Seminario de Seguridad Informática con énfasis en hacking ético.

joseroberto.rivas@itservicesin.com

503-78876717

CLASE 007 27/Marzo/2021

INGENIERO JOSE ROBERTO RIVAS MAGAÑA. MBA. M.SC.

DOCENTE MINED NIVEL I, GERENTE DE PROYECTOS Y AUDITOR LIDER INTEGRADO.

003-Defensa en profundidad

DEFENSA EN PROFUNDIDAD

22/3/2021 11:40:08

Proceso de defensa por capas, llamado Defensa en profundidad, Protección en profundidad o seguridad en profundidad. (Cada capa es un control).

- Múltiples oportunidades de monitoreo para detectar el ataque.
- Controles adicionales que el atacante debe superar, lo que crea un retraso que puede interrumpir o evitar el ataque.

A menudo es importante usar varios controles para proteger un activo y el número y los tipos de capas necesarios es una función de:

- Valor de activo y criticidad.
- La fiabilidad de cada control. El grado de exposición.

EN TERMINOS DE ARQUITECTURA

La defensa en profundidad, (Terminos de arquitectura)

- DEFENSA EN PROFUNDIDAD HORIZONTAL

➢ Los controles se colocan en varios lugares en la ruta de acceso para un activo (Modelo de Anillos Concéntricos).

- DEFENSA EN PROFUNDIDAD VERTICAL

➢ Los controles se colocan en diferentes capas del sistema. Hardware, sistema operativo, aplicaciones. Bases de datos y nivel de usuario.

IMPLEMENTACIONES DE DEFENSA EN PROFUNDIDAD

Al desarrollar implementaciones de defensa en profundidad, considere las siguientes preguntas:

- ¿Qué vulnerabilidades son tratadas por cada capa o control?
- ¿Cómo mitiga cada capa la vulnerabilidad?
- ¿Cómo interactúa o depende cada control con los otros controles?

004-Control de flujo de información.

FIREWALL

Un firewall es un sistema o combinación de sistemas que impone un límite entre dos o más redes.

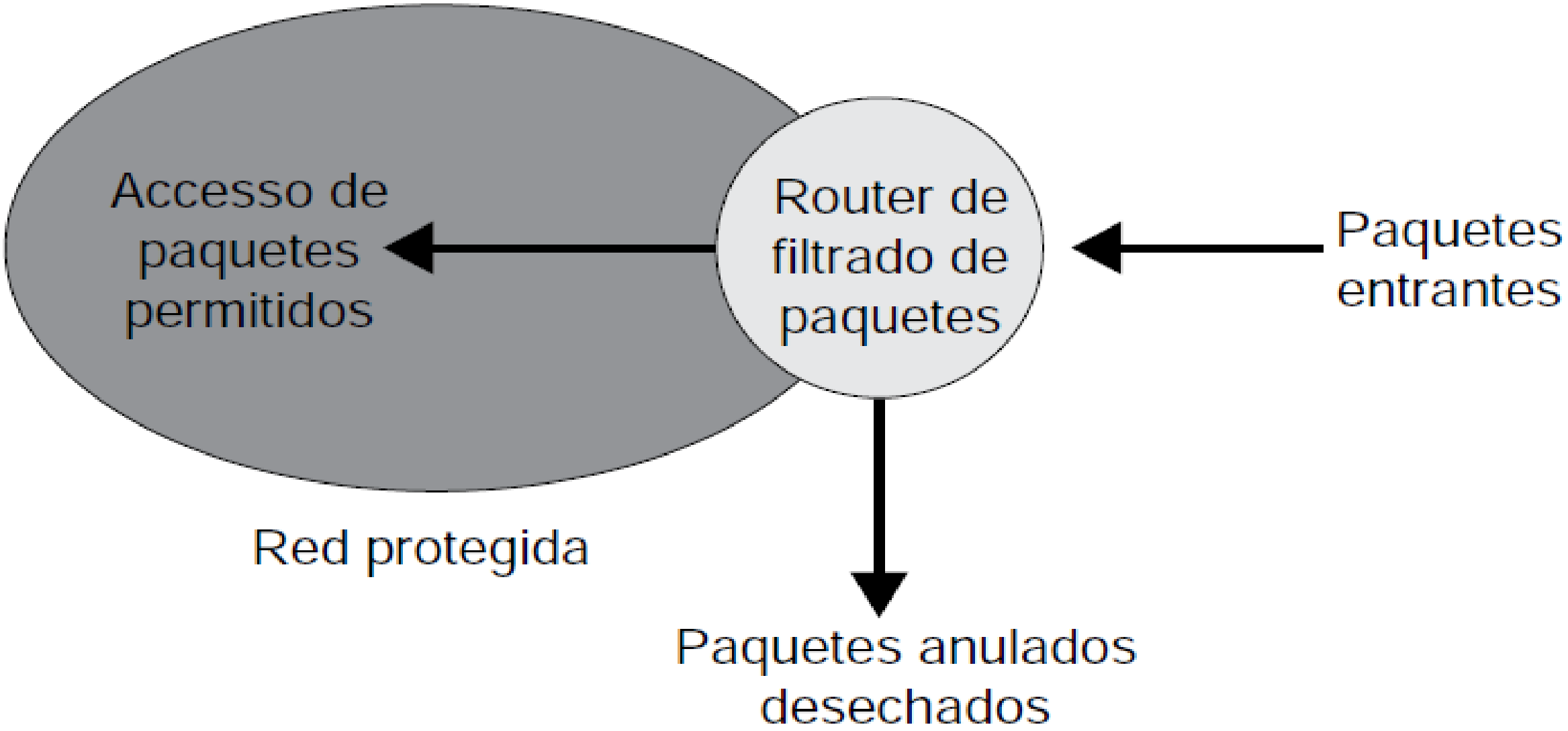
Por lo general, forma una barrera entre un entorno seguro y abierto, como Internet, aplica reglas para controlar el tipo de tráfico de red que entra y sale.

TECNOLOGÍAS DE FIREWALL

- Filtrados de paquetes.
- Firewall de Aplicación.
- Inspección a nivel del estado.
- Firewall de próxima generación

Figura 3.9—Firewall de filtrado de paquetes

22/3/2021 11:40:08



Fuente: ISACA, *Manual de Preparación al Examen CRISC 6ª edición*, EE.UU., 2015

Figura 3.10—Firewall de filtrado de paquetes

Ventajas	Desventajas
Simplicidad de un "choke point" (cuello de botella) de red	Vulnerable a ataques de filtros no configurados de manera apropiada
Minimo impacto en el rendimiento de la red	Vulnerable a ataques de túnel sobre servicios permitidos
Poco costoso o gratuito	Todos los sistemas de red privada son vulnerables cuando un router de filtrado de paquete se ve comprometido

Figura 3.11—Firewall de aplicación

22/3/2021 11:40:08

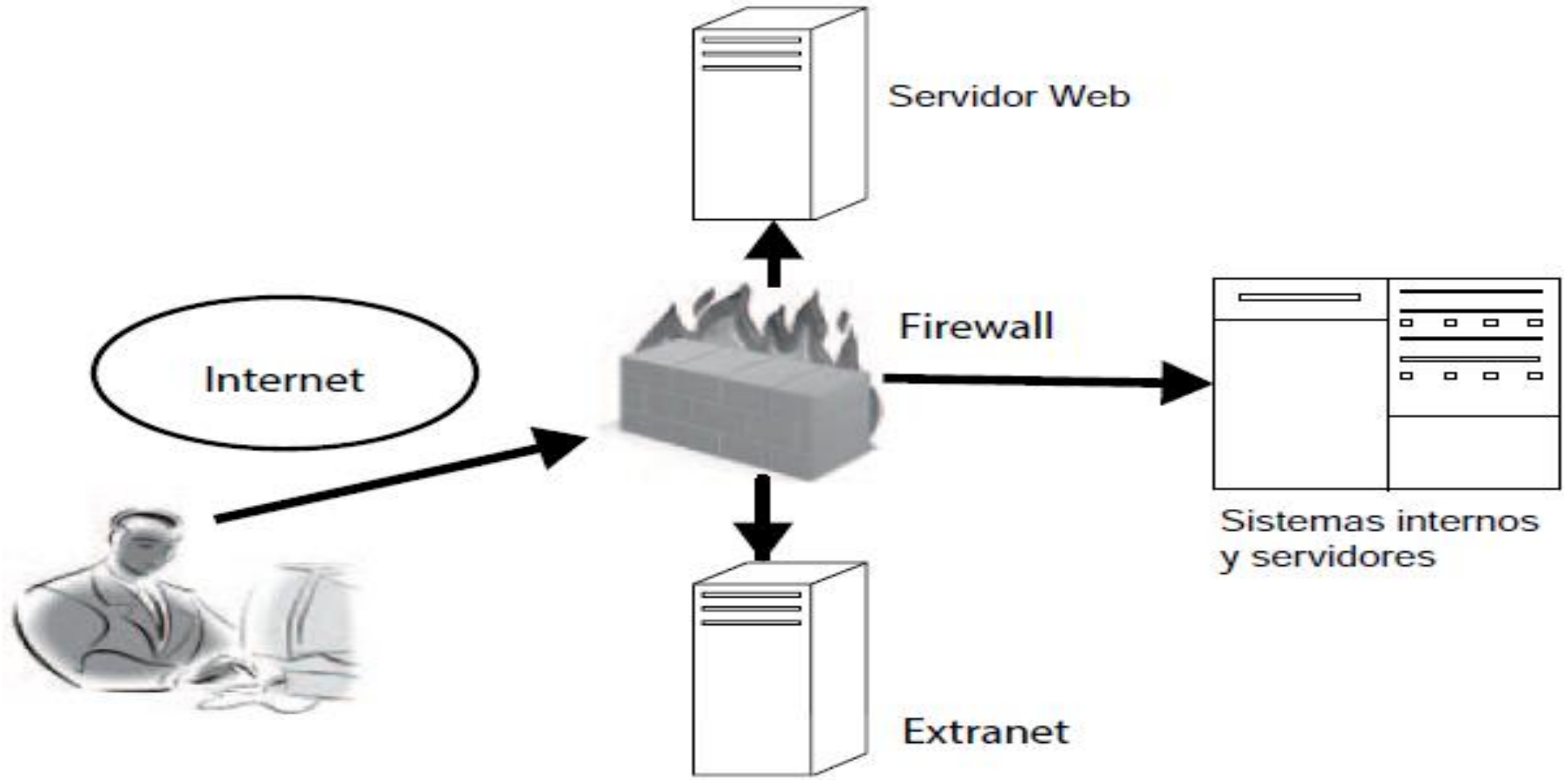
Ventajas	Desventajas
Proporcionan seguridad para los protocolos usados con más frecuencia	Reducción de rendimiento y escalabilidad conforme crece el uso de internet
Por lo general esconden la red de redes externas no confiables	
Tienen la habilidad de proteger toda la red a limitar los robos a la misma firewall	
Tienen la habilidad de examinar y asegurar el código de programar	

Figura 3.12—Firewall de inspección de estado

22/3/2021 11:40:08

Ventajas	Desventajas
Proporcionan un mayor control sobre el flujo de tráfico IP	Son complejas de administrar
Mayor eficiencia en el intensivo de CPU, en comparación con los sistemas de firewall de aplicación de tiempo completo	

Figura 3.13—La zona desmilitarizada



Fuente: ISACA, *Manual de Preparación al Examen CRISC 6ª edición*, EE.UU., 2015

FIREWALL DE APLICACIONES WEB (WAF)

Un firewall de aplicación web (WAF) es un complemento de servidor, dispositivo o filtro adicional que se puede usar para aplicar reglas a una aplicación web específica (generalmente a una comunicación HTTP).

WAF opera a niveles más altos en el modelo OSI, generalmente en el nivel 7.

En contraste, los firewalls de red operan en el nivel 3 o nivel 4.

WAF puede personalizarse para identificar y bloquear muchos tipos de ataques, como Cross-site scripting (XSS) y la Inyección de SQL, pero la personalización requiere un esfuerzo y muchos cambios cuando las aplicaciones cambian.

05-Aislamiento y segmentación

AISLAMIENTO Y SEGMENTACIÓN

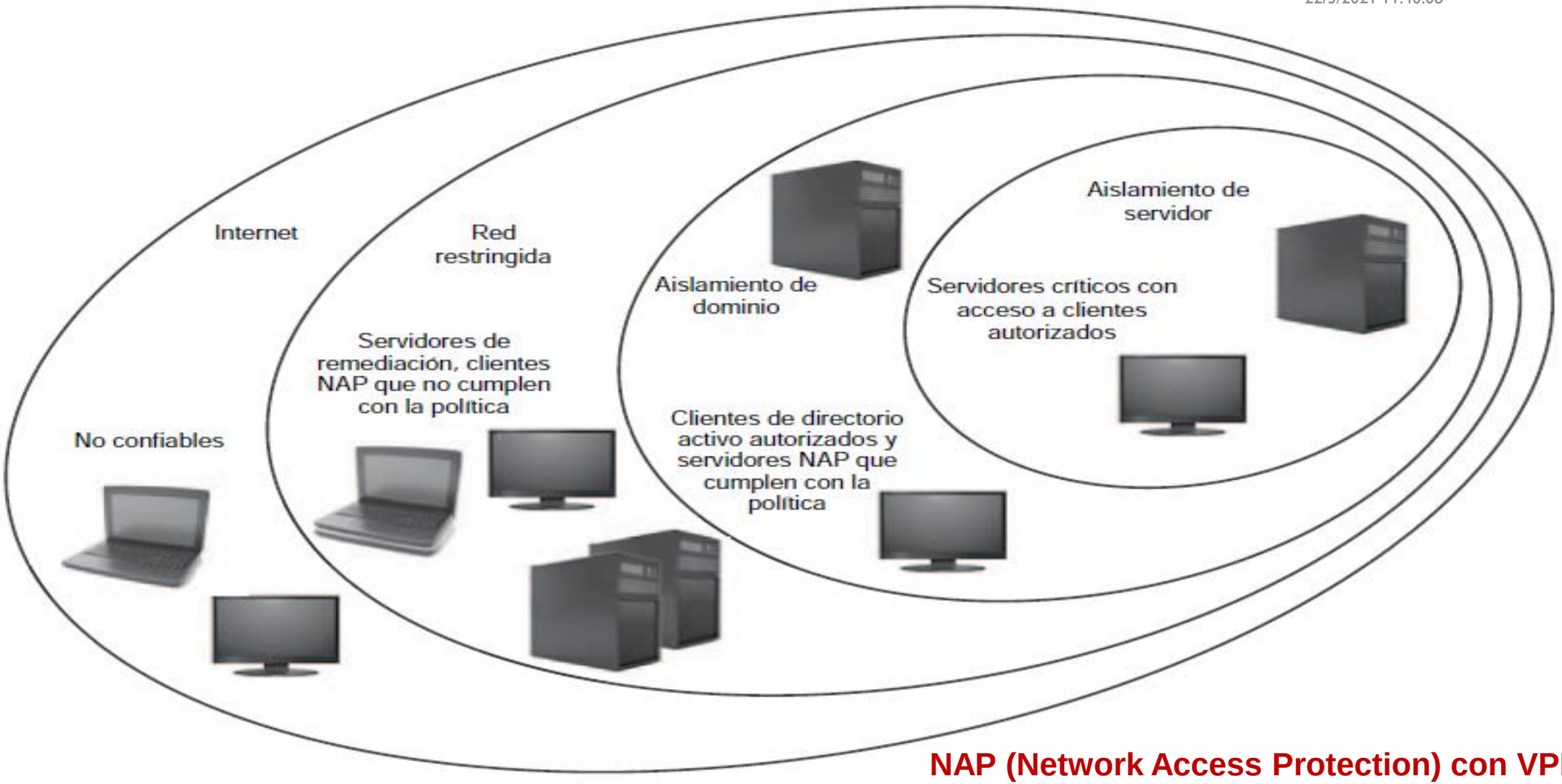
Una técnica común para implementar la seguridad de la red es segmentar la red de una organización.

Cada segmento puede ser controlado, monitoreado y protegido por separado.

Las redes de área local virtuales (VLAN) son grupos de dispositivos en una o más LAN segmentadas lógicamente. Características:

- Sin encriptación adicional
- Configurar configurando puertos en un conmutador
- Configuración basada en conexiones lógicas en lugar de físicas

Figura 3.14—Modelo de Aislamiento y Segmentación



NAP (Network Access Protection) con VPN

TEMA 6

Registro, monitoreo y detección

COMPONENTES INTEGRALES DE CIBERSEGURIDAD

El monitoreo, la detección y el registro son partes integrales de la ciberseguridad. Los ataques y la pérdida de datos representan problemas potenciales en ambos lados, por lo que es necesario monitorear los datos y la información que fluye dentro y fuera de una organización.

La mayoría de estos métodos giran en torno a los conceptos centrales de comunicación de ingreso, salida de la red y la prevención de pérdida de datos.

REGISTRO

Un registro de log, es un registro de eventos que ocurren dentro de los sistemas y redes de una organización.

El registro es una de las herramientas más valiosas para monitorear controles y detectar riesgos. Debe contener:

- Hora del evento, Cambios a permisos, Inicio o apagado del sistema
- Inicio de sesión y cierre de sesión, Cambios a datos, Errores o violaciones
- Tareas fallidas.

Si no se revisan los registros de logs, la organización puede no ser consciente de un ataque en curso.

REGISTRO (RETOS MAS COMUNES)

22/3/2021 11:40:08

Los retos mas comunes relativos al uso efectivo de los registros de log son:

- Tener demasiados datos
- Dificultad en la búsqueda de información relevante
- Configuración inapropiada (p.ej. no estar habilitados o no tener los datos apropiados)

Modificación o borrado de datos antes de su lectura (p.ej. espacio de almacenamiento demasiado pequeño

SISTEMAS SEM

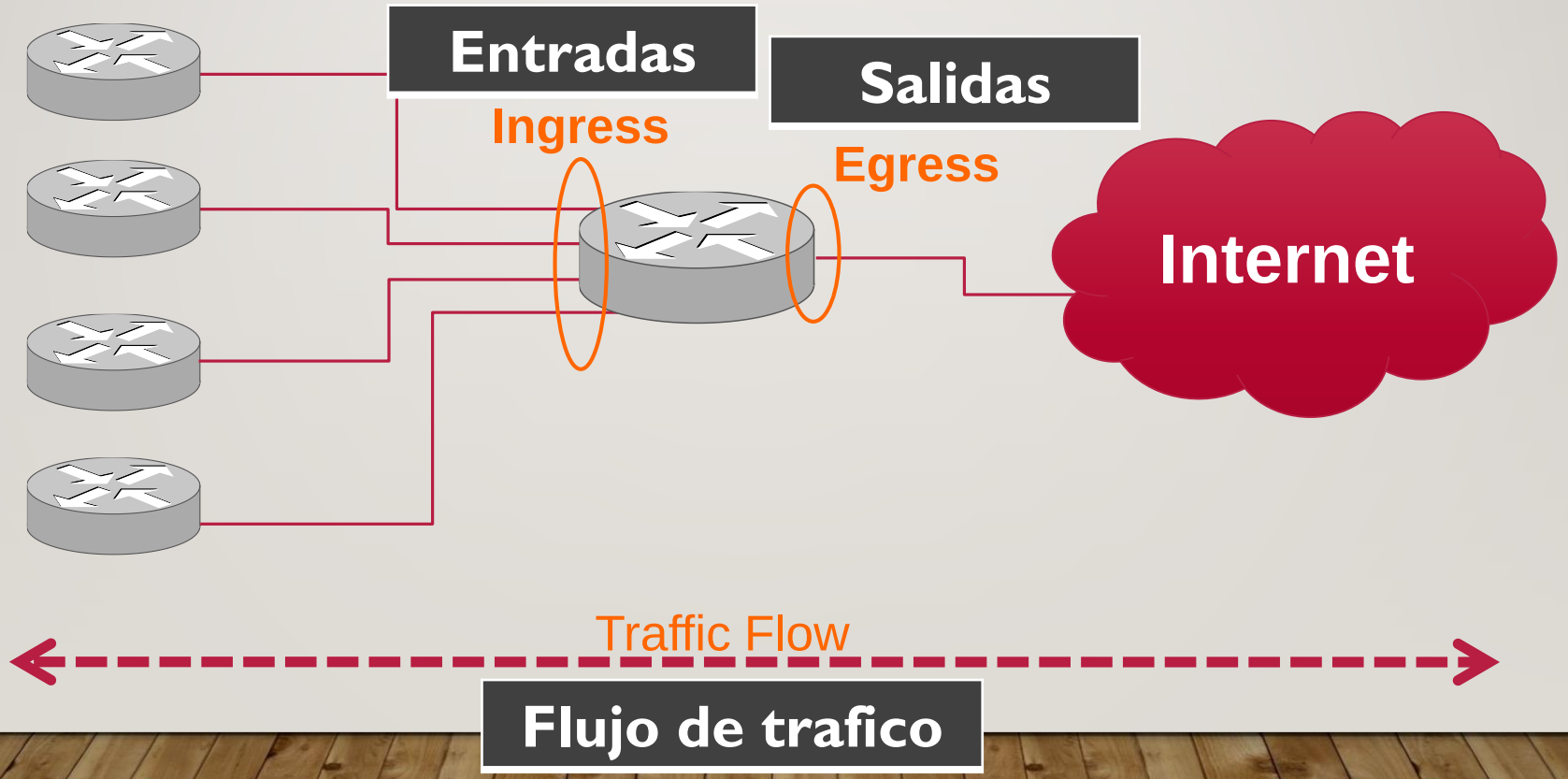
- El uso de una variedad de herramientas y plataformas de seguridad puede crear un gran volumen de datos entrantes relacionados con la seguridad, que deben analizarse e interpretarse para que sean útiles.
- Los sistemas de gestión de eventos de seguridad (security event management, SEM) (ayudan a reducir la sobrecarga resultante. El SEM agrega y correlaciona automáticamente los datos del registro de eventos de seguridad en varios dispositivos de seguridad.

SISTEMAS SIEM

Los sistemas de gestión de información y eventos de seguridad (*security information and event management*, SIEM) combinan las capacidades de SEM con el análisis histórico y las funciones de informes de los sistemas de gestión de información de seguridad (*security information management*, SIM).

INGRESOS Y EGRESOS

Hay dos tipos de vectores de ataque: entrada y salida.



IDS IPS

IDS (Sistema de Detección de Intrusiones) funciona junto con enrutadores y con cortafuegos monitorizando las anomalías en el uso de la red. Protege los recursos de los sistemas de información (SI) de una compañía tanto de abusos externos como internos.

Un IPS (Sistema de Prevención de Intrusiones) es un sistema diseñado no solo para detectar ataques, sino también para prevenir que los servidores víctimas se vean afectados por dichos ataques. Un IPS complementa las herramientas de firewall, antivirus y antispyware para proveer una protección más completa contra las amenazas emergentes.

IPS (VENTAJAS)

Un IPS bien gestionado ayuda a asegurar que las amenazas son rechazadas en el perímetro de la red; un IDS proporciona visibilidad y confirmación de la actividad interna en los nodos críticos de red.

La mayor ventaja de un **IPS** es que puede bloquear un ataque cuando ocurre; en lugar de simplemente mandar una alerta, ayuda activamente a bloquear tráfico malicioso y no deseado.

IPS (SOSPECHAS)

Un atacante inteligente podría enviar comandos a un gran número de hosts protegidos por un IPS con el fin de provocar su mal funcionamiento. Esa situación podría tener un resultado potencialmente catastrófico en el típico ambiente de computación corporativo de hoy en día, donde la continuidad del servicio es crítica.

Además, los IPS pueden generar falsos positivos que provoquen serios problemas si se emplean respuestas automáticas.

SOFTWARE DE PREVENCIÓN DE PÉRDIDA DE DATOS

DLP, cubren tres estados principales de información:

- **Los datos en reposo,** se refieren a datos almacenados.
- **Los datos en tránsito,** se refieren a los datos que viajan a través de la red. La inspección profunda de paquetes (DPI) se utiliza para analizar los datos en busca de contenido confidencial.
- **Los datos en uso,** se refieren al movimiento de datos a nivel de estación de trabajo del usuario, esto incluye información enviada a impresoras, unidades USB y el portapapeles copiar y pegar.

ANTIVIRUS Y ANTI-MALWARE

El software malicioso es uno de los vectores de ataque más comunes utilizados por los adversarios para comprometer los sistemas. Se requieren controles para su detección y prevención.

Los virus y malware se pueden controlar a través de:

- Restricción de tráfico saliente
- Políticas y capacitación de concientización
- Múltiples capas de software anti-malware

SISTEMA DE DETECCIÓN DE INTRUSOS

Un sistema de detección de intrusos (IDS) complementa la implementación de un firewall trabajando en conjunto con enrutadores y firewalls para monitorear anomalías en el uso de la red. Un IDS opera continuamente en el sistema.

Se ejecuta en segundo plano y notifica a los administradores cuando se detecta una amenaza percibida.

CATEGORÍAS IDS

IDS basados en red

- Identifica ataques dentro de la red monitoreada y emite una advertencia al operador
- Detecta intentos de ataque
- No es un sustituto de un firewall, sino un complemento

IDS basados en host

- Configurado para un entorno específico
- Supervisa los recursos del sistema operativo interno para advertir sobre ataques
- Puede detectar la modificación de programas ejecutables y la eliminación de archivos
- Emite una advertencia si se intenta un comando privilegiado

SISTEMAS DE PREVENCIÓN DE INTRUSIONES

Un sistema de prevención de intrusiones (IPS) es similar a IDS, pero detecta ataques y evita daños a la víctima / host previsto.

Un IPS está activo; en contraste, un IDS es pasivo.

La presencia de un IPS:

- Limita el daño o la interrupción de los sistemas que son atacados.
- Debe estar configurado correctamente para ser efectivo