Kapcsolók biztonsági konfigurációja

Portbiztonság megvalósítása

A 2. rétegű eszközöket a vállalat biztonsági infrastruktúrájának leggyengébb láncszemének tekintik. A 2. rétegű támadások a legegyszerűbben telepíthetők a hackerek számára, de ezek a fenyegetések néhány általános 2. rétegű megoldással is mérsékelhetők.

Az összes kapcsolóportot (interfészt) rögzíteni kell, mielőtt a kapcsolót üzemi használatra telepítenék. A portok biztonsága a funkciójától függ.

Egy egyszerű módszer, amellyel sok rendszergazda segít megvédeni a hálózatot az illetéktelen hozzáféréstől, az, hogy letiltja a kapcsoló összes nem használt portját. Például, ha egy Catalyst 2960 switch 24 porttal rendelkezik, és három Fast Ethernet kapcsolat van használatban, célszerű letiltani a 21 használaton kívüli portot. Keresse meg az egyes nem használt portokat, és adja ki a Cisco IOS leállítási parancsát. Ha egy portot később újra aktiválni kell, akkor a no shutdown paranccsal engedélyezhető.

A portok tartományának konfigurálásához használja az **interface range** parancsot.

```
Switch(config)# interface range type module/first-number – last-number
```

Például az Fa0/8-Fa0/24 portok leállításához a következő parancsot kell beírnunk:

```
S1(config)# interface range fa0/8 - 24
S1(config-if-range)# shutdown
%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to
administratively down
(output omitted)
%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to
administratively down
S1(config-if-range)#
```

MAC-címtáblázat támadásainak csökkentése

A MAC-címtábla túlcsordulási támadásainak megelőzésének legegyszerűbb és leghatékonyabb módja a portbiztonság engedélyezése.

A portbiztonság korlátozza a porton engedélyezett érvényes MAC-címek számát. Lehetővé teszi az adminisztrátor számára, hogy manuálisan konfigurálja a MAC-címeket egy porthoz, vagy engedélyezze a switch számára, hogy dinamikusan tanuljon meg korlátozott számú MAC-címet. Amikor egy portbiztonsággal konfigurált port kap egy keretet, a rendszer összehasonlítja a keret forrás MAC-címét a biztonságos forrás MAC-címek listájával, amelyeket manuálisan konfiguráltak vagy dinamikusan tanultak meg a porton.

Egy porton az engedélyezett MAC-címek számának egyre korlátozásával a portbiztonság segítségével ellenőrizhető a hálózathoz való jogosulatlan hozzáférés.

Portbiztonság bekapcsolása

Figyeljük meg a példában, hogy a switchport port-security parancsot elutasították. Ennek az az oka, hogy a portbiztonság csak manuálisan konfigurált hozzáférési portokon vagy manuálisan konfigurált fővonali portokon konfigurálható. Alapértelmezés szerint a 2. rétegbeli kapcsolóportok dinamikus automatikusra vannak állítva (trunking bekapcsolva). Ezért a példában a port a switchport mód hozzáférési interfész konfigurációs paranccsal van konfigurálva.

Megjegyzés: A trönk portok biztonsága túlmutat a tanfolyam keretein.

```
S1(config)# interface f0/1
S1(config-if)# switchport port-security
Command rejected: FastEthernet0/1 is a dynamic port.
S1(config-if)# switchport mode access
S1(config-if)# switchport port-security
S1(config-if)# end
S1#
```

A show port-security interface paranccsal jelenítheti meg a FastEthernet 0/1 aktuális portbiztonsági beállításait, ahogy a példában is látható. Figyelje meg, hogyan van engedélyezve a portbiztonság, a port állapota Biztonságos leállítás, ami azt jelenti, hogy nincs csatlakoztatva eszköz, és nem történt megsértés, a szabálysértési mód a Leállítás, és hogy a MAC-címek maximális száma 1. Ha egy eszköz csatlakozik a port, a kapcsoló port állapota a Secure up feliratot jeleníti meg, és a kapcsoló automatikusan hozzáadja az eszköz MAC-címét biztonságos MAC-címként. Ebben a példában egyetlen eszköz sem csatlakozik a porthoz.

```
S1# show port-security interface f0/1
Port Security              : Enabled
Port Status                : Secure-down
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
S1#
```

Megjegyzés: Ha egy aktív port a switchport port-security paranccsal van konfigurálva, és egynél több eszköz csatlakozik ahhoz a porthoz, a port átvált hibaletiltás állapotba. Ezt a feltételt ebben a témakörben később tárgyaljuk.

A portbiztonság engedélyezése után más portbiztonsági jellemzők is konfigurálhatók a példában látható módon.

MAC-címek korlátozása és megtanulása

A porton engedélyezett MAC-címek maximális számának beállításához használja a következő parancsot:

```
Switch(config-if)# switchport port-security maximum value
```

A port alapértelmezett biztonsági értéke 1. A konfigurálható biztonságos MAC-címek maximális száma a kapcsolótól és az IOS-től függ. Ebben a példában a maximum 8192.

```
S1(config)# interface f0/1
S1(config-if)# switchport port-security maximum ?
  <1-8192>  Maximum addresses
S1(config-if)# switchport port-security maximum
```

A kapcsolót háromféleképpen lehet beállítani úgy, hogy megismerje a biztonságos porton lévő MAC-címeket:

1. Kézi konfigurálás

A rendszergazda manuálisan konfigurál egy statikus MAC-cím(eke)t a következő paranccsal a porton lévő minden biztonságos MAC-címhez:

```
Switch(config-if)# switchport port-security mac-address mac-address
```

2. Dinamikusan tanult

A switchport port-security parancs beírásakor a porthoz csatlakoztatott eszköz aktuális forrás MAC-ja automatikusan védetté válik, de nem kerül hozzáadásra az indítási konfigurációhoz. Ha a kapcsolót újraindítják, a portnak újra meg kell tanulnia az eszköz MAC-címét.

3. Dinamikusan tanult – ragadós

Az adminisztrátor a következő paranccsal engedélyezheti, hogy a kapcsoló dinamikusan megtanulja a MAC-címet, és „ragassza” őket a futó konfigurációhoz:

```
Switch(config-if)# switchport port-security mac-address sticky
```

A futó konfiguráció mentése a dinamikusan tanult MAC-címet véglegesíti az NVRAM-ban.

A következő példa a FastEthernet 0/1 teljes portbiztonsági konfigurációját mutatja be, a Fa0/1 porthoz csatlakoztatott gazdagéppel. A rendszergazda legfeljebb 2 MAC-címet ad meg, manuálisan konfigurál egy biztonságos MAC-címet, majd konfigurálja a portot, hogy dinamikusan tanulja meg a további biztonságos MAC-címeket, legfeljebb 2 biztonságos MAC-címig. A konfiguráció ellenőrzéséhez használja a show port-security interface és a show port-security address parancsot.

```
*Mar  1 00:12:38.179: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed
state to up
*Mar  1 00:12:39.194: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to up
S1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#
S1(config)# interface fa0/1
S1(config-if)# switchport mode access
S1(config-if)# switchport port-security
S1(config-if)# switchport port-security maximum 2
S1(config-if)# switchport port-security mac-address aaaa.bbbb.1234
S1(config-if)# switchport port-security mac-address sticky
S1(config-if)# end
S1# show port-security interface fa0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 2
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : a41f.7272.676a:1
Security Violation Count   : 0
S1# show port-security address
               Secure Mac Address Table
------------------------------------------------------------------------
-
Vlan    Mac Address       Type                          Ports   Remaining
Age
                                                                   (mins)
----    -----------       ----                          -----   -----------
-
1    a41f.7272.676a    SecureSticky                 Fa0/1        -
1    aaaa.bbbb.1234    SecureConfigured             Fa0/1        -
------------------------------------------------------------------------
-
Total Addresses in System (excluding one mac per port)     : 1
Max  Addresses limit in System (excluding one mac per port) : 8192
```

A show port-security interface parancs kimenete ellenőrzi, hogy a portbiztonság engedélyezve van-e, van-e gazdagép csatlakoztatva a porthoz (azaz Secure-up), összesen 2 MAC-cím engedélyezett, és az S1 megtanult egy MAC-címet. statikusan és egy MAC-címet dinamikusan (azaz ragadósan).

A show port-security address parancs kimenete felsorolja a két tanult MAC-címet.

Port biztonság öregedés

A portbiztonsági öregítés használható a porton lévő statikus és dinamikus biztonságos címek öregedési idejének beállítására. Portonként kétféle öregítés támogatott:

```
   Abszolút – A porton lévő biztonságos címek törlődnek a megadott öregedési
idő után.
   Inaktivitás – A porton lévő biztonságos címek csak akkor törlődnek, ha
inaktívak a megadott öregedési ideig.
```

Az öregítés segítségével távolítsa el a biztonságos MAC-címeket egy biztonságos porton a meglévő biztonságos MAC-címek manuális törlése nélkül. Az öregedési időkorlátok is növelhetők, hogy a korábbi biztonságos MAC-címek megmaradjanak még új MAC-címek hozzáadásakor is. A statikusan konfigurált biztonságos címek öregítése portonként engedélyezhető vagy letiltható.

A switchport port-security aging parancs segítségével engedélyezheti vagy letilthatja a statikus öregítést a biztonságos porton, vagy beállíthatja az öregítési időt vagy típust.

```
Switch(config-if)# switchport port-security aging { static | time time |
type {absolute | inactivity}}
```

A következő példa azt mutatja, hogy egy rendszergazda 10 perces inaktivitásra konfigurálja az öregedés típusát, és a show port-security interface parancsot használja a konfiguráció ellenőrzésére.

```
S1(config)# interface fa0/1
S1(config-if)# switchport port-security aging time 10
S1(config-if)# switchport port-security aging type inactivity
S1(config-if)# end
S1# show port-security interface fa0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 10 mins
Aging Type                 : Inactivity
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 2
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : a41f.7272.676a:1
Security Violation Count   : 0
S1#
```

Portbiztonsági megsértési módok

Ha a porthoz csatlakoztatott eszköz MAC-címe eltér a biztonságos címek listájától, akkor portsértés történik. Alapértelmezés szerint a port hibamentes állapotba kerül.

A portbiztonsági megsértési mód beállításához használja a következő parancsot:

```
Switch(config-if)# switchport port-security violation { protect | restrict |
shutdown}
```

A következő példa azt mutatja be, hogy egy rendszergazda a biztonsági megsértést „korlátozásra” változtatja. A show port-security interface parancs kimenete megerősíti, hogy a változtatás megtörtént.

```
S1(config)# interface f0/1
S1(config-if)# switchport port-security violation restrict
S1(config-if)# end
S1#
S1# show port-security interface f0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 10 mins
Aging Type                 : Inactivity
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 2
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : a41f.7272.676a:1
Security Violation Count   : 0
S1#
```

A portok hiba miatt letiltott állapotban

Mi történik, ha a portbiztonság megsértése leáll, és port megsértése történik? A port fizikailag le van állítva, és hiba miatt letiltott állapotba kerül, és ezen a porton nem küldenek vagy fogadnak forgalmat.

Az ábrán a portbiztonság megsértése visszaállt az alapértelmezett leállítási beállításra. Ezután az a41f.7272.676a MAC-című gazdagépet leválasztják, és egy új gazdagépet csatlakoztatnak a Fa0/1-hez.

Figyelje meg, hogyan jön létre a portbiztonsággal kapcsolatos üzenetek sorozata a konzolon.

```
S1(config)# int fa0/1
S1(config-if)# switchport port-security violation shutdown
S1(config-if)# end
S1#
*Mar  1 00:24:15.599: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to down
*Mar  1 00:24:16.606: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed
state to down
```

```
*Mar  1 00:24:19.114: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed
state to up
*Mar  1 00:24:20.121: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to up
S1#
*Mar  1 00:24:32.829: %PM-4-ERR_DISABLE: psecure-violation error detected on
Fa0/1, putting Fa0/1 in err-disable state
*Mar  1 00:24:32.838: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation
occurred, caused by MAC address a41f.7273.018c on port FastEthernet0/1.
*Mar  1 00:24:33.836: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to down
*Mar  1 00:24:34.843: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed
state to down
S1#
```

Megjegyzés: A port protokoll és a kapcsolat állapota lefelé módosul, és a port LED kialszik.

A példában a show interface parancs a port állapotát err-disabledként azonosítja. A show port-security interface parancs kimenete mostantól a portállapotot Secure-shutdownként mutatja a Secure-up helyett. A biztonsági hiba számlálója 1-gyel növekszik.

```
S1# show interface fa0/1 | include down
FastEthernet0/18 is down, line protocol is down (err-disabled)
(output omitted)
S1# show port-security interface fa0/1
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 10 mins
Aging Type                 : Inactivity
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 2
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : a41f.7273.018c:1
Security Violation Count   : 1
S1#
```

Az adminisztrátornak meg kell határoznia, mi okozta a biztonság megsértését. Ha egy biztonságos porthoz illetéktelen eszköz csatlakozik, a biztonsági fenyegetés a port újbóli engedélyezése előtt megszűnik.

A következő példában az első gazdagép újracsatlakozik a Fa0/1-hez. A port újbóli engedélyezéséhez először használja a shutdown parancsot, majd a no shutdown paranccsal állítsa működőképessé a portot, ahogy a példában is látható.

```
S1(config)# interface fa0/1
S1(config-if)# shutdown
S1(config-if)#
*Mar  1 00:39:54.981: %LINK-5-CHANGED: Interface FastEthernet0/1, changed
```

```
state to administratively down
S1(config-if)# no shutdown
S1(config-if)#
*Mar  1 00:40:04.275: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed
state to up
*Mar  1 00:40:05.282: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to up
S1(config-if)#
```

Portbiztonság ellenőrzése

Miután konfigurálta a portbiztonságot egy kapcsolón, ellenőrizze az egyes interfészeket, és ellenőrizze, hogy a portbiztonság megfelelően van-e beállítva, és ellenőrizze, hogy a statikus MAC-címek megfelelően vannak-e konfigurálva.

Portbiztonság minden interfészhez

A kapcsoló portbiztonsági beállításainak megjelenítéséhez használja a show port-security parancsot. A példa azt jelzi, hogy csak egy port van konfigurálva a switchport port-security paranccsal.

```
S1# show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                (Count)       (Count)          (Count)
---------------------------------------------------------------------------
      Fa0/1              2            2                  0         Shutdown
---------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 1
Max Addresses limit in System (excluding one mac per port) : 8192
S1#
```

Portbiztonság egy adott interfészhez

Használja a show port-security interface parancsot egy adott interfész részleteinek megtekintéséhez, amint az korábban és ebben a példában is látható.

```
S1# show port-security interface fastethernet 0/1
Port Security               : Enabled
Port Status                 : Secure-up
Violation Mode              : Shutdown
Aging Time                  : 10 mins
Aging Type                  : Inactivity
SecureStatic Address Aging  : Disabled
Maximum MAC Addresses       : 2
Total MAC Addresses         : 2
Configured MAC Addresses    : 1
Sticky MAC Addresses        : 1
Last Source Address:Vlan    : a41f.7273.018c:1
Security Violation Count    : 0
```

```
S1#
```

Ellenőrizze a tanult MAC-címeket

Annak ellenőrzésére, hogy a MAC-címek „ragaszkodnak” a konfigurációhoz, használja a show run parancsot a FastEthernet 0/19 példájában látható módon.

```
S1# show run interface fa0/1
Building configuration...

Current configuration : 365 bytes
!
interface FastEthernet0/1
 switchport mode access
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky a41f.7272.676a
 switchport port-security mac-address aaaa.bbbb.1234
 switchport port-security aging time 10
 switchport port-security aging type inactivity
 switchport port-security
end

S1#
```

Ellenőrizze a biztonságos MAC-címeket

Az összes kapcsolófelületen kézzel konfigurált vagy dinamikusan betanított biztonságos MAC-cím megjelenítéséhez használja a show port-security address parancsot a példában látható módon.

```
S1# show port-security address
               Secure Mac Address Table
------------------------------------------------------------------------
-
Vlan    Mac Address       Type                          Ports   Remaining
Age
                                                                   (mins)
----    -----------       ----                          -----   -----------
-
   1    a41f.7272.676a    SecureSticky                  Fa0/1        -
   1    aaaa.bbbb.1234    SecureConfigured              Fa0/1        -
------------------------------------------------------------------------
-
Total Addresses in System (excluding one mac per port)     : 1
Max Addresses limit in System (excluding one mac per port) : 8192
S1#
```

VLAN-támadások csökkentése

VLAN támadások áttekintése

Gyors áttekintésként elmondható, hogy a VLAN ugrásos támadás háromféleképpen indítható:

- A támadó gazdagéptől érkező DTP-üzenetek meghamisítása, hogy a kapcsoló trunking módba lépjen. Innentől a támadó a cél VLAN-nal címkézett forgalmat küldheti, majd a kapcsoló eljuttatja a csomagokat a célállomásra.
- Bemutatjuk a szélhámos kapcsolót és engedélyezzük a trönkölést. A támadó ezután hozzáférhet az áldozat kapcsolón lévő összes VLAN-hoz a rogue kapcsolóról.
- A VLAN ugrásos támadások másik típusa a kettős címkézéses (vagy kettős beágyazású) támadás. Ez a támadás kihasználja a legtöbb kapcsoló hardverének működését.

Lépések a VLAN ugrásos támadások mérséklésére

A VLAN ugrásos támadások mérsékléséhez kövesse az alábbi lépéseket:

1. lépés: Tiltsa le a DTP (automatikus trönkelés) egyeztetéseket a nem trönkös portokon a switchport mód hozzáférési interfész konfigurációs parancsával.

2. lépés: Tiltsa le a nem használt portokat, és helyezze őket egy nem használt VLAN-ba.

3. lépés: Manuálisan engedélyezze a fővonali kapcsolatot egy trönkporton a switchport mode trunk paranccsal.

4. lépés: Tiltsa le a DTP (automatikus trunking) tárgyalásokat a trunking portokon a switchport nonegotiate paranccsal.

5. lépés: Állítsa be a natív VLAN-t az 1. VLAN-tól eltérő VLAN-ra a switchport trunk native vlan vlan_number paranccsal.

Tegyük fel például a következőket:

```
   A 0/1–fa0/16 FastEthernet portok aktív hozzáférési portok
   A 0/17 és 0/20 közötti FastEthernet portok jelenleg nincsenek
használatban
   A 0/21 és 0/24 közötti FastEthernet portok fővonali portok.
```

A VLAN ugrás a következő konfiguráció megvalósításával mérsékelhető.

```
S1(config)# interface range fa0/1 - 16
S1(config-if-range)# switchport mode access
S1(config-if-range)# exit
S1(config)#
S1(config)# interface range fa0/17 - 20
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 1000
```

```
S1(config-if-range)# shutdown
S1(config-if-range)# exit
S1(config)#
S1(config)# interface range fa0/21 - 24
S1(config-if-range)# switchport mode trunk
S1(config-if-range)# switchport nonegotiate
S1(config-if-range)# switchport trunk native vlan 999
S1(config-if-range)# end
S1#
```

- A 0/1-től 0/16-ig terjedő FastEthernet portok hozzáférési portok, ezért a trönkölés tiltva van azáltal, hogy kifejezetten hozzáférési portokká teszik őket.
- A 0/17-től 0/20-ig terjedő FastEthernet portok nem használt portok, le vannak tiltva, és nem használt VLAN-hoz vannak rendelve.
- A 0/21-től 0/24-ig terjedő FastEthernet portok fővonali kapcsolatok, és manuálisan engedélyezhetők trönkként a DTP letiltásával. A natív VLAN is megváltozott az alapértelmezett VLAN 1-ről egy nem használt VLAN 999-re.

DHCP-támadások mérséklése

A DHCP éhező támadás célja szolgáltatásmegtagadás (DoS) létrehozása a kliensek összekapcsolásához. A DHCP éhezési támadásokhoz olyan támadási eszközre van szükség, mint a Gobbler. Emlékezzünk vissza, hogy a DHCP-kiéhezési támadások hatékonyan mérsékelhetők a portbiztonság használatával, mivel a Gobbler minden elküldött DHCP-kéréshez egyedi forrás MAC-címet használ.

A DHCP-hamisítási támadások mérséklése azonban nagyobb védelmet igényel. A Gobbler beállítható úgy, hogy a tényleges interfész MAC-címét használja forrás Ethernet-címként, de adjon meg egy másik Ethernet-címet a DHCP hasznos adatban. Ez hatástalanná tenné a portbiztonságot, mivel a forrás MAC-címe legitim lenne.

A DHCP-hamisítási támadások mérsékelhetők a megbízható portokon végzett DHCP-snooping használatával.

DHCP leskelődés (DHCP Snooping)

A DHCP leskelődés nem támaszkodik a forrás MAC-címekre. Ehelyett a DHCP-snooping határozza meg, hogy a DHCP-üzenetek adminisztratívan konfigurált megbízható vagy nem megbízható forrásból származnak. Ezután kiszűri a DHCP-üzeneteket, és korlátozza a nem megbízható forrásokból származó DHCP-forgalmat.

Az adminisztratív irányítása alatt álló eszközök, például a kapcsolók, útválasztók és szerverek megbízható források. A tűzfalon kívüli vagy a hálózaton kívüli eszközök nem megbízható források. Ezenkívül az összes hozzáférési portot általában nem megbízható forrásként kezelik. Az ábra egy példát mutat megbízható és nem megbízható portokra.

Figyelje meg, hogy a csaló DHCP-szerver egy nem megbízható porton lesz, miután engedélyezte a DHCP-megfigyelést. Alapértelmezés szerint minden interfész nem megbízható. A megbízható interfészek általában fővonali hivatkozások és portok, amelyek közvetlenül csatlakoznak egy legitim

DHCP-kiszolgálóhoz. Ezeket az interfészeket kifejezetten megbízhatóként kell konfigurálni.

Létrejön egy DHCP-tábla, amely tartalmazza egy nem megbízható porton lévő eszköz forrás MAC-címét és a DHCP-szerver által az eszközhöz rendelt IP-címet. A MAC-cím és az IP-cím össze van kötve. Ezért ezt a táblát DHCP leskelődő kötési táblának nevezik.

A DHCP Snooping megvalósításának lépései

Kövesse a következő lépéseket a DHCP leskelődés engedélyezéséhez:

1. lépés: Engedélyezze a DHCP snooping funkciót az ip dhcp snooping globális konfigurációs paranccsal.

2. lépés: Megbízható portokon használja az ip dhcp snooping trust interface konfigurációs parancsot.

3. lépés: Korlátozza a nem megbízható portokon másodpercenként fogadható DHCP-felderítési üzenetek számát az ip dhcp snooping limit rate interfész konfigurációs parancsával.

4. lépés: Engedélyezze a DHCP snooping VLAN-on vagy egy sor VLAN-on keresztüli használatát az ip dhcp snooping vlan globális konfigurációs paranccsal.

DHCP Snooping konfigurációs példa

```
S1(config)# ip dhcp snooping
S1(config)# interface f0/1
S1(config-if)# ip dhcp snooping trust
S1(config-if)# exit
S1(config)# interface range f0/5 - 24
S1(config-if-range)# ip dhcp snooping limit rate 6
S1(config-if-range)# exit
S1(config)# ip dhcp snooping vlan 5,10,50-52
S1(config)# end
S1#
```

```
S1# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
5,10,50-52
DHCP snooping is operational on following VLANs:
none
DHCP snooping is configured on the following L3 Interfaces:
Insertion of option 82 is enabled
   circuit-id default format: vlan-mod-port
   remote-id: 0cd9.96d2.3f80 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:
```

```
Interface                   Trusted    Allow option    Rate limit (pps)
-----------------------     -------    ------------    ----------------
FastEthernet0/1             yes        yes             unlimited
  Custom circuit-ids:
FastEthernet0/5             no         no              6
  Custom circuit-ids:
FastEthernet0/6             no         no              6
  Custom circuit-ids:
S1# show ip dhcp snooping binding
MacAddress         IpAddress       Lease(sec) Type           VLAN Interface
------------------ --------------- ---------- ------------- ---- -----------
---------
00:03:47:B5:9F:AD  192.168.10.11   193185     dhcp-snooping 5
FastEthernet0/5
```

Az ARP támadások mérséklése

Dinamikus ARP ellenőrzés

Egy tipikus ARP-támadás során a fenyegetés szereplői kéretlen ARP-kéréseket küldhetnek az alhálózat más gazdagépeinek a fenyegetettség szereplőjének MAC-címével és az alapértelmezett átjáró IP-címével. Az ARP-hamisítás és az ebből eredő ARP-mérgezés megelőzése érdekében a kapcsolónak biztosítania kell, hogy csak érvényes ARP-kérések és válaszok kerüljenek továbbításra.

A dinamikus ARP-ellenőrzés (DAI) DHCP-figyelést igényel, és segít megelőzni az ARP-támadásokat:

- Érvénytelen vagy indokolatlan ARP-kérések továbbítása ugyanazon VLAN más portjaira.
- Minden ARP-kérés és válasz elfogása nem megbízható portokon.
- Minden egyes elfogott csomag ellenőrzése érvényes IP-MAC-kötéshez.
- Az ARP eldobása és naplózása Érvénytelen forrásból érkező kérések az ARP-mérgezés megelőzése érdekében.
- Hiba az interfész letiltásakor, ha az ARP-csomagok konfigurált DAI-számát túllépik.

DAI végrehajtási irányelvek

Az ARP-hamisítás és az ARP-mérgezés kockázatának csökkentése érdekében kövesse az alábbi DAI-megvalósítási irányelveket:

- Engedélyezze a DHCP-snoopot globálisan.
- Engedélyezze a DHCP-figyelést a kiválasztott VLAN-okon.
- A DAI engedélyezése a kiválasztott VLAN-okon.

Megbízható interfészek konfigurálása a DHCP leskelődéshez és az ARP ellenőrzéshez.

Általában tanácsos az összes hozzáférési kapcsoló portját nem megbízhatóként konfigurálni, és minden olyan uplink portot, amely más kapcsolókhoz csatlakozik, megbízhatóként konfigurálni.

DAI konfigurációs példa

```
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
```

A DAI úgy is konfigurálható, hogy ellenőrizze a cél- vagy forrás MAC- és IP-címeket:

- Cél MAC – Ellenőrzi a cél MAC-címét az Ethernet fejlécben az ARP törzsben lévő cél MAC-címével.
- Forrás MAC – Ellenőrzi az Ethernet fejlécben szereplő forrás MAC-címet az ARP törzsben található küldő MAC-címével.
- IP-cím – Ellenőrzi, hogy az ARP törzsében vannak-e érvénytelen és váratlan IP-címek, beleértve a 0.0.0.0, 255.255.255.255 címeket és az összes IP csoportos küldési címet.

Az ip arp ellenőrzés validate {[src-mac] [dst-mac] [ip]} globális konfigurációs parancs a DAI beállítására szolgál az ARP-csomagok eldobására, ha az IP-címek érvénytelenek. Akkor használható, ha az ARP-csomagok törzsében lévő MAC-címek nem egyeznek meg az Ethernet-fejlécben megadott címekkel. Figyelje meg a következő példában, hogy csak egy parancs konfigurálható. Ezért több ip arp ellenőrzés érvényesítése parancs beírása felülírja az előző parancsot. Ha egynél több érvényesítési módszert szeretne megadni, írja be őket ugyanabba a parancssorba, ahogyan a következő kimenetben látható és ellenőrzött.

```
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)#
```

STP-támadások csökkentése

PortFast és BPDU Guard

Emlékezzünk vissza, hogy a hálózati támadók a gyökérhíd meghamisításával és a hálózat topológiájának megváltoztatásával manipulálhatják a Spanning Tree Protocol-t (STP), hogy támadást hajtsanak végre. A Spanning Tree Protocol (STP) manipulációs támadások mérsékléséhez használja a

PortFast és a Bridge Protocol Data Unit (BPDU) Guard szolgáltatást:

- PortFast – A PortFast azonnal egy hozzáférési portként konfigurált interfészt hoz a továbbítási állapotba a blokkoló állapotból, megkerülve a figyelési és tanulási állapotokat. Alkalmazza az összes végfelhasználói portra. A PortFast csak a végeszközökhöz csatlakoztatott portokon konfigurálható.
- BPDU Guard – A BPDU őr azonnali hiba miatt letiltja a BPDU-t fogadó portot. A PortFasthoz hasonlóan a BPDU őrt is csak a végeszközökhöz csatlakoztatott interfészeken szabad konfigurálni.

PortFast konfigurációs példa

```
S1(config)# interface fa0/1
S1(config-if)# switchport mode access
S1(config-if)# spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
 host. Connecting hubs, concentrators, switches, bridges, etc... to this
 interface when portfast is enabled, can cause temporary bridging loops.
 Use with CAUTION
%Portfast has been configured on FastEthernet0/1 but will only
 have effect when the interface is in a non-trunking mode.
S1(config-if)# exit
S1(config)# spanning-tree portfast default
%Warning: this command enables portfast by default on all interfaces. You
 should now disable portfast explicitly on switched ports leading to hubs,
 switches and bridges as they may create temporary bridging loops.
S1(config)# exit
S1# show running-config | begin span
spanning-tree mode pvst
spanning-tree portfast default
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
(output omitted)
S1#
```

BPDU Guard konfigurációs példa

```
S1(config)# interface fa0/1
S1(config-if)# spanning-tree bpduguard enable
S1(config-if)# exit
S1(config)# spanning-tree portfast bpduguard default
S1(config)# end
S1# show spanning-tree summary
Switch is in pvst mode
Root bridge for: none
Extended system ID           is enabled
Portfast Default             is enabled
PortFast BPDU Guard Default  is enabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is disabled
EtherChannel misconfig guard is enabled
UplinkFast                   is disabled
BackboneFast                 is disabled
Configured Pathcost method used is short
(output omitted)
S1#
```