

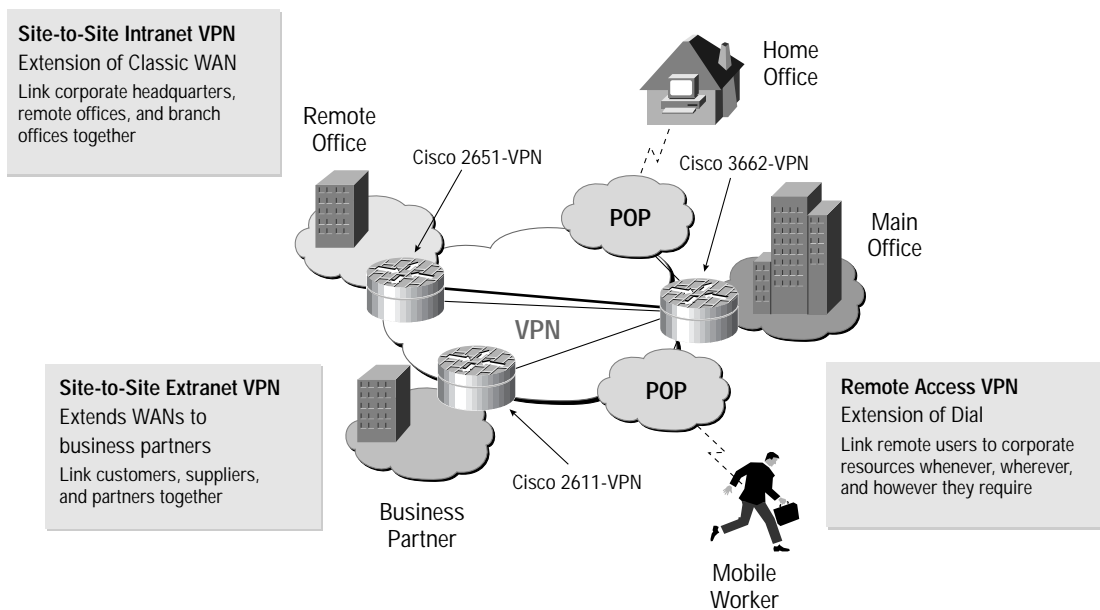
Cisco 2600/3600 VPN ルータバンドル

概要

シスコでは、Cisco 2600および3600モジュラ型マルチサービスルータプラットフォームをベースとする4つの新しいVPNルータバンドルを提供しています。これらのバンドル製品によって、1つの部品番号だけで必要な全VPNコンポーネントを装備したCisco VPNルータを発注していただくことができ、VPN（仮想プライベートネットワーク）を実現するための発注が簡単になります。しかも、各コンポーネントを別個に発注するより低価格になります。また、それぞれのVPNバンドルと一緒に他のWANモジュールも発注していただけます。VPNバンドルには56 DES（Data Encryption Standard）バージョンと3DESバージョンの両方が用意されていますが、必要であれば56DESバンドルを3DESライセンスに更新できます。

これらのバンドルは、VPN、侵入探知システム（IDS）、ファイアウォールといった実績あるセキュリティ機能を展開する能力に加え、高速インターネットアクセス、そしてエクストラネットやDMZ（非武装地帯）を構築するための機能を提供します。したがって、イントラネット、エクストラネット、およびリモートアクセスVPNの展開がサポートされています（図1参照）。ただしリモートアクセスVPNを展開する場合は、バンドルとともにCisco Secure VPN Client 1.1を使用する必要があります。年内には、シスコが最近リリースした新しい無料のCisco VPN Client 3.0がバンドルによってサポートされる予定です。

図1：VPNアプリケーション





機能概要

Cisco 2611-VPN ルータバンドル

- 1つのパーツ番号だけで簡単に発注することが可能
- 2つのWANインタフェースカード (WIC) スロットと1つのNMスロットを装着したデュアル10Mbpsイーサネットルータ
- フラッシュと DRAM の両方のメモリをアップグレード: 16-MBフラッシュおよび64-MB DRAM
- Cisco IOSソフトウェア: Cisco IOS IP/FW/IDS PLUS IPsec 56または3 DES
- VPNモジュール: AIM-VPN/BP(基本パフォーマンス)

Cisco 2651-VPN ルータバンドル

- 1つのパーツ番号だけで簡単に発注することが可能
- 2つのWICスロットと1つのNMスロットを装備した高性能デュアル10/100Mbpsイーサネットルータ
- フラッシュとDRAM両方のメモリアップグレード: 16-MBフラッシュおよび64-MB DRAM
- Cisco IOSソフトウェア: Cisco IOS IP/FW/IDS PLUS IPsec 56または3 DES
- VPNモジュール: AIM-VPN/ER(拡張パフォーマンス)

Cisco 3640-VPN ルータバンドル

- 1つのパーツ番号だけで簡単に発注することが可能
- Cisco 3640 4スロットモジュラ型ルータ
- 2つのイーサネットおよび2つのWANカードスロットを装備したネットワークモジュール
- フラッシュと DRAM 両方のメモリアップグレード: 16-MBフラッシュおよび64-MB DRAM
- Cisco IOSソフトウェア: Cisco IOS IP/FW/IDS PLUS IPsec 56または3 DES
- VPNモジュール: NM-VPN/MP(ミッドパフォーマンス)

Cisco 3662-VPN ルータバンドル

- 1つのパーツ番号だけで簡単に発注することが可能
- デュアル10/100MbpsイーサネットCisco 3662 6スロットモジュラ型ルータ(AC電源)
- フラッシュとDRAM両方のメモリアップグレード: 32-MBフラッシュおよび64-MB DRAM
- Cisco IOSソフトウェア: Cisco IOS IP/FW/IDS PLUS IPsec 56または3 DES
- VPNモジュール: AIM-VPN/HR(ハイパフォーマンス)

VPNバンドルの機能と利点

VPNによって企業は、WANコストの大幅削減、グローバルな接続性の向上、および信頼性の改善といった利点を享受しながら、セキュアなエクストラネット通信などの機能を実現できます。リモートダイヤル、インターネット、イントラネット、およびエクストラネットアクセスをすべてインターネットへの単一のWAN接続上に整理統合することができます。

Cisco 2600/3600 シリーズルータ

Cisco 2600/3600シリーズモジュラ型マルチサービスアクセスルータは、サイト間VPNに最適な製品です。これらのルータは、マルチサービスVPNアプリケーションのためのルーティング、ファイアウォール、ダイヤル、パケット音声ゲートウェイ、およびVPN機能の充実した統合パッケージを提供します。Cisco 2600/3600シリーズはVPNモジュールとともに、スモールオフィスを他のリモートオフィス、セントラルオフィスのイントラネット、またはパートナーエクストラネットに接続するための理想的なIPsec/VPNソリューションを提供します。

VPN モジュール

VPNルータバンドルに含まれているVPNモジュールは、複数の全二重T1/E1シリアル接続に適切な速度でDESおよび3DESアルゴリズムを使用してデータを暗号化します。VPN暗号化モジュールは、暗号化、ハッシング、キー交換、セキュリティアソシエーションの格納といった各種のIPsec関連タスクを処理します。このため、メインプロセッサやメモリは、他のルータ、音声、およびファイアウォール機能を実行することが可能になります。

侵入探知機能を持つ Cisco IOS ファイアウォール

バンドル製品に含まれているCisco IOS Firewall with Intrusion Detection System (FW/IDS) は、ネットワーク攻撃からLANを保護します。CBAC(コンテキストベースのアクセス制御)は、アプリケーションごとに動的またはステートフルなフィルタリング機能を提供し、セッションがアクティブな期間だけ正当なトラフィックがLANに到達できるようにします。CBAC機能は、効果的なファイアウォール機能の必須要素です。Cisco IOS Firewallは、他にも、Javaブロッキング、サービス拒否(DoS)の検出と阻止、監査追跡、およびリアルタイムの警告といった重要な機能をサポートしています。またCisco IOS Firewallは、AAA(Authentication, Authorization, and Accounting)機能を提供して、リモートユーザの認証、特定ネットワークリソースに対するアクセスの許可、およびこのアクティビティのアカウントングを行います。Cisco IOS FW/IDSは、シグネチャを使って最も一般的な59の攻撃を識別し、ネットワークトラフィックの悪用パターンを検出します。新しいCisco IOS Firewallリリースに含まれている侵入探知シグネチャは、侵入探知シグネチャの広範なクロスセッションから選択されたものです。シグネチャは、重大なセキュリティ侵害や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示します。



トンネリングと暗号化

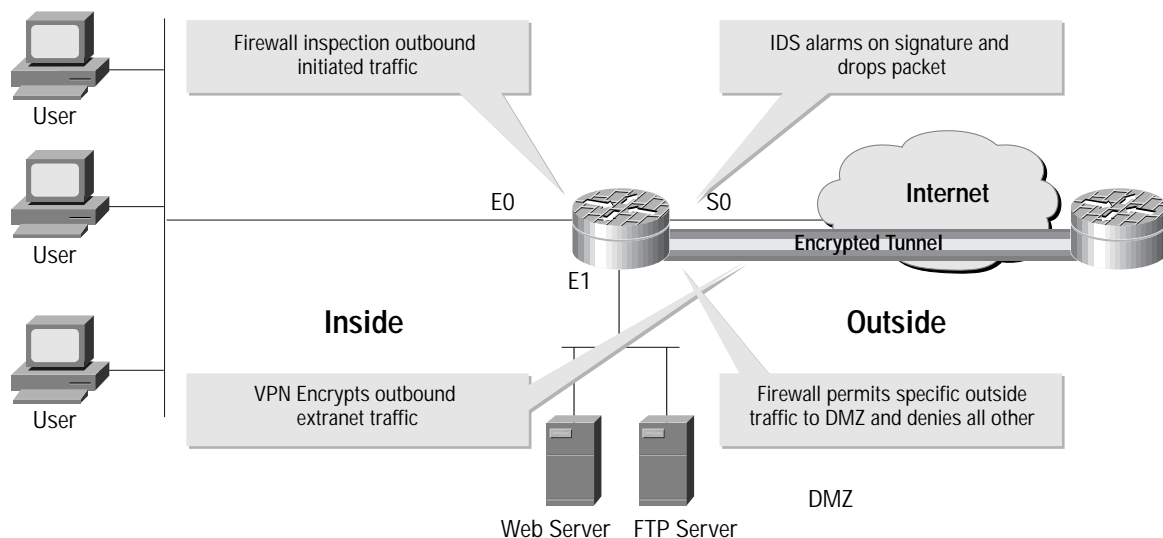
IPSecは以下のネットワークセキュリティサービスを提供します。

- プライバシー --- IPSecは、パケットがネットワーク上に送信される前にそれらを暗号化することができます。
- 完全性 --- IPSecは宛先ピアでパケットを認証して、送信中にデータが改ざんされていないことを保証します。
- 認証 --- IPSecピアは、IPSecで保護される全パケットの送信元を認証します。
- アンチリプレイ対策 --- IPSecはパケットのキャプチャとリプレイを阻止して、サービス拒否 (DoS) 攻撃から保護します。
- 暗号化トンネル --- 許可されていないエンティティによるデータの傍受と表示を阻止し、マルチプロトコルカプセル化を実行します。

Cisco IOS IPSec は、DES (56ビット) および3DES (168ビット) の両方をサポートします。GRE (Generic Routing Encapsulation) with IPSecはシスコ独自のソリューションで、これによってルーティング更新情報をVPNを通して送信できるようになるため、IPSecのみのソリューションよりネットワークの回復力が向上します。GREトンネルはフェイルオーバーメカニズムのほかに、マルチキャスト/ブロードキャストパケットおよび非IPプロトコルの暗号化機能を提供します。そのため、GRE with IPSecを使用することにより、シスコのサイト間VPNソリューションでAppletalkおよびNovell IPXをサポートできます。

Cisco IOSソフトウェアの機能であるトンネルエンドポイントディスカバリは、トンネル接続がネットワークセキュリティポリシーにしたがって動的に自己構成できるようにします。VPNの各ポイントツーポイントトンネルを手動で構成する必要性が軽減されるため、フルメッシュ型のサイト間VPN環境におけるクリティカルなトンネルのスケラビリティとサバイバル能力が高まります。

図2: Cisco VPN、ファイアウォール、およびIDSルータ



管理

ConfigMaker

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フェース) で、ユーザはコンソールポートまたはTelnetを使って、シンプルなIPSec構成を設定できます。ConfigMakerは、登録ユーザであれば、Cisco Software Center (<http://www.cisco.com>) から無料でダウンロードできます。ConfigMakerは、Cisco CLI (コマンド行インタフェース) をほとんど使ったことなく、3~10台のデバイスによるシンプルなVPNの展開を計画しているユーザを対象としています。

Cisco Secure Policy Manager

Cisco Secure 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管理製品の最新バージョンで、これによってお客様は中央ロケーションからネットワーク全体のセキュリティポリシーを定義、配布、実施、監査することができます。CSPMは、IPSecベースのVPNといった複雑なネットワークセキュリティエレメントの管理タスクを簡素化します。CSPMはCisco VPNルータの管理に加え、Cisco PIX FirewallおよびCisco IDSを管理することができます。CSPMによって管理者は、1つの中央ツールからハイレベルのセキュリティポリシーをビジュアルに定義することができるため、エンタープライズカスタマーのCisco IOS FirewallおよびCisco IOS IPSec VPNの展開が大幅に簡素化されます。CiscoWorks2000 VPN/VMS (Security Management Solution) は、包括的なブラウザベースのアプリケーションで、VPN接続を適切にセキュリティ保護および運用する際の管理上の独自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に加え、CSPMの簡易バージョン (10台のデバイス用) が含まれています。VMSは、IOSリリース12.2(4)Tが搭載された2600/3600 VPNバンドルをサポートします。



VPN Solution Center 2.0

Cisco VPN Solutions Center (VPNSC) リリース 2.0 により、プロバイダーはIPSecおよびMPLSベースのIP VPNの両方を1つのツールで管理することが可能となりました。さらにVPNSCは、サービスプロバイダーがVPNサービスを効果的に計画、プロビジョニング、運営、請求処理するためのサービス管理ソリューションを提供します。

サービスプロバイダーがWANスイッチ、ルータ、ファイアウォール、VPNコンセントレータ、そしてCisco IOSソフトウェアを含むVPNを構築する際は、ネットワークインフラストラクチャ上でこれらのデバイスをシームレスに管理して顧客にSLA(サービスレベルアグリーメント)を提供する必要があります。また、ビジネスカスタマーがそのネットワークサービスやアプリケーションへのアクセスを個別に設定できるようにする必要もあります。多くの企業が要求

しているアウトソース型のVPNサービスをサービスプロバイダーが迅速に展開できるように、VPNSCはコスト効果の優れた初のキャリアクラスのVPNサービス管理機能を提供します。このポートフォリオは、スモールオフィスから本社までの全サイトのプラットフォーム上に、強靱なIPSec VPNサービスとCisco IOSソフトウェアの全機能を結合します。VPNSC 2.0は、MPLS 顧客構内機器(CPE)およびIPSecデバイスの両方としてCisco 2600シリーズルータをサポートします。このため、プロバイダーは、IPSecおよびMPLSベースのIP VPNの両方を管理することができます。また、VPNSC 2.0は、MPLS CPEおよびIPSecデバイスとしてCisco 3600シリーズルータをサポートします。さらに、Cisco 3640および3662は、VPNSC 2.0によってプロバイダーエッジ(PE)デバイスとしてサポートされます。

技術情報

バンドル	Firewall with IDS	マルチプロトコルの GRE および IPsec サポート	MPLS VPN	VPN QoS	最大トンネル数	3DES Mbps パケット	3DES Mbps パケット
C2611-VPN		IP/IPX/Appletalk	CPE		300	2	10
C2651-VPN		IP/IPX/Appletalk	CPE		800	4	14
C3640-VPN		IP/IPX/Appletalk	PE		1000	5	18
C3662-VPN		IP/IPX/Appletalk	PE		1800	9	40

注：3DES 速度は、バックツーバックで接続されたファーストイーサネットルータのテスト結果に基づいています。WAN 速度、メモリ、および Cisco IOS で実行されているアプリケーションによって、この数字は変化します。

発注情報

部品番号	説明	オプション WIC の利用
56DESバンドル		
C2611-2E/VPN/K8	2611 VPNルータ、IPSec56DES、デュアル10 E、VPNカード、64DRAM	
C2651-2FE/VPN/K8	2651 VPNルータ、IPSec56DES、デュアル10/100 FE、VPNカード、64DRAM	
C3640-2FE/VPN/K8	3640 VPNルータ、IPSec56DES、デュアル10/100 FE、VPNカード、2×WAN	
C3662-2FE/VPN/K8	3662 VPNルータ、IPSec56DES、デュアル10/100 FE、VPNカード、64DRAM	
3DESバンドル		
C2611-2E/VPN/K9	2611 VPNルータ、IPSec3DES、デュアル10 E、VPNカード、64DRAM	
C2651-2FE/VPN/K9	2651 VPNルータ、IPSec3DES、デュアル10/100 FE、VPNカード、64DRAM	
C3640-2FE/VPN/K9	3640 VPNルータ、IPSec3DES、デュアル10/100 FE、VPNカード、2×WAN	
C3662-2FE/VPN/K9	3662 VPNルータ、IPSec3DES、デュアル10/100 FE、VPNカード、64DRAM	

注：K9 およびK8 は、含まれている DESまたは 3DES ライセンスを示します。

まとめ

Cisco 2600および3600 VPNバンドルによって、エンタープライズやサービスプロバイダーはCisco 2600/3600ルータをVPNとして簡単に展開し、バンドルが提供する新しいパワフルなVPNサービスを利用することができます。

Cisco 2600および3600バンドルはシスコのCisco 1700、7100、および7200 VPNバンドルを補完する理想的な製品で、機能と価格の点でVPN購入者の選択肢を拡大します。

©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