**Reduceți atacurile ARP**

**Inspecție ARP dinamică**

Într-un atac ARP tipic, un actor de amenințare poate trimite cereri ARP nesolicitate către alte gazde de pe subrețea cu adresa MAC a actorului amenințării și adresa IP a gateway-ului implicit. Pentru a preveni falsificarea ARP și otrăvirea ARP rezultată, un comutator trebuie să se asigure că sunt transmise numai solicitările și răspunsurile ARP valide.

Inspecția dinamică ARP (DAI) necesită DHCP snooping și ajută la prevenirea atacurilor ARP prin:

* Nu transmiterea solicitărilor ARP invalide sau gratuite către alte porturi din același VLAN.
* Interceptarea tuturor solicitărilor și răspunsurilor ARP pe porturi nede încredere.
* Verificarea fiecărui pachet interceptat pentru o legare IP-la-MAC validă.
* Eliminarea și înregistrarea solicitărilor ARP care provin din surse nevalide pentru a preveni otrăvirea ARP.
* Eroare la dezactivarea interfeței dacă numărul DAI configurat de pachete ARP este depășit.

**Ghid de implementare DAI**

Pentru a reduce șansele de falsificare ARP și otrăvire cu ARP, urmați aceste linii directoare de implementare a DAI:

* Activați 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.

În general, este recomandabil să configurați toate porturile comutatoarelor de acces ca nede încredere și să configurați toate porturile de legătură în sus care sunt conectate la alte comutatoare ca fiind de încredere.

Exemplul de topologie din figură identifică porturile de încredere și cele nede încredere.

Graficul arată o legendă cu un pătrat violet Trusted Port și un cerc roșu Untrusted Port, deasupra ei este o diagramă LAN care arată Dynamic ARP Inspection Trust. Diagrama ilustrează o rețea LAN cu porturi de încredere și nede încredere. Pe o interfață din stânga jos este un atacator pe un PC, iar în stânga sus este un P C obișnuit. Ambele dispozitive sunt conectate la comutator și ambele au un cerc roșu pe portul comutatorului pentru un port neîncrezat. În dreapta comutatorului se află un router care este, de asemenea, conectat la comutator. Conexiunea la router are un pătrat violet pe comutator care simbolizează o conexiune de încredere pentru ARP.

PC-AS1R1F0/1F0/2F0/24

Port neîncrezătorPort de încredereVLAN 10

**Exemplu de configurare DAI**

În topologia anterioară, S1 conectează doi utilizatori pe VLAN 10. DAI va fi configurat pentru a atenua atacurile ARP spoofing și ARP otravire.

După cum se arată în exemplu, DHCP snooping este activat deoarece DAI necesită ca tabelul de legare DHCP snooping să funcționeze. Apoi, DHCP Snooping și inspecția ARP sunt activate pentru computerele de pe VLAN10. Portul uplink către router este de încredere și, prin urmare, este configurat ca de încredere pentru DHCP snooping și inspecția ARP.

**S1(config)# ip dhcp snooping**

**S1(config)# ip dhcp snooping vlan 10**

**S1(config)# ip arp inspection vlan 10**

**S1(config)# interface fa0/24**

**S1(config-if)# ip dhcp snooping trust**

**S1(config-if)# ip arp inspection trust**

DAI poate fi, de asemenea, 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.

Comanda de configurare globală **ip arp validate { [ src-mac ] [ dst-mac ] [ ip ] }** este utilizată pentru a configura DAI să arunce pachetele ARP atunci când adresele IP sunt invalide. Poate fi folosit atunci când adresele MAC din corpul pachetelor ARP nu se potrivesc cu adresele specificate în antetul Ethernet. Observați în exemplul următor cum poate fi configurată o singură comandă. Prin urmare, introducerea mai multor comenzi **ip arp inspection validate** suprascrie comanda anterioară. Pentru a include mai multe metode de validare, introduceți-le pe aceeași linie de comandă așa cum este prezentată și verificată în rezultatul următor.

**S1(config)# ip arp inspection validate ?**

**dst-mac Validate destination MAC address**

**ip Validate IP addresses**

**src-mac Validate source MAC address**

**S1(config)# ip arp inspection validate src-mac**

**S1(config)# ip arp inspection validate dst-mac**

**S1(config)# ip arp inspection validate ip**

**S1(config)# do show run | include validate**

**ip arp inspection validate ip**

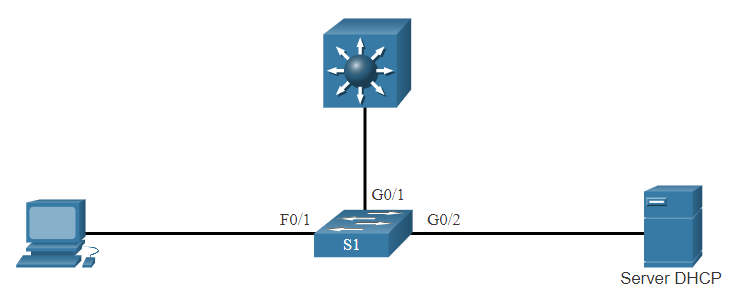
**S1(config)# ip arp inspection validate src-mac dst-mac ip**

**S1(config)# do show run | include validate**

**ip arp inspection validate src-mac dst-mac ip**

**S1(config)#**

**Syntax Checker - Atenuează atacurile ARP**

Implementați DAI pentru un comutator bazat pe următoarea topologie și cerințele specificate.

**You are currently logged into S1. Enable DHCP snooping globally for the switch.**

**S1(config)#ip dhcp snooping**

**Enter interface configuration mode for g0/1 - 2, trust the interfaces for both DHCP snooping and DAI, and then return to global configuration mode.**

**S1(config)#interface range g0/1 - 2**

**S1(config-if-range)#ip dhcp snooping trust**

**S1(config-if-range)#ip arp inspection trust**

**S1(config-if-range)#exit**

**Enable DHCP snooping and DAI for VLANs 10,20,30-49.**

**S1(config)#ip dhcp snooping vlan 10,20,30-49**

**S1(config)#ip arp inspection vlan 10,20,30-49**

**S1(config)#**

**You have successfully configured DAI for the switch.**