Packet Tracer - Konfiguracja zabezpieczeń przełącznika

Tabela VLAN

Przełącznik	Numer sieci VLAN	Nazwa sieci VLAN	Przypisanie portu	Sieć
SW-1	10	Admin	F0/1, F0/2	192.168.10.0/24
	20	Sales	F0/10	192.168.20.0/24
	99	Management	F0/24	192.168.99.0/24
	100	Native	G0/1, G0/2	Brak
	999	BlackHole	Wszystkie niewykorzystane	Brak
SW-2	10	Admin	F0/1, F0/22	192.168.10.0/24
	20	Sales	F0/10	192.168.20.0/24
	99	Management	F0/24	192.168.99.0/24
	100	Native	Brak	Brak
	999	BlackHole	Wszystkie niewykorzystane	Brak

Cele

Część 1: Tworzenie bezpiecznego łącza trunk

Część 2: Zabezpieczanie nieużywanych portów przełączników

Część 3: Wdrożenie bezpieczeństwa portu

Część 4: Włączenie DHCP Snooping

Część 5: Konfiguracja Rapid PVST PortFast i BPDU Guard

Wprowadzenie

Zwiększasz bezpieczeństwo na dwóch przełącznikach dostępu w częściowo skonfigurowanej sieci. Zaimplementujesz szereg środków bezpieczeństwa, które zostały omówione w tym module, zgodnie z poniższymi wymaganiami. Zwróć uwagę, że routing został skonfigurowany w tej sieci, więc łączność między hostami w różnych sieciach VLAN powinna działać po zakończeniu.

Instrukcje

Krok 1: Tworzenie bezpiecznego łącza trunk

a. Podłącz porty G0/2 dwóch przełączników warstwy dostępu.

b. Skonfiguruj porty G0/1 i G0/2 jako statyczne trunki na obu przełącznikach.

c. Wyłącz negocjacje DTP po obu stronach łącza.

d. Utwórz VLAN 100 i nadaj mu nazwę Native na obu przełącznikach.

e. Skonfiguruj wszystkie porty trunk na obu przełącznikach, aby używały VLAN 100 jako natywnej sieci VLAN.

Krok 2: Zabezpieczanie nieużywanych portów przełączników

a. Wyłącz wszystkie nieużywane porty przełącznika na SW-1.

b. Na SW-1 utwórz sieć VLAN 999 i nazwij ją BlackHole. Skonfigurowana nazwa musi dokładnie odpowiadać wymaganiu.

c. Przenieś wszystkie nieużywane porty przełączników do sieci VLAN BlackHole.

Krok 3: Wdrożenie bezpieczeństwa portu.

a. Aktywuj zabezpieczenia portów na wszystkich aktywnych portach dostępu na przełączniku SW-1.

b. Skonfiguruj aktywne porty, aby umożliwić nauczenie maksymalnie 4 adresów MAC na portach.

c. W przypadku portów F0/1 na SW-1 statycznie skonfiguruj adres MAC komputera za pomocą zabezpieczeń portu.

d. Skonfiguruj każdy aktywny port dostępu tak, aby automatycznie dodał adresy MAC poznane na porcie do bieżącej konfiguracji.

e. Skonfiguruj tryb naruszenia bezpieczeństwa portu, aby odrzucać pakiety z adresów MAC, które przekraczają maksymalne wartości, generować wpis Syslog, ale nie wyłączać portów.

Krok 4: Skonfiguruj DHCP Snooping.

a. Skonfiguruj porty trunk na SW-1 jako porty zaufane.

b. Ogranicz niezaufane porty na SW-1 do pięciu pakietów DHCP na sekundę.

c. Na SW-2 włącz globalne DHCP snooping oraz dla sieci VLAN 10, 20 i 99.

Uwaga: Konfiguracja DHCP snooping może nie być prawidłowo punktowana w Packet Tracer.

Krok 5: Skonfiguruj PortFast i BPDU Guard.

a. Włącz PortFast na wszystkich portach dostępu, które są używane w SW-1.

b. Włącz BPDU Guard na wszystkich portach dostępu, które są używane w SW-1.

c. Skonfiguruj SW-2 tak, aby wszystkie porty dostępu były domyślnie używane PortFast.