GLOSSARY

記号と数字

3DES
トリプル DES。3 つの 56 ビット DES 暗号キー（したがって、実際のキー長は 168 ビット）をすばやく連続して使用する暗号化アルゴリズム。また、2 つの 56 ビット DES キーを使用し、そのどちらかを 2 度使用する方法もあります。この場合、キーの実際の長さは 112 ビットになります。トリプル DES を合法的に使用できるのは、米国内に限られます。「DES」を参照してください。

802.1x
802.1x は、メディアレベルのアクセス コントロールに関する IEEE 標準です。ユーザまたはマシンの ID に基づき、ネットワーク接続の許可または拒否、VLAN アクセスの制御、およびトラフィック ポリシーの適用機能を実現します。

A

AAA
認証（Authentication）、許可（Authorization）、およびアカウンティング（Accounting）の頭文字。「トリプル A」と読みます。

AAL5-MUX
ATM Adaptation Layer 5 Multiplexing。

AAL5-SNAP
ATM Adaptation Layer 5 Subnetwork Access Protocol。

ACE
アクセス コントロール エントリ。ACL のエントリであり、送信元のホストまたはネットワークのほか、このホストからのトラフィックが許可または拒否されるかを指定します。ACE では宛先ホストまたはネットワーク、およびトラフィック タイプを指定することもできます。

ACL
アクセス コントロール リスト。デバイスに関する情報であり、そのデバイスまたはそのデバイスが属しているネットワークへのアクセスを許可するエンティティを指定します。アクセス コントロール リストは、1 つ以上のアクセス コントロール エントリ（ACE）によって構成されます。

ACS	Cisco Secure Access Control Server。RADIUS サーバまたは TACACS+ サーバの実装が可能な Cisco ソフトウェア。ACS には、Easy VPN、NAC、およびネットワークへのアクセスを制御するその他の機能によって使用されるポリシー データベースが保存されます。
ADSL	非対称デジタル加入者線。
AES	Advanced Encryption Standard。
AES-CCMP	Advanced Encryption Standard-Counter Mode with Cipher Block Chaining Message Authentication Code Protocol。AES-CCMP は、Wi-Fi Protected Access 2（WPA2）および IEEE 802.11i ワイヤレス LAN セキュリティで必要です。
AH	認証ヘッダー。これは、ほとんどのネットワークでは ESP より重要度の低い、古い IPSec プロトコルです。AH は認証サービスを提供しますが、暗号化サービスは提供できません。認証と暗号化の両方が可能な ESP をサポートしていない IPSec ピアとの互換性を保証するために提供されています。
AH-MD5-HMAC	MD5（HMAC の一種）ハッシュ アルゴリズムを使用する認証ヘッダー。
AH-SHA-HMAC	SHA（HMAC の一種）ハッシュ アルゴリズムを使用する認証ヘッダー。
AHP	認証ヘッダー プロトコル。送信元ホストの認証とデータの整合性を提供するプロトコル。データの機密性は提供しません。
AMI	Alternate Mark Inversion。
ARP	アドレス解決プロトコル。ノード ハードウェア アドレス（*MAC アドレス*と呼ばれる）を IP アドレスにマッピングする下位層の TCP/IP プロトコルです。
ASA	アダプティブ セキュリティ アルゴリズム。各内部システムとアプリケーションのための、明示的な設定のない一方向（内部から外部へ）の接続を可能にします。
ATM	非同期転送モード。複数のサービス タイプ（音声、ビデオ、データなど）を 53 バイトの固定長セルで伝送するセル リレーの国際標準。固定長セルの採用により、セルの処理をハードウェアで行うことが可能になるため、伝送遅延が低減されます。

B

BC 認定バースト。BC は、スケジューリングの問題を発生させることなく、特定の時間単位内に送信できるトラフィック量を 1 バーストあたりのビット数（またはバイト数）で指定する QoS ポリシング パラメータです。

BE 超過バースト。BE は、すべてのトラフィックでレート制限を超える状態が発生しない範囲の最大トラフィック量を指定する QoS ポリシング パラメータです。通常のバースト サイズから超過バースト サイズまでの範囲のトラフィックは、レート制限を超える可能性があります。この確率はバースト サイズが増えるにつれて高くなります。

BOOTP Bootstrap Protocol。ネットワーク ノードがネットワーク ブート時にイーサネット インターフェイスの IP アドレスを取得するために使用するプロトコルです。

BSSID Basic Service Set Identifier。BSSID は 802.11g 無線で使用する識別子です。MAC アドレスと同様の機能を持ちます。

C

C3PL Cisco Common Classification Policy Language。C3PL は機能固有の設定コマンドの代わりに使用できる、構造化された言語です。これを使用すると、イベント、条件、およびアクションに関する設定機能を表現できます。

CA 認証機関。デジタル証明書の発行および取り消しを行う、信頼できる第三者機関。*公証機関*または*認証局*と呼ばれることもあります。特定の CA のドメイン内では、デバイスは各自の証明書と CA のパブリック キーがあればそのドメイン内の他のデバイスを認証できます。

CA サーバ 証明機関サーバ。デジタル証明書の発行と取り消しに使用されるネットワーク ホストです。

CA 証明書 ある認証機関（CA）が別の認証機関に与えたデジタル証明書。

CBAC コンテキストベース アクセス コントロール。各アプリケーションおよびネットワーク周辺のすべてのトラフィックを内部ユーザが安全にアクセス制御できるようにするプロトコル。CBAC は送信元と宛先のアドレスを調べて、各アプリケーション接続のステータスを追跡します。

CBWFQ Class-Based Weighted Fair Queuing。CBWFQ はユーザ定義のトラフィック クラスをサポートします。CBWFQ では、プロトコル、アクセス コントロール リスト（ACL）、入力インターフェイスなどの一致条件に基づいてトラフィック クラスを定義します。

CDP Cisco ディスカバリ プロトコル。メディアおよびプロトコルに依存しないデバイス ディスカバリ プロトコルであり、Cisco 製のすべてのルータ、アクセス サーバ、ブリッジ、およびスイッチ上で動作します。CDP を使用することで、デバイスはその存在を他のデバイスに通知して、同じ LAN 上または WAN のリモート側にある他のデバイスに関する情報を受信できます。

CDP 証明書失効リスト配信ポイント。証明書失効リストを取得する場所です。通常、CDP は HTTP または LDAP URL として指定されます。

CEP Certificate Enrollment Protocol。証明書管理プロトコル。CEP は、IETF（インターネット技術特別調査委員会）に提案された標準である CRS（Certificate Request Syntax）の初期の実装です。デバイスと CA の通信方法を規定します。たとえば、CA のパブリック キーの取得方法、CA へのデバイスの登録方法、証明書失効リスト（CRL）の受信方法などです。CEP はキー コンポーネント技術として PKCS（Public Key Cryptography Standard）7 および 10 を使用します。IETF の PKIX（Public Key Infrastructure working group）がこれらの機能のためのプロトコル（CRS またはこれと同等のプロトコル）の標準化に取り組んでいます。IETF 標準が確定次第、Cisco はその標準のサポートを追加します。CEP は Cisco Systems と VeriSign, Inc. が共同開発したものです。

CET Cisco 暗号化技術。Cisco IOS Release 11.2 で導入された、独自のネットワーク層の暗号化方式。CET は IP パケット レベルでネットワーク データの暗号化を実現し、標準として DH、DSS、40 ビット DES、および 56 ビット DES を実装します。

CHAP Challenge Handshake Authentication Protocol。PPP カプセル化を使用する回線でサポートされるセキュリティ機能で、不正アクセスを防止します。CHAP 自体が不正アクセスを防止するわけではなく、リモート エンドを識別するだけです。次に、ルータまたはアクセス サーバが、そのユーザにアクセスが許可されているかどうかを判断します。「PAP」も参照してください。

chargen Character Generation。TCP 経由の場合、クライアントによって停止されるまで文字の連続ストリームを送信するサービス。UDP 経由の場合、サーバは、クライアントがデータグラムを送信するたびにランダムな数の文字を送信します。

CIR Committed Information Rate。適用される、設定済みの長期平均認定レート。

Cisco CP Cisco Configuration Professional。Cisco CP は、ルータ上で LAN、WAN、およびセキュリティ機能を設定できるインターネット ブラウザベースのソフトウェア ツールです。

CLI コマンド ライン インターフェイス。ルータに対する設定や監視コマンドの入力に使用される主要なインターフェイス。CLI から入力できるコマンドの詳細については、現在設定しているルータの設定ガイドを参照してください。

CM WAAS セントラル マネージャ。WAE-E が WAE-C と通信できるようにするには、その WAE-E を WAAS CM に登録する必要があります。

CME Cisco Call Manager Express。CME は VoIP（Voice over IP）ゲートウェイにコール処理のサービスを提供します。

CNS Cisco Networking Services。スケーラブルなネットワークの導入、設定、サービス保証監視、およびサービス配信をサポートするサービス スイートです。

comp-lzs IP 圧縮アルゴリズム。

cookie ユーザ設定などの情報を永続ストレージに格納したり取得したりする Web ブラウザ機能。Netscape と Internet Explorer では、cookie はローカル ハード ドライブに保存される小さいテキスト ファイルです。このファイルは、次回 Java アプレットを実行したとき、または Web サイトにアクセスしたときにロードできます。この方法を使用すると、ユーザ固有の情報をセッション間で保持できます。cookie の最大サイズは約 4KB です。

CPE 顧客宅内機器。

CRL 証明書失効リスト。期限切れではないが失効したデジタル証明書の、認証機関（CA）によって管理および署名されるリストです。

cTCP Cisco Tunneling Control Protocol。cTCP は TCP over IPSec や TCP トラバーサルとも呼ばれます。cTCP は、ESP トラフィックおよび IKE トラフィックを TCP ヘッダーにカプセル化するプロトコルです。クライアントとサーバまたはヘッドエンド デバイス間のファイアウォールは、このカプセル化されたトラフィックを TCP トラフィックとみなして通過を許可します。

D

DES データ暗号化標準。米国の National Institute of Standards and Technology（NIST）が開発および標準化した標準暗号化アルゴリズム。56 ビットの秘密暗号キーを使用します。DES アルゴリズムは多くの暗号化標準で採用されています。

DHCP ダイナミック ホスト コンフィギュレーション プロトコル。IP アドレスをホストにダイナミックに割り当てるメカニズムを提供します。ホストで IP アドレスが不要になると、その IP アドレスを再利用できます。

DH、Diffie-Hellman 安全でない通信チャネルを使用して 2 者間で秘密情報を共有できるようにするパブリック キー暗号プロトコル。インターネット キー交換（IKE）でセッション キーを確立するために使用されます。Diffie-Hellman は Oakley キー交換のコンポーネントです。

Diffie-Hellman キー交換 安全でない通信チャネルを使用して 2 者間で秘密情報を共有できるようにするパブリック キー暗号プロトコル。インターネット キー交換（IKE）でセッション キーを確立するために使用されます。Diffie-Hellman は Oakley キー交換のコンポーネントです。Cisco IOS ソフトウェアは、768 ビットおよび 1024 ビットの Diffie-Hellman グループをサポートしています。

DLCI データリンク接続識別子。フレーム リレー接続において、2 つのエンド ポイント間の特定のデータリンク接続を識別する値です。

DMVPN ダイナミック マルチポイント VPN。ルータが論理的なハブ アンド スポーク トポロジに配置され、ハブ間がポイントツーポイントの GRE over IPSec 接続でつながれている仮想プライベート ネットワーク。DMVPN は GRE と NHRP を使用して、パケットがネットワーク内の宛先に転送されるようにします。

DMZ 非武装地帯。DMZ は、インターネットとプライベート ネットワークの間にある緩衝地帯です。インターネット上の外部クライアントがアクセスする Web、FTP、および電子メール サーバ用に一般に使用されるパブリック ネットワークを DMZ として設定できます。これらのパブリック アクセス サーバを別の隔離されたネットワークに配置することで、内部ネットワークのセキュリティが強化されます。

DN 識別名。認証機関ユーザの一意の識別子であり、認証機関から受け取った各証明書に含まれます。通常、DN には、ユーザの通称、会社または組織の名称、2 文字の国コード、連絡先の電子メール アドレス、電話番号、部門番号、および居住地などが含まれます。

DNS ドメイン ネーム システム（またはサービス）。文字で構成したドメイン名を、数字で構成した IP アドレスに変換するインターネット サービス。

DPD デッド ピア検知。DPD では、ピアにキープアライブ メッセージを定期的に送信して、ピアからの応答を確認することで、ピアが現時点でアクティブかどうかを判断します。一定の時間内にピアから応答が得られない場合は、接続は切断されます。

DRAM ダイナミック ランダム アクセス メモリ。キャパシタ部分に情報が格納される RAM であり、定期的にリフレッシュする必要があります。

DSCP Differentiated Services Code Point。DSCP マーキングは、QoS 用にトラフィックを分類するために使用できます。「NBAR」も参照してください。

DSLAM デジタル加入者線アクセス マルチプレクサ。

DSS デジタル署名標準。*デジタル署名アルゴリズム*（DSA）とも呼ばれます。DSS アルゴリズムは、暗号署名の多くのパブリック キー標準で採用されています。

DVTI Dynamic Virtual Tunnel Interface。DVTI は、さまざまな宛先にトラフィックを選択的に送信できる、ルーティング可能なインターフェイスです。物理インターフェイスに対する DVTI のマッピングはスタティックではありません。そのため、あらゆる物理インターフェイスで暗号化したデータを送受信できます。

E

E1 2.048 Mbps の速度でデータを伝送する、ヨーロッパで広く使用されている広域デジタル伝送方式。

EAP-FAST Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling。Cisco Systems が開発した、802.1x EAP の一種。強力なパスワード ポリシーを適用できないお客様でも、デジタル証明書を必要としない種類の 802.1x EAP を展開できるようにします。

EAPoUDP Extensible Authentication Protocol over User Datagram Protocol。EOU と省略表記されることもあります。ポスチャの検証を実行するためにクライアントと NAD が使用するプロトコル。

Easy VPN Cisco Unified Client Framework をベースにした VPN 集中管理ソリューション。Cisco Easy VPN は、Cisco Easy VPN リモート クライアントと Cisco Easy VPN サーバの 2 つのコンポーネントから設定されています。

eDonkey eDonkey 2000 または ED2K とも呼ばれる、巨大なピアツーピア ファイル共有ネットワーク。eDonkey は Multisource File Transmission Protocol（MFTP）を実装しています。

EIGRP Enhanced Interior Gateway Routing Protocol。Cisco Systems が開発した IGRP の拡張版。収束特性と運用効率に優れており、リンク ステート プロトコルとディスタンス ベクタ プロトコルの利点を併せ持っています。

ERR イベント リスク評価。ユーザが誤検知の可能性を最小化するために選択するアクションのレベルを制御します。

ESP Encapsulating Security Payload。データの整合性と機密性の両方を提供する IPSec プロトコル。Encapsulating Security Payload とも呼ばれる ESP は、機密性、データ発信元認証、リプレイ検出、コネクションレスの整合性、部分的なシーケンスの整合性、および限定的なトラフィック フローの機密性を提供します。

esp-3des 168 ビットの DES 暗号化アルゴリズム（3DES またはトリプル DES）を使用する ESP（Encapsulating Security Payload）トランスフォーム。

esp-des 56 ビットの DES 暗号化アルゴリズムを使用する ESP（Encapsulating Security Payload）トランスフォーム。

ESP-MD5-HMAC MD5 の変形である SHA 認証アルゴリズムを使用する ESP（Encapsulating Security Payload）トランスフォーム。

esp-null 暗号化も機密性も提供しない ESP（Encapsulating Security Payload）トランスフォーム。

ESP-SHA-HMAC HMAC の変形である SHA 認証アルゴリズムを使用する ESP（Encapsulating Security Payload）トランスフォーム。

ESP_SEAL 160 ビット キーの SEAL（Software Encryption Algorithm）暗号化アルゴリズムを使用する ESP。この機能は、12.3(7)T で導入されました。この機能を使用するには、ルータでハードウェア IPSec 暗号化を無効にする必要があります。

F

Fasttrack 接続されたピア（スーパーノードと呼ぶ）に、インデックス機能が動的に割り当てられるファイル共有ネットワーク。

Finger ユーザに特定のインターネット サイトのアカウントがあるかどうかを確認するソフトウェア ツール。多くのサイトでは、インバウンド Finger 要求は許可されません。

FTP ファイル転送プロトコル。TCP/IP プロトコル スタックの一部で、ホスト間のファイル転送に使用されます。

G

G.SHDSL G.991.2 とも呼ばれます。国際電気通信連合が規定した対称型 DSL の国際標準です。G.SHDSL では、1 対の銅線を使用して、高速の対称データ ストリームを 192 kbps ～ 2.31 Mbps の速度で送受信できます。

Gnutella 分散型 P2P ファイル共有プロトコル。ユーザはインストールした Gnutella クライアントを使用することで、インターネット上のファイルを検索、ダウンロード、およびアップロードできます。

GRE ジェネリック ルーティング カプセル化。Cisco が開発したトンネリング プロトコルであり、IP トンネル内のさまざまなタイプのプロトコル パケットをカプセル化し、IP インターネットワーク上にリモートの Cisco ルータへの仮想ポイントツーポイント リンクを確立できます。シングルプロトコルのバックボーン環境にマルチプロトコル サブネットワークを接続して、GRE を使用した IP トンネリングを利用すれば、シングルプロトコルのバックボーン環境にまたがるネットワーク拡張が可能になります。

GRE over IPSec この技術では、IPSec を使用して GRE パケットを暗号化します。

H

H.323 ローカル エリア ネットワーク（LAN）などのパケット交換型ネットワーク上でのビデオ会議、およびインターネット上でのビデオの送受信を可能にする ITU-T 標準。

HDLC ハイレベル データリンク コントロール。ISO（国際標準化機構）が標準化したビット指向の同期データ リンク層プロトコル。フレーム文字とチェックサムを使用した同期シリアル リンク上でのデータ カプセル化方式を指定します。

HMAC ハッシュベースのメッセージ認証コード。HMAC は暗号ハッシュ関数を使用したメッセージ認証メカニズムです。MD5、SHA-1 などの反復暗号ハッシュ関数および秘密共有キーと組み合わせて使用できます。HMAC の暗号の強度は、使用されるハッシュ関数の特性によって異なります。

HMAC-MD5 ハッシュ メッセージ認証コードと MD5 の組み合わせ（RFC 2104）。キー付きの MD5 であり、送信者と受信者は共有プライベート キーを使用して転送情報を検証できます。

HTTP
HTTPS Hypertext Transfer Protocol、Hypertext Transfer Protocol, Secure。Web ブラウザおよび Web サーバがテキストファイルやグラフィック ファイルなどを転送するために使用するプロトコルです。

I

ICMP インターネット制御メッセージ プロトコル。ネットワーク層のインターネット プロトコルで、エラーを通知し、IP パケット処理に関するその他の情報を提供します。

IDM IDS デバイス マネージャ。IDS センサの管理に使用されるソフトウェアです。

IDS 侵入検知システム。Cisco IPS は、ネットワーク トラフィックをリアルタイムに分析し、シグニチャ ライブラリと照合することによって異常や悪用を検出します。不正なアクティビティまたは異常を検出すると、その状態を終結させてトラフィックによるホスト攻撃をブロックし、IDM にアラートを送信します。

IDS センサ IDS センサは、Cisco IDS が実行されているハードウェアです。スタンドアロン デバイスとして、またはルータにインストールされたネットワーク モジュールとして使用できます。

IEEE 米国電気電子学会。

IETF インターネット技術特別調査委員会。

IGMP Internet Group Management Protocol。IPv4 システムが IP マルチキャストのメンバ情報を隣接マルチキャスト ルータに通知するために使用するプロトコルです。

IKE インターネット キー交換。IPSec およびその他の標準とともに使用されるキー管理プロトコルの標準。IPSec は IKE を使用しないように設定できますが、IKE を使用した方が IPSec 標準の機能と柔軟性が向上し、設定が容易になります。IKE は IPSec ピアの認証と、IPSec キーおよび IPSec セキュリティ アソシエーションのネゴシエーションを行います。

IPSec トラフィックを通過させるには、各ルータ / ファイアウォール / ホストでピアの識別情報を確認できる必要があります。これは、手動で事前共有キーを両方のホストに入力するか、または CA サービスによって可能です。IKE は、Internet Security Association and Key Management Protocol（ISAKMP）フレームワークの内部に Oaklay と Skeme のキー交換を実装したハイブリッド プロトコルです。ISAKMP、Oakley、および Skeme は、IKE によって実装されるセキュリティ プロトコルです。

IKE ネゴシエーション 安全でないネットワーク上でプライベート キーを安全に交換するための方法。

IKE プロファイル ISAKMP パラメータのグループ。他の IP セキュリティ トンネルにマッピング可能です。

IM
インスタント メッセージング。発信者と受信者の双方が同時にオンライン化できる、リアルタイム通信サービスです。一般的な IM サービスには Yahoo! Messenger（YM）、Microsoft Networks Messenger、AOL Instant Messenger（AIM）などがあります。

IMAP
Internet Message Access Protocol。電子メール サーバと通信するクライアントによって使用されるプロトコルです。IMAP は RFC 2060 で定義されており、クライアントはこれによって電子メール サーバ上のメッセージを取得するだけでなく、メッセージの削除、メッセージのステータス変更、その他のメッセージ操作が可能です。

IOS
Cisco IOS ソフトウェア。CiscoFusion アーキテクチャに基づくすべての製品に共通の機能、スケーラビリティ、およびセキュリティを提供する Cisco システム ソフトウェア。Cisco IOS を使用すると、広範なプロトコル、メディア、サービス、およびプラットフォームがサポートされるだけでなく、インターネットワークのインストールと管理が中央に統合され、自動化されます。

IOS IPS
IPS
Cisco IOS 侵入防止システム。IOS IPS は、トラフィックを侵入シグニチャの広範なデータベースと照合して、侵入パケットを廃棄し、設定に基づいてその他のアクションを実行できます。シグニチャは、この機能をサポートする IOS イメージに組み込まれています。追加のシグニチャはローカルまたはリモートのシグニチャ ファイルに格納できます。

IP
インターネット プロトコル。インターネット プロトコルは、世界で最もよく知られているオープンシステム（非専有）プロトコル スイートです。相互接続された任意のネットワーク上での通信に使用でき、LAN 通信にも WAN 通信にも適しています。

IP アドレス
IP（バージョン 4）アドレスは 32 ビット長、つまり 4 バイト長です。このアドレス「空間」は、ネットワーク番号、オプションのサブネットワーク番号、およびホスト番号の指定に使用されます。32 ビットを 4 つのオクテット（8 バイナリ ビット）に分けて、ピリオドつまり「ドット」で区切った 4 つの 10 進数で表現します。ネットワーク番号、サブネットワーク番号、およびホスト番号を示すアドレス部分は、サブネット マスクで示されます。

IPSec
ピア間のデータ機密性、データ整合性、およびデータ認証を提供するオープン標準のフレームワーク。これらのセキュリティ サービスは IP 層で提供されます。IPSec では、IKE を使用して、ローカル ポリシーに基づいてプロトコルとアルゴリズムのネゴシエーションを処理し、IPSec で使用する暗号キーと認証キーを生成します。IPSec は、1 対のホスト間、1 対のセキュリティ ゲートウェイ間、またはセキュリティ ゲートウェイとホスト間のデータ フローを保護する目的に使用できます。

IPSec ポリシー
Cisco CP では、IPSec ポリシーは VPN 接続に関連付けられた暗号マップの名前付きセットです。

IPSec ルール
IPSec で保護するトラフィックを指定するために使用されるルール。

IRB Integrated Routing and Bridging。IRB では、1 つのスイッチ ルータ内において、経路選択済みインターフェイスとブリッジ グループ間で、所定のプロトコルをルーティングできます。

ISAKMP Internet Security Association Key Management Protocol は、IKE の基礎です。通信中のピアの認証、セキュリティ アソシエーションの作成と管理、およびキー生成方法の定義などを行います。

K

Kazaa2 ピアツーピアのファイル共有サービス。

L

L2F プロトコル レイヤ 2 転送プロトコル。インターネット上の安全なバーチャル プライベート ダイヤルアップ ネットワークの構築をサポートするプロトコルです。

L2TP レイヤ 2 トンネリング プロトコル。RFC 2661 で定義されている IETF（インターネット技術特別調査委員会）標準のトラック プロトコルであり、PPP のトンネリングを提供します。L2F と PPTP のすぐれた機能をベースにして、業界全体で使用できる VPDN の実装方法を提供します。L2TP は IPSec の代替として提案されていますが、認証サービスを提供するために IPSsec と組み合わせて使用されることもあります。

LAC L2TP アクセス コンセントレータ。リモート システムへのコール、およびリモート システムと LNS 間のトンネリング PPP セッションを終端するデバイスです。

LAN ローカル エリア ネットワーク。一定の場所に常設したネットワーク、または 1 つの組織に属するネットワーク。必須ではありませんが、通常は IP プロトコルを使用します。その他のインターネット プロトコルを使用する場合もあります。グローバル インターネットではありません。「イントラネット」、「ネットワーク」、「インターネット」も参照してください。

LAPB 平衡型リンク アクセス手順。

LBO Line Build Out。

LEFS ローエンド ファイル システム。

LLQ 低遅延キューイング（LLQ）では、遅延の影響が大きいデータ（音声など）を他のトラフィックより優先的に処理し、他のキューにあるパケットのキューイング解除よりも先にこのようなデータをキューイング解除して送信できます。

LNS L2TP ネットワーク サーバ。LAC からの L2TP トンネルの終端、および L2TP データ セッションを介したリモート システムへの PPP セッションの終端が可能なデバイスです。

M

MAC メッセージ認証コード。メッセージの信頼性を確認するために使用される暗号チェックサム。「ハッシュ」を参照してください。

MD5 Message Digest 5。128 ビットのハッシュ値を生成する単方向のハッシュ関数。MD5 と SHA（Secure Hashing Algorithm）は MD4 の変形であり、MD4 のハッシュ アルゴリズムのセキュリティを強化するように設計されています。Cisco は IPSec フレームワーク内での認証にハッシュを使用しています。MD5 は通信の整合性を検証し、通信の発信元を認証します。

MD5 Message Digest 5。128 ビットのハッシュ値を生成する単方向のハッシュ アルゴリズム。MD5 と SHA（Secure Hash Algorithm）は MD4 の変形であり、MD4 のハッシュ アルゴリズムのセキュリティを強化するように設計されています。Cisco は IPSec フレームワーク内での認証にハッシュを使用しています。SNMP v.2 ではメッセージ認証にも使用されます。MD5 は通信の整合性の検証、送信元の認証、適時性の確認などを行います。

mGRE マルチポイント GRE。

MTU 最大伝送ユニット。インターフェイスが送受信できる最大パケット サイズ（バイト単位）です。

N

NAC

ネットワーク アドミッション コントロール。コンピュータ ウィルスの侵入を防ぐために、ネットワークへのアクセスを制御する方式です。NAC は、さまざまなプロトコルやソフトウェア製品を使用して、ネットワークへのログオンを試みるホストの状態を評価し、そのホストの状態を示すポスチャに基づいて要求を処理します。感染したホストは検疫に回され、ウィルス防止ソフトウェアがアップデートされていないホストはアップデート版の取得が指示されます。また、感染しておらず、ウィルス防止ソフトウェアもアップデートされているホストは、ネットワークに入ることを許可されます。「ACL」、「ポスチャ」、「EAPoUDP」も参照してください。

NAD

ネットワーク アクセス デバイス。NAC 実装で、ネットワークへのログオンを求めるホストの要求を受信するデバイス。NAD（通常はルータ）は、ポスチャ エージェント ソフトウェア（ホストで稼働）、ウィルス防止ソフトウェア、ネットワーク上の ACS およびポスチャ / 修復サーバとともに動作し、コンピュータ ウィルスの感染を予防するため、ネットワークへのアクセスを制御します。

NAS

ネットワーク アクセス サーバ。インターネットと公衆交換電話網（PSTN）のインターフェイスとなるプラットフォーム。

ネットワークと端末エミュレーション ソフトウェアを使用して非同期デバイスを LAN または WAN に接続するゲートウェイ。サポートされているプロトコルの同期ルーティングと非同期ルーティングを実行します。

NAT

ネットワーク アドレス変換

ネットワーク アドレス変換。グローバルに一意の IP アドレスを使用する必要性をなくすためのメカニズム。NAT は、グローバルに一意でないアドレスを持つ組織がインターネットに接続できるように、それらのアドレスをグローバルにルート指定可能なアドレス空間のアドレスに変換します。

NBAR

Network-based Application Recognition。QoS においてトラフィックの分類に使用される方式です。

NetFlow

ルータがインバウンド パケットをフローに分類できるようにする機能。多くの場合、フロー内のパケットは同じ方法で扱うことができるので、この分類によってルータの一部の処理が省略され、スイッチング操作は高速化されます。

NHRP

Next Hop Resolution Protocol。ハブ ルータがサーバであり、スポークがクライアントである DMVPN ネットワークで使用されるクライアント / サーバ プロトコル。ハブは、各スポークのパブリック インターフェイス アドレスの NHRP データベースを保持します。各スポークは、ブート時に自身の実際のアドレスを登録し、宛先スポークの実際のアドレスを NHRP データベースに照会して、それらのスポークへの直接トンネルを構築します。

NTP ネットワーク タイム プロトコル。ネットワーク デバイス上のシステム時計を同期させるプロトコル。NTP は UDP プロトコルです。

NVRAM 不揮発性ランダム アクセス メモリ。

O

Oakley 認証された当事者が使用できる、プライベート キーを確立するプロトコル。Diffie-Hellman に基づき、ISAKMP の互換性のあるコンポーネントとなるように設計されています。

OFB 出力フィードバック。暗号化（必須ではないが、通常は DES 暗号化）された出力を元の入力に戻す IPSec 機能。平文は、対称キーで直接暗号化されます。これにより、擬似乱数ストリームが生成されます。

OSPF Open Shortest Path First。インターネット コミュニティで RIP の後継として提案された、リンクステート階層型 IGP ルーティング アルゴリズム。OSPF 機能には、最低コスト ルーティング、マルチパス ルーティング、負荷分散などがあります。

P

P2P 「ピアツーピア」を参照してください。

PAD Packet Assembler/Disassembler。特定のプロトコルの全機能をサポートしない単純なデバイス（キャラクタモードの端末など）をネットワークに接続するために使用されるデバイス。PAD は、データのバッファリング、およびエンド デバイスに送信されたパケットの組み立てと分解を行います。

PAM ポート ツー アプリケーション マッピング。PAM を使用して、ネットワーク サービスまたはアプリケーション用の TCP または UDP ポート番号をカスタマイズできます。PAM ではこの情報を使用し、アプリケーションに関連付けて登録されている一般的なポートと異なるポートを使用しているサービスを実行するネットワーク環境をサポートします。

PAP パスワード認証プロトコル。ピアが互いに相手を認証できるようにする認証プロトコル。PAP では、パスワードとホスト名またはユーザ名を、暗号化されていない形式で渡します。「CHAP」も参照してください。

PAT

ダイナミック PAT

ポート アドレス変換。ダイナミック PAT を使用すると、複数のアウトバウンド セッションが 1 つの IP アドレスから開始されているように見せることができます。PAT を有効にすると、ルータは各アウトバウンド変換スロット（xlate）用に PAT IP アドレスから固有のポート番号を選択します。この機能は、インターネット サービス プロバイダがアウトバウンド接続用に固有の IP アドレスを十分に割り当てられない場合に役立ちます。グローバル プール アドレスがすべて使用されてから PAT アドレスが使用されます。

PEM

Privacy Enhanced Mail 形式。デジタル証明書を保管するための形式です。

PFS

完全転送秘密。非対称キー合意プロトコルの特性であり、1 つのキーを使用することでセッション全体が危険にさらされることのないように、セッションの中で時間ごとに異なるキーを使用できるようにします。

ping

ホストがネットワーク上でアクセス可能かどうかを確認するために、ホスト間で送信される ICMP 要求。

PKCS12

Public Key Cryptography Standard No.12。デジタル証明書情報を保管するための形式です。「PEM」も参照してください。

PKCS7

Public Key Cryptography Standard No. 7。

PKI

パブリック キー インフラストラクチャの略。認証機関（CA）と登録機関（RA）で設定されるシステムであり、証明書管理、アーカイブ管理、キー管理、トークン管理などの機能によるデータ通信での非対称キー暗号法の使用をサポートします。

非対称キー交換の標準でもあります。

このタイプのキー交換では、メッセージの受信者はメッセージ内の署名を信頼することができ、送信者は受信者が復号化できるようにメッセージを暗号化できます。「キー管理」を参照してください。

POP3

Post Office Protocol version 3。電子メール サーバから電子メールを取得するためのプロトコルです。

PPP

ポイントツーポイント プロトコル。同期および非同期回線上の、ルータ間の接続およびホストとネットワーク間の接続を可能にするプロトコル。PPP には、CHAP や PAP などのセキュリティ メカニズムが組み込まれています。

PPPoA

非同期転送モード（ATM）を介したポイントツーポイント プロトコル。主に ADSL の一部として実装される PPPoA は、RFC1483 に依存し、Logical Link Control-Subnetwork Access Protocol（LLC-SNAP）モードまたは VC-Mux モードで動作します。

PPPoE PPP over Ethernet。イーサネット フレームでカプセル化された PPP。PPPoE を使用すると、イーサネット ネットワーク上のホストをブロードバンド モデム経由でリモート ホストに接続できます。

PPTP ポイントツーポイント トンネリング プロトコル。パケットを TCP/IP ベースのネットワーク経由で送信できるように IP データグラムにカプセル化することによって、クライアントが開始するトンネルを作成します。L2F および L2TP トンネリング プロトコルの代わりに使用できます。PPTP は Microsoft 独自のプロトコルです。

PVC 相手先固定接続。永続的に確立されている仮想回線。特定の仮想回線が常に必要な状況で、回線の確立と切断に必要な帯域幅を節約できます。ATM 用語では、相手先固定接続といいます。

Q

QoS Quality of Service。指定されたタイプのトラフィックに対して帯域幅を保証する方法。

R

RA 登録機関。PKI システム内のオプション コンポーネントとして機能するエンティティであり、認証機関（CA）が証明書の発行時またはその他の証明書管理機能の実行時に使用する情報を記録または確認します。CA 自体はすべての RA 機能を実行できますが、CA と RA は一般に別にします。RA が担当する処理は多種多様ですが、識別名の割り当て、トークンの配信、個人の認証機能の実行などが含まれます。

RADIUS Remote Authentication Dial-In User Service。転送プロトコルとして UDP を使用する、アクセス サーバの認証およびアカウンティングのプロトコル。「TACACS+」も参照してください。

RCP リモート コピー プロトコル。ユーザが、ネットワーク上のリモート ホストまたはサーバに常駐するファイル システムからファイルをコピーしたり、そのファイル システムにファイルをコピーしたりできるプロトコル。RCP プロトコルはデータを確実に転送するために TCP を使用しています。

RFC 1483 ルーティング

RFC1483 には、ATM ネットワーク上でコネクションレス型ネットワークの相互接続トラフィックを伝送する方法として、ルーテッド PDU（プロトコル データ ユニット）とブリッジド PDU の 2 つが記述されています。Cisco CP では、RFC 1483 ルーティングの設定がサポートされ、AAL5MUX と AAL5SNAP の 2 つのカプセル化タイプを設定できます。

AAL5MUX：AAL5 MUX カプセル化は、1 つの PVC あたり 1 つのプロトコル（IP または IPX）をサポートします。

AAL5SNAP：AAL5 Logical Link Control/Subnetwork Access Protocol（LLC/SNAP）カプセル化は、Inverse ARP をサポートし、プロトコル データグラムの前に LLC/SNAP を組み込みます。これにより、同じ PVC 上で複数のプロトコルが使用できます。

RIP

ルーティング インフォメーション プロトコル。ルーティング メトリックとして、パケットが宛先に到達するまでに経由する必要のあるルータの数を使用するルーティング プロトコルです。

RPC

リモート プロシージャ コール。クライアントによって作成または指定され、サーバ上で実行されるプロシージャ コールであり、その結果はネットワーク経由でクライアントに返されます。「クライアント / サーバ コンピューティング」も参照してください。

RR

リスク評価。RR は、ネットワーク上の特定のイベントに伴うリスクの高さを 0 ～ 100 の範囲の数値で表します。

RSA

大きな数の因数分解に基づく暗号キー交換技術で、開発者の Rivest、Shamir、および Adelman の頭文字を取って名付けられました。RSA は技術そのものの名前でもあります。暗号化と認証に使用でき、多くのセキュリティ プロトコルで採用されています。

RSA キー

RSA の非対称キー ペアは、一致するパブリック キーとプライベート キーの組み合わせです。

RSA 署名

IPSec で提供される 3 つの認証方式の 1 つ。他の 2 つの方式は、RSA 暗号化 nonce と事前共有キーです。また、FIPS（Federal Information Processing Standards）が認める、デジタル署名の生成と確認のための 3 つのアルゴリズムのうちの 1 つでもあります。認められている他の 2 つのアルゴリズムは DSA と Elliptic Curve DSA です。

S

SA セキュリティ アソシエーション。特定のトンネルの指定セッションを保護するために 2 つのピア間で合意されたセキュリティ パラメータのセット。IKE と IPSec は SA を使用しますが、両方の SA は互いに独立しています。

IPSec SA は単方向であり、各セキュリティ プロトコルにおいて一意です。IKE SA は IKE によってのみ使用され、IPSec SA とは違って双方向です。IKE は IPSec に代わって SA のネゴシエーションと確立を行います。ユーザは IPSec SA を手動で確立することもできます。

保護されたデータ パイプに 1 セットの SA が必要であり、プロトコルごとに 1 方向あたり 1 つ必要です。たとえば、ピア間の ESP（Encapsulating Security Protocol）をサポートしているパイプでは、各方向に ESP SA が 1 つ必要です。SA は宛先（IPSec エンドポイント）アドレス、セキュリティ プロトコル（AH または ESP）、およびセキュリティ パラメータ インデックス（SPI）によって一意に識別されます。

SAID セキュリティ アソシエーション ID。特定のリンクの SA に割り当てられた数値識別子です。

salt 暗号をさらに複雑にするために使用される擬似ランダムな文字列。

SCCP Skinny クライアント制御プロトコル。SCCP は Cisco Systems が独自に開発した端末制御プロトコルです。SCCP は Skinny クライアントと Cisco CallManager 間のメッセージング プロトコルとして使用します。

SDEE Security Device Event Exchange。パケットがシグニチャの特性と一致したときに生成されるアラームなどのセキュリティ イベントの通知に使用されるメッセージ プロトコルの 1 つです。

SDF シグニチャ定義ファイル。通常は XML 形式のファイルで、セキュリティ デバイスにシグニチャをロードするために使用できるシグニチャ定義が含まれています。

SDP Secure Device Provisioning。SDD では、Trusted Transitive Introduction（TTI）を使用して、2 つのエンド デバイス間（たとえば、Cisco IOS クライアントと Cisco IOS 証明書サーバ間）に PKI を簡単に導入できます。

SEAF シグニチャ イベント アクション フィルタ。定義したパラメータに一致するイベントからアクションを抽出するフィルタです。たとえば、特定の攻撃者のアドレスに関連付けられたイベントから、TCP 接続をリセットするアクションを抽出する SEAF を作成できます。

SEAO シグニチャ イベント アクション オーバーライド。SEAO を使用すると、アラームなどの IPS イベント アクション タイプにリスク評価（RR）の範囲を割り当てることができます。アクション タイプに割り当てた範囲の RR を持つイベントが発生すると、このアクションがイベントに追加されます。前述の例では、アラームがイベントに追加されます。

SEAP Signature Event Action Processor。SEAP を使用すると、イベント リスク評価（ERR）のフィードバックに基づくフィルタリングおよびオーバーライドを実行できます。

SFR シグニチャの信頼度評価。ターゲットについての特定の情報が存在しない場合に、このシグニチャがどれだけ信頼できるかを示す重み付けです。

SHA 一部の暗号化システムでは、MD5 の代わりに Secure Hashing Algorithm を使用してデジタル署名を生成します。

SHA-1 Secure Hashing Algorithm 1。長さが 264 ビット以下のメッセージから 160 ビットのメッセージ ダイジェストを生成するアルゴリズム。メッセージ ダイジェストが大きいため、総当たり攻撃や反転攻撃に対するセキュリティが強化されます。SHA-1 [NIS94c] は、1994 年に公開された SHA の修正版です。

SIP Session Initiation Protocol。コール処理セッション、特に 2 者間の電話会議、つまり「コール」を可能にします。SIP はコール シグナリング対応の SDP（Session Description Protocol）と連動します。SDP はメディア ストリーム用のポートを指定します。SIP を使用すると、ルータは SIP VoIP（Voice over IP）ゲートウェイと VoIP プロキシ サーバをサポートできます。

SMTP シンプルメール転送プロトコル。電子メール サービスを提供するインターネット プロトコルです。

SNMP 簡易ネットワーク管理プロトコル。TCP/IP ネットワーク専用のネットワーク管理プロトコル。ネットワーク デバイスの監視および制御と、設定、統計情報の収集、パフォーマンス、およびセキュリティの管理を行う手段を提供します。

SPD Selective Packet Discard。キューの輻輳が発生したときに、ルーティング プロトコル パケットやその他の重要なトラフィック制御のレイヤ 2 キープアライブに優先権を与えます。

SRB ソースルート ブリッジング。IBM によって開発されたブリッジング方式であり、トークン リング ネットワークでは広く利用されています。SRB ネットワークでは、宛先までのルート全体がリアルタイムに決定されてから、データが宛先に送信されます。

SSH セキュア シェル。TCP/IP などの信頼性のあるトランスポート層で実行されるアプリケーションであり、強力な認証および暗号化機能を提供します。ルータ コンソールに同時にアクセスできる SSH クライアントは最大 5 つです。

SSID Service Set Identifier（無線ネットワーク名とも呼ばれます）。無線ネットワークの識別に使用する一意の識別子。ステーションが他のステーションやアクセス ポイントと通信するには SSID が必要です。SSID は最大 32 文字の英数字で構成します。

SSL セキュア ソケット レイヤ。電子商取引におけるクレジット カード番号の送信時など、安全なトランザクションを提供するために使用される Web 用の暗号化技術です。

SSL VPN Secure Socket Layer 仮想プライベート ネットワーク。対応する Cisco ルータで SSL VPN を使用すると、リモート クライアントが使用可能なブロードバンドまたは ISP ダイアル接続による暗号化トンネルをインターネット上に構築することで、リモート クライアントにネットワーク リソースへのセキュアなアクセスを提供できます。

SSL VPN グループ ポリシー SSL VPN グループ ポリシーでは、これらのポリシーに含まれるユーザのためのポータル ページとリンクを定義します。SSL VPN グループ ポリシーは、SSL VPN コンテキスト下で設定します。

SSL VPN ゲートウェイ SSL VPN ゲートウェイは、SSL VPN コンテキストに IP アドレスと証明書を提供します。

SSL VPN コンテキスト SSL VPN コンテキストは、企業イントラネットをはじめとする各種プライベート ネットワークへの安全なアクセスの設定に必要なリソースを提供します。SSL VPN コンテキストには、関連する SSL VPN ゲートウェイが含まれていなければなりません。SSL VPN コンテキストでは 1 つまたは複数の SSL VPN グループ ポリシーを採用することができます。

SUNRPC SUN リモート プロシージャ コール。RPC は、クライアントがリモート サーバ上でプログラムまたはルーチンを実行できるようにするためのプロトコルです。SUNRPC は当初、SUN Open Network Computing（ONC）ライブラリに配布されていた RPC バージョンです。

T

T1 T1 リンクは、1.5 Mbps の速度でデータを伝送できるデータ リンクです。

TACACS+ Terminal Access Controller Access Control System plus。転送プロトコルとして TCP を使用する、アクセス サーバの認証およびアカウンティングのプロトコル。

TCP 転送制御プロトコル。信頼性のある全二重データ転送を提供する接続指向のトランスポート層プロトコルです。

TCP Syn Flood 攻撃 Syn Flood 攻撃は、ハッカーが大量の接続要求をサーバに送信した場合に発生します。これらのメッセージには到達不可能な戻りアドレスが含まれているため、接続は確立できません。したがって、未解決のオープン状態の接続が大量に発生します。これにより、サーバが過負荷状態になり、有効な要求に対するサービスが拒否されるため、正規のユーザが Web サイトに接続したり、電子メールにアクセスしたり、FTP サービスを利用したりできなくなる可能性があります。

Telnet インターネットなどの TCP/IP ネットワーク用の端末エミュレーション プロトコル。Web サーバをリモートで制御するために一般に使用される方法です。

TFTP Trivial File Transfer Protocol。ファイル転送に使用される単純なプロトコルです。UDP 上で実行されます。詳細については、RFC（Request For Comments）1350 を参照してください。

TVR ターゲットの価値評価。TVR は、ユーザにとってのターゲット ホストの価値を示す、ユーザ定義の値です。これを使用すると、ユーザは重要なシステムに関連するイベントのリスクを高く設定し、価値の低いターゲットのイベントのリスクを低く設定できます。

U

UDP ユーザ データグラム プロトコル。TCP/IP プロトコルのコネクションレス型のトランスポート層プロトコルで、インターネット プロトコル ファミリに属しています。

Unity クライアント Unity Easy VPN サーバのクライアント。

URI ユニフォーム リソース識別子。インターネット オブジェクト名をカプセル化し、名前空間の ID を割り当てた形式の識別子です。これにより、登録済み名前空間におけるユニバーサルな名前セットの名前を持ち、登録済みのプロトコルまたは名前空間を参照するアドレスを持つメンバを生成できます。[RFC 1630]

URL Universal Resource Locator。ブラウザを使用してハイパーテキスト文書やその他のサービスにアクセスするときの標準化されたアドレス指定方法。次に、2 つの例を示します。

http://www.cisco.com.

ftp://10.10.5.1/netupdates/sig.xml

V

VCI 仮想チャネル識別子。仮想パスには、個々の接続に対応する複数の仮想チャネルが存在する場合があります。VCI は使用されているチャネルを識別します。VPI と VCI の組み合わせによって ATM 接続が識別されます。

VFR Virtual Fragment Reassembly。IP フラグメントをブロックできるように、IOS Firewall が ACL をダイナミックに作成することを可能にします。IP フラグメントには、十分な情報が含まれていない場合が多いため、スタティック ACL によるフィルタが適用できないことがあります。

VoIP Voice over IP。IP ベースのインターネットにより、POTS（従来からある通常の電話サービス）同様の機能、信頼性、および音質で通常のテレフォニー形式の音声を搬送する機能。VoIP により、IP ネットワークを使用してルータから音声トラフィック（通話呼やファックスなど）を搬送できるようになります。

VPDN バーチャル プライベート ダイヤルアップ ネットワーク。ホーム ネットワークから離れた場所にダイヤルイン ネットワークを配置できるシステムであり、外見上は直接接続されているように見えます。VPDN は L2TP と L2F を使用して、ネットワーク接続のレイヤ 2 以上の部分を NAS（ネットワーク アクセス サーバ）ではなくホーム ゲートウェイで終端します。

VPI 仮想パス識別子。ATM 接続で使用される仮想パスを識別します。

VPN 仮想プライベート ネットワーク。パブリック インフラストラクチャを使用するユーザに、プライベート ネットワークを使用する場合と同様のネットワーク接続を提供します。VPN では、あるネットワークから別のネットワークへのすべてのトラフィックを暗号化することにより、IP トラフィックをパブリック TCP/IP ネットワークを介して安全に転送できます。VPN はトンネリングを使用して、すべての情報を IP レベルで暗号化します。

VPN 接続

サイト間 VPN。サイト間 VPN はピア間の VPN 接続のセットで設定され、各接続の定義属性には次のデバイス設定情報が含まれています。

- 接続名
- IKE ポリシーと事前共有キー（オプション）
- IPSec ピア
- この接続で保護する 1 つ以上のリモート サブネットまたはホストのリスト
- 暗号化するトラフィックを定義する IPSec ルール
- 保護するトラフィックの暗号化方法を定義するトランスフォーム セットのリスト
- 接続を適用するデバイス ネットワーク インターフェイスのリスト

VPN ミラー ポリシー

リモート システム上の VPN ポリシーであり、ローカル ポリシーと互換性のある値と、リモート システムとローカル システム間の VPN 接続を確立するために必要な値が含まれます。ミラー ポリシーの中には、ローカル ポリシーとの値の一致を必要とするものがあります。また、ピアの IP アドレスのように、ローカル ポリシーで対応する値とは逆の値とすることが必要なものもあります。

サイト間 VPN 接続を設定するときに、リモート管理者が使用するミラー ポリシーを作成できます。ミラー ポリシーの生成方法の詳細については、「ミラーの生成 ...」を参照してください。

VTI

仮想テンプレート インターフェイス。

vty

仮想端末。一般に、仮想端末回線の意味で使用されています。

W

WAAS

Wide Area Application Services。ワイド エリア ネットワークの規模で TCP ベースのアプリケーションのパフォーマンスを最適化する、Cisco のソリューション。

WAE

広域アプリケーション エンジン。この用語は、WAN の最適化とアプリケーションの高速化を実現する、Cisco のネットワーク アプライアンスを指します。

WAE-C

WAE-Core。コア WAE コンポーネントは、データセンターのサーバにインストールします。WAE-C は、ファイル サーバまたはネットワーク接続ストレージ（NAS）デバイスに直接接続します。

WAE-E

WAE-Edge。エッジ WAE はクライアントにインストールします。WAE-E はリモート サイトや支店のクライアント要求を処理するファイル キャッシング デバイスです。

WAN ワイドエリア ネットワーク。地理的に広範囲にわたるユーザにサービスを提供するネットワークであり、一般には、一般通信事業者が提供する転送デバイスが使用されます。「LAN」も参照してください。

WCCP Web Cache Communication Protocol。Web Cache Control Protocol および Web Cache Coordination Protocol とも呼ばれます。WCCP では、コンテンツ エンジンを使用して Web トラフィックを削減できるので、伝送コストを低減でき、Web サーバからのダウンロード時間も短縮できます。

WFQ Weighted Fair Queuing。次の 2 点を同時に処理する、フローベースのキューイング アルゴリズム。対話型トラフィックをキューの先頭に置くスケジュールを設定して応答時間を短縮するとともに、高い帯域幅を必要とするフローどうしで残りの帯域幅を平等に分配します。

WINS Windows Internet Naming Service。特定のネットワーク コンピュータに関連付けられた IP アドレスを決定する Windows システム。

WMM Wi-Fi Multimedia。Quality of Service（QoS）を扱う IEEE 802.11e のドラフト段階規格。WMM に準拠した機器は、Wi-Fi 無線接続を通じてオーディオ、ビデオ、および音声を扱うアプリケーションで高度なユーザ環境を実現するように設計されています。

WRED 重み付けランダム早期検出。輻輳時に優先度の高いトラフィックの損失率が他のトラフィックの損失率よりも低くなるようにするキューイング方式。

X

X.509 デジタル証明書の標準であり、証明書の構造を規定しています。主なフィールドは、ID、サブジェクト フィールド、有効期間、パブリック キー、CA 署名です。

X.509 証明書 X.509 ガイドラインに従った構造を持つデジタル証明書。

X.509 証明書失効リスト（CRL） 失効した証明書の番号のリスト。X.509 CRL は、X.509 で定義されている 2 つの CRL フォーマットのどちらかに従います。

XAuth IKE Extended Authentication。Xauth を使用すると、Cisco IOS ソフトウェアのすべての AAA 認証方式で、IKE 認証フェーズ 1 の交換後にユーザ認証を別のフェーズで実行できます。ユーザ認証を実行するには、AAA 設定のリスト名と Xauth 設定のリスト名が一致する必要があります。

Xauth は IKE の拡張であり、IKE 認証に代わるものではありません。

Z

ZPF

ゾーンベースのポリシー ファイアウォール。ZPF 構成では、各インターフェイスはゾーンに割り当てられ、ゾーン間を流れるトラフィックにインスペクション ポリシーが適用されます。

あ

アクセス コントロール、アクセス コントロール ルール

設定に入力される情報であり、インターフェイスへの通過を許可または拒否するトラフィック タイプを指定できます。デフォルトでは、明示的に許可されていないトラフィックは拒否されます。アクセス コントロール ルールは、アクセス コントロール エントリ（ACE）で設定されています。

アグレッシブ モード

ISAKMP SA を確立するモードであり、2 台以上の IPSec ピア間の IKE 認証のネゴシエーション（フェーズ 1）が簡略化されます。アグレッシブ モードはメイン モードより高速ですが、安全性は低くなります。「メイン モード（クイック モード）」を参照してください。

アドレス変換

ネットワーク アドレスまたはポートを別のネットワーク アドレスまたはポートに変換すること。「IP アドレス」、「NAT」、「PAT」、「スタティック PAT」も参照してください。

アルゴリズム

問題解決手順の論理シーケンス。セキュリティ アルゴリズムは、データ暗号化または認証のどちらかに関係します。

データ暗号化アルゴリズムの例として、DES と 3DES があります。

暗号化 / 復号化アルゴリズムには、ブロック暗号、CBC、NULL 暗号、ストリーム暗号などがあります。

認証アルゴリズムには、MD5、SHA などのハッシュが含まれます。

暗号

暗号化 / 復号化アルゴリズム。

暗号化

データに特定のアルゴリズムを適用してそのデータの外観を変更し、情報の参照を許可されていないユーザが理解できない状態にすること。

暗号化する

平文から暗号文を生成すること。

暗号化なし

暗号化されていないこと。

暗号文 復号化される前の、暗号化された、読めない状態のデータ。

暗号法 データの秘密性と確実性を保持し、データの変更や否認を防ぐための数学的および科学的な技術。

暗号マップ Cisco CP では、暗号マップを使用して、IPSec で保護するトラフィックのタイプ、IPSec で保護するデータの送信先、およびこのトラフィックに適用する IPSec トランスフォーム セットを指定します。

暗黙のルール デフォルト ルールに基づいて、またはユーザ定義のルールの結果として、ルータにより自動的に作成されるアクセス ルール。

イーサネット 広く使用されている LAN プロトコルで、Xerox Corporation によって発明され、Xerox、Intel、および Digital Equipment Corporation によって開発されました。イーサネット ネットワークは CSMA/CD 方式を採用し、さまざまなタイプのケーブル上で運用されます。その伝送速度は 10 Mpbs または 100 Mbps です。イーサネットは IEEE 802.3 シリーズの標準に似ています。

イベント アクション オーバーライド IOS IPS 5.x で使用されます。イベント アクション オーバーライドを使用すると、イベントの RR に基づき、このイベントに関連付けられたアクションを変更できます。

イベント アクション オーバーライド

インスペクション ルール CBAC インスペクション ルールを使用すると、ルータは指定されたアウトバウンド トラフィックを検査して、LAN 上で開始されたセッションに関連付けられている同じタイプのリターン トラフィックを許可できます。ファイアウォールが存在する場合、インスペクション ルールが設定されていなければ、ファイアウォールの内部で開始されたセッションに関連付けられているインバウンド トラフィックは破棄される可能性があります。

インターネット IP（インターネット プロトコル）を使用するグローバル ネットワーク。LAN ではありません。「イントラネット」も参照してください。

インターフェイス 特定のネットワークとルータ間の物理的な接続。ルータの LAN インターフェイスはルータのローカル ネットワークに接続します。ルータには、インターネットに接続する WAN インターフェイスが 1 つ以上あります。

イントラネット イントラネットワーク。IP、および SNMP、FTP、UDP などのインターネット プロトコルを使用する LAN。「ネットワーク」、「インターネット」も参照してください。

エコー 「ping」、「ICMP」を参照してください。

エンロールメント URL エンロールメント URL は、認証機関（CA）への HTTP パスです。Cisco IOS ルータはこのパスを使用して証明書要求を送信します。URL には DNS 名または IP アドレスが含まれます。URL の後に CA スクリプトへの完全パスが続くこともあります。

か

外部グローバル 外部ネットワーク上のホストの所有者によってそのホストに割り当てられた IP アドレス。アドレスはグローバルにルート指定可能なアドレスまたはネットワーク空間から割り当てられます。

外部ローカル 外部ホストを内部ネットワークから見たときの IP アドレス。必ずしも正規のアドレスではなく、内部でルート指定可能なアドレス空間から割り当てられます。

拡張ルール アクセス ルールのタイプ。拡張ルールでは、さまざまなパケット フィールドを検査して条件に一致するかどうかを判断できます。検査できるフィールドは、パケットの送信元と宛先の IP アドレス、プロトコル タイプ、送信元と宛先のポート、およびその他のパケット フィールドです。

カプセル化 データを特定のプロトコル ヘッダーに包み込むこと。たとえば、イーサネット データは、ネットワークに送信される前に特定のイーサネット ヘッダーに包み込まれます。また、異種ネットワークを相互接続する場合、一方のネットワークのフレーム全体が他方のネットワークのデータ リンク層プロトコルで使用されるヘッダーに単純に配置されます。

キー データの暗号化 / 復号化、またはメッセージ ダイジェストの計算に使用されるビット文字列。

キー エスクロー 暗号キーを保持する、信頼できる第三者。

キー ペア 「パブリック キー暗号化」を参照してください。

キー ライフタイム キー ペアの属性で、そのキー ペアのパブリック キーを含む証明書が有効である期間を指します。

キー リカバリ 紛失や破損のために復号キーを使用できなくなった場合に、暗号化された情報の復号化を可能にする、信頼できる方法。

キー管理 暗号キーの作成、配信、認証、および保管。

キー合意 2 人以上の当事者が同じ秘密対称キーを使用することに合意するプロセス。

キー交換 2 人以上の当事者が暗号キーを交換する方法。IKE プロトコルはその 1 つの方法を提供します。

擬似ランダム 表面上は本当にランダムなシーケンスのように見える規則正しいビット シーケンス。擬似乱数によって生成されたキーは、nonce と呼ばれます。

キャッシュ これまでのタスクの実行によって蓄積された情報の一時的な保管場所。再利用が可能であるため、タスクの実行に必要な時間が短縮されます。

キューイング トラフィック キューイングは、パケット ストリームを複数のキューに集約して、キューごとに異なるサービスを提供します。「LLQ」および「CBWFQ」も参照してください。

共有キー 対称キーベースの通信セッションで、すべてのユーザが共有するプライベート キー。

共有プライベート キー 暗号キー。

クイック モード Oakley において、セキュリティ アソシエーションの確立後に、セキュリティ サービスの変更（新しいキーなど）をネゴシエートするために使用されるメカニズムの名前。

クライアント / サーバ コンピューティング トランザクション処理がクライアント（フロント エンド）とサーバ（バック エンド）の 2 つの部分に分割される分散コンピューティング（処理）ネットワーク システムを表す用語。分散コンピューティングとも呼ばれます。「RPC」も参照してください。

クラス マップ ポリシー マップに指定されたアクションに従って処理するトラフィクを指定するために、ゾーンベースのポリシーで使用します。クラス マップでは、トラフィックのタイプを指定できるほか、トラフィックの送信元と宛先を定義する ACL も指定できます。

クリア チャネル 暗号化されていないトラフィックを転送できるチャネル。クリア チャネルでは、転送データにセキュリティ制限は適用されません。

クリアテキスト 暗号化されていないテキスト。*平文*とも呼ばれます。

グローバル IKE ポリシー デバイス上の 1 つのインターフェイスだけでなく、そのデバイス全体に適用される IKE ポリシー。

検証 ユーザまたはプロセスの識別情報を確認すること。

コンテンツ エンジン WAAS ソリューションの関連では、ネットワーク上に配置した、Web コンテンツのキャッシュを指します。

コンフィギュレーション、コンフィギュレーション ファイル Cisco CP を使用して管理できる設定、ユーザ設定、およびプロパティが格納されているルータ上のファイル。

さ

サイト間 VPN 一般に、サイト間 VPN とは、いくつかの条件を満足した上で 2 つのネットワークまたはサブネットワークを接続する VPN です。この条件としては、トンネルの両側でスタティック IP アドレスを使用すること、ユーザ側のステーションに VPN クライアント ソフトウェアがないこと、中央の VPN ハブ（ハブアンドスポークの VPN 設定に存在するようなハブ）がないことなどがあります。サイト間 VPN は、リモート ユーザまたはモバイル ユーザによるダイヤルイン アクセスに代わるものではありません。

サブネット ビット

サブネット マスク IP で使用される 32 ビットのアドレス マスクであり、ネットワーク アドレスとオプションのサブネット アドレスに使用する IP アドレスのビットを示します。サブネット マスクは 10 進数で表現されます。マスク 255.255.255.0 では、アドレスの最初の 24 ビットを指定します。単に「マスク」と呼ばれることもあります。「マスク」と「IP アドレス」も参照してください。

サブネット、サブネットワーク IP ネットワークにおいて、特定のサブネット アドレスを共有するネットワーク。サブネットワークは、ネットワーク管理者が任意に分割したネットワークです。マルチレベルの階層ルーティング構造が提供され、接続されたネットワークの複雑なアドレス指定を回避できます。「IP アドレス」、「サブネット ビット」、「サブネット マスク」も参照してください。

シェーピング トラフィック シェーピングでは、超過パケットをキューに保持しておき、後で時間をかけてこの超過分を伝送するようにスケジューリングを設定し直します。

シグニチャ エンジン 特定のカテゴリに属する多数のシグニチャをサポートするように設計された、Cisco IOS IPS のコンポーネント。エンジンは解析機能と検査機能とで構成されます。各エンジンは、値の有効範囲または有効値のセットを持つ正規のパラメータを保持します。

失効パスワード ルータのデジタル証明書の失効を要求するときに CA に提供するパスワード。*チャレンジ パスワード*と呼ばれることもあります。

事前共有キー

IPSec で提供される 3 つの認証方式の 1 つ。他の 2 つの方式は、RSA 暗号化 nonce と RSA 署名です。事前共有キーを使用すると、個別の共有プライベート キーを使用する 1 つ以上のクライアントが IKE を使用してゲートウェイへの暗号化されたトンネルを認証できます。事前共有キーは、一般に小規模ネットワーク（最大 10 クライアント）で使用されます。事前共有キーを使用すると、セキュリティのために CA を使用する必要がなくなります。

Diffie-Hellman キー交換は、パブリック キーとプライベート キーを組み合わせて共有プライベート キーを作成します。作成されたキーは IPSec ピア間の認証に使用されます。共有プライベート キーは、2 台以上のピアで共有できます。各ピアで、共有プライベート キーを IKE ポリシーの一部として指定します。通常、この事前共有キーの配信には、安全な帯域外チャネルが使用されます。事前共有キーを使用する場合は、いずれかのピアに同じ事前共有キーが設定されていないと IKE SA を確立できません。IKE SA は IPSec SA の前提条件です。事前共有キーはすべてのピアに設定する必要があります。

デジタル証明書とワイルドカードの事前共有キー（共有プライベート キーを使用する 1 つ以上のクライアントがゲートウェイへの暗号化されたトンネルを認証できるようにする）を事前共有キーの代わりに使用できます。デジタル証明書とワイルドカードの事前共有キーは両方とも事前共有キーよりもスケーラブルです。

証明書

「デジタル証明書」を参照してください。

証明書 ID

X.509 証明書には、その証明書を所有するデバイスまたはエンティティを識別する情報が含まれています。この識別情報は、以降に行われるピアの確認および認証のたびに検査されます。ただし、証明書 ID は、スプーフィング攻撃を受けやすくなる場合があります。

署名

ネットワークでのデータの誤使用を表す特定パターンを検出する、IOS IPS 内のデータ要素。

署名証明書

メッセージまたは文書にデジタル署名を関連付けたり、メッセージまたはファイルが伝送中に変更されなかったことを証明したりするために使用されます。

信頼度評価

シグニチャが正確なアラートを生成するかどうかに対し、評価者の信頼を示す 1 ～ 100 までの値。

スタティック PAT

スタティック ポート アドレス変換。スタティック アドレスは、ローカル IP アドレスをグローバル IP アドレスにマッピングします。スタティック PAT は、ローカル ポートのグローバル ポートへのマッピングも行うスタティック アドレスです。「PAT」も参照してください。

スタティック ルート
明示的に設定され、ルーティング テーブルに追加されているルート。スタティック ルートは、ダイナミック ルーティング プロトコルによって選択されるルートより優先されます。

ステート、ステートフル、ステートフル インスペクション
ネットワーク プロトコルでは、2 台のホスト間のネットワーク接続の両端に、ステート情報と呼ばれる特定のデータを保持します。ステート情報は、保証付きパケット配信、データの順序付け、フロー制御、トランザクション ID やセッション ID などのプロトコル機能を実装するために必要です。一部のプロトコル ステート情報は、プロトコルの使用中に各パケットに含めて送信されます。たとえば、Web サーバに接続された Web ブラウザは、HTTP とサポートされている TCP/IP プロトコルを使用します。各プロトコル レイヤは送受信するパケット内にステート情報を保持します。ルータは各パケット内のステート情報を調べて、その情報が最新であり、情報に含まれるどのプロトコルに対しても有効であることを確認します。この機能はステートフル インスペクションと呼ばれ、特定のタイプのコンピュータ セキュリティ脅威に対する強力な防壁を構築します。

スプーフィング
スプーフ
パケットが送信元のアドレスを偽ること。スプーフィングは、フィルタやアクセス リストなどのネットワーク セキュリティ メカニズムを回避するように設計されます。

スプリット DNS
スプリット DNS では、選択した仮想 DNS ネーム サーバで指定する内部ホスト名キャッシュを使用して、Cisco ルータから DNS クエリに応答できます。このホスト名キャッシュにある情報を使用しても応答できないクエリは、指定されたバックエンドの DNS ネーム サーバにリダイレクトされます。

スポーク
DMVPN ネットワークでは、スポーク ルータはネットワーク内の論理的なエンド ポイントであり、DMVPN ハブ ルータとのポイントツーポイントの IPSec 接続を確立しています。

セキュリティ アソシエーション ライフタイム
事前に決定された SA の有効期間。

セキュリティ ゾーン
ポリシーを適用可能なインターフェイス グループ。セキュリティ ゾーンは、類似した機能または特徴を共有するインターフェイスで構成する必要があります。たとえば、ルータ上で Ethernet 0/0 および Ethernet 0/1 というインターフェイスがローカル LAN に接続されているとします。この 2 つのインターフェイスはどちらも内部ネットワークを表すため、互いに類似しています。したがって、これらを 1 つのゾーンにグループ化してファイアウォール設定を適用することができます。

セッション キー
一度だけ使用されるキー。

ゾーン ゾーンベース ポリシー ファイアウォールにおいて、類似する機能または特徴を備えるインターフェイスのグループ。たとえば、FastEthernet 0/0 および FastEthernet 0/1 というインターフェイスが LAN に接続されている場合、これらを 1 つのゾーンとしてグループ化することができます。

ゾーンペア ゾーンペアを使用すると、2 つのセキュリティ ゾーン間を流れる単方向トラフィックを指定できます。「セキュリティ ゾーン」も参照してください。

た

対称キー 暗号化されている情報を復号化するために使用されます。

ダイジェスト ハッシュ関数の出力。

ダイナミック ルーティング ネットワーク トポロジまたはトラフィックの変更に合わせて自動的に調整されるルーティング。適応型ルーティングとも呼ばれます。

単一の DMVPN 単一の DMVPN 設定を持つルータは、1 台の DMVPN ハブに接続し、1 つの設定済み GRE トンネルを使用して DMVPN 通信を行います。ハブ アンド スポークの GRE トンネル アドレスは同じサブネット内に存在する必要があります。

チェックサム 転送データの整合性を確認するための計算方法であり、一連の算術演算で得られたオクテットのシーケンスから計算されます。受信側で値を再計算し、送信側の値と比較して整合性を確認します。

テールエンド トンネルのダウンストリームの受信側。

データの機密性 認証されていないユーザ、エンティティ、またはプロセスに対する情報の開示を防ぐためのデータ暗号化によってもたらされる成果。このような情報には、アプリケーション レベルのデータまたは通信パラメータがあります。「トラフィック フローの機密性またはトラフィック解析」を参照してください。

データの整合性 転送データが正確であると推定されること。送信者が信頼でき、データが変更されていないことを示します。

データ発信元認証 否認防止サービスの機能の 1 つ。

デジタル証明書 ユーザまたはデバイスの属性をデジタル表現し、暗号署名を付加したもので、キーを ID に関連付けます。パブリック キーに付加された固有の証明書によって、キーが改ざんされていないことが証明されます。証明書は、信頼できる認証機関によって発行および署名され、パブリック キーをその所有者に対応付けます。一般に、証明書には、所有者の名前とパブリック キー、および証明書のシリアル番号と有効期限が含まれます。その他の情報が含まれる場合もあります。「X.509」を参照してください。

デジタル署名 データの偽造を簡単に検出し、否認を防止する認証方式。さらに、デジタル署名を使用することで、送信データがそのまま受信されたかどうかも確認できます。一般に、送信タイム スタンプが含まれます。

デフォルト ゲートウェイ 最後の手段として使用されるゲートウェイ。パケットの宛先アドレスがルーティング テーブル内のどのエントリにも一致しない場合、パケットはこのゲートウェイにルーティングされます。

デルタ ファイル 署名への変更を保存するために Cisco IOS IPS によって作成されるファイル。

登録プロキシ ホスト 証明書登録サーバのプロキシ サーバ。

トラフィック フローの機密性またはトラフィック解析 通信パラメータの不正開示を防止するセキュリティ概念。この概念の実装に成功すると、送信元と宛先の IP アドレス、メッセージの長さ、および通信の頻度を不正ユーザから隠すことができます。

トランスフォーム セキュリティ プロトコルおよび対応するアルゴリズムの記述。

トランスフォーム セット IPSec で保護するトラフィックに適用できるセキュリティ プロトコル、アルゴリズム、およびその他の設定の組み合わせ。IPSec セキュリティ アソシエーションのネゴシエートで、ピアは特定のトランスフォーム セットを使用して特定のデータ フローを保護することで互いに合意します。

トンネリング あるプロトコルのストリームを別のプロトコルを介して送信するプロセス。

トンネル インターネットなどの共有手段を使用する仮想チャネルであり、カプセル化されたデータ パケットの交換に使用されます。

同一アドレッシング ネットワーク アドレス変換を使用し、EasyVPN 接続によって同一の IP アドレスを持つデバイスにアクセスする機能。

ドメイン名 インターネット上のホストのわかりやすく覚えやすい名前であり、IP アドレスに対応しています。

な

内部グローバル ネットワークの外部にあるデバイスから見た場合のネットワークの内部にあるホストの IP アドレス。

内部ローカル ネットワークの内部のホストに割り当てられた設定済み IP アドレス。

認証 セキュリティにおけるユーザまたはプロセスの識別情報の検証。認証では、データ ストリームが転送中に変更されていないことを確認し、データ ストリームの発信元を確認することによって、データ ストリームの整合性を立証します。

認証する 利用者が本人であることを確認すること。

ネットワーク ネットワークは、1 台のホストではなく IP アドレス空間の一部を共有するコンピューティング デバイスのグループです。IP アドレスを持つ複数の「ノード」またはデバイス（*ホスト*と呼ばれる場合もあります）で構成します。「インターネット」、「イントラネット」、「IP」、「LAN」も参照してください。

ネットワーク ビット サブネット マスクにおいて、2 進数の 1 に設定されたビットの数。サブネット マスク 255.255.255.0 は、マスクの 24 ビットが 1 に設定されているため、24 個のネットワーク ビットを持ちます。サブネット マスク 255.255.248 は、17 個のネットワーク ビットを持ちます。

ネットワーク モジュール ルータに機能を追加するために、ルータ シャーシにインストールされたネットワーク インターフェイス カード。たとえば、イーサネット ネットワーク モジュール、IDS ネットワーク モジュールなどがあります。

は

ハッシュ 任意のサイズの入力を、*メッセージ ダイジェスト*または単に*ダイジェスト*とも呼ばれる固定サイズのチェックサム出力に変換する単方向のプロセス。このプロセスは不可逆であるため、特定のダイジェストが生成されるようにデータを作成または変更することはできません。

ハッシュ アルゴリズム ハッシュ アルゴリズムは、メッセージ ダイジェストとも呼ばれるハッシュ値の生成に使用され、メッセージの内容が送信中に変更されていないことを保証します。最も広く使用されている 2 つのハッシュ アルゴリズムは、Secure Hash Algorithm（SHA）と MD5 です。

ハブ

DMVPN ネットワークでは、ハブはネットワーク内のすべてのスポーク ルータへのポイントツーポイント IPSec 接続を行うルータです。DMVPN ネットワークの論理的な中心になります。

バースト レート

トラフィック バーストの上限となるバイト数。

パスワード

保護された秘密の文字列（または他のデータ ソース）であり、特定のユーザまたはエンティティの識別情報に関連付けられます。

パスワード エージング

パスワードの有効期限が切れたことをユーザに通知し、新しいパスワードを作成する手段を提供するシステムの機能。

パスワード エージング

パディング

暗号システムにおける*パディング*は、メッセージの最初と最後にランダムな文字、空白、ゼロ、および null を追加することを意味します。これは、メッセージの実際の長さを隠したり、暗号のデータ ブロック サイズの要件を満たすために行われます。また、パディングにより、暗号コードの実際の開始位置もわかりにくくなります。

パブリック キー暗号化

パブリック キー暗号化システムでは、すべてのユーザにパブリック キーとプライベート キーが割り当てられます。各プライベート キーは、1 人のユーザだけが保持し、他のユーザとは共有されません。プライベート キーは固有のデジタル署名の生成やパブリック キーで暗号化された情報の復号化に使用されます。一方、ユーザのパブリック キーは誰でも使用でき、そのユーザ宛ての情報を暗号化したり、そのユーザのデジタル署名を確認したりできます。パブリック キー暗号法と呼ばれることもあります。

パラメータ マップ

パラメータ マップでは、サービス拒否攻撃からの保護、セッション タイマーと接続タイマー、ログ記録設定などのパラメータに対し、ゾーンポリシー ファイアウォールによるインスペクションの動作を指定します。また、パラメータ マップをレイヤ 7 クラス マップおよびポリシー マップと共に適用して、アプリケーション固有の動作を定義することもできます。たとえば、HTTP オブジェクト、POP3 および IMAP 認証要件、およびその他のアプリケーション固有の情報を指定できます。

非対称暗号化

*パブリック キー システム*とも呼ばれます。この方法では、ある人が誰か他の人のパブリック キーにアクセスし、そのキーを使用してその人に暗号化されたメッセージを送信できます。

非対称キー

数学的に関連している 1 対の暗号キー。パブリック キーで暗号化された情報はプライベート キーでしか解読できず、その逆も成り立ちます。また、プライベート キーを使って署名されたデータはパブリック キーでのみ認証可能です。

否認

暗号システムにおける否認とは、通信の当事者が、その通信の全部または一部に関与した事実を否定することを意味します。

否認防止サービス　すべての通信データの送信元と宛先に関する証拠を保管して、後で取得できるようにするサードパーティのセキュリティ サービス。実際のデータは保管されません。この証拠は、送信者が情報を送信した事実を否定したり、受信者が情報を受信した事実を否定したりできないように、その通信のすべての当事者を保護するために使用できます。

標準ルール　Cisco CP におけるアクセス ルールまたは NAT ルールのタイプ。標準ルールは、パケットの送信元 IP アドレスを IP アドレス条件と照合して、一致するかどうかを判断します。一致する必要のある IP アドレス部分は、ワイルドカード マスクを使用して指定します。

平文　通常の暗号化されていないデータ。

ピア　IKE の場合、ピアは、IKE トンネルに関与するデバイスのプロキシとして機能するルータです。IPSec の場合、ピアは、キー交換またはデジタル証明書の交換によって安全に通信するデバイスまたはエンティティです。

ピアツーピア　すべてのホストがほぼ同等の機能を共有するネットワーク設計。ピアツーピア ネットワーキングは P2P とも呼ばれ、多くのファイル共有ネットワークで使用されます。

ファイアウォール　接続されたすべてのパブリック ネットワークとプライベート ネットワークの間のバッファとして指定された、単一または複数のルータまたはアクセス サーバ。ファイアウォール ルータは、アクセス リストとその他の手段を使用してプライベート ネットワークのセキュリティを確保します。

フィンガープリント　CA 証明書のフィンガープリントは、CA 証明書全体に対する MD5 ハッシュによって得られた英数字の文字列です。CA 証明書を受け取ったエンティティは、そのフィンガープリントを既知のフィンガープリントと比較することによって、証明書が本物であるかどうかを確認できます。この認証の目的は、「man-in-the-middle」攻撃を防止することによって通信セッションの整合性を保証することです。

復号化　暗号化されたデータに対し、逆方向に暗号化アルゴリズムを適用することによって、データを元の暗号化されていない状態に戻す操作。

フラッシュ
フラッシュ メモリ　電源を切ってもデータが保持されるメモリ チップ。必要に応じてソフトウェア イメージをフラッシュに格納したり、フラッシュからブートしたり、フラッシュに書き込んだりすることができます。

フレーム リレー　接続されたデバイス間で HDLC カプセル化を使用して複数の仮想回線を処理する、業界標準のスイッチ データ リンク層プロトコル。フレーム リレーは X.25 よりも効率的であり、一般に X.25 に代わるものと考えられています。

物理インターフェイス ネットワーク モジュールによってサポートされているルータ インターフェイスで、ルータ シャーシにインストールされているか、またはルータの基本ハードウェアの一部です。

分散キー いくつかの部分に分割され、それぞれ異なる当事者に配信される共有暗号キー。

プライベート キー 「対称キー」を参照してください。

プライベート キー 「パブリック キー暗号化」を参照してください。

ヘッドエンド トンネルのアップストリームの送信側。

ホスト 個別の IP アドレスおよびオプションの名前が関連付けられた、コンピュータ（PC など）または他のコンピューティング デバイス（サーバなど）。TCP/IP ネットワーク上で IP アドレスを持つすべてのデバイスを意味します。また、任意のネットワーク上の、ネットワーク アドレス指定が可能な任意のデバイスでもあります。「ノード」には、通常は「ホスト」と呼ばれないルータやプリンタなどのデバイスも含まれます。

ポスチャ NAC 実装において、ネットワークへのアクセスを試みるホストの状態。ホストで稼働しているポスチャ エージェント ソフトウェアが NAD と通信して、ネットワークのセキュリティ ポリシーとのホストの準拠状況を通知します。

ポリシー マップ トラフィックに対して実行するアクションを規定します。トラフィックはクラス マップで定義されます。1 つのポリシー マップに複数のクラス マップを関連付けることができます。

ポリシング トラフィック ポリシングでは、バーストを伝搬します。設定されている最大レートにトラフィック レートが達すると、超過トラフィックは廃棄されるか、再マーキングされます。

ポリシング レート トラフィックの上限となる 1 秒あたりのビット数。

ま

マスク

サブネット マスク

ネットマスク

ネットワーク マスク

インターネット アドレスをネットワーク、サブネット、およびホスト部に分割する方法を指定する 32 ビットのビット マスク。ネット マスクでは、ネットワークおよびサブネット部に使用されるビット位置に 1、ホスト部に使用されるビット位置に 0 がセットされます。このマスクでは、アドレス クラスで定義した標準のネットワーク部を必ず指定し、サブネット フィールドをネットワーク部の隣に記述する必要があります。マスクは 2 進数の値を 10 進数に変換して設定します。

例：

10 進数：255.255.255.0
2 進数：11111111 11111111 11111111 00000000
先頭から 24 ビットはネットワーク アドレスとサブネットワーク アドレス、最後の 8 ビットはホスト アドレスです。

10 進数：255.255.255.248
2 進数：11111111 11111111 11111111 11111000
先頭から 29 ビットはネットワーク アドレスとサブネットワーク アドレス、最後の 3 ビットはホスト アドレスです。

「IP アドレス」、「TCP/IP」、「ホスト」、「ホスト / ネットワーク」も参照してください。

メッセージ ダイジェスト

大きいデータ ブロックを表現するビット文字列。この文字列は、128 ビット ハッシュ関数による正確な内容の処理に基づいてデータ ブロックを定義します。メッセージ ダイジェストはデジタル署名の生成に使用されます。「ハッシュ」を参照してください。

や

有効期限

証明書またはキーに指定されている有効期限は、ライフタイムの最終日時を示します。有効期限が過ぎると、証明書またはキーは信頼されなくなります。

ら

ライフ サイクル

「有効期限」を参照してください。

リプレイ検出 シーケンス番号と認証を組み合わせた標準の IPSec セキュリティ機能。通信の受信者は、リプレイ攻撃を防止するために、古いパケットまたは重複したパケットを拒否できます。

リモート サブネット サブネットワークは、ネットワーク管理者がサブネット マスクによって任意に分割した IP ネットワークです。マルチレベルの階層ルーティング構造が提供され、接続されたネットワークの複雑なアドレス指定を回避できます。「リモート サブネット」は、送信側に関連付けられていないサブネットです。

ルート インターネットワークを通るパス。

ルート CA 最上位の認証機関（CA）で、下位の CA の証明書に署名します。ルート CA には、固有のパブリック キーが含まれる自己署名した証明書があります。

ルート マップ ルート マップを使用すると、ルーティング テーブルに追加する情報を制御できます。IP アドレスによっては、NAT によるアドレス変換後にパケットが IPSec ルールの条件に一致しなくなることがあります。Cisco CP ではルート マップを自動的に作成しておき、このような場合には送信元アドレスを NAT で変換できないようにします。

ループバック ループバック テストでは、送信された信号は、通信パスをたどってある地点から送信元に戻ってきます。多くの場合、ループバック テストは、ネットワーク インターフェイスが使用可能かどうかを確認するために使用されます。

ルール セキュリティ ポリシーを定義するために条件文の形式で設定に追加される情報であり、特定の状況への対処法をルータに指示します。

例外リスト NAC 実装において、スタティック アドレスを持ち、NAC プロセスの省略が許可されているホストのリスト。このようなホストは、ポスチャ エージェントがインストールされていないため、あるいはプリンタや Cisco IP 電話であるため、例外リストに置かれることがあります。

レイヤ 3 インターフェイス レイヤ 3 インターフェイスは、インターネットワーク ルーティングを支援します。VLAN は論理レイヤ 3 インターフェイスの例であり、イーサネット ポートは物理レイヤ 3 インターフェイスの例です。

ローカル サブネット サブネットワークは、ネットワーク管理者がサブネット マスクによって任意に分割した IP ネットワークです。マルチレベルの階層ルーティング構造が提供され、接続されたネットワークの複雑なアドレス指定を回避できます。ローカル サブネットは、送信側に関連付けられるサブネットです。

論理インターフェイス 設定でのみ作成され、ルータ上の物理インターフェイスではないインターフェイス。論理インターフェイスの例として、ダイヤラ インターフェイスやトンネル インターフェイスなどがあります。

わ

ワイルドカード マスク アクセス ルール、IPSec ルール、および NAT ルールで、パケットの IP アドレスのどの部分がルールの IP アドレスと一致しなければならないかを指定するためのビットマスク。ワイルドカード マスクは 32 ビットであり、IP アドレスのビット数と同じです。ワイルドカード ビット値 0 は、パケットの IP アドレスの同じ位置のビットがルールの IP アドレスのビットと一致しなければならないことを示します。値 1 は、パケットの IP アドレスの対応するビットが 1 または 0 のどちらでもよい、つまり、ルールでビット値が確認されないことを示します。ワイルドカード マスク 0.0.0.0 は、パケットの IP アドレスの 32 ビットすべてがルールの IP アドレスと一致しなければならないことを示します。ワイルドカード マスク 0.0.255.0 は、最初の 16 ビットと最後の 8 ビットが一致しなければならないが、3 つめのオクテットはどんな値でもよいことを示します。ルールの IP アドレスが 10.28.15.0 でマスクが 0.0.255.0 の場合、IP アドレス 10.28.88.0 はルールの IP アドレスと一致し、IP アドレス 10.28.15.55 は一致しません。