InternetWeek 99チュートリアル

ファイアウォール

白崎 博生 <sirasaki@iij.ad.jp>
株式会社インターネットイニシアティブ

1999/12/14

なぜファイアウォール

- インターネットの拡大
- 悪意あるユーザの増加
- 使用するソフトウェアの増加
- 多数のホストを守るのは不可能
- 壁を設けよう → ファイアウォール
  - 壁の外には数台のホスト
  - 壁の中は低いセキュリティレベル
  - いくつかのサービスは壁を越えられる

ファイアウォールの得失

- セキュリティは利便性を下げる
  - 利用できなくなるサービスがある
- 安全はただではない
  - セキュリティ × 使いやすさ ＝ 体力 ＋ 気力
  - セキュリティ × 使いやすさ ＝ お金
- ファイアウォールで安全を手に入れることはできる
  - しかし、万能ではない

ファイアウォールの役割 -1

- 境界防御を実現する
  - 外部組織からの悪意あるアクセスを防ぐ
  - 内部のユーザやデータが外に出ていくのを制御／監視する
  - 内部ネットワークの構成を外部から隠蔽する

ファイアウォールの役割 -2

- 内部のホストに高いレベルのセキュリティ対策を施さなくてもよい
  - すべてのホストに対策を施すのはたいへん
    - セキュリティパッチ、ＯＳのサービスの構成
    - ユーザの操作
  - 管理コストの低減
- ログの記録とレポーティング

ファイアウォールの役割 -3

- プライベートアドレスによるネットワーク運用を実現する
  - 内部ネットワークの構成を隠蔽することによる副次的効果
  - ネットワークアドレス空間の有効利用

ファイアウォールの役割 -4

- ユーザには利用しやすい環境を提供する
  - 透過型プロキシ

ファイアウォールを構成する要素

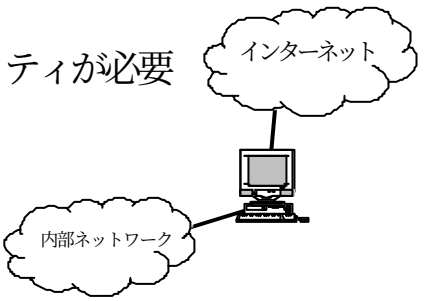
- 要塞ホスト
- デュアルホームホスト
- パケットフィルタリング
- NAT
- IP masquerade
- サーキットゲートウェイ
- アプリケーションゲートウェイ
- 透過型プロキシ

要塞ホスト
Bastion Hosts

- インターネットから直接アクセスできるホスト
  - 直接攻撃されるホスト
- 厳格なホストセキュリティが必要
  - OS
  - サービス構成
  - セキュリティパッチ
  - アカウント管理

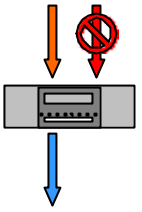
デュアルホームホスト

- ふたつのネットワークに接続したホスト
  - ３つ以上の場合もある（DMZ）
- IPフォワード機能を停止してファイアウォールにすることもある
  - 厳格なホストセキュリティが必要



パケットフィルタリング -1

- パケットレベルでのスクリーニング
  - アドレス
  - ポート番号
  - プロトコル（TCP、UDP、ICMP..）
  - インターフェース
  - 等々



パケットフィルタリング -2

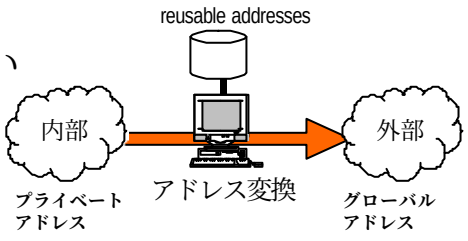
- 原則
  - 許可したものだけ通す（デフォルト拒否）
  - 拒否したもの以外を通す（デフォルト許可）

NAT
Network Address Translation - 1

- RFC-1631
- 背景
  - IP アドレスの枯渇
  - インターネットへの直接の接続を必要としないネットワークの増加
- プライベートアドレス空間の発信元アドレスをグローバル空間にマッピング

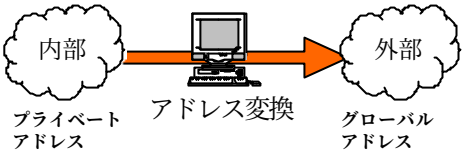
NAT
Network Address Translation - 2

- アドレスの変換
  - ポート番号は触らない
  - 静的対応
  - 動的対応
- 副次的効果として
  - 内部ネットワークの構造を隠蔽する
  - アクセス制御



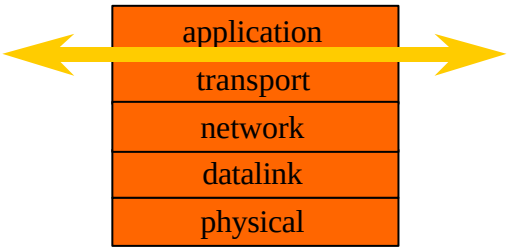
IP masquerade（NAPT）

- ポート番号も変換する
- IP masquerade ルータのアドレスだけで運用できる
  - IP アドレスを一つしか消費しない



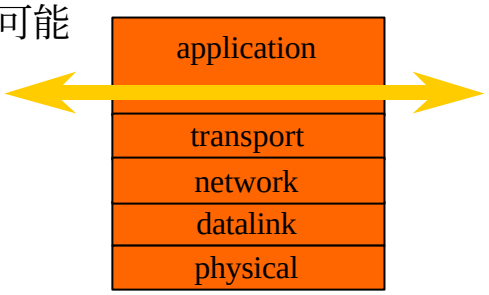
サーキットゲートウェイ

- アプリケーション層でデータを中継する
- プロトコルの内容は理解しない



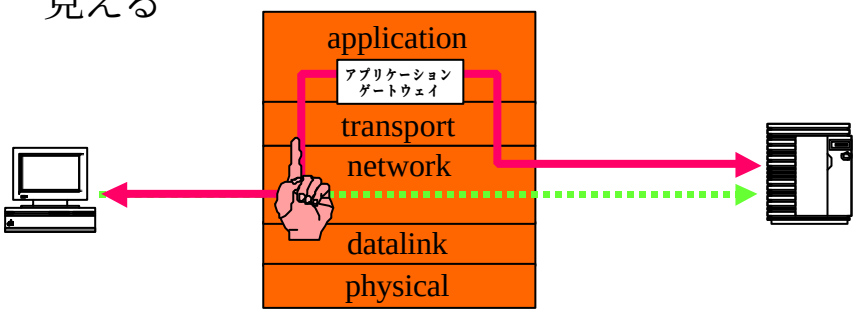
アプリケーションゲートウェイ

- アプリケーション層でデータを中継する
- プロトコルの内容を理解する
  - プロトコル内でのアクセス制御が可能
  - 監視情報の記録が可能
- ユーザ認証を組み込むことも可能



透過型プロキシ - 1

- 本来自分宛てではない接続を横取りする
- クライアントは相手と直接通信しているように見える



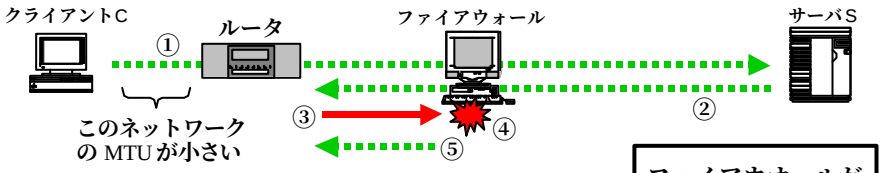
透過型プロキシ - 2

- TCP 接続のみ
- アドレス変換の効果も得られる
  - IP masquerade みたい
  - 中継しているレベルが異なる
- 特殊な状況ではトラブルの原因となることもある

  例：PathMTU Discovery が動作しない

透過型プロキシ - 3

- PathMTU Discovery が動作しない例



1. クライアントがサーバに接続する
2. サーバがクライアントにデータを送る
3. ルータが ICMP（UNREACH NEEDFRAG）を返す
4. ファイアウォールが ICMP を reject する
5. ファイアウォールが再送を繰り返す

ファイアウォールがクライアントに送信するパケット

送信元アドレス：S
送信先アドレス：C
TCPフラグ：DF

ファイアウォールの導入

ファイアウォール 導入のポイント

- セキュリティポリシーを策定する
  - ガイドライン
- 設置場所
  - 運用に支障をきたさないように
  - 物理的、論理的な位置
- 選定
  - 機能要求を明確にしておく
  - 商用 or フリー

ファイアウォールのセキュリティポリシー

- インターネットから内部へのアクセス
  - 許可する場合
    - 強力な認証と暗号化が必要
    - 他の入り口（ダイアルアップ等）を設ける
- 許可するサービスの選定
  - 全ユーザ共通 or クラス分け
- デフォルトは「許可」か「拒否」か
- 運用と監査

商用ファイアウォール-1

- コンピュータが専門ではないユーザの増加
- 攻撃手法の高度化
- インターネット上のサービスの複雑化
- 手作りファイアウォールはコストがかかりすぎ
  - 構築
  - アップデート
  - 安全性の検証

商用ファイアウォール-2

- サービスの統合
  - コンサルティング
  - 構築
  - トレーニング／セミナー
  - アップデート
  - 監視
  - 運用代行（アウトソーシング）

商用ファイアウォール-3

- ハイブリッド型ファイアウォール
  - 複数の技術を組み合わせる
  - パケットフィルタリングとアプリケーションゲートウェイ
- オールインワン型ファイアウォール
  - お手軽
  - カスタマイズの選択肢が少ない

商用ファイアウォール

- UNIX
  - Firewall-1、CyberGuard、Gauntlet、Raptor...
- Windows NT
  - Firewall-1、NetGuardian、Gauntlet、Raptor...
- Hardware
  - PIX、Firebox II、SonicWALL...

フリーファイアウォール

- 商用ファイアウォールは高い
  - セキュリティに予算をかけられるほど余裕はない
  - サポートはいらない
- 技術も時間も人材もあるが予算はない
  - 大学の研究室など
- 家庭に商用ファイアウォールなんて、、、
  - 常時接続料金の低価格化

フリーファイアウォール

- アプリケーションゲートウェイ
  - TIS FWTK
  - DeleGate
  - SOCKS
- パケットフィルタリング
  - IP filter
  - screend
  - DrawBridge
  - ルータ専用機、ダイアルアップルータ

ファイアウォール 選定のポイント -1

- 必要なアプリケーションは使えるか
- 拡張性はあるか
- 処理能力は十分か
- サポート体制は
- 動作環境
- かけられるコスト
  - 導入
  - 管理

ファイアウォール 選定のポイント -2

- プロダクトよりもサポートが重要
- 機能よりもコンセプト
- 枯れた技術
  - 新しい機能は思い通りに動かない場合も

ファイアウォール 選定のポイント -3

- フリーファイアウォールを構築する場合は
  - ポリシーとコンセプトを作る
    - 具体的に、明確に、、、
  - ベースとなる OS の選定が大切
    - 安定性と TCP/IP スタックの堅牢性
    - 不要なプログラムはインストールしない
    - いくつかのプログラムの入れ替えが必要な場合もある
  - ソフトウエアの調査をしっかりと
    - Web ページ、FAQ メーリングリスト、掲示板、書籍

アプリケーションゲートウェイ vs パケットフィルタリング

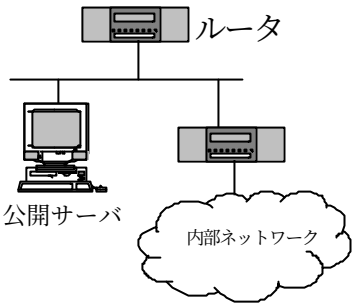
- 攻撃からの防御という点では
  - 原理的にはスキルがあればどちらでもいい
  - PF では防ぎにくい攻撃もある
  - AG でも防ぎにくい攻撃がある
- ファイアウォールを越える通信のログ
  - AG は様々なログを記録する
- 性能
  - PF が有利

ファイアウォールと UDP アプリケーション

- ファイアウォールを通すのは危険
  - UDP はパケットの偽造が簡単
- マルチメディア系のアプリケーション
  - 多くは UDP を使う
  - 汎用的なプロキシーの仕組みが難しい
  - Real Audio は独自で対応
    - UDP ポート固定、TCP 利用、proxy サーバ提供
  - RTSP に期待

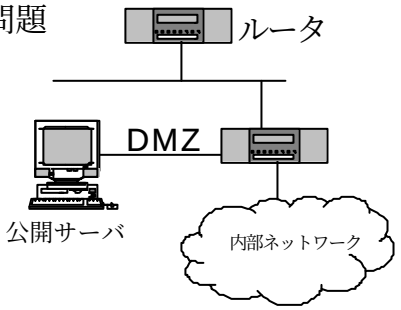
WWW、FTPサーバの配置 -1

- バリアセグメント
  - ルータのパケットフィルタリングと組み合わせる
  - サーバホストにはホストセキュリティ対策を
  - WWW と FTP は異なるホストで運用



WWW、FTPサーバの配置 -2

- 第三セグメント (DMZ)
  - Redirection proxy
    - Source address 保存の問題 (アクセスログ)
  - 性能の問題
  - ファイアウォールが止まればすべて止まる
  - すべての攻撃から防御できるわけではない



WWW、FTPサーバの配置 -3

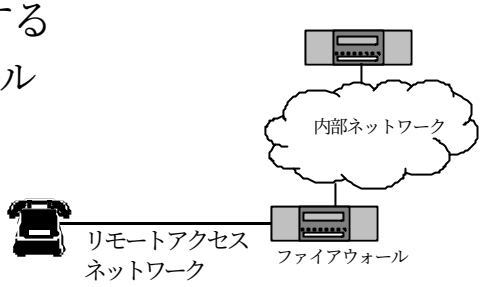
- 内部セグメント
  - おすすめしない
    - セキュリティポリシーの異なるサーバを混在させない

WWW、FTPサーバの運用

- 各サーバは chroot 環境内で稼働させたい
- サーバのコンテンツを管理する方法
  - 内部から telnet や ftp する
  - 内部からシリアル経由でログインする
  - オリジナルを内部で管理し、ミラーする
  - リムーバブルメディアを利用
- 内部の DB にアクセスする場合は
  - 専用プロキシ（SQL*Net など）

リモートアクセスサーバ

- 見落とされがち
- ここが侵入経路として利用されることも多い
- リモートアクセス用ネットワークを作り、ファイアウォールで分離する
  - 2重ファイアウォール
  - DMZ の利用



DMZ の利用

- DeMilitarized Zone（緩衝［非武装］地帯）
  - 「第三セグメント」と呼ばれることも
- 第三のセキュリティポリシーを持つネットワーク
  - 公開サーバ（WWW、FTP）を設置
  - リモートアクセスサーバを設置
  - 関連会社との接続ポイント

IPパケットのフィルタリング

- 少なくとも次のルールは設定しておきたい

方向	始点アドレス	終点アドレス	プロトコル	始点ポート	終点ポート	アクション	参照
内	自サイトのアドレス	任意	任意	任意	任意	禁止	
両方	プライベートアドレス	任意	任意	任意	任意	禁止	RFC 1597
外	自サイト以外のアドレス	任意	任意	任意	任意	禁止	RFC 2267
内	任意	ブロードキャスト	ICMP	—	—	禁止	CA-98.01

これだけでは十分ではない

Third party relay の対策

- 放置していると抗議が殺到する
- SPAM中継サイトのブラックリストに載る
  - MAPS RBL、ORBS など
- 自組織宛てではないメールは拒否する
  - 外から入ってきて外へ出ていくメール
  - ISPからメールサーバを使いたいユーザは不便
    - POP認証後SMTPを受け付ける
    - ISP の専用サービスを利用する

アプリケーションのバグへの対応

- ファイアウォール・アプリケーション
  - セキュリティパッチはすぐ当てる
- 外部からアクセスされるサーバ
  - 要塞ホストで運用する
  - サーバプログラムを信用しない
    - chroot 環境、セキュリティパッチ
- 外部にアクセスするクライアント
  - ファイアウォール上で安全な中継を行う
  - すべての中継内容の正当性を保証するのは不可能

サービス妨害攻撃への対応

- TCP/IP スタックへの DoS 攻撃
  - 難しい → よい（?）プロダクトを買う
- ネットワーク資源への DoS 攻撃
  - フィルタリングで対応
  - ISP の協力が必要な場合も
- アプリケーションへの DoS 攻撃
  - 一般にファイアウォールで防ぐのは難しい
  - 被害の拡大は防げるかも、、、

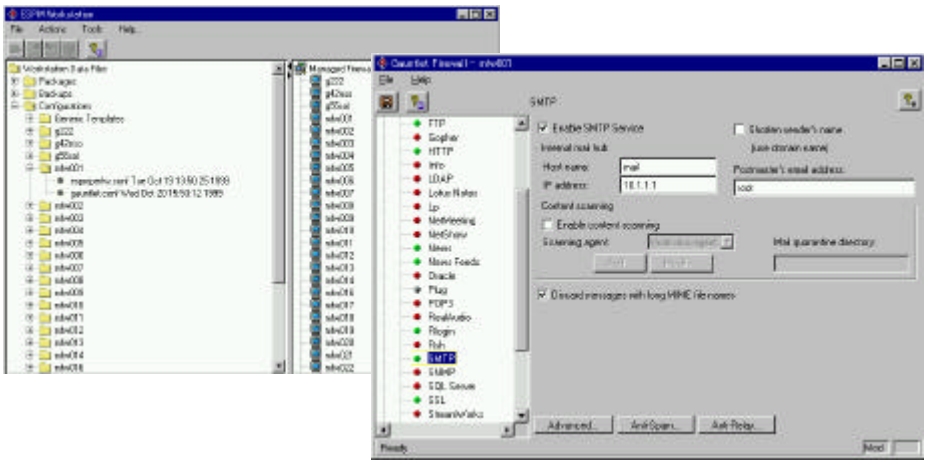
コンテンツフィルタリング

- 中継データのコンテンツをフィルタリング
  - データの内容を理解する必要がある
  - 賢いアプリケーションゲートウェイ
  - 性能上の問題
- コンピュータウィルス
  - 商用製品は実用的なレベルに達している
- Java/ActiveX
  - これからの技術革新に期待
- URL フィルタリング

ファイアウォールのリモート管理

- 複数のファイアウォールを集中管理する
  - 一つの組織内に複数のファイアウォールを導入
    - 本社と支店
    - 組織内ファイアウォール
  - 管理コストの増大
    - 一貫したセキュリティポリシーを実装
    - セキュリティパッチ、アップグレード
- リモート管理ツールを用いて集中管理

Gauntlet Firewall Maganer



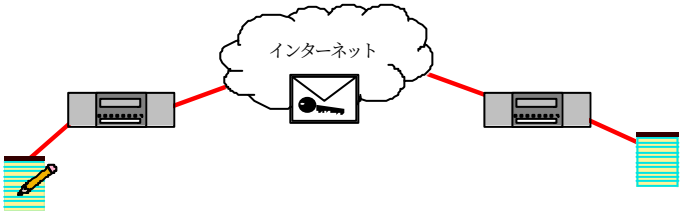
ファイアウォールの二重化

- ファイアウォールが停止すると、「自動的に」予備のファイアウォールに切り替わる
  - VRRP（Virtual Router Redundancy Protocol）
    - RFC2338
  - Firewall-1、Sidewinder、SunScreenEFS、Cisco PIX
- ファイアウォールの並列運用
  - Alteon ACE Director

暗号技術の応用

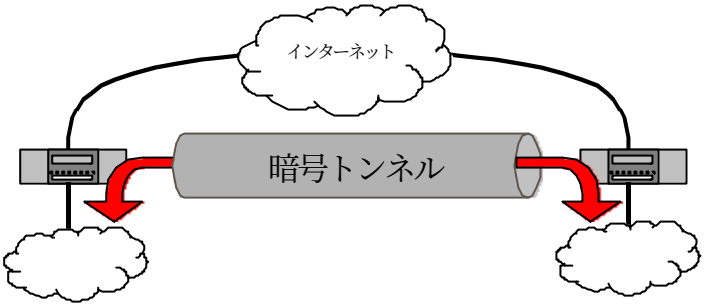
通信経路の暗号化

- インターネットを流れるデータを暗号化して、安全性を確保する
- ホスト間の暗号化
- ネットワーク間の暗号化



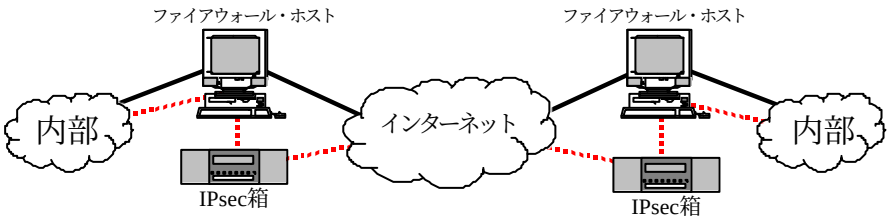
VPN
Virtual Private Network

- ネットワーク間のパケットをカプセル化する
- インターネットを使って、仮想的に専用線で接続したネットワークと同等の環境を構築できる



ファイアウォールでの暗号化

- VPN 機能を持つファイアウォール製品も多い
  - 機能的関連性は低い
- 次のような構成も可能



攻撃の防御

ファイアウォールの限界 -1

- 防げない攻撃もある
  - Denial of Service
  - ウィルス
  - 悪意ある Java や ActiveX
  - 悪意あるメッセージ
    - INNのコントロールメッセージ（JPCERT-E-INF-97-0002）
  - クライアントプログラムのバグ
    - Web ブラウザや FTP クライアント
    - 特定の URL にアクセスすると Buffer overflow が起きる

ファイアウォールの限界 -2

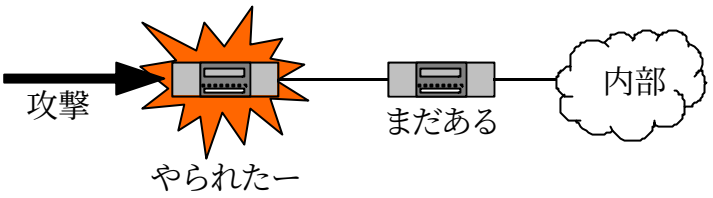
- 攻撃が成功したことを知らせてくれない
  - 失敗の検出は容易
  - 成功の検出は難しい
  - IDS との併用が必要？
- 重要なことは「限界を知る」こと
  - ファイアウォールは完全な「解」ではない

ファイアウォールへの攻撃

- ファイアウォール・アプリケーションへの攻撃
  - Buffer Overflow など
- TCP/IP スタックへの攻撃
  - Denial of Service
  - 独自実装にバグがある場合もある
- 他組織への攻撃の踏み台として利用
  - バリアセグメント上のホストを Amplifier として利用
  - http proxy も狙われやすい

それでもファイアウォール

- ファイアウォールを適切に構築しておけば、攻撃者の行動は大きく制限される。
  - 複数のコンポーネントを組み合わせる
  - フェイルセーフな設計



ユーザ教育

- ユーザは最大のセキュリティホール
- ユーザがこっそり作る穴
  - ISP にダイアルアップする
  - ファイアウォールをすり抜けるツールを仕込む
  - 自分のマシンにソフトウェアをインストールする
    - ウイルスやトロイの木馬の危険性
- ソーシャルエンジニアリング
  - 海の向こうの話ではない