Switch Security Configuration

**1. Care este cea mai bună practică recomandată atunci când aveți de-a face cu VLAN-ul nativ?**

a.Utilizați securitatea porturilor.

b.Dezactivați DTP.

**c.Atribuiți-l unui VLAN neutilizat.**

d.Atribuiți același număr de VLAN ca și VLAN-ul de gestionare.

**Explicație:** Securitatea porturilor nu poate fi activată pe un trunchi, iar trunchiurile sunt singurele tipuri de porturi care au un VLAN nativ. Chiar dacă dezactivarea DTP pe un trunk este cea mai bună practică, nu are nimic de-a face cu riscurile VLAN native. Pentru a preveni încălcările de securitate care profită de VLAN-ul nativ, plasați VLAN-ul nativ într-un VLAN neutilizat, altul decât VLAN-ul 1. VLAN-ul de gestionare ar trebui, de asemenea, să fie un VLAN neutilizat, diferit de VLAN-ul nativ și altceva decât VLAN-ul 1.

**2. Pe ce porturi de comutare ar trebui să fie activat PortFast pentru a spori stabilitatea STP?**

a.numai porturile care sunt alese ca porturi desemnate

b.toate porturile trunk care nu sunt porturi root

**c.toate porturile utilizatorului final**

d. porturile care se atașează la un comutator vecin

**Explicație:** PortFast va aduce imediat o interfață configurată ca port de acces sau trunchi în starea de redirecționare dintr-o stare de blocare, ocolind stările de ascultare și de învățare. Dacă este configurată pe o legătură trunchi, trecerea imediată la starea de redirecționare ar putea duce la formarea buclelor de Layer 2.

**3. Ce comandă ar fi cea mai bună de utilizat pe un port de comutator neutilizat dacă o companie respectă cele mai bune practici recomandate de Cisco?**

a.switchport port-security mac-address sticky mac-address

b.ip dhcp snooping

**c.shutdown**

d.switchport port-security violation shutdown

e.switchport port-security mac-address sticky

**Explicație:** Spre deosebire de porturile Ethernet ale routerului, porturile de comutare sunt activate implicit. Cisco recomandă dezactivarea oricărui port care nu este utilizat. Comanda ip dhcp snooping activează la nivel global DHCP snooping pe un comutator. Configurarea ulterioară permite definirea de porturi care pot răspunde la solicitările DHCP. Comanda switchport port-security este utilizată pentru a proteja rețeaua împotriva atașării neidentificate sau neautorizate a dispozitivelor din rețea.

**4. Care două caracteristici ale unui comutator Cisco Catalyst pot fi utilizate pentru a atenua atacurile de foame DHCP și falsificarea DHCP? (Alege doua.)**

a.DHCP server failover

b.extended ACL

**c.port security**

**d.DHCP snooping**

strong password on DHCP servers

**Explicație**: În atacurile de foame DHCP, un atacator inundă serverul DHCP cu solicitări DHCP de a utiliza toate adresele IP disponibile pe care serverul DHCP le poate emite. În atacurile de falsificare DHCP, un atacator configurează un server DHCP fals în rețea, astfel încât să ofere clienților adrese false de server DNS. Caracteristica de securitate a porturilor poate limita numărul de adrese MAC învățate dinamic per port sau permite conectarea numai a NIC-urilor valide cunoscute prin adresele MAC specifice ale acestora. Caracteristica DHCP Snooping poate identifica serverele DHCP legitime și poate bloca serverele DHCP false să emită informații despre adresa IP. Aceste două caracteristici pot ajuta la lupta împotriva atacurilor DHCP.

**5. Care este cel mai bun mod de a preveni un atac de salt VLAN?**

Utilizați încapsularea ISL pe toate legăturile trunk.

Dezactivați STP pe toate porturile nontrunk.

Utilizați VLAN 1 ca VLAN nativ pe porturile trunchiului.

**Dezactivați negocierea trunchiului (trunk negotion) pentru porturile trunk și setați static porturile non trunk ca porturi de acces.**

**Explicație:** Atacurile de salt VLAN se bazează pe faptul că atacatorul poate crea o legătură trunchială cu un comutator. Dezactivarea DTP și configurarea porturilor orientate către utilizator ca porturi de acces statice pot ajuta la prevenirea acestor tipuri de atacuri. Dezactivarea protocolului Spanning Tree (STP) nu va elimina atacurile de salt VLAN.

**6. Ce procedură este recomandată pentru a atenua șansele de falsificare ARP?**

a.Enable port security globally.

**b.Enable DHCP snooping on selected VLANs.**

c.Enable IP Source Guard on trusted ports.

d.Enable DAI on the management VLAN.

**Explicație**: Pentru a atenua șansele de falsificare ARP, se recomandă următoarele proceduri:

Implementați protecția împotriva falsificării DHCP prin activarea DHCP snooping la nivel global.

Activați DHCP Snooping pe VLAN-urile selectate.

Activați DAI pe VLAN-urile selectate.

Configurați interfețe de încredere pentru inspecția DHCP și inspecția ARP. Porturile nesigure sunt configurate implicit.​

**7. Care sunt două tipuri de porturi de comutare care sunt utilizate pe comutatoarele Cisco ca parte a apărării împotriva atacurilor de falsificare DHCP? (Alege doua.)**

a.unknown port

**b.trusted DHCP port**

c.unauthorized port

d.established DHCP port

**e.untrusted port**

f.authorized DHCP port

**Explicație:** DHCP Snooping recunoaște două tipuri de porturi pe switch-urile Cisco:

Porturi DHCP de încredere (Trusted DHCP ports ) – comutați porturile care se conectează la serverele DHCP din amonte

Porturi nesigure (Untrusted ports)– comutați porturile care se conectează la gazde care nu ar trebui să furnizeze mesaje server DHCP

**8. Ce două comenzi pot fi folosite pentru a activa PortFast pe un comutator? (Alege doua.)**

S1(config-if)# enable spanning-tree portfast

**S1(config-if)# spanning-tree portfast**

S1(config)# enable spanning-tree portfast default

**S1(config)# spanning-tree portfast default**

S1(config-line)# spanning-tree portfast

**Explicație:** PortFast poate fi configurat pe toate porturile fără trunchi folosind comanda de configurare globală implicită spanning-tree portfast. În mod alternativ, PortFast poate fi activat pe o interfață utilizând comanda de configurare a interfeței spanning-tree portfast.

**9. Un administrator care depanează problemele de conectivitate la un comutator observă că un port de comutator configurat pentru securitatea porturilor este în starea dezactivată de eroare. După verificarea cauzei încălcării, cum ar trebui administratorul să reactiveze portul fără a întrerupe funcționarea rețelei?**

a.Reporniți comutatorul.

**b.Lansați comanda shutdown urmată de comanda no shutdown de pe interfață.**

c.Lansați comanda no switchport port-security, apoi reactivați securitatea portului.

d.Lansați comanda de închidere a încălcării port-securității no switchport pe interfață.

**Explicație:** Dacă o interfață care a fost protejată cu securitatea porturilor intră în starea err-disabled, atunci a avut loc o încălcare și administratorul ar trebui să investigheze cauza încălcării. Odată ce cauza este determinată, administratorul poate lansa comanda shutdown urmată de comanda no shutdown pentru a activa interfața.

**10. Un administrator de rețea configurează DHCP Snooping pe un comutator. Ce comandă de configurare ar trebui folosită mai întâi?**

**ip dhcp snooping**

ip dhcp snooping limit rate

ip dhcp snooping vlan

ip dhcp snooping trust

**Explicație:** pașii pentru a activa DHCP snooping includ aceștia:

Pasul 1. Activați DHCP snooping folosind comanda de configurare globală ip dhcp snooping.

Pasul 2. Pe porturile de încredere, utilizați comanda de configurare a interfeței ip dhcp snooping trust.

Pasul 3. Activați DHCP snooping prin VLAN sau printr-o serie de VLAN-uri.

**11. Un administrator de rețea configurează DAI pe un comutator cu comanda ip arp inspection validate dst-mac. Care este scopul acestei comenzi de configurare?**

a.pentru a verifica adresa MAC de destinație din antetul Ethernet față de tabelul de adrese MAC

b.pentru a verifica adresa MAC de destinație din antetul Ethernet față de adresa MAC sursă din corpul ARP

c.pentru a verifica adresa MAC de destinație din antetul Ethernet cu ACL-urile ARP configurate de utilizator

**d.pentru a verifica adresa MAC destinație din antetul Ethernet față de adresa MAC țintă din corpul ARP**

**Explicație:** DAI poate fi configurat pentru a verifica ambele adrese MAC și IP de destinație sau sursă:

Destination MAC – Verifică adresa MAC destinație din antetul Ethernet cu adresa MAC țintă din corpul ARP.

Sursă MAC – Verifică adresa MAC sursă din antetul Ethernet cu adresa MAC a expeditorului din corpul ARP.

Adresă IP – Verifică corpul ARP pentru adrese IP nevalide și neașteptate, inclusiv adresele 0.0.0.0, 255.255.255.255 și toate adresele IP multicast.

**12. Ce caracteristică de securitate ar trebui să fie activată pentru a preveni un atacator să depășească tabelul de adrese MAC al unui switch?**

a.storm control

**b.port security**

c.BPDU filter

d.root guard

**Explicație:** Securitatea porturilor limitează numărul de adrese MAC sursă permise printr-un port de comutare. Această caracteristică poate împiedica un atacator să inunde un comutator cu multe adrese MAC falsificate.

**13. Ce atac Layer 2 este atenuat prin dezactivarea Dynamic Trunking Protocol?**

**a.VLAN hopping**

b.DHCP spoofing

c.ARP poisoning

d.ARP spoofing

**Explicație:** Atenuarea unui atac de salt VLAN se poate face prin dezactivarea Protocolului de trunchiere dinamică (DTP) și prin setarea VLAN-ului nativ al legăturilor trunchi la VLAN-urile care nu sunt utilizate.

**14. Un administrator de rețea configurează DAI pe un comutator. Ce comandă ar trebui utilizată pe interfața uplink care se conectează la un router?**

**ip arp inspection trust**

ip dhcp snooping

ip arp inspection vlan

spanning-tree portfast

**Explicație:** În general, un router servește ca gateway implicit pentru LAN sau VLAN pe switch. Prin urmare, interfața uplink care se conectează la un router ar trebui să fie un port de încredere pentru redirecționarea cererilor ARP.

**15. Unde sunt stocate adresele MAC învățate în mod dinamic atunci când învățarea sticky este activată cu comanda switchport port-security mac-address sticky?**

a.flash

b.NVRAM

**c.RAM**

d.ROM

**Explicație:** Când adresele MAC sunt învățate automat utilizând opțiunea de comandă sticky, adresele MAC învățate sunt adăugate la configurația care rulează, care este stocată în RAM.