Desafío - Soluciones de Firewalls

En este desafío validaremos nuestros conocimientos de configuración de un firewall ASA para controlar el tráfico LAN y WAN respectivo. Para lograrlo, necesitarás aplicar el archivo **M6_U1_Desafio.pkt**

Lee todo el documento antes de comenzar el desarrollo **individual** para asegurarte de tener el máximo de puntaje y enfocar bien los esfuerzos.

// Tiempo asociado: 1 hora cronológica (Si el desafío se desarrolla por los estudiantes en menos tiempo del indicado, se debe realizar la creación de uno adicional para completar el tiempo indicado de la sesión).

Descripción

Una empresa requiera implementar una pequeña red corporativa con un firewall ASA para proteger la conexión de su red LAN hacia la WAN, así como bloquear toda conexión que no se encuentra autorizada desde afuera hacia la red LAN. En este caso realizará las implementaciones necesarias para cumplir el objetivo requerido.

DHCP Snooping

Función de seguridad en capa 2 para proteger ataque de **spoofing**, permite al switch filtrar mensajes DHCP no autorizados usando una tabla de enlace para almacenar hosts legítimos y sus configuraciones de red.

- Si una IP no autorizada solicita DCHP es bloqueada impidiendo asignación.

Configuración

- **Habilitar DHCP snooping globalmente**.

```
Switch1(config)# ip dhcp snooping
```

- **Habilitar DHCP en una VLAN deseada globalmente**.

```
Switch1(config)# ip dhcp snooping vlan 10
```

a. Marcar puerto que conecta al servidor DHCP como confiable.

```
Switch1(config)# interface fastEthernet 0/1
Switch1(config-if)# ip dhcp snooping trust
```

b. Limitar número de solicitudes DHCP por segundo, en este caso mostramos como seria con 15 segundos.

```
Switch1(config)# interface fastEthernet 0/2
Switch1(config-if)# ip dhcp snooping limit rate 15
```

MPF Modular Policy Framework

Permite definir políticas avanzadas en Firewalls ASA usando 3 componentes:

1. **Class Map** – Define el tipo de tráfico (por ejemplo, todo el tráfico HTTP).
2. **Policy Map** – Aplica acciones al tráfico (como inspección o limitar ancho de banda).
3. **Service Policy** – Aplica la política al tráfico que entra o sale de una interfaz o globalmente.

Configuración

En el Firewall ASA

a. **Crear Class map**.

```
fwasa(config)# class-map HTTP_TRAFFIC
fwasa (config-cmap)# match protocol http
```

b. **Crear Policy Map**

Inspecciona el tráfico HTTP

```
fwasa(config)# policy-map INSPECT_HTTP
fwasa(config-pmap)# class HTTP_TRAFFIC
fwasa(config-pmap-c)# inspect http
```

c. **Aplicar Policy map a una interfaz o globalmente**.

```
fwasa (config)# service-policy INSPECT_HTTP global
```

Nota: Verificar los paquetes que coinciden con la política.

- `fwasa# show service-policy`

Requerimientos

1. Asignar direccionamiento IP, seguridad de puerto según es requerido y los mecanismos de estabilización de STP según es necesario.
   (**2 Puntos**)

2. Implementa solución de DHCP Snooping según es requerido. (**2 Puntos**)

3. Realiza configuración básica en firewall ASA, tales como crear y definir zona y modificar MPF para la conectividad. (**2 Puntos**)

4. Implementa NAT y PAT en firewall ASA para lograr la conectividad hacia redes externas. (**2 Puntos**)

5. Implementa protocolo de enrutamiento dinámico y estático para lograr la conectividad en la topología. (**2 Puntos**)

 ¡Mucho éxito!

Consideraciones y recomendaciones