概要：セキュア接続

この章の構成

このマニュアルについて

『*Cisco IOS セキュリティ コンフィギュレーション ガイド：セキュア接続*』では、Internet Key Exchange（IKE; インターネット キー エクスチェンジ）、Public Key Infrastructure（PKI; 公開鍵インフラストラクチャ）、および Virtual Private Network（VPN; バーチャル プライベート ネットワーク）の各テクノロジーを備えた IP security（IPsec; IP セキュリティ）を使用して、ネットワークを管理およびその安全を確保し、また通信の品質を落とさずに、音声アプリケーションおよびクライアント サーバ アプリケーションなど、複雑でミッション クリティカルなトラフィックを高い信頼性で転送する方法について説明します。

この章では、次の内容を説明します。

IPsec

IPsec により、インターネットなどの保護されていないネットワーク上で機密性の高い情報を送信する際にセキュリティを確保します。IPsec では、データ認証サービスおよびアンチ リプレイ サービスの他にデータ機密保持サービスが提供されます。

IKE

IKE とは、IPsec 標準とともに使用される鍵管理プロトコル標準です。IPsec の設定には必ずしも IKE は必要ありませんが、IKE では、IPsec 標準に対する新機能が追加されているほか、設定をより柔軟かつ容易に行えるよう、IPsec のサポートが強化されています。

PKI

PKI は、IPsec、Secure Shell（SSH; セキュア シェル）、および Secure Socket Layer（SSL）などの Cisco IOS セキュリティ プロトコルを導入することで、ネットワークの安全確保、管理オーバーヘッドの削減、およびネットワーク インフラストラクチャの導入の簡略化といったスケーラブルな方法を実現しています。Cisco IOS ソフトウェアは、PKI を使用して、アクセス リストおよび認証リソースを使用した認証を行うこともできます。

VPN

VPN ソリューションは、Standard IPsec、Dynamic Multipoint VPN（DMVPN; ダイナミック マルチポイント VPN）、Easy VPN、Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）トンネリング、および Group Encrypted Transport VPN（GET VPN）といった基礎となる 5 つの VPN テクノロジーに基づいて構築されています。各テクノロジーにはそれぞれ利点があり、特定の導入要件を満たすようカスタマイズされています。表 1 では、これらのテクノロジーを比較しています。

表 1　VPN ソリューションの比較

標準 IPsec VPN	
利点	**使用目的**
• サイト間を暗号化する。 • Quality of Service（QoS）をサポートする。	• マルチベンダー相互運用性が必要な場合。
Cisco DMVPN	
利点	**使用目的**
• ポイントツーポイントの暗号化設定と管理を簡略化する。 • オンデマンドのスポークツースポーク トンネルを提供する。 • QoS、マルチキャスト、およびルーティングをサポートする。	• QoS、マルチキャスト、およびルーティングをサポートしながら、ハブアンドスポーク VPN の設定を簡略化するため。 • ロースケールなオンデマンド メッシングを提供するため。
Cisco Easy VPN	
利点	**使用目的**
• ダイナミックな設定ポリシー プッシュを通して、IPsec およびリモートサイト デバイス マネジメントを簡略化する。 • QoS をサポートする。	• VPN および管理全体を簡略化することが主な目的（ただし、限られたネットワーキング機能だけを使用）の場合。 • さまざまな Cisco VPN 製品の単純でありながら統合された設定フレームワークを提供するため。

表 1　VPN ソリューションの比較 （続き）

標準 IPsec VPN	
Cisco GRE ベース VPN	
利点	**使用目的**
• IPsec VPN 全体でマルチキャストの転送とトラフィックのルーティングをイネーブルにする。 • 非 IP プロトコルをサポートする。 • QoS をサポートする。	• ルーティングを VPN 全体でサポートする必要がある場合。 • ハブアンドスポーク DMVPN と同じ機能を実行するが、より詳細な設定が必要な場合。
Cisco GET VPN	
利点	**使用目的**
• IP および Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）WAN 上の暗号化統合を簡略化する。 • ポイントツーポイント キー ペアではなく、グループ キー入力を使用して、暗号化管理を簡略化する。 • サイト間で、スケーラブルで管理可能な any-to-any 接続をイネーブルにする。 • QoS、マルチキャスト、およびルーティングをサポートする。	• any-to-any 接続およびネットワーキング機能を保持しながら、MPLS または IP WAN へ暗号化を追加するため。 • IPsec VPN に対して、スケーラブルな、フルタイム メッシングをイネーブルにするため。 • 小型のルータがメッシュ ネットワークに参加できるようにするため。 • QoS、マルチキャスト、およびルーティングをサポートしながら、暗号キー管理を簡略化するため。

関連資料

このマニュアルの他に、Cisco.com にはセキュア接続に関する他の資料もありますが、数が多いためここでは割愛します。セキュア接続の詳細またはその他の参考資料については、Cisco.com で、目的の題名またはタイトルを指定して検索してください。