数値

3DES DES を参照してください。

A

A レコード アドレス 「A」はアドレスの意味で、DNS の名前 / アドレス マップ レコードを指します。

AAA Authentication, Authorization, Accounting（認証、許可、アカウンティング）。TACACS+ および RADIUS も参照してください。

ABR Area Border Router（エリア境界ルータ）。OSPF では、マルチエリアのインターフェイスを持つルータ。

ACE Access Cntrol Entry（アクセス制御エントリ）。設定に入力された情報で、インターフェイスで許可または拒否するトラフィックのタイプを指定するものです。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。

ACL Access Control List（アクセス制御リスト）。ACE の集まり。ACL を使用すると、インターフェイス上で許可するトラフィックの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。通常、ACL は着信トラフィックの送信元のインターフェイスに適用されます。ルール、発信 ACL の項も参照してください。

ActiveX モバイル（ポータブル）プログラムを作成するために使用される、オブジェクト指向プログラミング テクノロジーとツールのセット。ActiveX プログラムは Java アプレットに類似したものです。

Address Resolution Protocol ARP を参照してください。

AES Advanced Encryption Standard（高度暗号規格）。情報を暗号化および復号化できる対称ブロック サイファ。AES アルゴリズムでは、128、192、256 ビットの暗号キーを使用して、128 ビットのブロック単位でデータの暗号化と復号化を行うことができます。DES の項も参照してください。

AH Authentication Header（認証ヘッダー）。データの整合性、認証、および再送検出を保証するための IP プロトコル（タイプ 51）。AH は、保護対象のデータに組み込まれます（完全 IP データグラムなど）。AH は、単独で使用することも、ESP と一緒に使用することもできます。これは古い IPSec プロトコルで、大部分のネットワークにおいて ESP ほどの重要性はありません。AH は認証サービスには対応していますが、暗号化サービスには対応していません。これは ESP（認証と暗号化の両方に対応）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用意されています。暗号化および VPN の項も参照してください。RFC 2402 を参照してください。

ARP Address Resolution Protocol（アドレス解決プロトコル）。ハードウェア アドレス（MAC アドレス）を IP アドレスにマッピングする下位レベルの TCP/IP プロトコル。ハードウェア アドレスは、00:00:a6:00:01:ba のようになります。最初の 3 つの文字グループ（00:00:a6）は製造メーカーを示し、残りの文字（00:01:ba）はシステム カードを示します。ARP は RFC 826 で定義されています。

ASA Adaptive Security Algorithm（アダプティブ セキュリティ アルゴリズム）。検査を実行するために FWSM で使用されます。ASA では、内部システムとアプリケーションの明示的な設定がなくても、一方向（内部から外部へ）の接続が可能です。インスペクション エンジンの項も参照してください。

ASA Adaptive Security Appliance（アダプティブ セキュリティ アプライアンス）。

ASDM Adaptive Security Device Manager（アダプティブ セキュリティ デバイス マネージャ）。シングル FWSM の管理と設定を行うためのアプリケーション。

B

BGP Border Gateway Protocol。BGP は、TCP/IP ネットワークのドメイン間ルーティングを行います。BGP は Exterior Gateway Protocol（EGP; 外部ゲートウェイ プロトコル）で、複数の Autonomous System（AS; 自律システム）やドメイン間のルーティングを行い、他の BGP システムとルーティング情報やアクセス情報を交換します。FWSM は BGP をサポートしていません。EGP の項も参照してください。

BLT ストリーム Bandwidth Limited Traffic（帯域幅制限トラフィック）ストリーム。帯域幅が制限されたパケットのストリームまたはフロー。

BOOTP Bootstrap Protocol（ブートストラップ プロトコル）。ディスクレス ワークステーションをネットワーク上でブートできます。RFC 951 および RFC 1542 に規定されています。

BPDU Bridge Protocol Data Unit（ブリッジ プロトコル データ ユニット）。ネットワークのブリッジ間で情報を交換するため、設定可能な間隔で送出されるスパニングツリー プロトコルの hello パケット。プロトコル データ ユニットはパケットに相当する OSI の用語です。

C

CA Certificate Authority、Certification Authority（認承局）。証明書の発行と取り消しを行うサードパーティの機関。CA の公開鍵を持つ装置は、CA が発行した証明書を持つ装置の認証を行うことができます。CA という用語は、CA サービスを提供するソフトウェアを指す用語としても使用されます。証明書、CRL、公開鍵、RA の項も参照してください。

CBC Cipher Block Chaining（暗号ブロック連鎖）。アルゴリズムの暗号化強度を高める暗号技法。CBC には、暗号化を開始するための Initialization Vector（初期化ベクトル）が必要です。IV は IPSec のパケットで明示的に与えられます。

CHAP Challenge Handshake Authentication Protocol。

CLI Command-Line Interface（コマンドライン インターフェイス）。FWSM にコンフィギュレーションおよびモニタリング コマンドを入力するためのプライマリ インターフェイス。

CPU Central Processing Unit（中央演算処理装置）。メイン プロセッサ。

CRC Cyclical Redundancy Check（巡回冗長検査）。エラーチェック技法。この技法では、フレーム受信側が、フレームの容量に生成多項式の除算を適用して剰余を計算し、それを送信側ノードがフレームに保存した値と比較します。

CRL Certificate Revocation List（証明書失効リスト）。所定の CA によってリスト化された、最新だが取り消された証明書をすべて記載したデジタル署名付きメッセージ。これは、店が不正なクレジット カードを拒否するために使用する、盗まれたクレジット カード番号のリストと同様のものです。証明書が取り消されると、その情報が CRL に追加されます。証明書を使用した認証を実装する場合、CRL を使用するかどうかを選択できます。CRL を使用すると、期限切れになる前に容易に証明書の取り消しが行えますが、CRL は一般的に CA や RA でのみ管理されています。CRL を使用していて、認証が要求されたときに CA や RA との接続ができない場合、認証要求は失敗します。CA、証明書、公開鍵、RA の項も参照してください。

CRV Call Reference Value（呼参照値）。2 つのエンティティ間で発信されるコール レッグを区別するために H.225.0 で使用されます。

CTIQBE Computer Telephony Interface Quick Buffer Encoding。IP テレフォニーにおいて、Cisco CallManager と CTI TAPI および JTAPI アプリケーションの間で使用されるプロトコル。CTIQBE は TAPI/JTAPI プロトコル検査モジュールで使用され、NAT、PAT、および双方向 NAT をサポートしています。これにより、Cisco IP SoftPhone や Cisco TAPI/JTAPI アプリケーションが、FWSM を越えて Cisco CallManager とコール セットアップや音声トラフィックの通信を行うことができます。

D

DES Data Encryption Standard（データ暗号化規格）。DES は 1977 年に米国商務省標準局によって発表された、IBM の Lucifer アルゴリズムに基づく秘密鍵暗号化方式です。Cisco では、標準暗号 DES（40 ビットおよび 56 ビットのキー長）、IPSec 暗号（56 ビットのキー）、3DES（トリプル DES：56 ビットのキーにより 3 回暗号化を行う）を使用しています。3DES は DES よりも安全性が高いですが、暗号化と復号化に多くの処理が必要となります。AES、ESP の項も参照してください。

DHCP Dynamic Host Configuration Protocol。ホストで IP アドレスが不要になったときにそのアドレスが再利用でき、モバイル コンピュータ（ラップトップなど）が接続する LAN で有効な IP アドレスを受け取れるよう、ホストにダイナミックに IP アドレスを割り当てるメカニズムを提供します。

Diffie-Hellman セキュアでない通信チャネルで 2 者が秘密情報を共有するための公開鍵暗号化プロトコル。Diffie-Hellman は、IKE 内でセッション 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 グループ 1、グループ 2、グループ 5、グループ 7 Diffie-Hellman とは、フェーズ 1 とフェーズ 2 の SA を確立するために、大きな素数に基づく非対称暗号化を使用した公開鍵暗号化のタイプです。グループ 1 はグループ 2 より小さな素数を使用しますが、IPSec ピアでグループ 1 しかサポートされていないこともあります。Diffie-Hellman グループ 5 では 1536 ビットの素数を使用するため、安全度が最も高く、AES での使用に最適です。グループ 7 は 163 ビットの楕円曲線フィールドを持ち、Movian VPN クライアントでの使用に適していますが、グループ 7（ECC）をサポートしているピアであれば一緒に使用することができます。VPN および暗号化の項も参照してください。

DMZ インターフェイスを参照してください。

DN Distinguished Name（認定者名）。OSI Direcroty（X.500）のグローバルな正規のエントリ名です。

DNS Domain Nama System（ドメイン ネーム システム）、Domain Name Service（ドメイン ネーム サービス）。ドメイン名を IP アドレスに変換するインターネット サービス。

DoS Denial of Service。ネットワーク サービスを利用不能にすることを目的としたネットワーク攻撃。

DSL Digital Subscriber Line（デジタル加入者線）。従来の銅線で距離の制限された高帯域を提供する公共ネットワーク テクノロジー。DSL はモデム ペアを介して利用可能で、1 台のモデムはセントラル オフィスに、もう 1 台のモデムは顧客サイトに設置されます。大部分の DSL テクノロジーではツイストペアの帯域幅全体を使用しないので、音声チャネルのための余裕があります。

DSP Digital Signal Processor（デジタル シグナル プロセッサ）。DSP は、音声信号をフレームに分割し、音声パケットに格納します。

DSS Digital Signature Standard（デジタル シグニチャ規格）。公開鍵暗号化に基づいて米国国立標準技術研究所によって規定されたデジタル署名アルゴリズム。DSS は、ユーザ データグラムの暗号化を行いません。DSS は標準暗号化や Redcreek IPSec カードのコンポーネントですが、Cisco IOS ソフトウェアで実装されている IPSec のコンポーネントではありません。

E

ECHO ping、ICMP の項を参照してください。インスペクション エンジンの項も参照してください。

EGP Exterior Gateway Protocol（外部ゲートウェイ プロトコル）。BGP で代用されています。FWSM は EGP をサポートしていません。BGP の項も参照してください。

EIGRP Enhanced Interior Gateway Routing Protocol。FWSM は EIGRP をサポートしていません。

EMBLEM Enterprise Management BaseLine Embedded Manageability。Cisco IOS のシステム ログ フォーマットとの互換性を考慮して設計された Syslog フォーマットです。CiscoWorks 管理アプリケーションとの互換性が高められています。

ESMTP Extended SMTP（拡張 SMTP）。配信通知、セッション配信などの付加機能を持つ拡張版の SMTP。ESMTP については、RFC 1869「SMTP Service Extensions」に規定されています。

ESP Encapsulating Security Payload。IPSec プロトコルである ESP は、セキュアでないネットワーク上で、セキュアなトンネルを確立するための認証および暗号化サービスを提供します。詳細については、RFC 2406 および 1827 を参照してください。

F

FQDN/IP Fully Qualified Domain Name（完全修飾ドメイン名）/IP アドレス。セキュリティ ゲートウェイであるピアを識別するための IPSec のパラメータ。

FragGuard IP フラグメント保護の機能を持ち、すべての ICMP エラー メッセージの完全再組み立てと、FWSM でルーティングされる残りの IP フラグメントの仮想再組み立てを行います。

FTP File Transfer Protocol（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、ホスト間でのファイルの転送に使用されます。

G

GGSN Geteway GPRS Support Node（ゲートウェイ GPRS サポート ノード）。携帯電話ユーザが公共データ ネットワークや指定のプライベート IP ネットワークにアクセスできるようにする無線ゲートウェイ。

GMT Greenwich Mean Time（グリニッジ標準時）。世界標準時は、1967 年に Coordinated Universal Time（UTC; 協定世界時）に変わりました。

GPRS General Packet Radio Service。欧州通信規格協会によって定義および標準化されたサービス。GPRS は GSM ネットワークを IP パケットベースで拡張したもので、モバイル無線データ通信を可能にします。

GRE RFC 1701 および 1702 で規定された Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）。GRE は、IP トンネル内の各種プロトコル パケットをカプセル化し、IP ネットワーク上のリモート ポイントでルータへの仮想のポイントツーポイント リンクを作成する、トンネリング プロトコルです。シングル プロトコル バックボーン環境でマルチプロトコル サブネットワークを接続することにより、GRE を使用した IP トンネリングは、シングル プロトコル バックボーン環境でのネットワーク拡張を可能にします。

GSM Global System for Mobile Communication。モバイル無線音声通信用に開発されたデジタル モバイル無線通信の規格。

GTP GPRS Tunneling Protocol（GPRS トンネリング プロトコル）。GTP は、GPRS ネットワークの SGSN と GGSN の間で、ユーザ パケットとシグナリング情報のフローを処理します。GTP は GPRS ネットワークの Gn および Gp インターフェイスで定義されます。

H

H.225 テレビ会議などの用途で TCP シグナリングのために使用するプロトコル。H.323 およびインスペクション エンジンの項も参照してください。

H.225.0 H.225.0 セッションの確立とパケット化を管理する ITU 規格。H.225.0 では、実際に数種類のプロトコルを規定しています。規定されているのは、RAS、Q.931 の使用、RTP の使用などです。

H.245 H.245 のエンドポイント制御を管理する ITU 規格。

H.320 ISDN、フラクショナル T-1、交換型 56 K 回線などの回線交換型メディア上でのテレビ会議に関する一連の ITU-T 標準仕様。ITU-T 標準 H.320 の拡張を使用することで、LAN やパケット交換ネットワークを使用したテレビ会議、およびインターネットを使用したテレビ会議も可能になります。

H.323 標準の通信プロトコルを使用して、異種の通信デバイスが相互に通信できます。H.323 では、CODEC の共通セット、コール セットアップとネゴシエーション手順、および基本的なデータ転送方式を定義しています。

H.323 RAS Registration, Admission, Status（RAS）シグナリング プロトコル。デバイスでの VoIP ゲートウェイとゲートキーパ間の登録、アドミッション、帯域幅変更、状態の検出と接続解除の手順の実行を可能にします。

H.450.2 H.323 へのコール転送サービスの補足。

H.450.3 H.323 へのコール迂回サービスの補足。

HMAC SHA-1 や MD5 などの暗号化ハッシュを使用したメッセージ認証のためのメカニズム。

HTTP HyperText Transfer Protocol。ファイル転送のためにブラウザや Web サーバで使用されるプロトコル。ユーザが Web ページを参照するとき、ブラウザは HTTP を使用して Web ページで使用するファイルを要求したり受信したりすることができます。HTTP 送信は暗号化されません。

HTTPS HTTP over SSL。SSL を暗号化したバージョンの HTTP。

I

IANA Internet Assigned Number Authority。インターネットで使用するポート番号とプロトコル番号を割り当てます。

ICMP Internet Control Message Protocol。エラーを報告し、IP パケット処理に関するその他の情報を提供するネットワーク レイヤ インターネット プロトコル。

IETF Internet Engineering Task Force。インターネットのプロトコルを定義する RFC ドキュメントを作成する技術標準化団体。

IGMP Internet Group Management Protocol。IGMP は、隣接するマルチキャスト ルータに IP マルチキャスト メンバーシップを報告するために IPv4 システムで使用されるプロトコルです。

IKE Internet Key Exchange（インターネット キー交換）。IKE は共有セキュリティ ポリシーを確立し、キーを必要とするサービス（IPSec など）のためにキーを認証します。IPSec トラフィックを通過させるには、FWSM でピアの ID を確認する必要があります。この確認は、両方のホストに事前共有鍵を手動で入力するか、または CA サービスにより行われます。IKE は、ISAKMP フレームワーク内で SKEME と呼ばれるプロトコル スイートと Oakley を部分的に使用するハイブリッド プロトコルです。このプロトコルは、以前は ISAKMP/Oakley と呼ばれていました。RFC 2409 で定義されています。

IKE 拡張認証 IKE Extended Authenticate（Xauth）は、IETF draft-ietf-ipsec-isakmp-xauth-04.txt（「extended authentication」ドラフト）に従って実装されます。このプロトコルは、TACACS+ または RADIUS を使用する IKE 内でユーザの認証を行う機能を提供します。

IKE モード コンフィギュレーション IKE モード コンフィギュレーションは、IETF draft-ietf-ipsec-isakmp-mode-cfg-04.txt に従って実装されます。IKE モード コンフィギュレーションを使用すると、セキュリティ ゲートウェイで IKE ネゴシエーションの一部として VPN クライアントに IP アドレス（および他のネットワーク レベル コンフィギュレーション）をダウンロードすることができます。

ILS Internet Locator Service。ILS は LDAP をベースにしており、ILSv2 に準拠しています。ILS は、Microsoft の NetMeeting、SiteServer、および Active Directory 製品で使用するために、Microsoft 社が開発したものです。

IMAP Internet Message Access Protocol。共有が可能なメール サーバに保存された、電子メールや掲示板メッセージにアクセスする方式。IMAP では、クライアントの電子メール アプリケーション からリモートのメッセージの格納場所へのアクセスを、メッセージの転送を行わずにローカルでアクセスしているかのように行うことができます。

IMSI International Mobile Subscriber Identity。GTP トンネル ID の 2 つのコンポーネントのうちの 1 つで、もう一方は NSAPI です。NSAPI の項も参照してください。

inside FWSM で保護された内部の「信頼できる」ネットワークに接続する最初のインターフェイス。通常はポート 1 です。インターフェイス、インターフェイス名の項目も参照してください。

intf*n* 名前と構成のカスタマイズが可能なユーザ設計のサブセット ネットワークに接続するインターフェイス。通常はポート 2 から始まります。

IP Internet Protocol。IP プロトコルは、最も広く使用されている公開プロトコルです。相互接続されたネットワークのどこからでも通信に利用でき、LAN 通信にも WAN 通信にも同様に適しています。

IPS Intrusion Prevention System（侵入防御システム）。広範囲のネットワーク攻撃の軽減に役立つ、インラインのディープ パケット検査を行うソリューション。

IPSec IP セキュリティ。参加するピア間でのデータの機密保持、データの整合性、データの認証を実現する公開規格のフレームワーク。IPSec では、IP レイヤでこれらのセキュリティ サービスが利用できます。IPSec は IKE を使用して、ローカル ポリシーに基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 で使用される暗号化および認証キーを生成します。IPSec は、ホストのペア間、セキュリティ ゲートウェイのペア間、またはセキュリティ ゲートウェイとホスト間の 1 つ以上のデータ フローを保護します。

IPSec トランスフォーム セット トランスフォーム セットには、IPSec ポリシーに一致するトラフィックで使用する IPSec プロトコル、暗号化アルゴリズム、およびハッシュ アルゴリズムを指定します。トランスフォームには、1 つのセキュリティ プロトコル（AH または ESP）とそれに対応するアルゴリズムが記述されます。大部分のトランスフォーム セットで使用される IPSec プロトコルは、認証用の DES アルゴリズムと HMAC-SHA を持つ ESP です。

IPSec フェーズ 1 IPSec ネゴシエーションの第 1 フェーズで、キー交換と IPSec の ISAKMP 部分が該当します。

IPSec フェーズ 2 IPSec ネゴシエーションの第 2 フェーズ。フェーズ 2 では、ペイロードに使用する暗号化ルール、暗号化に使用する送信元と宛先、アクセス リストに基づいて処理対象とするトラフィックの定義、および IPSec ピアが決まります。IPSec は、フェーズ 2 でインターフェイスに適用されます。

IP アドレス IP プロトコル アドレス。FWSM のインターフェイス IP アドレス。IPv4 アドレスは、32 ビット長です。このアドレス スペースは、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 ビットは 4 つのオクテット（8 個のバイナリ ビット）にグループ分けされ、ピリオド（ドット）で分割された 4 つの 10 進数で表現されます。4 つのオクテットのそれぞれの意味は、ネットワークでの使用方法によって決まります。

IP プール 名前、開始 IP アドレスおよび終了 IP アドレスで示した範囲で指定される、ローカル IP アドレスの範囲。IP プールは、内部インターフェイスのクライアントにローカル IP アドレスを割り当てるために、DHCP および VPN で使用されます。

ISAKMP Internet Security Association and Key Management Protocol。ペイロード フォーマット、キー交換プロトコルを実装するメカニズム、およびセキュリティ アソシエーションのネゴシエーションを定義するプロトコル フレームワーク。IKE を参照してください。

ISP Internet Service Provider（インターネット サービス プロバイダー）。電話音声回線を使用したモデム ダイヤルイン、DSL などのサービスを通してインターネットへの接続を提供する組織。

J

JTAPI Java Telephony Application Programming Interface。テレフォニー機能をサポートする Java ベースの API。TAPI の項も参照してください。

K

Kerberos 秘密鍵暗号化を使用する、クライアント / サーバ アプリケーション用の強力なネットワーク認証プロトコル。Kerberos は、LDAP サーバへのセキュリティ アプライアンス認証に利用可能な SASL メカニズムの 1 つです。

L

LAN Local Area Network（ローカルエリア ネットワーク）。1 つの建物やキャンパスなど、1 つの場所に存在するネットワーク。インターネット、イントラネット、およびネットワークの項も参照してください。

LCN Logical Channel Number（論理チャネル番号）。

LDAP Lightweight Directory Access Protocol。LDAP を使用すると、管理およびブラウザ アプリケーションで X.500 ディレクトリへのアクセスが行えます。

LDP Label Distribution Protocol。

LLA Link-Local Address（リンクローカル アドレス）。

M

MCR マルチキャストを参照してください。

MC ルータ マルチキャスト（MC）ルータは、マルチキャスト データ送信を、インターネットワークの各 LAN 上のホストにルーティングします。これらのホストは、特定のマルチメディアまたはその他のブロードキャストを受信するよう登録されています。マルチキャストの項も参照してください。

MD5 Message Digest 5。128 ビットのハッシュを生成する単一方向のハッシュ アルゴリズム。MD5 も SHA-1 も MD4 から派生したもので、MD4 ハッシュ アルゴリズムのセキュリティを強化するよう設計されています。SHA-1 は MD4 や MD5 よりも安全性が高くなっています。シスコでは、IPSec フレームワーク内で認証のためにハッシュを使用します。SNMP v.2 のメッセージ認証でも使用します。MD5 は通信の整合性を確認し、発信元を認証し、適時性を確認します。MD5 は SHA-1 よりもダイジェストが小さく、若干処理速度が速いと考えられます。

MDI Media Dependent Interface（メディア依存型インターフェイス）。

MDIX Media Dependent Interface crossover（メディア依存型インターフェイス クロスオーバー）。

MGCP Media Gateway Control Protocol。MGCP は、外部コール制御エレメント（メディア ゲートウェイ コントローラまたはコール エージェント）による VoIP コールの制御を行うプロトコルです。MGCP は IPDC プロトコル と SGCP プロトコルを統合したものです。

Mode Config IKE モード コンフィギュレーションを参照してください。

MS Mobile Station（モバイル ステーション）。ネットワーク サービスにアクセスするために使用する、モバイル ハンドセットまたはコンピュータなどの任意のモバイル デバイスの総称です。GPRS ネットワークは、MS の 3 つのクラスをサポートします。これらのクラスでは、GPRS および GSM モバイル無線ネットワーク内でサポートされる操作のタイプが記述されています。たとえば、クラス A の MS は GPRS と GSM サービスの同時操作をサポートしています。

MS-CHAP Microsoft の CHAP。

MSFC Multilayer Switch Feature Card（マルチレイヤ スイッチ フィーチャ カード）。MSFC は、Catalyst 6500 スイッチまたは Cisco 7600 ルータに搭載されるルータ カードです。

MTU Maximum Transmission Unit（最大伝送ユニット）。最適な応答時間でネットワーク上で効率的に転送できる 1 パケットの最大バイト数です。イーサネットのデフォルト MTU は 1500 バイトですが、各ネットワークで値は異なります。シリアル接続では最小のバイト数になります。MTU は RFC 1191 で定義されています。

N

N2H2 FWSM と連動してユーザの Web アクセスを制御するサードパーティ製のポリシー指向フィルタリング アプリケーション。N2H2 は、宛先ホスト名、宛先 IP アドレス、およびユーザ名とパスワードに基づいて、HTTP 要求をフィルタリングできます。N2H2 社は、2003 年 10 月に Secure Computing 社に買収されました。

NAT Network Address Translation（ネットワーク アドレス変換）。グローバルに一意な IP アドレスを使用する必要性を減らすメカニズムです。NAT を使用すると、グローバルに一意でないアドレスを持つ組織が、使用しているアドレスをグローバルにルーティング可能なアドレス スペースに変換することにより、インターネットに接続できるようになります。

NEM Network Extension Mode（ネットワーク拡張モード）。これを使用すると、VPN ハードウェア クライアントは、VPN トンネル経由でリモート プライベート ネットワークに 1 つのルーティング可能なネットワークを提供できるようになります。

NetBIOS Network Basic Input/Output System。Windows のホスト名登録、セッション管理、およびデータ転送をサポートする Microsoft のプロトコル。FWSM は、NBNS UDP ポート 137 および NBDS UDP ポート 138 のパケットの NAT 処理を実行することにより、NetBIOS をサポートします。

NMS Network Management System（ネットワーク管理システム）。ネットワークの少なくとも一部分の管理に責任を負うシステム。通常、NMS には、エンジニアリング ワークステーションなどの比較的、高性能高機能のコンピュータが使用されます。NMS は、エージェントとの通信により、ネットワーク統計情報やリソース情報を把握します。

NP Network Processor（ネットワーク プロセッサ）。

NSAPI Network Service Access Point Identifier（ネットワーク サービス アクセス ポイント識別子）。GTP トンネル ID の 2 つのコンポーネントのうちの 1 つです。もう一方は IMSI です。IMSI の項も参照してください。

NSSA Not-So-Stubby-Area。RFC 1587 で定義された OSPF 機能。NSSA は、Cisco IOS ソフトウェア Release 11.2 で最初に導入されました。既存のスタブ エリア機能を汎用的に拡張するもので、限定的な方法でスタブ エリアに外部のルータを導入することができます。

NTLM NT Lan Manager。Microsoft Windows のチャレンジ レスポンス認証方式。

NTP Network Time Protocol。

O

Oakley 認証済みキー関連情報を取得する方法を定義したキー交換プロトコル。Oakley の基本的なメカニズムは、Diffie-Hellman キー交換アルゴリズムです。Oakley は RFC 2412 で定義されています。

OSPF Open Shortest Path First。OSPF は IP ネットワーク用のルーティング プロトコルです。OSPF は、ネットワーク帯域幅を有効に使用し、トポロジー変更後の収束が速いため、大規模ネットワークで広く採用されています。FWSM は OSPF をサポートしています。

OU Organizational Unit（組織ユニット）。X.500 ディレクトリの属性です。

outside FWSM の外部にある「信頼できない」ネットワーク（インターネット）に接続する最初のインターフェイス。通常はポート 0 です。インターフェイス、インターフェイス名、発信の項も参照してください。

P

PAC PPTP Access Concentrator。1 つ以上の PSTN または ISDN 回線に接続され、PPP 操作と PPTP プロトコル処理のできるデバイス。PAC で 1 つ以上の PNS にトラフィックを渡すために必要なのは、TCP/IP の実装のみです。非 IP プロトコルのトンネリングを行うこともできます。

PAT ダイナミック PAT、インターフェイス PAT、およびスタティック PAT の項も参照してください。

Perfmon 接続 / 秒、xlates/ 秒など各種機能の統計情報を収集し、レポートする FWSM 機能。

PFS Perfect Forward Secrecy。PFS は IPSec フェーズ 1 とフェーズ 2 の SA に異なるセキュリティ キーを使用することにより、セキュリティを向上させます。PFS を使用しない場合、両方のフェーズで SA を確立するため同じセキュリティ キーが使用されます。PFS は、所定の IPSec SA キーが他のシークレット（他のキーなど）から派生していないことを保証します。つまり、キーが解読されそうになった場合、PFS は攻撃者が他のキーを導出できないようにします。PFS がイネーブルになっていない場合、IKE SA 秘密鍵が解読されれば、IPSec 保護データがすべてコピーされ、IKE SA シークレットの知識を使用して、この IKE SA によって設定された IPSec SA を脆弱化することができると推測されます。PFS を使用すると、IKE が突破されても、攻撃者にすぐに IPSec にアクセスされることはありません。攻撃者は、IPSec SA を個別に突破する必要があるためです。

PIM Protocol Independent Multicast。PIM は、特定のマルチキャスト送信をホスト グループに配信するための最良のパスを特定する、スケーラブルな方法を提供します。各ホストは、伝送を受信するため、IGMP を使用して登録されています。PIM-SM の項も参照してください。

PIM-SM Protocol Independent Multicast-Sparse Mode。PIM-SM は シスコ製ルータのデフォルトで、マルチキャスト送信の送信元がブロードキャストを開始すると、登録されたすべてのホストにパケットが到達するまで、1 つの MC ルータから次のルータへと、トラフィックが順次転送されていきます。PIM の項も参照してください。

ping 2 台めのホストがアクセス可能かどうかを判断するため、ホストによって送信される ICMP 要求。

PIX Private Internet eXchange。Cisco PIX 500 シリーズの FWSM は、小規模事業所用のコンパクトなプラグアンドプレイのデスクトップ モジュールから、要求の厳しい企業やサービス プロバイダー環境用のキャリアクラスのギガビット モジュールまで、幅広いモデルがあります。Cisco PIX FWSM は、急速に変化するネットワーク環境に対応した強力で多層的な防御を構築するための、堅牢なエンタープライズ クラスの統合ネットワーク セキュリティ サービスを提供します。

PKCS12 秘密鍵、証明書、その他のデータなど、PIK 関連のデータを転送するための規格。この規格をサポートするデバイスを使用することにより、管理者は個人 ID 情報を一括して管理できます。

PNS PPTP Network Server。PNS は、汎用コンピューティング / サーバ プラットフォーム上で動作することを想定されています。PNS は PPTP のサーバ側を処理します。PPTP は完全に TCP/IP に依存し、インターフェイス ハードウェアからは独立しているため、PNS では LAN および WAN デバイスなどの IP インターフェイス ハードウェアを任意に組み合わせて使用できます。

POP Post Office Protocol。クライアントの電子メール アプリケーションがメール サーバからメールを取り出すために使用するプロトコル。

PPP Point-to-Point Protocol（ポイントツーポイント プロトコル）。アナログ電話回線とモデムを使用するダイアルアップ ISP アクセスのために開発されました。

PPTP Point-to-Point Tunneling Protocol（ポイントツーポイント トンネリング プロトコル）。PPTP は、Windows ネットワークにセキュアなリモート アクセスを提供するために Microsoft によって導入されました。ただし、攻撃に対して脆弱なため、一般に PPTP が使用されるのは、強力なセキュリティ対策が利用できない場合や不要な場合だけです。PPTP のポートは pptp、1723/tcp、1723/udp、および pptp です。PPTP の詳細については、RFC 2637 を参照してください。PAC、PPTP GRE、PPTP GRE トンネル、PNS、PPTP セッション、および PPTP TCP の項も参照してください。

PPTP GRE PPP トラフィックをカプセル化するための GRE のバージョン 1。

PPTP GRE トンネル PNS-PAC ペアで定義されたトンネル。トンネル プロトコルは、GRE の修正バージョンで定義されています。トンネルは、PAC と PNS の間で PPP データグラムを送信します。1 つのトンネルで多数のセッションが多重処理されます。TCP 上で動作する制御接続は、セッションとトンネルの確立、解放、および維持を制御します。

PPTP TCP PPTP コール制御および管理情報がやりとりされる標準の TCP セッション。制御セッションは、PPTP トンネルでトンネリングされるセッションと論理的には対応付けられますが、実際には独立しています。

PPTP セッション PPTP はコネクション型です。PNS および PAC は、PAC に接続された各ユーザの状態を維持します。セッションは、ダイヤル ユーザと PNS の間でエンドツーエンドの PPP 接続が試みられた時点で作成されます。セッションに対応するデータグラムは、PAC と PNS の間でトンネルを介して送信されます。

Q

QoS Quality of Service（サービス品質）。送信品質とサービスの可用性を反映させた、送信システムのパフォーマンスの指標。

R

RA Registration Authority（登録局）。CA の公認の代理人。RA は証明書の登録と、CRL の発行ができます。CA、証明書、公開鍵の項も参照してください。

RADIUS Remote Authentication Dial-In User Service。RADIUS は、不正アクセスに対してネットワークのセキュリティ対策を施した分散クライアント / サーバ システムです。RFC 2058 および RFC 2059 では、RADIUS プロトコルの標準を定義しています。AAA および TACACS+ の項も参照してください。

RFC Request for Comments。RFC ドキュメントでは、インターネット上の通信のためのプロトコルと標準が定義されています。RFC は IETF によって作成され、公開されます。

RIP Routing Information Protocol。UNIX BSD システムで提供される Interior Gateway Protocol（IGP; 内部ゲートウェイ プロトコル）。インターネットで最も一般的な IGP。RIP では、ルーティング メトリックとしてホップ カウントを使用します。

RLLA Reserved Link Local Address。マルチキャスト アドレスの範囲は 224.0.0.0 ～ 239.255.255.255 ですが、利用できるのは 224.0.1.0 ～ 239.255.255.255 です。マルチキャスト アドレス範囲の最初の部分の 224.0.0.0 ～ 224.0.0.255 は、予約されており、RLLA と呼ばれます。このアドレスは利用できません。RLLA の範囲を除外するには、224.0.1.0 ～ 239.255.255.255 を指定します。224.0.0.0 ～ 239.255.255.255 を指定して、224.0.0.0 ～ 224.0.0.255 を除外すると、224.0.1.0 ～ 239.255.255.255 を指定したのと同じになります。

RP Rendezvous Point（ランデブー ポイント）。RP は、PIM マルチキャスト環境において、マルチキャスト データの送信元と受信者が出会う場として機能します。

RPC Remote Procedure Call。RPC は、クライアントによって指定され、サーバで実行されてから結果がネットワーク経由でクライアントに帰されるプロシージャ コールです。

RSA キー長が可変の公開鍵暗号化アルゴリズム（開発者の Rivest、Shamir、Adelman にちなんで命名）。RSA の大きな弱点は、DES などの一般的な秘密鍵アルゴリズムに比べて、処理速度が非常に遅いことです。シスコの IKE 実装では、秘密鍵の取得に Diffie-Hellman 交換を使用しています。この交換は RSA（事前共有鍵）によって認証が可能です。Diffie-Hellman 交換では、DES キーがネットワークを越えることはありません（暗号化された形式であっても）。RSA 暗号化および署名方式ではネットワークを越えます。RSA はパブリック ドメインではなく、RSA Data Security からライセンスを取得する必要があります。

RSH Remote Shell（リモート シェル）。ユーザがリモートのシステムにログインしなくてもリモート システムでコマンドを実行できるようにするプロトコル。たとえば、RSH を使用すると、各通信サーバに接続することなく多数のアクセス サーバのステータスをリモートで確認し、コマンドを実行して通信サーバとの接続を終了することができます。

RTCP RTP Control Protocol。IPv6 RTP 接続の QoS をモニタし、続行中のセッションに関する情報を伝達するためのプロトコル。RTP の項も参照してください。

RTP Real-Tme Transport Protocol。通常、IP ネットワークで使用されます。RTP は、音声、ビデオ、シミュレーション データなどのリアルタイム データをマルチキャストまたはユニキャスト ネットワーク サービス上で送信するアプリケーションのためのエンドツーエンドのネットワーク伝送機能を提供するために設計されています。RTP は、ペイロード タイプの識別、シーケンス番号付与、タイムスタンプ付与、リアルタイム アプリケーションへの配信モニタリングなどのサービスを提供します。

RTSP Real Time Streaming Protocol。音声、ビデオなどのリアルタイム データの制御配信を可能にします。RTSP は、RTP や HTTP などの確立されたプロトコルと連動するよう設計されています。

S

SA Security Association（セキュリティ アソシエーション）。データ フローに適用されたセキュリティ ポリシーおよびキー関連情報のインスタンス。SA は、IPSec の 2 つのフェーズで IPSec ピアによってペアで確立されます。SA は、セキュアなトンネルを作成するために使用される暗号化アルゴリズムとその他のセキュリティ パラメータを指定します。フェーズ 1 の SA（IKE SA）は、フェーズ 2 の SA のネゴシエーションのためのセキュアなトンネルを確立します。フェーズ 2 の SA（IPSec SA）は、ユーザ データの送信に使用されるセキュアなトンネルを確立します。IKE と IPSec の両方で SA が使用されますが、SA は互いに独立しています。IPSec SA は単一方向で、それぞれのセキュリティ プロトコル内で一意です。SA のセットは保護データ パイプに必要で、各プロトコルの各方向に 1 つ必要です。たとえば、ピア間で ESP をサポートするパイプがある場合、各方向に 1 つの ESP SA が必要です。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 インデックスによって一意に識別されます。IKE は IPSec の代わりに SA のネゴシエーションと確立を行います。IPSec SA を手動で確立することもできます。IKE SA は IKE でのみ使用され、IPSec SA とは異なり双方向です。

SASL Simple Authentication and Security Layer。コネクション型のプロトコルに認証サポートを追加するためのインターネット標準方式。SASL は、セキュリティ アプライアンスと LDAP サーバとの間で、ユーザ認証を安全に行うために使用できます。

SCCP Skinny Client Control Protocol。Cisco Call Manager と Cisco VoIP フォンの間で使用される Cisco 独自のプロトコル。

SCEP Simple Certificate Enrollment Protocol。CA に証明書を要求し、受け取る（「登録」ともいう）ための手段。

SDP Session Definition Protocol。マルチメディア サービスを定義するための IETF プロトコル。SDP メッセージは、SGCP および MGCP メッセージの一部とすることができます。

SGCP Simple Gateway Control Protocol。外部コール制御エレメント（コール エージェント）により VoIP ゲートウェイを制御します。

SGSN Serving GPRS Support Node。SGSN は、モビリティ管理、セッション管理、およびパケット リレー機能を保証します。

SHA-1 Secure Hash Algorithm 1。SHA-1 [NIS94c] は 1994 年に公開された SHA の改訂版です。SHA は MD4 に基づいてモデル化されており、160 ビットのダイジェストを生成します。SHA は 160 ビットのダイジェストを生成するため、128 ビットのハッシュ（MD5 など）よりも Brute-Force アタックに対して抵抗力がありますが、処理に時間がかかります。SHA-1 は米国国立標準技術研究所と米国国家安全保障局が共同開発しました。このアルゴリズムは、他のハッシュ アルゴリズムと同様、送信中にメッセージの内容が改ざんされていないことを保証するために下位層のプロトコルで使用される CRC のように機能するハッシュ値（メッセージ ダイジェスト）を生成するために使用されます。一般的に、SHA-1 は MD5 よりもセキュアだと考えられています。

SIP Session Initiation Protocol。特に二者間の音声会議（「コール」）のコール処理セッションを可能にします。SIP は、コール シグナリングのために SDP と連動します。SDP はメディア ストリームのためのポートを指定します。SIP を使用すると、FWSM は 任意の SIP VoIP ゲートウェイと VoIP プロキシ サーバをサポートすることができます。

SKEME 認証済みキー関連情報を導出する方法を定義したキー交換プロトコル。キー リフレッシュが迅速です。

SMR Stub Multicast Routing。SMR では、FWSM が「スタブ ルータ」として機能します。スタブ ルータとは、IGMP プロキシ エージェントとして機能するデバイスです。IGMP は、マルチキャスト ルータのある特定 LAN 上のマルチキャスト グループに特定ホストをダイナミックに登録するために使用されます。マルチキャスト ルータはマルチキャスト データ送信を、特定のマルチメディアやブロードキャストを受信するよう登録されたホストにルーティングします。スタブ ルータは、ホストと MC ルータの間で IGMP メッセージを転送します。

SMTP Simple Mail Transfer Protocol。SMTP は電子メール サービスをサポートするインターネット プロトコルです。

SNMP Simple Network Management Protocol（簡易ネットワーク管理プロトコル）。MIB（管理情報ベース）と呼ばれるデータ構造を使用してネットワーク デバイスを管理する標準方式。

SQL*Net Structured Query Language Protocol。クライアントとサーバ プロセスの間の通信に使用される Oracle のプロトコル。

SSH Secure Shell（セキュア シェル）。TCP/IP などのトランスポート レイヤの上位で動作し、強力な認証および暗号化機能を持つアプリケーション。

SSL Secure Sockets Layer。アプリケーション層と TCP/IP の間に常駐して、データ トラフィックの透過的な暗号化を提供するプロトコル。

SVC SSL VPN Client（SVC）は、ネットワーク管理者がリモート コンピュータに IPSec VPN クライアントのインストールと設定を行わなくても、リモート ユーザが IPSec VPN クライアントの機能を利用できるようにする VPN トンネリング テクノロジーです。SVC では、すでにリモート コンピュータ上に存在する SSL 暗号化と、セキュリティ アプライアンスの WebVPN ログインおよび認証を使用します。

SVI Switched Virtual Interface（スイッチ仮想インターフェイス）。SVI は MSFC に割り当てられた VLAN です。

T

TACACS+ Terminal Access Controller Access Control System Plus。コマンド許可を含む AAA サービスをサポートするクライアント / サーバ プロトコル。AAA、RADIUS の項も参照してください。

TAPI Telephony Application Programming Interface。テレフォニー機能をサポートする Microsoft Windows のプログラミング インターフェイス。

TCP Transmission Control Protocol。信頼性の高い全二重データ送信を可能にするコネクション型トランスポート層プロトコル。

TCP 代行受信 TCP 代行受信機能を使用すると、オプションの初期接続の上限に達した場合、初期接続のカウントがこのスレッシュホールドを下回るまで、当該サーバへのすべての SYN は代行受信されます。各 SYN に対して、サーバに代わって FWSM が空の SYN/ACK セグメントで応答します。FWSM は妥当なステート情報を保持し、パケットを廃棄し、クライアントの確認応答を待ちます。ACK を受信すると、クライアント SYN セグメントのコピーがサーバに送信され、FWSM とサーバの間で TCP スリーウェイ ハンドシェイクが実行されます。このスリーウェイ ハンドシェイクが完了すると、接続が通常どおり再開される場合もあります。クライアントが接続フェーズの間に応答しない場合、FWSM は指数のバックオフを使用して必要なセグメントを再送します。

TDP Tag Distribution Protocol。TDP は、タグ スイッチング ネットワーク内の複数のネットワーク レイヤ プロトコルのタグ バインディング情報を配信、要求、および解放するため、タグ スイッチング デバイスで使用されます。TDP はルーティング プロトコルを変更しません。その代わり、ルーティング プロトコルから学習した情報を使用してタグ バインディングを作成します。TDP は、TDP セッションの開始、モニタ、および終了や、このセッション中に発生したエラーを通知するためにも使用されます。TDP は、順次配信が保障されたコネクション型のトランスポート層プロトコル（TCP など）上で動作します。TDP を使用する場合でも、他のプロトコルのピギーバック情報などのタグ バインディング情報を配信する他のメカニズムも使用できます。

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。Telnet は Web サーバをリモート制御する一般的な方法ですが、セキュリティ面の脆弱性のため、SSH が使用されるようになってきています。

TFTP Trivial File Transfer Protocol（簡易ファイル転送プロトコル）。TFTP はファイルの転送に使用されるシンプルなプロトコルです。UDP 上で動作し、RFC 1350 で詳しく説明されています。

TLS Transport Layer Security。SSL に代わる将来の IETF プロトコル。

TSP TAPI Service Provider（TAPI サービス プロバイダー）。TAPI の項も参照してください。

U

UDP User Datagram Protocol。IP プロトコル スタックのコネクションレス型トランスポート層プロトコル。UDP は、確認応答や配信保証を行なわずに、データグラムを交換するシンプルなプロトコルであるため、エラー処理や再送を行うには別のプロトコルが必要となります。UDP は RFC 768 で定義されています。

UMTS Universal Mobile Telecommunication System。固定、無線、および衛星ネットワークを介してモバイル ユーザに商業サービスや娯楽サービスなどのブロードバンド情報を配信することにより、オール IP ネットワークを目指す、GPRS を拡張したネットワーク。

URL Uniform Resource Locator。ブラウザを使用してハイパーテキスト ドキュメントやその他のサービスにアクセスするための標準的なアドレス指定方式。http://www.cisco.com のように指定します。

UTC Coordinated Universal Time（協定世界時）。経度 0 のタイム ゾーン。以前は GMT（グリニッジ標準時）と呼ばれていました。世界標準時は、1967 年に GMT から UTC に変わりました。UTC は天文時よりも原子時に基づいています。

UTRAN Universal Terrestrial Radio Access Network。UMTS に無線ネットワークを導入するために使用するネットワーキング プロトコル。GTP では、GGSN、SGSN、および UTRAN の間で UMTS/GPRS バックボーンを経由してマルチプロトコル パケットをトンネリングすることができます。

UUIE User-User Information Element。メッセージに関係しているユーザを特定する H.225 パケットのエレメント。

V

VLAN Virtual LAN。実際には異なる多数の LAN セグメント上に存在していながら、同じ物理ネットワーク ケーブルに接続されているかのように通信できるよう（管理ソフトウェアを使用して）設定された、1 つ以上の LAN 上にあるデバイスのグループ。VLAN は物理接続ではなく論理接続に基づいているため、非常に柔軟性に優れています。

VoIP Voice over IP。VoIP は、電話やファックスなどの通常の音声トラフィックを、IP ベースのネットワーク上で伝送します。DSP は、音声信号をフレームにセグメント化し、2 つずつグループ化し、音声パケットに格納します。この音声パケットは、ITU-T 仕様 H.323 に準拠する IP を使用して送信されます。

VPN Virtual Private Network（仮想私設網）。ユーザの厳格な認証と全データ トラフィックの暗号化によりプライベート性が確保された公共ネットワーク上の 2 つのピア間でのネットワーク接続。PC などのクライアントや、FWSM などのヘッドエンドの間で VPN を確立することができます。

VSA Vendor-Specific Attribute（ベンダー固有属性）。RADIUS RFC ではなくベンダーによって定義された RADIUS パケットの属性。RADIUS プロトコルでは、VSA の識別のため IANA によって割り当てられたベンダー番号を使用します。これにより、異なるベンダーが同じ番号の VSA を持てるようになります。ベンダー番号と VSA 番号の組み合わせにより、VSA が一意になります。たとえば、cisco-av-pair VSA はベンダー番号 9 に対応付けられた VSA のセットのアトリビュート 1 になります。各ベンダーは最大 256 の VSA を定義することができます。RADIUS パケットには、ベンダー固有の名前が付けられた VSA アトリビュート 26 が含まれます。VSA はサブ属性と呼ばれることもあります。

W

WAN Wide-Area Network。広い地域にいるユーザにサービスを提供するデータ通信ネットワークであり、一般に、コモン キャリアが提供する伝送デバイスを使用します。

Websense 社員によるインターネット アクセスを管理するコンテンツ フィルタリング ソリューション。Websense は、ポリシー エンジンと URL データベースを使用して、Web サイトへのユーザ アクセスを制御します。

WEP Wired Equivalent Privacy。無線 LAN 用のセキュリティ プロトコル。IEEE 802.11b 規格で定義されています。

WINS Windows Internet Naming Service。特定のネットワーク デバイスに対応する IP アドレスを特定する Windows システムで、「名前解決」とも呼ばれます。WINS は、現在利用可能なネットワーク デバイスの NetBIOS 名と各デバイスに割り当てられた IP アドレスが自動的に更新される分散データベースを使用します。WINS は、ルーテッド ネットワーク環境でダイナミックな NetBIOS 名を IP アドレス マッピングに登録 / 照会するための分散データベースを提供します。複雑なネットワークでの名前解決に関して発生する問題を解決する目的で設計されているため、このようなルーテッド ネットワークでの NetBIOS の名前解決には最適です。

X

X.509 デジタル証明書の定義のために広く用いられている規格。X.509 は実際は ITU 勧告であるため、公式には規格としての使用が定義または承認されていない状態です。

xauth IKE 拡張認証を参照してください。

xlate xlate（トランスレーション エントリともいう）は、1 つの IP アドレスを別の IP アドレスにマッピングしたり、1 つの IP アドレス / ポートのペアを別のペアにマッピングしたりすることを意味します。

あ

アクセス モード FWSM CLI では、いくつかのコマンド モードを使用します。利用できるコマンドはモードによって異なります。ユーザ EXEC モード、イネーブル EXEC モード、グローバル コンフィギュレーション モード、コマンド固有コンフィギュレーション モードの項も参照してください。

アドレス変換 あるネットワークのアドレスやポートを別のネットワークのアドレスやポートに変換すること。IP アドレス、インターフェイス PAT、NAT、PAT、スタティック PAT、xlate の項も参照してください。

暗号 ネットワーク上のセキュアな通信のために使用される、暗号化、認証、整合性、キー、その他のサービス。VPN および IPSec の項も参照してください。

暗号化 データに特定のアルゴリズムまたは暗号を適用して、情報の表示を許可されていないユーザが理解できないデータにすること。復号化の項も参照してください。

暗号マップ FWSM で VPN の設定に使用される一意の名前とシーケンス番号を持つデータ構造。暗号マップは、セキュリティ処理の必要なデータ フローを選択し、これらのフローとトラフィックの宛先となる暗号ピアのためのポリシーを定義します。暗号マップはインターフェイスに適用されます。暗号マップの内容は、IKE と IPSec を使用した VPN 用のセキュリティ ポリシーを指定するために必要な ACL、暗号化基準、ピア、その他のパラメータです。VPN の項も参照してください。

暗黙の規則 デフォルトのルールに基づいて、またはユーザ定義のルールの結果として、FWSM によって自動的に作成されるアクセス規則。

い

イネーブル EXEC モード イネーブル EXEC モードでは、現在の設定を変更することができます。ユーザ EXEC モードのコマンドは、イネーブル EXEC モードで機能します。コマンド固有コンフィギュレーション モード、グローバル コンフィギュレーション モード、ユーザ EXEC モードの項も参照してください。

インスペクション エンジン FWSM は、トラフィック内で組み込まれたアドレッシング情報の場所を特定するため、特定のアプリケーション レベルのプロトコルを検査します。これにより、NAT は組み込まれたアドレスを変換し、変換によって影響を受けたチェックサムやフィールドを更新することができます。多くのプロトコルではセカンダリ TCP または UDP ポートをオープンするため、各アプリケーション インスペクション エンジンは、セッションをモニタして、セカンダリ チャネルのポート番号を特定します。well-known ポートでの初期セッションは、ダイナミックに割り当てられるポート番号のネゴシエーションに使用されます。アプリケーション インスペクション エンジンはこれらのセッションをモニタし、ダイナミックなポート割り当てを特定し、特定のセッションの間、このポートでのデータ交換を許可します。FWSM が検査可能なプロトコルには、CTIQBE、FTP、H.323、HTTP、MGCP、SMTP、SNMP などがあります。

インターネット IP を使用するグローバル ネットワーク。LAN とは異なります。イントラネットの項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 FWSM との間の物理的接続。

インターフェイス IP アドレス
FWSM ネットワーク インターフェイスの IP アドレス。インターフェイス IP アドレスは一意でなければなりません。複数のインターフェイスに同じ IP アドレス（同じ IP ネットワーク上の IP アドレス）を割り当ててはいけません。

インターフェイス PAT
PAT IP アドレスが外部インターフェイスの IP アドレスでもある状態で使用される PAT。ダイナミック PAT、スタティック PAT の項を参照してください。

インターフェイス名
FWSM ネットワーク インターフェイスに割り当てられた、人が読解可能な名前。内部インターフェイスのデフォルト名は「inside」で、外部インターフェイスのデフォルト名は「outside」です。境界インターフェイスのデフォルト名は「intf*n*」です。最初の境界インターフェイスは「intf2」、2 番めの境界インターフェイスは「intf3」というようになります。intf 文字列の番号は、FWSM のインターフェイス カードの位置に対応します。デフォルト名をそのまま使用することもできますが、経験のあるユーザの場合、わかりやすい名前に変更することもできます。inside、intfn、outside の項も参照してください。

イントラネット
イントラネットワーク。IP を使用する LAN。ネットワークおよびインターネットの項も参照してください。

お

オブジェクト グルーピング
プロトコル、サービス、ホスト、ネットワークなどのネットワーク オブジェクトのグループにアクセス制御ステートメントを適用できるようにして、アクセス制御を簡略化します。

か

仮想ファイアウォール
セキュリティ コンテキストを参照してください。

カットスルー プロキシ
ユーザ認証後の FWSM でのトラフィック フローを高速化します。カットスルー プロキシは、最初はアプリケーション レイヤでユーザとやりとりします。セキュリティ アプライアンスでユーザの認証が完了すると、セッション フローに移行するので、すべてのトラフィックが送信元と送信先の間で直接かつ迅速に伝送され、セッション ステート情報も保持されます。

き

キー
暗号化、復号化、または認証に使用されるデータ オブジェクト。

キャッシュ
以前に実行されたタスクから再利用可能な情報を蓄積した一時的なリポジトリ。タスクの実行に要する時間を短縮できます。

く

クッキー
クッキーはブラウザによって保存されるオブジェクトです。クッキーは、ユーザ プリファレンスなどの情報を固定ストレージに保存します。

クライアント / サーバ コンピューティング
トランザクションの責任が、クライアント（フロント エンド）とサーバ（バック エンド）に分散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。分散コンピューティングとも呼ばれます。RPC の項も参照してください。

グローバル コンフィギュレーション モード
グローバル コンフィギュレーション モードでは、FWSM のコンフィギュレーションを変更することができます。このモードでは、すべてのユーザ EXEC コマンド、イネーブル EXEC コマンド、およびグローバル コンフィギュレーション コマンドを使用できます。ユーザ EXEC モード、イネーブル EXEC モード、コマンド固有コンフィギュレーション モードの項も参照してください。

こ

公開鍵

公開鍵は、公開鍵インフラストラクチャに属するデバイスによって生成されるキーのペアの一方です。公開鍵で暗号化されたデータは、対応する秘密鍵を使用しなければ復号化することはできません。デジタル署名の作成に秘密鍵が使用されている場合、受信者は送信者の公開鍵を使用して、送信者によってメッセージが署名されていることを確認することができます。このキー ペアの特性により、インターネットなどのセキュアでないメディアにおいて、スケーラブルでセキュアな認証方式が可能になります。

コマンド固有コンフィギュレーション モード

一部のコマンドは、グローバル コンフィギュレーション モードからコマンド固有コンフィギュレーション モードを開始します。このモードでは、すべてのユーザ EXEC コマンド、イネーブル EXEC コマンド、グローバル コンフィギュレーション コマンド、およびコマンド固有コンフィギュレーション コマンドを使用できます。グローバル コンフィギュレーション モード、イネーブル EXEC モード、ユーザ EXEC モードの項も参照してください。

コンフィギュレーション、コンフィグ、コンフィグ ファイル

ASDM または CLI によって管理される設定、プリファレンス、プロパティに相当する FWSM のファイル。

さ

サイトツーサイト VPN

サイトツーサイト VPN は、リモート ネットワークを 1 つの VPN に接続する 2 つの IPSec ピア間で確立されます。このタイプの VPN では、IPSec ピアはユーザ トラフィックの宛先にも送信元にもなりません。その代わり、各 IPSec ピアは、各 IPSec ピアに接続された LAN 上のホストに暗号化および認証サービスを提供します。各 LAN 上のホストは、IPSec ピアのペアによって確立されたセキュアなトンネルを介してデータの送受信を行います。

サブネットマスク

マスクの項を参照してください。

し

事前共有鍵

事前共有鍵は、IPSec ピアの数が限られていてスタティックであるネットワークに適した IKE 認証の方法を提供します。この方法は、キーを IPSec ピアの各ペアに対して設定する必要があるため、スケーラビリティは高くありません。新しい IPSec ピアがネットワークに追加された場合、そのピアと通信する各 IPSec ピアに対して事前共有鍵を設定する必要があります。スケーラビリティの高い IKE 認証の方法は、証明書と CA を使用する方法です。

実行コンフィギュレーション

FWSM の RAM で現在実行されている設定。FWSM の動作特性を決定する設定。

証明書

ユーザまたは装置の ID と、証明書を発行した CA の公開鍵を持つ署名済み暗号オブジェクト。証明書には期限があり、妥当でないと判断された場合、CRL に登録されます。証明書は IKE ネゴシエーションのための否認防止も行うため、特定のピアとの間で IKE ネゴシエーションが完了していることを第三者に証明することができます。

シリアル送信

データ キャラクタのビットを 1 つのチャネルで順次伝信するデータ伝信方式。

す

スタティック PAT Static Port Address Translation（スタティック ポート アドレス変換）。スタティック PAT は、ローカル ポートをグローバル ポートにマッピングするスタティック アドレスです。ダイナミック PAT、NAT の項も参照してください。

スタンバイ ユニット セカンダリ ユニットを参照してください。

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 台のホストのネットワーク接続の両端で、ステート情報と呼ばれるデータが保持されます。ステート情報は、保証されたパケット配信、データのシーケンス処理、フロー制御、トランザクションまたはセッション ID などのプロトコル機能を実装するために必要となります。プロトコル ステート情報の一部は、プロトコルの使用中に、パケットに組み込まれて送信されます。たとえば、Web サーバに接続されたブラウザは、HTTP とサポートする TCP/IP プロトコルを使用します。各プロトコル層は、送受信するパケット内のステート情報を保持します。FWSM やその他のファイアウォールの一部は、パケット内のステート情報を検査して、使用しているプロトコルに対して最新で有効であるかどうかを確認します。これはステートフル インスペクションと呼ばれ、ある種のコンピュータ セキュリティの脅威に対して強力な防護壁を作成することを目的としています。

スプーフィング 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 メカニズムを破壊することを目的とした攻撃のタイプ。スプーフィング攻撃では、実際とは異なるアドレスから送信されているかのようなパケットが送信されます。

スプリット トンネリング リモート VPN クライアントがプライベート ネットワークへの暗号化アクセスと、インターネットへの非暗号化アクセスのクリアを同時に実行できるようにします。スプリット トンネリングをイネーブルにしない場合、VPN クアイアントと FWSM の間のトラフィックはすべて IPSec トンネル経由で送信されます。VPN クライアントから発信されるトラフィックは、トンネルを経由して外部インターフェイスに送信され、リモート サイトからインターネットへのクライアント アクセスは拒否されます。

せ

セカンダリ ユニット 2 台がフェールオーバー モードで動作している場合のバックアップの FWSM。

セキュリティ コンテキスト 1 つの FWSM をセキュリティ コンテキストと呼ばれる複数の仮想ファイアウォールに分割できます。各コンテキストはそれぞれが独立したファイアウォールであり、独自のセキュリティ ポリシー、インターフェイス、および管理者が与えられます。マルチコンテキストは、スタンドアロンのファイアウォールを複数使用することと同様です。

セキュリティ サービス） 暗号を参照してください。

た

ダイナミック NAT NAT およびアドレス変換を参照してください。

ダイナミック PAT Dynamic Port Address Translation（ダイナミック ポート アドレス変換）。ダイナミック PAT では、複数の発信セッションを 1 つの IP アドレスから発信されたように見せます。PAT をイネーブルにすると、FWSM は各発信変換スロット（xlate）に対して PAT IP アドレスから一意のポート番号を選択します。この機能は、ISP が発信接続のために一意の IP アドレスを十分に割り当てることができない場合に便利です。グローバル プール アドレスは、必ず PAT アドレスが使用される前に確保されます。NAT、スタティック PAT、および xlate の項も参照してください。

ターボ ACL ACL をコンパイルして、ルックアップ テーブルのセットにすることにより、ACL のルックアップを高速化します。既存の ACL のエントリ数に関係なく、少数かつ一定数のルックアップからなる複数のテーブルに対して、パケット ヘッダーを使用してアクセスします。

て

データの機密保持 攻撃者が読めないようにデータを操作する方法。通常これは、通信にかかわる当事者だけが利用できるデータ暗号化やキーによって実現されます。

データの整合性 秘密鍵や公開鍵アルゴリズムに基づいた暗号化を使用して、保護データの一部を受信するユーザが送信中にデータが改ざんされていないことを確認するためのメカニズム。

データ発信者認証 保護データがその送信者からのみ発信されていることを受信者が確認するためのセキュリティ サービス。このサービスには、データ整合性サービスと、秘密鍵が送信者と受信者の間だけで共有されるキー配布メカニズムが必要となります。

デジタル証明書 証明書を参照してください。

と

透過ファイアウォール モード FWSM がルータ ホップにならないモード。透過ファイアウォール モードを使用すると、ネットワーク構成を簡略化したり、FWSM を攻撃者から見えなくしたりすることができます。また、透過ファイアウォール モードの使用により、ルーテッド ファイアウォール モードではブロックされるトラフィックを通過させることもできます。ルーテッド ファイアウォール モードの項も参照してください。

登録局 RA を参照してください。

トラフィック ポリシング トラフィック ポリシング機能は、トラフィックが設定した最大レート（bps）を超えないことを保証します。したがって、1 つのトラフィック フローでリソース全体が占有されないことを保障します。

トランスフォーム セット IPSec トランスフォーム セットを参照してください。

トランスポート モード パケットのデータ部分（ペイロード）だけを暗号化し、ヘッダー部分は暗号化しない IPSec 暗号化モード。トランスポート モードはトンネル モードよりも安全性が低くなります。

トンネル あるプロトコルを別のプロトコル内にカプセル化してデータを転送する方式。トンネリングは、非互換性、実装の簡略化、セキュリティなどの理由で使用されます。たとえば、トンネルを使用すると、リモート VPN クライアントはプライベート ネットワークに暗号化アクセスを実行できます。

トンネル モード 各パケットのヘッダーとデータ部分（ペイロード）の両方を暗号化する IPSec 暗号化モード。トンネル モードはトランスポート モードよりも安全性が高くなります。

に

認証 ユーザの身元とデータの整合性を検証するための暗号化プロトコルおよびサービス。IPSec フレームワークの機能の 1 つ。認証により、データストリームの整合性が確立され、送信の途中で改ざんされていないことが保証されます。データストリームの発信元の確認も行います。AAA、暗号化、および VPN の項も参照してください。

ね

ネットマスク マスクを参照してください。

ネットワーク FWSM 設定においては、ネットワークは、IP アドレス スペース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を指し、1 台のホストを指すわけではありません。ネットワークは複数のノードまたはホストで構成されます。ホスト、インターネット、イントラネット、IP、LAN、およびノードの項も参照してください。

の

ノード
通常はホストとは呼ばれない、ルータやプリンタなどの装置。ホスト、ネットワークの項も参照してください。

は

ハッシュ、ハッシュ アルゴリズム
ハッシュ アルゴリズムは、任意の長さのメッセージで動作する単一方向の機能であり、データの整合性を保証するために暗号化サービスで使用される固定長のメッセージ ダイジェストを作成します。MD5 は、SHA-1 よりダイジェストが小さく、若干処理が早いと考えられます。シスコでは、IPSec フレームワークの実装において、SHA-1 と MD5 の両方のハッシュを使用しています。暗号化、HMAC、および VPN の項も参照してください。

発信
送信元インターフェイスよりもセキュリティの低いインターフェイスを宛先とするトラフィック。

発信 ACL
発信トラフィックに適用される ACL。

ひ

非対称暗号化
公開鍵システムとも呼ばれます。非対称暗号化を使用すると、誰でも別のユーザの公開鍵にアクセスできます。公開鍵へのアクセスが完了すると、公開鍵を使用して、相手に対して暗号化されたメッセージを送信できるようになります。暗号化、公開鍵の項も参照してください。

秘密鍵
秘密鍵は、送信者と受信者の間だけで共有されるキーです。キー、公開鍵の項を参照してください。

ふ

プール
IP プールを参照してください。

フィックスアップ
インスペクション エンジンを参照してください。

フェーズ 1
IPSec フェーズ 1 を参照してください。

フェーズ 2
IPSec フェーズ 2 を参照してください。

フェールオーバー、フェールオーバー モード
フェールオーバーでは、2 台の FWSM を設定し、1 台に障害が発生した場合にもう 1 台が処理を代行するようにできます。FWSM では、アクティブ / アクティブ フェールオーバー、アクティブ / スタンバイ フェールオーバーの 2 種類のフェールオーバー構成をサポートしています。それぞれのフェールオーバー構成には、フェールオーバーの判断と実行のための独自の方法があります。アクティブ / アクティブ フェールオーバーでは、2 台のユニットがネットワーク トラフィックを通過させることができます。これにより、ネットワークの負荷分散が可能になります。アクティブ / アクティブ フェールオーバーが利用できるのは、マルチコンテキスト モードで動作するユニットのみです。アクティブ / スタンバイ フェールオーバーでは、1 台のユニットのみでトラフィックの通過が可能で、もう 1 台のユニットはスタンバイ ステートで待ちます。アクティブ / スタンバイ フェールオーバーは、シングルまたはマルチコンテキスト モードで動作するユニットで利用できます。

不揮発性ストレージ、メモリ
RAM とは異なり、電源が入っていなくても内容が保持されるストレージまたはメモリ。不揮発性ストレージ デバイスのデータは、パワーオフ / パワーオン（電源再投入）やリブートを行っても失われません。

復号化
暗号化されたデータに特定アルゴリズムまたは暗号を適用して、情報の表示を許可されたユーザが理解できるデータにすること。暗号化の項も参照してください。

プライマリ、プライマリ ユニット
プライマリとセカンダリの 2 台で運用している FWSM は、通常はフェールオーバー モードで動作しています。

フラッシュ、フラッシュ メモリ
FWSM の停止時にコンフィギュレーション ファイルを格納しておくための不揮発性ストレージ装置。

プロキシ ARP
グローバル プール内の IP アドレスに対する ARP 要求に、FWSM が応答できるようにします。ARP の項も参照してください。

プロトコル、プロトコル文字列
ネットワーク ノード間の通信のためのパケット交換を定義した規格。プロトコルはレイヤ構造で連動します。プロトコルは、セキュリティ ポリシーの定義の一部として、文字列またはポート番号によって FWSM コンフィギュレーション内で指定されます。FWSM プロトコルの文字列としては、ahp、eigrp、esp、gre、icmp、igmp、igrp、ip、ipinip、ipsec、nos、ospf、pcp、snp、tcp、udp などが有効です。

へ

ヘッドエンド
公衆ネットワーク経由で VPN クライアント接続に対して、プライベート ネットワークへの入り口となるファイアウォール、コンセントレータ、その他のホスト。ISP および VPN の項も参照してください。

変換
xlate を参照してください。

ほ

ポート
パケットの送信元または宛先となる上位レベルのサービスを識別する TCP および UDP プロトコルのパケット ヘッダ内のフィールド。

ホスト
TCP/IP ネットワーク上の、IP アドレスを持つ装置の名前。ネットワークおよびノードの項も参照してください。

ホスト / ネットワーク
アドレス変換（xlate）や ACE などの FWSM コンフィギュレーションでシングル ホストやネットワーク サブネットを特定するために他の情報と一緒に使用する IP アドレスおよびネットマスク。

ポリシー NAT
ポリシー NAT では、アクセス リストで送信元と宛先のアドレス（またはポート）を指定することによって、アドレス変換対象のローカル トラフィックを識別します。

ま

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、およびホストの部分に分割する方法を示す 32 ビットのマスク。マスクには、ネットワークとサブネットの部分に使用されるビット位置の 1 部分と、ホストの部分に使用される 0 の部分があります。マスクでは、少なくとも標準のネットワーク部分を規定する必要があり、サブネット フィールドはネットワーク部分と連続している必要があります。

マルチキャスト
マルチキャストとは、送信元が複数の宛先（マルチキャスト グループ）に同時にパケットを送信するネットワーク アドレス指定方式を指します。PIM および SMR の項も参照してください。

め

メッセージ ダイジェスト
メッセージ ダイジェストは MD5 や SHA-1 などのハッシュ アルゴリズムによって作成され、メッセージの整合性を保証するために使用されます。

も

モード アクセス モードを参照してください。

モジュラ ポリシー フレームワーク Cisco IOS ソフトウェア Modular QoS CLI と同様の方法で FWSM 機能を設定する手段です。

ゆ

ユーザ EXEC モード ユーザ EXEC モードでは、FWSM の設定を表示できます。最初に FWSM にアクセスしたときに、ユーザ EXEC モード プロンプトが表示されます。コマンド固有コンフィギュレーション モード、グローバル コンフィギュレーション モード、およびイネーブル EXEC モードの項も参照してください。

ユニキャスト RPF Unicast Reverse Path Forwarding。ユニキャスト RPF は、パケットがルーティング テーブルに従った正しい送信元インターフェイスと一致する送信元 IP アドレスを持つように保証することによって、スプーフィングに対してガードします。

り

リプレイ検出 受信者が、リプレイ攻撃を防止するため、古いパケットや複製されたパケットを受信拒否できるセキュリティ サービス。リプレイ攻撃は、古いパケットや複製したパケットを受信者に送信する攻撃者と、偽のトラフィックを正しいものと思い込む受信者がいる状況で発生します。リプレイ検出は、シーケンス番号と認証を組み合わせて行われます。これは IPSec の標準機能です。

リフレッシュ FWSM から実行コンフィギュレーションをリフレッシュし、画面を更新します。アイコンとボタンで、同じ機能を実行できます。

る

ルーテッド ファイアウォール モード ルーテッド ファイアウォール モードの場合、FWSM はネットワーク上のルータ ホップとしてカウントされます。接続されたネットワーク間で NAT を実行します。OSPF または RIP を使用できます。透過ファイアウォール モードの項も参照してください。

ルート、ルーティング ネットワーク上のパス。

ルール 特定の状況に対するセキュリティ ポリシーを定義するために FWSM 設定に追加される条件のステートメント。ACE、ACL、NAT の項も参照してください。

れ

レイヤ ネットワーキング モデルは、異なるプロトコルが対応付けられたレイヤを実装します。最も一般的なネットワーキング モデルは OSI モデルです。このモデルは、物理層、データ リンク層、ネットワーク層、トランスポート層、セッション層、プレゼンテーション層、アプリケーション層という順序で、7 つの層により構成されています。