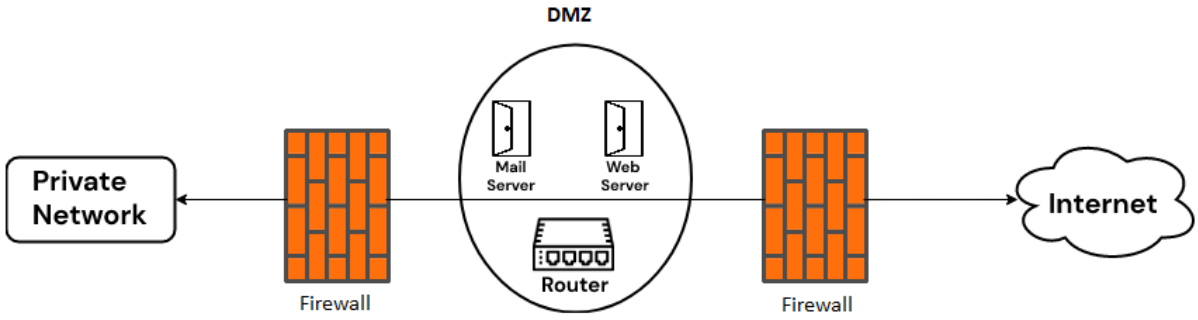
Secure Device Access

LAN güvenliği sağlayabilmek için öncelikle network üzerinde bulunan cihazların güvenliği sağlanmalıdır. Networkteki cihazların güvenliğini sağlayabilmek için de networke giren internet trafiğine müdahale edilmesi gerekiyor. Bunun için network trafiğinin internete çıkış noktasında çeşitli cihazlar ve yazılımlar kullanılarak trafik filtrelenmeye çalışılıyor. Bu filtrele işlemi için çeşitli yaklaşımlar kullanılabiliyor.

- Single Router Approach, network trafiğinin tek bir router üzerinden internete giriş/çıkış yapabildiği yaklaşımdır. Tüm güvenlik politikaları bu router üzerinde bulunur ve uygulanır. Daha çok orta veya küçük ölçekli networkler için kullanılan yaklaşımdır.
- Defense-in-Depth Approach, internet trafiği networke girmeden önce birçok güvenlik katmanına tabi tutularak filtreleniyor. Bu sayede zararlı bağlantıların bir kısmı daha networke girmeden engellenebiliyor.
    - Trafiği filtreleyebilmek için her katmanda Firewall, IPS, WSA, ESA gibi çeşitli güvenlik donanımları ve yazılımları kullanılıyor.
- DMZ Approach, internet üzerinden erişilebilmesi gereken sunucular/kaynaklar için kullanılan yaklaşımdır. Sunucuları internet üzerinden erişilebilir kılmak için ise Defense-in-Depth yaklaşımında kullanılan güvenlik katmanlarının arasında bir alana sunucuların konumlandırılmasıyla gerçekleştiriliyor. Bu sayede sunuculara internet üzerinden gelen trafikler daha esnek filtrelere tabi tutuluyor. Aynı zamanda sunuculara gelen trafikler LAN'dan da izole edilmiş oluyor.



Routerlarda Güvenlik Konusunda Dikkat Edilmesi Gereken Bazı Hususlar

- Fizeksel Güvenlik
    - Elektromanyetik parazit bulunmayan, yetkisiz personellerin erişemeyeceği ve sıcaklık değerlerinin dengeli olduğu ortamlarda bulundurulmalı.
    - Kesintilere karşı yedek güç sağlayıcıları kullanılmalı.
- İşletim Sistemi Güvenliği
    - İşletim sistemi ve konfigürasyon dosyalarının imajları alınmalı/yedeklenmeli.
    - İşletim Sistemine gelen güncellemeler belirli sıklıklarda kontrol edilmeli ve yeni gelen özellikler doğrultusunda konfigürasyonlar üzerinde de güncellemeler yapılmalı.
- Router Sıkılaştırma
    - Kullanılmayan bağlantı seçenekleri devre dışı bırakılmalı.
    - Sadece yetkili personellerin cihaza eriştiği ve personelin yalnızca erişim seviyesi kadar işlem yapabildiği kontrol edilmeli.
    - Gereksiz hizmetler devre dışı bırakılmalı

Router ve switchlere erişimlerin güvence altına alınması gerekiyor. Bu cihazlara yetkisiz bir kullanıcı erişebilirse networkün işleyişini baştan sona değiştirebilir. Bunun için alınabilecek birkaç güvenlik önlemi;

- Erişim seçenekleri ve bağlantı noktaları kısıtlanmalı.
- Cihaza yapılan tüm erişimler kayıt altına alınmalı/loglanmalı.
- Tespit edilen yetkisiz erişimler için gerekli mecralara başvurularak hukuki işlemler başaltılmalı.
- Yalnızca erişmesi gereken kullanıcılar için hesaplar tanımlanmalı ve bu hesapların yetkileri sınırlandırılmalı.
- Erişim sağlanırken bağlantı süreleri, oturum açma denemeleri gibi parametreler sınırlandırılmalı.

Switch ve Routerlarda Bağlantı Seçeneklerine Parola Atama

Cihazlar üzerinde alınabilecek ilk güvenlik önlemi cihazlara bağlanabilmek için kullanılan erişim seçeneklerine parola atanmasıdır. Erişim seçeneklerine bakıldığında;

- Console Port, Console portu kullanılarak gerçekleştirien erişimlere parola atayabilmek için ilk olarak Global konfigürasyon modunda "**line console 0**" komutuyla arayüze giriliyor. Ardından "**password <Password>"** komutuyla parola tanımlanıyor ve "**login**" komutuyla Console portu kullanılarak yapılan erişimlerde parola bilgsinin sorulması sağlanıyor.

```
R1(config)#line console 0
R1(config-line)#password ConsolePort4287
R1(config-line)#login
R1(config-line)#exit
```

- Aux Port, Aux portuna parola atayabilmek için "**line aux 0**" komutuyla AUX arayüzüne giriş yapılıyor. Bundan sonraki adımlar Console portuna parola atama süreciyle aynıdır.

```
R2(config)#line aux 0
R2(config-line)#password SecLab67
R2(config-line)#login
R2(config-line)#exit
```

- SSH veya Telnet ve benzeri protokoller kullanarak cihaza erişebilmek için kullanılan VTY hattına parola atanması gerekiyor. Bunun için Global konfigürasyon modunda "**line vty 0 <Connection Count>**" komutuyla ("**<Connection Count>**" ile aynı anda cihazda açılabilecek oturum sayısı belirleniyor) arayüze giriş yapılıyor. Bu kısımdan sonraki adımlar Console port konfigürasyonu ile aynıdır. Bu konfigürasyon sonunda cihaza Telnet üzerinden bağlanılabilmektedir.
    - Cihazlarda varsayılanda SSH ve Telnet bağlantısı aktif geliyor ancak konfigürasyonları yapılmadığı sürece kullanılamıyorlar. Cihazlara sadece Telnet veya sadece SSH kullanılarak bağlanılabilmesi siteniyorsa bu durum konfigürasyon içerisinde "**transport input (ssh | telnet)**" komutuyla ayrıca belirtiliyor.
    - VTY hattı kullanılarak gerçekleştirilen bağlantılarda kullanıcının belirli bir süre CLI üzerinde komut çalıştırmadığı durumlarda bağlantının kesilmesi sağlanabiliyor (konfigürasyon sonrasında cihaza bağlantının açık unutulmuş olma ihtimaline karşı önlem olarak). Bunun için "**line vty 0 <Connection Count>**" komutuyla VTY arayüzüne giriş yapılarak "**exec-timeout <Minute> <Seconds>**" komutu kullanılıyor.

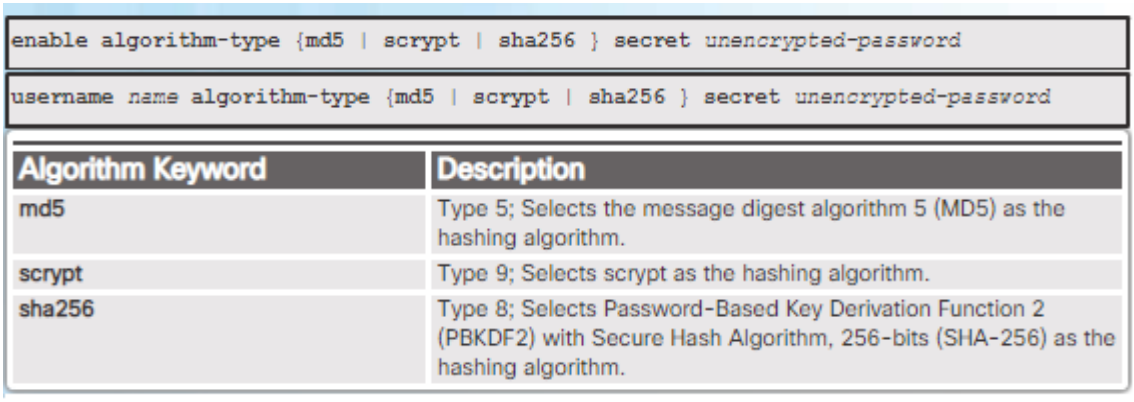
```
R2(config)#line vty 0 15
R2(config-line)#password SecLab67
R2(config-line)#login
R2(config-line)#exit
```

Parola Şifreleme Algoritmaları

Cihazlarda yapılan konfigürasyonlar Flash ünitesinde "config.text" isimli bir dosya üzerinde tutuluyor. Cihaza erişim için tanımlanan parola bilgileri de bu dosya içerisinde plain-text olarak ("password" kelimesiyle tanımlananlar) tutulmaktadır. Bu durum güvenlik zafiyeti oluşturmaktadır çünkü bu dosyaya erişebilen kullanıcılar herkesin parolasını açık bir şekilde görebilmektedir. Bu duruma önlem olarak "**service password-encryption**" komutuyla parola bilgilerinin config.text dosyasında Type7 isimli bir şifreleme algoritmasıyla şifreli şekilde tutulması sağlanabiliyor (şifrelenen parolalar "**do sh run**" komutuyla görüntülenebilir). Bu şifreleme algoritması her ne kadar zayıg ve çift yönlü bir şifreleme algoritması olsa da parola bilgilerinin açık bir şekilde görünmesinin önüne geçmektedir (Shoulder Surfing gibi saldırılara karşı önlem olarak kullanılabilmektedir).

Cihazlarda kulanılan parolaların konfigürasyon dosyasında şifreli tutulabilmesi için konfigürasyonlarda farklı şifreleme/Hash algoritmaları da kullanılabilmektedir. Örnek olarak Enable moduna parola atanırken veya kullanıcı oluştururken parola atama işlemi için "secret" kelimesi kullanılıyordu. Secret kelimesi kullanıldığında parola bilgileri konfigürasyon dosyasında varsayılanda Type5 yani MD5 Hash algoritması kullanılarak saklanıyor. Günümüzde MD5 Hash algoritması güvenli kabul edilmediği için kullanılması önerilmiyor. Parola bilgilerini şifrelemek/Hash'li skaklayabilmek için daha çok yeni Hash algoritmaları olan Type8 (scrypt) veya Type9 (sha256) algoritmalarının kullanılması öneriliyor. Konfigürasyonlarda ise bu algoritmalar "algorith-type" parametresi kullanılarak belirtiliyor. Örnek olarak;

- "**enable algorithm-type sha256 secret Security01**"
- "**username newUser algorithm-type scrypy secret Security01**"



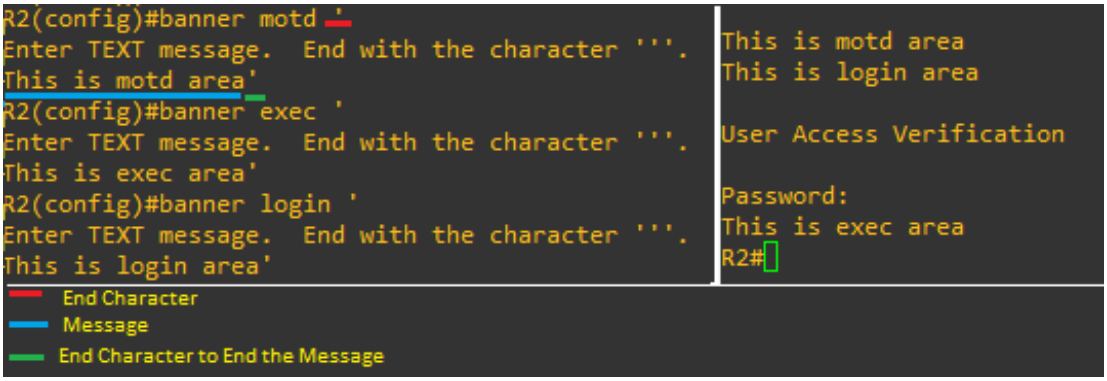
```
enable algorithm-type {md5 | scrypt | sha256 } secret unencrypted-password
```

```
username name algorithm-type {md5 | scrypt | sha256 } secret unencrypted-password
```

Algorithm Keyword	Description
md5	Type 5; Selects the message digest algorithm 5 (MD5) as the hashing algorithm.
scrypt	Type 9; Selects scrypt as the hashing algorithm.
sha256	Type 8; Selects Password-Based Key Derivation Function 2 (PBKDF2) with Secure Hash Algorithm, 256-bits (SHA-256) as the hashing algorithm.

Oturum Açma İşlemlerinde Özelleştirmeler

- Cihazlara erişimlerde kullanıcıların oturum açmadan hemen önce (motd), oturum açma sırasında (login) veya oturum açtıktan hemen sonrası (exec) için bilgilendirme/uyarı mesajları bırakılabiliyor. Bırakılan bu mesajların içeriğine ayrıca dikkat edilmesi gerekiyor. Buraya bırakılan mesajlar kurumu yasal açıdan koruyabilirken, "Welcome" ve benzeri davetkar mesajlar bırakmak kurumu hukuki açıdan zor durumlarada bırakacaktır.
  Konfigürasyon için Global konfigürasyon modunda "**banner { motd | exec | login} <End Character> <Messages> <End Character>**" komutu kullanılıyor.



- Cihazada oturum açma sırasında güvenliği arttırabilmek adına çeşitli güvenlik konfigürasyonları da yapılabiliyor. Bu konfigürasyonlar cihaz geneline uygulandığı için Global konfigürasyon modunda gerçekleştiriliyor.
    - Belirli zaman aralığında birkaç başarısız deneme yapılması durumunda kullanıcının bağlantısı bir süreliğine bloklanabiliyor. Bu önlem için "**login block-for <Blocking Time> attemts <Count of Attempts> within <Time of Try>**" komutu kullanılıyor. "**login block-for**" özelliği Normal Mode ve Quiet Mode olmak üzere iki modda çalışabiliyor.
        - Normal Mode, belirli bir sürede gerçekleştirilen başarısız oturum açma girişimlerinin sayısını tutar.
        - Quiet Mode, başarısız oturum açma denemelerinin sayısı cihazda tanımlanan sınırları aşması durumunda cihaz üzerinde bütün oturum açma girişimleri (Buna etwork yöneticisi de dahil) engellenir. Bu durumda dahi cihaza belirli kullanıcıların bağlanabilmesi için bir ACL hazırlanarak "**login quiet-mode access-class <ACL Name or Number>**" komutuyla buraya uygulanır. Bu sayede başarısız deneme sayısı sınırı aşsa dahi ACL ile tanımlanan kullanıcılar cihaza erişim sağlayabilir.
    - Cihazda oturum açabilecek kullanıcıları filtreleyebilmek için girişlere ACL uygulanabiliyor. Bunun için "**login quiet-mode access-class <ACL Name or Number>**" komutu kullanılıyor.
        - Erişim için tanımlanan ACL'ler ayrıca VTY hattına doğrudan da uygulanabiliyordu (cihazların her bir arayüzüne uygulamaya gerek kalmıyordu). Bu sayede cihazın arayüzlerine gelen trafikler gereksiz yere fazladan filtreye tabi tutulmuyordu – CCNA 3.04 – ACLs konusunda açıklanmıştı.
    - Kullanıcının oturum açma sırasında gerçleştirdiği başarısız denemeler arasında belirli bir süre beklemesi sağlanabiliyor. Bu sayede DOS saldırılarına yönelik de önlem alınmış oluyor. Bu tanımlama için "**login delay <Time>**" komutu kullanılıyor.
    - Kullanıcıların cihazda başarılı veya başaısız oturum açma denemelerini kayıt altına alınabiliyor. Bunun için "**login on-failure log {Every Login Count}**" veya "**login on-success log {every Login Count}**" komutları kullanılıyor. Loglamanın belirli bir deneme sayısından sonra yapılması isteniyorsa komut sonunda bu sayı belirtilebiliyor (örneğin "**login on-failure log 3**" → Her 3 hatalı denemede bir kayıt oluşturur/loglar).

```
R2(config)#login block-for 120 attempts 5 within 60
R2(config)#ip access-list standard ACLforLogin
R2(config-std-nacl)#permit 192.168.20.5
R2(config-std-nacl)#permit 192.168.10.3
R2(config-std-nacl)#exit
R2(config)#login quiet-mode access-class ACLforLogin
R2(config)#login delay 5
R2(config)#login on-success log
R2(config)#login on-failure log
```

- Burada "**login on-failure log {Every Login Count}"** komutuna alternatif olarak "**security authentication failure rate <Threshold Rate> log**" komutu da kullanılabiliyor.

```
R2(config)#security authentication failure rate 3 log
```

SSH Konfigürasyonu

Cihazlara güvenli bir şekilde uzak erişim sağlayabilmek için bağlantının/trafiğin şifrelenmesi gerekiyor. Bunun için bağlantılarda Telnet yerine SSH protokolü kullanılmalıdır. Cihaz üzerinde SSH protokolüne devreye almak için;

- Öncelikle "**hostname <Device Name>**" komutuyla cihaza yeni ve benzersiz bir Hostname veriliyor.
- "**ip domain name <Domain>"** komutuyla cihazda bir domain name tanımı yapılır. Bu domain bilgisi sertifikada kullandığı için domain tanımı yapılmadan RSA algoritması için key oluşturulamıyor.
- Bağlantı sürecinde trafiği şifrelemek için RSA algoritması kullanılmaktadır. RSA algıritmasının çalışabillmesi için "**crypto key generate rsa general-keys modulus <Key Size>**" komutuyla bir anahtar oluşturulması gerekiyor.
    - İsteğe bağlı olarak SSH devre dışı bırakilmak istendiğinde "**crypto key zeroize rsa**" komutuyla oluşturulan anahtar silinebiliyor.
- Cihaza giriş yapabilmek için "**username <Username> secret <Password>**" komutuyla cihaz üzerinde kullanıcı oluşturuluyor.
    - isteğe bağlı olarak "**algorithm-type**" parametresiyle kullanılacak Hash algoritması seçilebilir.
- Bağlantı kurabilmek için cihazın ilgili arayüzüne (Bu cihaz bir L2 switch ise VLAN arayüzüne, router ise herhangi bir arayüzüne atanabiliyor) girilerek "**ip address <Ip Address> <Subnet Mask>**" komutuyla ip bilgileri tanımlanarak "**no sh**" komutuyla arayüz kullanıma açılıyor.
- Son olarak bağlantı kurabilmek için "**line vty 0 <Connection Count>**" komutu kullanılarak VTY arayüzüne giiliyor ve "**transport input ssh**" komutuyla cihaza sadece SSH protokolü üzerinden bağlanılabilmesi sağlanıyor. Ardından "**login local**" komutuyla SSH bağlantılarında kullanıcı adı ve parola bilgilerinin sorulması ve girilen bilgilerin kontrolünün cihaz üzerinde tanımlanan kullanıcı adı ve parola bilgileriyle yapılacağı tarif ediliyor
    - Cihaz üzerinde tanımlı kullanıcılar yerine uzak bir sunucu (AAA, TACACS gibi) üzerinden de kullanıcı doğrulaması yapılabiliyor.
- Bu adımdan sonra artık cihaza SSH üzerinden bağlantı kurulabiliyor.

```
R2(config)#hostname R2
R2(config)#ip domain name security.ty
R2(config)#crypto key generate rsa general-keys modulus 2048
The name for the keys will be: R2.security.ty

% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]

R2(config)#
*Mar  1 00:55:23.155: %SSH-5-ENABLED: SSH 1.99 has been enabled
R2(config)#username NetSec secret NetSec67
R2(config)#int fastEthernet 0/1
R2(config-if)#ip address 192.168.10.1 255.255.255.0
R2(config-if)#no sh
R2(config-if)#exit
R2(config)#line vty 0 4
R2(config-line)#transport input ssh
R2(config-line)#login local
R2(config-line)#exit
R2(config)#end
R2#wr
*Mar  1 00:59:02.723: %SYS-5-CONFIG_I: Configured from console by console
R2#wr
Building configuration...
[OK]
R2#
```

SSH Ek Konfigürasyonlar

- Cihazlarda SSH konfigürasyonu yapıldıktan sonra bağlantıların güvenliğini arttırabilmek adına "**ip ssh time-out <Time>**" komutuyla kullanıcının kimlik doğrulama işlemi için izin verilen süre sınırlandırılabiliyor (varsayılanda 120 saniye).
- "**ip ssh authentication-retries <Count>**" komutuyla kullanıcıların kimlik doğrulama işlemi için ardışık deneme girişimleri sınırlandırılabiliyor (varsayılanda 3).

```
R2(config)#ip ssh time-out 50
R2(config)#ip ssh authentication-retries 2
```

- SSH konfigürasyonunda varsayılanda hem SSH v1 hem de SSH v2 devreye girmektedir. SSHv1 zafiyetlere sahip olduğu için v2 kullanılması tercih ediliyor. Bunu "ip ssh version 2" komutunu kullanarak sadece SSH v2 kullanılması sağlanabiliyor.

NOT

- Cihaz üzerinde konfigürasyonlar yapılırken kullanılabilecek minimum parola uzunluğunu "**security password min-length <Min Length>**" komutu kullanılarak sınırlandırılabiliyor.

Terminolojiler

- Local Access, kullanıcı ve cihaz fiziksel olarak aynı lokasyonda bulunur. Kullanıcı, cihaz üzerinde bulunan konsol portunu kullanarak bağlanır. Cihazlara ilk konfigürasyonlar da konsol portu kullanılarak yapılır.
- Remote Access, kullanıcı ve cihaz fiziksel olarak farklı konumlardadır ve kullanıcı cihaza erişebilmek için Telnet, SSH, SNMP gibi çeşitli protokoller kullanır.

Kontrol Komutları

- sh login
- sh login failures
- sh crypto key mypubkey rsa
- sh ip ssh