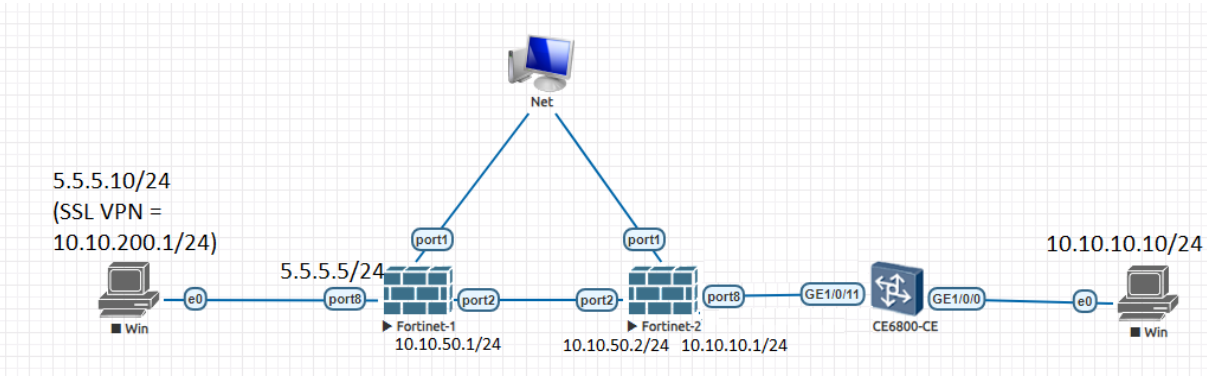
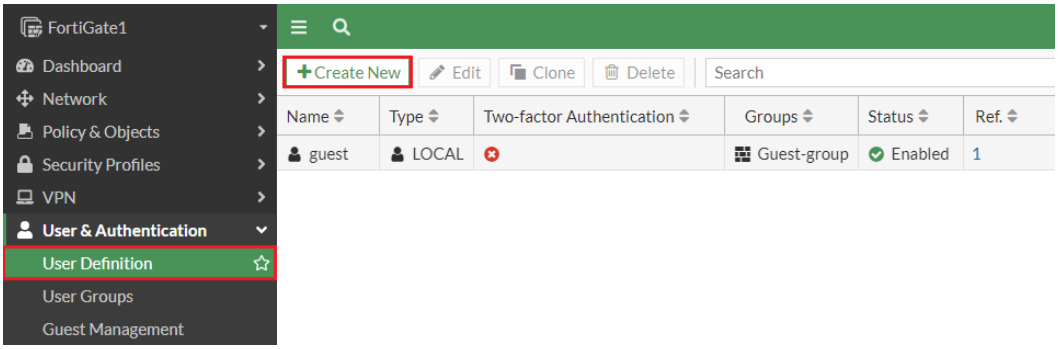
SSL VPN Configuration

Günümüzde uzaktan çalışma yöntemine geçişle beraber kullanıcıların kurum networklerine güvenli bir şekilde bağlanarak çalışabilmeleri için VPN teknolojilerine olan ihtiyaç artmıştır. Kullanıcıların kurum networküne erişebilmeleri için SSL VPN teknolojisi kullanılabilmektedir. 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 inceleyebilirsin.

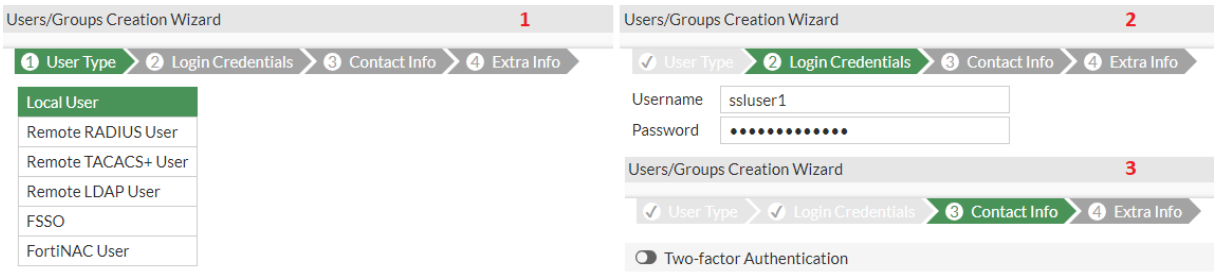


Topolojideki cihazların arayüzlerinde temel ayarlamalar yapıldıktan sonra ("Kullanılan Komutlar" belgesi içerisinde uygulanan komutları bulabilirsin);

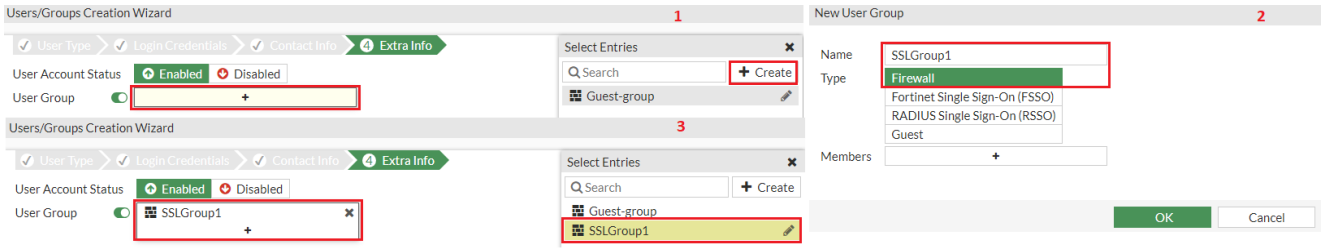
1- SSL VPN konfigürasyonu için ilk olarak cihaz üzerinde bağlanacak kullanıcılar için kullanıcı tanımının yapılması gerekiyor. Bu işlem için "**User&Authentication -> User Definitation -> Create New**" yolu takip edilmelidir.



Burada cihaz üzerinde (Local) bir kullanıcı tanımı oluşturulabileceği gibi uzak bir LDAP, TACACS, RADIUS sunucusu Fortigate'e ile ilişkilendirilerek kullanıcı yönetimi sağlanabilir. Burada ise cihaz üzerinde/Local kullanıcı tanımı oluşturulmuştur. İsteğe bağlı olarak 2FA özelliği devreye alınabilmektedir.



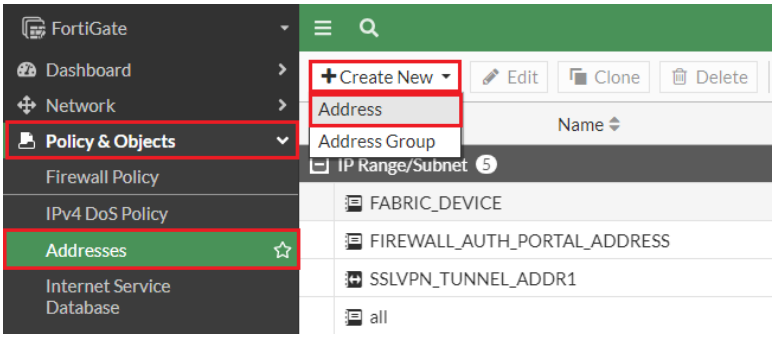
Kullanıcı tanımının son adımında kullanıcı durumu ve herhangi bir kullanıcı grubuna dâhil edilip edilmeyeceği belirlenmelidir. Burada tek bir kullanıcı dahi olsa mutlaka bir kullanıcı grubu oluşturulup kullanıcı bu gruba dâhil edilmelidir (“**SSL-VPN Settings -> Authentication/Portal Mapping**” kısmında Portal erişiminin bir kullanıcı grubuyla eşleştirilmesi gerekiyor. Tek bir kullanıcıyla eşleştirildiği takdirde kullanıcı SSL VPN bağlantısı kuramıyor). Bu nedenle kullanıcıyı dâhil etmek üzere yeni bir kullanıcı grubu oluşturulmuştur (SSL VPN tanımı yapıldıktan sonra tanımlanan kullanıcı grubunun eşleştirildiği Portal tanımına yeni bir kullanıcı daha dâhil edilmek/eklenmek istendiğinde sadece yeni bir kullanıcı oluşturulup kullanıcının bu gruba dâhil edilmesi yeterli olacaktır.).



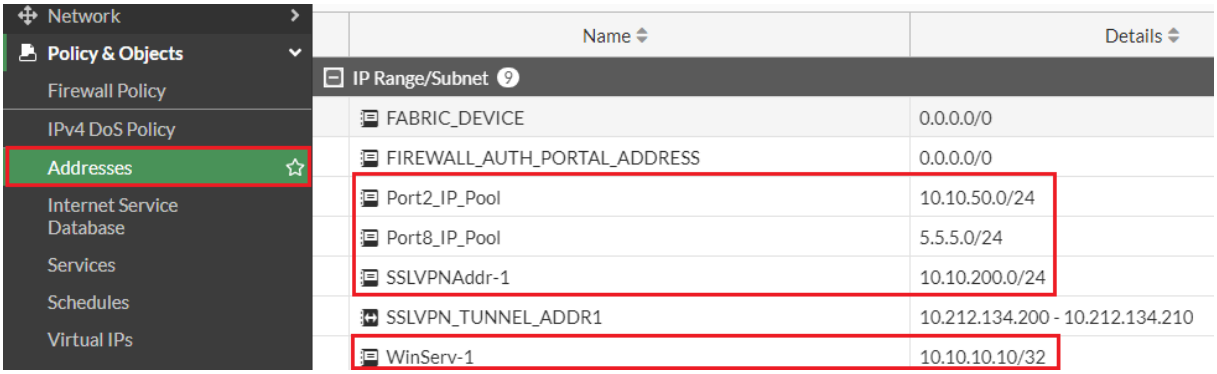

```
FortiGate # config user group

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 SSlUserlPass*

FortiGate (ssluser1) # end
```

2- Kullanıcı ve Grup tanımları yapıldıktan sonra hem SSL VPN Portal tanımında hem de SSL VPN üzerinden bağlanacak kullanıcıların erişmeleri istenen networkler için Policy tanımında kullanılmak üzere adres tanımlarının oluşturulması gerekiyor. Bu işlem için “**Policy&Objects –> Addresses –> Create New -> Address**” yolu takip edilmelidir.



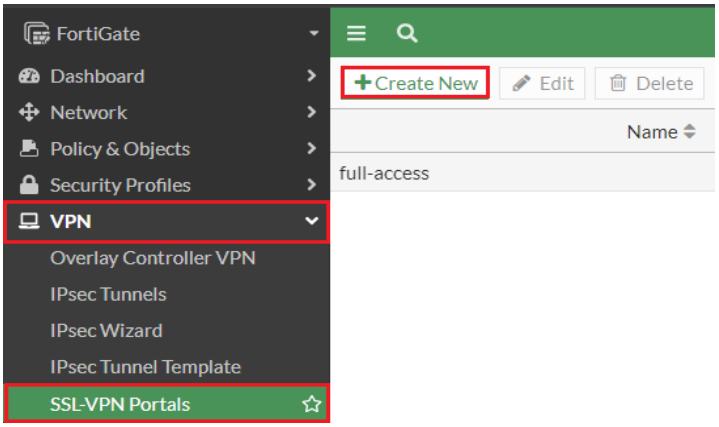
Burada SSL VPN kullanıcıları için topoloji üzerinde kullanılmayan/boş bir ip bloğu seçilmelidir. Bu bloğun boyutu/genişliği, SSL VPN için oluşturulan gruba dâhil edilen kullanıcıların sayısı göz önünde bulundurularak belirlenmelidir. Örnek olarak oluşturulan gruba 100 kullanıcı dâhil edilmişse bu durumda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




```
FortiGate1 # config firewall address

FortiGate1 (address) # edit SSLVPNAddr-1

FortiGate1 (SSLVPNAddr-1) # set type ipmask

FortiGate1 (SSLVPNAddr-1) # set subnet 10.10.200.0/24

FortiGate1 (SSLVPNAddr-1) # next

FortiGate1 (address) # edit WinServ-1

FortiGate1 (WinServ-1) # set type ipmask

FortiGate1 (WinServ-1) # set subnet 10.10.10.10/32

FortiGate1 (WinServ-1) # next
```

```
FortiGate1 (address) # edit Port2_IP_Pool
new entry 'Port2_IP_Pool' added

FortiGate1 (Port2_IP_Pool) # set type ipmask

FortiGate1 (Port2_IP_Pool) # set subnet 10.10.50.0/24

FortiGate1 (Port2_IP_Pool) # next

FortiGate1 (address) # edit Port8_IP_Pool
new entry 'Port8_IP_Pool' added

FortiGate1 (Port8_IP_Pool) # set type ipmask

FortiGate1 (Port8_IP_Pool) # set subnet 5.5.5.0/24

FortiGate1 (Port8_IP_Pool) # end
```

3- Ip 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.

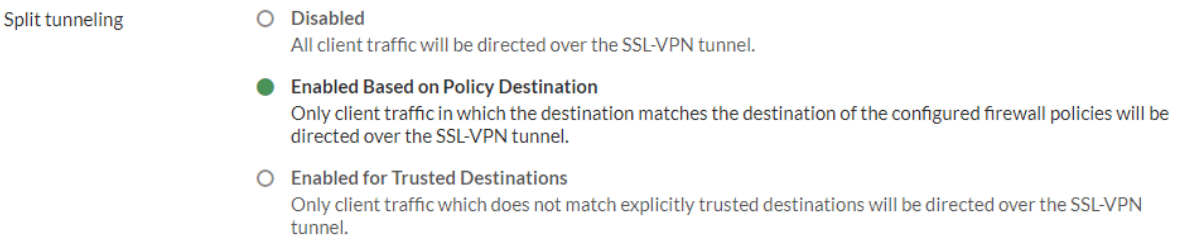


Burada temel anlamada "**Name**" alanıyla oluşturulan Portal tanımına bir isim tanımı yapılmalıdır. İsim tanımı yapıldıktan sonra SSL VPN üzerinde bağlanacak kullanıcılara **Web Mode** ve/veya **Tunnel Mode** olmak üzere iki farklı modda erişim tanımı yapılabilmektedir. Bu tanımların anlamlarına bakıldığında;

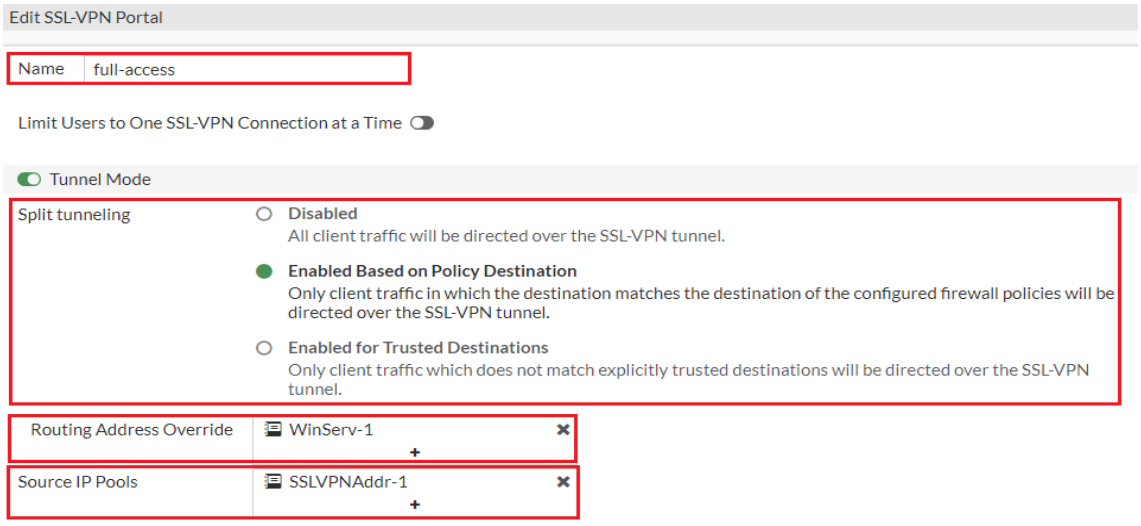
- **Web Mode**, SSL VPN üzerinden bağlanan kullanıcıların sadece network kaynaklarını kullanabilmelerini sağlayan moddur. FortiClient uygulamasına gerek kalmadan web sayfası üzerinden VPN bağlantısı yağabilme imkânı tanır.
- **Tunnel Mode**, SSL VPN üzerinden bağlanan kullanıcıların ağ kaynaklarını kullanmasına 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 politikalara ve çözümlerine de dâhil edilir. Bu mode 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 tineline 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 adrest 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 tanım algılanmayabiliyor.
    - **Enable for Trusted Destination**, Yalnızca açıkça güvenilen hedefle eşleşmeyen istemci trafiği SSL-VPN tüneli üzerinden yönlendirilecektir.



- "**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 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).




```
FortiGate1 # config vpn ssl web portal

FortiGate1 (portal) # edit full-access

FortiGate1 (full-access) # set tunnel-mode enable

FortiGate1 (full-access) # set split-tunneling enable

FortiGate1 (full-access) # set split-tunneling-routing-negate disable

FortiGate1 (full-access) # set split-tunneling-routing-address WinServ-1

FortiGate1 (full-access) # set ip-pools SSLVPNAddr-1

FortiGate1 (full-access) # end
```

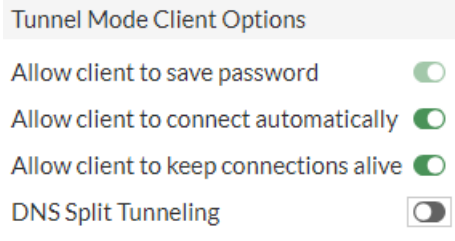
Tunnel Mode Portal tanımı yapıldıktan sonra isteğe bağlı olarak devreye alınabilecek birkaç özellik bulunuyor. Bu özelliklere bakıldığında;

a- **Allow client to save password**, FortiClient yazılımının kullanıcı parolasını kaydetmesini sağlayan özelliktir. Bu sayede istemci bir kez oturun açtıktan sonra ki süreçte yeniden bağlanmak istediğinde otomatik/Parola girmesine gerek kalmadan olarak VPN olabilecektir.

b- **Allow client to connect automatically**, istemci bilgisayarının bir sonraki açılışında FortiClient yazılımı otomatik olarak başlamaya ayarlıysa VPN bağlantısının otomatik olarak oluşturulmasını sağlayan özelliktir.

c- **Allow client to keep connections alive**, istemci oturumu belirli bir süre boşta kalsa dahi VPN bağlantısının kesilmemesini sağlayan özelliktir. Bunun için FortiClient yazılımının bağlantı ekranına bir bildirim gelir.

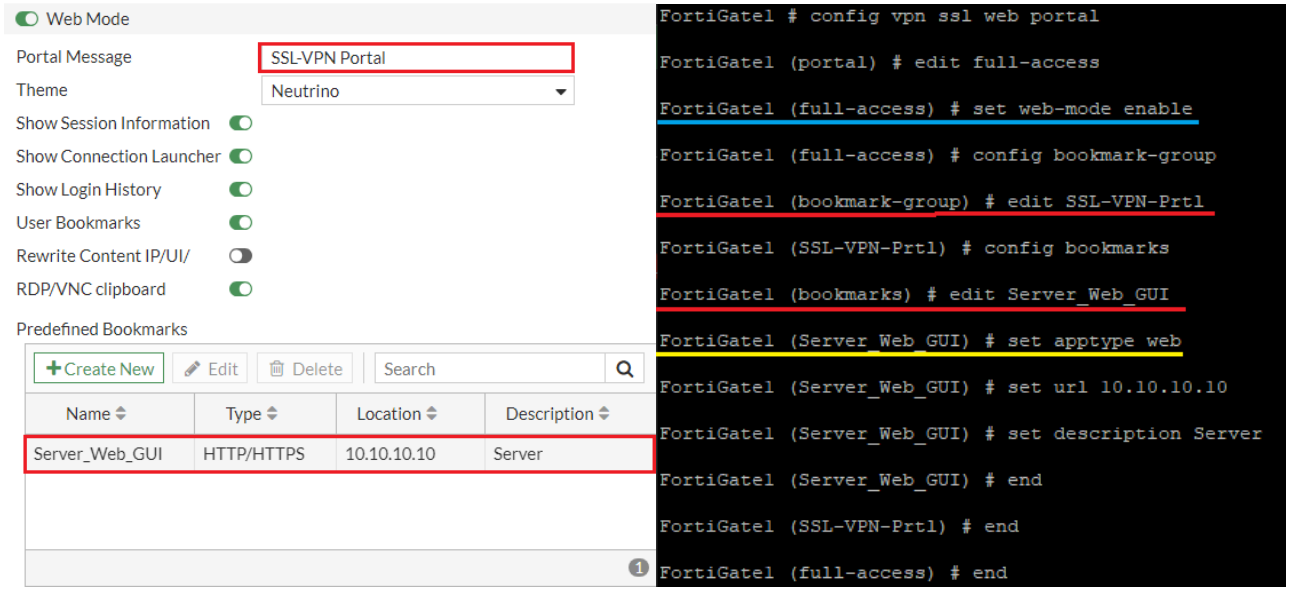
d- **DNS Split Tunneling**, tanımlı SSL VPN Portalıyla eşleştirilecek kullanıcı gruplarının belirli alan adlını çözümlemek için kullanılacak birincil ve ikincil DNS sunucularını belirlemek için kullanılan özelliktir (Farklı bir DNS'de yönlendirilmek istenildiğinde bu seçenek kullanılır.).




```
FortiGate1 # config vpn ssl web portal

FortiGate1 (portal) # edit full-access

FortiGate1 (full-access) # set auto-connect enable

FortiGate1 (full-access) # set keep-alive enable

FortiGate1 (full-access) # set save-password  enable

FortiGate1 (full-access) # end
```

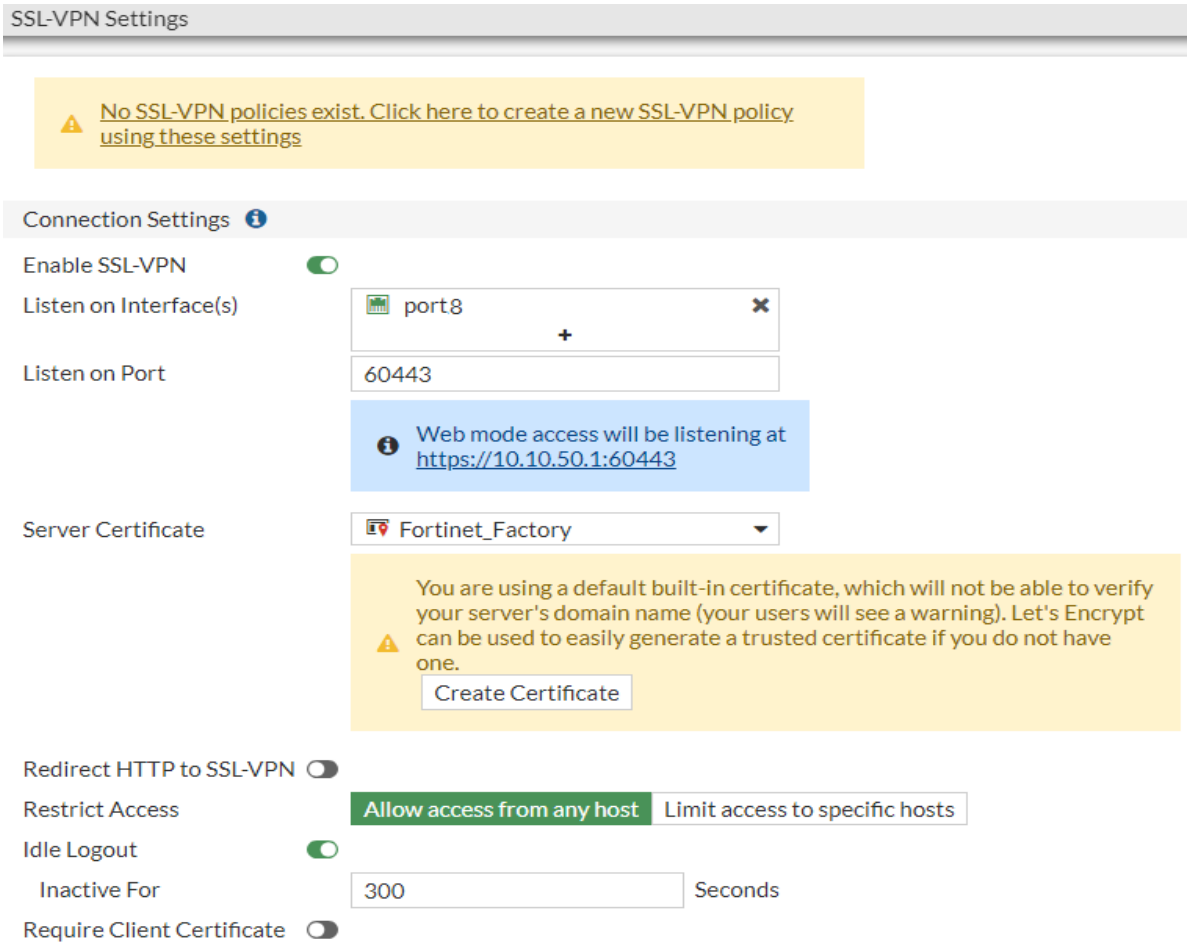
Web Mode konfigürasyonu için,

- 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.
    - Burada konsol satırında Apptype seçimine göre ayarlanacak parametreler de değişiklik göstermektedir (Trial Licanse olduğu için birden fazla Portal tanımı oluşturulmasına izin vermiyor. Bu nedenle yine varsayılanda gelen "full-access" Portal tanımı üzerinde uygulamasını gerçekleştirdim).

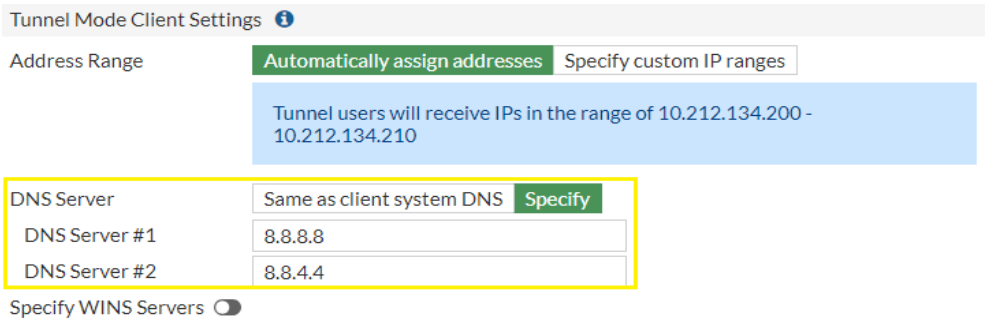


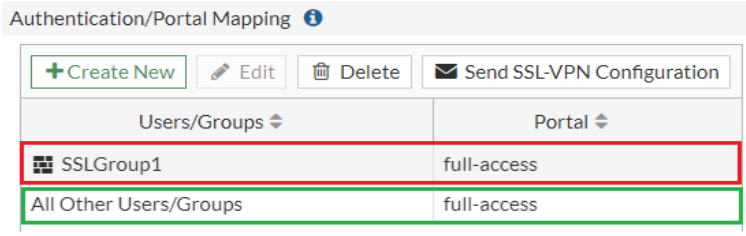
4- Portal tanımı için temelde bu kadar ayarlama yapılması yeterlidir. Portla tanımı yapıldıktan sonra artık "**SSL-VPN Settings**" kısmına geçilerek bağlantı kurulması için birkaç ayarlama yapılması gerekiyor. Burada;

- **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.



- **Address range**, "Authomatically assing addres" seçeneği seçildiğinde SSL-VPN portals menüsünün source kısmında tanımlanan ip/network adres tanımları otamatik 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.
    - Burada kullanıcı grubu yerine doğrudan kullanıcı tanımı bir Portal ile eşleştirildiği takdirde SSL VPN bağlantısı yapılamayacaktır.
    - 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).

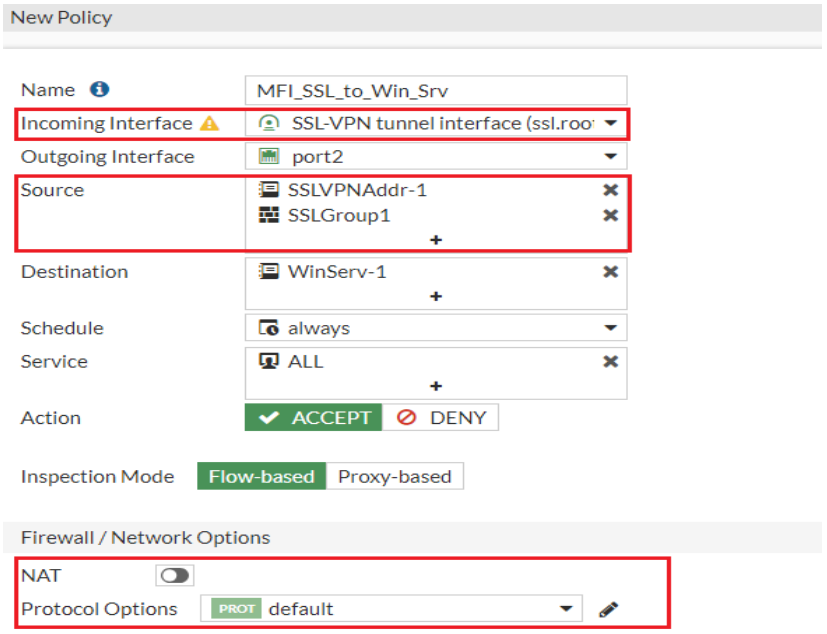





```
FortiGate1 # config vpn ssl settings

FortiGate1 (settings) # set status enable

FortiGate1 (settings) # set source-interface port8

FortiGate1 (settings) # set port 60443

FortiGate1 (settings) # set servercert Fortinet_Factory

FortiGate1 (settings) # set default-portal full-access

FortiGate1 (settings) # set dns-server1 8.8.8.8

FortiGate1 (settings) # set dns-server2 8.8.4.4

FortiGate1 (settings) #
FortiGate1 (settings) # config authentication-rule

FortiGate1 (authentication-rule) # edit 1
new entry '1' added

FortiGate1 (1) # set groups SSLGroup1

FortiGate1 (1) # set portal full-access

FortiGate1 (1) # end

FortiGate1 (settings) # end
Warning: You are using one of the factory default certificates.
For better security, please use a proper signed certificate.
```

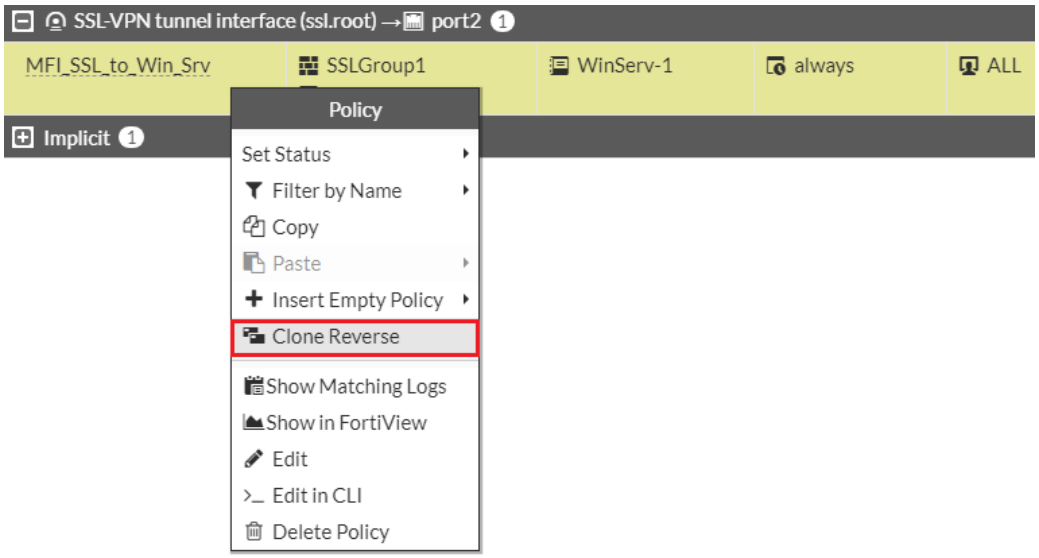
5- SSL VPN tanımı yapıldıktan sonra artık VPN olacak kullanıcıların network üzerinde kaynaklara erişim sağlayabilmesi için Policy tanımlarının yapılması gerekiyor. Policy tanımı için "**Policy&Objects -> Firewall Policy**" yolu takip edilmelidir. Burada kullanım amacına göre Policy tek yönlü veya çift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



SSL VPN üzerinden bağlanacak kullanıcıların network çerisindeki kaynaklarla karşılıklı olarak haberleşebilmeleri için aynı Policy'nin tersi de oluşturulmalıdır (Policy çift yönlü yazılmalıdır).

- 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).



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

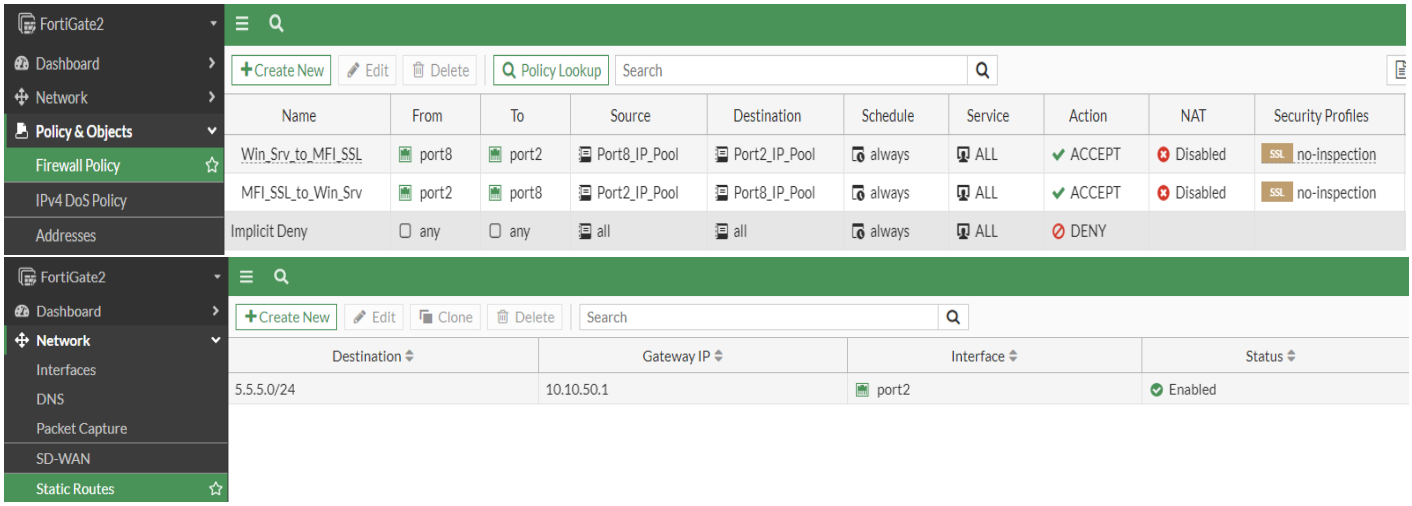
```
FortiGate1 (policy) # edit 10
new entry '10' added

FortiGate1 (10) # set name Win_Srv_to_MFI_SSL

FortiGate1 (10) # set srcintf ssl.root

FortiGate1 (10) # set dstintf port2

FortiGate1 (10) # set srcaddr SSLVPNAddr-1

FortiGate1 (10) # set groups SSLGroup1

FortiGate1 (10) # set dstaddr WinServ-1

FortiGate1 (10) # set action accept

FortiGate1 (10) # set schedule always

FortiGate1 (10) # set service ALL

FortiGate1 (10) # next
```

```
FortiGate1 (policy) # edit 11
new entry '11' added

FortiGate1 (11) # set name MFI_SSL_to_Win_Srv

FortiGate1 (11) # set srcintf port2

FortiGate1 (11) # set dstintf ssl.root

FortiGate1 (11) # set srcaddr WinServ-1

FortiGate1 (11) # set dstaddr SSLVPNAddr-1

FortiGate1 (11) # set action accept

FortiGate1 (11) # set schedule always

FortiGate1 (11) # set service ALL

FortiGate1 (11) # end
```


```
FortiGate1 # config router static

FortiGate1 (static) # edit 1

FortiGate1 (1) # set dst 10.10.10.1/24

FortiGate1 (1) # set gateway 10.10.50.2

FortiGate1 (1) # set device port2

FortiGate1 (1) # end
```

Son adımda eğer ki ulaşması gereken kaynak farklı bir network üzerinde ise bu durumda Static Route tanımı da yapılması gerekiyor. Uygulama yatığımız topolojide erişilmesi gereken kaynak Fortigate2 üzerinde tanımlı olduğu için Gortigate1 üzerinde hedef ip adresi Windows-Server'ın bulunduğu network olan paketlerin Fortigate2'ye gönderilmesi için Static Route tanımı yapılıyor.

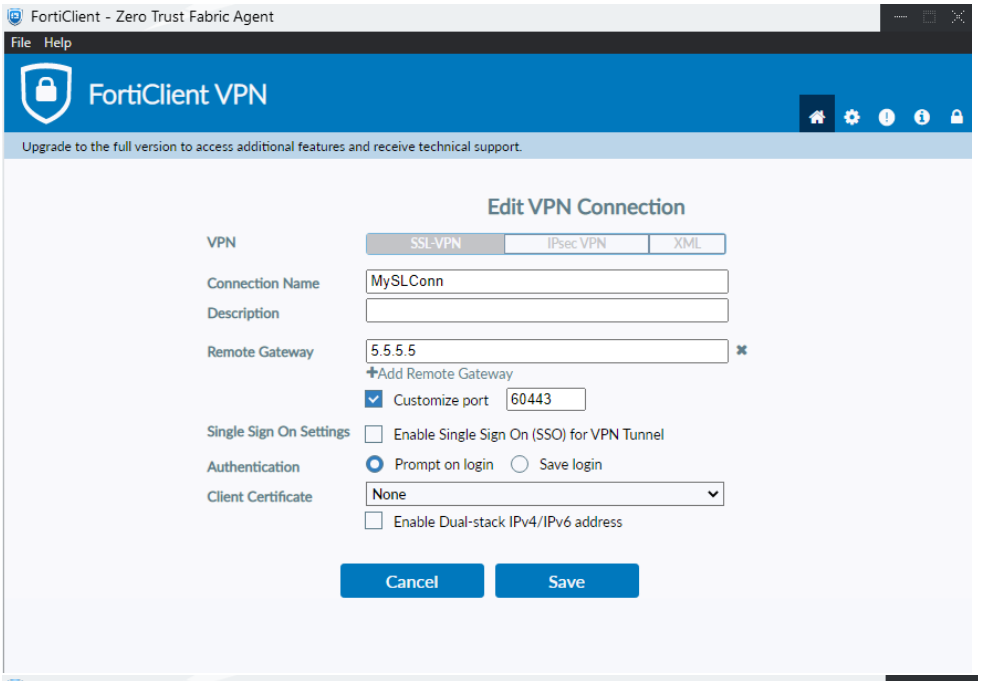
- SSL VPN kullanıcısının Windows-Server'a erişebilmesi için benzer şekilde Fortigate2 üzerinde de Static route ve Policy tanımlarının yapılması gerekiyor (**ÖRNEK KONFİGÜRASYONLARI "Kullanılan Komutlar" KISMINDA BULABİLİRSİN**).

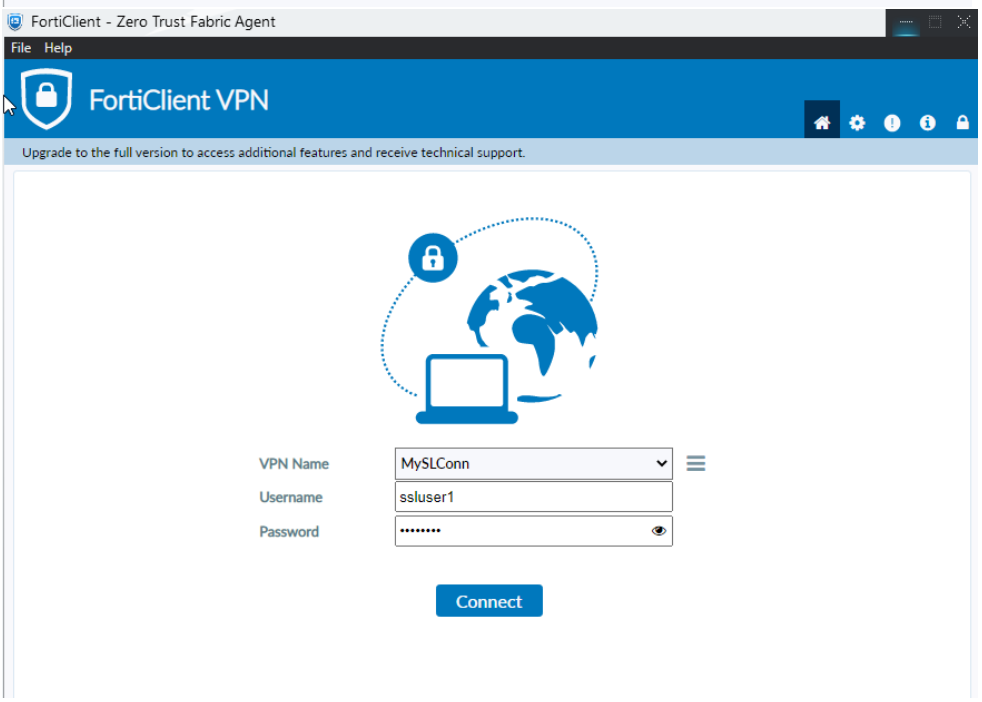


Artık FortiClient uygulamasını VPN olmak istenen istemci üzerine kurduktan sonra SSL-VPN Settings kısmında belirlenen WAN ip adresi ve port bilgilerini ayarlayıp kullanıcı adı ve parola bilgilerini girdikten sonra VPN bağlantısı sağlanabilir.

Bu süreçte karşılaşılan birkaç problemi listeleyecek olursak;

- İlk ayar sürecinde “Costumize Port” kısmında belirtilen port numarasını algılamayabiliyor. Bu durumda bağlantı %1’de kalıyor.
- Kullanıcı adı veya parola bilgisi hatalıysa %48’de takılıyor.
- “SSL-VPN Settings” kısmında kullanıcı grubu-Portal eşlemesi yerine doğrudan kullanıcı-Portal tanımı yapılmışsa %80’de takılı kalıyor.
- VPN olunduktan sonra hedef adrese erişemiyorsanız Tracert çekebilirsiniz. Bu durumda trafik tünele girmiyorsa Portal tanımında “**Routing Address Override**” kısmınd hedef ip adresini eklememişsinizdir.





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 I2t.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