Lección 5: Seguridad Perimetral

intypedia

INFORMATION SECURITY ENCYCLOPEDIA

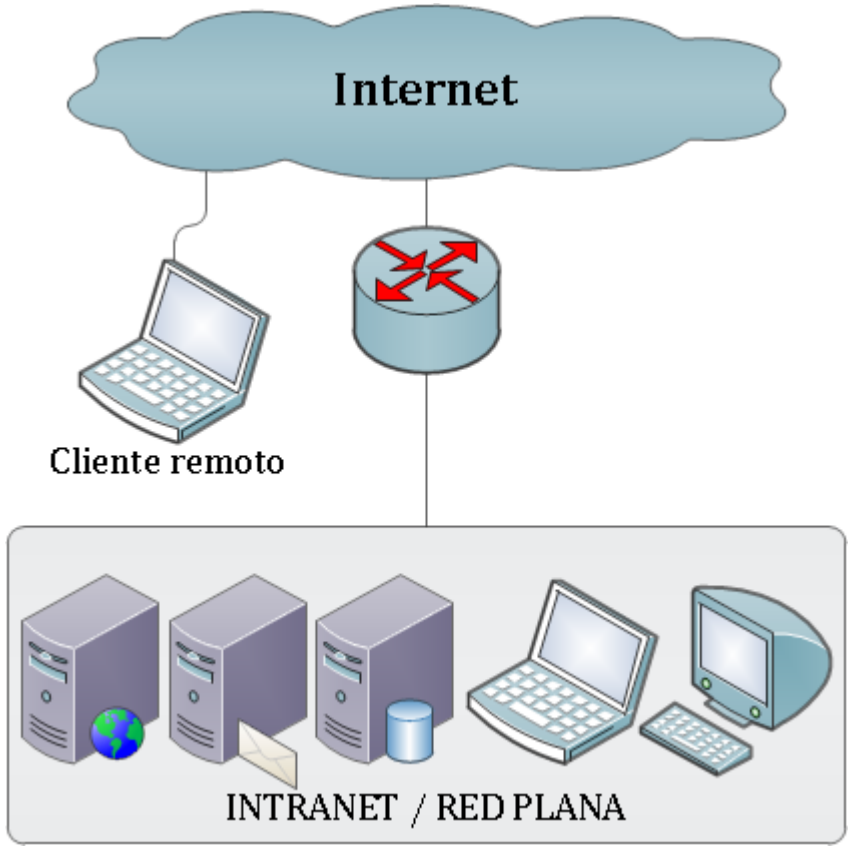
Alejandro Ramos Fraile
aramosf@sia.es
Tiger Team Manager (SIA company)
Security Consulting (CISSP, CISA)

Seguridad perimetral

- Arquitectura y elementos de red que proveen de seguridad al perímetro de una red interna frente a otra que generalmente es Internet.
  - Cortafuegos.
  - Sistemas de Detección y Prevención de Intrusos.
  - Pasarelas antivirus y antispam.
  - *Honeypots*

Ejemplo de arquitectura sin seguridad perimetral

- Red plana sin segmentar.
- Publicación de servicios internos: base de datos.
- No hay elementos de monitorización.
- No se filtra tráfico de entrada ni salida.
- No se verifica malware o spam en el correo electrónico.
- Cliente remoto accede directamente a los servicios.



Cortafuegos (Firewalls)

- Elemento de red donde se define la política de accesos, permitiendo o denegando el tráfico según se definan sus reglas.
- Dos filosofías distintos de uso:
  - √ **Política restrictiva** (lista blanca): se deniega todo menos lo que se acepta explícitamente.
  - x **Política permisiva** (lista negra): se acepta todo menos lo que se deniega explícitamente.

Cortafuegos - Tipos

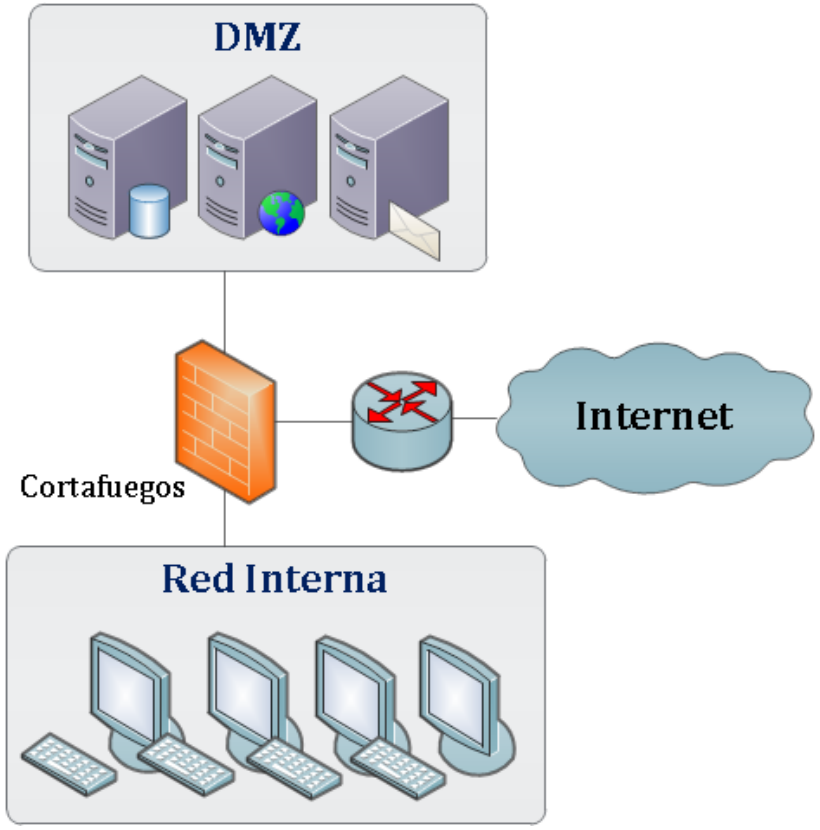
- Circuito a nivel de pasarela
  - Funciona para aplicaciones específicas.
- Cortafuegos de capa de red
  - Filtra en capa de red (IP origen/destino) o de transporte (puerto origen/destino).
- Cortafuegos de capa de aplicación
  - Funciona según el protocolo a filtrar, p. ej HTTP o SQL.
- Cortafuegos personal
  - Aplicación para sistemas personales como PCs o móviles.

Ejemplo de reglas de un cortafuegos

Regla	Acción	IP Origen	IP Destino	Proto-colo	Puerto Origen	Puerto Destino
1	Aceptar	172.16.0.0/16	192.168.0.4	tcp	cualquiera	25
2	Aceptar	cualquiera	192.168.10.8	tcp	cualquiera	80
3	Aceptar	172.16.0.0/16	192.168.0.2	tcp	cualquiera	80
4	Negar	cualquiera	cualquiera	cualquiera	cualquiera	cualquiera

Zona Desmilitarizada (DMZ)

- Diseño de una red local ubicada entre red interna y red externa (p. ej. Internet).
- Utilizada para servicios públicos: correo electrónico, dns, web, ftp, que serán expuestos a los riesgos de seguridad.
- Creada mediante uno o dos cortafuegos que restringe el tráfico entre las tres redes.
- Desde la DMZ no se permiten conexiones a la red interna.

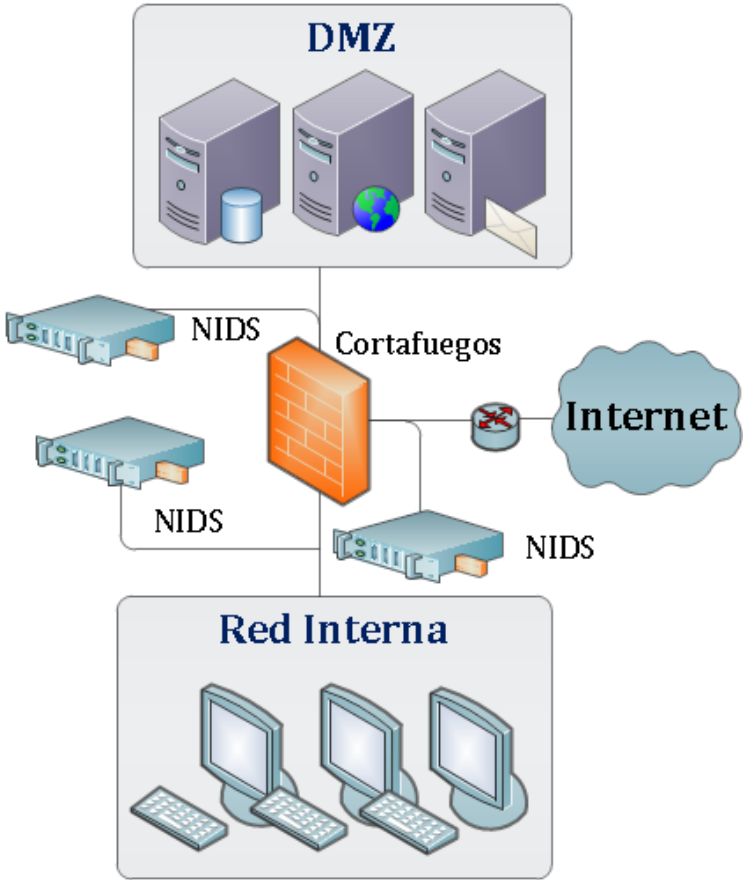


Sistemas de Detección y Prevención de Intrusos (IDS/IDPS)

- Dispositivo que monitoriza y genera alarmas si se producen alertas de seguridad.
- Los IDPS (Intrusion Detection and Prevention Systems) bloquean el ataque evitando que tenga efecto.
- Sus principales funciones:

Sistemas de Detección y Prevención de Intrusos (IDS/IDPS)

- Dos tipos de IDS:
  - **HIDS**: Host IDS, monitoriza cambios en el sistema operativo y aplicaciones.
  - **NIDS**: Network IDS, monitoriza el tráfico de la red.
- Dos métodos de detección:
  - Firmas.
  - Patrones de comportamiento.



Ejemplo de firma de IDS (snort)

alert tcp

$EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS

(**msg**:"WEB-IIS ISAPI .printer access";

flow:to_server,established;

uricontent:".printer"; nocase;

reference:arachnids,533; **reference**:bugtraq,2674; **reference**:cve,2001-0241; **reference**:nessus,10661; **classtype**:web-application-activity;

sid:971;

rev:9;)

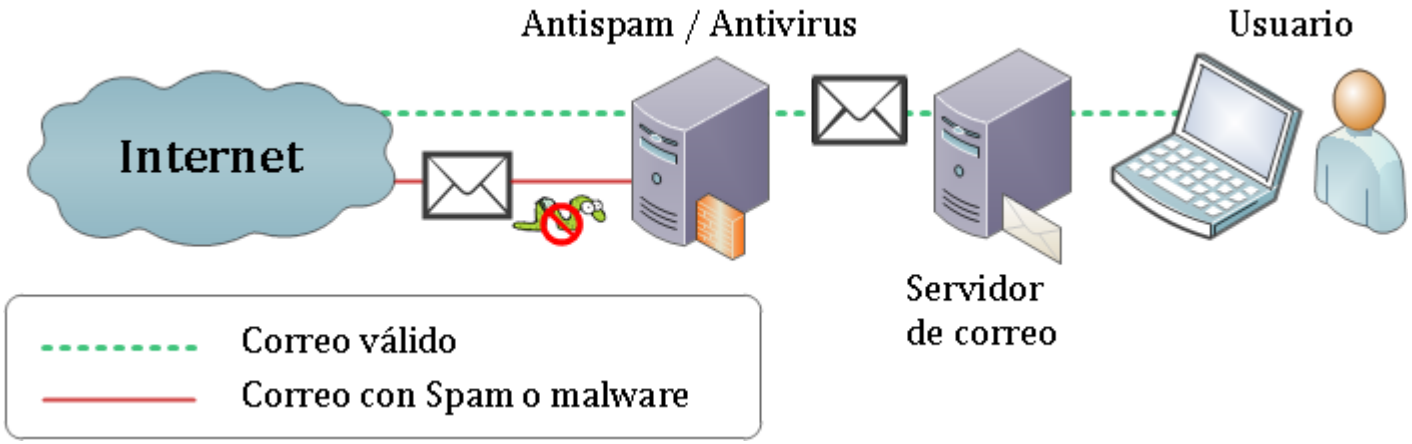
Honeypots

- Sistema configurado con vulnerabilidades usado para recoger ataques y estudiar nuevas técnicas.
- Dos tipos principales de honeypots:
  - **De baja interacción**: aplicación que simula vulnerabilidad y sistema operativo.
  - **De alta interacción**: el sistema operativo no es simulado.

- También se usan para recoger muestras de virus o spam.
- Han de permanecer especialmente controlados y desconectados de cualquier red.

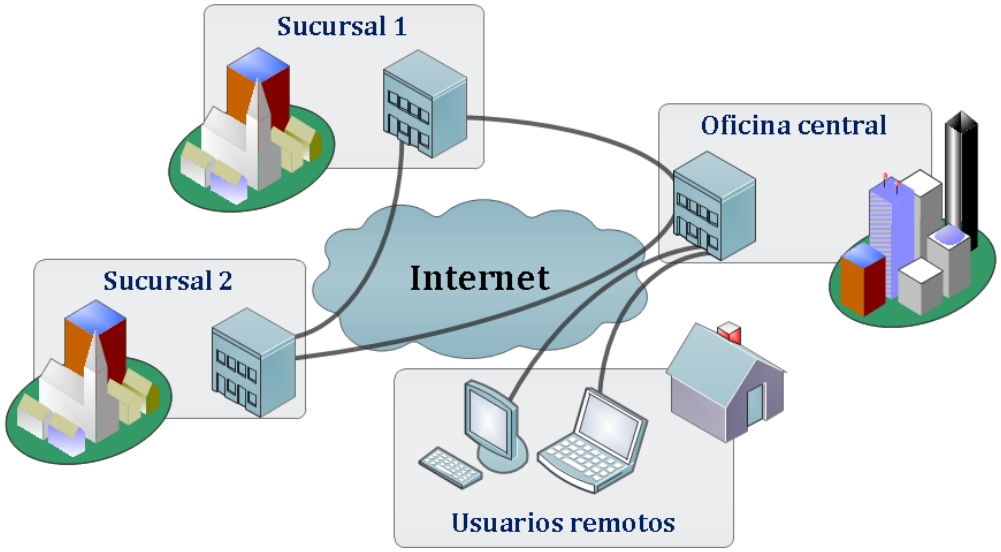
Pasarelas Antivirus y AntiSpam

- Sistemas intermedios que filtran contenido malicioso en canales de entrada a la red.
- Detección de malware en pasarelas web y servidores de correo.



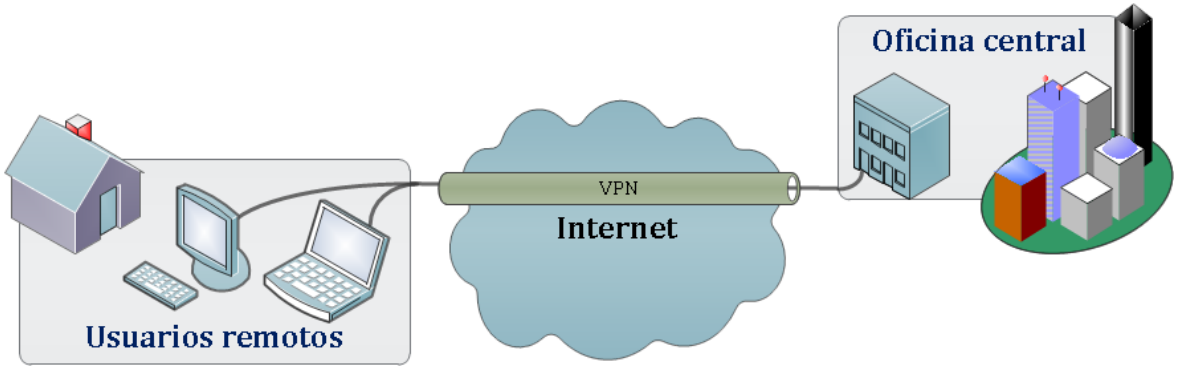
Redes Virtuales Privadas (VPN)

- Es un tipo de red que utiliza una infraestructura pública (y por lo tanto no segura) para acceder a una red privada de forma confiable.
- Es comúnmente utilizada para conectar usuarios remotos, sucursales u oficinas con su intranet (punto a punto).



Redes Virtuales Privadas - Características

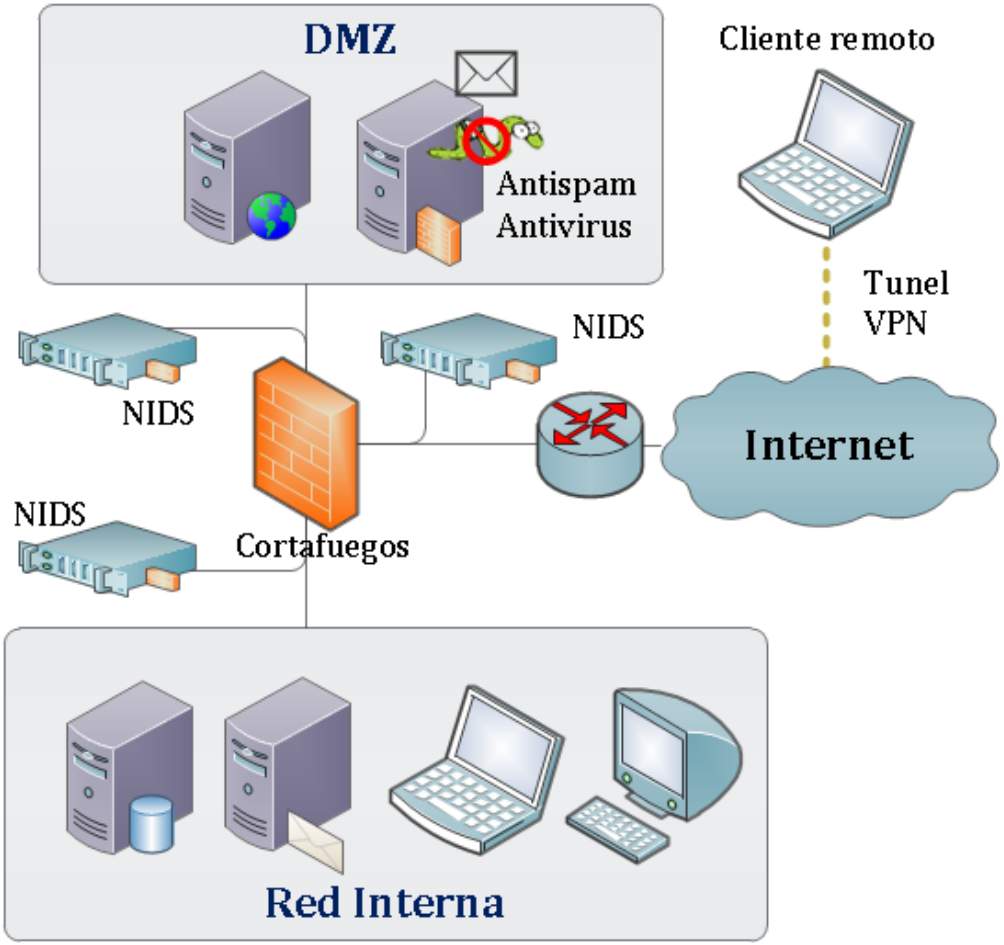
- **Autentificación y autorización**: mediante gestión de usuarios y roles y permisos.
- **Integridad**: con el uso de *funciones hash.*
- **Confidencialidad**: la información es cifrada con DES, 3DES, AES, etc.
- **No repudio**: los datos transmiten firmados.



Gestión Unificada de Amenazas / UTM

- Equipos que integran en un único dispositivo un conjunto de soluciones de seguridad perimetral:
  - Cortafuegos.
  - Sistemas de detección y prevención de intrusos.
  - Pasarelas antivirus/antispam.
  - Redes privadas virtuales.

Ejemplo de arquitectura con seguridad perimetral



- ✓ Instalación de cortafuegos.
  - ✓ DMZ y Red Interna
  - ✓ Política restrictiva
- ✓ Instalación de antispam y antivirus.
- ✓ Instalación de NIDS en las tres interfaces.
- ✓ Segmentación de servicios públicos: web y pasarela antivirus/antispam.
- ✓ Servicios internos movidos: base de datos y correo.
- ✓ Clientes remotos usan VPN.

intypedia

INFORMATION SECURITY ENCYCLOPEDIA

Contacto: info@intypedia.com