Contents

[GİRİŞ 1](#_Toc457766211)

[SWITCH SIKILAŞTIRILMASI 2](#_Toc457766212)

[1. Güncel switch yazılımının kullanılması 2](#_Toc457766213)

[2. Banner ekleme 2](#_Toc457766214)

[3. Konsol parolasının oluşturulması 2](#_Toc457766215)

[4. Uzaktan erişim parolasının oluşturulması 2](#_Toc457766216)

[5. “Enable secret” parolasının oluşturulması 2](#_Toc457766217)

[6. Parolaları şifreli olarak tutma 2](#_Toc457766218)

[7. Default vlan dışında bir vlan oluşturma 3](#_Toc457766219)

[8. Kullanılmayan portları kapama 3](#_Toc457766220)

[9. Uzaktan bağlantı için ssh servisini aktif etme 3](#_Toc457766221)

[10. Port güvenliği kurallarını uygulama 3](#_Toc457766222)

[11. Auto-trunking işlemini iptal etme 4](#_Toc457766223)

[12. Log tutma işlemini aktif etme 4](#_Toc457766224)

[13. Zaman aşımı süresini aktif etme 4](#_Toc457766225)

[ROUTER SIKILAŞTIRILMASI 5](#_Toc457766226)

[1. Güncel router yazılımının kullanılması 5](#_Toc457766227)

[2. Banner ekleme 5](#_Toc457766228)

[3. Konsol parolasının oluşturulması 5](#_Toc457766229)

[4. Uzaktan erişim parolasının oluşturulması 5](#_Toc457766230)

[5. “Enable secret” parolasının oluşturulması 5](#_Toc457766231)

[6. Parolaları şifreli olarak tutma 5](#_Toc457766232)

[7. Uzaktan bağlantı için ssh servisini aktif etme 6](#_Toc457766233)

[8. Log tutma işlemini aktif etme 6](#_Toc457766234)

[9. NTP protokolünü aktif etme 6](#_Toc457766235)

[10. Zaman aşımı süresini aktif etme 6](#_Toc457766236)

[Ağ Cihazları Sıkılaştırmalarının Kontrol Edilmesi 8](#_Toc457766237)

[Referanslar 9](#_Toc457766238)

# GİRİŞ

Bilgi güvenliği günümüzdeki en önemli konulardan birisidir. Bilgi güvenliği konusunda en büyük problemler genellikle son kullanıcı tarafında olmaktadır. Bu problemlerin en aza indirilmesi için olabilecek tehditlerin son kullanıcılara gelmeden minimize edilmesi gerekmektedir. Bu tehditlerin minimize edileceği yerler de aktif ağ cihazlarıdır. Switch ve router olan bu aktif ağ cihazlarının güvenli konfigürasyonu ile cihazlar sıkılaştırılacak ve iletişim güvenli hale getirilecektir. Bu dokümanda ağ cihazlarından önce switch sıkılaştırılması ve denetimi, daha sonra da router sıkılaştırılması ve denetimi anlatılacaktır.

Bu dokümanda kullanıcıların temel switch ve router konfigürasyonlarını yapabildiği ön koşul olarak kabul edilmiştir.

# SWITCH SIKILAŞTIRILMASI

## Güncel switch yazılımının kullanılması

Network yöneticisi düzenli aralıklarla yazılımları kontrol etmeli ve yeni bir güncelleme geldiği zaman tüm cihazlara yazılımı yüklemelidir. Bu süreç düzenli takip edilmesi ve mutlaka yapılması gereken bir adımdır. Ancak güncel yazılımın yüklenme işlemi bu raporun içerdiği konulardan birisi değildir.

## Banner ekleme

Cihaza konsol veya uzaktan erişim olması halinde kullanıcıyı uyaran bir mesaj eklenmelidir. Bu mesaj cihazın sadece yetkili kişiler tarafından yönetilebileceği uyarısını içermelidir. Bu işlem için gerekli komut:

**Switch(config): banner motd # Authorized Access Only! #**

“Authorized Access Only!” yazan kısma ağ yöneticisi istediği bir uyarıyı koyabilir. Bu sadece bir örnektir.

## Konsol parolasının oluşturulması

Yetkisiz kişilerin cihazın yakınına gelip konsol bağlantısı ile cihaza erişememesi için, cihaza erişimin ilk aşamasında bir parola oluşturulmalıdır. Bu işlem için gerekli komut:

**Switch(config): line console 0**

**Switch(config-line): password** *password*

**Switch(config-line): login**

Kullanıcı password yazan yere kendi belirlediği bir parolayı koymalıdır.

## Uzaktan erişim parolasının oluşturulması

Yetkisiz kişilerin ağa bağlanıp, uzaktan erişiminin engellenmesi için, cihaza erişimin ilk aşamasında bir parola oluşturulmalıdır. Bu işlem için gerekli komut:

**Switch(config): line vty 0 4**

**Switch(config-line): password** *password*

**Switch(config-line): login**

Kullanıcı password yazan yere kendi belirlediği bir parolayı koymalıdır.

## “Enable secret” parolasının oluşturulması

Yetkisiz kişilerin switch aygıtına konsol bağlantısı veya uzaktan bağlantı ile erişebildiği senaryoda cihazın konfigürasyonunda herhangi bir değişiklik yapamaması için bir parola konulmalıdır. Bu parola olmadan cihaz privileged exec moda geçiş yapılamamaktadır. Ayrıca bu parola cihazın konfigürasyon dosyasında şifreli olarak saklanmalıdır. Bu işlem için gerekli komut:

**Switch(config): enable secret** *password*

Kullanıcı password yazan yere kendi belirlediği bir parolayı koymalıdır.

## Parolaları şifreli olarak tutma

Yetkisiz kullanımı engellemek için koyulan parolalar cihazın konfigürasyon dosyasında açık bir şekilde tutulmaktadır. Ancak bu kullanım güvenli değildir. Bu sebeple parolalar konfigürasyon dosyasında şifreli bir şekilde tutulmalıdır. Bu işlem için gerekli komut:

**Switch(config): service password-encryption**

## Default vlan dışında bir vlan oluşturma

Fabrika çıkışında switchin tüm portları vlan 1’e üyedir. Bu herkes tarafından bilindiği için güvenli değildir. Bu yüzden kullanılmayan tüm portlar vlan 1 dışında bir vlana üye yapılmalıdır. Bu işlem için gerekli komut:

**Switch(config): vlan** vlan-id

**Switch(config-if):end**

**Switch(config): interface** interface-id

**Switch(config-if): switchport access vlan** vlan-id

## Kullanılmayan portları kapama

Fabrika çıkışında switchin tüm portları açık olarak gelmektedir. Fiziksel bir bağlantı olduğu anda portlar otomatik olarak aktif gelmektedir. Ancak kullanılan bir cihazın tüm portlarının kullanılmadığı senaryo düşünüldüğünde, cihazın kullanılmayan portları da aktif durumdadır. Bu da herhangi yetkisiz bir kimsenin kendi cihazını switche bağlayarak ağa dahil olabileceği anlamına gelmektedir ki bu bir güvenlik zaafiyetidir. Bu yüzden kullanılmayan portların kapatılması gerekmektedir. Bu işlem için gerekli komut:

**Switch(config): interface** interface-id

**Switch(config-if): shutdown**

## Uzaktan bağlantı için ssh servisini aktif etme

Cihaza uzaktan bağlanma senaryosunda iki alternatif vardır. Birisi telnet, diğeri de ssh’dır. Telnet ile yapılan konfigürasyonda komutlar açık olarak gitmektedir ve kötü niyetli bir üçüncü kişi tarafından izlenebilir. Ancak uzaktan bağlantı ssh ile yapılırsa komutlar şifreli olarak gider ve üçüncü bir kişi tarafından izlenemez. Bu işlem için gerekli komut:

**Switch(config): ip domain-name** domainname.com

**Switch(config): crypto key generate rsa**

**Switch(config): line vty 0 4**

**Switch(config-line): transport input ssh**

**Switch(config-line): exit**

## Port güvenliği kurallarını uygulama

Kötü niyetli bir kişi cihaza bağlanarak, özel bir yazılım ile cihazın MAC adresi tablosunu doldurabilir ve eğer bu senaryo gerçekleşirse switch, hub gibi çalışmaya başlar ve amacını yerine getiremez. Daha da önemlisi herhangi bir porta gitmesi gereken bir trafik tüm portlara iletilerek güvenlik ihmal edilir. Bunun için cihazın bir portundan kaç adet MAC adresi öğrenebileceği sınırlandırılmalıdır. Bu işlem için gerekli komut:

**Switch(config): interface** interface-id

**Switch(config-if): switchport port-security maximum** value

Ağ yöneticisi value yerine 1 ile 3072 arasında bir değer yazarak o porttan öğrenebileceği maksimum MAC adresi sayısını belirler.

## Auto-trunking işlemini iptal etme

Kötü niyetli bir kişinin cihaza bağlanarak, özel bir yazılım ile vlan hopping saldırısı yapmasını engellemek için cihaz portlarının ayarlanması gerekmektedir. Bu ayarlarda hangi portun son kullanıcıya ait olduğunu, hangi kullanıcıdan birden fazla vlan numaralı trafik geçebileceği ayarlanır. Bu işlem için gerekli komut:

Eğer switch portu son kullanıcıya aitse veya sadece bir adet vlan’a üye portlardan gelen trafiği geçirecekse:

**Switch(config): interface** interface-id

**Switch(config-if): switchport mode access**

Eğer switch portu birden fazla vlan’a ait trafiği geçirecekse:

**Switch(config): interface** interface-id

**Switch(config-if): switchport mode trunk**

## Log tutma işlemini aktif etme

Log tutma tüm cihazlarda olduğu gibi switchlerde de önemli bir yer tutmaktadır. Cihaz yöneticisi düzenli aralıklarla logları kontrol etmeli ve yetkisiz erişim denemelerini kontrol etmeli buna göre önlemlerini arttırmalıdır.

## Zaman aşımı süresini aktif etme

Tüm cihaz ve uygulamalarda olduğu gibi cisco switchlerinde de zaman aşımı güvenlik açısından önemli bir önlemdir. Son kullanıcı hatalarını minimize etmek için ayarlanması gereken bir kuraldır. Bu işlem için gerekli komut:

**Switch(config): line console 0**

**Switch(config-line): exec-timeout** value

Value, ağ yöneticisinin belirleyeceği birimi saniye olan zaman aşımı süresidir.

# ROUTER SIKILAŞTIRILMASI

## Güncel router yazılımının kullanılması

Network yöneticisi düzenli aralıklarla yazılımları kontrol etmeli ve yeni bir güncelleme geldiği zaman tüm cihazlara yazılımı yüklemelidir. Bu süreç düzenli takip edilmesi ve mutlaka yapılması gereken bir adımdır. Ancak güncel yazılımın yüklenme işlemi bu raporun içerdiği konulardan birisi değildir.

## Banner ekleme

Cihaza konsol veya uzaktan erişim olması halinde kullanıcıyı uyaran bir mesaj eklenmelidir. Bu mesaj cihazın sadece yetkili kişiler tarafından yönetilebileceği uyarısını içermelidir. Bu işlem için gerekli komut:

**Router(config): banner motd # Authorized Access Only! #**

“Authorized Access Only!” yazan kısma ağ yöneticisi istediği bir uyarıyı koyabilir. Bu sadece bir örnektir.

## Konsol parolasının oluşturulması

Yetkisiz kişilerin cihazın yakınına gelip konsol bağlantısı ile cihaza erişememesi için, cihaza erişimin ilk aşamasında bir parola oluşturulmalıdır. Bu işlem için gerekli komut:

**Router(config): line console 0**

**Router (config-line): password** *password*

**Router (config-line): login**

Kullanıcı password yazan yere kendi belirlediği bir parolayı koymalıdır.

## Uzaktan erişim parolasının oluşturulması

Yetkisiz kişilerin ağa bağlanıp, uzaktan erişiminin engellenmesi için, cihaza erişimin ilk aşamasında bir parola oluşturulmalıdır. Bu işlem için gerekli komut:

**Router (config): line vty 0 4**

**Router (config-line): password** *password*

**Router (config-line): login**

Kullanıcı password yazan yere kendi belirlediği bir parolayı koymalıdır.

## “Enable secret” parolasının oluşturulması

Yetkisiz kişilerin router aygıtına konsol bağlantısı veya uzaktan bağlantı ile erişebildiği senaryoda cihazın konfigürasyonunda herhangi bir değişiklik yapamaması için bir parola konulmalıdır. Bu parola olmadan cihaz privileged exec moda geçiş yapılamamaktadır. Ayrıca bu parola cihazın konfigürasyon dosyasında şifreli olarak saklanmalıdır. Bu işlem için gerekli komut:

**Router (config): enable secret** *password*

Kullanıcı password yazan yere kendi belirlediği bir parolayı koymalıdır.

## Parolaları şifreli olarak tutma

Yetkisiz kullanımı engellemek için koyulan parolalar cihazın konfigürasyon dosyasında açık bir şekilde tutulmaktadır. Ancak bu kullanım güvenli değildir. Bu sebeple parolalar konfigürasyon dosyasında şifreli bir şekilde tutulmalıdır. Bu işlem için gerekli komut:

**Router (config): service password-encryption**

## Uzaktan bağlantı için ssh servisini aktif etme

Cihaza uzaktan bağlanma senaryosunda iki alternatif vardır. Birisi telnet, diğeri de ssh’dır. Telnet ile yapılan konfigürasyonda komutlar açık olarak gitmektedir ve kötü niyetli bir üçüncü kişi tarafından izlenebilir. Ancak uzaktan bağlantı ssh ile yapılırsa komutlar şifreli olarak gider ve üçüncü bir kişi tarafından izlenemez. Bu işlem için gerekli komut:

**Router (config): crypto key generate rsa**

**Router (config): line vty 0 4**

**Router (config-line): transport input ssh**

**Router (config-line): exit**

## Log tutma işlemini aktif etme

Log tutma tüm cihazlarda olduğu gibi routerlarda da önemli bir yer tutmaktadır. Cihaz yöneticisi düzenli aralıklarla logları kontrol etmeli ve yetkisiz erişim denemelerini kontrol etmeli buna göre önlemlerini arttırmalıdır.

## NTP protokolünü aktif etme

Cihazların hem iletişimi için hem de cihazların takibi için ortak bir zaman diliminde olmaları yöneticiye kolaylık sağlamaktadır. Bu işlem için gerekli komut:

**Router (config): feature ntp**

## Zaman aşımı süresini aktif etme

Tüm cihaz ve uygulamalarda olduğu gibi cisco routerlarında da zaman aşımı güvenlik açısından önemli bir önlemdir. Son kullanıcı hatalarını minimize etmek için ayarlanması gereken bir kuraldır. Bu işlem için gerekli komut:

**Router (config): line console 0**

**Router (config-line): exec-timeout** value

Value, ağ yöneticisinin belirleyeceği birimi saniye olan zaman aşımı süresidir.

Switch checklist:

|  |  |
| --- | --- |
| [1. Güncel switch yazılımının kullanılması](#_Toc457601274) |  |
| [2. Banner ekleme](#_Toc457601275) |  |
| [3. Konsol parolasının oluşturulması](#_Toc457601276) |  |
| [4. Uzaktan erişim parolasının oluşturulması](#_Toc457601277) |  |
| [5. “Enable secret” parolasının oluşturulması](#_Toc457601278) |  |
| [6. Parolaları şifreli olarak tutma](#_Toc457601279) |  |
| [7. Default vlan dışında bir vlan oluşturma](#_Toc457601280) |  |
| [8. Kullanılmayan portları kapama](#_Toc457601281) |  |
| [9. Uzaktan bağlantı için ssh servisini aktif etme](#_Toc457601282) |  |
| [10. Port güvenliği kurallarını uygulama](#_Toc457601283) |  |
| [11. Auto-trunking işlemini iptal etme](#_Toc457601284) |  |
| [12. Log tutma işlemini aktif etme](#_Toc457601285) |  |
| [13. Zaman aşımı süresini aktif etme](#_Toc457601287) |  |

Router checklist:

|  |  |
| --- | --- |
| [1. Güncel switch yazılımının kullanılması](#_Toc457601274) |  |
| [2. Banner ekleme](#_Toc457601275) |  |
| [3. Konsol parolasının oluşturulması](#_Toc457601276) |  |
| [4. Uzaktan erişim parolasının oluşturulması](#_Toc457601277) |  |
| [5. “Enable secret” parolasının oluşturulması](#_Toc457601278) |  |
| [6. Parolaları şifreli olarak tutma](#_Toc457601279) |  |
| [9. Uzaktan bağlantı için ssh servisini aktif etme](#_Toc457601282) |  |
| [12. Log tutma işlemini aktif etme](#_Toc457601285) |  |
| [13. NTP protokolünü aktif etme](#_Toc457601286) |  |
| [14. Zaman aşımı süresini aktif etme](#_Toc457601287) |  |

# Ağ Cihazları Sıkılaştırmalarının Kontrol Edilmesi

Yukarıda anlatılan sıkılaştırma önlemleri güvenlik konusu göz önünde bulundurulduğunda kullanılan tüm ağ cihazlarına uygulanması gereken kurallardır. Konfigürasyonu var olan bir ağ cihazının sıkılaştırılma derecesini gözlemlemek ve eksikliklerini kullanıcıya bildirmek amacıyla bir ptyhon scripti hazırlanmıştır. Bu ptyhon scripti ekte sunulmaktadır.

Python scripti sıkılaştırma kurallarına cihazı denetleyecektir. Bu scriptte girdi olarak ağ cihazının switch mi router mı olduğu, ve ağ cihazının konfigürasyon dosyası girdi olarak verilecektir. Script de çıktı olarak kullanıcıya bir rapor üretecektir. Bu raporda denetim maddelerinin kaç tanesinden geçtiği ve denetim sonucunun skoru kullanıcıya iletilecektir.

**Script’in örnek çalışma durumu:**

>>**Cisco\_switch\_router\_hardening\_test.py switch\_konfig\_dosyasi.txt switch**

# Referanslar

1. [www.cisco.com](http://www.cisco.com)
2. NSA – Cisco Security Switch Configuration Guide
3. Daniel B. Cid – 8 Steps to Protect Your Cisco Router
4. SANS – Cisco Router Hardening Step by Step
5. ISACA – Cisco Switch & Router Hardening