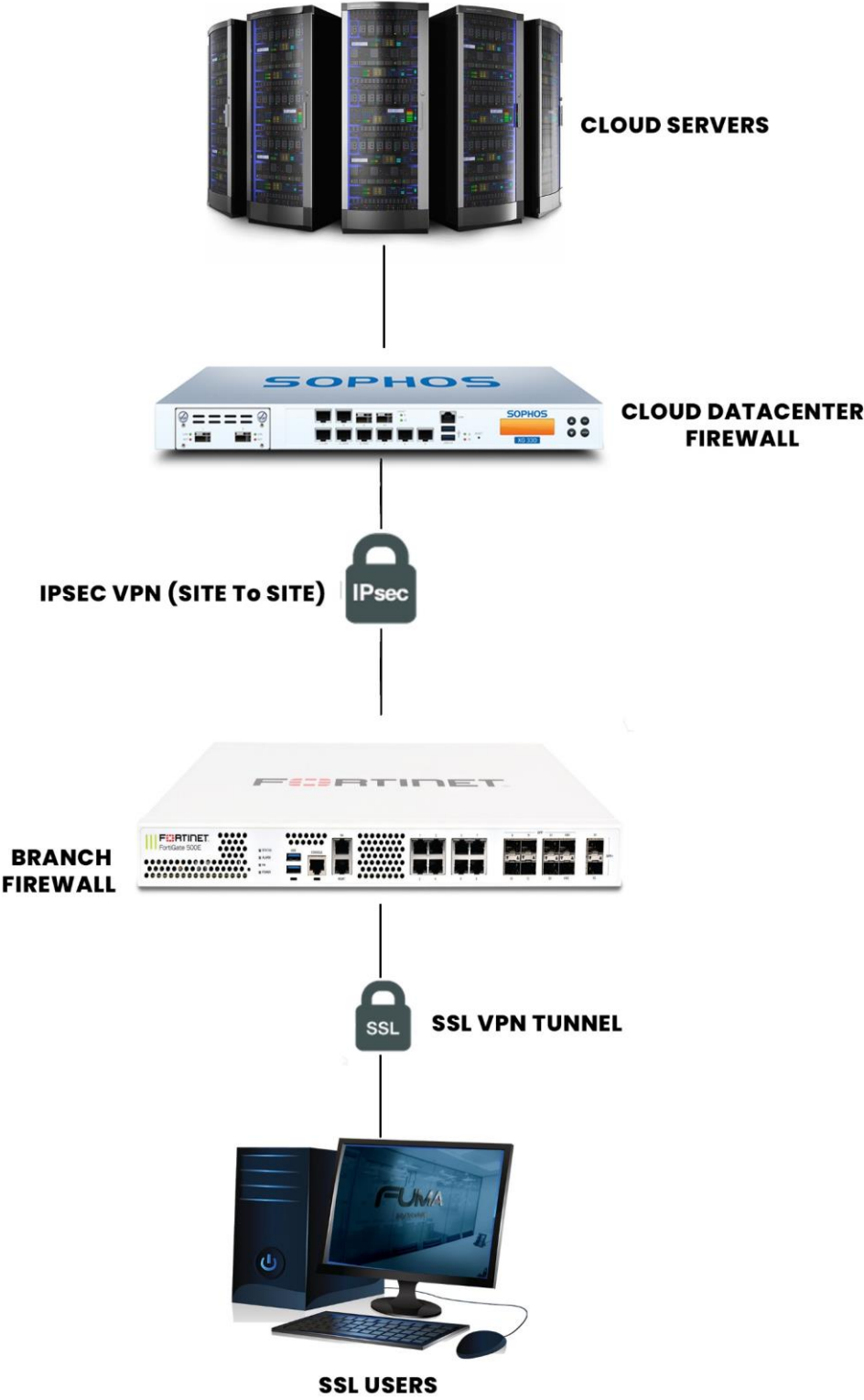
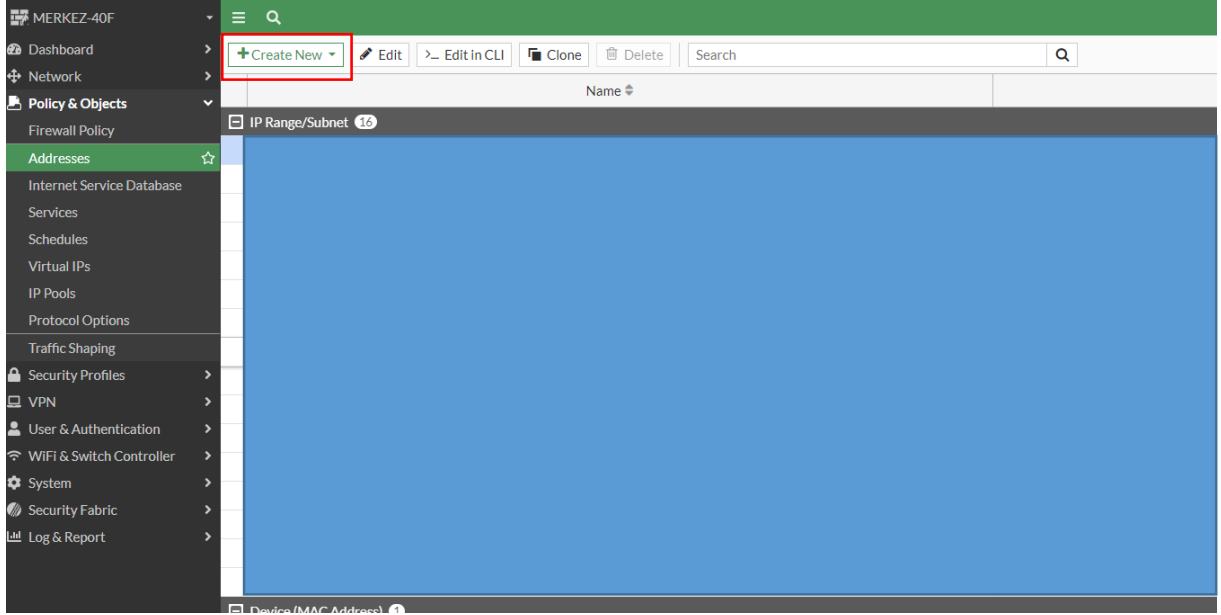


SSL VPN TO IPSEC VPN



İşlemlerimize ilk olarak firewall üzerinde adresses tanımlamaları yaparak başlıyoruz. Firewall ana menüsünden “policy & objects” altından “Adresses” seçeneğine tıklıyorum. Karşıma gelen menüden “create new” butonuna tıklıyorum.



Karşıma gelen menüden adresimize isim veriyorum ve ilgili network tanımlamamı yapıyorum.

Name	CLOUD
Color	Change
Interface	<input type="checkbox"/> any
Type	Subnet
IP/Netmask	<div></div>
Static route configuration	<input type="checkbox"/>
Comments	Write a comment... 0/255

Aynı işlemleri ne kadar network varsa yada adres varsa tekrarlıyorum.

Sonraki adımda merkez ile cloud arasındaki IPSEC bağlantımı tamamlıyorum.

MERKEZ-40F

Dashboard

Network

Policy & Objects

Security Profiles

VPN

IPsec Tunnels

IPsec Wizard

IPsec Tunnel Template

SSL-VPN Portals

SSL-VPN Settings

SSL-VPN Clients

VPN Location Map

User & Authentication

WiFi & Switch Controller

System

Security Fabric

Log & Report

Name: MERKEZ To CLOUD

Comments: Comments 0/255

Network Edit

Remote Gateway : Static IP Address [Redacted], Interface : wan

Authentication Edit

Authentication Method : Pre-shared Key

IKE Version : 2

Phase 1 Proposal Edit

Algorithms : AES256-SHA256

Diffie-Hellman Groups : 14, 5

Phase 2 Selectors

Name	Local Address	Remote Address	
MERKEZ To CLOUD	192.168.2.0/255.255.255.0	10.80.90.0/255.255.255.0	Add Edit Delete

Sonraki adımda IPSEC bağlantım için IPV4 kurallarımı çapraz şekilde oluşturuyorum.

MERKEZ-40F

Dashboard

Network

Policy & Objects

Firewall Policy

Addresses

Internet Service Database

Services

Schedules

Virtual IPs

IP Pools

Protocol Options

Traffic Shaping

Security Profiles

VPN

User & Authentication

WiFi & Switch Controller

System

Security Fabric

Log & Report

Create new Edit Delete Policy lookup Search

Name	From	To	Source	Destination
Lan to Cloud	Lan	MERKEZ To CLOUD	Merkez	CLOUD
Cloud To Lan	MERKEZ To CLOUD	Lan	CLOUD	Merkez

Implicit

Sonraki adımda ilgili IPSEC bağlantım için statik route tanımlaması gerçekleştiriyorum.

Destination	Gateway IP	Interface	Status
0.0.0.0	818.73.149	INTERNET (wan)	Enabled
192.168.1.0/24		MERKEZ-TO-MUKR	Enabled
10.10.10.0/24		MERKEZ To CLOUD	Enabled
		MERKEZ-TO-SD-WAN	Enabled
		Blackhole	Enabled
		MERKEZ To CLOUD	Enabled

Arayüz IPSEC Monitor ü kontrol ettiğimde bağlantım başarılı şekilde sağlandığını teyit ediyorum.

Name	Remote C
Site to Site - FortiGate 2	
Custom 1	
MERKEZ To CLOUD	

İlgili adımları tamamladıktan sonra ssl vpn için SSL VPN portalımı yapılandırıyorum.

SSL VPN Portal

Name: full-access

Limit Users to One SSL-VPN Connection at a Time: ☒

Tunnel Mode

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

☐ Enabled Based on Policy Destination
Only client traffic to 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.

Source IP Pools:

Tunnel Mode Client Options

Allow client to save password: ☐

Allow client to connect automatically: ☐

Allow client to keep connections alive: ☐

DNS Split Tunneling: ☐

Host Check

☐ Restrict to Specific OS Versions

Web Mode

Landing page:

Portal Message:

Theme:

Show Session Information: ☒

Show Connection Launcher: ☒

Show Login History: ☒

User Bookmarks: ☒

Rewrite Content IP/UI: ☒

RDP/VNC clipboard: ☒

Predefined Bookmarks

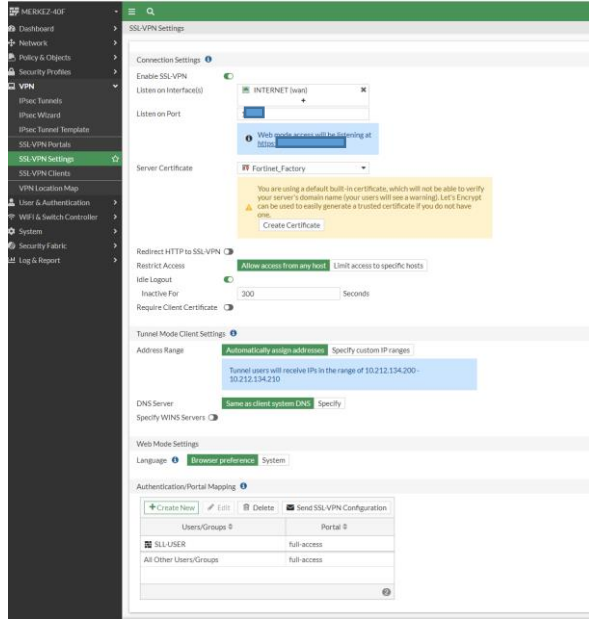
Name	Type	Location	Description
No results			

FortiClient Download

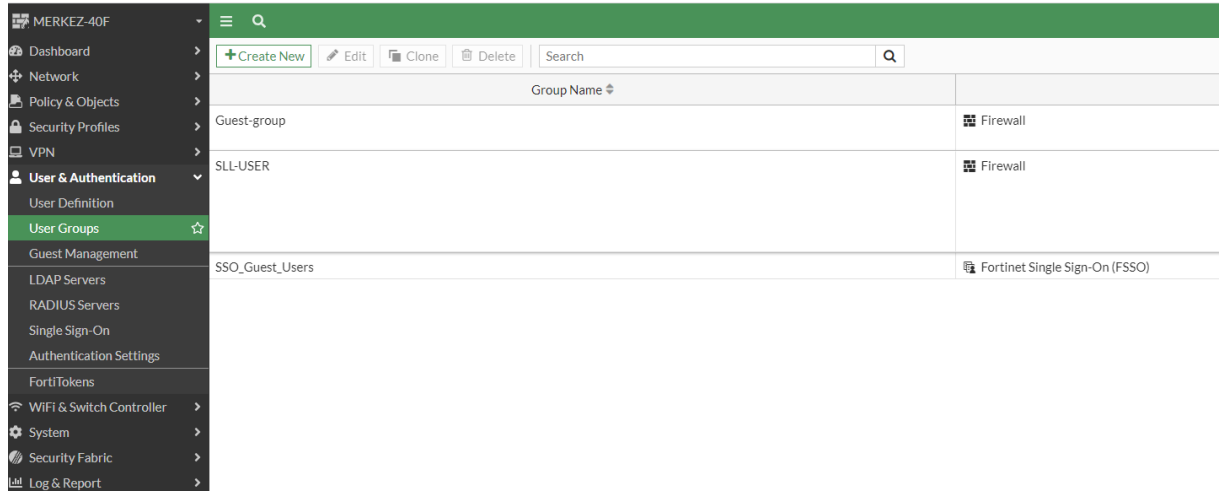
Download Method:

Customize Download Location:

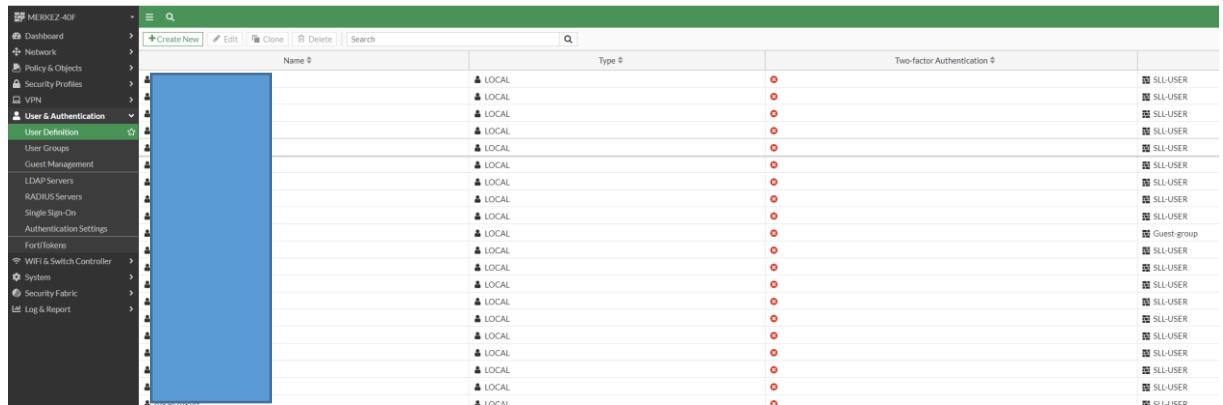
Sonraki adımda SSL ayarlarımı yapılandırıyorum.



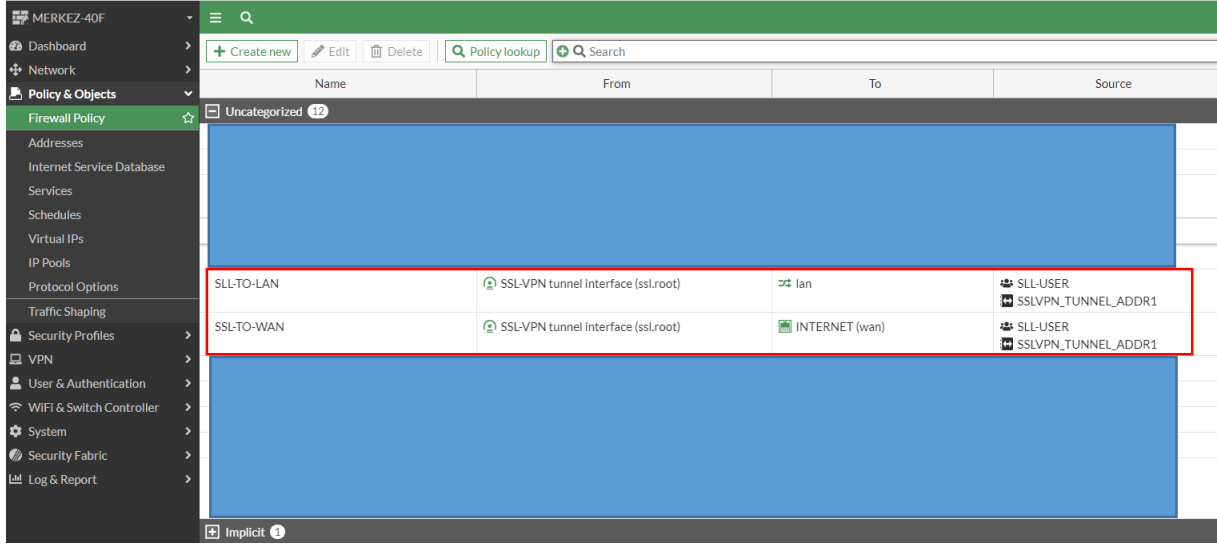
SSL VPN için kullanıcı gruplarımı oluşturun.



Sonraki adımda kullanıcıları oluşturup ilgili gruplara atıyorum.

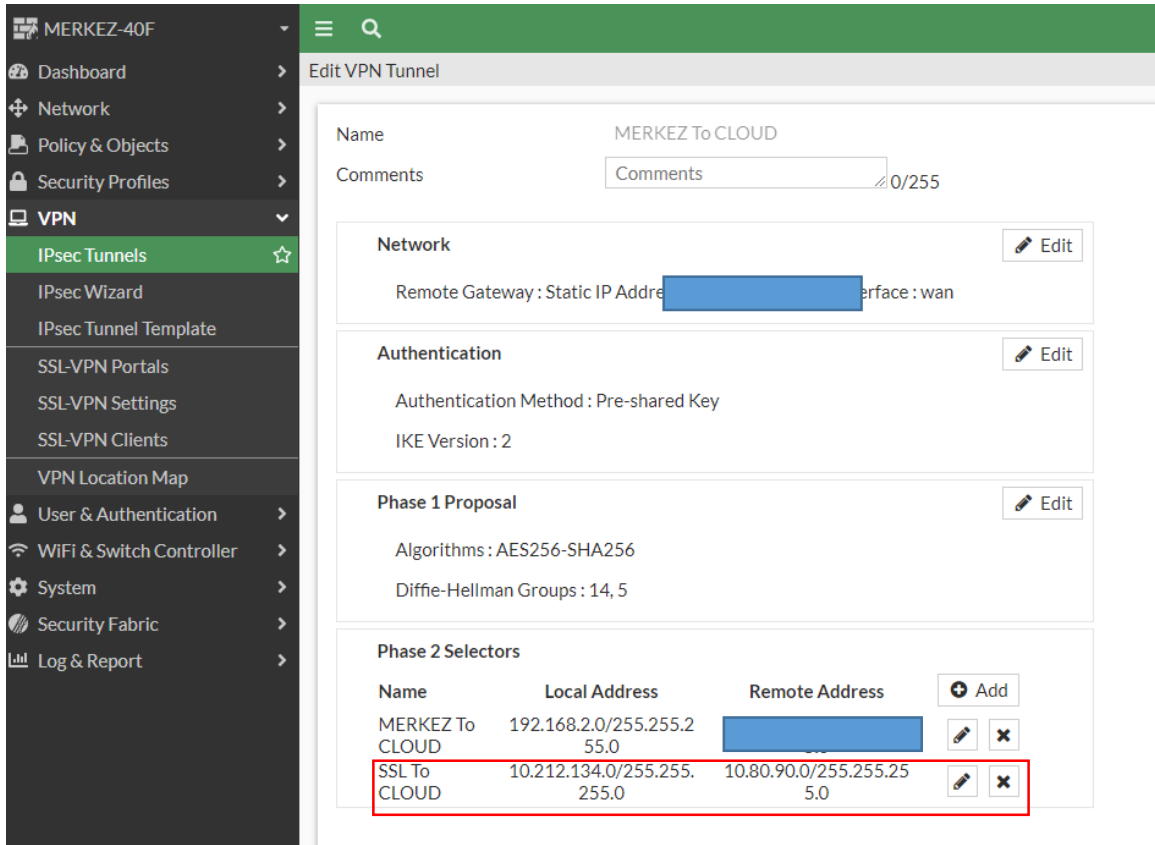


Sonraki adımda SSL Kullanıcılarım için local ve internete çıkış kuralları oluştuyorum.



Böylece SSL VPN kurulumumuz tamamlanmış oldu. Sonrasında SSL VPN kullanıcıların IPSEC VPN üzerinden CLOUD tarafındaki sunucuya ulaşması için ilgili yapılandırmama geçiyorum.

İlk olarak SSL VPN network ü IPSEC cloud VPN phase 2 yapılandırması eklemekle başlıyorum.



SSL local networkü ekledikten sonra SSL kullanıcıların IPSEC CLOUD tarafına ulaşması için ilgili IPV4 kurallarımı yapılandırıyorum.

Merkez-40F

Dashboard

Network

Policy & Objects

Firewall Policy

Addresses

Internet Service Database

Services

Schedules

Virtual IPs

IP Pools

Protocol Options

Traffic Shaping

Security Profiles

VPN

User & Authentication

WiFi & Switch Controller

System

Security Fabric

Log & Report

Edit Policy

Name: SSL To CLOUD

Incoming Interface: SSL-VPN tunnel interface (ssl.roo)

Outgoing Interface: MERKEZ To CLOUD

Source: Guest-group, SSL-USER

Destination: CLOUD

Schedule: always

Service: ALL

Action: ACCEPT

Firewall/Network Options

NAT: disabled

Protocol Options: default

Security Profiles

AntiVirus: disabled

Web Filter: disabled

DNS Filter: disabled

Application Control: disabled

IPS: disabled

SSL Inspection: no-inspection

Logging Options

Log Allowed Traffic: disabled

Security Events: All Sessions

Comments: Write a comment... 0/1023

Enable this policy: checked

Kuralımı yazdıktan sonra SSL VPN networkünü CLOUD networküne yönlendirmek için static route oluşturuyorum.

Merkez-40F

Dashboard

Network

Interfaces

DNS

IPAM

FortiExtenders

SD-WAN

Static Routes

Diagnostics

Policy & Objects

Security Profiles

VPN

User & Authentication

WiFi & Switch Controller

System

Security Fabric

Log & Report

Edit Static Route

Destination: Subnet

Interface: MERKEZ To CLOUD

Administrative Distance: 10

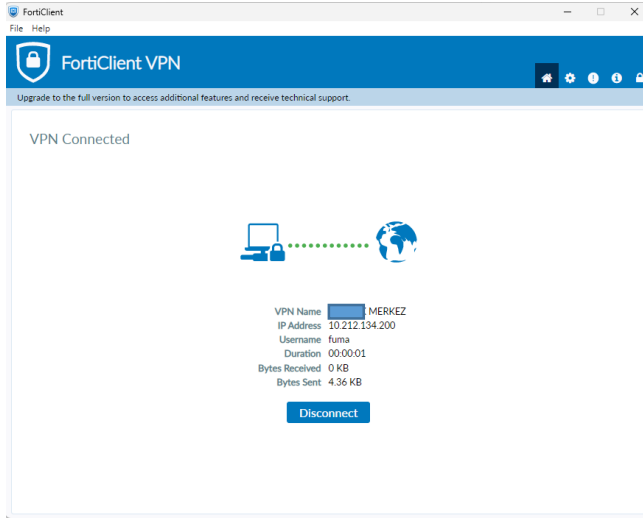
Comments: Write a comment... 0/255

Status: Enabled

Advanced Options

Tüm ayarlarımı tamamladıktan sonra testimi gerçekleştiriyorum.

Forticlient ile SSL VPN bağlantımı sağlıyorum.



Sonrasında CLOUD networküne ping atıyorum. Ve bağlantımın başarılı olduğunu teyit ediyorum.

```
C:\Windows\system32\cmd.e  X  +  v
Microsoft Windows [Version 10.0.22621.1848]
(c) Microsoft Corporation. Tüm hakları saklıdır.

C:\Users\Utekin>ping 10.80.90.1

Pinging 10.80.90.1 with 32 bytes of data:
Reply from 10.80.90.1: bytes=32 time=31ms TTL=62
Reply from 10.80.90.1: bytes=32 time=29ms TTL=62
Reply from 10.80.90.1: bytes=32 time=32ms TTL=62
Reply from 10.80.90.1: bytes=32 time=29ms TTL=62

Ping statistics for 10.80.90.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 29ms, Maximum = 32ms, Average = 30ms

C:\Users\Utekin>
```