ACTIVIDAD 1

Infraestructura de defensa: Diseño de seguridad en redes

Datos del estudiante
Nombre y apellidos: Josué David Hernández Ramírez
Fecha de entrega: Semana 6

1 Objetivos de la actividad

El presente documento detalla el diseño e implementación de una infraestructura de seguridad robusta para una organización que presta servicios a terceros, manejando información sensible y confidencial. La arquitectura propuesta integra múltiples capas de seguridad, incluyendo firewalls, sistemas IDS/IPS, VPN, y seguridad inalámbrica, garantizando la protección de datos y la continuidad operativa.

La organización cuenta con:

- Un centro de Procesamiento de Datos (CPD).
- Servdores web y de base de datos.
- Sistema de backup y mirror.
- Equipos portátiles para trabajo remoto.

2 Diseño de Arquitectura de Seguridad

2.1 Segmentación de la Red

La arquitectura implementa una segmentación en capas que incluye:

Capa 1 - Perímetro externo:

- Firewall perimetral (FW1) como primera línea de defensa.
- IDS/IPS en modo inline para análisis de tráfico entrante.

Capa 2 - Zona Desmilitarizada:

- Servidores web con acceso público controlado.
- VPN Gateway para conexiones remotas.
- Proxy server para gestión de tráfico saliente.

Capa 3 - Red Interna:

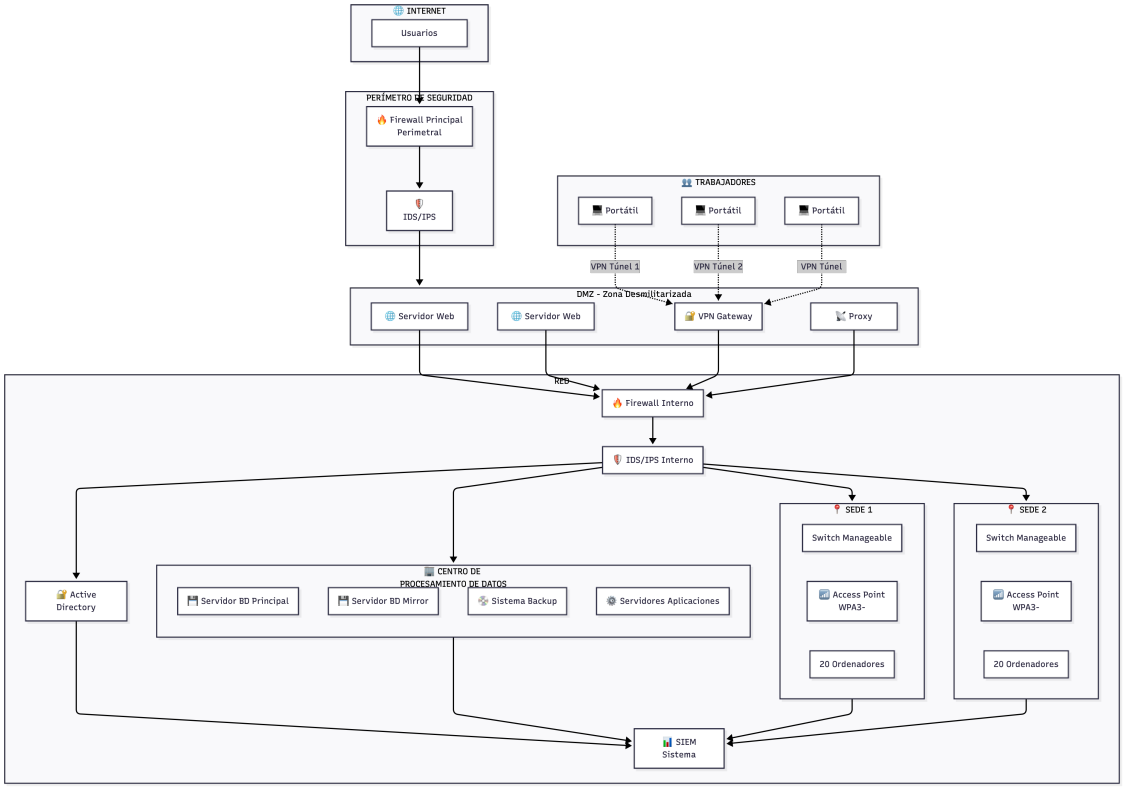

Figura 1: Diagrama de red

- Firewall interno (FW2) protegiendo recursos críticos.
- Segmentación por VLANs:
  - VLAN 10: CPD y servidores críticos
  - VLAN 20: Sede 1
  - VLAN 30: Sede 2
  - VLAN 40: Gestión y administración.
  - VLAN 50: Wireless.

Capa 4 - CPD (Centro de Procesamiento de Datos):

- Máximo nivel de seguridad.
- Acceso controlado mediante ACLs estrictas.
- Sistemas de respaldo y redundancia.

3 Configuración de Firewalls

3.1 Firewall perimetral (FW1)

Tecnología: Firewall Next-Generation (NGFW) - Fortinet FortiGate o Palo Alto
Reglas de Filtrado:

```
    # POLÍTICA POR DEFECTO: DENEGAR TODO
    # Regla 1: Permitir HTTPS hacia servidores web DMZ
    Origen: ANY
    Destino: WEB1, WEB2 (DMZ)
    Puerto: 443/TCP
    Acción: PERMITIR
    Log: SÍ
    Inspección: Deep Packet Inspection (DPI)

    # Regla 2: Permitir HTTP hacia servidores web DMZ (redirigir a
    HTTPS)
    Origen: ANY
    Destino: WEB1, WEB2 (DMZ)
    Puerto: 80/TCP
    Acción: PERMITIR (redirect to 443)
    Log: SÍ

    # Regla 3: Permitir VPN IPSec
    Origen: ANY
    Destino: VPN_GW
    Puerto: 500/UDP, 4500/UDP, ESP Protocol
    Acción: PERMITIR
    Log: SÍ
    Inspección: Verificar certificados

    # Regla 4: Permitir DNS saliente (desde Proxy)
    Origen: PROXY (DMZ)
    Destino: ANY
    Puerto: 53/UDP, 53/TCP
    Acción: PERMITIR
    Log: SÍ

    # Regla 5: Bloquear países de alto riesgo
    Origen: Lista Geo-IP (Países bloqueados)
    Destino: ANY
    Acción: DENEGAR
    Log: SÍ
    Alerta: Enviar a SIEM

    # Regla 6: Rate Limiting para prevenir DDoS
    Origen: ANY
    Destino: DMZ
    Límite: 1000 conexiones/minuto por IP
```

```
    Acción: DENEGAR exceso
    Log: SÍ

    # Regla 7: Denegar todo lo demás
    Origen: ANY
    Destino: ANY
    Acción: DENEGAR
    Log: SÍ
```

Listing 1: Reglas del Firewall Perimetral

Características Avanzadas:

- Protección anti-DDoS integrada.
- SSL/TLS Inspection para tráfico cifrado.
- Application Control (control de aplicaciones por firma).
- Web Filtering (categorización de URLs).
- Antivirus y Anti-malware en gateway.

3.2 Firewall interno (FW2)

Tecnología: Firewall de próxima generación con capacidades de microsegmentación.
Reglas de Filtrado:

```
    # POLÍTICA POR DEFECTO: DENEGAR TODO

    # Regla 1: Permitir acceso DMZ a Servidores BD (solo consultas)
    Origen: WEB1, WEB2 (DMZ)
    Destino: DB_MAIN, DB_MIRROR (CPD)
    Puerto: 3306/TCP (MySQL), 5432/TCP (PostgreSQL)
    Acción: PERMITIR
    Log: SÍ
    Horario: 24/7
    Inspección: Query validation

    # Regla 2: Permitir acceso Sedes a Servidores Aplicaciones
    Origen: VLAN 20 (Sede1), VLAN 30 (Sede2)
    Destino: APP (CPD)
    Puerto: 8080/TCP, 8443/TCP
    Acción: PERMITIR
    Log: SÍ
    Autenticación: Verificar con AD

    # Regla 3: Permitir VPN a recursos internos
    Origen: VPN_USERS (autenticados)
    Destino: VLAN 20, VLAN 30, APP
```

```
    Puerto: Según perfil de usuario
    Acción: PERMITIR
    Log: SÍ
    2FA: REQUERIDO

    # Regla 4: Permitir gestión centralizada
    Origen: VLAN 40 (Gestión)
    Destino: ALL
    Puerto: 22/TCP (SSH), 3389/TCP (RDP), 443/TCP (HTTPS mgmt)
    Acción: PERMITIR
    Log: SÍ
    Origen específico: Solo IPs de administradores

    # Regla 5: Denegar acceso directo a CPD desde Wireless
    Origen: VLAN 50 (Wireless)
    Destino: VLAN 10 (CPD)
    Acción: DENEGAR
    Log: SÍ
    Alerta: ALTA

    # Regla 6: Permitir backup schedule
    Origen: DB_MAIN, DB_MIRROR
    Destino: BACKUP
    Puerto: Protocolo backup (custom)
    Acción: PERMITIR
    Horario: 02:00-04:00 AM
    Log: SÍ

    # Regla 7: Permitir sincronización DB Mirror
    Origen: DB_MAIN
    Destino: DB_MIRROR
    Puerto: 3306/TCP, puerto replicación
    Acción: PERMITIR
    Log: SÍ
    Cifrado: TLS obligatorio

    # Regla 8: Denegar todo lo demás
    Origen: ANY
    Destino: ANY
    Acción: DENEGAR
    Log: SÍ
```

Listing 2: Reglas del Firewall Interna

4 Implementación de IDS/IPS

4.1 Sistema IDS/IPS de Entrada

Tecnología: Snort / Suricata en modo IPS inline Ubicación: Entre Firewall perimetral y DMZ