

Cisco 1700 シリーズ用 VPN モジュール

Cisco 1700 シリーズルータのVPNモジュールは、Cisco 1700プラットフォームでVPN機能を最大限に活用できるように設計された製品です。VPNを使用すると、インターネットのような公衆網を使いながら、私設網の持つ有利な特長(セキュリティ、管理機能、サービス品質など)を活用でき、さらにコストが削減されて柔軟性が向上します。このVPNモジュールは、業界標準であるIPSec(IP Security)を実装することによってVPNセキュリティを実現し、公衆IPネットワークでの情報の機密性、完全性、正当性を保証します。

Cisco 1700シリーズには、Cisco 1720と1750という2つのモデルがあります。どちらも中小規模企業および支店・営業所向けのモジュラアクセスルータで、次世代サービスに対応できる機能を備えています。ルーティング、ファイアウォール、VPNなど、多彩な機能が統合されている他、データと音声の統合アプリケーションにも対応できます。Cisco 1700シリーズとVPNモジュール、そしてCisco IOS Firewallフィーチャセットの組み合わせは、支店・営業所がその他のリモートオフィス、モバイルユーザー、本社イントラネット、または取引先とのエクストラネットと接続するための理想的なIPSec/VPNソリューションとなります。

VPNモジュールは、Cisco 1720シャーシまたは1750シャーシの内部スロットに搭載できます。このモジュールは、DES(Data Encryption Standard)および3DESのアルゴリズムをサポートし、全二重T1/E1シリアル接続相当の速度(1518バイト/パケットで4Mbps)でデータの暗号化を実行します。また、Cisco 1700プラットフォームの機能と統合することにより、モバイルユーザーや他のサイトのユーザーとの間で最大100の暗号化トンネル(同時セッション)を確立できます。

図1 : Cisco 1700シリーズのVPNモジュール



Cisco 1700シリーズのVPNモジュールは、暗号化だけでなく、ハッシュ、キー交換、セキュリティアソシエーションの保存など、さまざまなIPSec関連の処理を実行します。したがって、Cisco 1700のメインプロセッサやメモリは、これらの処理を専用モジュールにまかせて、ルーティング、音声、ファイアウォールなどの処理に専念できます。

VPNモジュールを搭載したCisco 1700シリーズは、Cisco 7100 VPNルータやCisco 2600、3600、7200、7500のモジュール/アダプタとともに、スケーラブルな高性能IPSec/VPNソリューションファミリを構成します。

機能概要

3DESの処理速度を最大4Mbpsに向上(1518バイトのパケット)

最大100の同時セッション(IPSecトンネル)が可能

3DESまたはDESの実装によるデータ保護

RSAおよびDiffie-Hellmanアルゴリズムによる認証をサポート
データ完全性の保証にSHA-1(Secure Hash Algorithm 1)またはMD5(Message Digest 5)ハッシュアルゴリズムを使用

機能説明

シスコは、IPSecおよび関連プロトコルを記述しているRFC (Request For Comment) 2401 ~ 2410を完全にサポートしています。これらのサポート機能について具体的に説明します。

IPSec - IPSecは暗号化技術を使用して、私設網のピア間でやりとりされるデータの機密性、完全性、正当性を保証するプロトコル群です。シスコは、IPSecの暗号化(ESP: Encapsulating Security Payload)および認証ヘッダ(AH: Authentication Header)を完全にサポートしています。

IKE(Internet Key Exchange) - セキュリティアソシエーション(SA)の管理を担うプロトコルです。以前は、Internet Security Association Key Managementプロトコル(ISAKMP/Oakley)と呼ばれていました。IKEは、IPSecトランザクションの各ピアの認証、セキュリティポリシーのネゴシエーション、セッションキーの交換処理を実行します。

証明書の管理 - シスコは、デバイス認証用のX.509.V3証明システム、および認証局との通信プロトコルであるCEP(Certificate Enrollment Protocol)を完全にサポートしています。Verisign社やEntrust Technologies社など、いくつかのベンダーがシスコのCEPをサポートしており、Ciscoデバイスとの相互動作を保証しています。シスコの証明書ソリューションは、PKI(公開キーインフラストラクチャ)ソリューションに必要な階層証明書構造や相互証明の機能にも対応しています。

DESおよび3DES - DESや3DESの暗号処理は、IPSecトンネルを宛先とするすべてのパケットに必要なので、プロセッサに大きな負荷をかけます。Cisco 1700シリーズにVPNモジュールを搭載すれば、このモジュールがDESまたは3DESを使用したデータ暗号化を最大4 Mbpsの速度で処理するため、メインプロセッサの能力を他の処理作業に専念させることができます。

RSAおよびDiffie-Hellman - この2つのアルゴリズムはIPSecトンネルが確立されるたびに使用されます。RSAはリモートデバイスの認証を実行し、Diffie-Hellmanアルゴリズムは暗号化

に使用されるキーの交換を実行します。Cisco 1700シリーズでは、RSAはソフトウェアに実装されていますが、Diffie-Hellmanはモジュールそのものに組み込まれています。このようなアーキテクチャによって、1秒ごとに複数のIPSecトンネルを確立する性能が実現されているのです。

セキュリティの拡張 - ハードウェアベースの暗号化によるセキュリティは、鍵の拡張保護など、いくつかの点でソフトウェアベースのソリューションよりも有利です。また、Cisco 1700シリーズとVPNモジュールは、FIPS 140-1 Level 2セキュリティにも適合するように設計されています(現時点では未認可)。

Cisco 1700シリーズ用VPNモジュールのソフトウェア

VPNモジュールには、リリース12.1(1)XX、12.1(2)T以上のCisco 1700シリーズIOSソフトウェアを使用する必要があります。IPSec 3DESソフトウェアは、Cisco 1700シリーズIOSソフトウェアのすべてのIPSec機能を備え、3DESとDES(56ビット)を両方サポートしています。IPSec 56ソフトウェアも、同じIPSec機能を備えています。このソフトウェアはDES(56ビット)しかサポートしていません。Cisco 1700シリーズIOS 12.1(2)TのIP Firewall Plus IPSec 3DESソフトウェアには、完全なIPSecパッケージ、3DESおよびDES、Firewall、およびPlusの各フィーチャセットの機能が含まれています。

VPNモジュールが搭載されたCisco 1700シリーズルータには、Cisco 1700シリーズIOSソフトウェア(12.1(1)XX、12.1(2)T以上)のあらゆるフィーチャセットを使用できます。ただし、このモジュールを使用するためには、IPSecフィーチャセットが必要です。したがって、VPNモジュールが搭載されたCisco 1700シリーズルータでCisco 1700 IOS 12.1(2)TのIPフィーチャセットソフトウェアを稼働することは可能ですが、このソフトウェアにはIPSec機能が含まれていないため、VPNモジュールの機能を活用できません。

Cisco 1700シリーズIPSecソフトウェア(Cisco IOS リリース12.1:12.1(1)XX、12.1(2)T以上)のメモリ要件

製品番号	イメージ名	ソフトウェアイメージ	必要なフラッシュメモリ	必要なDRAMメモリ	起動メモリ
S17CL-12.1.2T	IP Plus IPSec 56 (DES)	c1700-sy56i-mz	8	32	RAM
S17CHL-12.1.2T	IP/FW Plus IPSec 56 (DES)	c1700-o3sy56i-mz	8	32	RAM
S17CK2-12.1.2T	IP Plus IPSec 3DES	c1700-k2sy-mz	8	32	RAM
S17CHK2-12.1.2T	IP/FW Plus IPSec 3DES	c1700-k2o3sy-mz	8	32	RAM
S17QHL-12.1.2T	IP/IPX/AT/IBM/FW Plus IPSec 56 (DES)	c1700-bno3r2sy56i-mz	8	32	RAM
S17QHK2-12.1.2T	IP/IPX/AT/IBM/FW Plus IPSec 3DES	c1700-bk2no3r2sy-mz	8	32	RAM
S17CVL-12.1.2T	IP/Voice Plus IPSec 56 (DES)	c1700-sv3y56i-mz	8	32	RAM
S17CVHL-12.1.2T	IP/FW/Voice Plus IPSec 56 (DES)	c1700-o3sv3y56i-mz	8	32	RAM
S17CVK2-12.1.2T	IP/Voice Plus IPSec 3DES	c1700-k2sv3y-mz	8	32	RAM
S17CVHK2-12.1.2T	IP/FW/Voice Plus IPSec 3DES	c1700-k2o3sv3y-mz	8	32	RAM
S17QVHL-12.1.2T	IP/IPX/AT/IBM/FW/Voice Plus IPSec 56 (DES)	c1700-bno3r2sv3y56i-mz	16	48	RAM
S17QVHK2-12.1.2T	IP/IPX/AT/IBM/FW/Voice Plus IPSec 3DES	c1700-bk2no3r2sv3y-mz	16	48	RAM

VPN モジュールに関する輸出規制

VPN モジュールのDESおよび3DESソフトウェアは、暗号化製品に対する米国輸出規制の対象となります。ただし、このモジュール自体は輸出規制の対象製品ではありません。米国輸出規制により、DESおよび3DESソフトウェアの受領者の住所および氏名を登録することが義務づけられています。シスコは、DESおよび3DESソフトウェアの発注の際にこの規制要求を満たす方法を探っています。詳細は、<http://www.cisco.com/wwl/export/encrypt.html> を参照してください。

仕様

製品番号および名称

MOD1700-VPN : Cisco 1700 シリーズ VPN モジュール

サポート標準 (IOS IPsec)

IPsec - RFC 2401 ~ 2410
 DES/3DESを使用したESP (Encapsulating Security Payload)
 - RFC 2406
 MD5またはSHA を使用したIPsec AH (Authentication Header) - RFC 2403 ~ 2404
 IKE (Internet Key Exchange) - RFC 2407 ~ 2409

寸法と重量

幅

5.72 cm (2.25 インチ)

高さ

1.78 cm (0.70 インチ)

奥行き

9.53 cm (3.75 インチ)

重量

35.5 g (0.078 lb)

環境条件

動作時の温度 : 0 ~ 40 (32 ~ 104° F)
 非動作時の温度 : - 20 ~ 65 (- 4 ~ 149° F)
 動作時の相対湿度 : 10 ~ 85% (結露しないこと)
 非動作時の相対湿度 : 5 ~ 95% (結露しないこと)

規制遵守、安全性、EMC、電気通信、ネットワーク認定

Cisco 1720 ルータまたは1750 ルータにVPN モジュールを搭載しても、ルータ自体の規格適合状況(規制遵守、安全性、EMC、電気通信、ネットワーク認定)は変わりません。Cisco 1720 ルータおよび1750 ルータのデータシートを参照してください。

©2000 Cisco Systems, Inc. All rights reserved.

Cisco と Cisco Systems は商標です。Cisco のロゴは Cisco Systems, Inc. の登録商標です。

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。

本仕様は予告なしに変更される場合があります。



シスコシステムズ株式会社

URL: <http://www.cisco.com/jp/>

E-mail: cnac@cisco.com

〒100-0005 東京都千代田区丸の内3-2-3 富士ビルヂング

TEL.03-5645-8856 FAX.03-5641-3523

お問い合わせ先