

## Layer 2 Güvenlik Yöntemleri(Bölüm1)

### SAFA Kısıqçılar / İTÜ'BİDB 2010

Pekçok güvenlik ve network yöneticisi sistemlerinin güvenliğini sağlayabilmek için gelebilecek tehditleri üst katmanlara kadar taşımaktansa, olabildiğince alt katmanda yapılacak gerekli yapılandırma veya kısıtlamalarla çözüm arayışına gitmektedirler. Gelelim yönetilebilir bir switch'i sahada kullanmaya başlamadan önce bu cihaz üzerinde uygulanması gereken güvenlik aşamalarına. Öncelikle network'e dahil edilecek her cihazda olması gerektiği gibi, cihazın şifreleri belirlenmelidir. Bu şifreler belirlenirken, herkes tarafından kolayca tahmin edilebilen ya da herhangi bir sözlük atakla kolaylıkla tespit edilebilen bir şifre vermemeye özen gösterilmelidir. Birden fazla switch ve network yöneticisinin bulunduğu yerlerde, en iyi yöntem AAA Authentication modu aktive edilerek, bunun üzerinde kullanıcıların sorgularının yapılacağı yerel kullanıcı veritabanı, TACACS+ ya da RADIUS sunucu üzerinden kimlik doğrulaması yapılmasıdır. TACACS+ bunlar arasında ayrıntılı log tutma özelliğiyle diğerlerinden bir adım önde olarak gözükse ihtiyaca göre kullanılacak yöntem de değişebilmektedir.

#### 1) SSH erişimini aktive etme ve kimlik doğrulama yöntemi

Ayrıca, yine cihazı yönetebilmek için, cihazın performans ve yüküne göre ssh ya da telnet erişimleri aktif edilmelidir. Tercih daima kriptolu olan ssh bağlantısı olması gerekir fakat yine de belirlenecek güvenlik seviyesine göre telnet erişimi de tercih edilebilmektedir.

Cisco IOS üzerinde Örnek SSH Yapılandırması	
Komut	Açıklama
username <i>deneme</i> privilege 15 password 0 <i>deneme-şifre</i>	Kullanıcı eklenir ve şifre atanır.
aaa new-model	Yerel veritabanı kullanılarak,AAA modu ayarlamaları yapılır.
aaa authentication login default local	
aaa authorization exec default local	
aaa authorization network default local	
aaa session-id common	

ip domain name <b>Agciyiz.com</b>	Alan adı belirlenir.
crypto key generate rsa	Sertifika oluşturulur.(en az 768 bit Diffie-Hellman key kullanılır)
line vty 0 4	İlgili vty belirlenir.
transport input ssh	Yalnızca SSH bağlantılarına izin verilir.

### Cisco Catalyst OS Üzerinde Örnek SSH Yapılandırması

Komut	Açıklama
set crypto key rsa 1024	1024 bit RSA key oluşturur.
set ip permit 10.0.0.0 255.255.255.0 ssh	Belirlenen ip aralığıdaki SSH bağlantılarına izin verilir.
set ip enable	

## 2)VTP ve SNMP yapılandırması

Kullanıcı sayısı ve bunun paralelinde cihaz sayısı yüksek networklerde VLAN yapılandırmasının network'ü rahatlatan ve düzeni sağlayan bir işlevi olsa da, düzgün konfigüre edilmeyen bir VLAN yapılandırması çok ciddi güvenlik açıklarına neden olmaktadır.Bu konuda yapılabilecek en iyi düzenleme ise,, switch üzerinde oluşturulan vlan veritabanının paylaşımını gerekli etki alanı altında, belirlenen şifreyle sadece ilgili cihazlara aktarılmasını sağlamaktır. Ayrıca VTP pruning özelliğiyle de switchler arasında akan broadcast trafiği sadece ilgili cihazlara yönelerek, cihazın üzerinden gereksiz trafiğin geçmesini engelleyecektir.

### Cisco IOS Üzerinde Örnek VTP Konfigürasyonu

Komut	Açıklama
vtp domain <b>VTP-Adı</b>	VTP adı belirlenir

vtp password <b>VTP-Şifresi</b>	VTP şifresi belirlenir.
vtp pruning	VTP pruning aktive edilir.
<b>Cisco Catalyst OS Üzerinde Örnek VTP Konfigürasyonu</b>	
<b>Komut</b>	<b>Açıklama</b>
set vtp domain <b>VTP-Adı</b>	VTP adı belirlenir
set vtp passwd <b>VTP-Şifresi</b>	VTP şifresi belirlenir.
set vtp pruning enable	VTP pruning aktive edilir.

Bunun yanına cihazın üzerinden anlık bilgileri okuyabilmek gibi pek çok farklı şekilde kullanılan SNMP'nin ayarlamaları da en düzgün şekilde belirlenmelidir. Cihaz üzerine gelen SNMP sorgularının kontrolü sağlanmadığı sürece, SNMP kullanılarak yapılabilen farklı uygulamalarla cihaz kolaylıkla ele geçirilebilir. SNMP versiyonları arasında da en güvenli sürümü v3 sürümüdür. Bu sürümde v1 ve v2 de kullanılan topluluk belirleme ve kullanıcı işlemleri gibi işlemlere ek olarak şifreleme gibi özellikler eklenmiştir.

<b>Cisco IOS Üzerinde Örnek SNMP Konfigürasyonu</b>	
<b>Komut</b>	<b>Açıklama</b>
snmp-server community <b>Read-Only- Sorgusu</b> ro 10	ACL 10 ile korunan read-only SNMP sorgusu belirlenir.
snmp-server community <b>Read-Write-Sorgusu</b> rw 11	ACL 11 ile korunan read-write SNMP sorgusu belirlenir.
access-list 10 permit <b>IP-adresi-ro_için</b>	Read-only SNMP sorgusunun yapılabileceği ip(ler) belirlenir.
access-list 11 permit <b>IP-adresi-rw_için</b>	Read-write SNMP sorgusunun yapılabileceği ip(ler) belirlenir.

<b>Cisco Catalyst OS Üzerinde Örnek SNMP Konfigürasyonu</b>	
<b>Komut</b>	<b>Açıklama</b>
set snmp community read-only read-only-string	read-only sorgu belirlenir.
set snmp community read-write read-write-string	read-write sorgu belirlenir.
set snmp community read-write-all rwo-string	read-write-all sorgu belirlenir.

### 3) Port kısıtlamaları ve tanımlamaları

Cihaz üzerinde gerekmedikçe trunk port bırakılmamalıdır. Hatta, switch üzerinde kullanılmayan bir vlan oluşturularak, tüm kullanılmayan portlar bu vlan'e atanmalıdır. Ayrıca yine kullanılmayan portlar gerek duyulmadıkça "shutdown" durumunda bırakılmalıdır ve "description PORTUN-AÇIKLAMASI" komutuyla kullanılan her porta olası bir hata tespit durumunda sonuca daha çabuk ulaştırabilecek tanımlamalar yapılmalıdır. Son olarak bu konuda dikkat edilmesi gereken en önemli nokta ise, vlan yapılandırmasında pek çok konuda (native vlan) portlara varsayılan olarak atanan VLAN 1, gerekmedikçe kullanılmamalıdır.

<b>Cisco IOS Üzerinde Temel Port Örnek Kısıtlamaları</b>	
<b>Komut</b>	<b>Açıklama</b>
int range FastEthernet0/1 - 48	interface 1 – 48 arasına komut girilebilecek interface moda girilir
switchport access vlan 8	Portu VLAN 8'e atar.
switchport mode access	Portu access moda çeker.
Shutdown	Portu kapatır.

### 4.) Allowed-Vlan belirleme

Trunk olarak belirlenen portlar dahil, üzerinden tüm vlanlerin geçmesine izin verilmeyip, sadece o porttan akması gereken vlan trafiklerine izin verilmelidir.

<b>Cisco IOS Üzerinde Örnek VLAN Trunking Kısıtlamaları</b>	
<b>Komut</b>	<b>Açıklama</b>
interface GigabitEthernet0/1	Kısıtlama yapılacak interfacenin içine girilir.
switchport mode trunk	Port trunk moda ayarlanır.
Switchport trunk encapsulation dot1q	Encapsulation türü belirlenir.
switchport trunk allow 10-14, 26-28	10-14 ve 26-28 arası vlanlere izin verilir.