

Cisco IOS Software is
hard at work behind the
scenes providing multilayer
network protection.

Background CHECKS

ネットワーク背後の守りをチェックしよう!

Cisco IOS Softwareは
その高い性能でネットワークを守りつづける

Cisco IOS Softwareは、アクセス制御、インラインファイアウォールフィルタリング、侵入検知機能等を駆使し、企業やサービスプロバイダのネットワークを長年にわたり静かに守ってきた。そして今、プライバシー侵害の脅威がインターネットエッジから、企業のデータセンター、無線LANアクセスポイント、およびユーザーのデスクトップへと内側に広がるにつれ、Cisco IOSのセキュリティ機能はさらに高度なものへと進化している。

Cisco IOS Softwareはネットワークセキュリティに対してさまざまなレベルで統合型のアプローチを取っている。まず第1に、IPSec(IP Security)、VPN (Virtual Private Network)、インラインファイアウォール、および侵入防止システムなど、多くのセキュリティ装置の機能を1つのデバイスに統合している。もちろんパケット転送用の高性能ルータ、あるいはスイッチとしても使用できる。

「私たちは複数のセキュリティ機能やネットワークサービス機能を1つのデバイスに統合することにより、複雑な管理を簡略化し、TCO(所有コスト総額)を削減することに成功しています」とシスコのIPサービス&セキュリティ担当マネージャーであるマーク・デニーは語っている。

このTCO削減の効果は、設備投資費そのものの削減、それに関連する複数のネットワーク機能を実現す

るのに必要な機器構成費の削減、そして年間のサポート費およびソフトウェア更新(Cisco SMARTnetに含まれる)費などの削減によってもたらされる。「Cisco IOS Softwareを採用すれば、顧客は自社ネットワーク内にセキュリティ機能を組み込む場所を決定するだけでよいのです。後はソフトウェアで設定するだけで、そのネットワークセグメントにあるデバイスにCisco IOS Softwareの最新技術を実装できます」とデニーは強調する。

現在では、無線LANユーザーに企業ネットワークへのアクセスを提供する無線ベースのレイヤ2ハブとなるCisco Aironet1100シリーズ無線LANアクセスポイントでも、Cisco IOS Softwareの多くのIOS機能をサポートするようになった。無線LANアクセスポイントは企業ネットワークへの入口となる。そのため、シスコでは卓越した技術で賞を獲得したCisco Wireless Security

SuiteをすべてのCisco Aironet製品に搭載している(21ページの『無線LANの安全を確保しよう!』を参照)。

これらの製品は無線通信機能、アクセス制御のための相互認証機能、エンド・ツー・エンドのトラフィック優先順位を決めるQoS(Quality of Service)機能、およびその他の機能を分離するためのVLAN(virtual LAN)機能もサポートしている。

シスコのルータおよびスイッチへのセキュリティ機能の統合は、機能を一体化するだけにとどまらない。「Cisco IOSにおけるセキュリティは、シスコプラットフォームにおけるネットワーク制御、データ、およびマネジメントプレーンなど全般に及んでおり、QoS、VoIP(Voice over IP)、マルチキャスト、ルーティング・プロトコルなどのIPサービスとの統合がスムーズに行えるよう配慮されています」とシスコのインターネットテクノロジー部門マーケティングプログラム・マネージャーであるアナンド・ヌギハリは語っている。

組み合わせにより、さらに威力を発揮

Cisco IOS Softwareベースのセキュリティ機能を実装する最大のメリット。Cisco IOSの豊富なIPサービスやネットワークサービス機能とセキュリティおよびVPN機能を併用することにより、管理性を高めたコストパフォーマンスの高いセキュリティソリューション構築が可能となる。

たとえば、GRE(Generic Routing Encapsulation)をIPSecと併用することにより、安全なルーティングとマルチキャストの双方を提供することができる。また、DHCP(Dynamic Host Control Protocol)とARP(Address Resolution Protocol)を併用することにより、ハッカーがライブセッションを乗っ取る可能性を軽減できる(最近追加されたCisco IOSセキュリティ機能は、cisco.com/go/packet/iossecurityのPacket Onlineで参照可能)。

また、最近発表されたCisco IOSの3つの機能、DMVPN(Dynamic Multipoint VPN)、IPSec上のLLQ(Low-Latency Queuing)、およびStateful IPSecフェイルオーバーを組み合わせることによりVPNネットワーク全体で遅延やジッタを減らすことができる。

さらに、障害回復力を向上させ、展開の大部分を自動化することにより運用スタッフの負担を軽減することができる。

DMVPN

Cisco IOS Release 12.3(13)Tから追加されたDMVPN(Dynamic Multipoint VPN)機能により、ユーザーはGREトンネル機能、IPSec暗号機能、およびNHRP(Next Hop Resolution Protocol)を組み合わせることで、さまざまな規模のIPSec VPNを拡張できるようになる。DMVPNはスポークサイト間の接続を自動化し、ネットワークのトラフィック・パターンに基づいて動的に接続を確立することにより、メッシュ型VPN展開をしやすいとする。このDMVPN機能はハブサイトを経由していたコミュニケーションをスポーク間に任せて遅延やジッタを軽減する上で非常に優れている。この新しいIOS機能は、マルチポイントGREを使うことにより音声およびビデオのマルチキャスト・トラフィックもサポートする。

IPSecでもQoSプレクラシフィケーションやLLQを

暗号化されたリンク上でリアルタイムの音声(およびビデオ)を流すには注意が必要だ。これは、暗号化がQoSマーキングを含むデータパケットとアドレスを隠すためである。

シスコではこの問題を克服するため、Cisco IOS Software内のQoSプレクラシフィケーションとLLQの2機能をIPSecと併用し、暗号化されたセッション全体で必ず音声最優先されるようにしている。

パケットのプレクラシフィケーションは、DSCP(Differentiated Services Code Point)とIP Precedenceの優先順位マーキングが隠されるのを防ぐため、最初に行われる。QoSマーキングは、暗号化の前に送信ルータのアウトバウンド・インタフェースで適用される。送信前にこのマーキングが新しい外部のIPSecトンネルヘッダにコピーされる。

プレクラシフィケーション機能は、IOS Release 12.1(5)Tから使えるようになった機能だが、現在ではCisco IOS Release 12.2(8)Tを実行する、ほとんどのCisco IOS VPNルータで利用できる。通常、プレクラ

シフィケーションは単体でもVoIPに対して十分なIPSec QoSを提供する。しかし、すべての基盤技術を包括するため、最近ではIPSecでもLLQを認識するようになった。Cisco LLQは、プライオリティ・キュー、すなわちシスコルータ内に音声トラフィック専用の“追い越し車線”を提供する。

「LLQを認識するIPSecは、暗号化/復号化が行われる場所の輻輳が原因で生じる音声遅延を回避する働きをします。したがって、優先順位の高いリアルタイムのトラフィックを認識するIPSec能力がなければ、IPSecルータの1つで輻輳が起こった場合、優先順位が高いパケットが内部ルータのキューで優遇措置を受けることができなくなってしまう」とシスコのIOS IPSec製品マネージャーであるミカ・ルーコラは説明している。

IPSecステートフルフェイルオーバー

この機能は、2つのIPSecエンドポイント間のVPNセッションに高速で拡張性のあるネットワーク障害回復能力を提供し、中央サイトのプライマリVPNルータへの接続が切れている間も途切れることなくVPNセッションを保持する。

IPSecステートフルフェイルオーバーは、HSRP(Hot Standby Router Protocol)を使い、アクティブルータとバックアップルータ間のIPSecセッションのステート情報を維持している。IPSecセッションのステート情報を維持することにより、1秒未満のフェイルオーバー時間での切り替えをリモートVPNルータに対してトランスペアレントに提供する。

コントロールプレーンのセキュリティ

ルータまたはスイッチのコントロールプレーンとは、ルーティング情報のシグナリング、保存、アップデート、およびフォワーディングパスの設定を担当する一連のプロセスのことを指している。Cisco IOS Softwareはこれらの機能の安全を確保する能力を持っている。たとえば、BGP(Border Gateway Protocol)やIS-IS (Intermediate System-to-Intermediate System)などのルーティング・プロトコルは、ピアから受信する情報が本当にそのピアを発信元としているかをMD5 (Message Digest Algorithm 5)で検証することによ

て保護されている。

その他にもコントロールプレーンのセキュリティ機能は、安全度の高いVPN設定や構成を実現する。たとえばIPSecは、安全に暗号化されたトンネルを作成するためにIKE(Internet Key Exchange)を利用している。したがって、Cisco IOS Release 11.3(3)Tおよびそれ以降のソフトウェアでは、IKEを利用することによって、ピアルータにIPSecセキュリティ・パラメータをマニュアル操作で指定する必要がない。さらに、IPSecセッション中であっても暗号化キーが変更できるようになっており、ピアの認証を動的に行うことができる。

データプレーンのセキュリティ

Cisco IOS Softwareには、データのプライバシーを保護するため、企業のセキュリティポリシーに従ったパケットのフィルタリング、不正コードに対するトラフィックフローの監視、およびトンネリングを使ったトラフィックの分離といった諸機能が統合されている。

インラインファイアウォール・フィルタリング

統合されたCisco IOS Firewall Feature Setは、各IPパケットのコンポーネントを検査し、その有効性を確認するために、すべてのファイアウォール・インタフェース上にある個々の接続を追跡する機能を有している。これは、パケットの内容をアプリケーション層まで認識し、関連するファイアウォールルールに従い、それぞれのパケットに対してセキュリティアクションを実行する。

このファイアウォール機能は、TCP/IPパケットを検査し、TCPハンドシェイクが適切な順序で行われているかどうかを判断する。

これにより、仮にクラッカーがハンドシェイクを開始するパケットを数千ユーザーがTCPセッションを開始したように見せかけて送信したとしても、ファイアウォールはこのような攻撃を撃退できる。対策が取られていないとこの攻撃はTCPコントロールブロックをクラッシュする原因となる。

侵入防止(Intrusion Protection)

この機能は、既知の不正シグニチャ、すなわちパケ

ット内の数バイトのコードを探すことにより、悪意のある発信元からのネットワーク攻撃を防ぐものである。不正シグニチャが検出された場合、ネクストホップルータにその発信元からの接続を拒否するよう自動的に伝える。

Cisco IOS Softwareは101のシグニチャを認識する能力を備えているが、そのうち42個は、最近Cisco IOS Release 12.2(13)YJに追加されたものである。また、この侵入防止機能はCisco IOSファイアウォールとしてバンドルされ、Cisco IOS Release 12.0(5)Tまたはそれ以降のソフトウェアで利用することができる。

トンネリング

Cisco IOS Softwareは、公共のインターネットで使用可能なさまざまなトンネリング技術をサポートしている。たとえばGRE機能は、シスコのリモートルータ間にポイント・ツー・ポイントの仮想リンクを作るため、IPトンネル内で多種多様なプロトコル・パケットをカプセル化するものである。

GREおよび関連機能であるL2TP(Layer 2 トンネリング Protocol)では、L2TPがユーザー認証を要求するが、暗号化を行うわけではない。その代わりに、これらの体系により、公共のインターネット全体にルータ・ホップでフォワーディングの決定をしなくてもよい貫通(cut-through)トンネルが作られる。GREおよびL2TPのサイトは、NAT(Network Address Translation)を避けているため、ネットワークエッジにおけるパケット処理を増強することができる。

ルータ用はマルチキャスト・ルーティング・プロトコルがIPSecトンネルを通過できるよう、GREをIPSecと併用するのが一般的である。IPSecおよびIKEに最近追加された新しいAES(Advanced Encryption Standard)暗号化手法としてはAES-128、AES-192、およびAES-256という3種類がある。

さらに、Cisco IOS Software Release 12.2(13)Tでは、Cisco IOSがDES(Data Encryption Standard)および3DES(Triple DES)ciphersに加え、AESをサポートしている。したがって、公共のインターネットで送られるトラフィックに対しては、できる限りIPSecを使うよう推奨したい。

WANのエッジルータおよびアクセス回線に対する投資効果を最大限に高めるためには、スプリット・トンネリングを利用することができる。この構成では、IPSecトンネルがブランチオフィスからのVPNトラフィックだけを共通のアクセスリンクを通じて安全に転送し、平文(クリアテキスト)のインターネットトラフィックは直接インターネットに送られる。スプリット・トンネリングは、トラフィックフローが中央サイトを通過するときにブランチオフィスで発生する余分なホップや遅延を防いでくれる。

「ただし、スプリット・トンネリングを展開するには、エッジにファイアウォール機能と侵入検知機能を備えておくことが重要です。そうでない場合、インターネットからの侵入者がブランチサイトを乗っ取り、ブランチ経由で本社へ侵入することもあり得るからです」とルーコラは助言している。

なお、LAN内でトラフィックの分離が必要となった場合には、Cisco IOS Softwareを使うことで、IEEE 802.1Q、すなわちイーサネットのレイヤ2で実行されるVLANトンネルを作成することができる。この機能はシスコのルータ、スイッチ、および無線LANのアクセスポイントで実行する。IPSecは、社内でも非常に機密性が高い通信を保護するためにVLANと併用してイーサネットLAN上のトラフィックを暗号化するために使われることもある。

また、メトロネットワークおよびWANでレイヤ2の高速LAN拡張サービスを提供したいサービスプロバイダに対しては、802.1Qを強化した、いわゆる802.1Qトンネリングを使うことができる。「Cisco 802.1Qトンネリングは、サービスプロバイダのネットワークエッジにあるスイッチ内で、顧客のトラフィックに対して臨時的802.1Qタグを追加します」とシスコのメトロイーサネット・グループのテクニカルマーケティングエンジニアであるチアラ・リゲールは説明している。「このタグは、サービスプロバイダのネットワーク内で個々のVLANに対して固有のVLAN ID番号を与えることにより、すべての顧客のVLANを分離します」

ご存知でしたか？

自分の組織を守るために必要なのは、Cisco IOS Softwareに組み込まれたステートフルインラインファイアウォール機能と侵入防止機能をアクティブにするだけ。具体的には下記の機能を実行する。

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

ユーザー毎のアクセス制御ポリシー

ユーザー毎の認証と認可

サポートしている幅広いアプリケーションとプロトコルの検査

悪意のあるJavaアプレット攻撃、ICMP(Internet Control Message Protocol)パケット、SIP、H.323v2などのブロックならびにN2H2およびWebsense URLフィルタリング

信用できる送信元から信頼できるルーティング情報を確実に受信するためにピアルータを認証

101の侵入検知シグニチャを認識、阻止、および対処

重大度(Severity): 40の情報シグニチャ、61の攻撃シグニチャ

複合性(Complexity): 74の単パケット(atomic)シグニチャ、27の複合パケット(compound)シグニチャ

DoS(サービス拒絶: Denial-of-Service)攻撃、またはアプリケーション別、機能別を基礎に構成可能で事前に定義されたその他の状態に関するリアルタイムのアラート送信

マネージメントプレーンのセキュリティ

Cisco IOS Softwareにおける一連のマルチファセット化された機能は、ID管理および認証管理を含むマネージメントプレーンのセキュリティの分野に入るものである。たとえば、Cisco IOS SoftwareはRADIUS(Remote Access Dial-In User Service)やTACACs+などの認証、認可、およびアカウントング(AAA: Authentication, Authorization, and Accounting)体系をサポートする一方、きめ細かいアクセス制御を行うために、16レベルに及ぶユーザー特権をサポートしている。「Cisco IOS Softwareを使ってネットワーク管理を行えば、16の特権レベルの中で使えるコマンドを構成し、ユーザー毎の管理を基本としたアクセス認証や、コマンド毎の認可も可能になります」とデニーは助言している。

管理の観点から見ると、Cisco IOS Release 12.0(5)Sに導入されたリモートアクセスルータの構成法であるSSH(Secure Shell)は、Telnetセッション全体にわたって、リモートコンソールとネットワークルータ間のパスワードを含むすべてのトラフィックを暗号化する。SSHはクリアテキストのトラフィックを全く送らないため、ネットワーク管理者は、一般のインターネット利用

者側にリモートアクセス・セッションを覗かれることなくデバイスの管理を行うことができる。

たとえば、CiscoWorks VMS(VPN/Security Management)はVPNトンネルを安全に構成するため、多くのルータ上、あるいは公共のネットワーク全体にわたってSSHを使っている。

詳しい情報

IPSecセキュリティの構成 (Configuring IPSec security) :

cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca7b1.html

Cisco IOSのセキュリティ (Cisco IOS security) :

cisco.com/warp/public/732/Tech/security