Switch Güvenlik Konfigürasyonları

Kurumlarda, kablolar duvar içlerinden geçirilerek bina geneline dağıtımı yapılır. Bu kabloların switchlere bağlı ihtimali yüksektir. Buradaki risk, boşta duran bir kabloya yetkisiz bir kullanıcının bilgisayarını bağlamasıdır. Kullanıcı bu sayede kablonun bağlı olduğu porta yani portun dahil olduğu VLAN'a erişim sağlayacaktır. Bu nedenle switchlerde alınması gereken ilk güvenlik önlemi kullanılmayan portların kapatılmasıdır. Genelde L2 switch portları varsayılanda açık gelir. Portları kapatmak için ilgili portun arayüzüne girilerek "**shutdown**" komutu kullanılıyor.

Port Security

Switchlerde MAC adres tablosu taşırılarak (MAC Address Flood) switchlerin HUB gibi çalışmasnı (switchlerden geçen framelerin bütün portlara anahtarlanması) sağlanıyor. Bu sayede saldırgan saldırı anından itibaren MAC adresi CAM tablosunda kayıtlı olmayan her istemcinin network trafiğini dinleyebiliyor. Bu saldırıya önlem olarak switchlerde Port Security özelliği kullanılıyor. Port Security özelliği sayesinde switchin bir portundan öğrenebileceği maksimum MAC adres sayısı sınırlandırılabiliyor. Burada saldırının bir istemci tarafından yapılması beklendiği için daha çok istemci bağlı portlarda sınırlama yapılıyor (Switcler arasında bağlantı için kullanılan portlardan çok fazla MAC adresi öğrenilebiliyor).

Port Security özelliğini portlarda açabilmek için port arayüzüne giriş yapılarak öncelikle "**switchport mode access**" komutuyla portun Access moduna alınması gerekiyor. Ardından "**switchport port-securtiy**" komutunun kullanılması yeterli. Bu komut sonrasında Port Security özelliği varsayılan ayarlarında devreye alınıyor (1 MAC adresi öğrenilebilir, kural ihlali yapılırsa port kapatılır). Özelleştirmek için;

```
SW1(config)#interface fastEthernet 0/1
SW1(config-if)#switchport port-security ?
  aging         Port-security aging commands
  mac-address   Secure mac address
  maximum       Max secure addresses
  violation     Security violation mode
  <cr>
SW1(config-if)#
```

- **Switchport port-security maximum**
  - Porttan öğrenilebilecek Maximum MAC adresi sayısı değiştirilebilir

```
SW1(config-if)#switchport port-security maximum ?
  <1-132>  Maximum addresses
SW1(config-if)#
```

- **Switchport port-security mac-address**
  - Porta bağlı tek cihaz varsa cihazın MAC adres bilgileri tanımlanarak porta farklı bir cihaz bağlandığında bloklanması sağlanabiliyor.
  - Portun öğrenebileceği Maximum MAC adres sayısı değiştirilerek birden fazla MAC adresi de manuel olarak tanımlanabilir.
- **Switchport port-security mac-address sticky**
  - Büyük networklerde her porta bağlanan cihazların MAC adreslerinin tek tek manuel olarak girmek yerine porta bağlanan cihazların MAC adresini otamatik olarak öğrenilmesini sağlayan komuttur. Bu özellik devreye alındığında öğrenilen MAC adresler kalıcı olarak kaydedilmemektedir. Öğrenilen MAC adreslerinin kalıcı olmasını sağlamak için cihazlar porta bağlandırktan sonra switchde "**write**" komutu

kullanılıyor (“**write**” komut sonrasında switch yeniden başlatıldığında öğrenilen MAC adresleri kullanılmaya devam edecektir).

- Mac-address komutuyla MAC adreslerinin bir kısmı manuel olarak girilebilirken bir kısmının da Sticky özelliğiyle otomatik öğrenilmesi sağlanabilir (Örnek olarak Maximum –> 5 tanımlandığında 2 MAC adresi manuel tanımlanıp kalan 3 adresin Sticky ile otomatik öğrenilmesi sağlanabilir)

```
SW1(config-if)#switchport port-security mac-address ?
  H.H.H    48 bit mac address
  sticky   Configure dynamic secure addresses as sticky
SW1(config-if)#
```

- **Swtitchport port-security aging time**
  - Porta bağlanan cihazın MAC adresinin dinamik olarak yenilenmesini sağlayan özelliktir. Sticky özelliğinde öğrenilen MAC adresleri sınıra ulaştığında yeni MAC adresi öğrenilemiyordu. Aging özelliğinde ise portta öğrenilen MAC adresleri istemci trafik oluşturmadığı durumlarda belirli aralıklarla MAC adresinin silinmesi sağlanarak porta bağlanacak farklı istemcilerin MAC adreslerinin yeniden öğrenilebilmesi sağlanıyor.
  - Bu özelliğe ek olarak “**switchport port-security aging type**” komutuyla MAC adreslerini silinme kriteri de belirlenebiliyor.
    - **Absolute**, öğrenilen MAC adresi için belirlenen süre tamamlandıktan sonra silinmesini sağlıyor.
    - **İnactivity**, öğrenilen MAC adresi belirtilen süre içerisinde trafik oluşturmamışsa siliniyor.

```
SW1(config-if)#switchport port-security aging time ?
  <1-1440>  Aging time in minutes. Enter a value between 1 and 1440
SW1(config-if)#
```

- **Switchport port-security violation**
  - Portlarda kural ihlali yapılması durumunda porta gerçekleştirilecek aksiyonu belirlemek için kullanılıyor.
    - **Shutdown**, port kapatılır ve kural ihlali loglanır. Portu tekrar devreye alabilmek için önce “**sh**” komutuyla port manuel olarak kapatılır. Ardından “**no sh**” komutuyla tekrar açılır.
    - **Restrict**, portta kural ihlali olduğunda port kapanmaz ama kural ihlali yapan istemci loglanır ve bloklanır.
    - **Protect**, portta kural ihlali yapıldığında port hizmet vermeye devam eder. Kural ihlali yapan istemci bloklanır ama loglanmaz.

```
SW1(config-if)#switchport port-security violation ?
  protect   Security violation protect mode
  restrict  Security violation restrict mode
  shutdown  Security violation shutdown mode
SW1(config-if)#
```

Protection fot VLAN Attacks

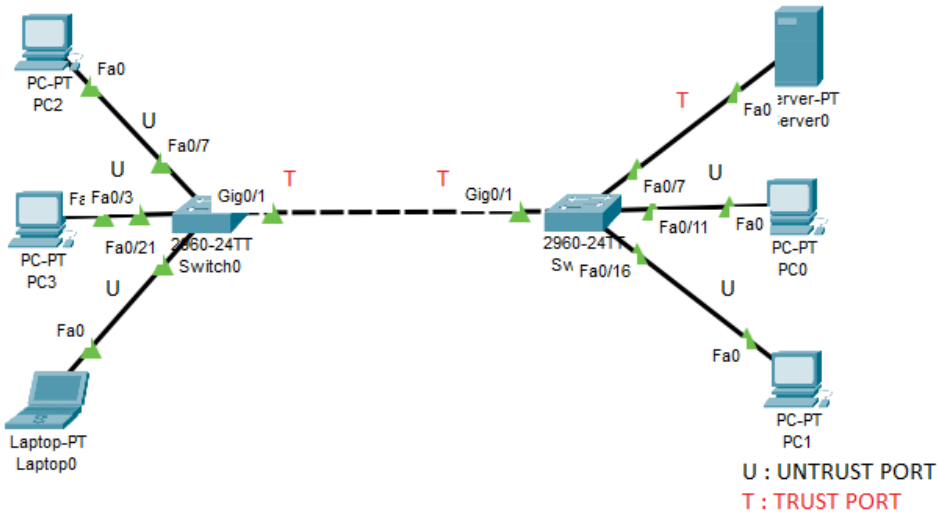
Switchlerde VLAN saldırılarına yönelik alınabilecek ilk önlem varsayılanda Cisco switchlerde portlar DTP modunda geliyor. DTP modu “**switchport nonegotiate**” komutuyla kapatılabilir. Bu çözüme ek olarak portlar Access moduna da alınabilir. Bunun için portların arayüzüne girilerek “**switchport mode access**” komutu kullanılmalı. Bu sayede saldırganların portu Trunk moduna çekerek VLAN trafiklerini izleyip müdahil olmasının önüne geçilmektedir.

VLAN Hoping saldıısına karşı önlem olarak Native VLAN, VLAN 1'den farklı bir VLAN'a alınmalı ve mümkünse kullanılmamalı (Bunu yaparken unutulmaması gereken kural; Native VLAN her switchde aynı olmak zorunda. Aksi taktirde VLAN'lar birbirine girecektir). Bu sayede saldırgan Native VLAN'ı dahil olamayacağı için (saldırıyı gerçekleştirebilmek için Native VLAN'a dahil olması gerekiyor) farklı VLAN'a frame gönderemeyecektir.

Protection fot DHCP Attacks

DHCP protokolüne yönelik saldırılar arasında DHCP Starvation ve Rouge DHCP Server saldırıları bulunuyordu. İlk olarak Rouge DHCP Server saldırısı için **DHCP Snooping** özelliği kullanılıyor. DHCP Snooping özelliği sayesinde switch portları "**Trust**" veya "**Untrust**" olarak tanımlanıyor. Trust tanımlanan portlarda, DHCP sunucularının oluşturabileceği DHCP paketlerine (DHCP OFFER, DHCP ACK - Sadece sunucu değil istemcilerin oluşturabileceği DHCP DİSCOVER, DHCP REQUEST paketlerine de izin veriyor) izin verilirken, Untrust tanımlanan portlarda, sadece istemcilerin oluşturabileceği DHCP paketlerine (DHCP DİSCOVER, DHCP REQUEST) izin veriliyor. Bu sayede Untrust tanımlanan portlarda saldırgan DHCP hizmeti veremiyor.

|→ Portlar Trust veya Untrust olarak tanımlanırken dikkat edilmesi gereken noktalardan biri DHCP sunucusu networkte farklı bir swtich üzerinde hizmet veriyor olabilir. DHCP sunucusunun farklı switche bağlı istemcilere de hizmet verebilmesi için switchler arasında kullanılan portların da Trust tanımlanması gerekiyor.



DHCP protokoüne yönelik gerçekleştirilen saldırılardan bir diğeri olan DHCP Starvation Attack saldırısına önlem olarak yine **DHCP Snooping** özelliği kullanılıyor. DHCP Snooping özelliği sadece portların Trust veya Untrust olarak tanımlanabilmesini sağlamıyor. Aynı zamanda DHCP sunucusunun istemcilere ip bilgisi verilirken switch üzerinde ek bir tablo tutarak (**Binding Tablosu**) bu tabloya istemcinin bağlı olduğu **port bilgisinin, MAC adresinin ve DHCP sunucusu tarafından kendisine verilen ip adresinin** kaydını tutuyor (Normalde DHCP Snooping özelliği açık olamdığında swirchler L2'de çalıştığı için ip kaydı tutmazlar). Switch istemciye verilen ip adresini DHCP sunucusundan istemciye gönderilen paketleri dinleyerek belirliyor.

DHCP Snooping konfigürasyonu için;

- Öncelikle global konfigürasyon modunda "**ip dhcp snooping**" komutu kullanılarak DHCP snooping özelliği açılıyor ama devreye alınmıyor.
- Özellik açıldıktan sonra Trust tanımlanması gereken portların arayüzlerine girilerek "**ip dhcp snooping trust**" komutu kullanılıyor.
- Trust portlar tanımlandıktan sonra istemci bağlı portlarda DHCP Starvation saldırısını önlemek için "**ip dhcp snooping limit rate <Limit Rate>**" komutuyla portlardan saniyede gönderebilecekleri DHCP DİSCOVER paketlerinin sayısı sınırlandırılıyor.
- DHCP Snooping özelliği için gereken tanımlamalar yapıldıktan sonra global konfigürasyon modunda "**ip dhcp snooping vlan <VLAN IDs>**" komutuyla hizmet verilecek VLAN'lar belirleniyor. Bu komut sonrasında DHCP Snooping özelliği devreye giriyor.
  |→ Burada dikkat edilmesi gereken nokta, hizmet verilecek VLAN'lar belirlendikten sonra DHCP Snooping özelliği Trust tanımlanmayan bütün portları Untrust belirleyerek hizmet vermeye başlıyor. Bu nedenle switchler arası bağlantıların ve DHCP sunucusunun bulunduğu portlar VLAN'lar belirlenmeden önce Trust olarak konfigüre edilmesi gerekiyor. Portlar Trust tanımlanmadan DHCP Snooping özelliği devreye alınırsa portlar Trust tanımlanana kadar istemciler DHCP hizmeti alamazlar.

```
SW1(config)#ip dhcp snooping
SW1(config)#interface gi 0/1
SW1(config-if)#ip dhcp snooping trust
SW1(config-if)#exit
SW1(config)#interface range fa 0/1-24
SW1(config-if-range)#ip dhcp snooping limit rate 10
SW1(config-if-range)#exit
SW1(config)#ip dhcp snooping vlan 1,2-5,10
SW1(config)#end
SW1#
```

Protection fot ARP Attacks

L2'de gerçekleştirilebilen bir başka saldırı ise ARP protokolüne yönelik gerçkeleştirilen ARP Poisining saldırısıdır. Bu saldırıya önlem olarak **DAI** (**Dynamic Arp Inspection**) özelliği kullanılıyor. DAI özelliği, DHCP Snooping özelliğinde istemcilerin MAC ve DHCP sunucusu tarafından veirlen ip adreslerinin tutulduğu **Binding tablosunu** temel alarak çalışır. Bu nedenle **DAI özelliği açıldığında DHCP Snooping özelliğinin devrede olması gerekiyor**.

DAI özelliği, networke bir ARP Request gönderildiğinde DAI özelliğiyle bu paketin içindeki ip ve MAC adreslerinin kaydını Binding tablosunda aranır. Aranan ip-MAC adres eşleniği Binding tablosunda bulunamazsa ARP paketi drop edilir. Bu sayede istemici herhangi bir MAC adresi öğrenemez, networkte erişimi engellenir.

|→ DAI özelliği kullanılırken dikkat edilmesi gereken noktalardan biri networkte yazıcı, ip telefon gibi statik ip adresi alan cihazlardır. Bu cihazlar DHCP sunucusundan ip adresi almadığı için Binding tablosunda istemcinin kaydı bulunmayacaktır. DAI özelliği Binding tablosunu temel alarak çalıştığı için istemcinin MAC ve ip adreslerini tabloda bulamayacağından istemcilerin ARP paketlerini drop edecektir. Bu nedenle statik ip adresi verilen istemcilerin bağlı olduğu portların arayüzlerine girilerek "**ip arp inspection trust**" komutuyla portlar DAI özelliği için Trust olarak tanımlanmılı veya Binding tablosuna bu bilgilerin manuel olarak girilmesi gerekmektedir.

|→ ARP Inspection özelliği için Trust tanımlanan portlarda ARP paketlerinin içeriğine bakılmazken, Untrust tanımlanan portlar için Binding tablosu göz önünde bulunduruluyor. İstemciler binding tablosundaki kayıtlı MAC-ip eşlemesi dışında farklı adreslerle ARP sorgusu yapamıyor. Bu sayede ARP Poisining saldırısının önüne geçilmiş oluyor.

Dynamic ARP Inspection konfigürasyonu için;

- İlk olarak "**ip dhcp snooping**" komutuyla DHCP Snooping özelliğinin açılması ve devreye alınmadan önce gereken tanımlamalar yapılır.
- DHCP Snooping özelliği "**ip dhcp snooping vlan <VLAN IDs>**" komutuyla devreye alınır.
- DAI özelliği için Trust tanımlanması gereken portların (statik ip verilen) arayüzlerine girilerek "**ip arp inspection trust**" komutu uygulanır.
- Son olarak da "**ip arp inspection vlan <VLAN IDs>**" komutuyla verilen VLAN'lar için DAI özelliği devreye alınıyor.

```
SW1(config)#ip dhcp snooping
SW1(config)#interface gi 0/1
SW1(config-if)#ip dhcp snooping trust
SW1(config-if)#exit
SW1(config)#ip dhcp snooping vlan 1
SW1(config)#interface fa 0/11
SW1(config-if)#ip arp inspection trust
SW1(config-if)#exit
SW1(config)#ip arp inspection vlan 1
SW1(config)#end
```

ARP Poisining saldırısına ek önlem olarak **IP Source Guard** özelliği de kullanılabiliyor. IP Source Guard, DAI özelliği gibi DHCP Snooping ile tutulan Binding tablosunu temel alarak çalışmaktadır ve paketlerdeki kaynak ip adresine göre filtreleme yapmaktadır (DAI'den farklı olarak her frame için kontrol ediyor). Bu koruma sayesinde ip çalınmasının ya da sunucudan habersiz istemcilerin komşu istemcilerdeki ip adreslerini alarak trafik oluşturmasının önüne geçilmektedir. IP Source Guard özelliğiyle binding tablosunda tanımlı ip adresi dışındaki adreslerle trafik oluşturulmasına izin verilmemektedir.

|→ Konfigürasyonu için öncelikle DHCP Snooping özelliği açılır. Ardından ilgili arayüze girilerek "**ip verify source**" komutuyla IPSG özelliği devreye alınır (https[:]//www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3.2_0_se/multibook/configuration_guide/b_consolidated_config_guide_3850_chapter_0110110.html#:~:text=IP%20Source%20Guard%20(IPSG)%20is,manually%20configured%20IP%20source%20bindings. - IPSG özelliğini devreye alma, binding tablosuna manuel kayıt ekleme ve çok daha fazlası için ...).

Protection fot STP Attacks

Switchlerde STP protokolünde BPDU paketleriyle manipülasyonlar yapılabiliyordu. Bu manipülasyonlara önlem olarak **BPDU Guard** özelliği kullanılıyor. BPDU Guard özelliğiyle, porta bir BPDU paketi gönderildiğinde port kapatılıyor. Bu sayede saldırgan içeriği değiştirilmiş BPDU paketleri gönderemiyor.

BPDU Guard konfigürasyonu için öncelikle port Access moduna alınmalıdır. İsteğe bağlı olarak portta "**spanning-tree portfast**" komutuyla STP protokolü devre dışı bırakılabilir. Son olarak "**spanning-tree bpduguard enable**" komutu kullanılarak BPDU Guard koruması devreye alınır.

|→ BPDU Guard koruması için portun PortFast moduna alınması şart değildir ama eğer ki porta bağlı uçtan BPDU paketi gönderilirse port kapanacaktır.

```
SW1(config)#interface fastEthernet 0/1
SW1(config-if)#switchport mode access
SW1(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.
SW1(config-if)#spanning-tree bpduguard enable
SW1(config-if)#exit
```

NOT:

- DHCP Starvation saldırısında saldırgan farklı MAC adreslerine sahip paketler göndererek ip talebinde bulunuyordu. Port Security özelliği kullanıp portun öğrenebileceği maximum MAC adres sayısını 1 yaparak bu saldırının önüne geçilemiyor. Nedeni, Port Securtiy özelliği L2'deki MAC adresini kontrol ediyordu. DHCP protokolü ise L7 protokolüdür ve DHCP sunucusu kendisine gelen paketin L7 içerisinde yazan MAC adresini dikkate alarak değerlendirir. Yani L2'de bulunan MAC adresini dikkate almaz çünkü merkezi bir DHCP sunucusuna DHCP Relay Agent özelliğiyle DHCP pketleri yönlendirilebiliyordu. Bu paketler routerlar arasında yönlendirilirken kaynak MAC adresleri değişiyor ve sunucuya varmadan önce geçtiği son routerun MAC adresini alıyordu. Bu durumda eğer ki DHCP sunucusu L2 MAC adresine bakarak ip bilgisi dağıtsaydı o zaman routerun vekillik yaptığı (Relay Agent özelliğiyle gelen oaketler) paketlere ip bilgiis veremeyecekti.
- DAI özelliği kullanılarak bir ARP paketlerinin geçerliliği kontrol ettirilebiliyor. Yani anlamlı-anlamsız ARP protokolünün kullanılmasının önüne geçilebiliyor. Bunun için "**ip arp inspection validate**" komutuyla kaynak/hedef MAC adresleri veya ip adresleri kontrol ettiriliyor. Bu sayede gereksiz ARP trafiğinin önüne geçiliyor. Konfigürasyon için "**ip arp inspection validate**" komutu devreye alınmak istenen switchlerde tek satırda tanımlanıyor.

```
SW1(config)#ip arp inspection validate ?
  dst-mac  Validate destination MAC address
  ip       Validate IP address
  src-mac  Validate source MAC address
SW1(config)#ip arp inspection validate dst-mac src-mac ip
```

- Switchlerde bütün portlarda Spanning-Tree protokolü devreye alınmak istendiğinde global konfigürasyon modunda "**spanning-tree portfast default**" komutu kullanılıyor. Ek olarak bütün portlarda PortFast ve PBDU Guard özelliği aynı anda devreye alınmak istendiğinde "**spanning-tree portfast bpduguard default**" komutu kullanılıyor.

```
SW1(config)#spanning-tree portfast bpduguard default
```

- Uygulamalarını "**Lab –> Çalışmalar -> LAN Security**" dizini altında bulabilirsin.

Kontrol Komutları :

- Sh port-security
- Sh ip dhcp snooping
- Sh ip dhcp snooping binding //hangi istemcinin hangi port- ip-MAC adresini aldığı görünür.