Switch Güvenliği ve Port Security Konfigürasyon Rehberi

Hazırlayan: Furkan Yaşar *LinkedIn*

Bu rehber, Cisco switch'lerde port security ve Layer 2 güvenlik konfigürasyonları için tüm detayları içermektedir.

1. Port Security Konfigürasyonu

KRİTİK BİLGİ: Port Security, MAC tablosu taşma saldırılarını ve yetkisiz erişimleri önlemenin en etkili yoludur.

Port Security Temel Konfigürasyonu

```
Switch(config)# interface fastethernet 0/1
Switch(config-if)# switchport mode access      # Portu access moda al (zorunlu)
Switch(config-if)# switchport port-security     # Port security'yi etkinleştir
Switch(config-if)# switchport port-security maximum 2 # İzin verilen maksimum MAC adresi sayısı
Switch(config-if)# switchport port-security mac-address sticky # MAC adreslerini otomatik öğren ve kaydet
```

Port Security İhlal Modları

Mod	Komut	Açıklama
Shutdown (Varsayılan)	**switchport port-security violation shutdown**	Portu error-disabled durumuna alır, LED'i kapatır ve syslog mesajı gönderir
Restrict	**switchport port-security violation restrict**	Bilinmeyen trafiği düşürür, syslog mesajı gönderir ve ihlal sayacını artırır
Protect	**switchport port-security violation protect**	Bilinmeyen trafiği sessizce düşürür, syslog mesajı göndermez (en az güvenli)

Errdisable Recovery Ayarları

```
Switch(config)# errdisable recovery cause psecure-violation
Switch(config)# errdisable recovery interval 300    # 5 dakika sonra otomatik açılır
```

Port Security Doğrulama Komutları

```
Switch# show port-security              # Tüm portların güvenlik durumu
Switch# show port-security interface fastethernet 0/1 # Belirli portun detayları
Switch# show port-security address         # Tüm güvenli MAC adresleri listele
Switch# show errdisable recovery         # Hangi ihlallerden sonra recovery aktif?
```

UYARI: Port security sadece access portlarda veya manuel olarak trunk moda alınmış portlarda çalışır. Dinamik trunk portlarda etkinleştirilemez.

2. VLAN Saldırılarını Önleme

KRİTİK TEHDİT: VLAN hopping saldırıları, saldırganın farklı VLAN'lara erişmesine ve hassas verilere ulaşmasına olanak sağlar.

VLAN Hopping Önleme Adımları

```
Switch(config)# interface range fastethernet 0/1 - 24
Switch(config-if-range)# switchport mode access  # Tüm kullanıcı portlarını access moda al
Switch(config-if-range)# exit

Switch(config)# interface range gigabitethernet 0/1 - 2
Switch(config-if-range)# switchport mode trunk    # Trunk portları manuel olarak trunk moda al
Switch(config-if-range)# switchport nonegotiate   # DTP (Dynamic Trunking Protocol) müzakerelerini devre dışı bırak
Switch(config-if-range)# switchport trunk native vlan 999 # Native VLAN'ı varsayılan (VLAN 1) dışına ayarla
Switch(config)# no dtp run                # Global DTP devre dışı bırak
```

Kullanılmayan Portların Güvenliği

```
Switch(config)# interface range fastethernet 0/20 - 24
Switch(config-if-range)# shutdown            # Kullanılmayan portları kapat
Switch(config-if-range)# switchport access vlan 999 # Kullanılmayan bir VLAN'a ata
```

> **ÖNEMLİ:** Native VLAN'ın VLAN 1 olmaması, çift etiketleme (double-tagging) saldırılarını önlemeye yardımcı olur.

3. DHCP Saldırılarını Önleme

> **TEHDİT ANALİZİ:** DHCP Starvation ve Spoofing saldırıları, ağdaki istemcilere yanlış IP konfigürasyonu sağlayarak Man-in-the-Middle saldırılarına zemin hazırlar.

> **DHCP Attack Review:** Starvation: Sahte DHCP discovery paketleriyle havuzdaki IP'leri tüketerek DoS oluşturur. Spoofing: Rogue DHCP sunucu ile istemcilere yanlış gateway, DNS veya IP bilgisi atar.

DHCP Snooping Konfigürasyonu

```
Switch(config)# ip dhcp snooping           # DHCP Snooping'i global olarak etkinleştir
Switch(config)# ip dhcp snooping vlan 10,20,30 # Belirli VLAN'lar için etkinleştir

Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# ip dhcp snooping trust    # DHCP sunucuya bağlı portu trusted olarak işaretle

Switch(config)# interface range fastethernet 0/1 - 24
Switch(config-if-range)# ip dhcp snooping limit rate 5 # Untrusted portlarda DHCP paket hızını sınırla
```

Doğrulama Komutları

```
Switch# show ip dhcp snooping             # DHCP Snooping ayarlarını göster
Switch# show ip dhcp snooping binding      # Öğrenilmiş DHCP bağlamalarını listele
Switch# show ip dhcp snooping statistics     # Rate-limit istatistiklerini göster
```

> **KURUMSAL GÜVENLİK:** DHCP Snooping, Dynamic ARP Inspection (DAI) için zorunlu bir önkoşuldur. DAI etkinleştirmeden önce mutlaka DHCP Snooping konfigüre edilmelidir.

4. ARP Saldırılarını Önleme

> **YAYGIN SALDIRI:** ARP Spoofing/Poisoning saldırıları, saldırganın kendisini varsayılan ağ geçidi gibi göstererek tüm trafiği ele geçirmesine olanak sağlar.

Dynamic ARP Inspection (DAI) Konfigürasyonu

> **DAI Implementation Guidelines:**
>
> - Global DHCP Snooping'i etkinleştir
> - Hedef VLAN'larda DHCP Snooping'i aç
> - Hedef VLAN'larda DAI'yi etkinleştir
> - Access portları untrusted, uplink/router portları trusted olarak işaretle

```
Switch(config)# ip dhcp snooping           # Önkoşul: DHCP Snooping
Switch(config)# ip arp inspection vlan 10,20  # DAI'yi belirli VLAN'lar için etkinleştir

Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# ip arp inspection trust   # Router bağlantılı portu trusted olarak işaretle

Switch(config)# ip arp inspection validate src-mac dst-mac ip # Ek doğrulamalar etkinleştir
```

IP Source Guard Konfigürasyonu

```
Switch(config)# ip verify source      # Untrusted portlarda IP spoofing'i engelle
Switch(config)# ip source binding <MAC> vlan <VLAN> interface <TYPE/NUM> # Statik IPSG kaydı
```

Doğrulama Komutları (DAI)

```
Switch# show ip arp inspection         # DAI durumu göster
Switch# show ip arp inspection statistics  # İstatistikleri görüntüle
```

5. STP Saldırılarını Önleme

> **TOPOLOJİ DEĞİŞİKLİĞİ:** STP manipülasyon saldırıları, saldırganın root bridge olmasını sağlayarak tüm ağ trafiğini ele geçirmesine olanak tanır.

PortFast ve BPDU Guard Konfigürasyonu

```
Switch(config)# spanning-tree portfast default # Tüm access portlarda PortFast etkinleştir
Switch(config)# spanning-tree portfast bpduguard default # Tüm access portlarda BPDU Guard etkinleştir

Switch(config)# interface fastethernet 0/1
Switch(config-if)# spanning-tree bpduguard enable # Port bazında BPDU Guard etkinleştir
Switch(config-if)# spanning-tree guard root     # Root Guard etkinleştir
```

Doğrulama Komutları

```
Switch# show spanning-tree summary        # STP özet durumunu göster
Switch# show spanning-tree interface fastethernet 0/1 detail # Port detaylarını göster
```

6. Access Control (AAA ve 802.1X)

AAA (Authentication, Authorization, Accounting)

```
Switch(config)# aaa new-model            # AAA modelini etkinleştir
Switch(config)# username admin secret Str0ngP@ss # Lokal kullanıcı oluştur
Switch(config)# aaa authentication login default local # Varsayılan login metodunu lokal olarak ayarla
Switch(config)# aaa authorization exec default group radius local # Exec authorization
Switch(config)# aaa accounting exec default start-stop group radius # Exec accounting
Switch(config)# aaa accounting commands 15 default start-stop local # Komut accounting
```

RADIUS/TACACS+ Server Ayarları

```
Switch(config)# radius-server host 10.0.0.5 auth-port 1812 key Cisco123
Switch(config)# tacacs-server host 10.0.0.6 key TacacsKey
```

802.1X Port Tabanlı Kimlik Doğrulama

```
Switch(config)# dot1x system-auth-control  # 802.1X kontrolünü etkinleştir
Switch(config)# interface range fastethernet 0/1-24
Switch(config-if-range)# dot1x port-control auto # Portlarda 802.1X otomatik modunu etkinleştir
```

7. Layer 2 Güvenlik Tehditleri

Yaygın Layer 2 Saldırıları ve Önleme Yöntemleri

Saldırı Türü	Örnekler	Önleme Yöntemi
MAC Tablosu Saldırıları	MAC adresi taşırma (flooding)	Port Security
VLAN Saldırıları	VLAN hopping, çift etiketleme	DTP devre dışı bırakma, Native VLAN değiştirme
DHCP Saldırıları	DHCP Starvation, Spoofing	DHCP Snooping
ARP Saldırıları	ARP Spoofing, Poisoning	Dynamic ARP Inspection (DAI)
Adres Taklit Saldırıları	MAC/IP adresi taklidi	IP Source Guard
STP Saldırıları	Root bridge taklidi	BPDU Guard, Root Guard
CDP/LLDP Keşif Saldırıları	Ağ topolojisi keşfi	CDP/LLDP devre dışı bırakma

> **Detay:** MAC Flooding saldırılarında switch, "unknown unicast" moduna geçerek tüm trafiği flood'lar. Port Security ile belirlenen MAC sınırları bu saldırıyı önler.

Yönetim Protokolleri ve Management Plane Koruması

> **ÖNERİ:** Yönetim erişimi için her zaman SSH, SCP, SFTP veya SSL/TLS gibi güvenli protokoller kullanın. Out-of-band yönetim ağı ve dedicated management VLAN oluşturun, erişimi ACL ile filtreleyin.

```
Switch(config)# ip domain-name ornek.com
Switch(config)# crypto key generate rsa modulus 2048
Switch(config)# ip ssh version 2
Switch(config-line)# transport input ssh
Switch(config)# access-list 10 permit 192.168.0.0 0.0.0.255
Switch(config)# interface vlan 99
Switch(config-if)# ip address 192.168.0.2 255.255.255.0
Switch(config-if)# ip access-group 10 in
```

SON GÜVENLİK ÖNERİSİ: Layer 2 güvenliği için port security, DHCP snooping, dynamic ARP inspection ve BPDU guard konfigürasyonları bir bütün olarak uygulanmalıdır. Tek başına hiçbir önlem tam koruma sağlamaz.