Internet Week 99
Tutorial C22

セキュア・ネットワーク構築術

1999年12月16日

白橋明弘
ネットワンシステムズ(株)

目次

- ファイアウォール
- 認証
- リモートアクセス
- VPN
- 教育・研究機関でのセキュリティ

FIREWALL

Firewall導入の心得

- ファイアウォール導入には幅広い知識が必要
  - TCP/IPからアプリケーション、DNSやメールの設定
- ファイアウォールはその導入にともなうシステム構築の問題を自動的に解決してはくれない
- ファイアウォールは、設定作業を容易にし間違いの可能性を減らしてくれるが、セキュリティポリシーが正しく実現されていることを保証してはくれない
- 管理者は、何の目的のために何をしているのかをしっかり理解してファイアウォールの構築を進める必要がある

Firewallの本質的な難しさ

- Firewall 的なもの(負荷分散装置なども同様)には本質的な限界がある
- エンドノード間の通信の途中に立ちはだかり、不完全な情報しか与えられず、通信のコンテキストを記憶・分析するためのリソースも限られた状況で、通信の中継を行わなくてはならない
- しかも、通信相手は正しい実装をしてくれているとは限らない
- 以下に FTP の中継に関連したトラブルの事例を通じて、やや詳しく検討してみることにする

FTP問題の復習

- FTPは２つのconnectionを使う
  - data connection
    サーバ側のport 20→クライアントの非特権port
  - 内部の任意の非特権ポートへのアクセス許可が必要
- クライアントがPASVモードに対応
  - data connection をクライアント側からはる
  - ncftp, FFF, ws_ftp, Fetch 3 などが対応
- Firewall では FTP に特別な扱い
  - PORT コマンドを監視して、戻りのコネクションを通す

トラブル例1

- ある Firewall 越しのFTPの通信で、特定のFTPサーバ (Windows QuickFTP) との間で data connection が通らない。Passive mode だと問題ない。
- 原因は data connection の source port が標準の20ではなく、≧1024のportを使っていたことであった。 (Windows 系の FTP サーバはこのような実装のものが散見される。)
- Firewall のFTPプロキシがこれを厳格にチェックしていたため data connection の接続がリジェクトされていた。

トラブル例2

- Firewall越しにFTPサーバに接続すると、最初のWelcomeメッセージも出ない。パケットダンプを取ってみると、FirewallからFTPサーバのport 21に接続し、Welcomeメッセージが FTPサーバから戻ってきているが、Firewallがこれをクライアントに中継していない。
- 通常FTPのコマンドと応答は改行コードがCR+LFであるが、このFTPサーバは特殊なもので改行コードがLFであった。FirewallのFTPプロキシがこれを改行コードが来てないと判断して止まってしまっていた。

トラブル例3

- ウィルス対策ゲートウェイ(プロキシ)とパケットフィルタリング型 Firewall の組み合わせで、FTP がログインした後ですぐに切断されてしまう。
- ウィルス対策ゲートウェイが、PORTコマンドを「PORT 」のところでIPデータグラムを切って送っていた(TCPデータストリームとしてはもちろん連続している)。Firewall はこれを見て不正な PORT コマンドであると判断してセッションを切断していた。

トラブル例からの教訓

- 世の中のアプリケーションはRFC等に従った常識的な実装を行っているとは限らない。Firewall でのチェックは概して厳格なので、問題が起る場合がある。
- 勝手な拡張している「もどき」アプリケーションに要注意。例えばFTPコマンドを勝手に拡張して使っていたりする。
- 上位層の内容を下位層でチェックするアプローチには限界がある。たとえば、FirewallがTCPデータストリームを完全に再構成することは現実的にはできない。

アプリケーションへの対応

- TCP/IP だからＯＫではない
- アプリケーションを全てリストアップして確認が必要
- 「単純」でないアプリケーションへは Firewall での個別対応が必要
- アプリケーションゲートウェイ(プロキシ)でも、パケットフィルタリングでも基本的に事情は同じ
- セキュリティ度外視で「通す」だけならパケットフィルタリングの方が融通は利く
- パケットフィルタリングでも NAT をかけると対応できなくなるアプリケーションもあるので注意

対応可能なアプリケーションの条件

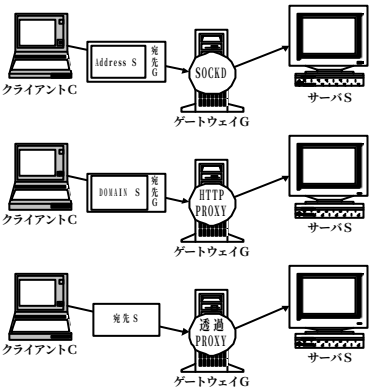
- Firewall の対応リストに載っていなくても、一定の条件を満たす「単純な」アプリケーションは、設定で対応できる
  - Destination ポート番号が固定している
  - Connection はクライアント側からサーバ側に張られる
  - サーバ側から張り返される connection は無い
  - ソース IP アドレスは変換されても問題無い
  - ソース port 番号は変換されても問題無い
  - データ中に IP address、port などの情報を持たない
- アプリケーションゲートウェイでは「汎用プロキシ」のような仕組みで対応

プロキシ方式の分類

- クライアントは直接にはプロキシサーバと通信する
  - IP packet の destination address は proxy server
- プロキシサーバは何らかの方法でクライアントが通信をしたい宛先を知る必要がある
  - 固定割り当て (DeleGateの TCPrelay, UDPrelay)
  - 対話的に入力 (FWTK の ftp, telnet gateway)
  - プロトコルに組込みでデータとして渡す
    - http proxy (ドメイン名で), SOCKS (IPアドレスで)
  - 透過的 (transparent) プロキシ
    - dest. address はプロキシサーバでなく宛先アドレス

プロキシの方式の違い

- SOCKS
  サーバSのIPアドレスをゲートウェイGに渡す
- HTTP Proxy
  サーバSのドメイン名URLをゲートウェイに渡す
- Transparent Proxy
  デステネーションIPアドレスがサーバSのアドレス



Transparent Proxy (1)

- Transparent (on the fly) proxy （透過プロキシ）
  - パケットを検出して proxy process を自動起動
  - Operating System のカーネルに自分のアドレス宛てでないパケットを処理するための仕掛けが必要
- Transparent Proxy の利点
  - クライアント設定変更の必要無し
  - 明示的プロキシができない(プロトコル上プロキシが定義されていない、非対話的な)プロトコルでも使える
  - 商用 Firewall においては transparent なプロキシの利用が主流
  - 内部→インターネットで使うのが一般的だが、イントラネットのケース(双方向)でも有用

Transparent Proxy (2)

- Transparent Proxy 利用の条件
  - 宛先アドレスへの routing が設定されていること
  - ドメイン名で宛先指定する場合は、クライアントから DNS の解決ができること
  - ユーザ認証や、URL Filtering/Virus Check などのコンテンツフィルタリングとの組み合わせには制限に注意
- Redirection/Reverse Proxy
  - 逆に routing の設定ができないケースでは、Firewall の(こちら側の)アドレスに接続して宛先アドレスを実サーバアドレスに変換して中継する設定 (redirection/reverse proxy, static map) を使う
  - サーバ１台１台に対して Firewall の設定が必要

Transparent Cache

- Web Cache Proxy の Transparent な利用
  - ブラウザのプロキシ設定の必要無し
  - port 80 のみ対象
  - トラフィックを横取りする仕組みが(別に)必要
    - L4 Switch, Policy Routing, WCCP, IP Filter
- Transparent Cache の注意点
  - port 80 以外は全部禁止か全部許可になる
    - Cache としては問題ないが、URL filtering や Virus check と組み合わせる場合は要注意
  - 上位の明示的プロキシとの cascade 接続は可能か
  - 複数 Cache を array として使う機能は分散装置による

複数の Proxy Server の使い分け

- 複数の対外接続の出口に複数の http Proxy Server
  - 冗長性および接続先による経路の使い分け
- クライアントでの振り分け
  - ブラウザの Proxy Automatic Configuration の利用
    - JavaScript のスクリプトでプロキシサーバを指定
    - ドメイン名/IPアドレスでプロキシを振り分ける
    - PACスクリプトの場所をURLでブラウザに設定
- サーバでの振り分け
  - SQUID では acl によりドメイン名/IPアドレス/URLによる振り分けが可能

Proxy Server の負荷分散

- 複数のプロキシサーバ→負荷分散と冗長性確保
- アクセスの分散の方法
  - Round Robin DNS
  - Proxy Automatic Configuration
  - L4 Switch の利用
- キャッシュの共有の方法
  - 単純な振り分けではHit率下がりDiskの利用効率悪い
  - NFS でのディスク共有
  - SQUID ICP の利用
  - URLハッシング、CARP
  - L4 Switch による振り分け
  - Transparent Cache での宛先 IPアドレスによる振り分け

NAT/アドレス変換

- NAT = Network Address Translation
  - 狭義では NAT = RFC1631 だが
  - 広義ではアドレス変換技術の総称
  - Port 変換を伴う NAT の呼称は定着してない
    - NAPT, IP masquerade, PAT, ...
- 基本は3つのモード - Firewall 的特性が異なる
  - １対１の静的変換 (static map)
  - アドレスプールから動的にアドレスを割り当て
  - １つのアドレスをport変換で多重化して割り当て

NATの注意点

- NATが適しているケース
  - 内から外はアクセス制限はあまりしない
  - サーバの管理ができるスキルがある
  - 高速な対外接続を持つ
- 「アドレス変換」という言葉の印象よりもずっとややこしい技術である (例えばアプリケーション対応)
- 実装による機能差が以外と大きい (例えば Cisco IOS と PIX の NAT ではずいぶん違う)
- 設定に際しては、実装仕様についての細かい知識が必要で、意外と難しい (例えば routing との関係)

Firewall での ident 問題

- sendmail 8.8.X は、標準的な sendmail.cf の設定では SMTP の接続要求に対して ident (port 113) での認証要求をする
- ICMP destination unreachable (port unreachable) を返せば、何事もなく先に進む
- しかし、これを単にフィルタリングでブロックしたり、ICMP destination unreachable (host unreachable) を返したりすると、timeout を待たされたり、connection が切られてしまう場合がある
- tcp_wrapper などでも同様の問題が起る場合がある

Firewall と DNS

- 内向きDNS と外向きDNS (Split Brain DNS/Dual DNS)
- 内向きDNS: slave forward で動作
  - 内部のドメインの primary または secondary となる
  - それ以外は外向き DNS にフォワードする
- 外向きDNS: sub allocation 時の逆引きに注意
- 内/外共に primary/secondary のオプション

  内: 別立てサーバが primary, Firewall が secondary

  外: Firewall が primary, ISP に secondary を頼む

Firewall と DNS/注意点

- サブドメインの delegation の問題
  - 自身がauthorityでないゾーンは(NSを参照せず)フォワードする
  - 全てのサブ(サブ...)ドメインのセカンダリとならないといけない
  - 大きなサブドメインのツリーを持つ場合は管理上これは困難
  - BIND 4.9 with No Forward Patch, BIND 8.2 ではゾーン毎にフォワードするか否かを指定できる
- Private Address (RFC1918) の逆引き
  - 必ずローカルに解決されるようにしなくてはいけない、
  - インターネットに問い合わせると read-rfc1918-for-details.iana.net が返される

Firewall と Routing

- Transparent proxy を使う場合，宛先アドレスへの routing を firewall の内側インターフェースに向ける必要がある
- インターネット接続の場合は default gateway を firewall にすることになる
- Firewall ではセキュリティ上 dynamic routing protocol は積極的にはサポートされない場合もある
  - 内部の subnet に対する経路は static に設定する
- ICMP redirect もサポートされていない場合が多い
  - そもそも packet forward は普通してくれない
  - default gateway だけですまない場合は要注意

Private address の使用

- 正しい Private Address (RFC1918) を使いましょう
  - 10/8, 172.16/12, 192.168/16
- Private Address はかち合わないように選ぶ
  - 10.0.0.0/N から使いはじめてはいけない
  - 合併、関連企業間接続、VPN 等で困ります
- Local address を使って renumber できない場合は
  - プロキシ(or NAT)2 段構成という対策はある
  - IP address を参照する外側のサーバには内部の Local address を見せないようにする
  - 対応機能を内蔵する Firewall, NAT 製品もある

AUTHENTICATION

固定・使い捨てパスワード

- ２種類のパスワード方式
  - Reusable Password (固定パスワード)
    パスワードを知られると Replay 攻撃の危険性
  - One Time Password (使い捨てパスワード)
    知られても再利用できないので安全
- よくある誤解
  - 「Reusable Password ≡ 平文パスワード」ではない
  - 「One Time Password ≡ 暗号パスワード」ではない
- 「暗号化されている固定パスワード」は必ずしも安全な認証ではない

One Time Password

- Challenge Response 型
  - ホストからの challenge
  - Local で password (secret) を入力し演算
  - 結果を response として送る
  - サーバ側でも同じ演算をして、一致すればＯＫ
- 同期型
  - 時刻またはカウンターで同期をとる
  - challenge の替りにシードとして時刻/カウンタを使う
- One Time Password の例
  - S/Key, OTP, TokenCard 製品 (SecurID, SafeWord)

One Time Password を簡単にする

- ワンタイムパスワードは面倒→使われない
  - Challenge/Response は特に敬遠されがち
  - S/Key, OTP の自動入力ツール dotkey, optsock
- Software Token
  - Cut & Paste が可能
  - ダイアルアップネットワークとの連携
  - PCと一体化してしまうことによるセキュリティの低下
  - SmartCard (IC Card) に「secret」の情報を格納

認証クライアント/サーバ

- 認証しようとするアプリケーションのプロトコルが認証に対応している必要がある
  - Challenge & Response の場合、既存の認証方式(ユーザ名/パスワード)の流用は難しいことが多い
- 接続を受け付けた「アプリケーションのサーバ」＝「認証のクライアント」で認証リクエストが発生
  - ホスト(ログイン)、アクセスサーバ、VPN装置、ファイアウォール、Webサーバ等、認証クライアント機能を持っていないといけない
- 「認証クライアント」と「認証サーバ」との間は「認証プロトコル」でやり取りする。
  - RADIUS が代表的な認証プロトコル、その他 Token Card 独自プロトコル、NTドメイン、将来的には LDAP

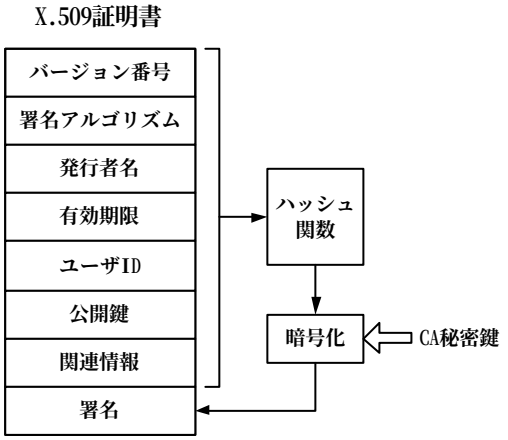
認証した情報の利用

- 認証することと認証した情報(クライアントとユーザ名の対応)を利用することは別の話。
- 一般的には、認証したサーバでしかその情報は利用できない (アクセスサーバで認証した情報を Firewall や Web サーバで使うことはできない)
- Single Sign On を実現するためには、クライアントとユーザ名の対応を認証をしたサーバ以外から参照できるような仕組みが必要
- クライアントのIPアドレスをキーとして連携させたり、何らかのチケット(例えばWebのcookie)をクライントに発行するなどの仕組みが実際的な方策として使われている

Digital Certificate による認証

- 公開鍵暗号に基づく認証
  - チャレンジ→秘密鍵で暗号→公開鍵で複号→一致
  - 秘密鍵はクライアントだけが知っていればよく、サーバは公開鍵だけ知っていればよい
- Digital Certificate とは
  - 公開鍵に対象を特定する情報などを合わせて、CA(Certificate Authority)が「電子署名」した証明書
  - CAの公開鍵を使って証明書の正当性を検証可能

X.509証明書



X.509 と PKI

- X.509v3
  - Digital Certificate のフォーマット、ITU で標準化
  - SSL/TLS, S/MIME, SET, IPsec など様々なアプリケーションで利用可能
- PKI (Public Key Infrastructure) 公開鍵基盤
  - Digital Certificate を「インフラ」として利用する仕組み
  - IETF PKIX Working Group で標準化作業進行中
    - RFC2510, 2511, 2527, 25287, 2528, 2559
  - RSA Data Security PKCS や Entrust/PKI が大きな影響を持つ

PKIの扱う範囲

- ほぼ問題なく標準化・実装されている部分
  - 証明書のフォーマット (X.509v3)
  - 無効証明書の管理 (Certificate Revocation List)
- 標準化されたが、製品によっては独自仕様の残る部分
  - 証明書発行(enrollment)と管理に関するプロトコル (Certificate Management Protocol)
  - 証明書を配布するためのプロトコル (LDAPを使用)
- これからの課題で、一部の製品で実装されている機能
  - 証明書の有効性チェック (Online Certificate Status Protocol)
  - CA間の相互認証 (Cross Certification)
  - Key Management も重要な課題

PKIにまつわる誤解(1)

- デジタル証明書はワンタイムパスワードよりも強力な認証である
  - 認証の強度には(アルゴリズムの強度以上の)差はない
- 証明書の保管は厳重に行う必要がある
  - 厳重に管理しなくてはいけないのは秘密鍵で、証明書は公開してしまってかまわない (公開できないと証明書の意味が無い)
- 認証は証明書を相手に提示することにより行われる
  - 公開鍵暗号を使った challenge & response により、秘密鍵を知っていることを検証することにより認証は行われる
- 証明書の正当性はディレクトリサーバにより保証される
  - 証明書にされた CA による署名を検証する事により保証される

PKIにまつわる誤解(2)

- CAサーバは認証サーバである
  - CAは単に証明書を発行する(署名する)だけである。認証を行うのはその証明書を利用するクライアントとサーバ
- CAサーバは常時オンラインで参照できる必要がある
  - 純粋に証明書を発行する機能だけなら、オンラインである必要はない。必要な時以外は金庫にしまっておいてもよい
  - ディレクトリサービスや、Enrollment(証明書の申請・発行)を行う機能にはオンラインである必要がある

認証の相補性

- 「秘密」をネットワーク上で流す
  「秘密」そのものは認証するサーバ上で必要ない
  「秘密」の（例えば）ハッシュ値のみでよい
- 「秘密」をネットワーク上で流さない
  （例えば）チャレンジ&レスポンスによる認証
  「秘密」そのものが認証するサーバ上で必要

- 「共有秘密」の方式では両条件を同時に満たせない
- 「公開鍵暗号」を使うと、「秘密」をネットワーク上に流さず、またサーバ上に「秘密」を持つ必要もない

「秘密」をしまう場所

- 「共有秘密」あるいは公開鍵暗号の「秘密鍵」はクライアントの安全な場所にしまう必要がある。
- 「秘密」をハードディスクに（暗号化して）格納し、これを何か（ローカルパスワード, PIN, カード, 指紋, etc）で活性化して使えるようにするのが一般的
- さらにコンピュータと別の媒体（Token Card, IC Card, SmartCard, etc.）に「秘密」を格納するようにすれば安全

REMOTE ACCESS

リモートアクセスの問題点

- リモートアクセスの本格導入
  - イントラネット普及で、外からアクセスするニーズ
  - ダイアルアップPPPの技術の一般化
- リモートアクセスの問題点
  - セキュリティ
    - バックドアになりやすい
  - 構築および管理のコスト
    - アクセスサーバ、認証サーバ、トークンカード

リモートアクセスの認証

- 電話網における認証
  - Caller-ID (発信電話番号による制限)
    - ナンバーディスプレイサービスにより注目
    - 電話網、アクセスサーバの仕様により使用できない組み合わせもあるので注意
  - Call Back
    - Windows の Call Backは独自仕様だが、多くのアクセスサーバが対応している
- PPPにおける認証
  - PAP: クリアテキスト(平文)のパスワード
  - CHAP: Challenge & Response による認証

認証サーバ

- 認証サーバ
  - ユーザ管理・ロギングのために認証サーバを置くのが一般的
  - アクセスサーバと認証サーバ間の通信はRADIUS が事実上の標準プロトコル
  - 拡張機能の部分は個々のアクセスサーバに依存する部分が多く、設定も意外に面倒なので注意が必要
  - フリーソフトRADIUS サーバ (Livingston版、Ascend版) が多く使われていたが、商用サーバ製品も多数あり
- One Time Password
  - 認証サーバと２段構成になると管理が複雑になる
  - しかし、One Time Password 認証サーバ付属の RADIUS では機能不足の場合が多い

アクセスコントロール

- クラス分けアクセス制限は実際上有効
  - 一般ユーザはパスワードによる認証ですますが、メールサーバにしかアクセスさせない
  - 管理者は Token Card で認証を行い、全てのネットワーク資源にアクセスできる
- 実現方法
  - 「アクセスサーバ=接続時の認証を行う機器=接続後のフィルタリングを行う機器」が現時点では実際的な解
  - フィルタリングルールの設定をアクセスサーバ上で行い認証サーバ上ではフィルター番号だけを指定するか、フィルタリングルールそのものを認証サーバ上に設定するか
  - 「リモートアクセスVPN」の場合でも同じ考え方は有効

リモートアクセス３つの解

- アクセスサーバを拠点毎に配置
  - 導入および管理のコストが問題
  - 回線・機器の増強・アップグレードが大変
- ISP, VAN会社のサービスの利用
  - 閉じたサービスによる安全性とアウトソーシング
  - 認証やアクセスコントロールの自由度が問題
- VPNの利用
  - ISPに普通にダイアルアップ接続し、インターネット経由のVPNで社内システムに接続

リモートアクセスのセキュリティ

	自前アクセスサーバ	ISP,VAN のサービス利用	リモートアクセス VPN
発信番号通知	○	△	×
コールバック	○	×	×
ワンタイムパスワード	○	△	△
アクセスコントロール	○	△	○
アクセスポイントの集約	×	○	○
情報の秘匿	○	△	○

Internet からリモートログイン

- 安全な認証と暗号化が必要
- 平文パスワードはパケット盗聴の餌食に

- リモートログイン
  - One Time Password による telnet, ftp の利用
  - SSL-Telnet
  - SSH (Secure Shell)
  - PET (Privacy Enhanced Telnet)
  - VPN (IPsec, PPTP) によるリモートアクセス

SSH (Secure Shell)

- SSH = Secure な r-コマンド
  - 暗号化 DES/Triple-DES/IDEA/RC4
  - 認証 RSAを用いたチャレンジ&レスポンス
    - サーバが256bitの乱数を公開鍵で暗号化して送る
    - クライアントが秘密鍵で復号化してMD5値を送り返す
- port forwarding の仕組み
  - SSH上で X-window や POP なども使用可能
  - VPN のように全てのアプリケーションが透過的に使えるわけではない、使い方もやっかい

Windows用 SSH クライアント

- SSH の普及には Windows クライアントが鍵となる
- win32 コマンドライン版
- Cedomir Igaly 氏の SSH Windows Client
  - なかなかよく出来たGUI のクライアント
- 商用の F-Secure
  - アプリケーションの起動などの工夫で使い易い
- TeraTerm SSH plug-in
  - リモートログイン用としては日本語対応のこれがお薦め

Internet からメールアクセス

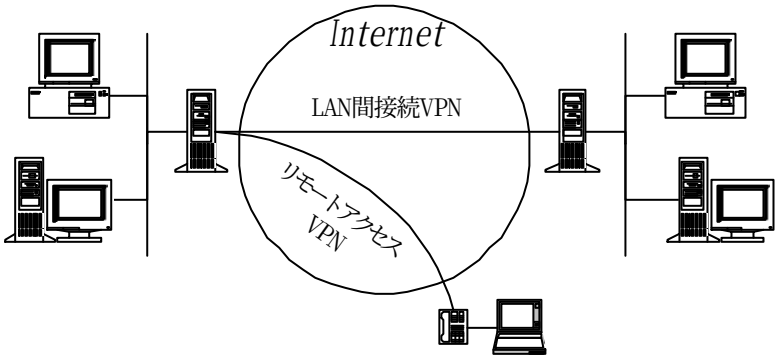
- 内部メールサーバへのアクセス
  - POP では平文パスワードが盗聴される恐れ
- APOP
  - Challenge & Response によるパスワード暗号化
  - サーバ: qpopper, DeleGate
  - クライアント: EudoraPro, Winbiff, Becky!, AL-Mail32
- WWW/Mail gateway の利用
  - ヘビィユーザ以外は、手軽に使える解
  - WebMail ゲートウェイ,メールサーバのWebサービス
  - IMAPサーバと組み合わせが特に便利
- SSL-POP, SSL-IMAP, VPN による暗号化

Virtual Private Network

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**

VPNの２つの利用形態



LAN間接続とRemote Access

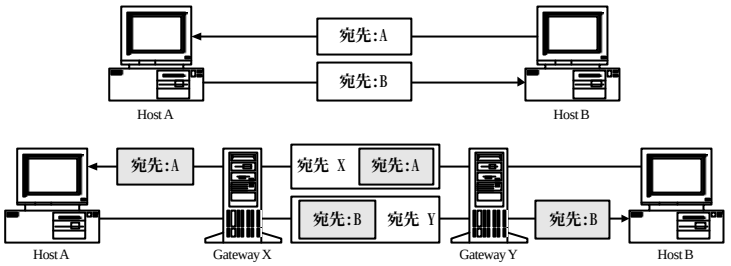
- LAN間接続VPN
  - WAN接続の置き換え、エクストラネット
  - 専用線のコストの削減
  - 帯域・遅延など全てが置き換え可能ではない
- Remote Access VPN
  - Internet から社内ネットワークにアクセス
  - アクセスサーバによるダイアルアップ接続の置き換え
  - 電話代とアクセスサーバ管理コストの削減
  - 近年関心高まる
- 同じVPNと言ってもLAN間接続とリモートアクセスでは検討すべき点・求められる機能は相当に異なる

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
- 新規格の特徴
  - 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 (ESP only での使用)
  - 鍵管理プロトコル IKE の標準化

Transport and Tunnel Mode

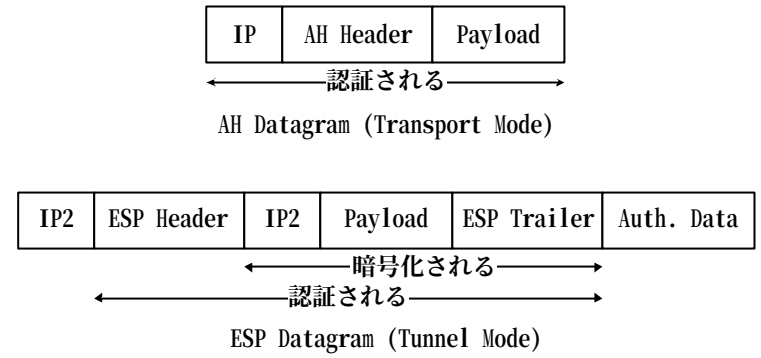
- Transport モードと Tunnel モード
  Transport モード: データ部だけを暗号化/ホスト間通信
  Tunnel モード: IPヘッダまで暗号化/VPNに適用



AH and ESP headers

- AH (Authentication Header)
  - 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)
- ESP (Encapsulating Security Payload)
  - 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)

AH and ESP Datagram



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自信で使うSAを確立
  - Phase 2 IPSecで使うSAを確立
- 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

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

IPsec の利用できる環境

- Firewall 製品の VPN オプションを持つ
- VPN 専用製品
  - LAN間接重視型とリモートアクセス重視型がある
- ルータ Cisco, Ascend, Yamaha など
- PC-UNIX
  - BSD には KAME, Linux には SWAN
- Microsoft
  - IPSec サポートは Windows 2000 から
  - Firewall, VPN製品ベンダから提供されるクライアント

IPsec の Interoperability

- 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)
  - 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

VPN と Firewall 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

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 ならゾーン別にフォワード先を変えられる

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

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。先取りで実装している製品もかなりある。

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
- 動的割り当ての機能は IETF で IPsec/IKE の拡張として検討中。先取りして実装している製品もある。

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

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

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”

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	○	○

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定額IPサービスでの利用の計画
- 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考えるベンダーもある
- 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

教育・研究機関でのセキュリティ

教育・研究機関の特殊性(1)

- 現状の把握が困難
  - 誰が何のアプリケーションを使っているかわからない
- セキュリティポリシーの策定・合意が困難
  - 多くの場合、管理者は権限者ではない
- わがままなユーザ
  - 見切り発車すると、クレーム続出
- 既存環境の変更が困難
  - 研究室単位にサーバが運用されているため
  - 設定・利用の変更の周知徹底が困難

教育・研究機関の特殊性(2)

- 「××のアプリケーションが使えなくなった」
  - 導入後にいろいろ変更が必要になる場合が多い
- 「内部から外部へは全部通す」設定にしてくれ
  - あらゆるアプリケーションに対応できる魔法のファイアウォールは存在しない
  - NAT箱の方が設定は楽なことは多い
- 問題になりやすいアプリケーション
  - H.323などマルチメディア系、ICQ、…
- IDS(侵入検地システム)の利用も一案

教育・研究機関の特殊性(3)

- 外部(インターネット)からのアクセスが必須
  - SSH、VPN などの解はあるが
  - UNIX, Windows, Macintosh のサポートが必要という点が問題
- Windows より簡単になった Linux
  - 危ないサーバがますます増える
- 悪いことをする子供の問題
- <情報コンセント>に接続される機器の管理
- 危機管理体制

参考文献

参考書籍

- 「ネットワークセキュリティ」、プレンティスホール、517頁、5200円、ISBN4-931356-98-2
- 「暗号化によるセキュリティ対策ガイド」、翔泳社、384頁、4500円、ISBN4-88135-746-8
- 「ポイント図解式VPN/VLAN教科書」、アスキー、430頁、3600円、ISBN4-7561-3191-3
- "IPSec The New Security Standard for the Internet, Intranets, and Virtual Private Networks", Prentice Hall, $44.90, ISBN0-13-011898-2
- "Virtual Private Networks", O'Reilly, 180頁, 4790円, ISBN1-56592-319-7

参考記事

http://www.netone.co.jp/doc/index.html

- インターネット・セキュリティ概論
- ファイアウォール導入の手引き
- PC環境におけるセキュリティ -電子メールを中心に-
- セキュリティのためのプロトコル
- インターネットセキュリティその現状と対応
- セキュリティポリシーの決定とファイアウォールの選び方

http://www.firewall.gr.jp/docs/

- Firewall Defenders セキュリティ関連ドキュメント

雑誌記事 (VPN)

- 「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年8月号～10月号、http://www.wide.ydc.co.jp/~sakane/doc/public/report-ipsec-cnlan9808.html
- 「TCP/IPの標準暗号プロトコルとなるIPSec」 Internet Magazine 1998年12月号、http://www.firewall.gr.jp/docs/IM199812/IM199812.html
- 「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年1月号
- 「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年10月号

雑誌記事 (認証)

- 「シングル・サイン・オンを目指す」 日経インターネットテクノロジー 1999年3月号
- 「PKIが企業ネットワークのインフラになること」 INTEROP MAGAZINE 1999年7月号
- 「カード型ユーザー認証製品」 日経インターネットテクノロジー 1999年7月号
- 「個人認証デバイスのホープ バイオメトリックス」 INTEROP MAGAZINE 1999年8月号
- 「PKI時代に備える」日経インターネットテクノロジー 1999年10月号
- 「秒読み迫る! ICカードの本格導入」 INTEROP MAGAZINE 1999年10月号
- 「PKI実践構築法」 INTEROP MAGAZINE 1999年11月号～