Internet Week 2000 T5

IPsecによるVPN構築

2000/12/18

白橋明弘
ネットワンシステムズ(株)

本日の内容

1. 暗号技術と Virtual Private Network
2. IPsec の基本
3. IPsec による VPN
4. IPsec 以外の VPN プロトコル

Copyright ©2000, Akihiro Shirahashi, Net One Systems Co.,Ltd.

暗号技術と
Virtual Private Network

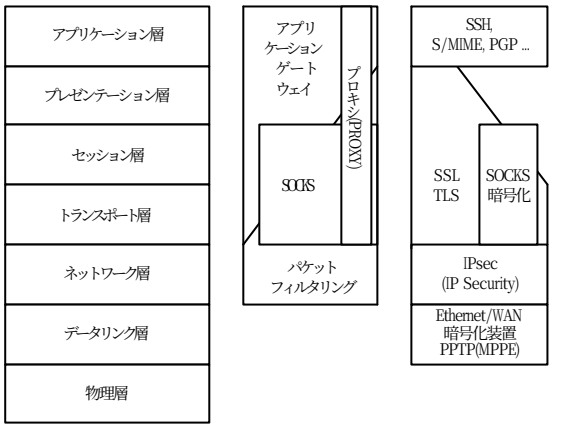
Copyright ©2000, Akihiro Shirahashi, Net One Systems Co.,Ltd.

暗号化技術のレイヤ分類

データリンク	Ethernet, WAN の暗号化装置など PPTP(PPP)
ネットワーク	IPSec
トランスポート セッション	SSL/TLS SOCKS V5 の暗号化
アプリケーション	SSH, SSL-Telnet, PET など遠隔ログイン PGP, S/MIME など暗号化メール

Copyright ©2000, Akihiro Shirahashi, Net One Systems Co.,Ltd.

OSI参照モデルと暗号化技術



OSI参照モデル
(OSI Reference Model)

ファイアウォール
技術

暗号化技術

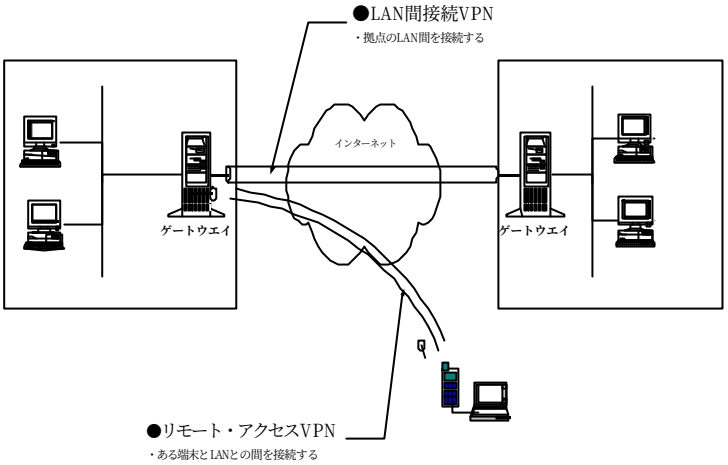
Copyright ©2000, Akihiro Shirahashi, Net One Systems Co.,Ltd.

暗号化技術の使い方

- ２組織間でやり取りするメールを暗号化したい、その方法は？
  - » VPN で２組織間の通信路を暗号化
  - » メールサーバ間の SMTP 通信を IPsec で暗号化
  - » メールサーバ間の SMTP 通信を SSLで暗号化
  - » メールサーバで PGP、S/MIME を代理適用
  - » ユーザ to ユーザで PGP、S/MIME を使用
  - » ユーザ to ユーザで独自方式でメッセージ暗号化
  - » SMTP 以外のプロトコルでメッセージを送る (https 等)

Copyright ©2000, Akihiro Shirahashi, Net One Systems Co.,Ltd.

VPNの２つの利用形態



Copyright ©2000, Akihiro Shirahashi, Net One Systems Co.,Ltd.

LAN間接続とリモートアクセス

- LAN間接続VPN
  - » WAN接続の置き換え、エクストラネット
  - » 専用線のコストの削減
  - » 帯域・遅延など全てが置き換え可能ではない
- Remote Access VPN
  - » Internet から社内ネットワークにアクセス
  - » アクセスサーバによるダイアルアップ接続の置き換え
  - » 電話代とアクセスサーバ管理コストの削減
  - » 近年関心高まる
- 同じVPNと言ってもLAN間接続とリモートアクセスでは検討すべき点・求められる機能は相当に異なる

Copyright ©2000, Akihiro Shirahashi, Net One Systems Co.,Ltd.

IPsec の基本

Copyright ©2000, Akihiro Shirahashi, Net One Systems Co.,Ltd.

IPsec (IP Security)

- IPsec
  - » アドレス、ヘッダ、データの改竄防止・暗号化
  - » 暗号化の枠組みと鍵管理方式を分離
  - » IPv4 と IPv6 の両方に適用できる
- IPsec の歴史
  - » 1995 Aug～ RFC1825-1829
  - » 1998 Nov～ RFC2401-RFC2412
    (通称「IPsec Version 2」と呼ばれることもある)

Copyright ©2000, Akihiro Shirahashi, Net One Systems Co.,Ltd.

IPsec 対応製品の例

製品ジャンル	製品例
VPN専用装置	・clPro（イスラエルのラッドガード） ・Contivity Extranet Switch（加ノーテル・ネットワークス） ・LanRover VPN Gateway（米インテル） ・PERMIT（加タイムステップ） ・Ravlin（米レッドクリーク・コミュニケーションズ） ・SafeNet（米セーフネット） ・VPNet（米VPNetテクノロジーズ）
ファイアウォール	・Firebox II（米ウォッチガード・テクノロジーズ） ・Firewall-1（イスラエルのチェック・ポイント・ソフトウェア・テクノロジーズ） ・NetScreen（米ネットスクリーン・テクノロジーズ） ・Raptor（米アクセント・テクノロジーズ） ・Sidewinder（米セキュア・コンピューティング）
ルーター	・AR720（アライドテレシス） ・Ciscoシリーズ（米シスコ・システムズ） ・NETBuilder（米3Com） ・NR60（日立製作所） ・MAXファミリ（米ルーセント・テクノロジーズ） ・MUCHO-EV（古河電気工業） ・RTシリーズ（ヤマハ）
OS	KAME（for BSD UNIX），SWAN（for Linux），Windows 2000

Copyright ©2000, Akihiro Shirahashi, Net One Systems Co.,Ltd.

IPsec documents (1)

RFC2411	IP Security Document Roadmap
RFC2401	Security Architecture for the Internet Protocol
RFC2402	IP Authentication Header
RFC2406	IP Encapsulating Security Payload (ESP)
RFC2403	Use of HMAC-MD5-96 within ESP and AH
RFC2404	Use of HMAC-SHA-1-96 within ESP and AH
RFC2405	ESP DES-CBC Cipher Algorithm With Explicit IV
RFC2410	NULL Encryption Algorithm and Its Use With IPsec

Copyright ©2000, Akihiro Shirahashi, Net One Systems Co.,Ltd.

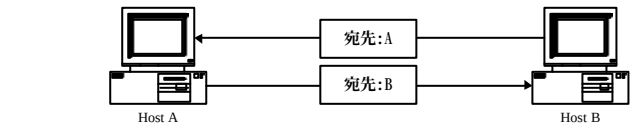
IPsec documents (2)

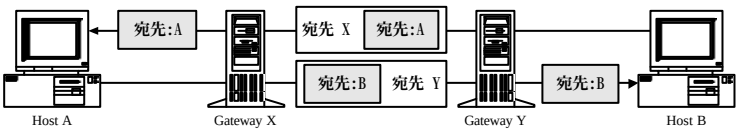
RFC2408	Internet Security Association and Key Management Protocol (ISAKMP)
RFC2412	OAKLEY Key Determination Protocol
RFC2409	Internet Key Exchange (IKE)
RFC2407	Internet IP Security Domain of Interpretation for ISAKMP

Copyright ©2000, Akihiro Shirahashi, Net One Systems Co.,Ltd.

IPsec の２つのモード

- Transport モードと Tunnel モード
  - » Transport モード: データ部だけを暗号化
  - » Tunnel モード: IPヘッダまで暗号化

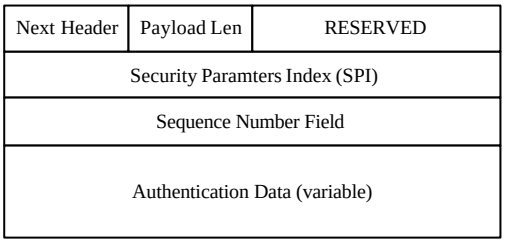




Copyright ©2000, Akihiro Shirahashi, Net One Systems Co.,Ltd.

AH ヘッダー (RFC2402)

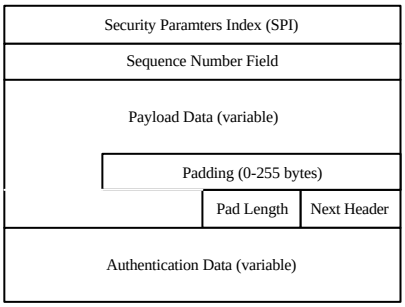
- AH (Authentication Header)　IP Protocol Number = 51
  - » パケットが改ざんされていないこと
  - » パケットの発信元が偽られていないこと
  - » リプレイ攻撃に対する防御 (オプション)



Copyright ©2000, Akihiro Shirahashi, Net One Systems Co.,Ltd.

ESP ヘッダー (RFC2406)

- ESP (Encapsulating Security Payload)
  IP Protocol Number = 50
  - » データの暗号化
  - » トラフィックフロー解析への(限定された)防御
  - » パケットが改ざんされていないこと (オプション)
  - » パケットの発信元が偽られていないこと (オプション)
  - » リプレイ攻撃に対する防御 (オプション)



Copyright ©2000, Akihiro Shirahashi, Net One Systems Co.,Ltd.

AH/ESPでの認証の仕組み

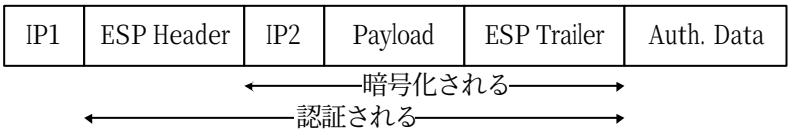
- AH(or ESP)の認証(完全性検査)では
  HMAC-MD5-96 (RFC2403)
  HMAC-SHA-1-96 (RFC2404)
  の鍵付きハッシュアルゴリズムが使われる

- HMAC (Keyed Hashing for Message Authentication) by RFC2401 方式に従い、「鍵」の情報をパラメータとして含むハッシュ値が計算される
  → 正しい「鍵」を知らないと、ハッシュ値は計算できない
  →「改ざん」されると、検出が可能

Copyright ©2000, Akihiro Shirahashi, Net One Systems Co.,Ltd.

IPsec AH/ESP Datagram

AH Datagram (Transport Mode)

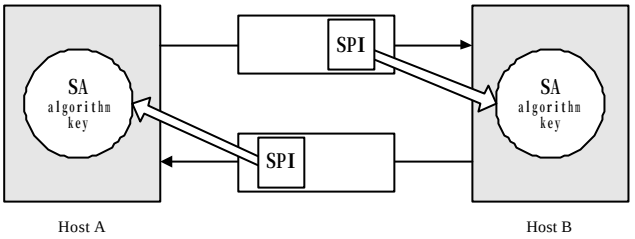


ESP Datagram (Tunnel Mode)

Copyright ©2000, Akihiro Shirahashi, Net One Systems Co.,Ltd.

IPsec SA と SPI

- SA (Security Association)
  - » ホスト同士が共有するアルゴリズムや鍵の情報
- SPI (Security Parameters Index)
  - » パケットヘッダ中に含まれる SA に対するポインタ
  - » 暗号・認証のアルゴリズムをプロトコルから分離



Copyright ©2000, Akihiro Shirahashi, Net One Systems Co.,Ltd.

IPsec 新規格の変更点

- Sequence Number Field の新設
  - » replay attack の防止
- ESP にパケット認証の機能も盛り込まれる
  - » 通常 ESP only, no AH で使用
  - » ESP のパケット認証では outer IP header は認証の対象外
- 鍵管理プロトコル IKE の標準化

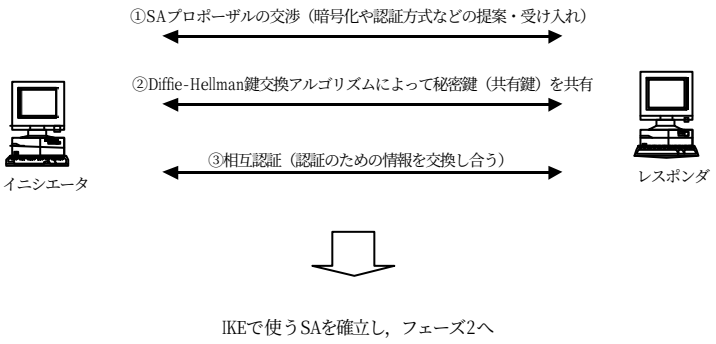
Copyright ©2000, Akihiro Shirahashi, Net One Systems Co.,Ltd.

IPsec 鍵管理/IKE

- 手動鍵管理 (Manual Key Management)
  - » パケット認証・暗号化パラメータを管理者が設定
- 自動鍵管理
  - » パラメータを動的に生成し自動的に設定する
  - » IKE (Internet Key Exchange: ISAKMP/Oakley) が標準
- IKE の手順
  - » Phase 1 IKE自身で使うSAを確立
  - » Phase 2 IPSecで使うSAを確立
  - » UDP Port 500 を使用
- IKE での認証
  - » パケット認証・暗号化のパラメータは動的に決まるので、その前の接続確立時の「相互認証」が重要

Copyright ©2000, Akihiro Shirahashi, Net One Systems Co.,Ltd.

IKE フェーズ1



Copyright ©2000, Akihiro Shirahashi, Net One Systems Co.,Ltd.

Main Mode と Aggressive Mode

- IKEフェーズ１には２つのモードがある
  - » Main Mode
    - ６個(３往復)のメッセージを交換
      1. SAの折衝、2. DH法による交換、3.相手の認証
    - 全ての折衝機能を利用可能
  - » Aggressive Mode
    - Main Mode の半分の３個のメッセージを交換
      SA提案・DH公開値・身元情報を１つのメッセージで提示
    - 折衝範囲が限られる (複数のオプションを提案できない)
    - 選択されるであろうオプションが予め解っている場合、例えばリモートアクセス VPN の場合などに使用

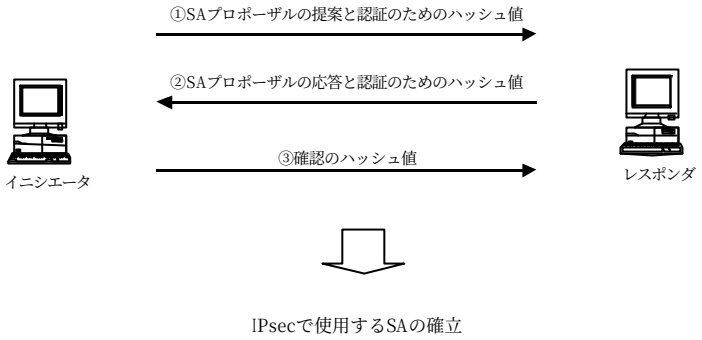
Copyright ©2000, Akihiro Shirahashi, Net One Systems Co.,Ltd.

IPsec IKE の認証

- IKE 認証の方式
  - » Shared Secret (実装必須)
  - » Public Key Encryption
  - » Digital Certificate (X.509) (本命)
- X.509 認証
  - » PKI (Public Key Encryption) の IPsec への適用
    RFC2510,RFC2511,RFC2559などで標準化の過程
- リモートアクセスVPNの場合は、これらの認証スキームだけでは必ずしも十分ではない → Xauth の提案

Copyright ©2000, Akihiro Shirahashi, Net One Systems Co.,Ltd.

IKE フェーズ2



Copyright ©2000, Akihiro Shirahashi, Net One Systems Co.,Ltd.

Quick Mode と PFS

- IKEフェーズ2のモードはQuick Mode 1つ
  - » IPsec SA のパラメータの折衝と鍵生成が行われる
  - » フェーズ1で確立された IKE SA を使い保護される
  - » IKE SA で交換した鍵をつかって、HMACハッシュを生成して Quick Mode のメッセージを保護
- PFS (Perfect Forward Secrecy)
  - » IPsec SA で使う全ての鍵は、IKE SA で交換した鍵から生成する → 万一後者が推定されると、非常に問題
  - » これを防ぐため、Quick Mode に PFS をサポートするオプションがある → 追加のDH交換を行って共有した新たな鍵から IPsec SA の鍵を生成し、元の鍵は破棄

Copyright ©2000, Akihiro Shirahashi, Net One Systems Co.,Ltd.

IPsec による VPN

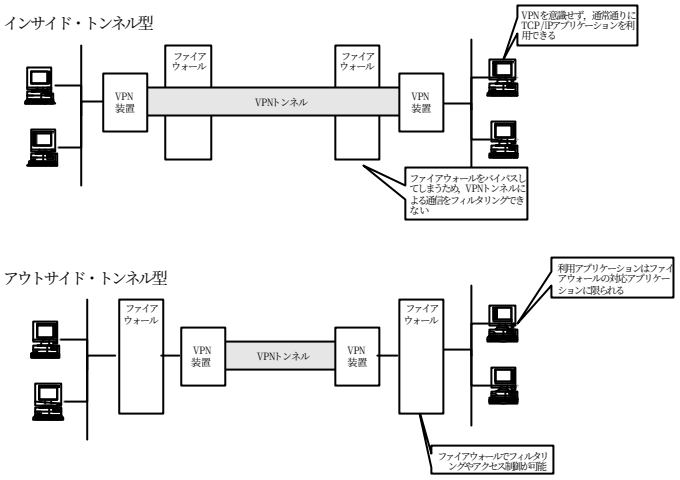
Copyright ©2000, Akihiro Shirahashi, Net One Systems Co.,Ltd.

VPNとファイアウォールの運用

- VPNとFirewallは論理的には独立した存在
  - » 実際には組み合わせで使われることが多い
  - » Firewall の VPN オプションの場合は一体化して提供される
- VPNのトンネルの張りかた
  - » Firewall の内側と内側を結ぶ
    - 制限無し、任意のアプリケーションを利用可能
    - Firewall が VPN トラフィックを通せることが必要
    - 同じ会社の拠点間接続
  - » Firewall の外側と外側を結ぶ
    - 制限有り、Firewall で対応可能なアプリケーションのみ
    - 取引先企業との接続

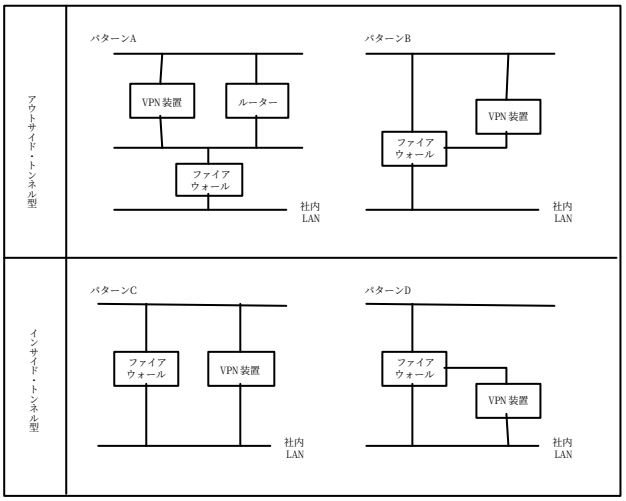
Copyright ©2000, Akihiro Shirahashi, Net One Systems Co.,Ltd.

インサイド/アウトサイド・トンネル



Copyright ©2000, Akihiro Shirahashi, Net One Systems Co.,Ltd.

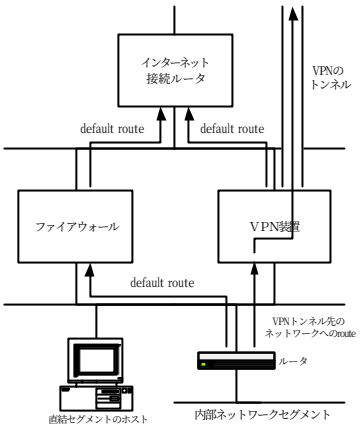
ファイアウォールとVPN機器の構成



Copyright ©2000, Akihiro Shirahashi, Net One Systems Co.,Ltd.

VPN/ファイアウォールとルーティング

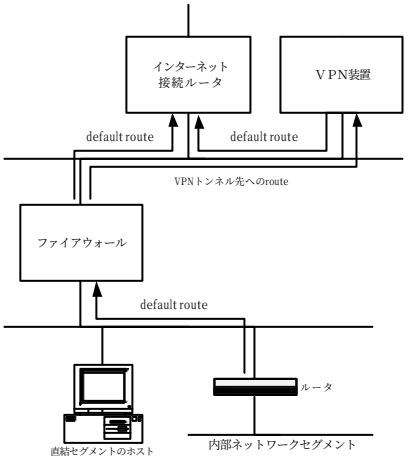
- VPNのトンネル先のルーティングをVPN装置に向けるのが基本の考え方
- 直結セグメントにあるホストには要注意
  →default gatewayをファイアウォールに向ける
  →ファイアウォールは(ルータではないので)ルーティングしてくれない場合がある
  →きちんとVPNトンネル先へのstatic routeを設定するか、内部向けルータにdefault gatewayを向けておけばＯＫ



Copyright ©2000, Akihiro Shirahashi, Net One Systems Co.,Ltd.

既存環境にVPNを導入する場合

- ３つの方法
  - » ファイアウォールとVPN装置を併置
  - » 既存インターネット接続ルータをVPN対応にする
  - » 既存インターネット接続ルータとVPN装置を併置
- ネットワーク構成を変更できない場合、図のようは１本足折り返し構成も一考
  (VPN装置によってはこれは出来ない場合もある)



Copyright ©2000, Akihiro Shirahashi, Net One Systems Co.,Ltd.

VPN における動的ルーティング

- 大規模なVPN環境では、VPNのトンネルを介しての動的ルーティングが必要となる
- IPsec のトンネルを介して RIP や OSPF といった動的ルーティングプロトコルをやり取りできるか？
  → RIP、OSPF は broadcast で隣のルータと情報交換する
  → IPsec のトンネルに broadcast を流せるか？
- IPsec のトンネルが、"direct connect" のインターフェースと見えるかどうかがポイント
  →これは実装に依存する、例えば Cisco IOSは不可
- IPsec トンネルモードを使う変わりに、GREなどのトンネルに IPsec トランスポートモードを組み合わせるという別法

Copyright ©2000, Akihiro Shirahashi, Net One Systems Co.,Ltd.

VPN における MTU 問題

- (VPNの)トンネルインターフェースは MTU が小さくなる
  → パケットの fragmentation が起る可能性がある
- パケットの DF (Don't Framgent) bit がONの場合
  → パケットは破棄され、ICMP (Type=3/Code=4 すなわち dategram too big = fragmentation needed) が送信元に返される
- このICMPが送信元まで届き、かつ送信MTUが調整されるようになっていることが必要
  →ファイアウォールがあったりすると問題となる可能性

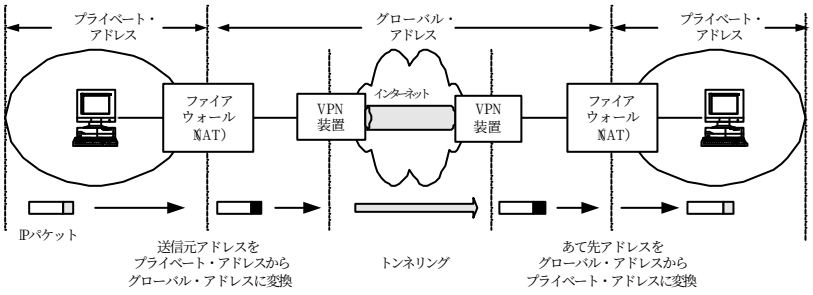
Copyright ©2000, Akihiro Shirahashi, Net One Systems Co.,Ltd.

VPN と IPアドレス/DNS

- LAN間VPN接続の両側でネットワークアドレスが重複している場合
  - » VPN だからといって特別なことはない、基本的には普通のWAN接続の場合と同じ
  - » RFC1918のプライベートアドレスでの衝突の可能性高い
  - » NAT, Proxy などの技術を組み合わせて対応する。あらゆるケースに通用する一般解は無い。
  - » 重複アドレスに対応できる特別な機能を持ったVPN装置もある
- DNSの運用
  - » 相互に必要なドメインのセカンダリになる
  - » BIND 8.2 以降ならゾーン別にフォワード先を変えられる

Copyright ©2000, Akihiro Shirahashi, Net One Systems Co.,Ltd.

アドレス衝突問題の解決法の１つ



Copyright ©2000, Akihiro Shirahashi, Net One Systems Co.,Ltd.

VPN と NAT

- IPsec の通信を NAT 越しに行うこと
  - » ファイアウォール越しでのVPNの構築
  - » リモートアクセスVPNとダイアルアップルータの組み合わせ
- IPsec と NAT の相性は良くない
  - » AHのパケット認証→アドレス変換不可
  - » ESP only→一応アドレス変換は可能
    (新しいESPではIPヘッダがパケット認証の対象外となっているので)
  - » 但し、1対1変換(静的・動的)の NAT なら通る可能性が高いが、
    tcp/udp の port 番号を変換する1対N変換では多重化できないのは
    当然として通るかどうかも実装依存
  - » IKE が udp で source/dest ports=500 を使い port 変換不可という制
    約もある

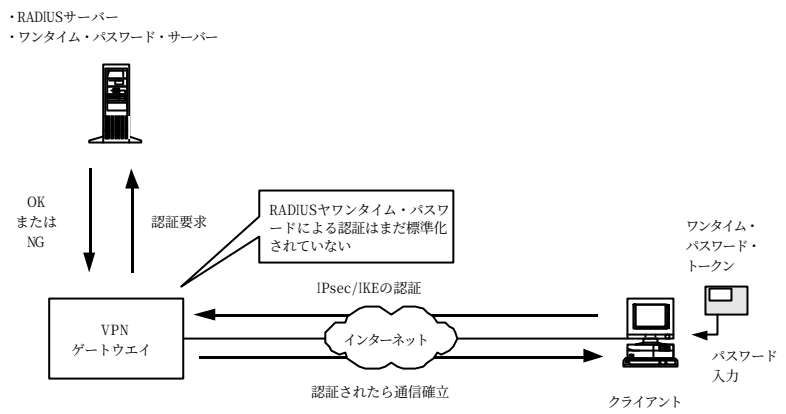
Copyright ©2000, Akihiro Shirahashi, Net One Systems Co.,Ltd.

リモートアクセスVPNの認証

- リモートアクセスVPNでは認証がより重要
  - » 不特定IPアドレスからの接続を受ける
  - » 多数のユーザの登録・管理が必要である
- IPsec/IKE の認証の対応
  - » Shared Secret
    - 固定IPアドレスでのみ利用可能という実装が普通
  - » X.509 Digital Certificate
    - VPN の為だけでは導入・管理コストが大きい
  - » RADIUSサーバとの連携/One Time Password の利用
    - 既存システムの継承の意味から重要。IPsec/IKE の拡張として
      IETF で検討されている(Xauth)。先取りで実装している製品も
      かなりある。

Copyright ©2000, Akihiro Shirahashi, Net One Systems Co.,Ltd.

リモートアクセスVPNの認証モデル



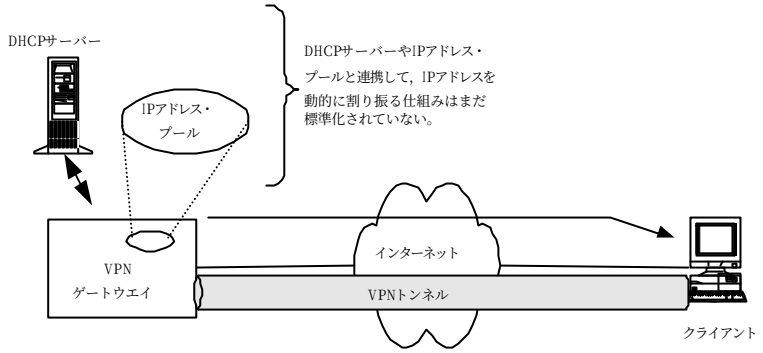
Copyright ©2000, Akihiro Shirahashi, Net One Systems Co.,Ltd.

アドレスの動的割り当ての機能

- リモートアクセスVPNではカプセル化される方のIPパケットのアドレス(仮想アドレス)を割り当てる機能が重要
  - » Global address と同じアドレス
  - » クライアントで固定的に設定したアドレス
  - » VPN装置がアドレスプールから動的に割り当てたアドレス
  - » VPN装置がDHCPを使って取得したアドレスを割り当て
- 静的割り当てしかサポートされていないと、ネットワーク構成あるいはアドレス配布・設定がかなり困難
- アドレスの動的割り当てやDNSサーバのアドレスの配布の機能はIETF で IPsec/IKE の拡張として検討中(mode-config)。先取りして実装している製品もある。

Copyright ©2000, Akihiro Shirahashi, Net One Systems Co.,Ltd.

クライアントへのアドレス配付



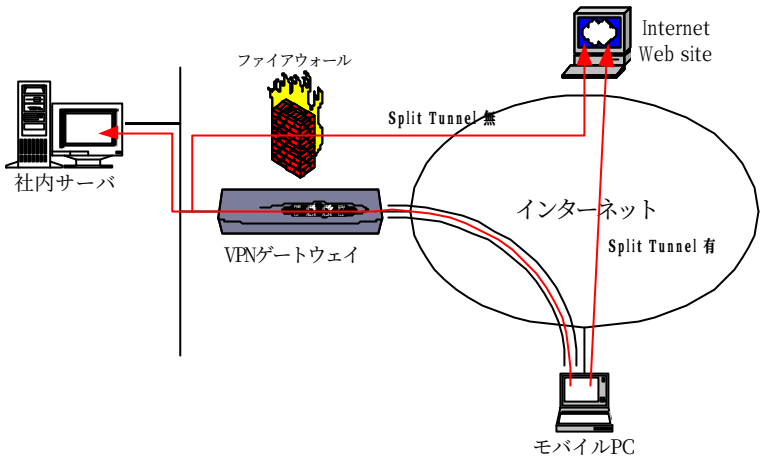
Copyright ©2000, Akihiro Shirahashi, Net One Systems Co.,Ltd.

VPNと直接接続の同時利用

- リモートアクセスVPNで、トンネル確立後は、
  全てのパケットをトンネルに向けて投げる
  - » Internet のWebサイトへのアクセスも、トンネルを
    通って折り返しになる
  - » ローカルの Network Printer にアクセスできない
- 組織内部のアドレス宛てのパケットはVPNトンネルに、
  それ以外は、物理インターフェースの default gateway に
  投げるというルーティングができると使い分けができる
  → "Split Tunneling" と呼ばれる機能
- 組織内部のアドレスの指定は、クライアントPC側でする
  場合と、VPN機器側で設定して配付する場合がある

Copyright ©2000, Akihiro Shirahashi, Net One Systems Co.,Ltd.

Split Tunneling の効果



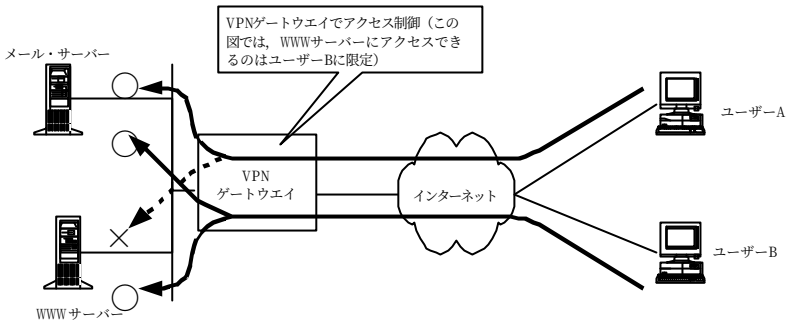
Copyright ©2000, Akihiro Shirahashi, Net One Systems Co.,Ltd.

VPN とアクセス制御

- リモートアクセスVPNではユーザ(グループ)別のアクセス制御が必要な場合がある
  - » 考え方はアクセスサーバの場合と同様
  - » VPN装置がユーザ認証の結果によって異なるアクセス制御ができる機能を持つ必要がある
  - » Source/Destination IP address, Port番号, TCP接続の方向性などによるフィルタリングが一般的
  - » ファイアウォールとの連携は？
- ユーザ(グループ)別に固定アドレス(プール)を割り当てて、それを基にアクセス制御する方法も一案

Copyright ©2000, Akihiro Shirahashi, Net One Systems Co.,Ltd.

VPN装置でのフィルタリング



Copyright ©2000, Akihiro Shirahashi, Net One Systems Co.,Ltd.

IPsec の相互接続性

- マルチベンダ環境のIPsec相互接続性
  - » エクストラネットでの利用のためには必須
  - » 精力的に努力はされているが現時点ではまだ不十分
  - » 相互接続テスト
    - S/WAN, ANX, ICSA, Interoperability Workshops
    - 日本 NTT (98/5,98/9,99/5), vpnops (99/4,99/6) , JNSA
  - » Manual 鍵管理、IKE(shared secret)、IKE(X.509) とハードルは何段もある
  - » 実験でつながっても、安定して使えるとは限らない
  - » rekey 問題や reboot 時の再接続など課題

Copyright ©2000, Akihiro Shirahashi, Net One Systems Co.,Ltd.

IPsec 以外の VPN プロトコル

Copyright ©2000, Akihiro Shirahashi, Net One Systems Co.,Ltd.

PPTP/L2F/L2TP

- PPTP (Point to Point Tunneling Protocol)
  - » Microsoft が提案、Ascend 等が支持
  - » RASを GRE(Generic Routing Encapsulation) でトンネル
  - » コントロール用の TCP port 1723 を使用
  - » 暗号化・認証機能は RASに依存
    暗号化はMPPEで、国際版では RC4 40bit, MS-CHAP 必須
    但しMS-CHAPには対応してない RADIUS サーバが多い
    弱点が指摘され MS-CHAPv2 にバージョンアップ
  - » IPX など IP 以外のプロトコルにも対応できる
- PPTP は Cisco L2F (Layer 2 Forwarding) と統合されて L2TP (Layer 2 Tunneling Protocol) へ

Copyright ©2000, Akihiro Shirahashi, Net One Systems Co.,Ltd.

PPTPの利用

- サーバ・ゲートウェイ・ルータ
  - » Windows NT 4.0 Server
    LAN間接続には “Routing and RAS Update” 必要
  - » Extranet Switch, MN128SOHO/R (暗号化未対応)
- アクセスサーバの PPTP サポート
  - » Ascend MAX, 3COM Total Control
- クライアント
  - » Windows NT 4.0, Windows 98 では標準
  - » Windows 95 + “DialUp Networking 1.3 Upgrade”

Copyright ©2000, Akihiro Shirahashi, Net One Systems Co.,Ltd.

IPsec と PPTP の比較

	IPSec	PPTP
LAN 間接続	◎	○
Remote Access	○	◎
サーバ	◎	○
クライアント	○	◎
Multi Vendor	◎	○
Interoperability	○	○

Copyright ©2000, Akihiro Shirahashi, Net One Systems Co.,Ltd.

L2TP の位置付け

- ISPがVPNサービスを使うためのプロトコルという位置付けが強い
  - » NTTの「フレッツ・ISDN」サービスで利用されている
- LAC (L2TP Access Concentrator) がトンネル化し LNS (L2TP Network Server) が終端
- PPTP と同じくリモートアクセスの環境として相性が良い
  - » IPsec/IKE を拡張するより、L2TP+IPsec のコンビネーションの方が良いとする考えもある
- 暗号化・認証は L2TP 内では規定しない
  - » IPsec と組み合わせるか、PPP で暗号化するか
- Cisco, Ascend, 3COM のルータ/アクセスサーバ(LAC および LNS) や Nortel Extranet Switch (LNS のみ) で実装されている

Copyright ©2000, Akihiro Shirahashi, Net One Systems Co.,Ltd.

参考書籍

- 是友春樹/マルチメディア通信研究会編著、「ポイント図解式VPN/VLAN教科書」、アスキー、1999年
- チャーリー・スコット・ポール、ウォルフェ・マイク・アーウィン著「VPN (第2版)」、オーム社、2000年
- エリザベス・カウフマン、アンドリュー・ニューマン著、「IPsec導入の手引き、VPN/イントラネット/エクストラネット上でのセキュリティ」、翔泳社、2000年
- ナガナンド・ドラスワミー、ダン・ハーキンス著、「IPSecテクニカルガイド、インターネット・イントラネット・VPNのセキュリティ標準」、ピアソン・エデュケーション、2000年
- ドナルド・C・リー著、「シスコ ネットワーク エンハンスドIPサービス、QoS、セキュリティ、IPルーティング、VPNサービスを使いこなす実践ガイド」、ソフトバンクパブリッシング、2000年

Copyright ©2000, Akihiro Shirahashi, Net One Systems Co.,Ltd.

参考雑誌記事

- 「検証テクノロジー IPSEC インターネットVPNの基本技術」日経コミュニケーション 1998.6.15
- 「IPsecセミナー・ルーム」 コンピュータ&ネットワークLAN 1998/8～10
- 「TCP/IPの標準暗号プロトコルとなるIPSec」Internet Magazine 1998/12
- 「ダイアルアップVPNでより安く,より手軽に」日経インターネットテクノロジー 1999/1
- 「再点検:インターネットVPN」日経コミュニケーション 1999.6.7
- 「VPN製品の相互接続性をテスト」日経コミュニケーション 1999.8.2
- 「通信コスト削減の武器としてのVPN」INTEROP MAGAZINE 1999/10
- 「IPSecにより機能格差が薄れるVPN機器」INTEROP MAGAZINE 1999/11
- 「インターネットVPN構築の基礎」日経コミュニケーション 2000.1.3～1.17
- 「安価なルータで実現するVPN」INTEROP MAGAZINE 2000/9
- 「1から始めるVPN」Software Design 2000/12

Copyright ©2000, Akihiro Shirahashi, Net One Systems Co.,Ltd.