして提供される前に、最新の先端セキュリティ機能を必要とする企業向けに Cisco ASA 5500 適応型セキュリティ アプライアンスで提供されます。

まとめ

今日、多くの企業にとってネットワークは欠くことのできない存在です。また、迫り来る脅威からネットワークを保護しようと努力している IT マネージャにとって、ネットワーク セキュリティ対策は優先すべき課題です。セキュリティに対する要求が高まり、ネットワークのすべてのエントリ ポイントを保護する統合型セキュリティ ソリューションが求められつつある中で、シスコはセキュリティ ポートフォリオを強化し、ネットワークの脅威の識別、防御、対処機能を大幅に向上させています。

組み込みのセキュリティ ハードウェア アクセラレーションが搭載された次世代型のシスコ サービス統合型ルータは、Cisco IOS VPN、ファイアウォール、インライン型 IPS サービスをシスコのルータ製品ファミリに統合することによって、業界随一の包括的で適応力に優れたセキュリティ ソリューションを実現しています。これらのルータは、セキュリティ機能を統合することによって OS (オペレーティング システム) やデバイスの数を最小限に抑え、限られた IT リソースでの管理を可能にする必要のある小規模オフィスやリモート オフィスのニーズに対応しています。

シスコの統合セキュリティ ソリューションは、堅牢な Cisco IOS ソフトウェア機能と LAN/WAN 接続機能に、卓越したセキュリティ機能を融合させているため、企業は既存のネットワーク インフラストラクチャを活用しながら必要な場所にセキュリティを導入することができます。ハードウェアを追加する代わりに Cisco IOS ソフトウェアを利用すれば、既存のルータで最新の統合セキュリティ機能を使用し、ネットワークの任意の場所にセキュリティ機能を適用できます。シスコのサービス統合型ルータは、ネットワークのすべてのエントリ ポイントを保護するだけでなく、ネットワーク インフラストラクチャを直接狙った攻撃の防御も行います。

関連情報

Cisco ISR 1800/2800/3800 シリーズの統合セキュリティ機能については、Web に掲載されている次の資料を参照してください。

データ シート

Cisco ISR 1800、2800、および 3800 のセキュリティ機能

http://www.cisco.com/jp/product/hs/routers/isr/isr3800/prodlit/sfisir_ds.shtml

Q&A

Security Features on the Cisco Integrated Services Routers (英語)

http://www.cisco.com/en/US/products/ps5854/products_qanda_item0900aecd80169bba.shtml

Miercom 社ラボ評価試験サマリー レポート

Cisco Integrated Services Routers (英語)

<http://www.miercom.com>

NAC

<http://www.cisco.com/jp/go/nac/>

Cisco IOS のセキュリティ機能

Cisco IOS セキュリティサービスによるネットワーク インフラストラクチャの保護

http://www.cisco.com/jp/product/hs/ios/security/nfp/prodlit/pnicioss_ds.shtml

Cisco Router and Security Device Manager

<http://www.cisco.com/jp/go/sdm/>

©2006 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

〒 107-0052 東京都港区赤坂 2-14-27 国際新赤坂ビル東館
<http://www.cisco.com/jp>

お問い合わせ先 (シスコ コンタクトセンター)
<http://www.cisco.com/jp/service/contactcenter>

0120-092-255 (通話料無料)

電話受付時間: 平日 10:00 ~ 12:00, 13:00 ~ 17:00