Práctica 3.

El enunciado de la presente práctica consta de dos documentos:

1. Descripción del ejercicio a realizar
2. Anexo I. Escenario inicial

Objetivo de la práctica

El objetivo de la práctica es proteger la estructura interna de la red corporativa configurada en las prácticas anteriores para lo que deberéis aplicar las medidas oportunas para restringir el tráfico no autorizado, que se define en la política de seguridad especificada en la matriz de envío que se puede ver a continuación.

Al mismo tiempo que se permite que los equipos que se indican a continuación, con direcciones IP privadas, puedan conectarse a Internet.

Tecnologías a utilizar

Para resolver de forma adecuada los desafíos que se plantean en esta práctica es necesario que utilicéis en el escenario las tres tecnologías vistas durante la explicación de esta práctica:

- ACLs estándar: configurada/s en el router frontera para evitar que llegue a Firewall todo el tráfico procedente de Internet cuyas direcciones IP de origen sean sospechosas de estar relacionadas con un ataque (IPs marcianas).
- ACLs extendidas: switches de capa de distribución y/o Firewall
- CBAC: switches de capa de distribución y/o Firewall

Para resolver de forma adecuada los desafíos que se plantean en esta práctica es necesario que utilicéis en el escenario dos de las tecnologías de traducción de direcciones vistas durante la explicación de esta práctica:

- Port Forwarding / Mapeo de puertos
- NAT Dinámico con sobrecarga

La especificación de cómo debe llevarse a cabo la traducción de direcciones IP, es la siguiente:

a) Las direcciones privadas 10.1.0.0/16 se deben traducir a 192.0.0.10
b) Las direcciones privadas 10.2.0.0/16 se deben traducir a 192.0.0.11
c) Las direcciones privadas 10.3.0.0/16 se deben traducir a 192.0.0.12
d) La IP y Puerto 10.255.1.10:443 se debe publicar como 192.0.0.13:443
e) Las IP y Puerto 10.255.2.10:443 se debe publicar como 192.0.0.14:443

Interacción con las ACLs

Debéis tener en cuenta que el proceso de traducción de direcciones puede afectar a las ACLs. Por favor, tenedlo en cuenta.

Tráfico del plano de control

La política de seguridad de la organización define qué tráfico del plano de datos (es decir, tráfico de usuarios, servidores, etc.) se va a permitir, pero no hace referencia al tráfico del plano de control. ¿Cuál es el tráfico del plano de control? Todo aquel que permite que la red funcione adecuadamente, como por ejemplo: RIP, OSPF, HSRP, STP, etc. En esta práctica es clave que entendáis que los mensajes OSPF y HSRP se encapsulan en paquetes IP y, por lo tanto, son susceptibles de ser bloqueados por las ACLs.

Otra cuestión importante que debéis tener en cuenta es que las ACLs salientes NO afectan al tráfico generado desde el propio router, pero las ACLs entrantes SÍ afectan al tráfico que va dirigido al router.

Consideraciones especiales

Esta práctica entraña una especial dificultad y está diseñada para que integréis en un solo escenario todo lo visto en la materia hasta ahora. Hago especial énfasis en que utilicéis las tutorías y preguntéis vuestras dudas a través del foro de Moodle puesto que así lo que vayamos comentando a través de ese canal será de utilidad para todos.

Defensa de la práctica

La defensa de esta práctica se llevará a cabo la semana del 26 de abril en las sesiones de prácticas. El sistema de defensa será similar al utilizado en las defensas de las prácticas anteriores.

Política de Seguridad

Tráfico Permitido	10.1.1.0 /24	10.1.2.0/ 24	10.1.3.0 /24	10.1.4.0 /24	10.2.1.0 /24	10.2.2.0 /24	10.2.3.0/ 24	10.2.4.0 /24	10.0.0.0/ 8	10.255.1.0/24	10.255.2.024	Internet
10.1.1.0/24	NA	-	-	-	-	-	-	-	-	HTTP, HTTPS a todos los servidores de la Subred 10.255.1.0/24 DNS-UDP a 10.255.1.10	-	HTTPS, ICMP
10.1.2.0/24	-	NA	-		-	-	-	-	-	-	HTTP, HTTPS a todos los servidores de la Subred 10.255.2.0/24 SMTP, POP3 Y DNS (UDP) A 10.255.2.10	HTTPS, ICMP
10.1.3.0/24	-	-	NA	-	-	-	-	-	-	HTTP, HTTPS a todos los servidores de la Subred 10.255.1.0/24 DNS-UDP a 10.255.1.10	-	HTTPS, ICMP
10.1.4.0/24	-	-	-	NA	-	-	-	-	-	-	HTTP, HTTPS a todos los servidores de la Subred 10.255.2.0/24 SMTP, POP3 Y DNS (UDP) A 10.255.2.10	HTTPS, ICMP
10.2.1.0/24	-	-	-	-	NA	-	-	-	-	HTTP, HTTPS a todos los servidores de la Subred 10.255.1.0/24 DNS-UDP a 10.255.1.10	-	HTTPS, ICMP
10.2.2.0/24	-	-	-	-	-	NA	-	-	-	-	HTTP, HTTPS a todos los servidores de la Subred 10.255.2.0/24 SMTP, POP3 Y DNS (UDP) A 10.255.2.10	HTTPS, ICMP
10.2.3.0/24	-	-	-	-	-	-	NA	-	-	HTTP, HTTPS a todos los servidores de la Subred 10.255.1.0/24 DNS-UDP a 10.255.1.10	-	HTTPS, ICMP
10.2.4.0/24	-	-	-	-	-	-	-	NA	-	-	HTTP, HTTPS a todos los servidores de la Subred 10.255.2.0/24 SMTP, POP3 Y DNS (UDP) A 10.255.2.10	HTTPS, ICMP

NA: No aplica. Las ACLs no pueden controlar el tráfico dentro de una LAN, puesto que la comunicación entre dispositivos no se hace a través del firewall

- : No se permite ningún tipo de tráfico

La primera columna representa el origen del tráfico y los encabezamientos del resto de columnas el destino.

Tráfico Permitido	10.0.0.0/8	10.1.1.0 /24	10.1.2.0/24	10.1.3.0 /24	10.1.4.0 /24	10.2.1.0 /24	10.2.2.0 /24	10.2.3.0/24	10.2.4.0 /24	10.255.1.0/24	10.255.2.024	Internet
10.255.1.0/24	-	Tráfico de respuesta a peticiones procedentes de la subred	Tráfico de respuesta a peticiones procedentes de la subred	Tráfico de respuesta a peticiones procedentes de la subred	Tráfico de respuesta a peticiones procedentes de la subred	Tráfico de respuesta a peticiones procedentes de la subred	Tráfico de respuesta a peticiones procedentes de la subred	Tráfico de respuesta a peticiones procedentes de la subred	Tráfico de respuesta a peticiones procedentes de la subred	NA	-	HTTPS, ICMP
10.255.2.0/24	-	Tráfico de respuesta a peticiones procedentes de la subred	Tráfico de respuesta a peticiones procedentes de la subred	Tráfico de respuesta a peticiones procedentes de la subred	Tráfico de respuesta a peticiones procedentes de la subred	Tráfico de respuesta a peticiones procedentes de la subred	Tráfico de respuesta a peticiones procedentes de la subred	Tráfico de respuesta a peticiones procedentes de la subred	Tráfico de respuesta a peticiones procedentes de la subred	-	NA	HTTPS, ICMP
Internet	-	Tráfico de respuesta a peticiones procedentes de la subred	Tráfico de respuesta a peticiones procedentes de la subred	Tráfico de respuesta a peticiones procedentes de la subred	Tráfico de respuesta a peticiones procedentes de la subred	Tráfico de respuesta a peticiones procedentes de la subred	Tráfico de respuesta a peticiones procedentes de la subred	Tráfico de respuesta a peticiones procedentes de la subred	Tráfico de respuesta a peticiones procedentes de la subred	HTTPS a 10.255.1.10 y tráfico de retorno	HTTPS a 10.255.2.10 y tráfico de retorno	NA