



VÍDEO intypedia005es

LECCIÓN 5: SEGURIDAD PERIMETRAL

AUTOR: Alejandro Ramos Fraile

Tiger Team Manager (SIA Company), Security Consulting (CISSP, CISA)

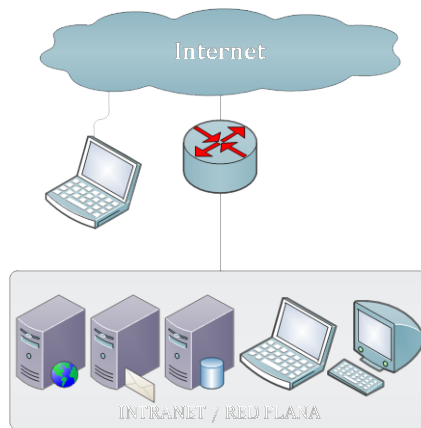
BERNARDO

Hola, bienvenidos a intypedia. Hoy vamos a explicar los fundamentos de la seguridad perimetral. Un concepto emergente que asume la integración de diversos elementos y sistemas para proteger los perímetros de una red informática, la detección de tentativas de intrusión e incluso la disuasión de los potenciales atacantes. Un tema muy interesante... ¡Acompáñanos!

ESCENA 1. FUNDAMENTOS DE LA SEGURIDAD PERIMETRAL. INTRODUCCIÓN A LOS CORTAFUEGOS

ALICIA

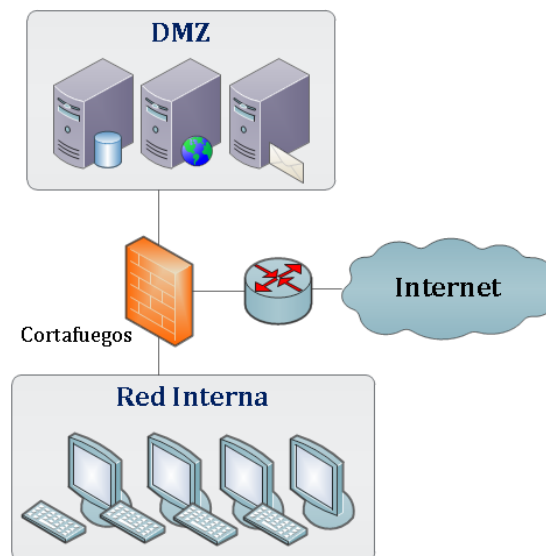
Hola Bernardo. La nueva empresa para la que trabajo me ha pedido que evalúe las medidas de seguridad perimetral de su arquitectura de red informática y les proponga mejoras. Mira, me han facilitado este diagrama en el cual todos los equipos se conectan directamente a Internet a través de un router y esto podría acarrear problemas. Quieren que les proponga alternativas para tener una red más segura.



Me han sugerido que debería comenzar por separar los servicios ofrecidos a través de Internet, que son los que más ataques reciben, del resto de la red y ubicarlos en un segmento especial llamado Zona Desmilitarizada DMZ (*Demilitarized Zone*). De esta forma, si consiguen acceder a alguno de ellos, no podrán acceder al resto de la red. ¿Cómo puedo hacerlo?

BERNARDO

Alicia, es típico separar servicios accesibles a través de Internet, como puede ser la página Web de una empresa o su correo electrónico, del funcionamiento de su red interna o intranet. En este sentido las DMZ son de gran utilidad. Las DMZ generalmente se crean con un dispositivo llamado cortafuegos o *firewall*. Esta tecnología está diseñada para filtrar tráfico tanto de entrada como de salida. Si implantas este elemento y separas los servicios públicos de la red interna, el mapa de una nueva arquitectura podría quedar así.



Si te fijas, el tráfico desde la red interna y la DMZ hacia Internet está permitido. En cambio el cortafuegos bloqueará todas las peticiones hacia la red interna, sea cual sea su origen, y sólo aceptará el tráfico hacia la DMZ de aquellos servicios para lo que esté configurado.

ALICIA

Claro, con ese método si hubiese un incidente en uno de los servidores de la DMZ, el intruso quedaría aislado. Pero... ¿realmente cómo funciona un cortafuegos?

BERNARDO

Un cortafuegos funciona en base a reglas. Existen dos grandes filosofías para definir las: por un lado está la política permisiva, que acepta todo el tráfico menos el que sea denegado expresamente y, por otro, la política restrictiva, que deniega todo el tráfico menos lo que se acepte expresamente. Esta última política es más difícil de mantener pero más segura y es la que se debería utilizar siempre.

En general se puede hablar de cuatro tipos de cortafuegos, según sus características y la capa OSI en la que funciona. En primer lugar tenemos los denominados cortafuegos de pasarela, que funcionan para aplicaciones específicas como telnet, ftp o Web; en segundo lugar los cortafuegos de capa de red que permiten una configuración en base a dirección IP y puerto de origen y destino. Luego están los cortafuegos de aplicación que entienden y analizan protocolos concretos como HTTP y filtran peticiones según patrones o comportamientos determinados y, por último, los cortafuegos personales que se usan en equipos de escritorio, como por ejemplo ZoneAlarm, Comodo Pro, etc.

Para que entiendas mejor cómo funcionan estos dispositivos basados en reglas vamos a ver un pequeño ejemplo con un cortafuegos de capa red que sería de utilidad en tu situación.

Regla	Acción	IP Origen	IP Destino	Proto	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

Por ejemplo, podríamos tener un cortafuegos con una regla que indicase que el rango de red 172.16.0.0/16 puede acceder al servidor SMTP (puerto 25) con dirección IP 192.168.0.4 y al servicio Web (puerto 80) con dirección 192.168.0.2. Otra regla podría establecer que cualquier dirección podría tener acceso a otro servicio Web en la dirección 192.168.10.8. Lógicamente el resto de conexiones serían denegadas.

ALICIA

Gracias Bernardo, empiezo a darme cuenta del potencial de estos dispositivos. Los tendré en cuenta...

ESCENA 2. SISTEMAS DE DETECCIÓN DE INTRUSOS. IDS y HONEYPOTS

ALICIA

Bernardo, una vez que he considerado los cortafuegos, ¿por dónde debería continuar?

BERNARDO

La verdad es que te quedan aún bastantes medidas de seguridad que puedes aplicar, como por ejemplo instalar un sistema de detección de intrusos IDS (*Intrusion Detection Systems*) que se utilizan para identificar ataques en tiempo real, almacenar los registros y reportar al personal de administración y seguridad para que puedan tomar medidas adicionales.



ALICIA

Vaya, otro aparato. Tiene apariencia de ser un sistema complejo y poco productivo si sólo sirve para que reporte ataques.

BERNARDO

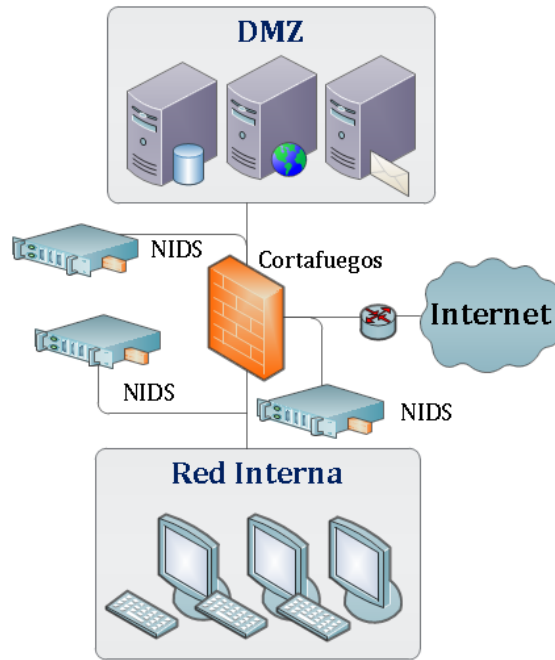
No te apures en los juicios Alicia, los IDS tienen mucho valor como cuaderno de bitácora y pueden ser el punto de partida para identificar el origen de un ataque. Además, los IDS han evolucionado a los Sistemas de Detección y Prevención de Intrusos IDPS (*Intrusion Detection and Prevention Systems*), unos elementos más complejos que también son capaces de bloquear la conexión si detectan que el evento es peligroso, al igual que hacen los cortafuegos de aplicación.

ALICIA

¡Qué interesante!... Me surgen ahora dos dudas, ¿dónde debería conectarlo y cómo es capaz de identificar lo que es un ataque de lo que no lo es?

BERNARDO

La arquitectura típica de un sistema de detección y prevención de intrusos IDPS consiste en la instalación de sondas (sensores) que informarán sobre anomalías en los elementos bajo estudio. Un ejemplo de estas sondas son las sondas de sistema HIDS (*Host-based Intrusion Detection Systems*), que monitorizan los cambios en un ordenador, por ejemplo, en el sistema operativo, en su configuración, el registro del equipo y sus aplicaciones, etc. Otro tipo de IDS son los basados en sondas de red NIDS (*Network Intrusion Detection Systems*), que se basan en instalar una sonda en cada segmento de la red que se quiera monitorizar.



Los NIDS pueden funcionar de dos formas distintas. El método más común es comprobar el tráfico contra una base de datos de firmas y si hay coincidencias, generar la alarma. La otra opción consiste en registrar tráfico durante un tiempo y crear un patrón de comportamiento; posteriormente todos los paquetes recibidos son comprobados contra el patrón inicial causando una alerta si no hubiese coincidencias.

Por aquí tengo una firma sencilla para que veamos cómo funciona.

```

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;)

```

En este ejemplo puedes ver en la primera línea cómo se identifica en qué interfaz, protocolo y servicio sería comprobada la firma. La segunda línea identifica el mensaje que sería enviado como alerta si, tal y como dice la tercera y cuarta línea, en una conexión establecida se encuentra la cadena “.printer” dentro de una petición Web URI (*Uniform Resource Identifier*). Las últimas líneas reflejan las referencias a esta vulnerabilidad y otros datos de identificación y clasificación.

ALICIA

Pero... ¿esta base de datos con firmas se actualizará periódicamente para que los nuevos ataques sean detectados rápidamente, no?

BERNARDO

Efectivamente, estos sistemas y la configuración general de seguridad han de mantenerse siempre actualizados. Las firmas son muy efectivas para detectar ataques rápidamente, pero además existen otras tecnologías para conocer nuevas tendencias y técnicas utilizadas por los intrusos; en este sentido son muy útiles las *honeypots*. Se denomina *honeypot* al software o conjunto de ordenadores cuya intención es atraer a atacantes; para ello se instalan y configuran con fallos graves precisamente para que sean vulnerados. Cuando los intrusos entren, todas sus acciones serán controladas y monitorizadas para mejorar la arquitectura de seguridad.

ALICIA

Esto me parece algo peligroso. ¿Dónde se definen las vulnerabilidades, en el sistema operativo o en aplicaciones? Es más, ¿qué vulnerabilidades se utilizan?

BERNARDO

Es verdad, estas trampas tienen riesgos y por eso requieren mucho trabajo para asegurar que su aislamiento, su desconexión de las redes principales, es completo. Este es uno de los principales motivos por los que su uso no es habitual. En cuanto a las vulnerabilidades, depende del tipo de *honeypot*. Hay dos clases: de baja interacción, en las que se simula el sistema operativo y las aplicaciones, o bien las de alta interacción en las que los fallos se encuentran en los servicios. Un ejemplo puede ser algo tan sencillo como establecer una contraseña fácilmente adivinable como 1234 para el usuario root de un ftp o ssh.

ALICIA

Y cuando intenten entrar... ¡el cazador es cazado!

BERNARDO

¡Exacto! Y junto a él, obtendremos muestras de nuevas vulnerabilidades, gusanos, correos con spam y todo lo que no desearíamos en nuestra red.

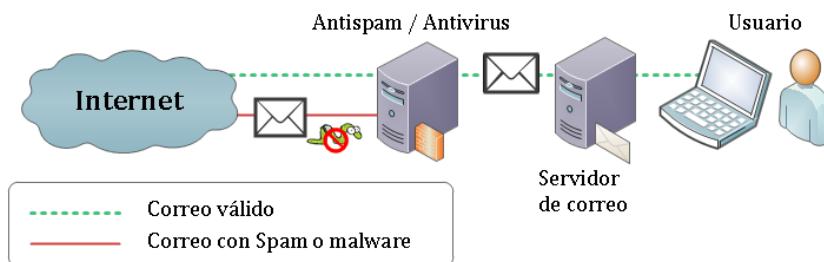
ESCENA 3. TRÁFICO EN LA RED. ANTIVIRUS, ANTISPAM y VPN

ALICIA

Bernardo, tengo una duda. Dentro de la seguridad perimetral, ¿se podría establecer algún tipo de solución a nivel de arquitectura de red para evitar que contenido dañino, como malware o spam, llegue a los equipos de mi empresa?

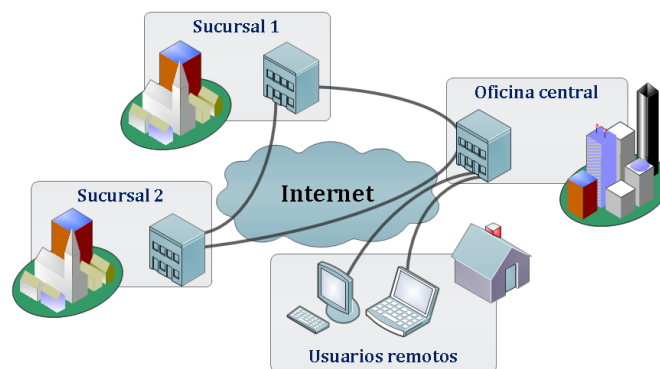
BERNARDO

Además del correspondiente antivirus en cada uno de las estaciones de trabajo, la organización debería disponer de una pasarela Antivirus y AntiSpam que sea la que reciba todo el correo electrónico, lo procese y posteriormente lo entregue al servidor de correo tradicional si considera que está limpio; de ahí los usuarios lo descargarán con normalidad.



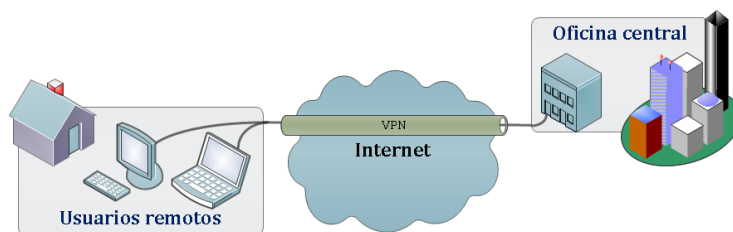
ALICIA

Esto será muy útil, pues recibimos muchos correos basura que pueden incluir malware. En ocasiones éstos vienen de empleados que desde su casa sin saberlo lo envían. Tenemos muchos trabajadores que comprueban su correo desde Internet o acceden a aplicaciones internas cuando teletrabajan, y no sólo eso sino que también hay algunas sucursales en otras poblaciones que se conectan a nuestra red.



BERNARDO

Ya veo. Alicia, además de analizar la información intercambiada en tu empresa, es aconsejable que para asegurar las comunicaciones y proteger la información cuando se utiliza una infraestructura pública como Internet, se utilice una red privada virtual VPN (*Virtual Private Network*) con la que se encapsule y cifre todo el tráfico en una nueva red "virtual". Las redes privadas virtuales garantizan la autenticación e integridad de los datos y la autorización de cada uno de los usuarios. Además estas redes minimizan que se expongan servicios internos al exterior y que éstos puedan ser vulnerados.



ALICIA

Gracias Bernardo, vuelvo al trabajo con todas estas observaciones. Ya te contaré qué tal me ha ido.

[Animación: Unas semanas más tarde]

ESCENA 4. GESTIÓN UNIFICADA DE AMENAZAS. CONCLUSIONES

ALICIA

Buenos días Bernardo, ya hemos rediseñado la arquitectura de red y hemos hecho muchos cambios teniendo en cuenta los aspectos de seguridad que comentamos.

BERNARDO

Buenos días Alicia, me alegro. Dime qué habéis hecho exactamente.

ALICIA

La compañía después de estudiar costes, adquirió un sistema de Gestión Unificada de Amenazas UTM (*Unified Threat Management*), un único equipo que incluye múltiples características de seguridad: cortafuegos, sistemas de detección y prevención de intrusos, pasarelas antivirus y antispam y redes privadas virtuales.

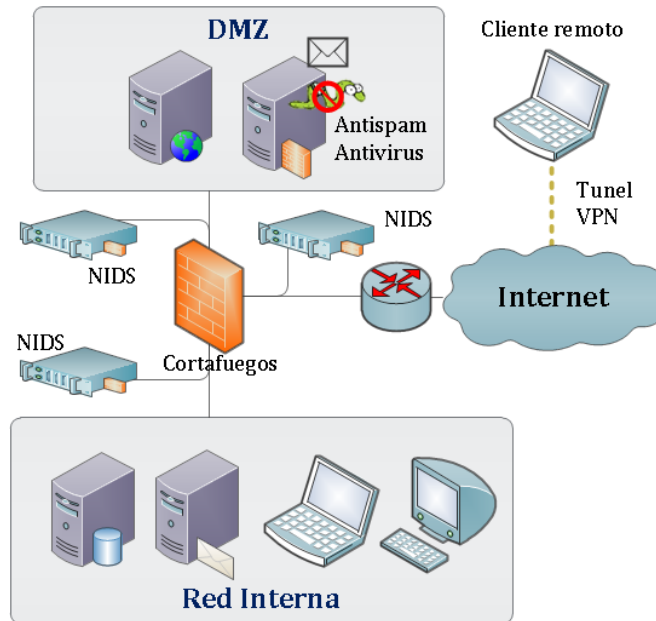


BERNARDO

Bien pensado, estos elementos son muy cómodos para centralizar soluciones. ¿Cómo ha quedado configurada la arquitectura? Supongo tendrás un mapa actualizado.

ALICIA

Así es, lo tengo aquí mismo, te lo enseño y te cuento todos los cambios.



Lo primero que hemos hecho ha sido configurar el cortafuegos, segmentando los servicios de Web y la pasarela de correo en la DMZ con una política restrictiva. Luego hemos configurado el sistema de detección y prevención de intrusos, escuchando en las tres interfaces para conocer todos los ataques posibles. Con los cambios, hemos movido el servidor de base de datos que se ha quedado junto al servidor de correo en la red interna inaccesible desde Internet. Y ahora todos los trabajadores y sucursales se conectan usando una VPN.

BERNARDO

¡Vaya cambio! Se nota que has estudiado muy bien el nuevo diseño. Ahora la arquitectura es mucho más segura.

ALICIA

Gracias a tus consejos.

BERNARDO

No hay de qué. En la página web de intylopedia encontrarás información complementaria sobre este interesante tema... yo me quedo revisando mientras tanto los registros de mis IDS... hasta la próxima lección. ¡Adiós!

ALICIA

¡Adiós!

Guión adaptado al formato intypedia a partir del documento entregado por D. Alejandro Ramos Fraile.

Madrid, España, febrero de 2011

<http://www.intypedia.com>

<http://twitter.com/intypedia>

