Packet Tracer - Cambiar configuración de seguridad

Tabla de VLAN

Switch	Número de VLAN	Nombre de la VLAN	Asociación de puertos	Red
SW-1	10	Administrador	F0/1, F0/2	192.168.10.0/24
	20	Ventas	F0/10	192.168.20.0/24
	99	Administración	F0/24	192.168.99.0/24
	100	Nativo	G0/1, G0/2	No
	999	BlackHole	Todos sin usar	Ninguna
SW-2	10	Administrador	F0/1, F0/22	192.168.10.0/24
	20	Ventas	F0/10	192.168.20.0/24
	99	Administración	F0/24	192.168.99.0/24
	100	Nativo	Ninguna	Ninguna
	999	BlackHole	Todos sin usar	Ninguna

Objetivos

Parte 1: Crear un troncal (trunk) seguro

Parte 2: Asegurar los puertos del switch no utilizados

Parte 3: Implementar seguridad en los puertos (Port Security)

Parte 4: Habilitar la inspección DHCP

Parte 5: Configurar Rapid PVST PortFast y BPDU Guard

Aspectos básicos

Está mejorando la seguridad en dos switches de acceso en una red configurada parcialmente. Implementará el rango de medidas de seguridad cubiertas en este módulo de acuerdo con los requisitos a continuación. Tenga en cuenta que el router se ha configurado en esta red, por lo que la conectividad entre hosts en diferentes VLAN debería funcionar cuando se complete.

Instrucciones

Paso 1: Crear un troncal seguro (Secure Trunk).

a. Conecte los puertos G0/2 de los dos switches de capa de acceso.

b. Configure los puertos G0/1 y G0/2 como troncales estáticos en ambos switches.

c. Deshabilite la negociación DTP en ambos lados del enlace.

d. Cree VLAN 100 y asígnele el nombre Nativo en ambos switches.

e. Configure todos los puertos troncales en ambos switches para usar la VLAN 100 como la VLAN nativa.

Paso 2: Asegure los puertos del switch no utilizados.

a. Apague todos los puertos del switch no utilizados en SW-1.

b. En SW-1, cree una VLAN 999 y asígnele el nombre Agujero Negro. El nombre configurado debe coincidir exactamente con el requisito.

c. Mueva todos los puertos de switch no utilizados a la VLAN Agujero Negro.

Paso 3: Implemente seguridad en los puertos.

a. Active la seguridad del puerto en todos los puertos de acceso activos en el switch SW-1.

b. Configure los puertos activos para permitir que se aprenda un máximo de 4 direcciones MAC en los puertos.

c. Para los puertos F0 / 1 en SW-1, configure estáticamente la dirección MAC de la PC utilizando la seguridad del puerto.

d. Configure cada puerto de acceso activo para que agregue automáticamente las direcciones MAC aprendidas en el puerto a la configuración en ejecución.

e. Configure el modo de violación de seguridad del puerto para descartar paquetes de direcciones MAC que excedan el máximo, generar una entrada de Syslog, pero no deshabilitar los puertos.

Paso 4: Configure la detección DHCP.

a. Configure los puertos troncales en SW-1 como puertos confiables.

b. Limite los puertos no confiables en SW-1 a cinco paquetes DHCP por segundo.

c. En SW-2, habilite la inspección DHCP globalmente y para las VLAN 10, 20 y 99.

Nota: La configuración de indagación DHCP puede no puntuar correctamente en Packet Tracer.

Paso 5: Configure PortFast y BPDU Guard.

a. Habilite Puerto rápido (PortFast) en todos los puertos de acceso que están en uso en SW-1.

b. Habilite BPDU Guard en todos los puertos de acceso que están en uso en SW-1.

c. Configure SW-2 para que todos los puertos de acceso usen PortFast de manera predeterminada.