



TEMA 4 : Defensa Perimetral

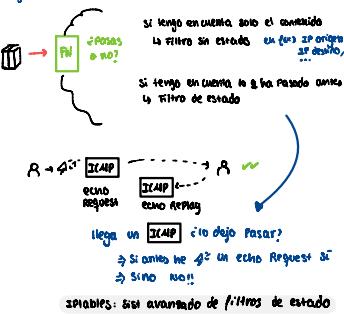
Introducción

Defensa en profundidad.



- objetivo:** Evitar que flujos de info. pase a la red de internet de autoridad externa.
→ No entendido → evitando flujos info dentro de la propia red
- **límite:** → Frontera, defendida por nuestra red
 - **implementación:** con prácticas de seguridad
 - **Soluciones técnicas empleadas:**
 - Corafuegos (firewalls)
 - Segmentación (VLAN)
 - Direccionamiento (CIDR, NIDS, IPS)
 - SSL / Portál (captive...)
 - ↳ Bonito desmitificando: El controlador A gestiona accesos A a los wifi solos/desmitificando y se utilizan para extender servicios accesibles públicamente

Ejemplo de Firewall:



Ejemplos de políticas:

- Rechazar conexiones a servicios externos o sitios comprometidos
- Permitir solo ciertos tipos de tráfico (p. ej., correo electrónico) o hacia/desde ciertos hosts.
- Canalizar la salida al exterior a través de servidores de confianza
- Redirigir el tráfico entrante a los sistemas adecuados dentro de la red interna

Corta Fuegos (FW)

Corta Fuegos: Sist o conjunto de sistemas q implementan una política de seguridad entre la red corporativa y al exterior (normalmente Internet)



Clasificación

- **Filtrado de IP:** Conjunto de reglas q se aplican a los IP y circuitos a través del firewall (adisa como router)
 - ↳ **Tipos de filtrado:** Equitativo, Dinámico, Circuito, con estado
- **Pasarela de nivel de aplicación (Proxy)**
- **Pasarela de nivel de circuito**
- **Habilitados:** Ej: Filtrado con estado e inspección contenido



El Router actúa como Router restringiendo datos rumores IP en IP q verifiquen o no las reglas de filtrado

Tipos de filtrado

Estricto: las decisiones de toman de forma lineal. Para cada IP se tiene en cuenta: interface, rumbo cabecera IP o **info orquestado nivel superior** cabeceras TCP, UDP, ICMP, ...

Dinámico: se crean nuevas reglas de filtrado en IP del tráfico cuando surgen cambios (reglas reflexivas)

↳ Esto permite aceptar respuestas q han sido originadas por nuestro tráfico

Con Estado: se maneja info. sobre las conexiones activas permitir un control más sofisticado

Ej: NO aceptar segmentos TCP invertidos, solo aceptar respuestas TCP a interacciones generadas por nuestros distinguimos enviados

Pasarelas de Aplicación (Proxy)

Application-level Gateways

- Actua como un intercambiador, reenviando las peticiones entre zonas. No hay intercambio de IP entre las internas y externas (forward desacreditado)
- **Gateway:** det. las reglas de tránsito y/o autenticación + habitualmente, filtra contenidos

ej: Savid



• Se config. en servidores segurizados (hosts bastion) q están ubicados donde la red externa (vive ser BASH)

• **Bashon:** se routing ≠ servicios de proxy

controles → Bashon → nuevos contenidos → dependientes del protocolo anterior
procesos sub reglas de atención → dependientes del protocolo anterior

• Pueden incluir autenticación de usuarios
• Control exclusivo de la conexión
↳ análisis, contenido
↳ control de accesos por servicios, usuarios,...

• Puede config. como servidor transparente → requiere su config. a los clientes

Proxy o Pasarela de Circuitos

Circuit-level Gateways

- 2 Pasarelas de aplicación pero sin revisar su contenido

Ej: Protocolo SOCKS vs



Host Bastión

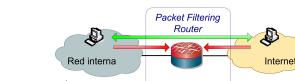
- config. para realizar las tareas de seguridad
- ↳ host secuizado < usuarios y servicios ejecutan necesarios
- ↳ Sigue estar protegido por FW y otros Sist de filtrado
- Gest. de Intrusos (IDS)
- Permite implementar pasarelas de **Aplicación** Circuito

Arquitecturas de Cortafuegos

Packet Filtering Router Dual-homed host Screened host
Screened Subnet Split Screened Subnet

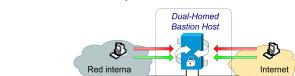
Packet Filtering Router

ARQ más simple → con capacidad de filtrado se definen reglas de paso



Dual-homed host

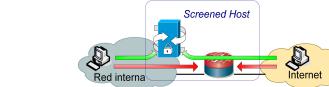
Se config. un host bastión con al menos dos interfaces
desabilita la IP externa y se config. los servidores proxy



Screened host

↳ bloques todo el tráfico hacia/desde red interna, excepto si está originado/destinado al bastión

↳ se config. los proxies [filtrado IP ?]



TEMA 4 : Defensa Perimetral

Corta Fuegos (FW)

Arquitecturas de Cortafuegos

Screened Subnet

- \square DMZ \rightarrow implementa los proxy
- \square s \rightarrow aislan las redes y obligan a pasar por el \square



Split Screened Subnet

Variante con más nivel de aislamiento
No hay visión directa entre los \square s, todo pasa por el Bastión



Nota: en cualquier ARD puedes colocar IDS para q lo detecte automaticas

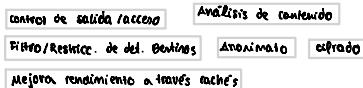
Implementación de un Cortafuegos

- 1) Escoger Arq adecuada a las necesidades de la red
- 2) Def. política de filtrado para los routers
- 3) Def. Proxy + Política de accesos \rightarrow Bastión
- 4) Seleccionar la variedad productos \rightarrow instalar config. iguales
- 5) Def. política de monitorización y mantenimiento de los sistemas
- 6) Concentración de los usuarios, especialmente sobre la apertura nuevas puertas (accesos ADSL, conexiones Móviles, Access Points)

Proxies e Intermediarios

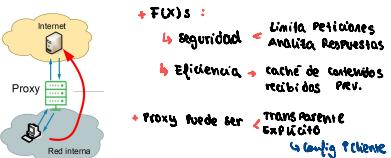
Servicio red q actua como **intermediario** en los intercambios territorialmente red \leftrightarrow Internet

Funcionalidades

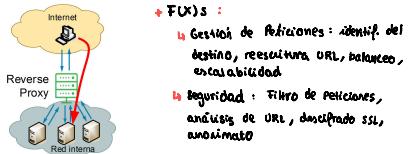


- Tipos
 - P. Directo \rightarrow controla tráfico \leftrightarrow Internet \rightarrow siguiente
 - P. Inverso \rightarrow controla tráfico \leftrightarrow Internet entrante

Proxy o Forward Proxy



Proxy inverso o Reverse Proxy



- Funciones:
 - Gestión de Peticiones: identif. del destino, redirección, URL, balanceo, escalabilidad
 - Seguridad: filtro de peticiones, análisis de URL, desencriptado SSL, encriptado
 - Eficiencia: caché de contenidos servidos previamente

Detección de Intrusiones

Intrusión

conjunto de acciones q intentan comprometer CID de un sistema informático evitando los mecanismos \square

IDS: Sistema de Detección de Intrusos

- Sist SW/HW q detecta \rightarrow identifica a actividades no autorizadas/anormales (anomalías)
- Monitoreo + análisis continuo de eventos q/o tráfico curioso
- Las intrusiones pueden activar mecanismos de respuesta
 - \hookrightarrow IPS Intrusion Prevention System

Típs de los IDS

Detección ataques desde sus direccs

Documentación ataques notificados (forenses)

Detección actividades indebidas, anormales o no autorizadas q no han sido bloqueadas por otros medios

Control de calidad de los sistemas de seguridad \exists

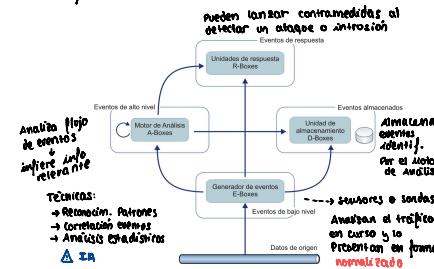
Reconocer info maliciosas comunes + detección usos inesperados

ARQ de un zOS \rightarrow CISIF

Common Intrusion Detection Framework

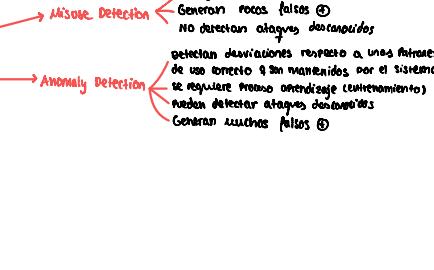
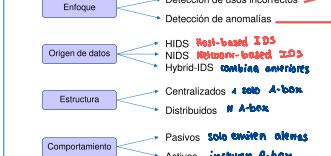
- Intento unificar componentes y formatos:
 - \Rightarrow CISI: Common Intrusion Specification Language
 - \Rightarrow IDMEF: Intrusion Detection Message Exchange Format
- 4 Componentes básicos de CISIF q se comunican mediante \square s
 - Generador de eventos E-boxes
 - Motor de análisis A-boxes
 - Unidades de Almacenaje D-boxes
 - Unidades de Respuesta R-boxes

Ejemplo:



Clasificación IDS

IDS. Criterios de clasificación



Misuse Detection \rightarrow config para reconocer patrones de ataque NO detectan ataques desconocidos
detectan deviaciones respecto a unas fórmulas de uso correcto q son mantenidas por el sistema se requiere proveer entorno de ejecución
pueden detectar ataques conocidos
Generan muchos falsos \square

Anomaly Detection \rightarrow detectan ataques desconocidos
detectan ataques que no cumplen con las normas establecidas
generan muchos falsos \square

IPS !!