

## SSL VPN Kullanıcılarına Statik IP Atama

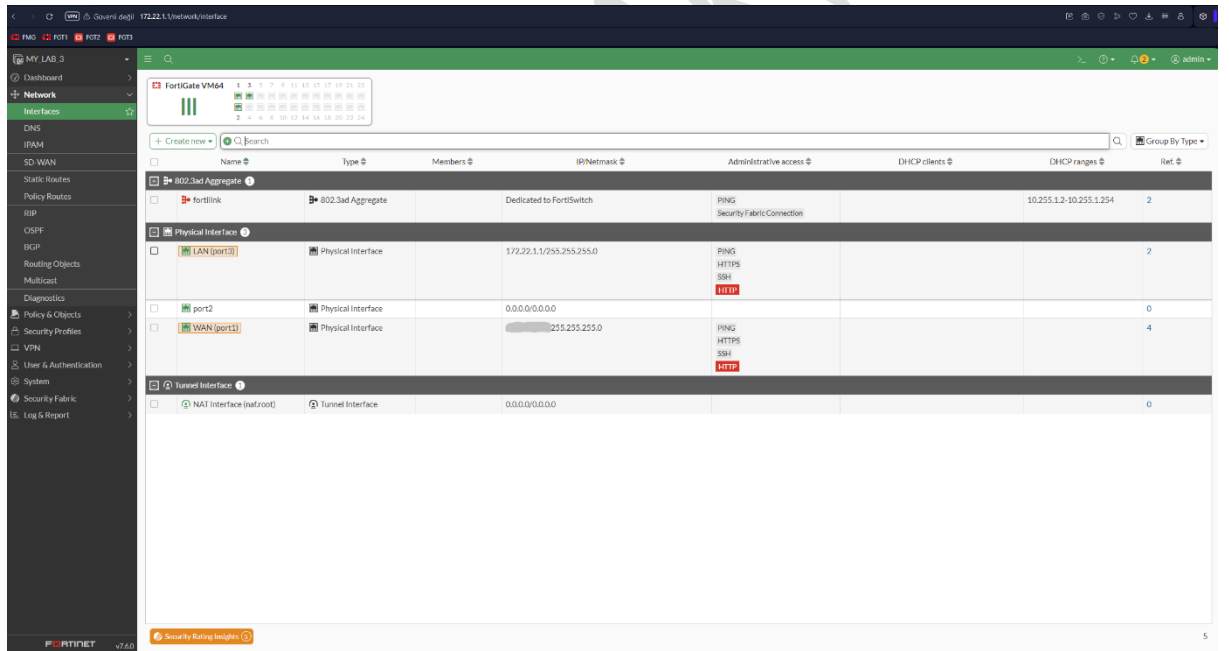
SSL VPN, uzak kullanıcıların şirket ağına güvenli bir şekilde erişmesini sağlayan kritik bir teknolojidir. Çoğu durumda, SSL VPN kullanıcılarına dinamik IP adresleri atanır. Ancak bazı durumlarda, belirli kullanıcıların sabit bir IP adresine ihtiyaç duyduğu senaryolar oluşur. Bu gereksinimlerin başında şunlar gelir:

- Ağda kullanıcı bazlı erişim kontrolü veya güvenlik politikalarının uygulanması.
- Belirli hizmetlere veya sistemlere yalnızca belirli IP adreslerinden erişim izni verilmesi.
- Trafik analizi veya loglama gereksinimleri.

Fortigate üzerinde SSL VPN kullanıcılarına statik IP atamanın adımları şu şekildedir:

### 1- Ön Hazırlık: Arayüzlerin Kontrolü

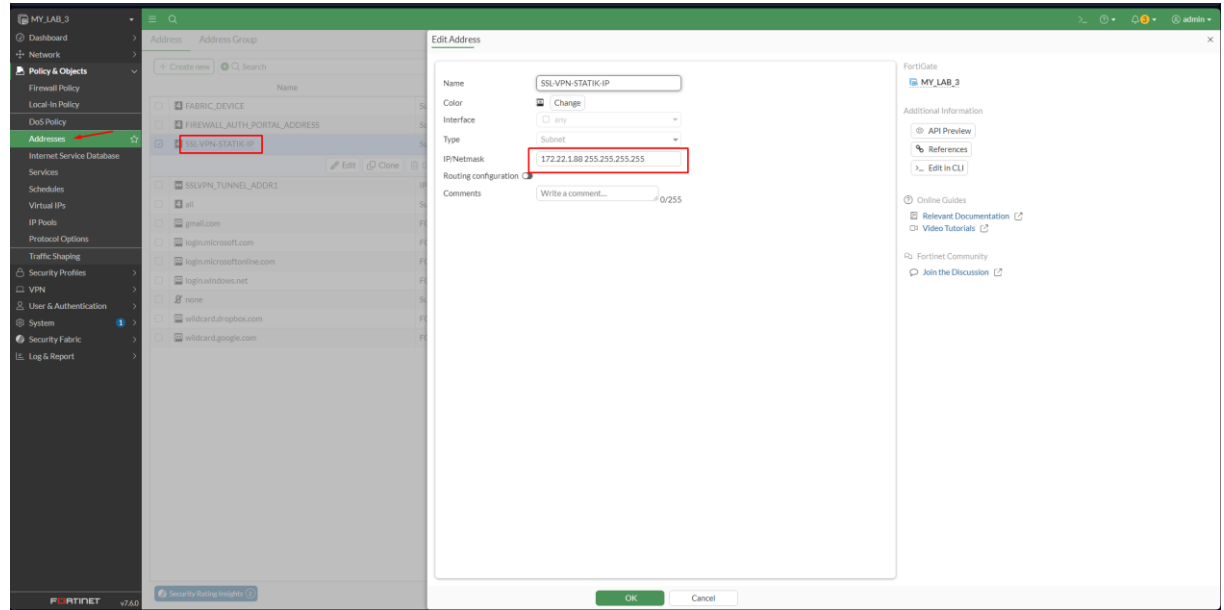
SSL VPN yapılandırmasına başlamadan önce, ağ altyapısındaki temel unsurları (LAN ve WAN arayüzleri gibi) gözden geçirin. Bu, yapılandırma sürecinde oluşabilecek sorunların daha hızlı çözülmesine yardımcı olacaktır.



## 2- SSL VPN için Adres Tanımlama

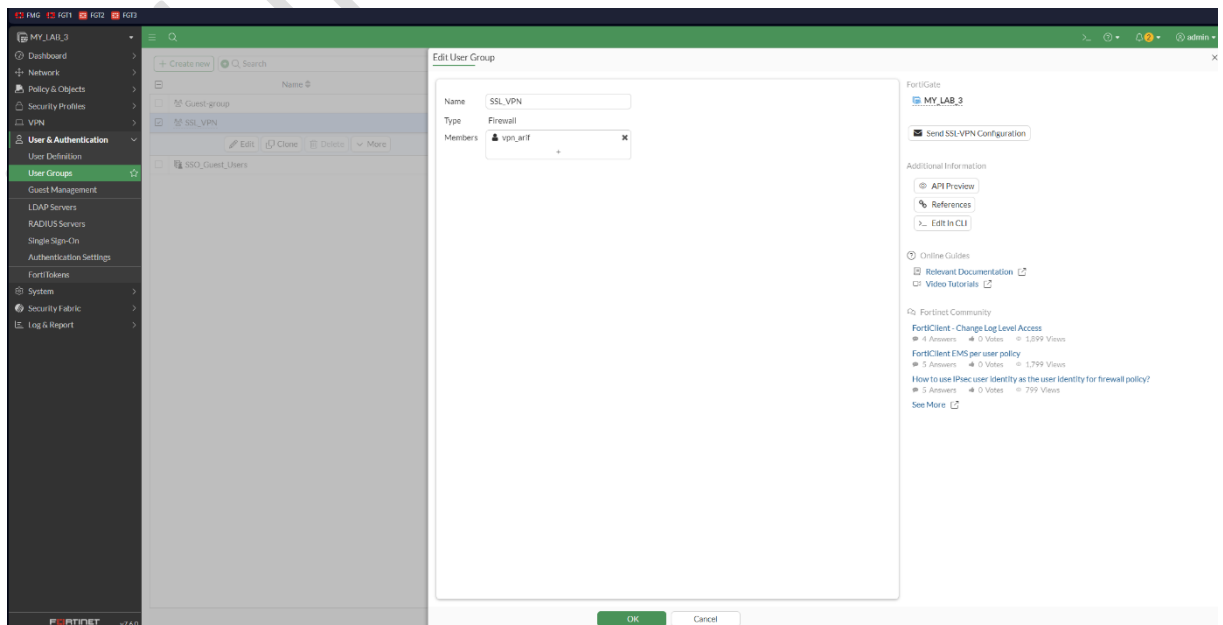
Fortigate üzerinde SSL VPN kullanıcılarına statik IP ataması yapmak veya belirli bir IP havuzunu tanımlamak için bir adres nesnesi oluşturmanız gereklidir.

Varsayılan olarak sistemde SSLVPN\_TUNNEL\_ADDR1 adres nesnesi bulunur. Ancak, örneğimizde kullanıcılar için özel bir IP havuzu tanımlamak adına yeni bir adres nesnesi oluşturuldu. Tek bir IP adresi almasını istiyoruz. Örneğimizde **172.22.1.88/32** Ip adresi verilmiştir. (Alternatif olarak bir IP aralığı (IP Range) da belirleyebilirsiniz.)



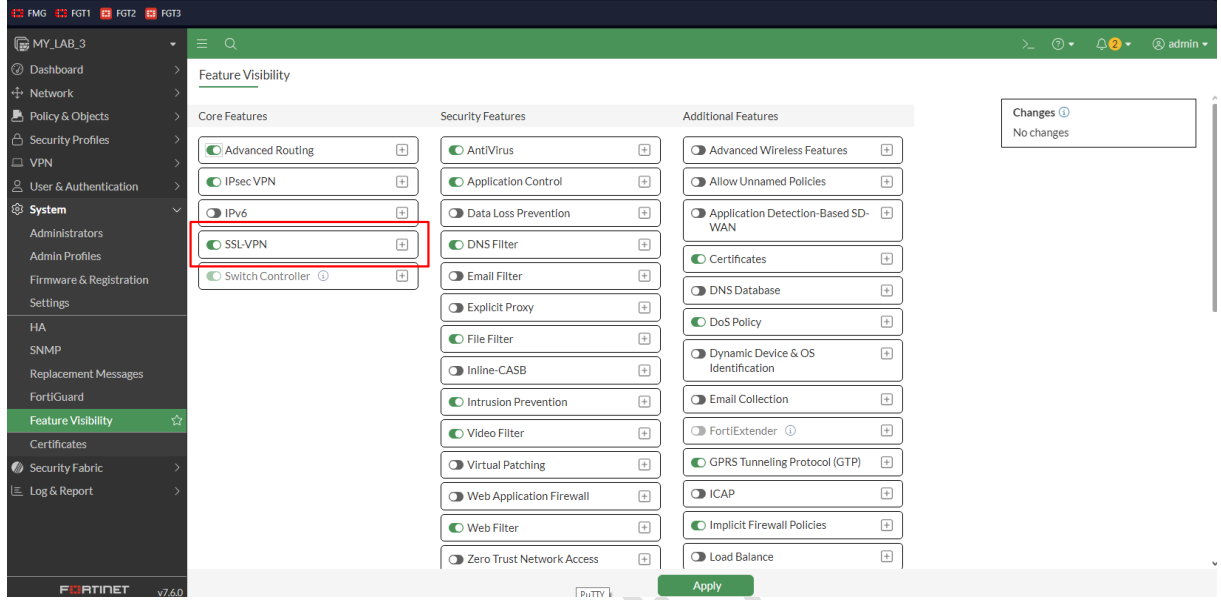
## 3- Kullanıcı ve Kullanıcı Grubu Oluşturma

Statik IP ataması ve erişim kontrolü yapılandırmalarının bir parçası olarak, Fortigate üzerinde bir kullanıcı ve bu kullanıcıyı içeren bir kullanıcı grubu oluşturmanız gerekir.



#### 4- Feature Visibility -> SSL-VPN aktifleřtirme

Fortigate cihazında bazı özellikler varsayılan olarak gizlenmiş olabilir. SSL VPN ile ilgili yapılandırmalara erişebilmek için bu özelliđi etkinleřtirmeniz gerekir.



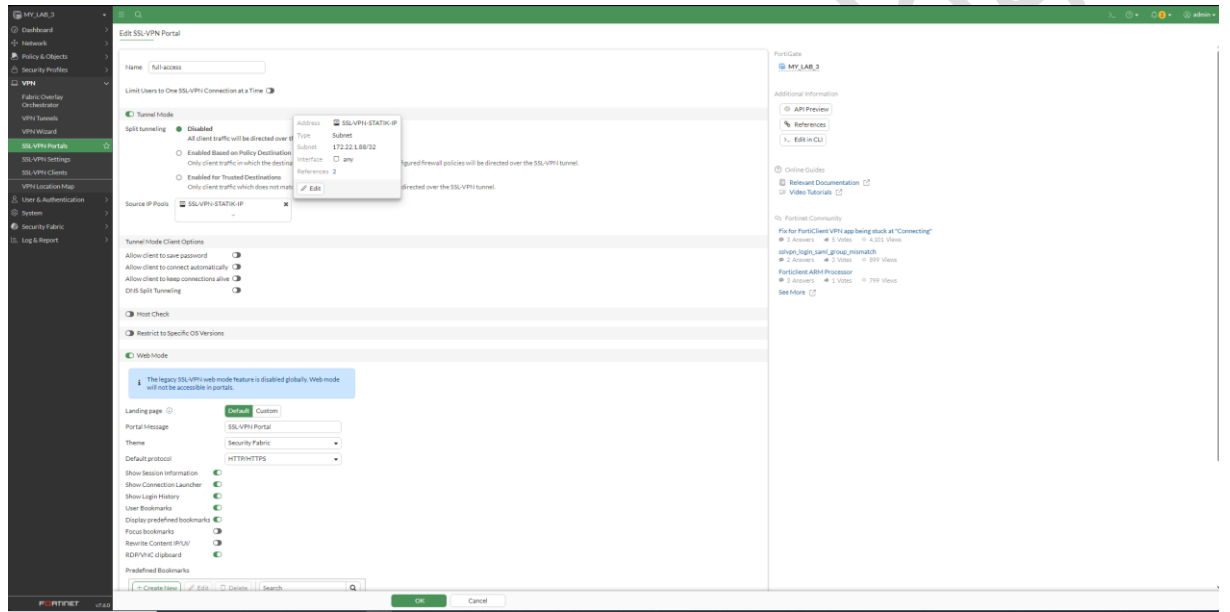
## 5- SSL VPN Portal Ayarları

Fortigate üzerinde SSL VPN Portal ayarları, VPN kullanıcılarına sağlanacak erişim türünü ve kaynakları yapılandırmak için kullanılır. Kullanıcılarınızın bağlantı sırasında ne tür erişim haklarına sahip olacağını belirleyebilirsiniz.

Varsayılan olarak üç portal bulunur:

- **full-access:** Tam erişim izni sağlar.
- **web-access:** Sadece web tabanlı erişim sunar.
- **tunnel-access:** VPN tünel bağlantısı için tasarlanmıştır.

Yeni bir portal oluşturabilir veya mevcut bir portalı düzenleyebilirsiniz.



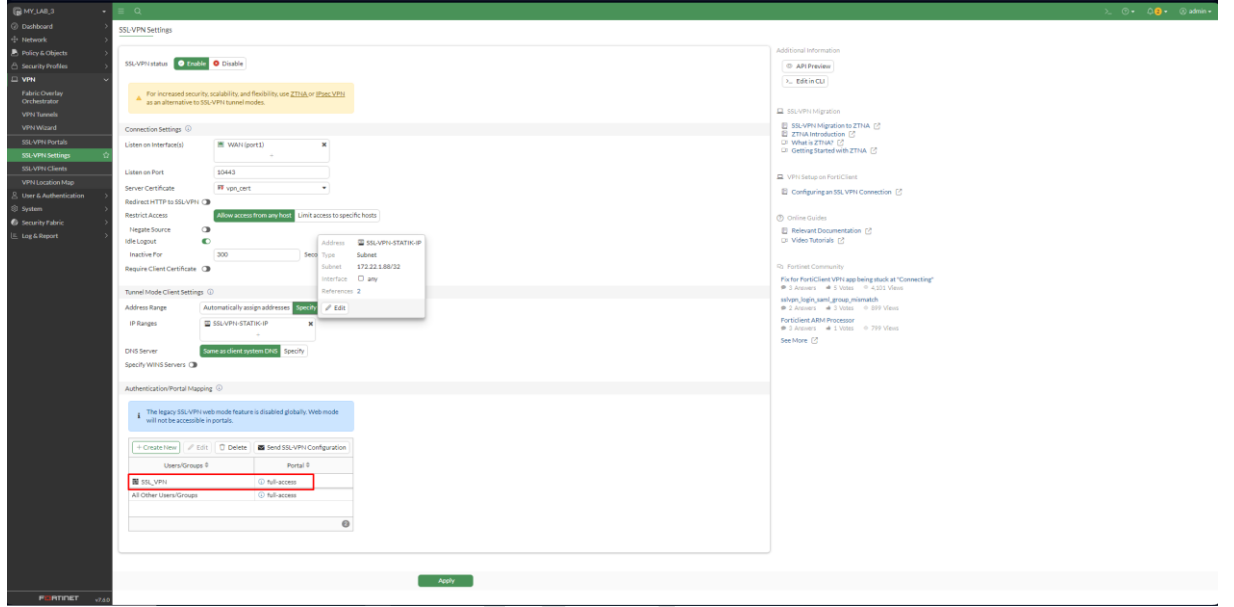
Portalın kullanıcı ihtiyaçlarına uygun şekilde yapılandırılması gerekir. Örnek bir yapılandırma:

- **Name :** Portal için bir isim belirleyin (örn. SSL\_VPN\_Static\_IP\_Portal ).
- **IP Pools:** Kullanıcılara atanacak IP havuzunu seçin (örneğin, daha önce oluşturduğumuz SSL-VPN-Static-IP).
- **Enable Split Tunneling:** Eğer işaretlenirse, yalnızca belirli ağlara VPN üzerinden erişim sağlanır, internet trafiği kullanıcı cihazından çıkar. İşaretlenmezse, tüm trafik VPN üzerinden yönlendirilir.
- **Web Mode:** Fortigate SSL VPN portalında Web Mode özelliği devre dışı bırakıldığında, SSL VPN tünel modu düzgün yapılandırılmış olsa dahi, kullanıcılar web tarayıcıları aracılığıyla portala erişmeye çalıştıklarında bir hata mesajı alırlar. Bu durum, Web Mode'un etkinleştirilmediği ortamda, web tabanlı erişimin sağlanamaması anlamına gelir.

**Not:** 'Limit Users to One SSL-VPN Connection at a Time' etkinleştirilirse, kullanıcı aynı anda bir SSL VPN bağlantısı yapabilir.

## 6- SSL VPN Settings (SSL VPN Ayarları)

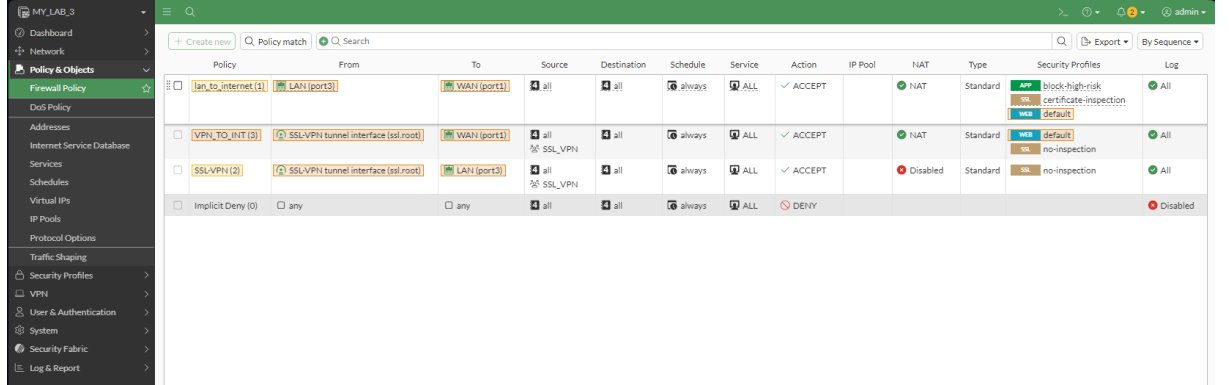
Fortigate üzerinde **SSL VPN Settings** bölümü, SSL VPN yapılandırmasındaki en önemli adımlardan biridir. Burada SSL VPN bağlantısının genel ayarlarını yapılandırabilir ve bağlantı için gerekli parametreleri belirleyebilirsiniz.



- **Listen on Interface:** SSL VPN bağlantısının dinleyeceği arayüz (genellikle WAN).
- **Listen on Port:** Varsayılan olarak 443 (HTTPS) portu kullanılır. Gerekirse değiştirilebilir.
- **IP Pool Seçimi:** Kullanıcılara atanacak IP adres havuzunu belirleyin.
- **Authentication Method:** Kullanıcı doğrulama yöntemini seçin (örneğin, Local User Database veya LDAP).
- **Portal Atama:** Kullanıcı veya kullanıcı gruplarına uygun portalı atayın.

## 7- Kural Oluşturma

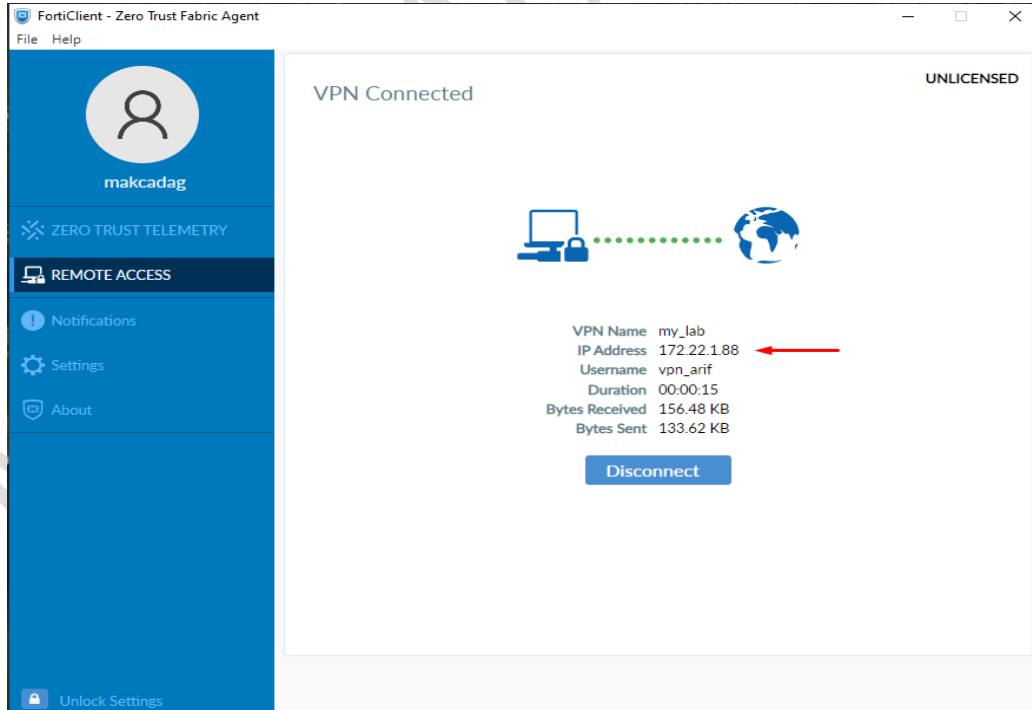
SSL VPN kullanıcılarının erişim ihtiyaçlarına göre hedef LAN belirlenerek bu doğrultuda uygun kurallar oluşturulur. Ayrıca, SSL VPN kullanıcılarının internet erişimini sağlamak ve diğer test senaryolarını gerçekleştirmek için de gerekli kurallar yapılandırılabilir.



Policy	From	To	Source	Destination	Schedule	Service	Action	IP Pool	NAT	Type	Security Profiles	Log
lan_to_internet (1)	lan (port3)	WAN (port1)	all	all	always	ALL	✓ ACCEPT		✓ NAT	Standard	block-high-risk certificate-inspection	All
VPN_TO_INT (3)	SSLVPN tunnel interface (ssl.root)	WAN (port1)	all	all	always	ALL	✓ ACCEPT		✓ NAT	Standard	no-inspection	All
SSLVPN (2)	SSLVPN tunnel interface (ssl.root)	LAN (port3)	all	all	always	ALL	✓ ACCEPT		Disabled	Standard	no-inspection	All
Implicit Deny (0)	any	any	all	all	always	ALL	✗ DENY					Disabled

## 8- Sonuç: Statik IP Ataması

Bu adımları tamamladıktan sonra, kullanıcılar Fortigate SSL VPN portalına bağlandıklarında, tanımladığınız statik IP havuzundan bir adres alacaktır. Böylece, kullanıcı bazlı erişim kontrolü ve diğer özel gereksinimlere uygun bir yapılandırma gerçekleştirilmiş olur.



Kaynakça: <https://docs.fortinet.com/document/fortigate/7.6.0/administration-guide/371626/ssl-vpn>