

## 2.AĞ CİHAZ GÜVENLİĞİ

### 2.1.Güvenli Cihaz Erişimi

Ağdan dışarı çıkan veya içeri giren trafiğin güvenliği ağ güvenliği açısından önemlidir. Kenar routerlar ağı dış ağlara bağladıkları için güvenlikte ilk adım olarak çok önemlidir.

Cihaz güvenliği ağ güvenliği sağlarken kritik bir görevdir. Bu kapsamda routerların fiziksel güvenliği ve onlara yönetsel erişiminin güvence altına alınması gerekir.

#### 2.1.1.Kenar Router Güvenliği

Erişim yetkisi olmayan bir personelin omuz sörfü yapması ihtimaline dikkat edilmelidir. Omuz sörfü ile basitçe erişim yetkileri elde edilir.

Saldırgan routera erişim hakkı elde ederse ağ içinde bulunan diğer cihazlar ve sunucular da risk altındadır.

Kenar router iç ağ ile güvenilmez dış ağ arasındaki son cihazdır. Kurumun tüm internet trafiği bu cihaz üzerinden geçer. Bu yüzden bu nokta ilk veya son savunma noktasıdır. Aynı zamanda güvenlik ilkelerinin uygulanabileceği noktadır.

##### 2.1.1.2

Kenar router kullanımı kurumun büyüklüğü ve karmaşıklığına göre üç farklı şekilde uygulanabilir:

Tek router (single router) yaklaşımı

Bu yaklaşımda tek bir router iç ağı dış ağa veya internete bağlar. Tüm güvenlik politikaları bu cihaz üzerine uygulanır. Bu küçük işletmeler ve şube ofisler için yaygın olarak kullanılan yöntemdir.

Derinlemesine Savunma (Defense-in-depth) yaklaşımı

Tek router yaklaşımına göre daha güvenli bir yöntemdir. Kenar router ilk savunma hattını oluşturur ve ekranlama routerı olarak da isimlendirilir. Tüm trafik iç ağdaki firewall üzerinden geçirilir. İkinci savunma hattı firewalldur. Kenar routerın geçirdiklerini yakalar ve ekstra filtre uygular.

DMZ yaklaşımı

Derinlemesine savunma yönteminin bir çeşididir ve bir ara nokta oluşturur. Bu ara noktaya DMZ denir. DMZ internetten veya dış ağdan erişilebilirdir. DMZ korunaklı bir ağa bağlayan bir router ile korunaksız bir ağa bağlayan diğer routerın arasına kurulur. Alternatif olarak tek routera ilave port olarak da uygulanabilir. Örneğin ağdaki bir web sunucuya dış ağdan http trafiklerinin gelebilmesi gerekir.

##### 2.1.1.3

Cihazların fiziksel güvenliklerinin de sağlanması gerekir. Bunun için:

- Routerlar ve diğer cihazlar kapısı kilitli odalarda bulunmalı ve sadece yetkili personel bu odalara girebilmeli, odanın elektostatik ve manyetik yalıtımı olmalı, yangın söndürme sistemi olmalı ve nem sıcaklıkları kontrol edilebilmelidir
- Kesintisiz güç kaynağı (UPS) olmalı ve bu sayede cihazların elektrik kesintileri ile DoS atağına maruz kalması engellenmelidir

Router Sıkılaştırma

Kullanılmayan portlar ve servisler kötü kullanıma karşı kapatılmalıdır:

- Güvenli yönetsel erişim sağlanmalı ve sadece yetkili personelin kendi yetkileri seviyesinde erişimlerine izin verilmelidir.

- Kullanılmayan port ve interfaceler kapatılmalıdır. Bu cihaza erişimi azaltır.
- Kullanılmayan servisler devre dışı bırakılmalıdır.

#### İşletim Sistemi Güvenliği

İşletim sistemi şu güvenlik özelliklerini sağlamalıdır:

- Router mümkün olan en yüksek bellek miktarı ile konfigüre edilmelidir. Bu durum DoS saldırısı durumunda belleğin boğulmasını engeller.
- İşletim sisteminin kararlı çalışan son sürümü kullanılmalıdır.
- Router IOS'unun ve konfigürasyon dosyalarının bir kopyasını saklamalıdır.

##### 2.1.1.4

Yetkisiz bir kişi routera yönetimsel erişim sağlarsa parametrelerini değiştirebilir, fonksiyonlarını devre dışı bırakabilir veya diğer ağ cihazlarını keşfedip onlara erişim kazanabilir.

Güvenli yönetimsel arayüz erişimi şu özelliklere sahip olmalıdır:

- Sınırlı cihaz erişimi: Erişim portları sınırlanmalı, haberleşme portlarına sınırlı izin verilmeli ve erişim yöntemleri sınırlanmalıdır.
- Tüm erişimlerin logu ve hesap bilgileri tutulmalı: Bir kimse eriştiğinde veya eriştiği zaman denetim amacıyla loglanmalıdır.
- Erişim hesabı: Sadece yetkili kullanıcı veya gruplara lara izin verildiğinden emin olunmalı başarısız giriş sayısı ve belirli zaman aralığındaki giriş sayısı sınırlanmalıdır.
- Eylemleri yetkilendirme: Herhangi bir kullanıcı, grup veya hizmet tarafından izin verilen eylemler kısıtlanmalıdır.
- Yasal bildirim görüntüleme: İnteraktif oturumlarda yasal bir bilgilendirme görüntülenmelidir.
- Veri gizliliğini sağlamak: Hassas veriler görüntülenme ve kopyalanmaya karşı korunmalıdır. Koklama, oturum çalma ve man-in-the-middle (MITM) saldırıları için iletişim kanalı güvenli tutulmalıdır.

##### 2.1.1.5

Yönetimsel amaçlı olarak bir cihaza erişmenin iki yolu vardır. Yerel veya uzak erişim.

#### Yerel erişim

Cihazın arayüzlerine yerel ağdan erişilir. Yerel erişim için router konsol portuna bir bilgisayar doğrudan bağlamak gerekir.

#### Uzak erişim

Cihazlara uzaktan erişmek gerekebilir. Bunun için telnet, SSH, http https veya SNMP protokollerinden biri ile bağlanılabilir. Bilgisayar router ile aynı veya farklı ağda bulunabilir. Bazı uzak erişim protokolleri kullanıcı adı ve şifreyi clear text olarak gönderebilir. Bir saldırgan ağ trafiğini yakalarsa şifreyi ve konfigürasyon bilgilerini elde edebilir.

Bu yüzden ya lokal erişim yapılmalı ya da uzak erişim yapmak gerekiyorsa bazı tedbirler alınmalı:

- Yönetici bilgisayarı ile router arasındaki trafik kriptolanmalı. Bunun için telnet yerine SSH, http yerine https kullanılmalı.
- Adanmış bir yönetim ağı kurulmalı. Yönetim ağı sadece yönetici bilgisayarı ile yönetim interfacelerini içermeli.

- Sadece yönetici bilgisayarlarının belirli protokollerle router interfacelerine erişimi için paket filtreleme yapılmalı. Örneğin sadece yöneticinin IP adresinden SSH protokolü ile bağlantı kurmaya izin verilmeli.

Bu tedbirler önemlidir ancak tümüyle ağı güvenli hale getirmez. Bunun yanında diğer yöntemler de uygulanmalıdır. Mesela karmaşık şifre kullanmak gibi.

### 2.1.2.Güvenli Yönetimsel Erişim Konfigürasyonu

Saldırganlar yönetim şifresini ele geçirmek için çok değişik yöntemler uygularlar. Omuz sörfü, kişisel bilgilerden şifre tahmini, clear text paketleri koklama gibi. Veya şifre kırma araçları ve programları kullanabilirler.

Router ve switch gibi donanımları korumak için güçlü şifreler seçilmelidir. Aşağıdaki tavsiyelere uyulursa kırma programları ve insanların zor tahmin edecekleri şifreler kullanılabilir:

- Şifre 10 karakter veya daha uzun olmalıdır.
- Şifreler büyük harf, küçük harf, sayılar, özel karakterler ve boşluk karakteri içermelidir.
- Şifrede tekrarlardan kaçınılmalı, sözlükteki kelimeler, sayı dizileri, kullanıcı adı, akraba adlarıbiyografik bilgiler (doğum tarihi, kimlik no, ana baba adları gibi) veya diğer tahmin edilebilir bilgiler kullanılmamalıdır.
- Kelimelere yakın karakterler içeren kelimelerden kaçınılmalıdır. Örneğin Smith kullanıcısı Smyth, 5mYth gibi kelimeler kullanmamalıdır.
- Sık sık şifre değiştirilmelidir.
- Şifre kağıda yazılıp ortada bırakılmamalıdır.

#### 2.1.2.2

Bir çok erişim portu Cisco'da şifre isteyebilir. Konsol, aux, telnet portları gibi. Şifre yönetimi TACACS+ veya RADIUS üzerinden yapılmalıdır. Tüm routerlar user ve privileged exec mod şifresine sahi olmalıdır.

#### Enable Secret şifresi

*Enable secret* global config komutu privileged exec modu şifreler.

#### Console Şifresi

Varsayılan olarak konsol şifre gerektirmez. Ancak şifre atanmalıdır. *line console 0* komutu ve devamında *login* ve *password* komutları ile şifre atanmalıdır.

#### Virtual Terminal (Telnet) şifresi

Varsayılan olarak cisco routerlar 5 eşzamanlı terminal oturumunu (telnet veya SSH) destekler. *Line vty 0 4* ve devamında *login* ve *password* komutlarıyla atama yapılır.

```
R1(config)# line console 0
R1(config-line)# password csc5io
R1(config-line)# login
```

```
R1(config)# line vty 0 4
R1(config-line)# password csc5io
R1(config-line)# login
```

```
R1(config)# line aux 0
R1(config-line)# password csc5io
R1(config-line)# login
```

```
R1(config)# enable secret csc5io
```

Enable secret haricindeki komutlar varsayılan olarak şifreleri konfigürasyon dosyasında clear text olarak saklar.

#### 2.1.2.3

Şifre güvenliği için birkaç yöntem kullanılabilir:

Minimum şifre uzunluğuna zorlama

Kullanılmayan bağlantıları kapatma

Konfig dosyasındaki tüm şifreleri kriptolayarak atama

16 karakter uzunluğunda şifre kullanmaya zorlamak için

*Security passwords min-length karakter\_sayısı*

Komutu kullanılmalıdır.

Kullanılmayan bağlantılar sonlandırılmalıdır. *Exec-timeout* ile kullanılmayan bağlantılar sonlandırılır.

*Service password-encryption* komutu ile tüm şifre bilgileri kriptolanabilir.

```
router(config-line)#
```

```
exec-timeout minutes [seconds]
```

Parameter	Description
<i>minutes</i>	This integer specifies the number of idle minutes before the session is timed out.
<i>seconds</i>	(Optional) This integer specifies the additional time interval in seconds.

#### 2.1.2.4

Bir diğer güvenlik özelliği kimliklendirmedir. Cisco routerlar için iki yöntem vardır.

username name password password

username name secret password

Username secret komutu daha güvenlidir. MD5 hashing ile şifreyi kriptolar. MD5, service password-encryption ile yapılan tip 7 güvenlikten daha iyidir. Username şifre kombinasyonunun erişim esnasında sorulması için *login local* komutu ile aktif edilmelidir.

```
router(config)#
```

```
username name secret {[0] password | 5 encrypted-secret}
```

Parameter	Description
<i>name</i>	This parameter specifies the username.
<b>0</b>	(Optional) This option indicates that the plaintext password is to be hashed by the router using MD5.
<i>password</i>	This parameter is the plaintext password to be hashed using MD5.
<b>5</b>	This parameter indicates that the encrypted-secret password was hashed using MD5.
<i>encrypted-secret</i>	This parameter is the MD5 encrypted-secret password that is stored as the encrypted user password.

#### Örnek komut uygulaması

```
R1(config)# service password-encryption
R1(config)# username JR-ADMIN password letmein
% Password too short - must be at least 10 characters. Password
configuration failed
R1(config)# username JR-ADMIN password cisco12345
R1(config)# username ADMIN secret cisco54321
R1(config)# line con 0
R1(config-line)# login local
```

```
R1# show run | include username
username JR-ADMIN password 7 060506324F41584B564347
username ADMIN secret 5 $1$G3oQ$heVsd5iz76WJUSJvtzs8I0
R1#
```

#### 2.1.3.Telnet Erişimi için Artırılmış Güvenlik

Şifre atama ve local erişim DoS ataklarını engellemez. Cihaza çok fazla sayıda istek göndererek DoS saldırısı yapılabilir. Binlerce kullanıcı adı-şifre çifti ile erişim elde edilmeye çalışılınca cihaz hizmet dışı kalır. Bunu engellemek için belirli bir zaman aralığında gelecek erişim isteği sayısı sınırlandırılmalıdır. Bu ise ACL ile yapılabilir.

Sözlük ataklarını ve DoS ataklarını durdurmak için şu parametrelerle login işlemi konfigüre edilmelidir:

Ardarda login girişimleri arasında gecikme

DoS atağı şüphesi varsa login kapatma

Login algılandığında sistem loglaması

Bu iyileştirmeler konsol erişiminde uygulanmaz. Konsoldan sadece yetkili kullanıcının fiziksel erişimi olduğu varsayılır.

#### 2.1.3.2

Şu komutlarla iyileştirme yapılır:

Router# configure terminal

Router(config)# login block-for *seconds* attempts *tries* within *seconds*

Router(config)# login quiet-mode access-class {*acl-name* | *acl-number*}

Router(config)# login delay *seconds*

Router(config)# login on-failure log [every login]

Router(config)# login on-success log [every login]

```

R1(config)# login block-for 15 attempts 5 within 60
R1(config)# ip access-list standard PERMIT-ADMIN
R1(config-std-nacl)# remark Permit only Administrative hosts
R1(config-std-nacl)# permit 192.168.10.10
R1(config-std-nacl)# permit 192.168.11.10
R1(config-std-nacl)# exit
R1(config)# login quiet-mode access-class PERMIT-ADMIN
R1(config)# login delay 10
R1(config)# login on-success log
R1(config)# login on-failure log
R1(config)#

```

#### 2.1.3.3

Varsayılan olarak tüm login iyileştirme işlemleri devre dışıdır. Login block-for komutu devreye alır. İki modda bu işlemler yürütülür:

- Normal mod (izleme modu): Router belli bir zaman dilimindeki başarısız login girişimlerini sayar.
- Sessiz mode: Başarısız login girişimi sayısı belli bir eşik değeri aşarsa tüm login girişleri yasaklanır.

Sessiz mod aktif edildiğinde geçerli yönetici girişleri de dahil olmak üzere tüm girişler yasaklanır. Ancak kritik hostlardan erişim her zaman izinlidir. Bu işlem ACL ile yapılır. ACL *login quiet-mode access-class* komutu ile oluşturulmalıdır.

#### 2.1.3.4

Auto secure komutu başarısız girişimleri loglar. Başarılı girişler varsayılan olarak loglanmaz.

Bu komutlar başarılı ve başarısız girişimleri izlemeye yardımcı olur.

login on-failure log [every login] Başarısız login girişimlerini loglar.

login on-success log [every login] Başarılı login girişimlerini loglar.

security authentication failure rate threshold-rate log komutu başarısız login sayısı eşik değeri aştığında log üretir.

```

R1(config)# login on-success log [every login]
R1(config)# login on-failure log [every login]
R1(config)# exit
or
R1(config)# security authentication failure rate 10 threshold-rate log

```

#### 2.1.3.5

Anlık olarak kullanıcılara yasal bildirimde bulunmak için banner mesajları verilir.

banner {exec | incoming | login | motd | slip-ppp} d message d

```

R1(config)# banner {exec | incoming | login | motd | slip-ppp} d message d

```

#### 2.1.4.SSH Konfigürasyonu

Bir routera SSH yapılandırmadan evvel şu dört adımın uygulanması gerekir:

Adım 1. Routerın SSH destekleyen bir IOS sürümüne sahip olması gerekir.

Adım 2. Her bir routerın tekil hostname'i olması gerekir

Adım 3. Routerın doğru domain adını kullanması gerekir

Adım 4. Router'ın kullanıcı adı ve parola çiftinin kimlik doğrulaması için yerel kimlik doğrulama veya AAA servislerini kullanmalıdır.

#### 2.1.4.2

CLI kullanarak, SSH yapılandırma işlemi şu dört adımla gerçekleştirilir:

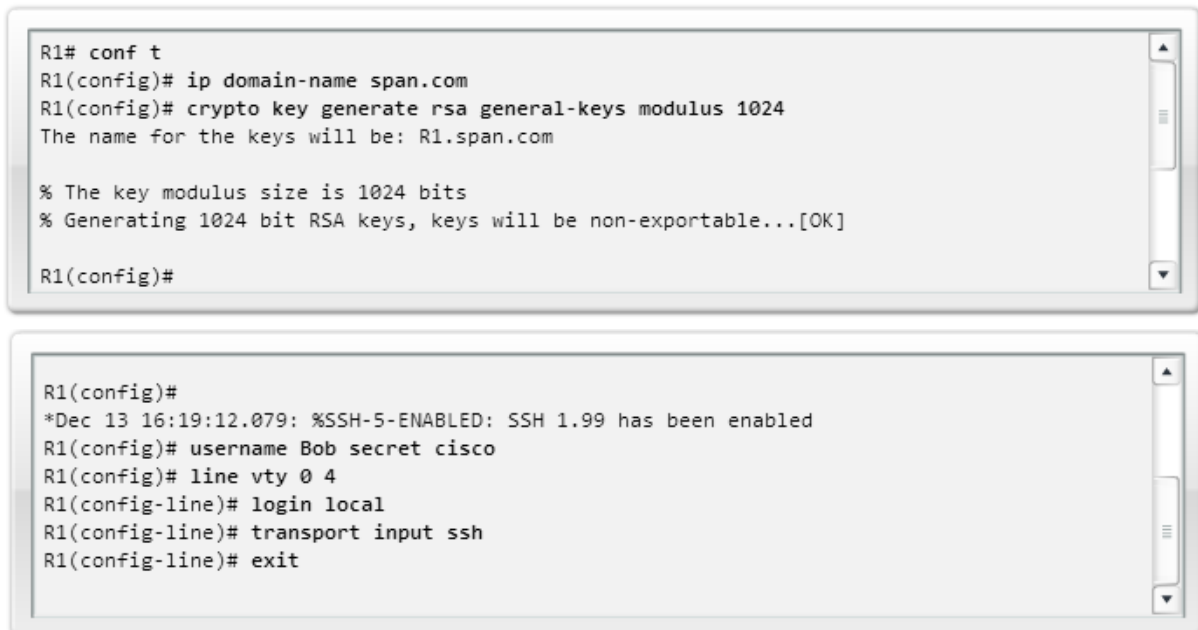
Adım 1. *ip domain-name domain-name* komutu ile domain adı yapılandırılır

Adım 2. Routerın SSH trafiğini kriptolaması için tek yön secret key oluşturulur. RSA anahtarı oluşturmak için, *crypto key generate rsa general-keys modulus modulus-size* komutu kullanılır.

Adım 3. Geçerli bir yerel kullanıcı bilgisinin veritabanında olduğundan emin olunur. Yoksa username name secret secret komutu ile oluşturulur.

Adım 4. Telnet erişiminde SSH girişi aktif edilir. login local ve transport input ssh komutları ile.

SSH'in çalıştığını doğrulamak ve üretilen kripto anahtarını görüntülemek için show crypto key mypubkey rsa komutu kullanılır.



```
R1# conf t
R1(config)# ip domain-name span.com
R1(config)# crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R1.span.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R1(config)#

R1(config)#
*Dec 13 16:19:12.079: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)# username Bob secret cisco
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# exit
```

#### 2.1.4.3

Diğer SSH komutları

Opsiyonel olarak kullanılacak SSH komutları:

- SSH version
- SSH timeout period
- Number of authentication retries

#### 2.1.4.4

SSH çalıştıran bir routera iki şekilde bağlanılabilir:

Ya enable moddaki ssh komutu kullanarak Router-Router bağlantısı yapılabilir

Ya da PuTTY, OpenSSH veya TeraTerm gibi bir yazılım kullanarak host-router bağlantısı

#### 2.1.4.5

CCP (Cisco Configuration Professional) yazılımı ile router üzerindeki SSH deamen'ı yapılandırılabilir. RSA keyi üretilebilir.

## 2.2. Yönetimsel Rollerin Atanması

### 2.2.1.Yetki Seviyelerinin Konfigürasyonu

Yetki seviyeleri konfigürasyonu ağ güvenliğini korumanın sonraki adımıdır. Yetki seviyeleri hangi kullanıcıların cihazlar üzerinde hangi işleri yapabilmek için izni olduğunu tanımlar.

Cisco IOS üzerinde User Exec mod (yetki seviyesi 1) ve Privileged Exec mod ( yetki seviyesi 7) olmak üzere iki seviyeye sahiptir.

IOS üzerinde kontrollü erişim için

- Privilege level (yetki seviyeli)
- Role-based CLI (rol tabanlı)

Olmak üzere iki yöntem vardır.

#### Yetki seviyeleri

- Level 0:
  - Ön tanımlı kullanıcı seviyesi erişim yetkileri
  - Seyrek kullanılır ancak şu beş komutu içerir: disable, enable, exit, help, and logout
- Level 1(User EXEC mode):
  - Login için varsayılan seviyedir. Promptu Router>.
  - Kullanıcı bu yetki seviyesinde konfigürasyon değişikliği yapamaz ve çalışan konfigürasyonu görüntüleyemez
- Levels 2 –14:
  - Kullanıcı seviyesinde yetkiler özelleştirilebilir
  - Alt seviyedeki komutlar üst seviyeler veya üst seviyelerdeki komutlar alt seviyelere taşınabilir
- Level 15 (Privileged EXEC mode):
  - Enable mode yetkileri için reserve edilmiştir (enable komutu).
  - Kullanıcılar konfigürasyon değişikliği yapabilirler ve değişiklikleri kaydedebilirler



router (config) #

**privilege** *mode* {**level** *level* *command* | **reset** *command*}

Command	Description
<i>mode</i>	This command argument specifies the configuration mode. Use the <b>privilege ?</b> command to see a list of router modes.
<b>level</b>	(Optional) This command enables setting a privilege level with a specified command.
<i>level command</i>	(Optional) This parameter is the privilege level that is associated with a command. You can specify up to 16 privilege levels, using numbers 0 to 15.
<b>reset</b>	(Optional) This command resets the privilege level of a command.
<i>command</i>	(Optional) This is the command argument to use when you want to reset the privilege level.

Farklı seviyelere şifre atamak için iki yöntem vardır:

- Yetki seviyeleri için, **enable secret level password** global configuration mode komutu
- Bir kullanıcıya özel bir yetki seviyesi atamak için, **username name privilege level secret password** global configuration mode komutu kullanılır

```
R1# conf t
R1(config)# username USER privilege 1 secret cisco
R1(config)#
R1(config)# privilege exec level 5 ping
R1(config)# enable secret level 5 cisco5
R1(config)# username SUPPORT privilege 5 secret cisco5
R1(config)#
R1(config)# privilege exec level 10 reload
R1(config)# enable secret level 10 cisco10
R1(config)# username JR-ADMIN privilege 10 secret cisco10
R1(config)#
R1(config)# username ADMIN privilege 15 secret cisco123
R1(config)#
```

- Seviye 10 ve **reload** adlı EXEC mode komutunu çalıştırma yetkisi veren komut JR-ADMIN kullanıcısı için aşağıdaki komut dizisi ile yapılabilir:
  - **privilege exec level 10 reload**
  - **enable secret level 10 cisco10**
  - **username JR-ADMIN privilege 10 secret cisco10**
- Oluşturulan yetki seviyesine erişmek için **enable level** komutu user modda iken yazılır ve şifre girilir

```
R1# enable 15
Password: <cisco123>
R1# show privilege
Current privilege level is 15
R1# show running-config
Building configuration...

Current configuration : 1145 bytes
!
version 12.4

<Output omitted>
```

### 2.2.2.Rol Tabanlı CLI erişimi

Yeni versiyon IOS'lar daha spesifik roller için daha kontrollü erişim sunar.

CLI komutları tarafından tanımlanmış cihaz geliştirilmiş güvenliği özel kullanıcılar tarafından kullanılabilir

Yetkisiz kullanıcıların istenmeyen kullanımı engellenmiş olur

Kullanıcılar sadece CLI komutlarını görebilirler ve erişim izni olanlara erişebilirler

Rol Tabanlı Görüntüleme

- **Root view:**
  - Sistemin görüntülenmesi yapılandırılabilir, administrator root view'da olmak zorundadır.
  - Seviye 15 erişim yetkisine sahip kullanıcıların hepsi aynı erişim haklarına sahiptir.
  - Sadece root view kullanıcısı yeni bir view oluşturup ona komut ekleyip çıkarabilir
- **CLI view**
  - Özel bir komut seti bu görünüm için özelleştirilebilir
- **Superview**
  - Bir veya daha fazla CLI görünümü içerebilir. Yöneticiler hangi komutların Kabul edilebilir olduğunu ve hangi konfigürasyon bilgilerinin görüntülenebilir olduğunu ayarlayabilirler.

## 2.3.Cihazları Yönetme ve Görüntüleme

### 2.3.1.IOS İmaj ve Konfigürasyon Dosyalarının Güvenliği

IOS imajını güvenli hale getirmek için **secure boot-image** komutu kullanılır

Router konfigürasyon dosyasının yedeğini almak ve güvenli biçimde saklamak için **secure boot-config** global configuration mod komutu kullanılır.

#### Birincil Bootset İmajı Geri Alma

Güvenli dosyalar **dir** komutu çıktısında listelenmez. Bunun için **show secure bootset** komutu ile yedek arşivi doğrulanır.

Birincil bir bootsetinin arşivden alınıp geri yüklenmesi için şu adımlar uygulanır:

**Adım 1.** Router **reload** komutu ile yeniden başlatılır.

**Adım 2.** ROMmon modunda, **dir** komutu ile güvenli bootseti görüntülenir. CLI'den **show secure bootset** komutu kullanılarak cihaz adını içeren dosya bulunabilir.

**Adım 3.** **boot** komutu ile router 2. Adımda bulunan dosya adı ile boot edilir.

**Step 4.** Global configuration moda girilir.

**Step 5.** **secure boot-config restore filename** komutu kullanılarak bulunmuş olan dosya parameter olarak uygulanır.

### Router Şifresini Geri Alma

Unutulan Router Şifresini Geri almak için şu prosedür uygulanır

- Konsol porttan bağlanılır
- Configuration register ayarları kaydedilir
- Router Power düğmesi ile başlatılır.
- Break tuşuna basılır ve ROMMON moduna erişilir.
- **confreg 0x2142** komutu yazılarak register ayarı değiştirilir.
- **reset** komutu ile router yeniden başlatılır.
- Başlangıç konfigürasyon dosyası atlanarak router açılır.
- privileged EXEC moda girilir.
- startup configuration , running configuration üzerine kopyalanır.
- running configuration dosyası show komutu ile görüntülenir.
- Global configuration moda girilip **enable secret password** komutu ile şifre değiştirilir.
- Kapalı interfaceler yeniden açılır.
- configuration register ayarları **config-register 0x2102** komutu ile yeniden eski haline getirilir
- Değişiklikler kaydedilip yeniden başlatılır.

### Şifre Geri Almayı Devre Dışı Bırakma

Yönetici isterse güvenlik riskini azaltmak için **no service password-recovery** global configuration mod komutu ile bu işlemi devre dışı bırakabilir

```
R1 (config)# no service password-recovery
WARNING:
Executing this command will disable password recovery
mechanism.
Do not execute this command without another plan for
password recovery.
Are you sure you want to continue? [yes/no]: yes
R1 (config)#
```

**no service password-recovery** komutunu devre dışı bırakıp yeniden şifre almayı etkinleştirmek için :

**Adım1.** Router açılırken imaj dosyasının decompress işlemi esnasında ilk beş saniye içinde break tuşuna basılır

**Step 2.** Break tuşu algılandıktan sonrastartup config dosyası silinerek şifre geri alma yeniden aktif edilir

### 2.3.2.Güvenli Yönetim ve Raporlama

Güvenli yönetim ve log görüntüleme için şu kriterler göz önünde bulundurulur:

- En önemli loglar nelerdir?
- Önemli log mesajları ile rutin bilgilendirme mesajları nasıl ayırdedilebilir?
- Logların sıkıştırılması nasıl engellenebilir?

- Zaman damgası eşleşmelerinden nasıl emin olunur?
- Kriminal inceleme için hangi log bilgileri gereklidir?
- Log mesajlarının büyüklüğü sizi ne kadar ilgilendiriyor?
- Cihazların tümü nasıl yönetilebilir?
- Ataklar ve network arızaları olduğunda nasıl izleyebiliriz?

### İç ve Dış Ağdan Görüntüleme

Loglama ve Log bilgilerinin görüntüleyen host ile ağ cihazları arasında gidiş gelişi iki yoldan olabilir:

- **In-band** - Bilgi akışı normal veri kanalı kullanılarak bir kurum ağında, internette veya her ikisinde gerçekleşebilir
  - Sadece yönetilen veya görüntülenen cihaza uygulanır
  - Mümkünse Ipsec, SSL veya SSH kullanılır
  - Cihaz gerektiği her zaman bilgi akışında bulunur
- **Out-of-band (OOB)** - Bilgi atanmış bir yönetim ağı üzerinden akar ve bu ağda normal ağ trafiği bulunmaz
  - Daha güvenli bir mekanizma sunar

### 2.3.3.Ağ Güvenliği için SysLog Kullanımı

Syslog loglama servisi üç ana göreve sahiptir:

- Log bilgilerini toplama, görüntüleme ve arıza bulma işlemi yapabilir
- Yakalanan loglama bilgilerinin türünü seçebilir
- Yakalanan mesajların hedeflerini özelleştirebilir

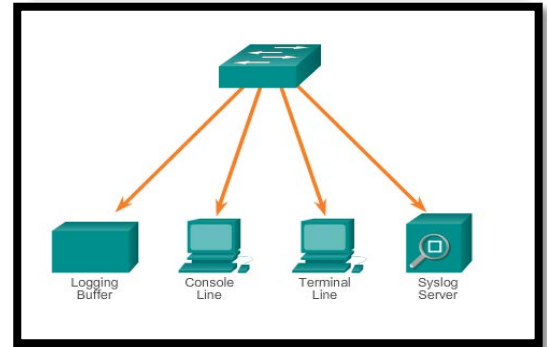
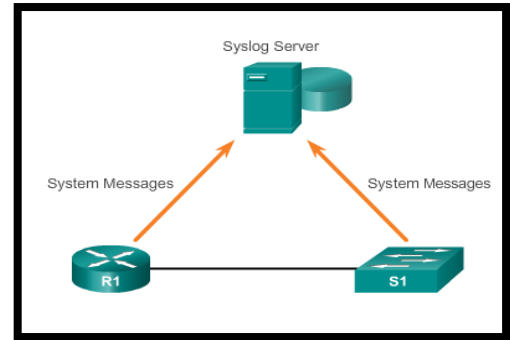
#### Syslog İşlemleri

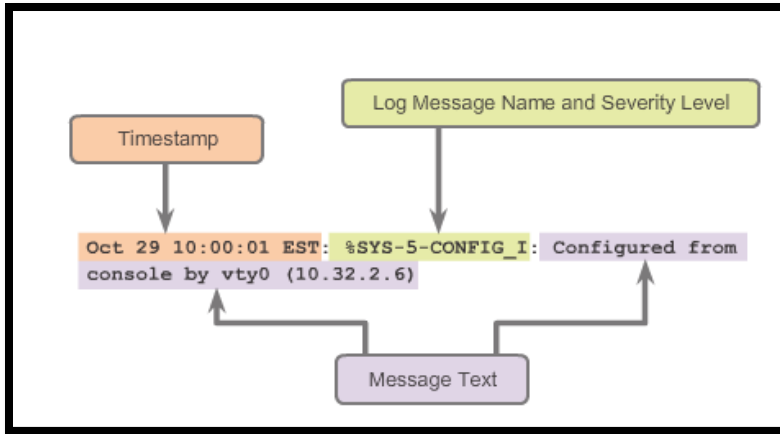
Router konfigürasyon değişikliklerini, ACL ihlallerini, interface durumlarını ve diğer bir çok önemli olayın bilgilerini loglayabilir.

Router syslog mesajlarını yandaki şekildeki yerlere göndermek üzere konfigüre edilebilir.

Cihazlar network olayları sonucu syslog mesajları üretir.

	Level	Keyword	Description	Definition
Highest Level	0	emergencies	System is unusable	LOG_EMERG
	1	alerts	Immediate action is needed	LOG_ALERT
	2	critical	Critical conditions exist	LOG_CRIT
	3	errors	Error conditions exist	LOG_ERR
	4	warnings	Warning conditions exist	LOG_WARNING
	5	notifications	Normal but significant condition	LOG_NOTICE
	6	informational	Informational messages only	LOG_INFO
Lowest Level	7	debugging	Debugging messages	LOG_DEBUG



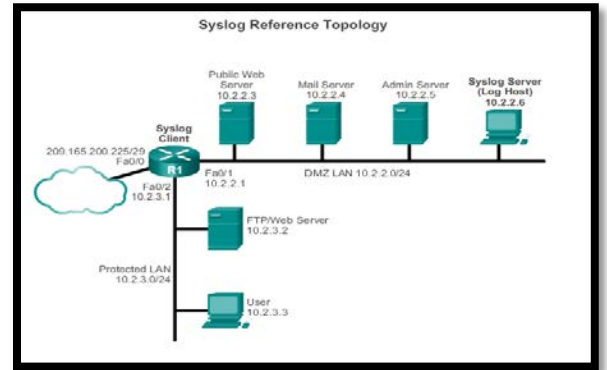


## Seviye 5 Syslog Mesajları

## Syslog Sistemleri

Syslog uygulayabilmek için syslog server ve client'a ihtiyaç duyulur:

- **Syslog server** – Aynı zamanda log bilgisayarı olarak da bilinir. Syslog clientından gelen log mesajlarını kabul eder, kaydeder ve işler. these systems accept and process log messages from syslog clients.
- **Syslog client** – Router veya mesaj üreten diğer cihazlardır. Ürettikleri mesajı syslog clienta gönderirler.



## Sistem Loglarını Yapılandırma

**Adım 1. logging host** komutu ile hedef syslog sunucusu ayarlanır.

**Step 2. logging trap level** komutu ile logların seviyesi ayarlanır (opsiyonel)

**Step 3. logging source-interface** komutu ile source interface ayarlanır. Bu komut IPv4 veya IPv6 adresi içeren paketi n hangi interfaceden çıkacağını belirler

**Step 4. logging on** komutu ile login işlemi aktif edilir. Giriş işlemi **logging buffered**, **logging monitor** ve **logging global** configuration mod komutları ile aktif veya pasif yapılabilir. Ancak **logging con** komutu desabel yapılırsa log gönderme işlemi yapılmaz sadece konsolda loglar görüntülenebilir.

## Sistem Loglarını CCP ile Yapılandırma

**Adım 1.** Cisco Configuration Professional menu çubuğunda **Configure > Router > Logging** seçilir

**Adım 2.** Logging diyalog penceresinde **Edit** seçilir.

**Adım 3.** **Enable Logging Level** check box tıklanır ve **Logging Level** drop-down list elemanı içinden loglama seviyesi seçilir.

**Adım 4.** **Add** seçilir ve loglanacak hostun IP adresi **IP Address/Hostname** alana yazılır.

**Adım 5.** OK düğmesi seçilip Logging dialog box'a dönülür.

**Adım 6.** OK düğmesi ile değişiklikler onaylanıp çıkılır.

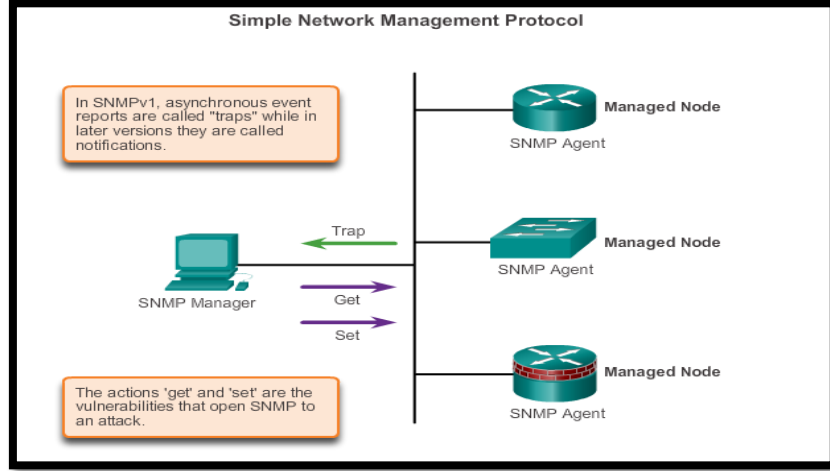
#### 2.3.4.Ağ Güvenliği için SNMP Kullanma

##### SNMP

Bir diğer yaygın kullanılan görüntüleme sistemi SNMP'dir. SNMP network cihazları arasında yönetim bilgilerinin iletimine imkan sağlayan bir uygulama katmanı protokolüdür. 1, 2 ve 3 olmak üzere üç versiyonu vardır.

SNMP sistemleri üç bileşenden oluşur:

- SNMP yöneticisi
- SNMP ajanı (yönetilen düğüm)
- Yönetim Bilgi Tabanı -Management Information Base (MIB)

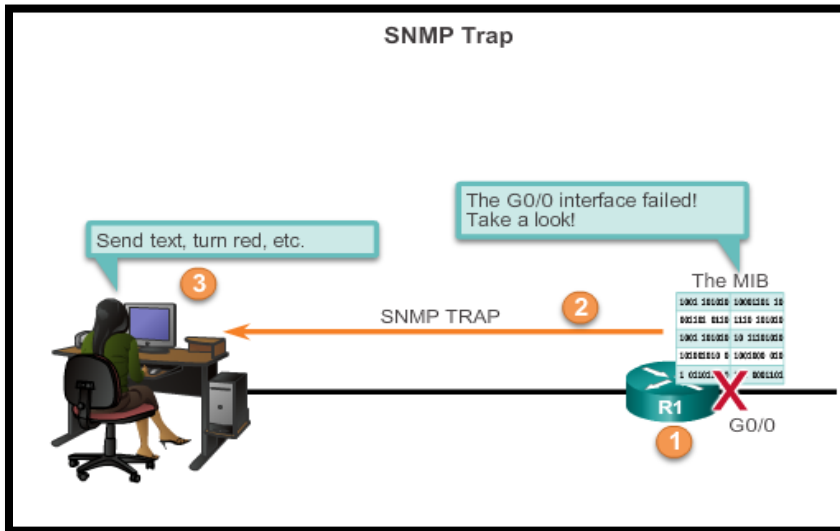


##### SNMP İşlemleri

- SNMP ajanı yönetilen cihaz tarafında bulunur ve ondan gelen bilgileri toplayıp depolar.
- Bu bilgiler ajan tarafından yerel olarak MIB'de depolanır.
- SNMP yöneticisi SNMP ajanını kullanarak MIB'deki bilgilere erişir.

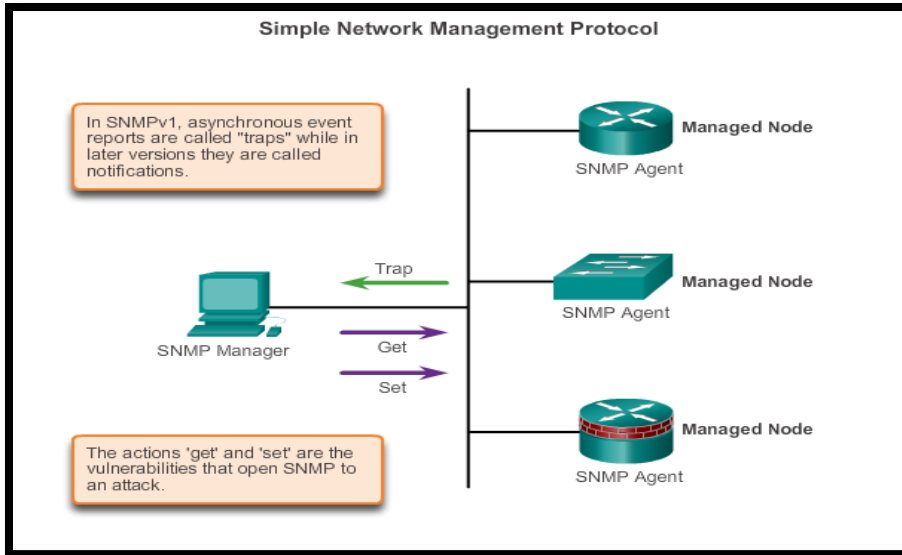
##### SNMP Ajan İşlemleri

- SNMP ajanları NMS'leri bilgilendirmek için trap mesajları üretip gönderebilir.
- Trap mesajları ağdaki bir durum ya da olayla ilgili SNMP yöneticisini uyanan mesajlardır.



##### SNMP Güvenlik Açıkları

SNMP mesaj alma ve gönderme işlemleri güvenlik açıklarına yol açabilir.



- **SNMP Topluluk Stringleri** Community stringleri yönetim istasyonu ile SNMPv1 ve SNMPv2 motoru arasında kimliklendirme için kullanılır.
- Read-write community stringleri bir ajana bilgi ve istek gönderebilir.

İki tip community stringi var:

- **Read-only community strings** - MIB'deki tüm nesnelere read-only erişim sağlar, community stringleri hariç.
- **Read-write community strings** - MIB'deki tüm nesnelere read-only erişim sağlar, community stringleri hariç.

### SNMPv3

SNMPv3 şu güvenlik özelliklerine sahiptir:

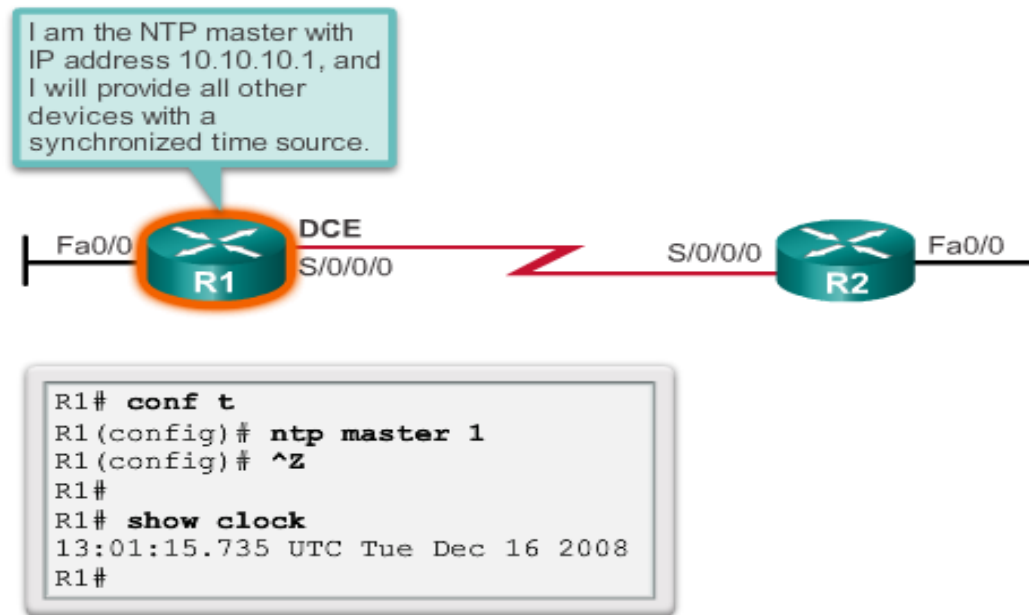
- **Mesaj bütünlüğü ve kimlik doğrulama** - Mesajın bir tuzak mesajı olmadığından ve geçerli bir kaynaktan geldiğinden emin olur.
- **Kriptolama** - Paket içeriğini karmaşıktırarak yetkisiz kaynaklar tarafından anlaşılmasını engeller.
- **Erişim Kontrolü** - Belirli veri kısımları üzerinde belli eylemleri kısıtlar

### 2.3.5.NTP Kullanımı

#### Network Time Protocol

- Routerın tarih ve saatini ayarlamak için şu yöntemlerden biri kullanılır:
  - Manuel olarak ayarlama
  - Network Time Protocol (NTP) ile konfigüre etmek
- NTP bir networkte zaman senkronizasyonu yapar, UDP protokolünü kullanır.

- NTP, genel olarak zaman bilgisini bir radio clock veya atomic clock gibi bir otorite zaman sunucusundan alır.
  - NTP bu bilgileri tüm ağa dağıtır.
  - NTP pakentin iki cihaz arasında 1ms zaman içinde mükemmel senkronizasyonunu sağlayabilir
- NTP servisleri varsayılan olarak tüm interfacede aktiftir. Bir interfacede devre dışı bırakmak için **ntp disable** komutu interface configuration modda yazılır.
- NTP ayarlanmış bir ağda bir veya daha fazla router master clock cihazı olarak ayarlanır. Bu aynı zamanda NTP master olarak da adlandırılır. Bunun için **ntp master** global configuration mod komutu kullanılır.
- NTP istemcileri master ile bağlantı kurarlar veya masterdan gelen mesajları dinlerler. Master ile senkronize olabilmek için **ntp server ip-address** komutu kullanılır.
- Bir LAN'da, NTP IP broadcast mesajları yerine **ntp broadcast client** interface configuration mod komutu ile aktif edilir.



## NTP Authentication

Üç güvenlik mekanizması kullanılabilir:

- ACL-based restriction şema
- Kriptolu kimlik doğrulama NTP version 3 veya daha sonraki versiyonlar tarafından sağlanır

NTP version 3 veya yenisi tavsiye edilir. Şu komutlarla yapılandırılır, NTP master ve NTP client için:

- **ntp authenticate ntp authentication-key key-number**



- **md5** *key-value*
- **ntp trusted-key** *key-number*

Üç güvenlik mekanizması kullanılabilir:

- ACL-based restriction şema
- Kriptolu kimlik doğrulama NTP version 3 veya daha sonraki versiyonlar tarafından sağlanır

NTP version 3 veya yenisi tavsiye edilir. Şu komutlarla yapılandırılır, NTP master ve NTP client için:

- **ntp authenticate ntp authentication-key** *key-number*
- **md5** *key-value*
- **ntp trusted-key** *key-number*

## 2.4. Otomatik Güvenlik Özellikleri Kullanımı

### 2.4.1. Bir Güvenlik Denetimi Uygulama

#### Cisco Discovery Protocol

CDP, Ağdaki cihazları keşfeden bir protokoldür.

- The Cisco Discovery Protocol (CDP) varsayılan olarak routerlarda aktiftir.
- CDP ağ yöneticilerinin ağ keşfedip arızayı kolay bulmasını sağlar.
- Bir saldırgan CDP'yi kullanarak local ağ keşfedebilmesini sağlar.
- CDP'yi kullanan yazılımlar yardımıyla kolayca network görüntülenebilir.
- Güvenlik gerekçelerinden dolayı CDP dikkatli kullanılmalıdır.
- Kenar cihazlarda CDP devre dışı bırakılması tavsiye edilir.

#### Protocol ve Servislerin Varsayılan Ayarları

Aşağıdaki bileşenlerin devre dışı bırakılması ve kısıtlanması cihazların güvenli kalmasına yardımcı olur:

- Gereksiz servis ve interfaceler.
- Yaygın olarak kullanılan yönetim servisler, SNMP gibi.
- Araştırma ve tarama servisleri, ICMP gibi. Terminal erişimi güvenliğinden emin olunmalıdır.
- Address Resolution Protocol (ARP)
- IP-directed broadcast.

### 2.4.2. AutoSecure ile Router Güvenliği

## Cisco AutoSecure

Cisco AutoSecure özelliği CLI'den başlatılır ve bir script çalıştırır. Güvenlik açıklarını gidermek için öneriler sunar ve routerin güvenlik konfigürasyonlarını yapar.

```
R1# auto secure
--- AutoSecure Configuration ---

*** AutoSecure configuration enhances the security
of the router but it will not make router
absolutely secure from all security attacks ***

All the configuration done as part of AutoSecure
will be shown here. For more details of why and
how this configuration is useful, and any possible
side effects, please refer to Cisco documentation of
AutoSecure.

At any prompt you may enter '?' for help.
Use ctrl-c to abort this session at any prompt.

Gathering information about the router for
AutoSecure

Is this router connected to internet? [no]:yes
```

**auto secure** komutu AutoSecure özelliklerini kurmaya başlar. Bu işlem interactive veya non-interactive olabilir.

- Interactive modda (varsayılan yöntem budur), router güvenlik özelliklerini aktif veya pasif etmeyle ilgili prompt görüntüler.
- Interactive olmayan modda varsayılan ayarlarla güvenlik özellikleri uygulanır. Bu mod için **auto secure no-interact** komutu çalıştırılır.