Guía Seguridad de Puertos (Port Security) en Switches Cisco

1. Introducción a la Seguridad de Puertos (Port Security)

La seguridad de puertos, o *Port Security*, es una función de los switches Cisco que permite controlar qué dispositivos tienen acceso a una red restringiendo las direcciones MAC en los puertos. Esto es fundamental para proteger la red de accesos no autorizados y para mitigar posibles ataques, como el *MAC flooding*.

Objetivos de la Guía

- Configurar la seguridad de puertos en un switch Cisco.
- Establecer un límite en la cantidad de dispositivos permitidos en un puerto.
- Aprender las acciones de seguridad ante violaciones en el puerto.

2. Beneficios de Implementar Port Security

Configurar Port Security ofrece múltiples beneficios, tales como:

- Control de acceso: Permite restringir la cantidad y tipo de dispositivos conectados a la red.
- Mitigación de ataques: Protege contra ataques de inundación de direcciones MAC (MAC flooding).
- Notificación y respuesta rápida: Puede enviar alertas y bloquear dispositivos sospechosos.

3. Preparativos Previos

Antes de configurar Port Security, asegúrate de que:

- Tienes acceso administrativo al switch.
- Conoces las interfaces en las que se aplicará Port Security.
- Decides la acción de seguridad a aplicar en caso de violación.

4. Comandos de Configuración de Port Security

A continuación, presentamos los comandos de configuración en una lista completa, seguidos de una explicación de cada uno para comprender su función en el switch.

- Switch> enable
- Switch# configure terminal
- Switch(config)# interface FastEthernet0/1
- Switch(config-if)# switchport mode access
- Switch(config-if)# switchport port-security
- Switch(config-if)# switchport port-security maximum 2
- Switch(config-if)# switchport port-security mac-address sticky
- Switch(config-if)# switchport port-security mac-address 0011.2233.4455
- Switch(config-if)# switchport port-security violation restrict
- Switch(config-if)# switchport port-security violation shutdown
- Switch(config-if)# end
- Switch# copy running-config startup-config

Explicación Detallada de Cada Comando

1. **`Switch> enable`**
   Activa el modo privilegiado en el switch, que es necesario para realizar configuraciones.
2. **`Switch# configure terminal`**
   Ingresa al modo de configuración global. Este modo permite aplicar cambios a nivel del sistema o de las interfaces individuales.
3. **`Switch(config)# interface FastEthernet0/1`**
   Selecciona la interfaz `FastEthernet0/1` en la que se configurará Port Security. Puedes reemplazar `FastEthernet0/1` con cualquier otra interfaz específica según tus necesidades.
4. **`Switch(config-if)# switchport mode access`**
   Cambia el modo de la interfaz a modo acceso, que es un requisito para habilitar Port Security. Este modo se usa cuando el puerto se conecta a un solo dispositivo, como una computadora o una impresora.
5. **`Switch(config-if)# switchport port-security`**
   Activa Port Security en la interfaz. Al activarlo, el switch aplicará las restricciones de acceso configuradas en la interfaz.
6. **`Switch(config-if)# switchport port-security maximum 2`**
   Establece el número máximo de direcciones MAC permitidas en la interfaz. En este ejemplo, el valor es 2, lo cual limita la conexión a solo dos dispositivos a la vez.
7. **`Switch(config-if)# switchport port-security mac-address sticky`**
   Configura el switch para que aprenda automáticamente las direcciones MAC de los dispositivos conectados y las guarde de forma persistente en la configuración. Esto facilita la administración y asegura que las direcciones aprendidas permanezcan autorizadas después de reiniciar el switch.

8. **`Switch(config-if)# switchport port-security mac-address 0011.2233.4455:`** Permite solo al dispositivo con la dirección MAC `0011.2233.4455` acceder a la red a través de este puerto. Si otro dispositivo intenta conectarse, se activará la acción de seguridad configurada.
9. **`Switch(config-if)# switchport port-security violation restrict`**
   Define la acción de seguridad que tomará el switch si se detecta una violación de Port Security. En este caso, se ha configurado `restrict`, lo que significa que:
   - El switch bloqueará el tráfico de dispositivos no autorizados.
   - Generará una alerta en el registro de sistema (Syslog).
   - No deshabilitará el puerto, solo bloqueará las direcciones no autorizadas.
10. **`Switch(config-if)# switchport port-security violation shutdown:`** Cuando se detecta una violación, el puerto se desactiva (entra en estado "error-disabled"), apaga el LED del puerto, y se envía un mensaje de registro al sistema. Este modo es el más restrictivo, y el puerto debe reactivarse manualmente con los comandos `shutdown` y `no shutdown`.
11. **`Switch(config-if)# end`**
    Sale del modo de configuración de interfaz y vuelve al modo privilegiado.
12. **`Switch# copy running-config startup-config`**
    Guarda la configuración actual en la configuración de inicio (startup-config) del switch, asegurando que los cambios persistan después de reiniciar el dispositivo.