Clase XIV

Diseño de redes de datos (DRD101)

Agenda

- Seguridad perimetral
- Firewalls

Seguridad Perimetral / Firewalls

Seguridad perimetral

Los objetivos principales de la seguridad perimetral informática son:

- Soportar los ataques externos
- Detectar e identificar los ataques recibidos y alertar acerca de ellos
- Segmentar y asegurar los sistemas y servicios en función de su superficie de ataque
- Filtrar y bloquear el tráfico ilegítimo

Antivirus

Es un programa informático que se utiliza para prevenir, detectar y eliminar el malware.

Se desarrolló originalmente para detectar y eliminar virus informáticos, de ahí el nombre. Sin embargo, con la proliferación de otros programas maliciosos, el software antivirus comenzó a protegerse de otras amenazas informáticas. En particular, el software antivirus moderno puede proteger a los usuarios de troyanos, gusanos, adware, spyware, etc.

Servidor AAA

Autenticación, autorización y contabilidad (**AAA**), es un conjunto de servicios que se utilizan para controlar el acceso a los recursos informáticos, hacer cumplir las políticas, evaluar uso y proporcionar la información necesaria para facturar los servicios.

Servidor AAA

Autenticación.

Proporciona una forma de identificar a un usuario, normalmente haciendo que el usuario ingrese un nombre de usuario válido y contraseña válida antes de que se conceda el acceso. El servidor AAA compara las credenciales de autenticación de un usuario con otras credenciales de usuario almacenadas en una base de datos. Si las credenciales coinciden, el usuario puede acceder a la red. Si las credenciales no coinciden, la autenticación falla y se deniega el acceso a la red.

Servidor AAA

Autorización.

Es el proceso de hacer cumplir las políticas: determinar qué tipos de actividades, recursos o servicios a los que un usuario puede acceder. Después de que un usuario está autenticado, ese usuario puede estar autorizado para diferentes tipos de accesos o actividades.

Servidor AAA

Accounting

Mide los recursos que consume un usuario durante el acceso, que pueden incluir la cantidad de tiempo del sistema o la cantidad de datos que un usuario ha enviado o recibido durante una sesión. Se lleva la contabilidad a través del registro de estadísticas de sesión e información de uso, que se utiliza para la autorización actividades de control, facturación, análisis de tendencias, utilización de recursos y planificación de la capacidad.

Servidor AAA

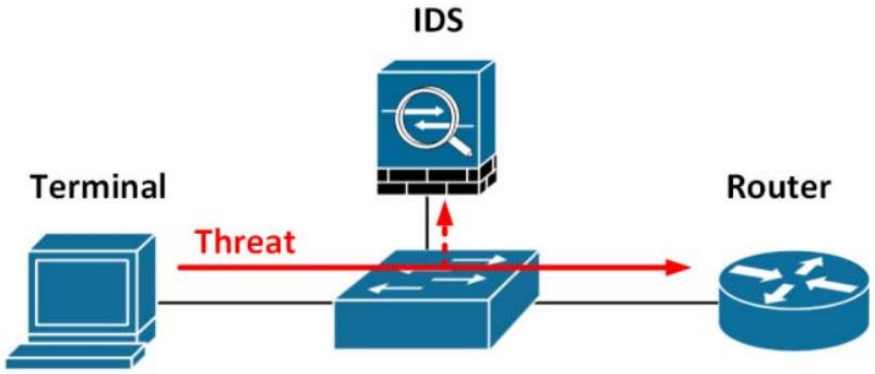
Servidores AAA

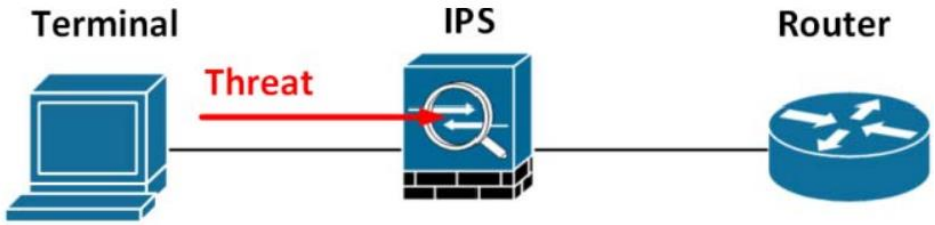
El servidor AAA es un servidor de red que se utiliza para el control de acceso. La autenticación identifica al usuario. La autorización implementa políticas que determinan qué recursos y servicios un usuario autenticado puede acceder. La contabilidad (Accounting) realiza un seguimiento del tiempo y los recursos de datos que se utilizan para la facturación y el análisis.

IDS / IPS

Sistemas de detección y/o prevención de intrusión (IDS/IPS)

Inspeccionan el tráfico de red en base a firmas de ataques conocidos o en base a comportamientos/patrones de tráfico anómalos para la detección y/o prevención de intrusiones.





Sistemas anti-DDoS

Este tipo de sistemas que previenen o mitigan los ataques de **denegación de servicio (DoS)** o los **ataques distribuidos de denegación de servicio (DDoS)**.

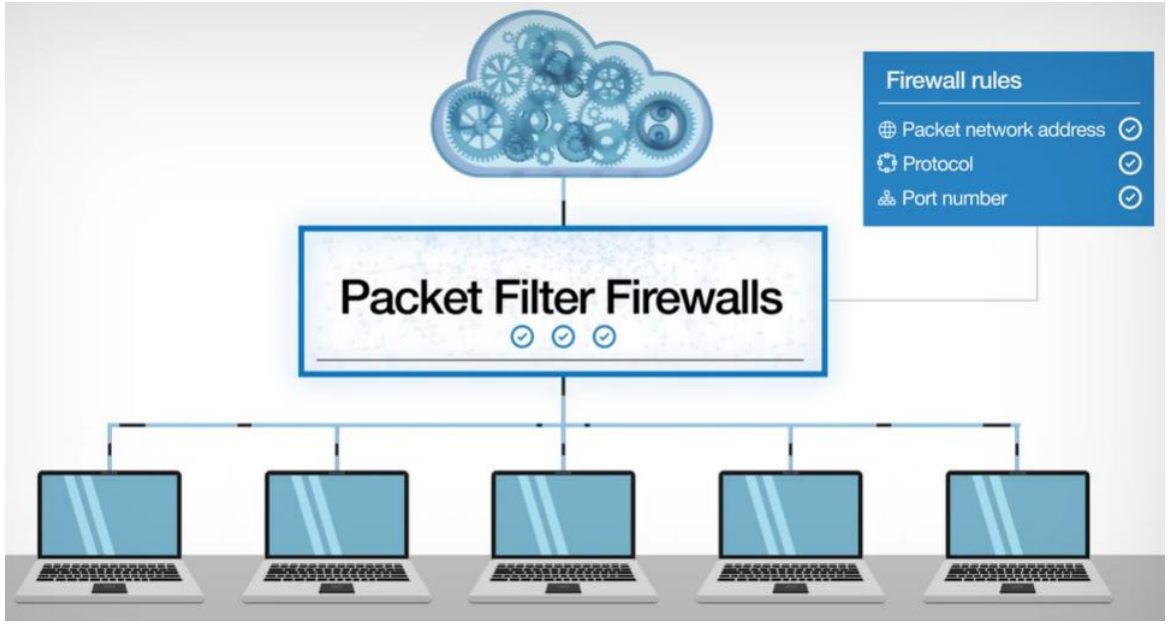
Generalmente necesitan un tiempo de aprendizaje para modelar cuál es el comportamiento normal o las tendencias en el tráfico de la red, estableciendo unas líneas base de los distintos volúmenes de tipos de tráfico para que una vez se pongan en modo bloqueo, cuando se produzca un ataque y se detecten desviaciones de las líneas base, sean capaces de bloquear o mitigar dichos ataques evitando que el tráfico anómalo ingrese a la red.

Firewall

Un **firewall** o cortafuego, se utiliza para mantener la seguridad de la red interna bloqueando accesos no autorizados, también se encarga de filtrar el tráfico originado desde la red interna. Un firewall puede ser implementado mediante software, hardware o una combinación de ambos.

Primera generación de firewalls

Desarrollados en 1988, son conocidos como **packet filter firewalls**, se encargan de inspeccionar paquetes, si el paquete hace match con una regla de acceso es permitido, sino es denegado (con la posibilidad de enviar un mensaje al emisor)



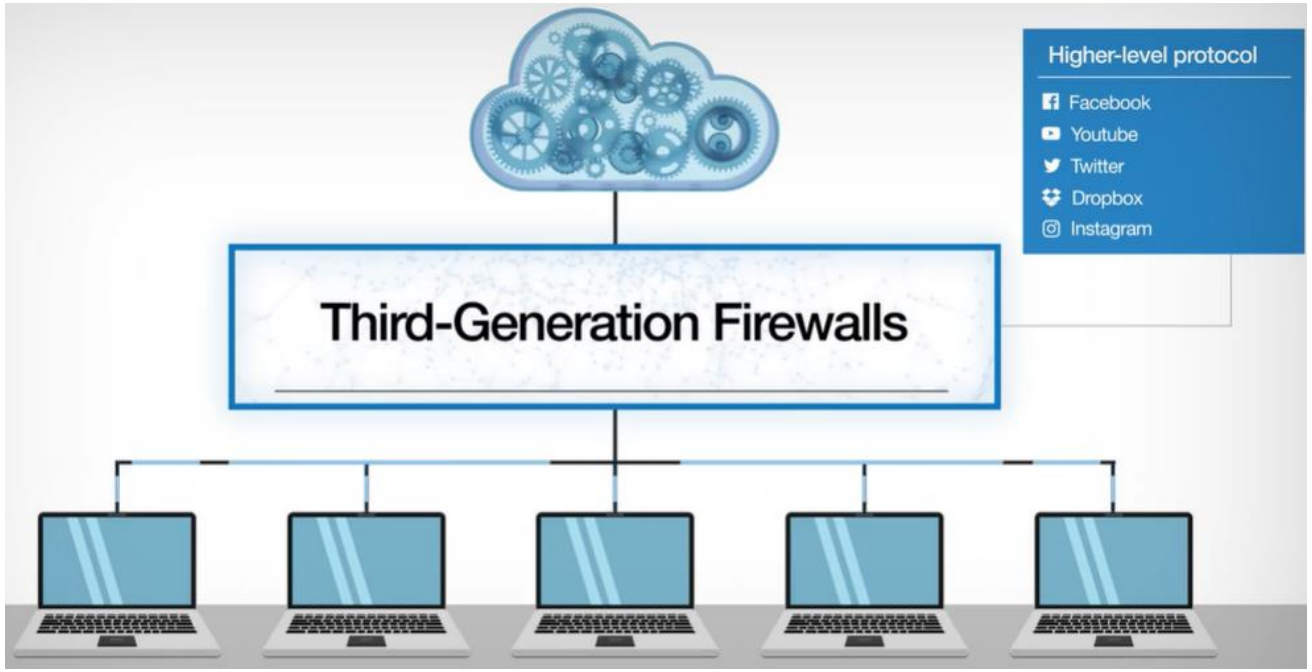
Segunda generación de firewalls

Conocidos como **stateful firewalls**, realiza las funciones de proxy e intercepta los paquetes para revisar su contenido y decidir si debe ser aceptado o bloqueado.

HTTP
- Static text content
- E-commerce
- File hosting
- Web applications

Tercera generación de firewalls

Conocidos como **application layer firewalls**, permiten generar alertas en tiempo real, consultar bases de datos de amenazas en Internet, identifican actividades sospechosas, tienen la capacidad de manejar altas cantidades de tráfico.



VPN IPsec

El termino **IPSec** viene de IP “Internet Protocol” y sec “Secure”. IPsec es un grupo de protocolos que son utilizados juntos para la configuración de conexiones encriptadas entre dispositivos. Lo anterior mantiene los datos seguros cuando son transmitidos por una red pública. IPSec es utilizado para la configuración de **VPNs** (Virtual Private Networks) y trabaja encriptando paquetes IP con autenticación en el origen de la transmisión de los paquetes.

¿Cómo funciona IPsec?

Paso 1: Definición de tráfico interesante (dominio de cifrado).

Las listas de control de acceso con accion **permit** indican cuál es el tráfico que sera encriptado por el túnel VPN.


```
access-list 101 permit ip 10.0.1.0  0.0.0.255 10.0.2.0 0.0.0.255
```

Access lists determine traffic to encrypt

- Permit—traffic must be encrypted
- Deny—traffic sent unencrypted

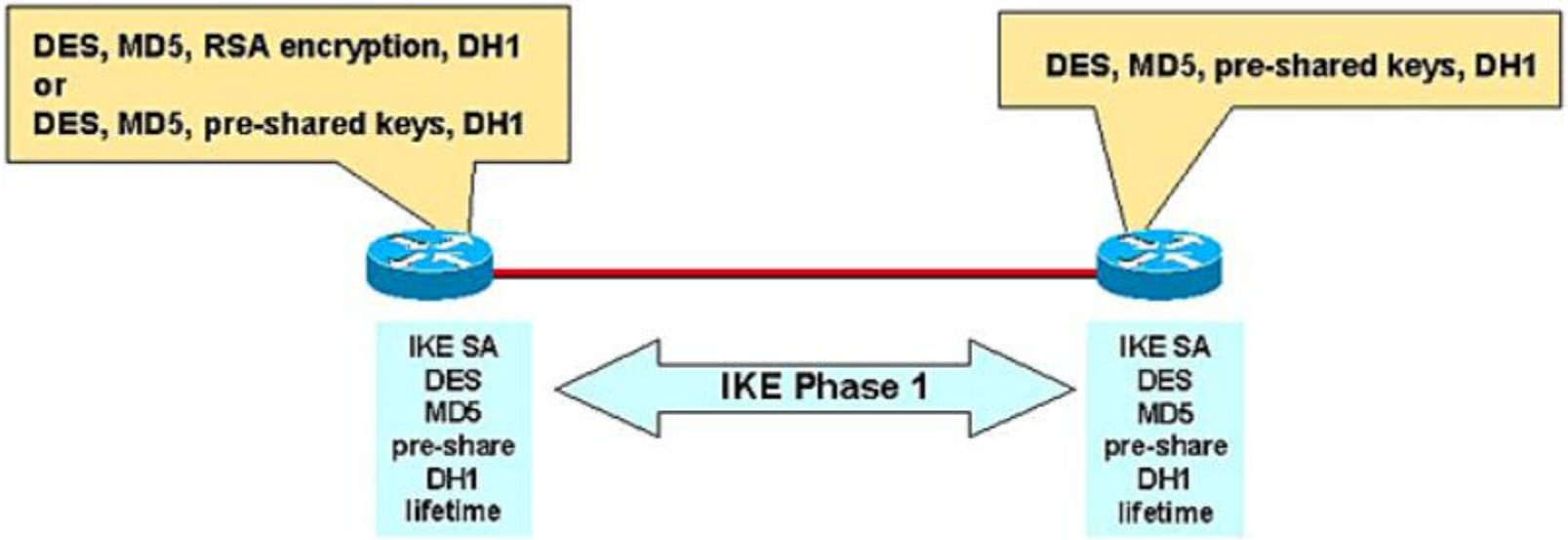
¿Cómo funciona IPsec?

Paso 2: Definición de fase 1 (IKE / ISAKMP).

El propósito básico de fase 1 es autenticar los peers IPSec y configurar un canal seguro entre ellos. Fase 1 realiza las siguientes funciones:

- Autentica y protege las identidades de los peer IPSec.
- Negocia y empareja las **IKE SA (Security Associations)** entre los peers durante el intercambio **IKE (Internet Key Exchange)**.
- Realiza un intercambio de llaves **PSK (Private Shared Keys)**

¿Cómo funciona IPSec?



- Autentica peers IPSec.
- Negocia el emparejamiento de políticas para proteger el intercambio IKE.
- Intercambia las llaves criptográficas mediante el método Diffie-Hellman.
- Establece la asociación de seguridad IKE.

¿Cómo funciona IPsec?

Paso 3: Definición de fase 2 (IPsec).

El propósito de fase 2 es negociar las IPSec SA y configurar el túnel IPsec. Fase 2 realiza las siguientes funciones:

- Negocia los parámetros IPsec SA protegidos por un existente IKE SA.
- Establece los IPsec SA
- Periódicamente renegocia los IPsec SA para garantizar la seguridad.

¿Cómo funciona IPsec?

Paso 4: Túnel IPsec Encriptado

Después que la fase 2 ha sido completada, los paquetes son encriptados y desencriptados usando la encripción definida en el IPsec SA.

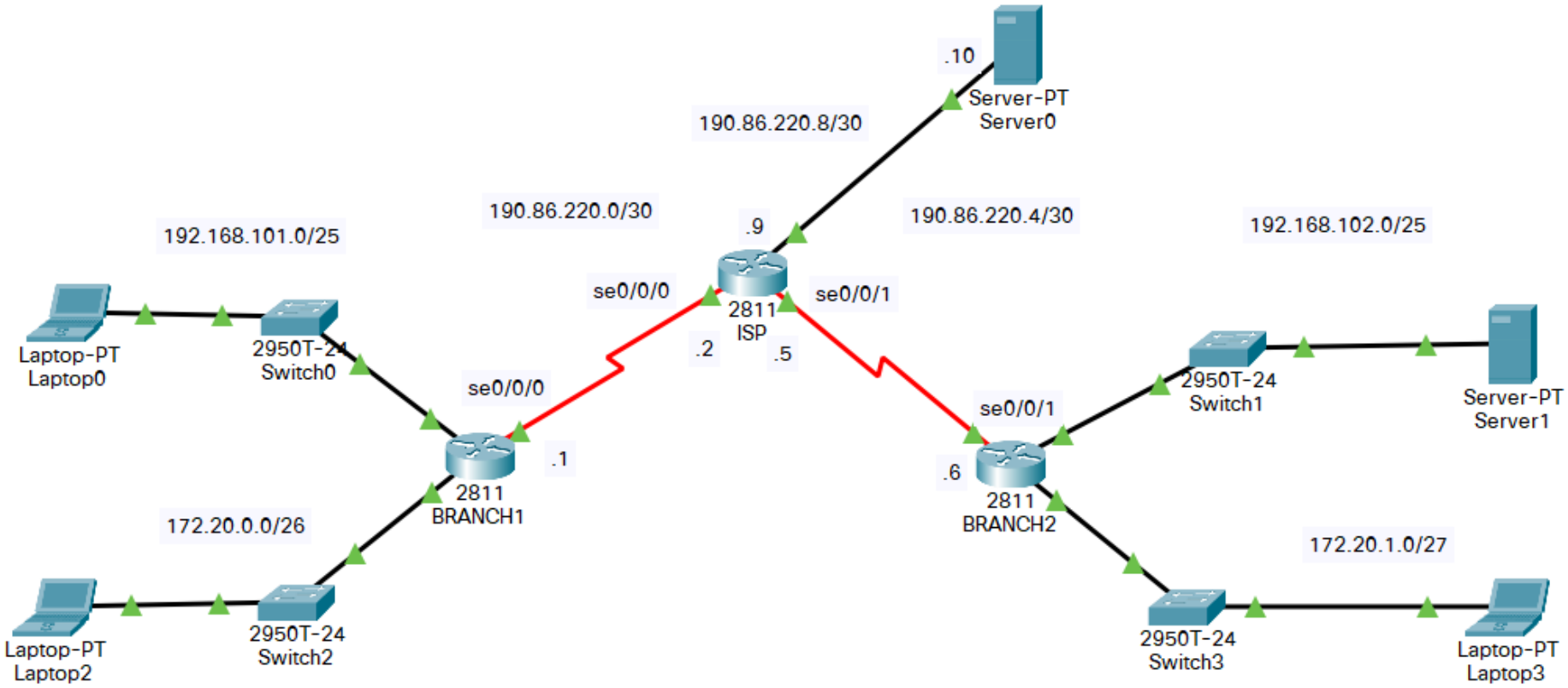
¿Cómo funciona IPsec?

Paso 5: Terminación de túnel

IPsec SA finaliza a través de su borrado o agotamiento de tiempo de espera. Si es necesario se reestablecimiento se negociarán nuevas SAs y nuevas llaves.

Ejemplo práctico

Con base a la siguiente topología:



Ejemplo práctico

Configurar una VPN S2S utilizando los siguientes parámetros:

IKE/ ISAKMP Encryption (Phase 1)

Parámetro	Valor
IKE Version	1
Authentication method	PSK
Encryption method	AES-256
Authentication algorithm	SHA-1
Diffie-Hellman group	5
Encryption lifetime	86400 secs

IPsec Encryption (Phase 2)

Parámetro	Valor
Encryption method	AES-256
Authentication algorithm	SHA-1
PFS	Enabled
PFS Diffie-Hellman Group	5
Key renegotiation time	86400 secs

UNIVERSIDAD DON BOSCO

VITAM IMPENDERE VERO

EDUCACIÓN SUPERIOR CON ESTILO SALESIANO

AUTORIDAD DE AVIACIÓN CIVIL A.A.C. EL SALVADOR
Certificación del Técnico en Mantenimiento Aeronáutico
2016-2021

ACAAI
Agencia Centroamericana de Acreditación de Programas de Arquitectura y de Ingeniería

ISPO
INTERNATIONAL SOCIETY FOR PROSTHETICS AND ORTHOTICS
Acreditación Internacional en la carrera de Técnico en Ortesis y Prótesis
Presencial 2016-2021
A distancia 2018-2020

CdA
Comisión de Acreditación Calidad de la Educación Superior
UNIVERSIDAD DON BOSCO
ACREDITADA
2017 - 2022

Instituciones Salesianas de Educación Superior