INSec#9 ネットワークの防御

要素技術

ファイアウォール

- 防火壁-防火戸付き
- WIDE：ファイアウォール 基礎から応用
- 実装方式
- ファイアウォールとUTM

導入設計

方式の決定

- 付加機能
  - 侵入検知や防御機能
    - どのような攻撃検知に対応？
      - 攻撃検知のパターン=シグネイチャ
      - プロトコル
      - 攻撃種別
      - 危険度
    - 各攻撃の検知に対し、警告のみor通信の遮断？
  - ウイルス対策機能
    - ウイルス検知対象の通信
    - ウイルス検知パターンの更新頻度と更新時刻
    - 未知ウイルス検知機能利用の有無
    - 新種のマルウェア対策
  - スパム対策機能
    - 新種のマルウェア対策
    - 誤認の可能性
    - 排除メールの通知、保管
  - URLフィルタ機能
    - 新種のマルウェア対策
    - ブラックリストからホワイトリストへ
    - 利便性の考慮と相反する機能
  - VPN機能
    - 接続相手の確認
    - 通信経路上の盗聴、改ざん防止
    - …適切なポリシーに基づくアクセス制御
- 性能
  - 予備調査事項
    - インターネットの利用者数と利用パターン
    - アクセス回線の帯域
  - パケットフィルタ方式の場合
    - 性能：スループット値　bps(Bit per second)
    - FWの主な処理はパケットのヘッダに対して
      - 高：大きなパケット
      - 低：小さなパケット
        - UDP
        - ストリーミング
  - プロキシ方式の場合
    - 性能：1利用者当りの消費リソースに影響
      - CPU
      - メモリ
        - 仮想記憶
          - スワッピング…優先度により
          - メモリ領域をディスクに待避
    - 通信滞留を防ぐ
      - 利用者側の並列ダウンロード…
    - 同時接続数の制限
      - 処理性能を上げる
      - 上流、下流の回線帯域での調整
- 可用性設計と冗長化
  - コールドスタンバイ方式
    - 本番機と同じ設定・性能の予備機 → サービス停止：手動交代
  - ホットスタンバイ方式
    - 予備機が本番機を監視 → サービス停止：自動交代
    - Active/Passive(Active/Stand-by)方式
  - 本番機を複数同時稼働
    - 性能面での負荷分散
    - 障害対策
    - Active/Active方式
    - FWの負荷分散
      - 特定のIPアドレス群を同じFWへ
      - ftp系のコネクションを同じFWへ
    - persistence(持続、永続、保持)機能考慮
    - 障害時の処理能力が問題
- ポリシー設計
  - ブラックリスト方式
  - ホワイトリスト方式
  - 対象
    - IPアドレス
    - サービス
  - ネットワークのグループ化
    - cc
    - osn
    - ie
    - tec
  - サービスのグループ化
    - CLNT-OUT　http, https, ftp …
    - DMZ-OUT　dns, smtp …
    - DMZ-IN　smtp, dns, http, https …
    - SERVER-IN　dns, ftp, http, https …
- ログ監理設計
  - 利用目的
必要ログ
保存期間
    - 通信ログ　大量ログ
    - 拒否ログ　ファイアウォールによる通信拒否
    - エラーログ　ファイアウォールのエラーログ
    - 管理(監査)ログ
      - 管理画面からの参照
      - ファイルへの保存
      - syslogとしての転送
      - ftpなどによる転送
    - 通信の記録
      - 監視・調査　通信ログ　3か月～1年程度
      - 集計・統計　通信ログ　1日～1か月程度
    - セキュリティ問題の発見・調査　拒否ログ
管理ログ
通信ログ　3か月～1年程度
    - 障害の発見・調査　エラーログ
管理ログ　1週間～1か月程度
    - 運用の記録と監査　管理ログ
エラーログ　1年以上
    - ネットワーク利用の監査　通信ログ
拒否ログ　1年以上
  - リアルタイム性
↑高
↓低
    - 不正や誤りの発見
    - システム障害発見
    - システム利用傾向把握
    - システム稼働状況把握
    - 対策、統制の検証
    - 問題発生時の原因究明
  - 運用設計
    - 必要事項
      - 監視とログの検査
      - ポリシーや設定の変更
      - 障害への対応
      - ソフトウェア、ファームウェアの更新
    - 作業
      - 局面の特定(利用者からの申請、障害発生、定期保守作業等)
      - 作業を行う主体と依頼者
      - 作業の実施承認者と承認方法
      - 作業記録の保存・管理
      - 作業完了確認方法
      - 完了報告者と承認者

攻撃の検知と防御