
Fortinet Firewall

Amaç: Amacımız Sanal Cihazlar kullanarak Fortinet Firewall ile internet ağıımız için güvenli bir alan oluşturmak, gelen protokol isteklerini cihaz veya cihazlara yönlendirmek, misafir ağı oluşturmak ve farklı networkler arası bağlantı kurmak için VPN oluşturmak.

1-) Fortinet Konfigürasyonu

2-) İnternete Çıkmak

3-) Misafir Ağı

4-) Site to Site VPN

1-) Fortinet Konfigürasyonu

- Fortinet cihazımızda 2 adet network adaptörü bulunmaktadır. Adım 3'te oluşturacağımız misafir ağ'ına bağlanan kişilerde direk local ağımıza bağlanacaktır. Eğer misafir ağı farklı bir ağ olsun isterseniz ayrıca 1 network adaptörü daha eklemeliyiz.

Port1 internete çıkan kartımız olup, port2 local ağ kuracağımız kartımızdır. Konfigürasyon için şu komutlar girilir.

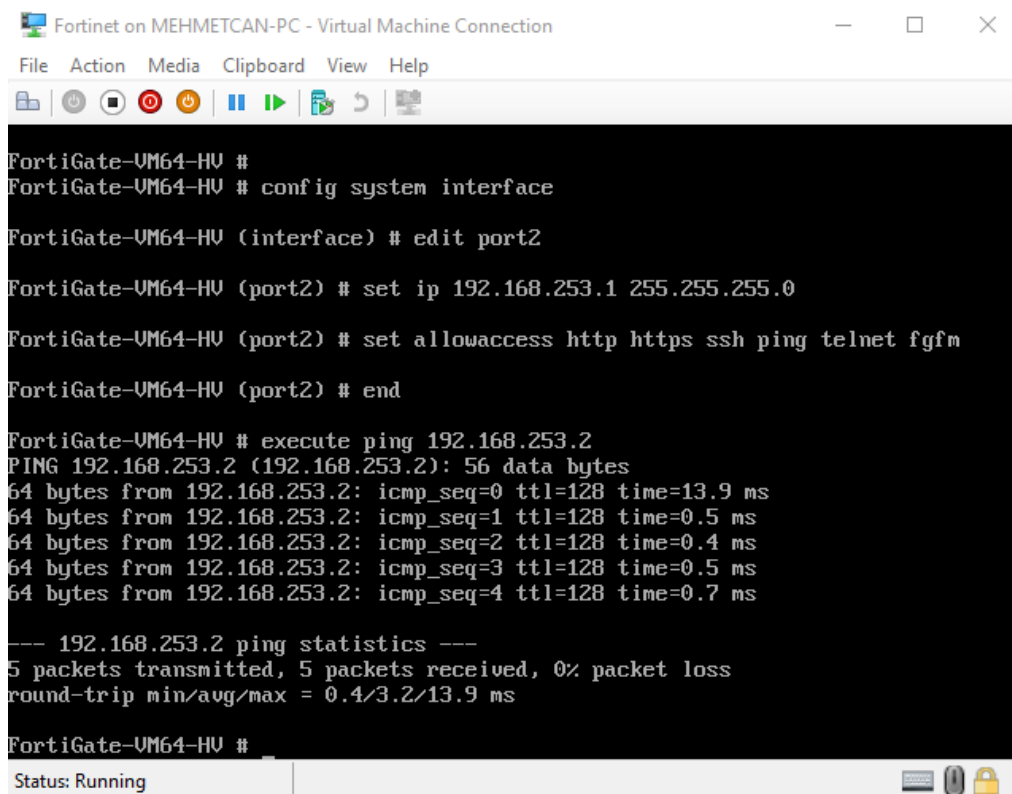
- config system interface
- edit port2
- set ip <local ip> <subnet mask>
- set allowaccess http https ssh ping telnet fgfm

Komutları girildikten sonra bilgisayardan fortinet arayüzüne bağlanmak için ilk olarak local ağın içinde olacak şekilde cihazımıza static IP vermeliyiz. Çünkü Fortinet'in otomatik DHCP konfigürasyonu yoktur, kendimiz yapacağız.

Cihazımıza 192.168.253.2 IP'sini verdikten sonra haberleşmenin sağlandığını görmek için Fortinet içinde şu komut girilir,

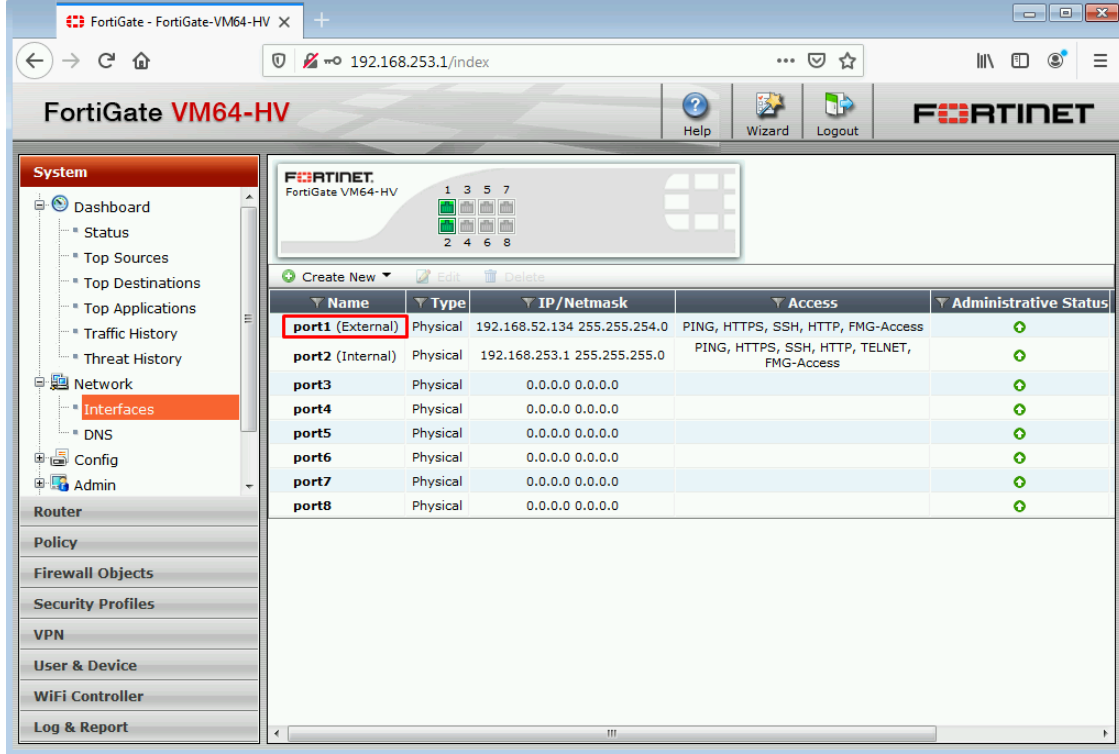
- execute ping <cihaz IP'si>

Haberleşme sağlandıktan sonra cihazdan bağlanılır.

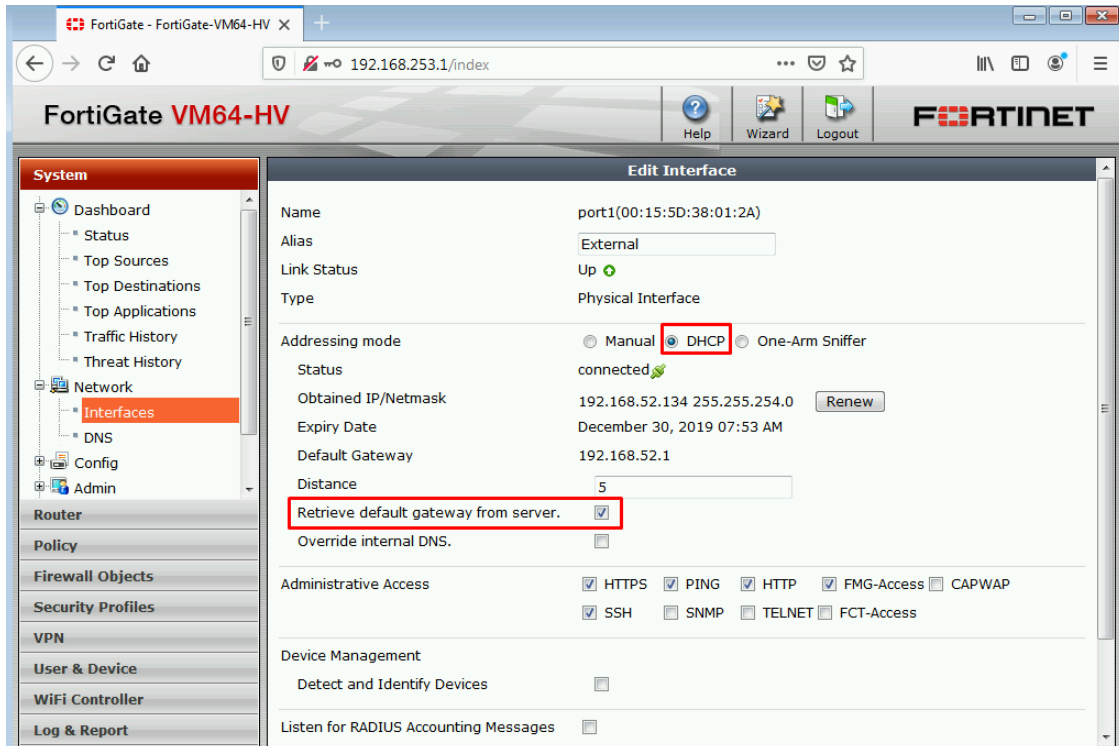


```
Fortinet on MEHMETCAN-PC - Virtual Machine Connection
File Action Media Clipboard View Help
FortiGate-VM64-HU #
FortiGate-VM64-HU # config system interface
FortiGate-VM64-HU (interface) # edit port2
FortiGate-VM64-HU (port2) # set ip 192.168.253.1 255.255.255.0
FortiGate-VM64-HU (port2) # set allowaccess http https ssh ping telnet fgfm
FortiGate-VM64-HU (port2) # end
FortiGate-VM64-HU # execute ping 192.168.253.2
PING 192.168.253.2 (192.168.253.2): 56 data bytes
64 bytes from 192.168.253.2: icmp_seq=0 ttl=128 time=13.9 ms
64 bytes from 192.168.253.2: icmp_seq=1 ttl=128 time=0.5 ms
64 bytes from 192.168.253.2: icmp_seq=2 ttl=128 time=0.4 ms
64 bytes from 192.168.253.2: icmp_seq=3 ttl=128 time=0.5 ms
64 bytes from 192.168.253.2: icmp_seq=4 ttl=128 time=0.7 ms
--- 192.168.253.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.4/3.2/13.9 ms
FortiGate-VM64-HU #
Status: Running
```

- Firewall IP'si ile arayüze giriş yaptıktan sonra internete çıkacak olan WAN adaptörümüzün ayarlamaları yapılır. Bunun için "System" altında "Network" → "Interfaces" tıklanır. İnternete bağlı olan adaptörümüzün portuna giriş yapılır.

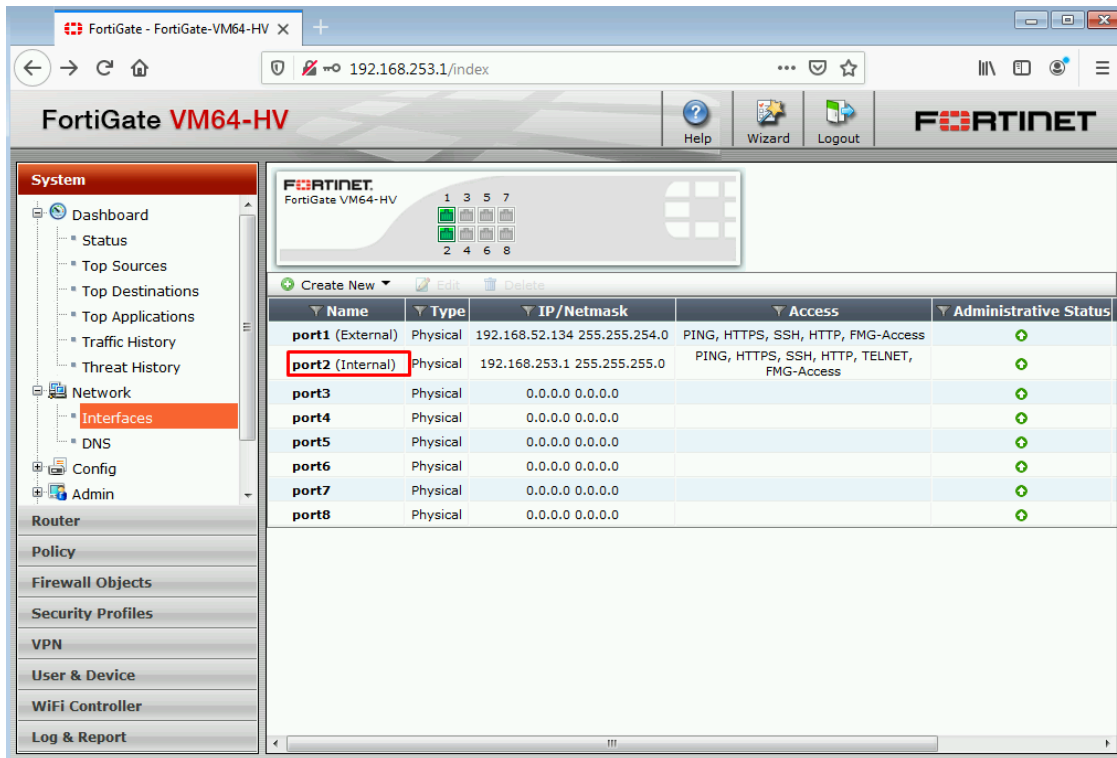


- "Addressing Mode" kısmı projemize göre DHCP olarak seçilir ve "Retrieve default gateway from server" tiklenir ve ayarlar kaydedilir.

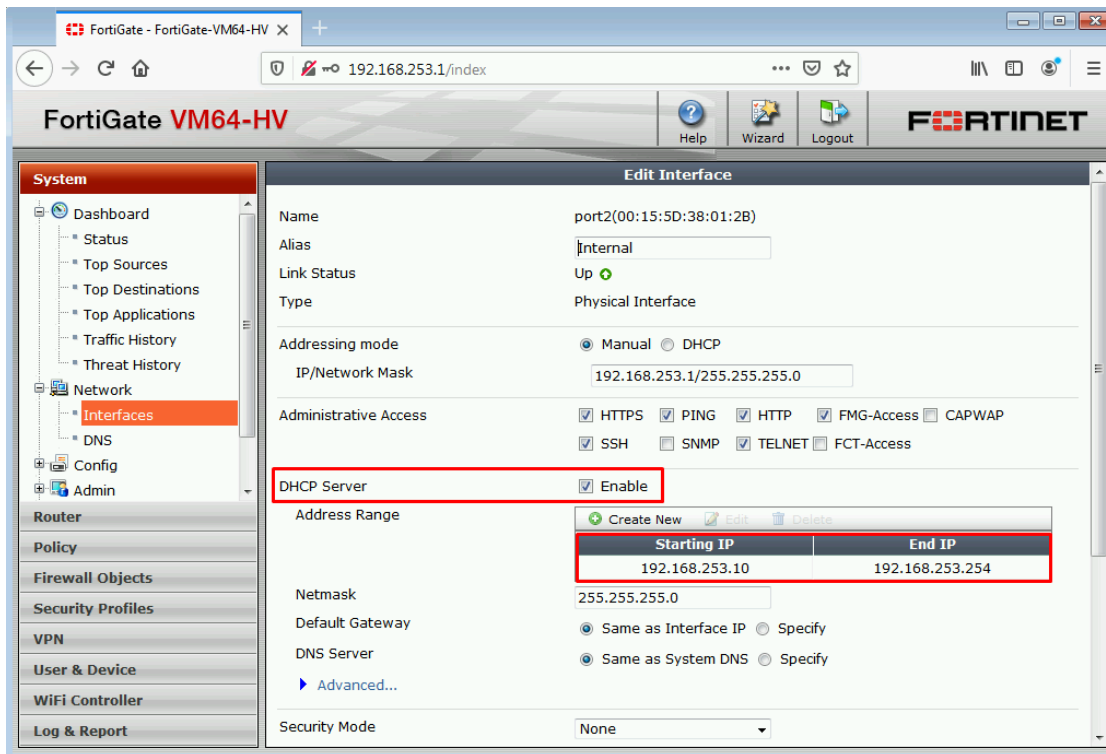


- Port1 IP almazsa firewall “reboot” edilir, ardından IP alındığı görülür.

Local ağımızın konfigürasyonu için port2’ye giriş yapılır.



- “DHCP Server” enable yapılır ve isteğe bağlı olarak dağıtılacak IP aralığı belirlenir. Ve Local ağımızın otomatik IP dağıtımı başlamıştır.



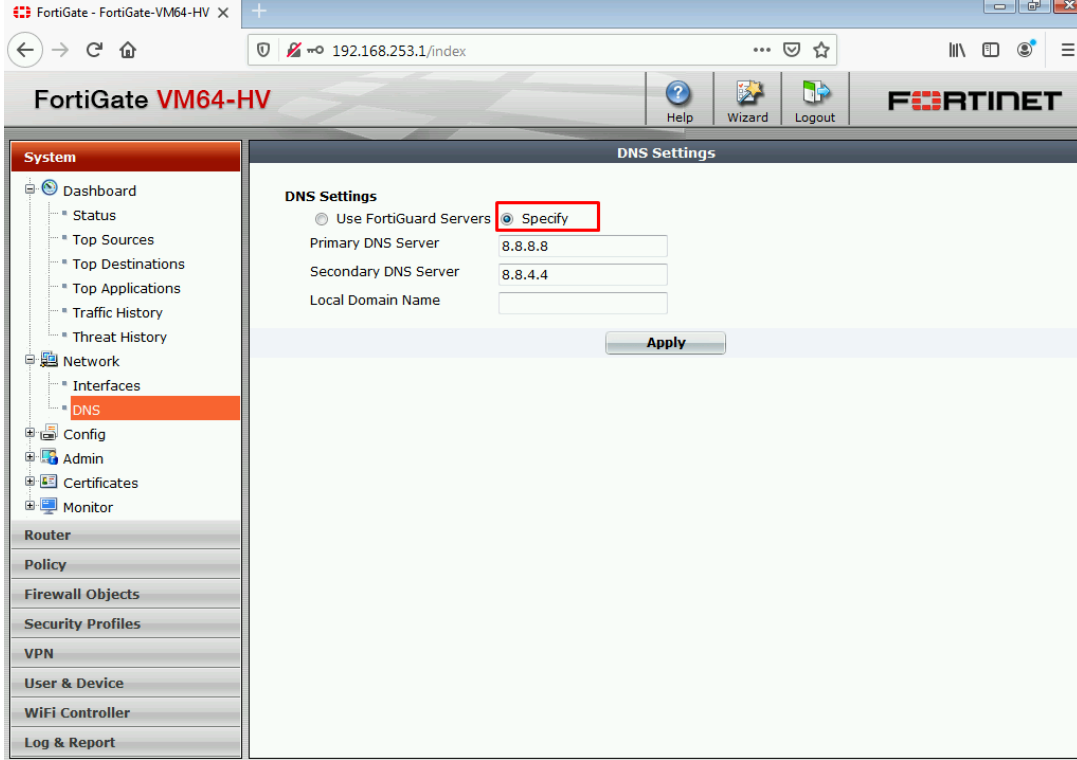
```
root@kali: ~
File Actions Edit View Help
root@kali: ~ x
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.253.10 netmask 255.255.255.0 broadcast 192.168.253.255
    inet6 fe80::215:5dff:fe38:120 prefixlen 64 scopeid 0x20<link>
    ether 00:15:5d:38:01:20 txqueuelen 1000 (Ethernet)
    RX packets 1019 bytes 139485 (136.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 876 bytes 70038 (68.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 12 bytes 552 (552.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 12 bytes 552 (552.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

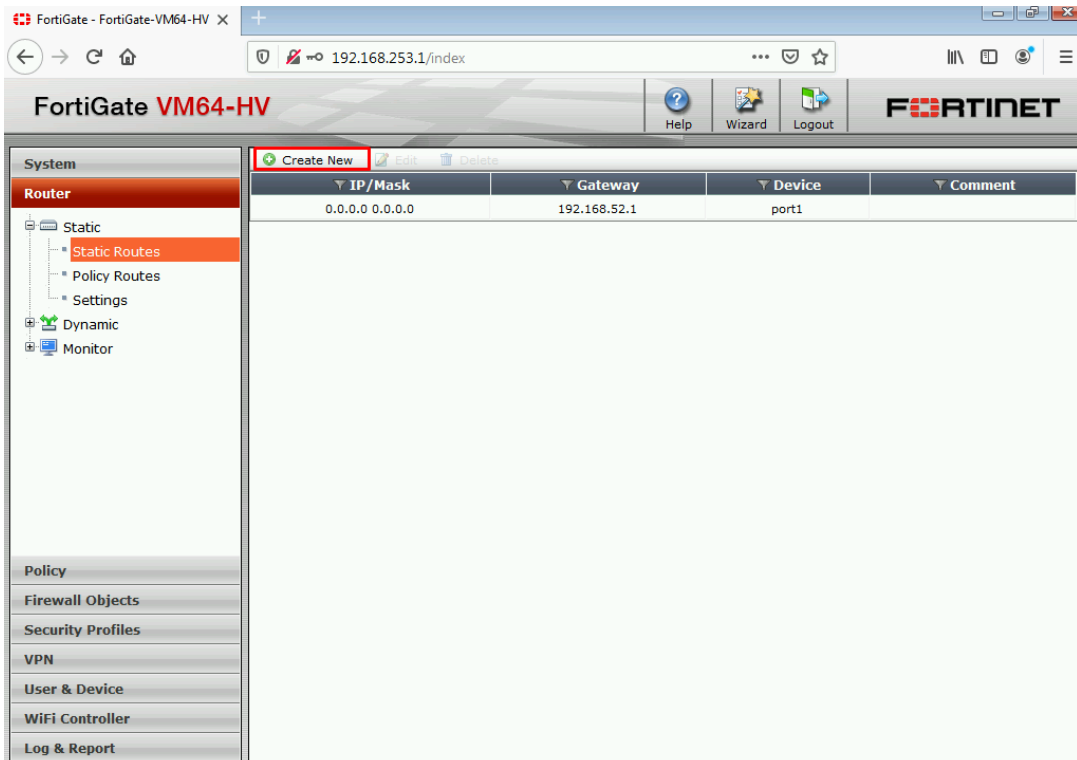
root@kali:~#
```

2-) İnternete Çıkmak

- DNS ayarları projeye göre ve duruma göre yapılandırılıp yapılandırılmayabilir. Biz burda Google'ın DNS adresini kullanacağız. Bunun için "System" → "Network" → "DNS" → "Specify" tiklenir ve Serverlar girilir.



- Ardından "Router" → "Static Routes" kısmından "Create New" tıklanır.



-
- The screenshot displays the FortiGate VM64-HV web interface. The top navigation bar includes the FortiGate logo, the device name 'FortiGate-VM64-HV', and buttons for Help, Wizard, and Logout. The left sidebar contains a navigation menu with the following items: System, Router (selected), Policy, Firewall Objects, Security Profiles, VPN, User & Device, WiFi Controller, and Log & Report. The main content area is titled 'Edit Static Route' and contains the following configuration fields:
- Destination IP/Mask: 0.0.0.0/0.0.0.0
 - Device: port1 (External) (highlighted with a red box)
 - Gateway: 192.168.52.1 (highlighted with a red box)
 - Distance: 10 (1-255, Default=10)
 - Priority: 0 (0-4294967295)
 - Comments: Write a comment... (0/255)
- At the bottom of the configuration area, there are 'OK' and 'Cancel' buttons.

-
- The screenshot shows the FortiGate VM64-HV web interface. The left sidebar contains a tree view with the following items: System, Router, Policy (highlighted), Monitor, Firewall Objects, Security Profiles, VPN, User & Device, WiFi Controller, and Log & Report. The main content area is titled 'Policy' and shows a table of existing policies. The table has columns: Seq.#, Source, Destination, Schedule, Service, Authentication, Action, AV, Web Filter, and Application Control. The table lists two policies: 'port2 (Internal) - port1 (External) (1 - 1)' and 'Implicit (2 - 2)'. The 'Create New' button is highlighted in the top left of the main area.

- “Incoming Interface : Local Ağımız”
- “Source Address : all”
- “Outgoing Interface : WAN”
- “Destination Address : all”
- “Schedule : always”
- “Service : ALL”
- “Action : ACCEPT” olarak ayarlanır.

“Enable NAT” işaretlenir ve Policy oluşturulur.

FortiGate - FortiGate-VM64-HV

192.168.253.1/index

FortiGate VM64-HV

Help Wizard Logout

System

Router

Policy

Policy

DoS Policy

Proxy Options

SSL/SSH Inspection

Monitor

Firewall Objects

Security Profiles

VPN

User & Device

WiFi Controller

Log & Report

Edit Policy

Policy Type: Firewall

Policy Subtype: Address

Incoming Interface: port2 (Internal)

Source Address: all

Outgoing Interface: port1 (External)

Destination Address: all

Schedule: always

Service: ALL

Action: ACCEPT

☒ Enable NAT

☒ Use Destination Interface Address ☐ Fixed Port

☐ Use Dynamic IP Pool

Click to add...

Logging Options

☐ No Log

☒ Log Security Events

☐ Log all Sessions

Security Profiles

Antivirus: OFF

Web Filter: OFF

Application Control: OFF

- Bu ayarlamalar ardından internete çıkmaktayız. Firewall güvenliği için oluşturduğumuz Policy'nin "Service" kısmı aşağıdaki gibi değiştirilir.

The screenshot displays the FortiGate VM64-HV web interface. The left sidebar shows the navigation menu with 'Policy' selected. The main content area is titled 'Edit Policy'. The 'Policy Type' is set to 'Firewall'. The 'Policy Subtype' is set to 'Address'. The 'Incoming Interface' is 'port2 (Internal)', 'Source Address' is 'all', 'Outgoing Interface' is 'port1 (External)', and 'Destination Address' is 'all'. The 'Schedule' is set to 'always'. The 'Service' field is highlighted with a red box, showing a list of services: HTTP, HTTPS, IMAP, DNS, PING, SSH, and TELNET. The 'Action' field is set to 'ACCEPT'. The 'Logging Options' section shows 'Log Security Events' selected.

Service	Action
HTTP	X
HTTPS	X
IMAP	X
DNS	X
PING	X
SSH	X
TELNET	X

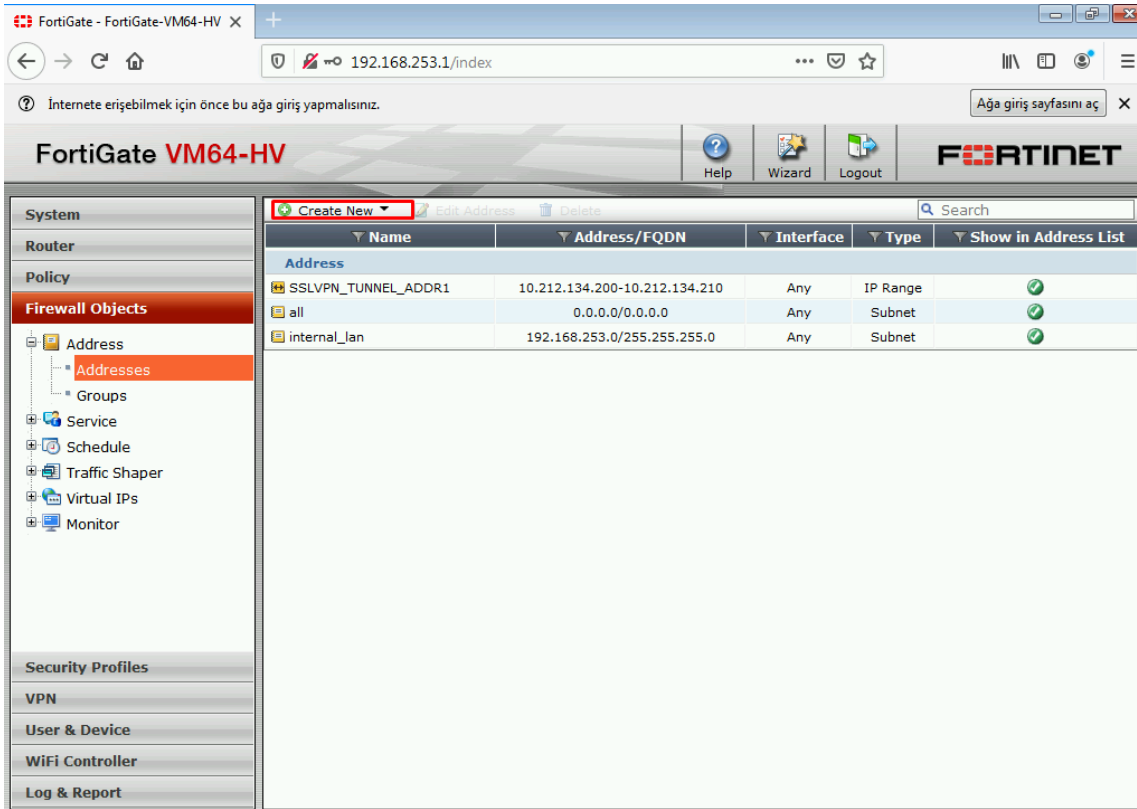
3-) Misafir Ağı

- Misafir ağı için local portumuza giriş yapıp “Security Mode” kısmından “Captive Portal” seçilir ve “User Groups” kısmından otomatik var olan “Guest-group” seçilir ve ayarlar kaydedilir.

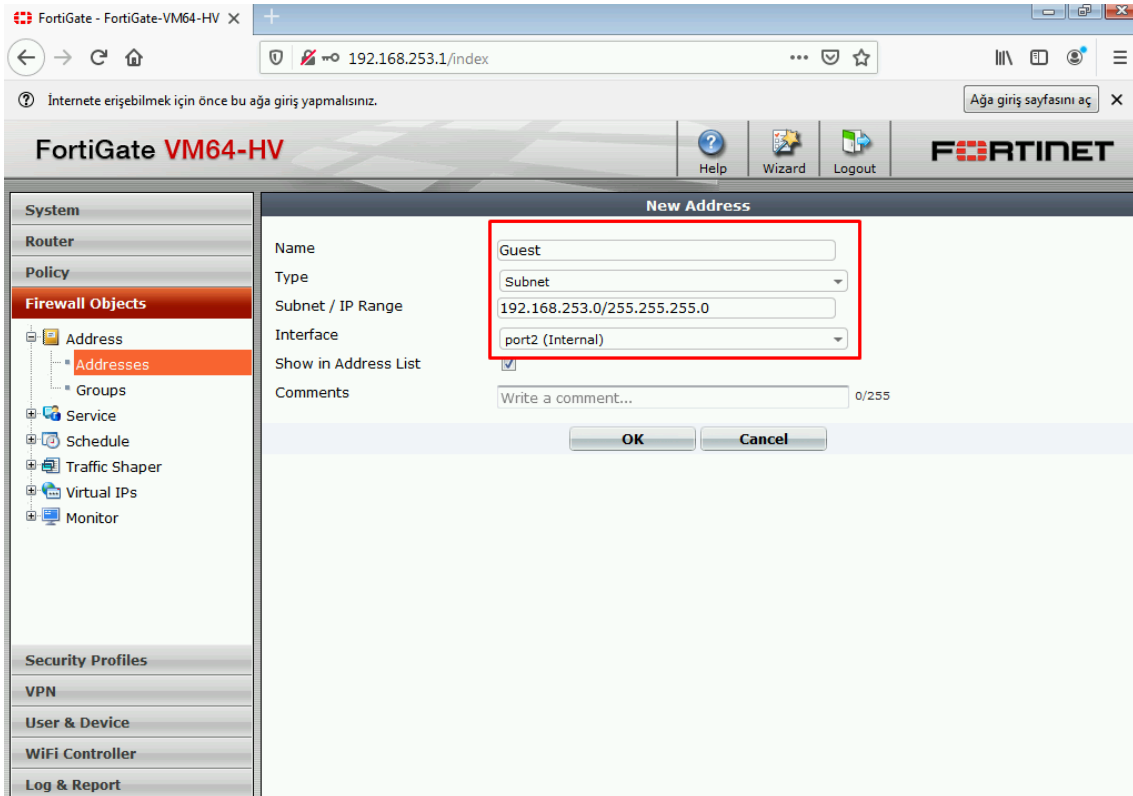
The screenshot displays the FortiGate VM64-HV web interface. The left sidebar shows the navigation menu with categories like System, Network, Router, Policy, Firewall Objects, Security Profiles, VPN, User & Device, WiFi Controller, and Log & Report. The 'Network' category is expanded, and the 'Interfaces' sub-category is selected. The main content area shows the 'Edit Interface' configuration page for the 'Internal' interface. The interface is set to 'Physical Interface' with a manual IP address of 192.168.253.1/255.255.255.0. The 'Security Mode' is set to 'Captive Portal' and the 'User Groups' are set to 'Guest-group'. The 'Advanced...' link is visible below the 'User Groups' field.

Starting IP	End IP
192.168.253.10	192.168.253.254

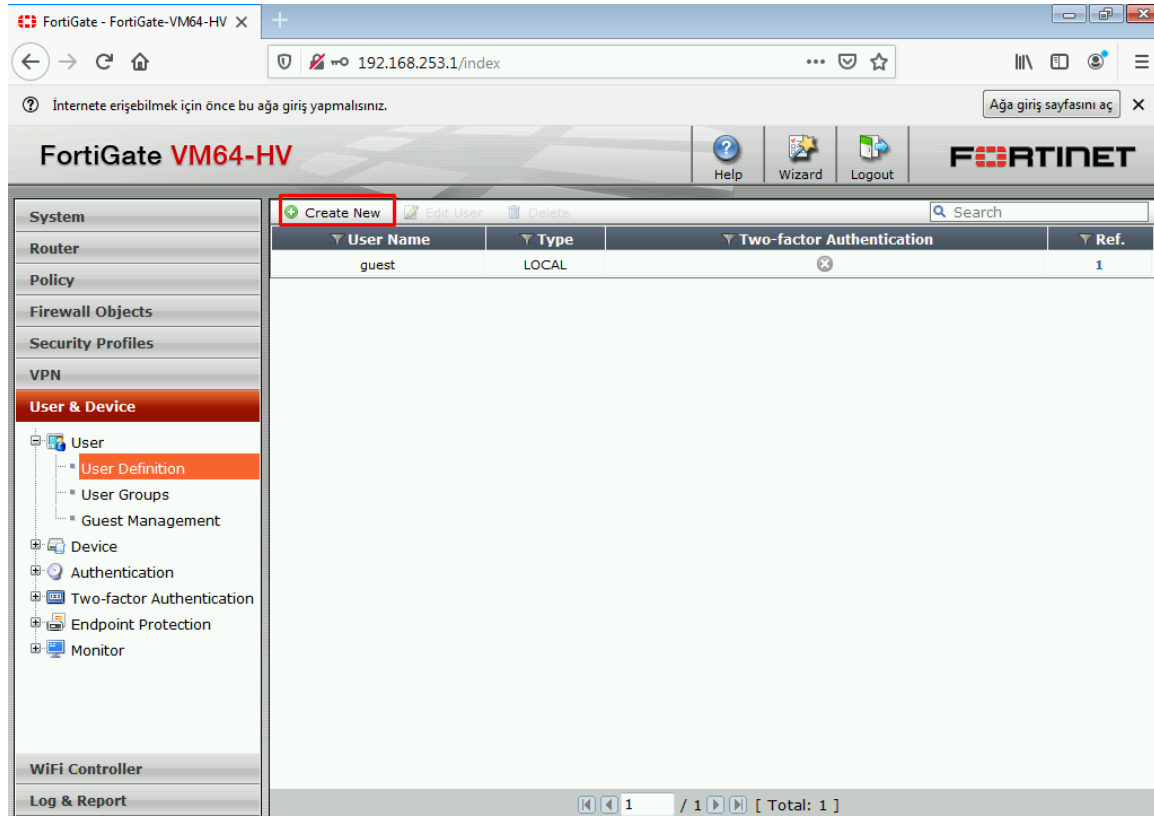
- Ardından “Firewall Objects” → “Addresses” → “Create New” tıklanır.



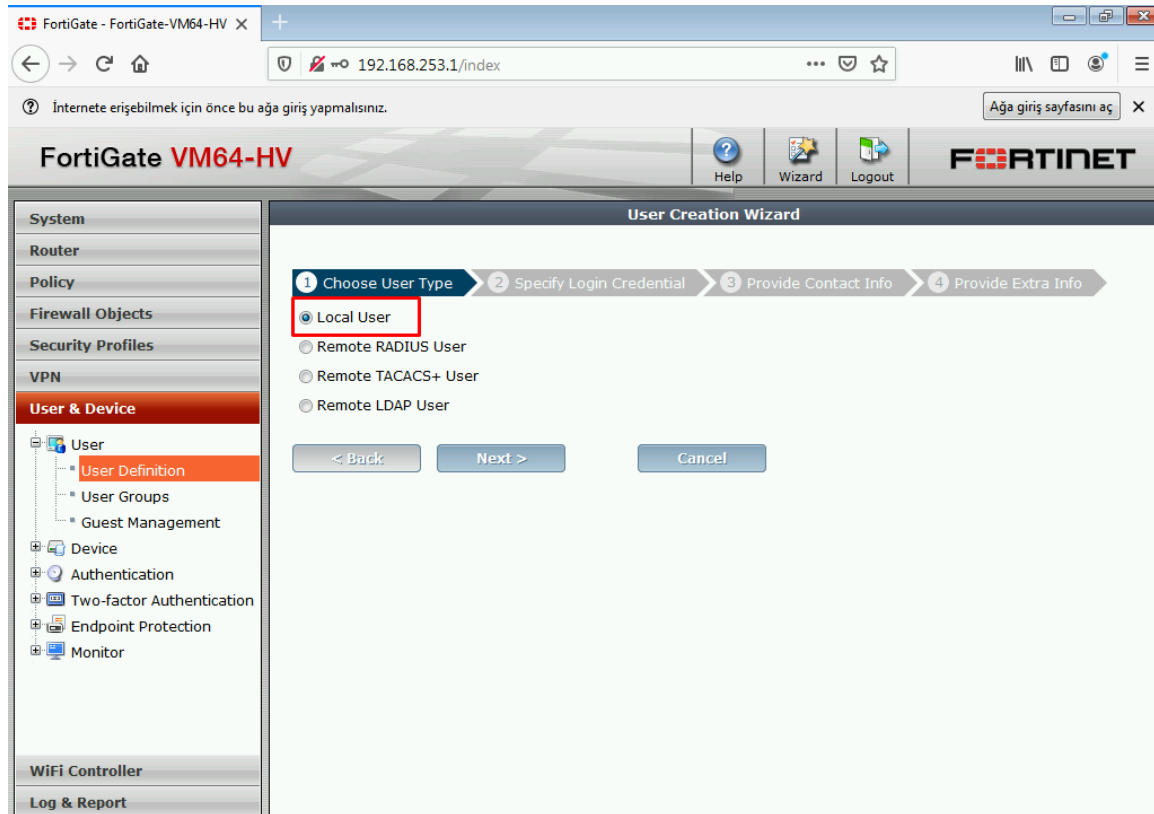
- Guest ağının ismi girilir, **Type** : Subnet, ağın IP adresi ve subnet mask'ı yazılır, **Interface** : ağın olduğu port seçilir.



- Misafir ağa kullanıcı oluşturmak için, “User & Device” → “User” → “User Definition” → “Create New”



- “Local User” seçilir ve next denir.



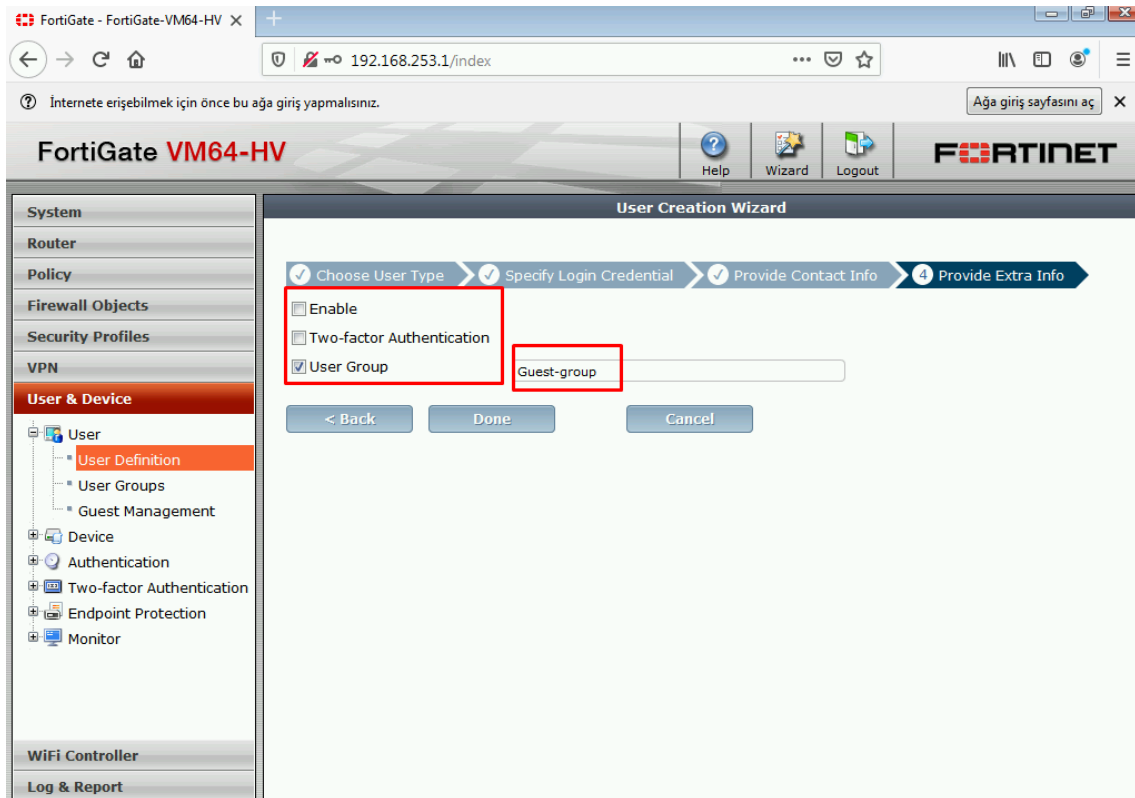
- Kullanıcının adı ve şifresi belirlenir.

The screenshot shows the FortiGate VM64-HV web interface. The left sidebar is expanded to 'User & Device' > 'User' > 'User Definition'. The main area displays the 'User Creation Wizard' with four steps: 1. Choose User Type (completed), 2. Specify Login Credential (current step), 3. Provide Contact Info, and 4. Provide Extra Info. In Step 2, the 'User Name' field contains 'memo' and the 'Password' field is masked with dots. Below the fields are three buttons: '< Back', 'Next >', and 'Cancel'. A red arrow points to the 'Next >' button.

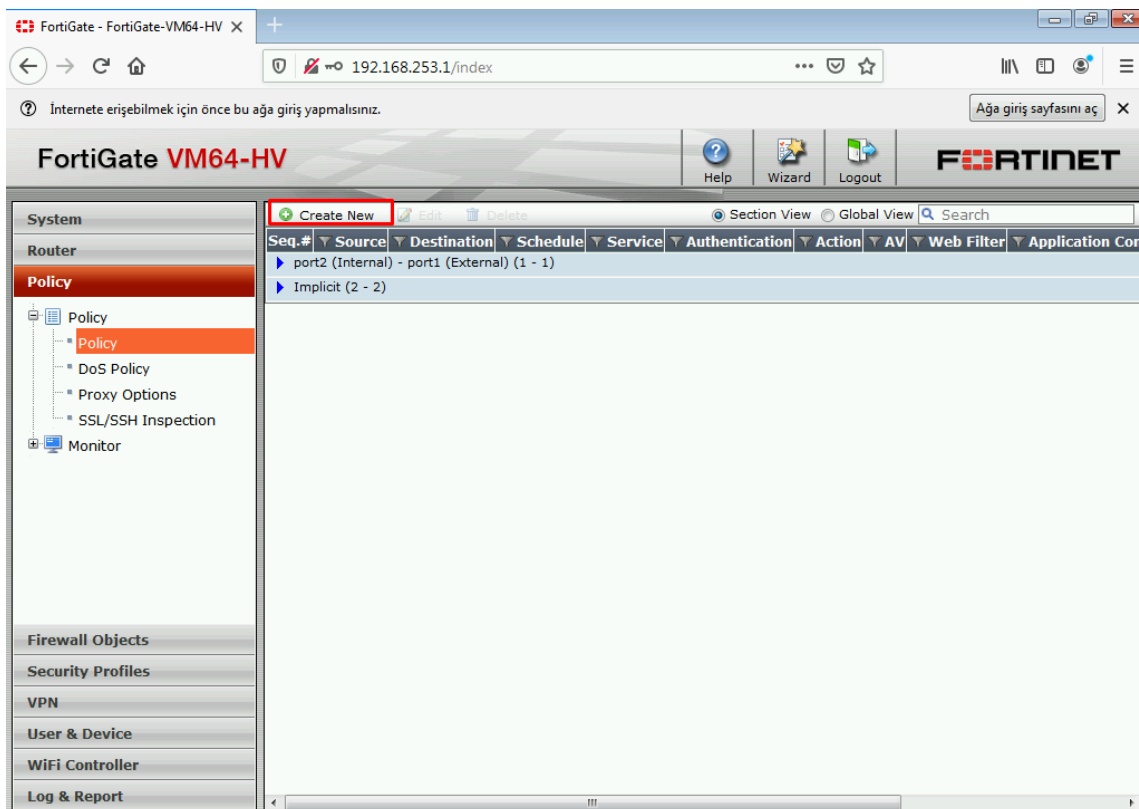
- İsteğe bağlı olarak mail adresi girilir.

The screenshot shows the FortiGate VM64-HV web interface. The left sidebar is expanded to 'User & Device' > 'User' > 'User Definition'. The main area displays the 'User Creation Wizard' with four steps: 1. Choose User Type (completed), 2. Specify Login Credential (completed), 3. Provide Contact Info (current step), and 4. Provide Extra Info. In Step 3, the 'Email Address' field is empty. Below the field is a checkbox labeled 'SMS'. Below the checkbox are three buttons: '< Back', 'Next >', and 'Cancel'. A red arrow points to the 'Next >' button.

- Sadece “User Group” kısmı işaretli kalır ve “Guest Group” seçilir ve “Done” denir.



- Ardından misafir ağı için yeni bir Policy oluşturacağız.



- “Incoming Interface : Misafir Local Ağı”
- “Source Address : Guest”
- “Outgoing Interface : WAN”
- “Destination Address : all”
- “Schedule : always”
- “Service : ALL”
- “Action : ACCEPT” olarak ayarlanır.

“Enable NAT” tiklenir ve “Logging Options” kısmının işareti “Log all Sessions”a kaydırılır ve ayarlar kaydedilir.

FortiGate - FortiGate-VM64-HV X

192.168.253.1/index

İnternete erişebilmek için önce bu ağa giriş yapmalısınız. Ağa giriş sayfasını aç X

FortiGate VM64-HV

Help Wizard Logout FORTINET

System

Router

Policy

Policy

DoS Policy

Proxy Options

SSL/SSH Inspection

Monitor

Firewall Objects

Security Profiles

VPN

User & Device

WiFi Controller

Log & Report

New Policy

Policy Type: Firewall VPN

Policy Subtype: Address User Identity Device Identity

Incoming Interface: port2 (Internal)

Source Address: Guest

Outgoing Interface: port1 (External)

Destination Address: all

Schedule: always

Service: ALL

Action: ACCEPT

☒ Enable NAT

☒ Use Destination Interface Address ☐ Fixed Port

☐ Use Dynamic IP Pool

Click to add...

Logging Options

☐ No Log

☐ Log Security Events

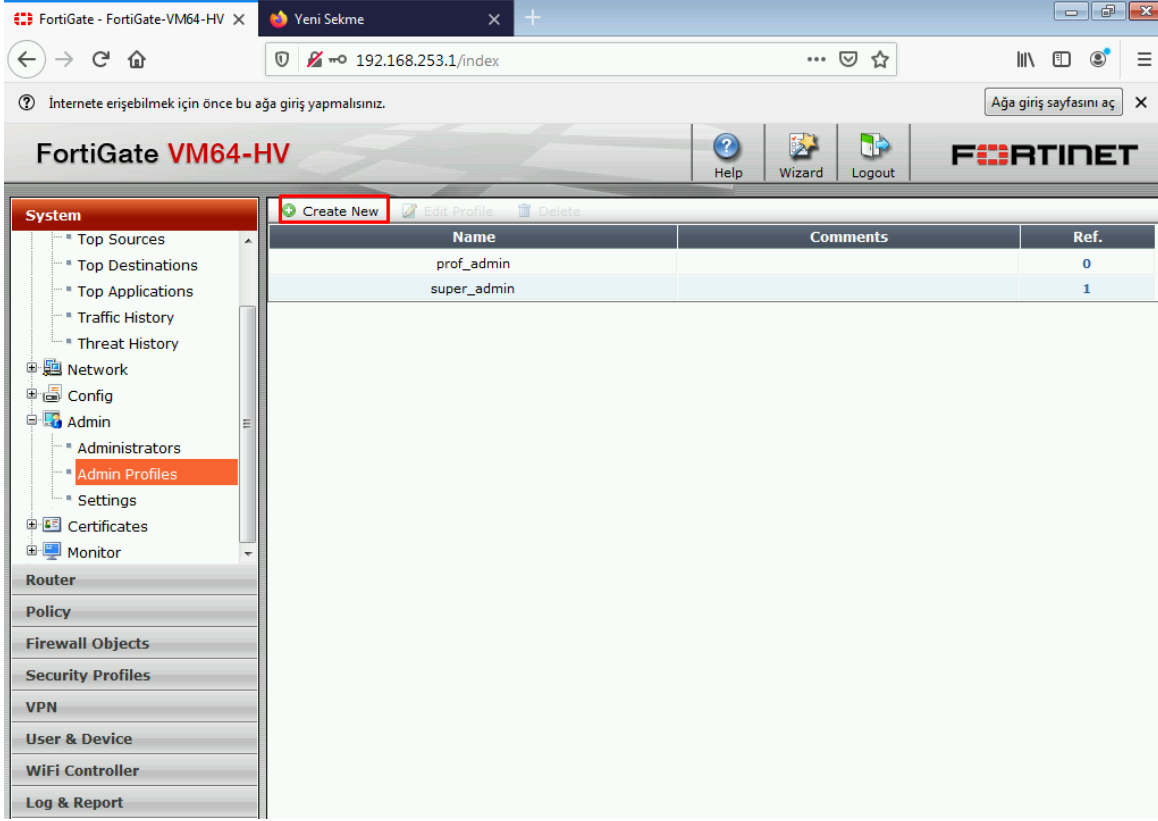
☒ Log all Sessions

☐ Generate Logs when Session Starts

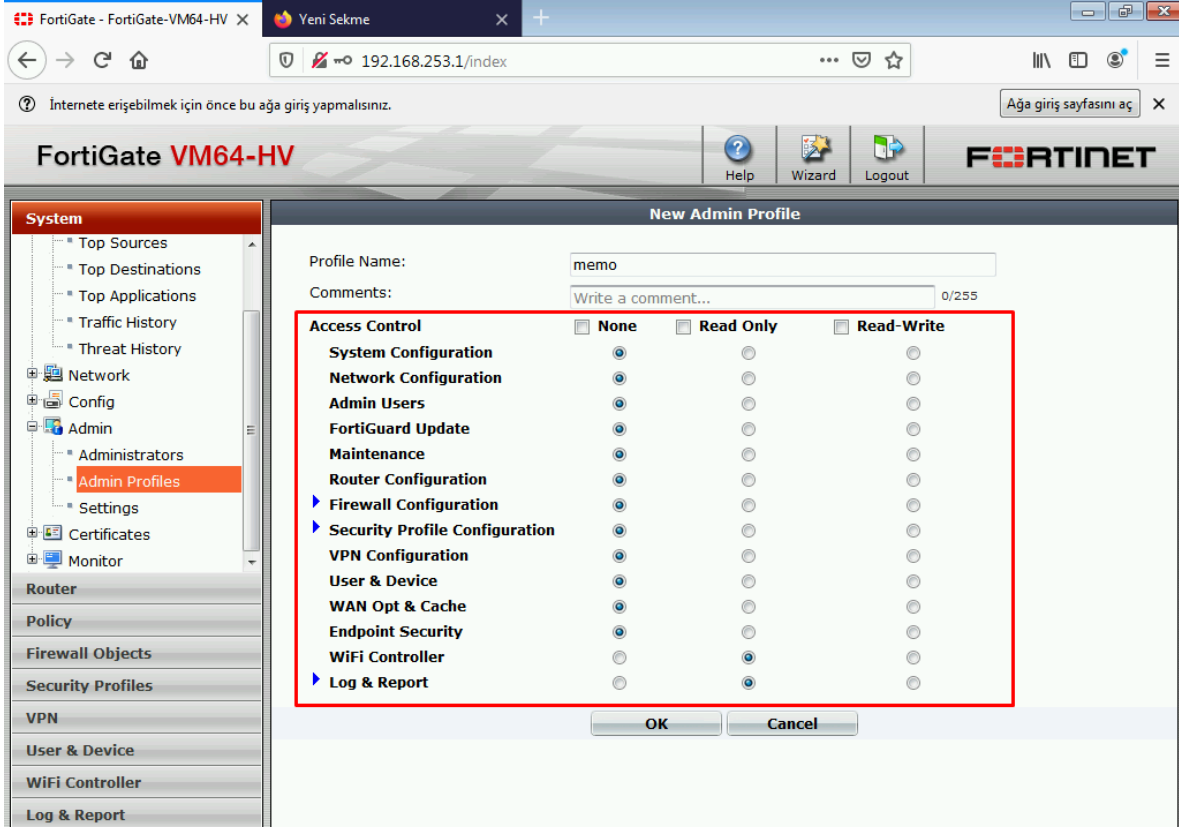
☐ Capture Packets

Security Profiles

- Kullanıcının yetkileri için “System” → “Admin” → “Admin Profiles” → “Create New” tıklanır.



- Kullanıcının adı girilir ve yetkiler verilir.



- Adres kısmının sağı altında yer alan “Ağı giriş sayfasını aç” butonuna tıkladığımızda kullanıcı ile giriş ekranı gelmektedir.

Oturumu Geri Getir x Firewall Authentication x +

192.168.253.1:1000/fgtauth?030e088c9c88e0d6

İnternete erişebilmek için önce bu ağı giriş yapmalısınız.

FORTINET®

Terms and Disclaimer Agreement

You are about to access Internet content that is not under the control of the network access provider. The network access provider is therefore not responsible for any of these sites, their content or their privacy policies. The network access provider and its staff do not endorse nor make any representations about these sites, or any information, software or other products or materials found there, or any results that may be obtained from using them. If you decide to access any Internet content, you do this entirely at your own risk and you are responsible for ensuring that any accessed material does not infringe the laws governing, but not exhaustively covering,

☐ I accept the terms and disclaimer agreement

Authentication for SSID: N/A

Please enter your username and password to continue

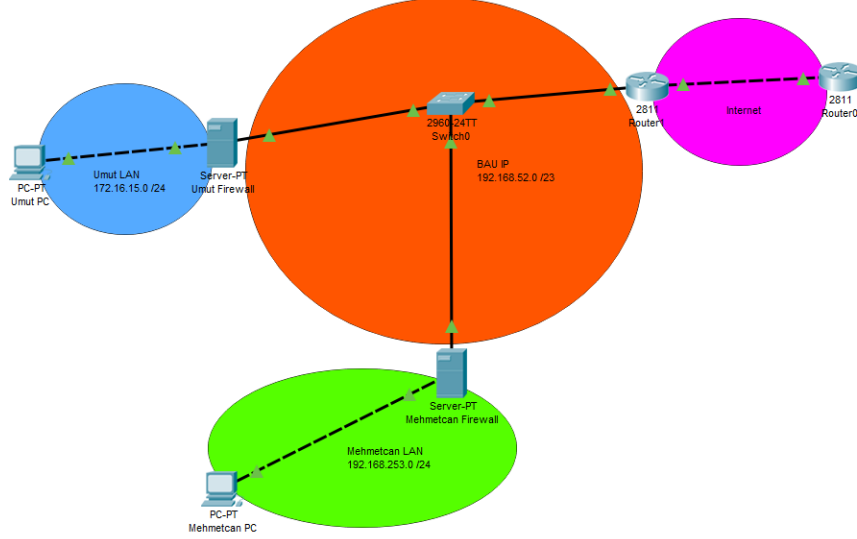
Username:

Password:

Continue

4-) Site to Site VPN

- Topoloji üzerinde olan Mehmetcan LAN ve Umut LAN Ağlarını VPN ile haberleştireceğiz, aşağıda yapacağımız tüm adımlar Mehmetcan PC tarafında yapılmaktadır, adımlar aynı şekilde Umut PC tarafında da yapılır.



- VPN kurulumu için Firewall'umuza kendi internal ve bağlanacağımız ağın internal IP adreslerini oluşturmamız gerekli. "Firewall Objects" → Addresses kısmından eklenir.

FortiGate - FortiGate-VM64-HV

192.168.253.1/index

FortiGate VM64-HV

Help Wizard Logout FORTINET

System

Router

Policy

Firewall Objects

Address

Addresses

Groups

Service

Schedule

Traffic Shaper

Virtual IPs

Monitor

Security Profiles

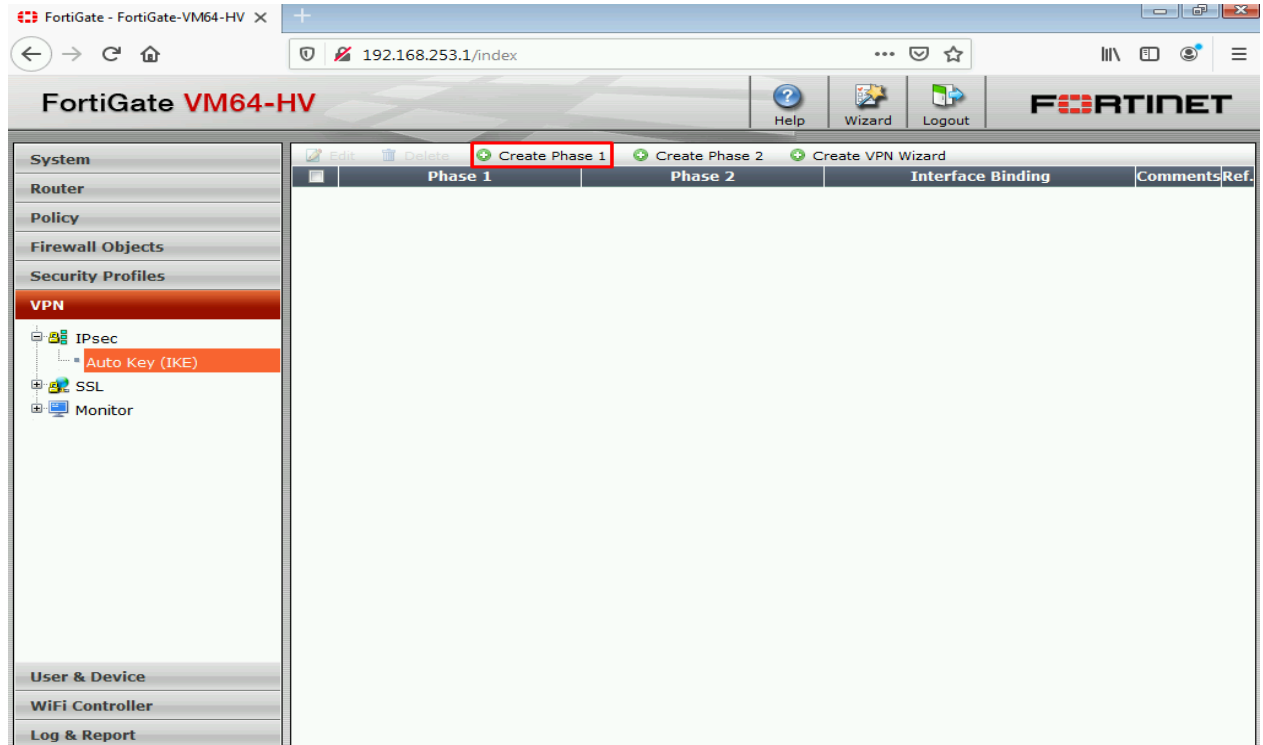
VPN

User & Device

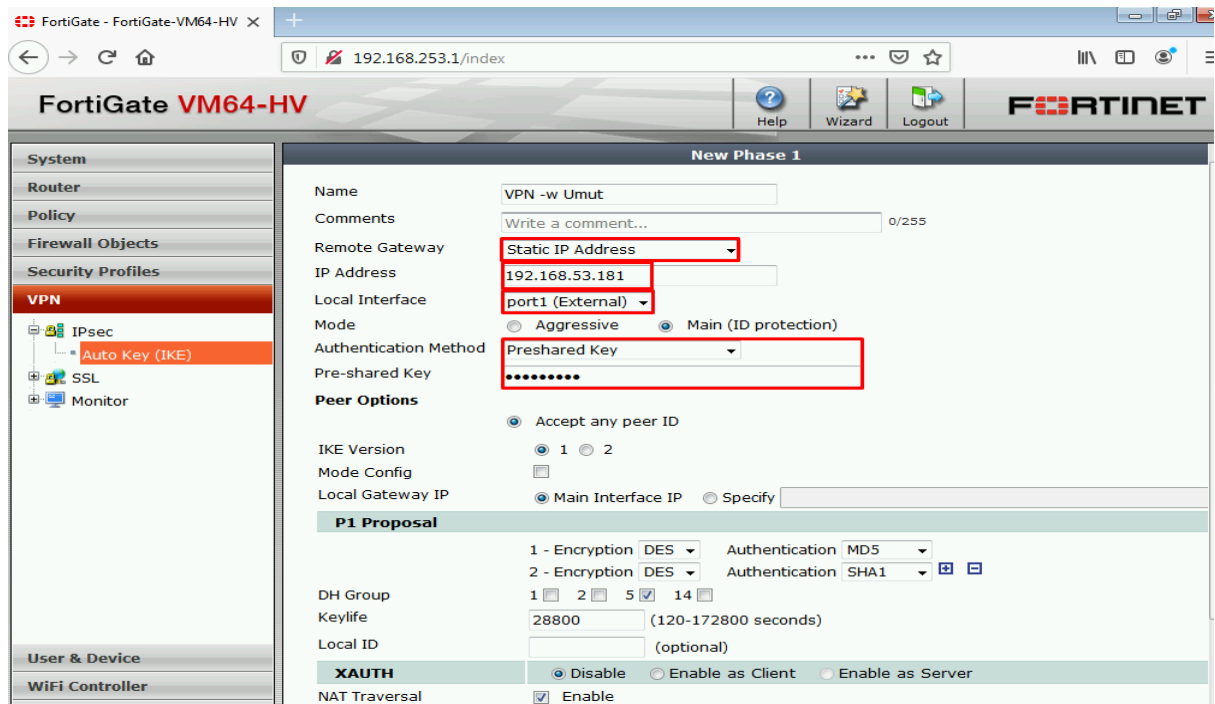
WiFi Controller

Name	Address/FQDN	Interface	Type	Show in Address List
Guest	192.168.253.0/255.255.255.0	port2	Subnet	✓
SSLVPN_TUNNEL_ADDR1	10.212.134.200-10.212.134.210	Any	IP Range	✓
Umut_LAN	172.16.15.0/255.255.255.0	Any	Subnet	✓
all	0.0.0.0/0.0.0.0	Any	Subnet	✓
internal_lan	192.168.253.0/255.255.255.0	Any	Subnet	✓

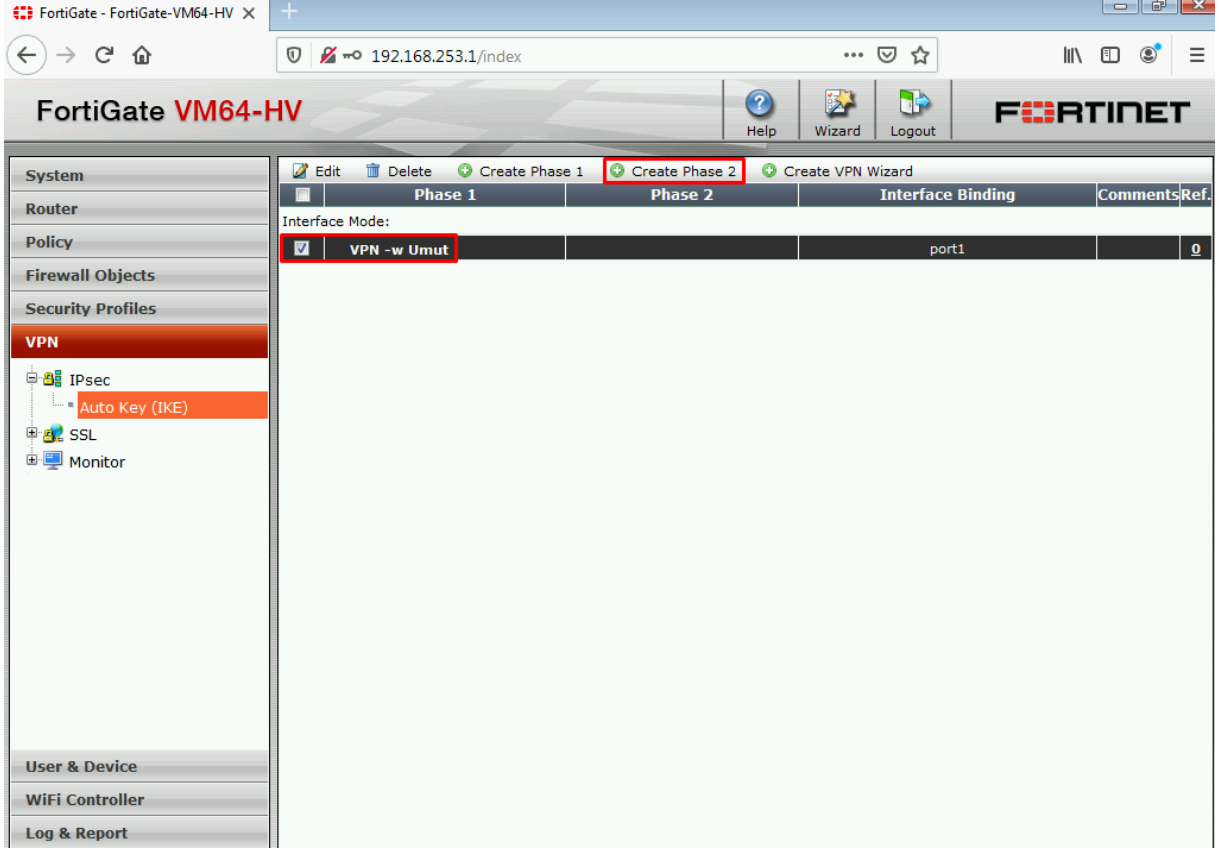
- Internal IP adresleri girildikten sonra VPN Ipsec oluşturmak için “VPN” → “Ipsec” → “Auto Key” kısmına girip “Create Phase1”e tıklarız.



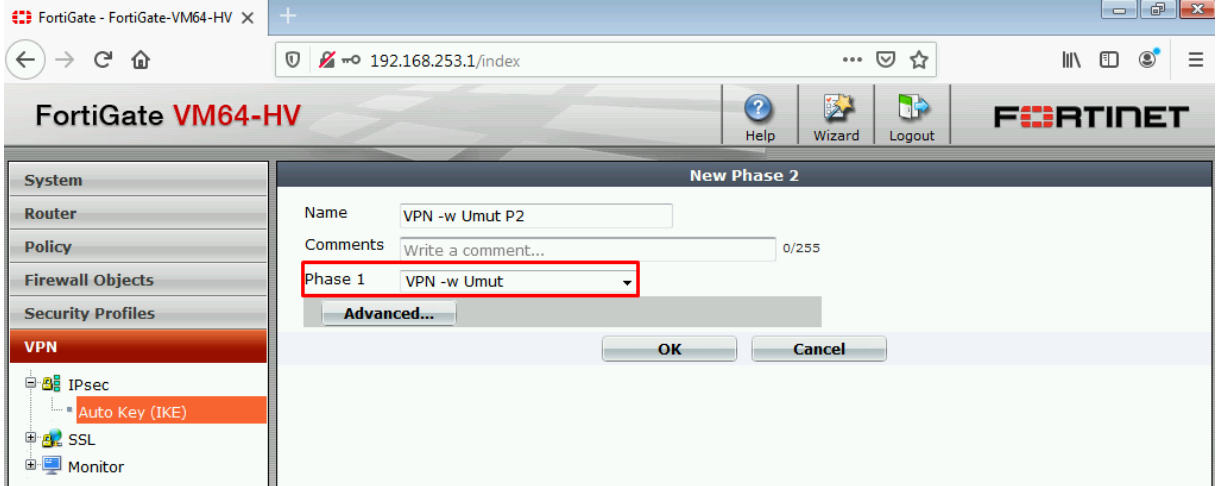
- İsim verilir, “Remote Gateway : Static IP Address”
- “IP Address : Remote WAN” karşı tarafın WAN IP’si
- “Local Interface : External” internete çıkan portumuz
- “Authentication Mode : Preshared Key” seçilir ve şifre oluşturulur ve ayarlar kaydedilir.



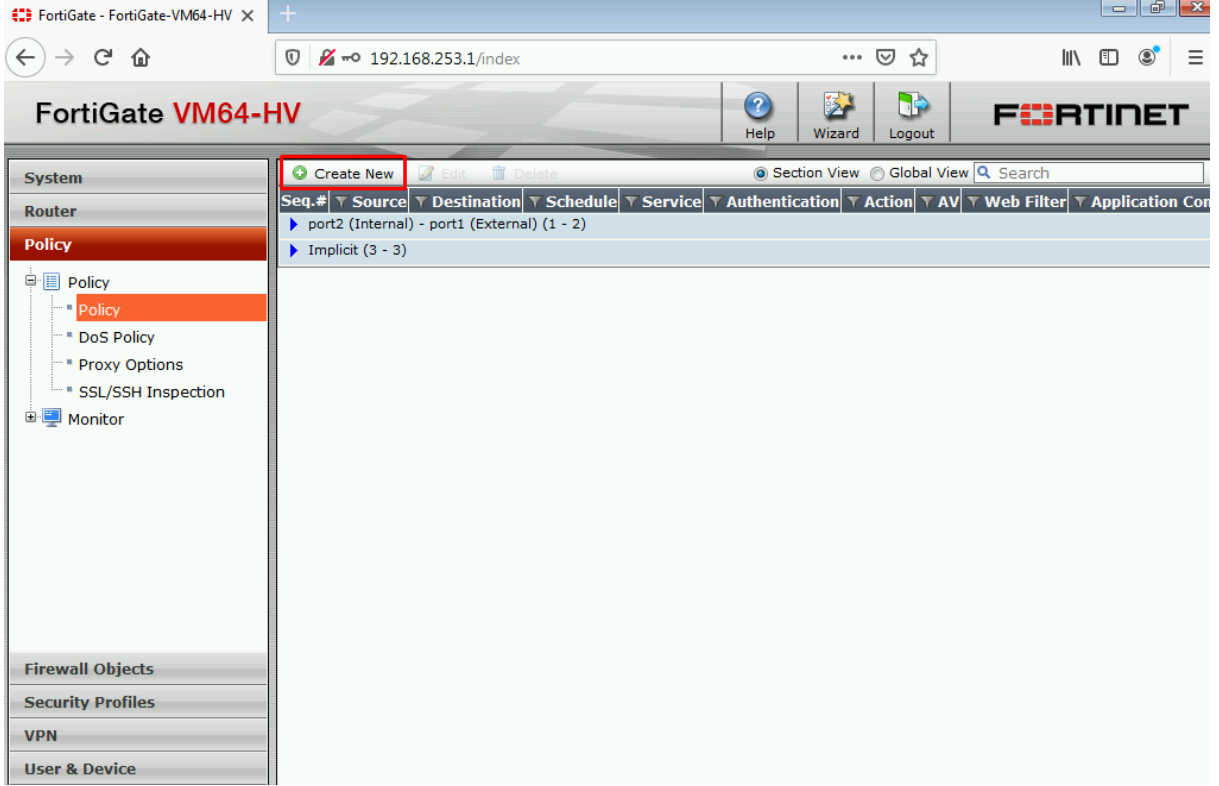
- Phase1 oluřturulduktan sonra VPN'imizi iřaretleyip "Create Phase2"e tıklarız.



- "Phase1" kısmına oluřturduėumuz VPN'i seėer ve ayarları kaydederiz.



- VPN'i oluřturduk, haberleřmeyi saęlamak iin policy ayarları yapmamız gerekmektedir. VPN iin 2 adet Policy oluřturmak gerekmektedir. Bunun iin "Policy" → "Policy" → "Create New" tıklanır.



- “Policy Type : Firewall” seçilir,
- “Policy Subtype : Address” seçilir,
- “Incoming Interface : Internal” portumuz,
- “Source Address : Internal_lan” adres kısmında oluşturduğumuz internal adresi,
- “Outgoing Interface : VPN” oluşturduğumuz VPN seçilir,
- “Destination Address : umut_lan” adres kısmında oluşturduğumuz bağlanacağımız ağın internal adresi,
- “Schedule : always” seçilir,
- “Service : All” seçilir,
- “Action : Accept” seçilir,

Ve ayarlar kaydedilir.

FortiGate - FortiGate-VM64-HV X

192.168.253.1/index

FortiGate VM64-HV

Help Wizard Logout

FortINET

System

Router

Policy

Policy

DoS Policy

Proxy Options

SSL/SSH Inspection

Monitor

Firewall Objects

Security Profiles

VPN

User & Device

WiFi Controller

Log & Report

New Policy

Policy Type

Policy Subtype

Incoming Interface

Source Address

Outgoing Interface

Destination Address

Schedule

Service

Action

Enable NAT

Logging Options

No Log

Log Security Events

Log all Sessions

Security Profiles

AntiVirus

Web Filter

Application Control

IPS

SSL/SSH Inspection

default

default

default

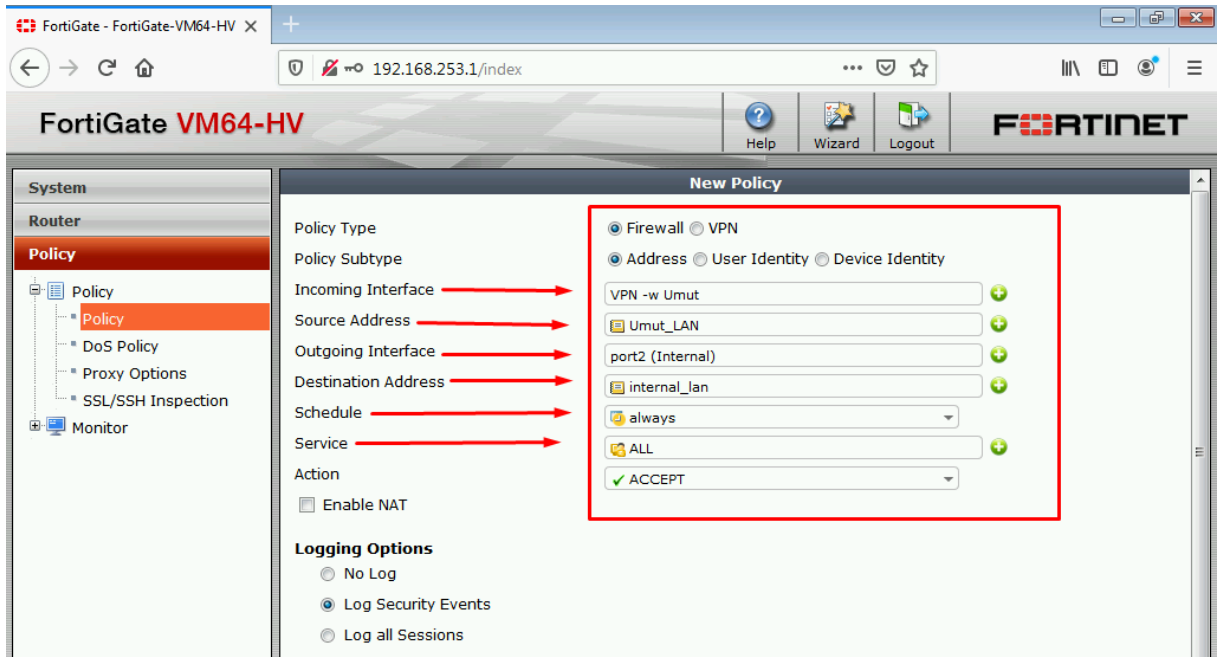
default

default

- “Policy Type : Firewall” seçilir,
- “Policy Subtype : Address” seçilir,
- “Incoming Interface : VPN” oluşturduğumuz VPN seçilir,
- “Source Address : umut_lan” adres kısmında oluşturduğumuz bağlanacağımız ağın internal adresi,
- “Outgoing Interface : Internal” portumuz,
- “Destination Address : Internal_lan” adres kısmında oluşturduğumuz internal adresi,
- “Schedule : always” seçilir,
- “Service : All” seçilir,
- “Action : Accept” seçilir,

- 2 policy arasındaki tek fark Incoming ve Outgoing Interfaces, Source ve Destination Address farkıdır.

Mantığı ise giden paketlerin geri gelmesi ile alakalıdır.

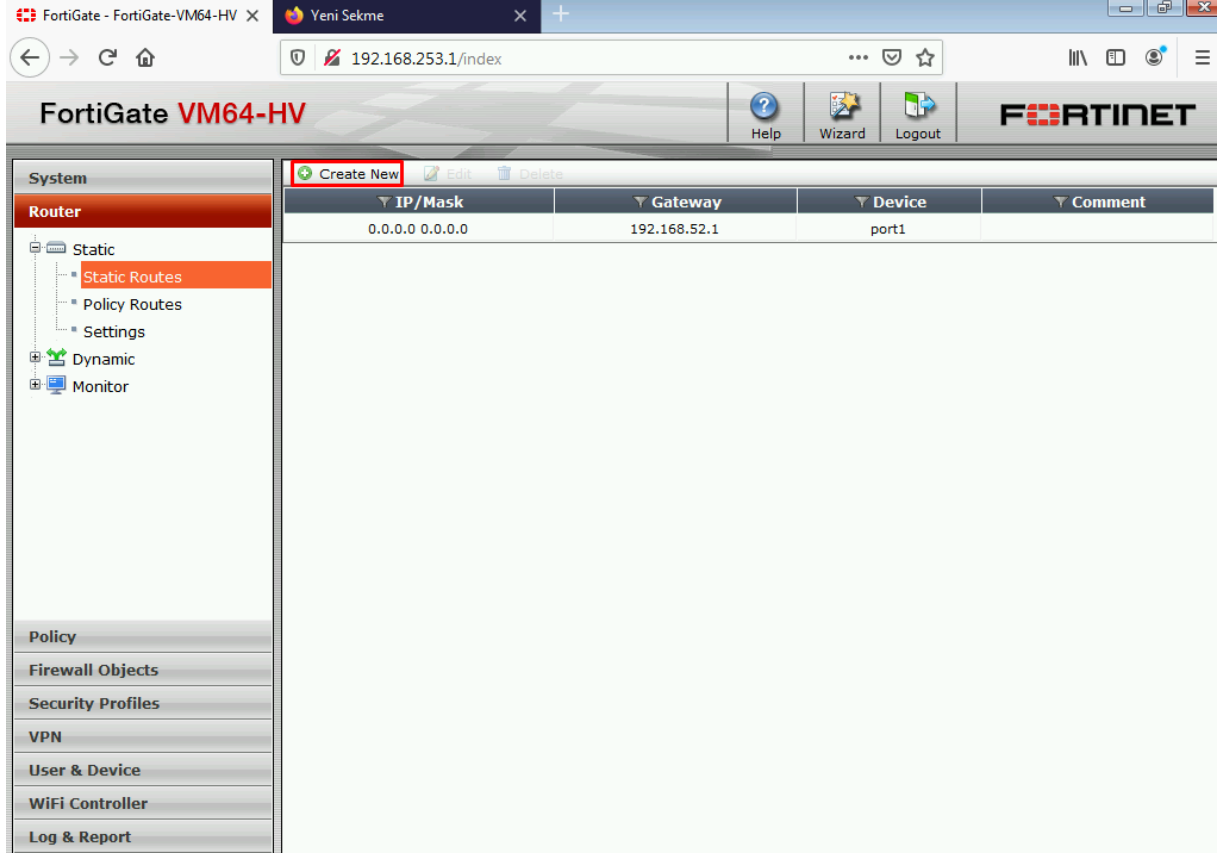


- Policy ayarları tamamlandığında “VPN” → “Monitor” → “Ipsec Monitör” tıklanır, ekran sağ kaydırıldığında “Status” kısmı “Bring Up” gözükp ve kırmızı yanarsa üzerine tıklayıp direk online olur. Ok işareti yukarı bakıp yeşil yanıyor ve “Bring Down” yazıyorsa VPN’imiz bağlanmıştır demektir.

The screenshot shows the FortiGate VM64-HV web interface. The left sidebar contains a navigation menu with the following items: System, Router, Policy, Firewall Objects, Security Profiles, VPN (highlighted), User & Device, WiFi Controller, and Log & Report. Under the VPN section, the following items are listed: IPsec, Auto Key (IKE), SSL, Monitor, IPsec Monitor (highlighted), and SSL-VPN Monitor. The main content area displays a table with the following columns: Timeout, Proxy ID Source, Proxy ID Destination, Status, Incoming Data, Outgoing Data, and Uptime. The table contains one row with the following data: Timeout: 1742, Proxy ID Source: 0.0.0.0/0, Proxy ID Destination: 0.0.0.0/0, Status: Bring Down (highlighted with a red box), Incoming Data: 0 B, Outgoing Data: 0 B, and Uptime: 66 seconds. The bottom of the interface shows a pagination bar with the text "1 / 1" and a link to "Column Settings".

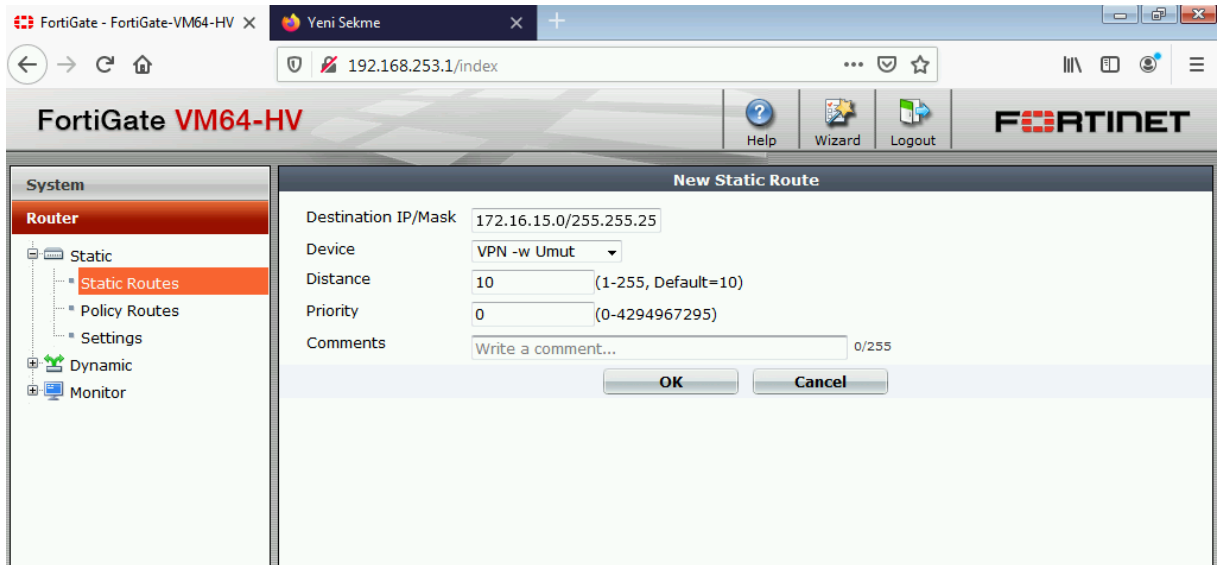
Timeout	Proxy ID Source	Proxy ID Destination	Status	Incoming Data	Outgoing Data	Uptime
1742	0.0.0.0/0	0.0.0.0/0	Bring Down	0 B	0 B	66 seconds

- VPN'imizi static route ile bařladıktan sonra aęlar arası haberleşme saęlanacaktır. Bunun için "Router" → "Static Routes" → "Create New"



- "Destination IP/Mask : Karşı aęın network ve subnetmask'ı"
- "Device : Oluşturduğumuz VPN"

Ayarlar kaydedilir. Haberleşmenin saęlanıp saęlanmadığı için ping kontrolü yapılır.



- Mehmetcan PC'den Umut PC'ye ping atabilmekteyiz ve traceroute ile de pingin geçtiği IP adreslerini görmekteyiz.

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2010 Microsoft Corporation. All rights reserved.

C:\Users\Mehmetcan.Mehmetcan-PC>ping 172.16.15.18

Pinging 172.16.15.18 with 32 bytes of data:
Reply from 172.16.15.18: bytes=32 time=18ms TTL=126
Reply from 172.16.15.18: bytes=32 time=2ms TTL=126
Reply from 172.16.15.18: bytes=32 time=1ms TTL=126
Reply from 172.16.15.18: bytes=32 time=2ms TTL=126

Ping statistics for 172.16.15.18:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 18ms, Average = 5ms

C:\Users\Mehmetcan.Mehmetcan-PC>tracert 172.16.15.18

Tracing route to 172.16.15.18 over a maximum of 30 hops
  0  <1 ms    <1 ms    <1 ms    192.168.253.1
  1  1 ms     1 ms     12 ms    192.168.53.181
  2  1 ms     1 ms     7 ms     172.16.15.18

Trace complete.

C:\Users\Mehmetcan.Mehmetcan-PC>
```