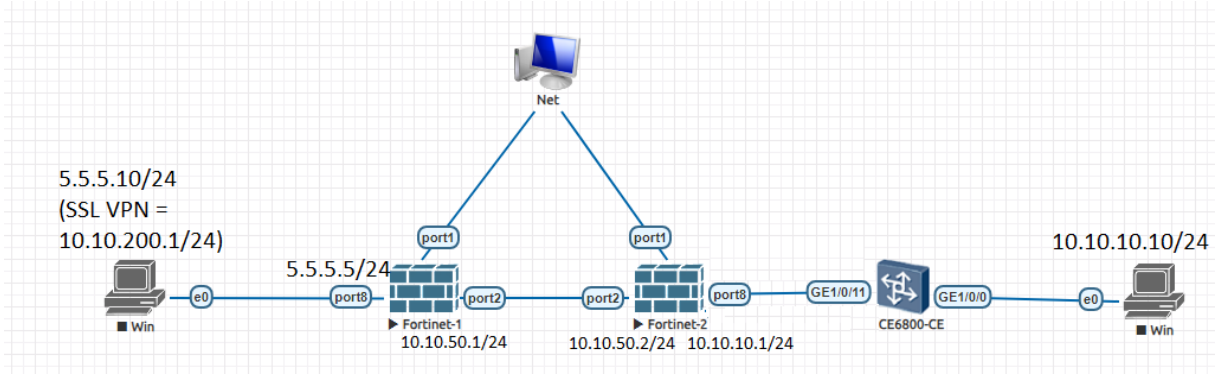


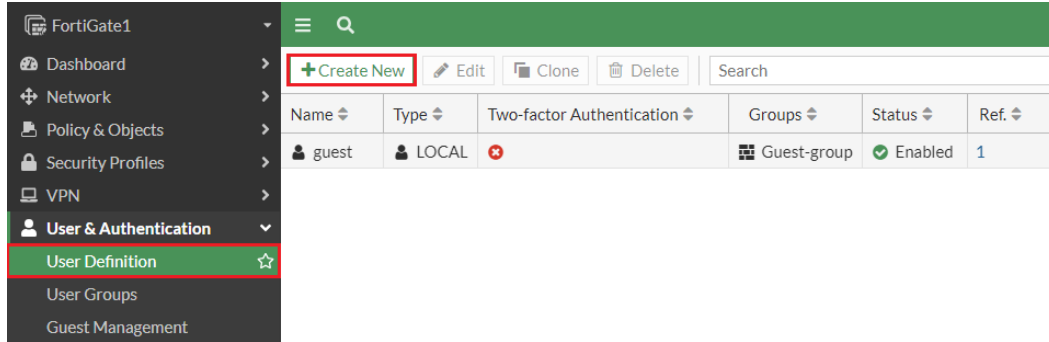
SSL VPN Configuration

Günümüzde uzaktan çalışma yöntemine geçişle beraber kullanıcıların kurum networklerine güvenli bir şekilde bağlanarak çalışabilmeleri için VPN teknolojilerine olan ihtiyaç da artmıştır. Kullanıcıların kurum networküne erişebilmeleri için SSL VPN teknolojisi tercih edilebilmektedir. Bu yazıda Fortigate FW üzerinde SSL VPN konfigürasyonu için gereken temel tanımlar açıklanmaya çalışılacaktır (Bu süreçte aşağıdaki topoloji üzerinden ilerlenecektir). Detaylar için “**Fortigate FW -> Fortigate Fundamentals**” notlarını inceleyebilirsiniz.

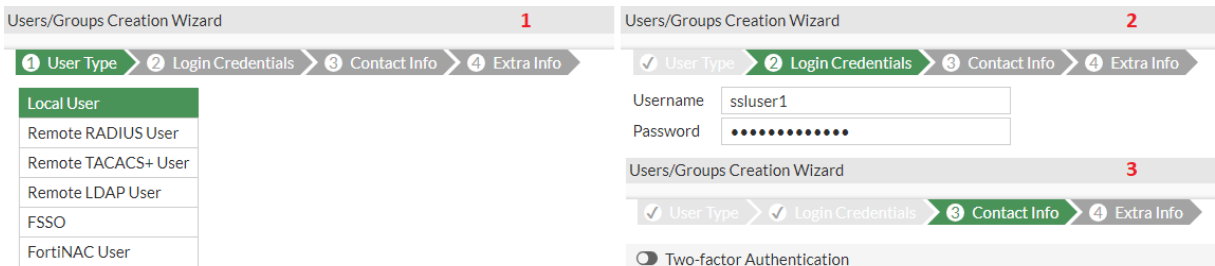


Topolojideki cihazların arayüzlerinde temel ayarlamalar yapıldıktan sonra (“Kullanılan Komutlar” belgesi içerisinde uygulanan komutları bulabilirsiniz);

- 1- SSL VPN konfigürasyonu için ilk olarak SSL VPN bağlantısı kuracak kullanıcılar için kullanıcı tanımının yapılması gerekiyor. Bu işlem için “**User&Authentication -> User Definition -> Create New**” yolu takip edilmelidir.



Burada cihaz üzerinde (Local) bir kullanıcı tanımı oluşturulabileceği gibi uzak bir LDAP, TACACS, RADIUS sunucusu Fortigate ile ilişkilendirilerek kullanıcı hesaplarının yönetimi sağlanabilir. Biz bu uygulamada cihaz üzerinde/Local kullanıcı tanımı oluşturarak ilerleyeceğiz. Kullanıcı hesabı oluşturulurken isteğe bağlı olarak 2FA özelliği devreye alınabilir.



Kullanıcı tanımının son adımında kullanıcı durumu ve herhangi bir kullanıcı grubuna dâhil edilip edilmeyeceği belirlenmelidir. **Burada tek bir kullanıcı dahi olsa mutlaka bir kullanıcı grubu oluşturulup kullanıcı bu gruba dâhil edilmelidir ("SSL-VPN Settings -> Authentication/Portal Mapping" kısmında Portal erişiminin bir kullanıcı grubuyla eşleştirilmesi gerekiyor. Tek bir kullanıcıyla eşleştirildiği takdirde kullanıcı SSL VPN bağlantısı kuramıyor).** Bu nedenle oluşturulan kullanıcı hesabını dâhil etmek üzere yeni bir kullanıcı grubu oluşturulmuştur (SSL VPN tanımı yapıldıktan sonra aynı erişim kapsamına sahip yeni bir kullanıcı eklenmek istendiğinde yeni bir kullanıcı hesabı oluşturularak hesabın bu kullanıcı grubuna eklenmesi yeterli olacaktır. Bu sayede oluşturulan kullanıcı kullanıcı grubunun eşleştirildiği Portal tanımına doğrudan dâhil edilmiş olacaktır).

The image shows two screenshots of the FortiGate configuration interface. The first screenshot (labeled 1) shows the 'Users/Groups Creation Wizard' with the 'Extra Info' tab selected. The 'User Account Status' is set to 'Enabled', and the 'User Group' is set to 'SSLGroup1'. The second screenshot (labeled 2) shows the 'New User Group' configuration. The 'Name' is 'SSLGroup1', the 'Type' is 'Firewall', and the 'Members' list is empty. The 'OK' button is highlighted.

```

FortiGate # config user group
FortiGate (group) # edit SSLGroup1
new entry 'SSLGroup1' added
FortiGate (SSLGroup1) # set group-type firewall
FortiGate (SSLGroup1) # set member ssluser1
FortiGate (SSLGroup1) # end

FortiGate # config user local
FortiGate (local) # edit ssluser1
new entry 'ssluser1' added
FortiGate (ssluser1) # set status enable
FortiGate (ssluser1) # set type password
FortiGate (ssluser1) # set passwd SSLUser1Pass*
FortiGate (ssluser1) # end

```

- 2- Kullanıcı ve Grup tanımları yapıldıktan sonra bu kullanıcı grubunun SSL VPN üzerinden FW'a bağlanırken kullanacakları bir ip adresi belirlenmelidir. Dolayısıyla hem SSL VPN Portal tanımında hem de SSL VPN üzerinden bağlanacak kullanıcıların erişimleri istenen networkler için oluşturulacak Policy tanımlarında kullanılmak üzere bir ip adres aralığı tanımlanması gerekiyor. Bu işlem için **"Policy&Objects -> Addresses -> Create New -> Address"** yolu takip edilmelidir.

The image shows the 'Policy & Objects' configuration page in FortiGate. The 'Addresses' tab is selected. The 'Create New' button is highlighted, and the 'Address' option is selected from the dropdown menu. The 'Name' field is empty, and the 'IP Range/Subnet' field is set to '5'. The 'FABRIC_DEVICE' and 'FIREWALL_AUTH_PORTAL_ADDRESS' options are visible in the list.

Burada SSL VPN kullanıcıları için topoloji üzerinde kullanılmayan/boş bir ip bloğu seçilmelidir. Bu bloğun boyutu/genişliği, SSL VPN için oluşturulan gruba dâhil edilen kullanıcıların sayısı göz önünde bulundurularak belirlenmelidir. Örnek olarak oluşturulan gruba 100 kullanıcı dâhil edilmişse bu durumda en azından /25 Prefix Length ($2^7 - 2 = 126$ kullanılabilir ip adresi yapar) genişliğinde bir ip bloğu seçilmelidir. SSL VPN için oluşturulan kullanıcı grubuna verilecek ip adres tanımıyla beraber SSL VPN üzerinden bağlanacak kullanıcıların erişimine izin verilecek hedef ip adreslerinin/bloklarının da tanımlanması gerekiyor.

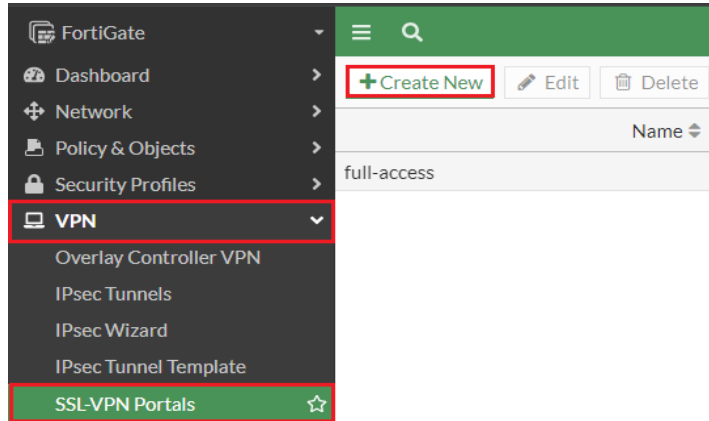
Name	Details	Interface	Type	Ref
FABRIC_DEVICE	0.0.0.0/0		Address	0
FIREWALL_AUTH_PORTAL_ADDRESS	0.0.0.0/0		Address	0
SSLVPNAddr-1	10.10.200.0/24		Address	4
SSLVPN_TUNNEL_ADDR1	10.212.134.200-10.212.134.210		Address	0
WinServ-1	10.10.10.10/32		Address	3

```

Fortigate-1 # config firewall address
Fortigate-1 (address) # edit SSLVPNAddr-1
Fortigate-1 (SSLVPNAddr-1) # set type ipmask
Fortigate-1 (SSLVPNAddr-1) # set subnet 10.10.200.0/24
Fortigate-1 (SSLVPNAddr-1) # next
Fortigate-1 (address) # edit WinServ-1
Fortigate-1 (WinServ-1) # set type ipmask
Fortigate-1 (WinServ-1) # set subnet 10.10.10.10/32
Fortigate-1 (WinServ-1) # end

```

- 3- İp adres tanımları oluşturulduktan sonra “VPN – SSL VPN Portals – Create New” yolu takip edilerek SSL VPN ile bağlanacak kullanıcıların erişim sağlamasına izin verilecek adresler için bir portal tanımı oluşturulması gerekiyor.



Burada temel anlamada “Name” alanıyla oluşturulan Portal tanımına bir isim verilmelidir. İsim tanımı yapıldıktan sonra SSL VPN üzerinde bağlanacak kullanıcılara **Web Mode** ve/veya **Tunnel Mode** olmak üzere iki farklı modda erişim tanımı yapılabilmektedir. Bu tanımların anlamlarına bakıldığında;

- **Web Mode**, SSL VPN üzerinden bağlanan kullanıcıların sadece network kaynaklarını kullanabilmelerini sağlayan moddur. Kullanıcıların FortiClient uygulamasını yüklemesine gerek kalmadan web sayfası üzerinden VPN bağlantısı yapabilme imkânı tanır.
- **Tunnel Mode**, SSL VPN üzerinden bağlanan kullanıcıların ağ kaynaklarını kullanmasına izin verirken aynı zamanda internet trafiği de dâhil olmak üzere tüm trafiği Fortigate üzerinden geçecek şekilde internete çıkarmasına da imkân veren moddur. Bu durumda Fortigate üzerinde tanımlı tüm güvenlik politikalarına ve çözümlerine de dâhil edilir. Bu mod devreye alındığında VPN bağlantısı kurulabilmesi için FortiClient yazılımına ihtiyaç duyulmaktadır.

Tunnel Mode konfigürasyonu için,

- **“Split Tunneling”** özelliğiyle, kullanıcıların SSL-VPN trafiği ile internet trafiğinin ayırt edilip edilmeyeceği belirtilmelidir. **Bu özellik devreye alındığında VPN bağlantısı yapan kullanıcıların kendi internetleri ile kuruma bağlanmaları sağlandıktan sonra erişim verilen ip adresleri dışındaki ip adreslerine kendi internetleri üzerinden çıkış yapması sağlanır.** Eğer bu özellik devre dışı bırakılırsa kullanıcılar kurum networkü üzerinden internete çıkarılacağı (tüm hedef ip adresleri için oluşturulan trafiklerin SSL VPN tüneline yönlendirileceği anlamına geliyor) anlamına gelmektedir. Bu durumda kullanıcıların internete erişebilmeleri için ayrıca Policy tanımı yazılmalıdır. Bu özellik devreye alındığında;
 - **Disable**, tüm istemci trafiğini SSL-VPN tüneline yönlendirilir.
 - **Enable Based on Policy Destination**, yalnızca portal tanımının **“Routing Address Override”** kısmında belirtilen adres tanımlarına ilişkin oluşturulan Policy tanımlarıyla eşleşen trafiklerin SSL VPN tüneline girmesine izin verilmesi sağlanır (**“Routing Address Override”** kısmında tanımlanmayan adresler için oluşturulan trafiklerin tünele girişine izin verilmez).
 - SSL VPN tanımları bu seçenek seçilerek yapıldıktan sonra zaman içerisinde yeni bir ip adresine/subnete daha erişmesi istenebiliyor. Bu durumda ilgili Portal tanımı altında Static Route ve Policy tanımı yapılmasına rağmen Tracert aracı çalıştırıldığında trafiğin tünele girmediği görülebilir. Bu durumda Portal kısmına da bu adres tanımının eklenmesi gerektiği unutulmamalıdır. **Bu tanım Portal tanımı altına eklendikten sonra “Authentication/Portal Mapping” kısmında ilgili kullanıcı grubu ile Portal tanımının eşleştirildiği kısımdan bu tanım kaldırılıp yeniden tanımlanmadığı sürece yapılan değişiklikler algılanmayabiliyor.**
 - **Enable for Trusted Destination**, Yalnızca açıkça güvenilen hedefle eşleşmeyen istemci trafiği SSL-VPN tüneli üzerinden yönlendirilecektir.

Split tunneling

- ☐ **Disabled**
All client traffic will be directed over the SSL-VPN tunnel.
- ☒ **Enabled Based on Policy Destination**
Only client traffic in which the destination matches the destination of the configured firewall policies will be directed over the SSL-VPN tunnel.
- ☐ **Enabled for Trusted Destinations**
Only client traffic which does not match explicitly trusted destinations will be directed over the SSL-VPN tunnel.

- **“Routing Address Override”** kısmı **“Enabled Based on Policy Destination”** seçeneği seçildiğinde açılmaktadır. SSL VPN üzerinden bağlanacak istemcilerin erişmesi istenen networklerin ip adres/subnet tanımları belirtilmelidir.
- **“Source IP Pools”** kısmında, bu portal tanımı üzerinden bağlanacak SSL VPN kullanıcı grubuna verilecek ip adresi/bloğu/aralığı için oluşturulan adres tanımları seçilmelidir (Trial Version kullandığım için birden fazla Portal tanımı yapılmasına izin verilmiyor. Bu nedenle varsayılanda gelen **“full-access”** portal tanımı üzerinde düzenleme yapmak durumunda kaldım). Normalde burada her SSL VPN grubu için farklı bir Portal tanımı yapılabilir.

Edit SSL-VPN Portal

Name full-access

Limit Users to One SSL-VPN Connection at a Time

Tunnel Mode

Split tunneling

☐ Disabled
All client traffic will be directed over the SSL-VPN tunnel.

☒ Enabled Based on Policy Destination
Only client traffic in which the destination matches the destination of the configured firewall policies will be directed over the SSL-VPN tunnel.

☐ Enabled for Trusted Destinations
Only client traffic which does not match explicitly trusted destinations will be directed over the SSL-VPN tunnel.

Routing Address Override WinServ-1

Source IP Pools SSLVPNAAddr-1

```

FortiGate # config vpn ssl web portal
FortiGate (portal) # edit full-access
FortiGate (full-access) # set tunnel-mode enable
FortiGate (full-access) # set split-tunneling enable
FortiGate (full-access) # set split-tunneling-routing-negate disable
FortiGate (full-access) # set split-tunneling-routing-address WinServ-1
FortiGate (full-access) # set ip-pools SSLVPNAAddr-1
FortiGate (full-access) # end

```

Tunnel Mode Portal tanımı yapıldıktan sonra isteğe bağlı olarak devreye alınabilecek birkaç özellik bulunuyor. Bu özelliklere bakıldığında;

- Allow client to save password**, FortiClient yazılımının kullanıcı parolasını kaydetmesini sağlayan özelliktir. Bu sayede istemci bir kez oturum açtıktan sonra ki süreçte yeniden bağlanmak istediğinde otomatik/Parola girmesine gerek kalmadan olarak VPN olabilecektir.
- Allow client to connect automatically**, istemci bilgisayarının bir sonraki açılışında FortiClient yazılımı otomatik olarak başlamaya ayarlıysa VPN bağlantısının otomatik olarak oluşturulmasını sağlayan özelliktir.
- Allow client to keep connections alive**, istemci oturumu belirli bir süre boşa kalsa dahi VPN bağlantısının kesilmemesini sağlayan özelliktir. Bunun için FortiClient yazılımının bağlantı ekranına bir bildirim gelir.
- DNS Split Tunneling**, tanımlı SSL VPN Portalıyla eşleştirilecek kullanıcı gruplarının belirli alan adlarını çözümlmek için kullanılacak birincil ve ikincil DNS sunucularını belirlemek için kullanılan özelliktir (Farklı bir DNS’de yönlendirilmek istenildiğinde bu seçenek kullanılır.).

Tunnel Mode Client Options

Allow client to save password

Allow client to connect automatically

Allow client to keep connections alive

DNS Split Tunneling

FortiGate # config vpn ssl web portal
FortiGate (portal) # edit full-access
FortiGate (full-access) # set auto-connect enable
FortiGate (full-access) # set keep-alive enable
FortiGate (full-access) # set save-password enable
FortiGate (full-access) # end

Web Mode konfigürasyonu için,

- SSL-VPN bağlantısı yaptıktan sonra istemcinin bağlanmak istediği bir kaynak için **Bookmark** tanımlarının oluşturulması gerekiyor. Bunun için Bookmark ismi, bağlantı için kullanılacak protokol ve bu kaynağa erişim için kullanılacak bağlantı tanımlanmalıdır.
 - o Bu adımda konsol satırında Apptype seçimine göre ayarlanacak parametreler de değişiklik göstermektedir (Trial Licens e olduğu için birden fazla Portal tanımı oluşturulmasına izin vermiyor. Bu nedenle yine varsayılanda gelen “full-access” Portal tanımı üzerinde uygulamasını gerçekleştirdim).

Web Mode

Portal Message: SSL-VPN Portal

Theme: Neutrino

Show Session Information: ☒

Show Connection Launcher: ☒

Show Login History: ☒

User Bookmarks: ☒

Rewrite Content IP/UI: ☐

RDP/VNC clipboard: ☒

Predefined Bookmarks

+ Create New

Edit

Delete

Search

Q

Name	Type	Location	Description
Server_Web_GUI	HTTP/HTTPS	10.10.10.10	Server

```
FortiGate # config vpn ssl web portal
FortiGate (portal) # edit full-access
FortiGate (full-access) # set web-mode enable
FortiGate (full-access) # config bookmark-group
FortiGate (bookmark-group) # edit SSL-VPN-Prtl
FortiGate (SSL-VPN-Prtl) # config bookmarks
FortiGate (bookmarks) # edit Server_Web_GUI
FortiGate (Server_Web_GUI) # set apptype web
FortiGate (Server_Web_GUI) # set url 10.10.10.10
FortiGate (Server_Web_GUI) # set description Server
FortiGate (Server_Web_GUI) # end
FortiGate (SSL-VPN-Prtl) # end
FortiGate (full-access) # end
```

4- Portal tanımı için temelde bu kadar ayarlama yapılması yeterlidir. Portla tanımı yapıldıktan sonra artık “SSL-VPN Settings” kısmına geçilerek bağlantı kurulması için birkaç ayarlama yapılması gerekiyor. Burada;

- **Enable SSL-VPN**, SSL VPN hizmetinin devreye alınması/devre dışı bırakılması için kullanılıyor.
- **Listen on interface(s)**, SSL VPN bağlantısı için kullanılacak arayüz seçilmelidir. Genelde internet üzerinden gerçekleştirildiği için cihazların ISP bağlı arayüzü seçilir.
- **Listen on port**, SSL VPN bağlantısı için kullanılacak portu belirlemek için kullanılıyor. Varsayılanda 443. Port seçili gelmektedir.
- **Redirect HTTP to SSL-VPN**, HTTP bağlantı isteklerinin SSL VPN’e yönlendirilmesi için kullanılan özelliktir.
- **Allow access from any host | Limit access to specific host**, SSL VPN bağlantısını yapabilecek kullanıcıları/adresleri kısıtlamak için kullanılan alandır. “Allow access from any host” seçeneği seçildiğinde bütün kullanıcılar/adresler SSL VPN bağlantısı yapabilir. “Limit access to specific host” seçeneği seçildiğinde sadece izin verilen kullanıcılar/adresler SSL VPN bağlantısı yapabilir.
- **Idle logout**, SSL VPN ile bağlanan kullanıcıların ne kadar süre tepkisiz kalması durumunda bağlantının koparılacağını belirlemek için kullanılıyor.
- **Server Certificate**, SSL-VPN bağlantısı karşılandığında gelecek olan sertifikayı ayarlamak için kullanılan kısımdır.
- **Require client certificate**, kullanıcı veya kullanıcı gruplarında sertifika bazlı doğrulama yapılması istendiği durumda devreye alınan özelliktir.

SSL-VPN Settings



No SSL-VPN policies exist. [Click here to create a new SSL-VPN policy using these settings](#)

Connection Settings

Enable SSL-VPN ☒

Listen on Interface(s)

port8

+

Listen on Port

60443



Web mode access will be listening at <https://10.10.50.1:60443>

Server Certificate

Fortinet_Factory



You are using a default built-in certificate, which will not be able to verify your server's domain name (your users will see a warning). Let's Encrypt can be used to easily generate a trusted certificate if you do not have one.

[Create Certificate](#)

Redirect HTTP to SSL-VPN ☐

Restrict Access

[Allow access from any host](#) [Limit access to specific hosts](#)

Idle Logout



Inactive For

300

Seconds

Require Client Certificate ☐

- **Address range**, “Authomatically assing adres” seçeneği seçildiğinde SSL-VPN portals menüsünün source kısmında tanımlanan ip/network adres tanımları otomatik olarak eklenir/algılanır. Erişilmesi istenen adresler arttırılmak istendiğinde, “specifiy custom ip range” seçeneği seçilerek ek ip/network adres tanımları eklenebilir.
- **DNS Server**, SSL VPN üzerinden bağlanan istemcilerin DNS sunucusu olarak hangi ip adresin tanımlanacağını belirlemek için kullanılıyor. Burada sistem üzerinde tanımlı DNS adresi seçilebileceği gibi farklı bir DNS sunucusunun ip adresi de girilebilir.
- **Specify Wins Server**, herhangi bir Windows sunucusu kullanıldığı durumlarda burada tanımlanır.
- **Authentication/Portal Mapping**, SSL VPN üzerinden bağlanacak kullanıcı gruplarının hangi Portal tanımı kullanarak erişeceğini belirlemek için Kullanıcı Grubu – Portal eşlemesinin yapıldığı kısımdır.
 - o Burada kullanıcı grubu yerine doğrudan kullanıcı tanımı bir Portal ile eşleştirildiği takdirde SSL VPN bağlantısı yapılamayacaktır.
 - o Burada spesifik şekilde belirtilmeyen Kullanıcı Grubu – Portal tanımları için varsayılanda kullanılmak üzere Portal tanımı yapılması gerekiyor. Aksi takdirde SSL VPN hizmeti devreye alınamıyor (Trial Licanse olduğu için birden fazla Portal tanımı oluşturulmasına izin vermiyor. Bu nedenle yine varsayılanda gelen “full-access” Potal tanımını seçmek durumunda kaldım).

Tunnel Mode Client Settings ⓘ

Address Range Automatically assign addresses Specify custom IP ranges

Tunnel users will receive IPs in the range of 10.212.134.200 - 10.212.134.210

DNS Server Same as client system DNS Specify

DNS Server #1 8.8.8.8

DNS Server #2 8.8.4.4

Specify WINS Servers ☐

Authentication/Portal Mapping ⓘ

+ Create New Edit Delete Send SSL-VPN Configuration

Users/Groups ↕	Portal ↕
SSLGroup1	full-access
All Other Users/Groups	full-access

```
Fortigate-1 # config vpn ssl settings
Fortigate-1 (settings) # set status enable
Fortigate-1 (settings) # set source-interface port8
Fortigate-1 (settings) # set port 60443
Fortigate-1 (settings) # set servercert Fortinet_Factory
Fortigate-1 (settings) # set default-portal full-access
Fortigate-1 (settings) # set dns-server1 8.8.8.8
Fortigate-1 (settings) # set dns-server2 8.8.4.4
Fortigate-1 (settings) #
Fortigate-1 (settings) # config authentication-rule
Fortigate-1 (authentication-rule) # edit 1
Fortigate-1 (1) # set groups SSLGroup1
Fortigate-1 (1) # set portal full-access
Fortigate-1 (1) # end
Fortigate-1 (settings) # end
```

- 5- SSL VPN tanımı yapıldıktan sonra artık VPN olacak kullanıcıların network üzerinde kaynaklara erişim sağlayabilmesi için Policy tanımlarının yapılması gerekiyor. Policy tanımı için **“Policy&Objects -> Firewall Policy”** yolu takip edilmelidir. Burada kullanım amacına göre Policy tek yönlü veya çift yönlü yazılabilir.

Policy yazılırken dikkat edilmesi gereken noktalardan birisi de **“Incoming Interface”** kısmında **“SSL-VPN Tunnel Interface (ssl.root)”** seçeneği seçilmelidir. Source kısmında ise **SSL VPN için oluşturulan ip/network adres tanımına ek olarak SSL VPN için kullanılacak kullanıcı grubunun da eklenmesi gerekiyor (seçilmediğinde uyarı verecektir zaten).**

New Policy

Name *i* MFI_SSL_to_Win_Srv

Incoming Interface *w* SSL-VPN tunnel interface (ssl.root)

Outgoing Interface port2

Source SSLVPNAAddr-1
SSLGroup1

Destination WinServ-1

Schedule always

Service ALL

Action ☒ ACCEPT ☐ DENY

Inspection Mode ☒ Flow-based ☐ Proxy-based

Firewall / Network Options

NAT ☐

Protocol Options ☒ default

SSL VPN üzerinden bağlanacak kullanıcıların network çerisindeki kaynaklarla karşılıklı olarak haberleşebilmeleri için aynı Policy'nin tersi de oluşturulabilir.

- Bunun için ilgili Policy'e sağ tıklayıp **"Clone Reverse"** seçeneği ile Reverse Policy tanımı oluşturulabilir. Reverse Policy tanımı oluşturulduktan sonra üzerine tıklanarak bir isim verilip **"Comments"** kısmındaki açıklamalar silinip **"Enable This Policy"** seçeneği aktif edilerek Policy devreye alınabilir (Policy'nin tersi oluşturulurken "Destination" kısmında SSL VPN için kullanılan ip/network adres tanımının yanında SSL VPN için oluşturulan kullanıcı grubunun eklenmesine gerek kalmıyor).

SSL-VPN tunnel interface (ssl.root) → port2 1

MFI_SSL_to_Win_Srv SSLGroup1 WinServ-1 always ALL

Implicit 1

Policy

- Set Status
- Filter by Name
- Copy
- Paste
- Insert Empty Policy
- Clone Reverse**
- Show Matching Logs
- Show in FortiView
- Edit
- Edit in CLI
- Delete Policy

Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Security Profiles
Win_Srv_to_MFI_SSL	SSL-VPN tunnel interface (ssl.root)	port2	SSLGroup1 SSLVPNAAddr-1	WinServ-1	always	ALL	✓ ACCEPT	✗ Disabled	SSL no-inspection
MFI_SSL_to_Win_Srv	port2	SSL-VPN tunnel interface (ssl.root)	WinServ-1	SSLVPNAAddr-1	always	ALL	✓ ACCEPT	✗ Disabled	SSL no-inspection
Implicit Deny	any	any	all	all	always	ALL	✗ DENY		

```

FortiGate (policy) # edit 10
new entry '10' added

FortiGate (10) # set name Win_Srv_to_MFI_SSL
FortiGate (10) # set srcintf ssl.root
FortiGate (10) # set dstintf port2
FortiGate (10) # set srcaddr SSLVPNAddr-1
FortiGate (10) # set groups SSLGroup1
FortiGate (10) # set dstaddr WinServ-1
FortiGate (10) # set action accept
FortiGate (10) # set schedule always
FortiGate (10) # set service ALL
FortiGate (10) # next

```

```

FortiGate (policy) # edit 11
new entry '11' added

FortiGate (11) # set name MFI_SSL_to_Win_Srv
FortiGate (11) # set srcintf port2
FortiGate (11) # set dstintf ssl.root
FortiGate (11) # set srcaddr WinServ-1
FortiGate (11) # set dstaddr SSLVPNAddr-1
FortiGate (11) # set action accept
FortiGate (11) # set schedule always
FortiGate (11) # set service ALL
FortiGate (11) # end

```

Son adımda eğer ki ulaşması gereken hedef network farklı bir FW üzerinde ise bu durumda Static Route tanımı da yapılması gerekiyor.

New Static Route

Automatic gateway retrieval ☐

Destination

Gateway Address

Interface

Administrative Distance

Comments

Status

Advanced Options

```

FortiGate # config router static
FortiGate (static) # edit 1
FortiGate (1) # set dst 10.10.10.1/24
FortiGate (1) # set gateway 10.10.50.2
FortiGate (1) # set device port2
FortiGate (1) # end

```

Fortigate-1

Dashboard

Network

Interfaces

DNS

Packet Capture

SD-WAN

Static Routes

Menu

Search

Create New

Edit

Clone

Delete

Search

Destination	Gateway IP	Interface	Status
10.10.10.0/24	10.10.50.2	port2	Enabled

Uygulama yaptığımız topolojide erişilmesi gereken kaynak Fortigate2 üzerinde tanımlı olduğu için Fortigate1 üzerinde hedef ip adresi Windows-Server'ın bulunduğu network olan paketlerin Fortigate2'ye gönderilmesi için Static Route tanımı yapılıyor.

- SSL VPN kullanıcısının Windows-Server'a erişebilmesi için benzer şekilde Fortigate2 üzerinde de Static route ve Policy tanımlarının yapılması gerekiyor (**ÖRNEK KONFIGÜRASYONLARI “Kullanılan Komutlar” KISMINDA BULABİLİRSİN**). Burada hedef adres olarak SSL VPN grubuna belirlenen subnet için rota tanımı yapıldığına dikkat etmelisin.

Fortigate-2

Dashboard

Network

Policy & Objects

Firewall Policy

IPv4 DoS Policy

Addresses

Policy Lookup

Search

Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Security Profiles
Win_Srv_to_MFI_SSL	port8	port2	Win_Srv_IP_POOL	SSL_VPN_Addr_1	always	ALL	ACCEPT	Disabled	SSL no-inspection
MFI_SSL_to_Win_Srv	port2	port8	SSL_VPN_Addr_1	Win_Srv_IP_POOL	always	ALL	ACCEPT	Disabled	SSL no-inspection
Implicit Deny	any	any	all	all	always	ALL	DENY		

Özetle;

- 1- SSL VPN için bağlanacak kullanıcıların ve kullanıcı grubunun tanımlanması gerekiyor.
- 2- Tünel tanımında kullanılacak hedef ve kaynak ip adresleri oluşturulmalı.
 - a. Tünel için boşta bir ip bloğu seçilerek adres tanımı oluşturulmalıdır.
- 3- SSL VPN Portal tanımı oluşturulması gerekiyor.
- 4- SSL VPN Settings kısmında genel olarak port ve arayüz ayarları yapıldıktan sonra;
 - a. **“Tunnel Mode Client Settings → Address Range”** kısmında SSL VPN tanımında kullanıcı için tanımlanan adres tanımının eklenmesi gerekiyor.
 - b. **“Authentication/Portal Mapping”** kısmında oluşturulan Tunnel Mode ile ilgili kullanıcı GRUBU eşleştirilerek buraya işlenmesi gerekiyor (kullanıcı grubu yerine doğrudan kullanıcı tanımı eklenirse VPN %80 de kalıyor).
- 5- SSL VPN tanımı tamamlandıktan sonra kullanıcının bağlanarak trafik oluşturabilmesi için çift yönlü olacak şekilde Policy tanımının yapılması gerekiyor.
 - a. Policy tanımında SSL Tünelden Fortigate’e gelen yönde Policy tanımında kaynak adres olarak SSL VPN tanımı için oluşturulan KULLANICI GRUBUNUN da eklenmesi gerekiyor.
 - b. Policy tanımında Interface için aşağıdaki gibi l2t.root tanımı seçiliyor. Adres tanımı olarak da kullanıcı için oluşturulan adres tanımı ekleniyor.
- 6- Farklı bir adrese yönlendirilecekse Statik Route tanımı yapılması gerekiyor.
 - a. Ek olarak hedef L3 cihaz üzerinde de Policy ve Static Route tanımlarının yapılması gerekiyor.

Kaynaklar

- <https://docs.fortinet.com/document/fortigate/7.4.4/administration-guide/29900/user-groups>
- <https://docs.fortinet.com/document/fortigate/7.0.6/cli-reference/360620/config-vpn-ssl-web-portal>
- <https://video.fortinet.com/products/fortigate/5.4/cookbook-ssl-vpn-web-and-tunnel-mode-5-4#:~:text=Web%20Mode%20allows%20users%20to,FortiGate's%20security%20policies%20and%20profiles.>
- <https://docs.fortinet.com/document/fortigate/5.6.0/cookbook/478309/ssl-vpn-using-web-and-tunnel-mode>
- <https://docs.fortinet.com/document/fortigate/6.2.16/cookbook/307303/ssl-vpn-split-tunnel-for-remote-user>
- https://www.beyaz.net/tr/guvenlik/makaleler/fortigate_firewall_ssl_vpn_kurulumu.html
- <https://docs.fortinet.com/document/fortigate/7.4.4/administration-guide/629245/split-tunneling-settings>
- <https://docs.fortinet.com/document/fortigate/6.2.16/cookbook/579694/ssl-vpn-web-mode-for-remote-user>
- https://www.beyaz.net/tr/network/makaleler/fortigate_cihazinda_ssl_vpn_konfigurasyonu.html
- <https://docs.fortinet.com/document/fortigate/6.2.16/cookbook/579694/ssl-vpn-web-mode-for-remote-user>