

Cisco VPN ルータ

サイト間 VPN ソリューションの標準を確立



サイト間 VPN (仮想プライベート ネットワーク) は、専用回線、フレームリレー、または ATM を使用する既存の私設ネットワークを置換または拡張して、リモート/ブランチオフィスと中央サイトをより柔軟に、かつ優れた費用効果で接続する WAN インフラストラクチャです。複数サイトの相互接続には、多様なトラフィックタイプへの適応、ネットワークの全デバイスの到達可能性と信頼性の保証、各地に分散した非常に多くのデバイスを管理するためのフレームワークの提供のほか、VPN 集約ハブサイトのスケーラビリティといった固有の要件があります。現在市販されている多くの VPN デバイスは、リモート アクセス VPN アプリケーションが前提になっており、こうしたサイト間 VPN に固有の要件には対応していません。

Cisco IOS®ソフトウェアを利用する Cisco VPN ルータは、市場で最高のワイドエリア ネットワーキング サービスを提供して、サイト間 VPN ソリューションの標準となっています。Cisco VPN ルータは、次のようなサイト間 VPN にとって重要な機能を提供します。

• **多様なネットワーク環境をサポート** --- IPSec (IP Security) は、ユニキャストの IP 専用プロトコルです。Cisco IOS ソフトウェア機能を利用する Cisco VPN ルータは、マルチキャストおよびマルチプロトコルトラフィック、ならびに VPN 上のルーティングにも適応して、最も多様な VPN 環境に対応する柔軟なソリューションを提供します。

- 遅延に影響されやすいトラフィックを高い信頼性でタイムリーに配送 --- Cisco VPN ルータの帯域幅管理機能によって、アプリケーションレイヤまでトラフィックを優先付けできるため、単なる TCP ポート番号ではなくアプリケーションタイプによって差別化された QoS (Quality of Service) ポリシーを促進できます。この結果、VPN 上で実行される業務上重要なアプリケーションの伝送の信頼性と応答時間が改善されます。
- サイト間に固有の VPN スケーラビリティ --- シスコでは専用ヘッドエンド VPN ルータから、WAN インターフェイスとステートフルファイアウォールを完備したシングルボックスのリモートオフィス VPN ルータソリューションに至るまで、最も広範な VPN デバイスを取り揃えています。キャリアが供給する DSL およびケーブル デバイスの背後で使用する費用効果の高いオーバーレイ ブロードバンド VPN デバイスも、Cisco VPN ルータ ポートフォリオに不可欠な要素です。
- 包括的な VPN 機能 --- Cisco VPN ルータは、IPSec データ暗号化、トンネリング、PKI (公開キー インフラストラクチャ) のための広範な認証局のサポートといった VPN の鍵を握る全機能に加え、証明書自動登録、VPN 復元力、ステートフル ファイアウォール、侵入検知、およびサービスレベル検証といった拡張機能をサポートしています。
- すべてを完備したサイト間 VPN 管理フレームワーク --- 複数サイト上の複数 VPN デバイスを管理するには、堅牢な VPN 構成管理やモニタリング機能だけでなく、デバイスインベントリやソフトウェアバージョン管理機能も必要とされます。シスコでは Cisco Secure Policy Manager や VPN Monitor といったアプリケーションによって包括的な VPN 構成およびモニタリングを提供するだけでなく、Cisco Works2000 によってインフラストラクチャ管理機能も提供します。



表 1: Cisco VPN ルータのポートフォリオ

サイト	モデル	VPN パフォーマンス	トンネル数	内蔵インターフェイス	モジュラ インターフェイス オプション
統合ブロードバンド SOHO	Cisco 800	384 kbps	50 未満	10BaseT + DSL または 10BaseT + ISDN	なし
	Cisco 900	6 Mbps	50 未満	10BaseT + ケーブル	
オーバーレイブロードバンド SOHO	Cisco 800	384 kbps	50 未満	10BaseT × 2	なし
	Cisco 1700	3 Mbps	100	10BaseT × 2	
リモートオフィス	Cisco 1700	3 Mbps	100	10BaseT	シリアル、DSL、ISDN、イーサネット、音声
	Cisco 2600	14 Mbps	800	10/100BaseT × 1 または 2	シリアル、DSL、ATM、ISDN、E/FE、音声
ブランチオフィス	Cisco 2600	14 Mbps	800	10/100BaseT × 1 または 2	シリアル、DSL、ATM、ISDN、E/FE、音声
	Cisco 3600	30 Mbps	2000	なし、あるいは 10/100BaseT × 1 または 2	シリアル、DSL、ATM、ISDN、E/FE、音声
セントラル ハブ サイト	Cisco 3600	30 Mbps	2000	なし、あるいは 10/100BaseT × 1 または 2	シリアル、DSL、ATM、ISDN、E/FE、音声
	Cisco 7100	140 Mbps	3000	10BaseT × 2	シリアル、POS、ATM、ISDN、E/FE/GE
	Cisco 7200	145 Mbps	5000	10BaseT × 2	シリアル、POS、ATM、ISDN、E/FE/GE、音声

「VPN パフォーマンス」は、1400 バイト パケット上で IPsec 3DES (Triple Data Encryption Standard) HMAC-SHA1 を使用して判定しています。

サイト間 VPN の利点とアプリケーション

WAN コストを削減して WAN の柔軟性を向上

インターネットを使って伝送する VPN は、繰り返し発生する WAN コストをフレームリレーなどの従来の WAN テクノロジーと比較して 50% 以上も削減します。またフレームリレーとは異なり、VPN は新しいロケーションや「エクストラネット」を利用するビジネス パートナーに簡単かつ迅速に拡張できます。

VPN によって収益を伸ばす新しいアプリケーションを提供

VPN により、DSL などの費用効果の優れた高速リンクをセキュアに使用して、インスタント オンライン カタログ / 注文のような収益を生み出すアプリケーションやオンライン トレーニングといった能率的なツールを提供できます。

データとネットワークのセキュリティを改善

フレームリレー、専用回線、または ATM を使用する従来の WAN は、トラフィックを隔離するだけで、伝送上のセキュリティは提供しません。VPN は WAN 上で伝送されるトラフィックを暗号化および認証して、セキュリティリスクのあるネットワーク接続された世界に本当の意味でのネットワーク セキュリティを提供します。

機能

VPN トンネリング

- IPsec (RFC 2401 ~ 2411, 2451)
- GRE (RFC 1701 ~ 1702)
- L2TP (RFC 2661)
- PPTP (RFC 2637)

暗号化

- ESP DES および 3DES (RFC 2406, 2451)
- MPPE RC4 (40/128 ビット)

認証

- X.509 デジタル認証 (RSA シグニチャ)
- 共有秘密情報
- Simple Certificate Enrollment Protocol
- RADIUS (RFC 2138)
- TACACS+
- CHAP/PAP (RFC 1994)

統合性

- HMAC-MD5 & HMAC-SHA-1 (RFC 2403 ~ 2404)

キー管理

- IKE インターネット キー交換 (RFC 2407~ 2409)
- IKE-XAUTH
- IKE-CFG-MODE

IP 圧縮

- IPPCP-LZS (RFC 2401 ~ 2402)

認証局のサポート

- Entrust
- Verisign
- Microsoft
- iPlanet
- Baltimore Technologies

帯域幅管理 / QoS

- NBAR (Network-Based Application Recognition) コンテンツ対応分類
- クラス / フローベースの WFQ (均等化キューイング)
- GTS (汎用トラフィックシェーピング)
- レート制限 CAR [専用アクセスレート]
- 輻輳回避 WRED [重み付けランダム早期検出]

復元力

- HSRP (ホットスタンバイ ルータ プロトコル)
- IKE キーブアライブ
- IPSec 上のルーティング

管理オプション

- Cisco Secure Policy Manager (CSPM)
- VPN Device Manager
- VPN Monitor
- CiscoWorks 2000
- SSH (Secure Shell) または Kerberized Telnet を使ったセキュアなコマンド行インターフェイス

ルーティング プロトコル

- BGP4
- RIP/RIP2
- OSPF
- EIGRP/IGRP
- NHRP
- IS-IS

セキュリティ

- CBAC (コンテキストベース アクセス制御) ステートフルファイアウォール
- Java ブロッキング
- アクティブ監査侵入検知
- サービス拒絶の検知と防止

セキュリティ認証

- FIPS-140-1, level 2
- ICSA IPsec v1.0

©2002 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