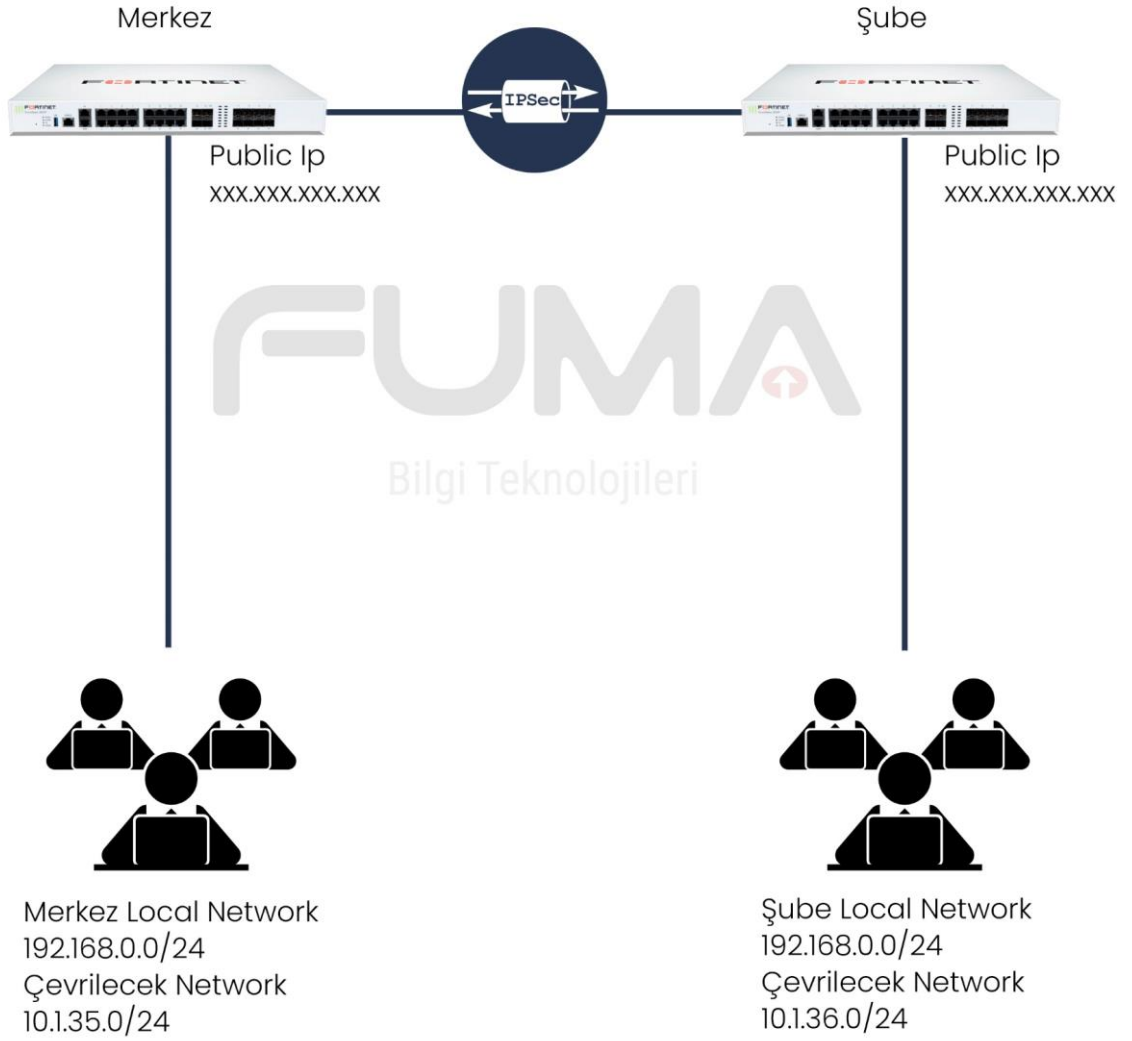


Fortigate IPSEC Vpn Overlapping Subnet



İşlemlere ilk olarak MERKEZ ve ŞUBE arası IPSEC Vpn bağlantı yaparak başlıyorum.

İlgili topolojime göre VPN bağlantımı gerçekleştiriyorum.

- VPN – IPSEC wizard seçeneğine tıklıyor ve karşıma gelen ekrandan CUSTOM seçiyorum ve Name kısmına bir isim belirliyor Next ile ilerliyorum.

The screenshot shows the 'VPN Creation Wizard' interface. The left sidebar has a dark theme with a green header. The 'VPN' menu is expanded, and 'IPsec Wizard' is selected. The main area has a green header with a search icon. Below the header, there's a 'VPN Setup' section with a green arrow icon. The 'Name' field is set to 'Mrk-Şube' and the 'Template type' is set to 'Custom'. A red box highlights the 'Name' field and the 'Custom' button. A red arrow points from the 'Custom' button to the 'Next >' button at the bottom right.

Karşıma gelen pencereden IPSEC bağlantım için yapılandırma bilgilerimi gireceğim.

Burada dikkat etmem gereken husus Phase 2 selectors kısmında tanımladığımız local ve remote adresler topolojide belirlediğimiz çevrilecek adreslerdir.

Phase 2 de network bilgilerini girdikten sonra advanced kısmından Auto-negotita kutucuğunu seçmeyi unutmayalım.

Edit VPN Tunnel

Name: [Blue Box]
Comments: [Comments]

Network [Edit]
Remote Gateway : Static IP Address [Blue Box] Interface : wan1

Authentication [Edit]
Authentication Method : Pre-shared Key
IKE Version : 1 , Mode : Main (ID protection)

Phase 1 Proposal [Edit]
Algorithms : 3DES-SHA1
Diffie-Hellman Group : 2

XAUTH [Edit]
Type : Disabled

Phase 2 Selectors

Name	Local Address	Remote Address	
[Blue Box]	10.1.35.0/255.255.255.0	10.1.36.0/255.255.255.0	[Add] [Edit]

OK

Merkez firewall Ipsec tanımlamalarımı tamamladıktan sonra VPN için merkezen şubaya gidecek network için statik rota oluşturuyorum.

Dashboard

Network

Interfaces

DNS

DNS Servers

IPAM

FortiExtenders

Static Routes

Policy Routes

RIP

OSPF

BGP

Routing Objects

Multicast

Diagnostics

Policy & Objects

Security Profiles

VPN

User & Authentication

WiFi Controller

System

Security Fabric

Log & Report

Edit Static Route

Destination

SubnetInternet Service

10.1.36.0/255.255.255.0

Interface

Mrk-Sube

+

Administrative Distance

200

Comments

Write a comment...

0/255

Status

EnabledDisabled

Advanced Options

Sonraki adımda network ve ip adres tanımlamaları için policy & Objects altından addresses seçeneğine ve oradan create new tıklıyorum.

The screenshot shows the Palo Alto Networks management interface. On the left, the 'Policy & Objects' menu is expanded, with 'Addresses' highlighted. In the top right, the '+ Create New' button is highlighted. A red arrow points from the 'Addresses' menu item to the 'Create New' button. The main content area shows a table with columns for 'Name' and 'IP Range/Subnet', with a filter of '20' applied. The table contains several entries, each with a document icon in the first column and a numerical value in the last column.

Karşıma gelen ekrandan ilk olarak local network (LAN) bilgilerimi giriyorum. Interface kısmından LAN interface i seçmeyi unutmuyorum.

New Address

Category

Address Multicast Address

Name

Merkez

Color

Change

Type

Subnet

IP/Netmask

192.168.0.0/24

Interface

lan

Static route configuration

0

Comments

Write a comment...0/255

Aynı işlemi Şube tarafı içinde gerçekleştiriyorum. Fakat burada şube tarafındaki çevrilecek olan network ü tanımlıyorum ve Interface olarak VPN interface i seçiyorum.

New Address

Category

Address Multicast Address

Name

Şube

Color

Change

Type

Subnet

IP/Netmask

10.1.36.0/24

Interface

Mrk-Şube

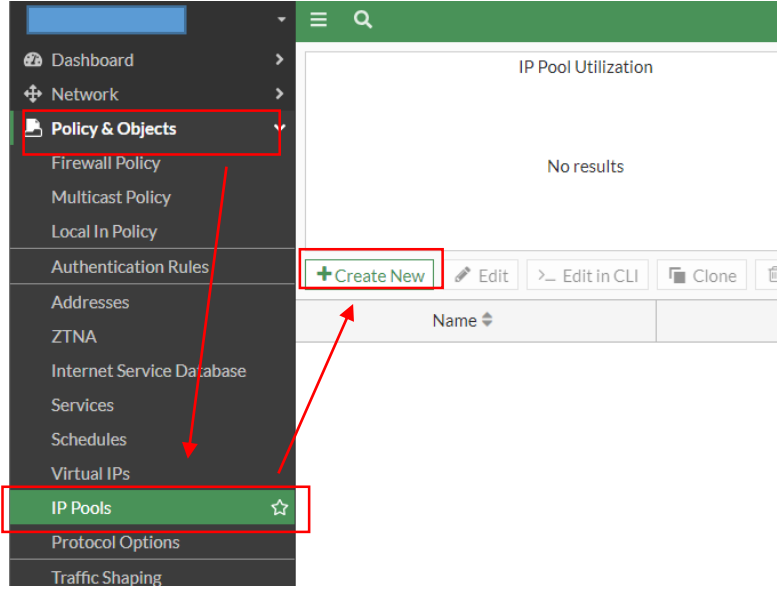
Static route configuration

0

Comments

Write a comment...0/255

Sonraki adımda bir ip havuzu oluşturacağım. Bu nedenle policy & objects altından IP pools tıklıyom karşıma gelen ekrandan yeni bir ip havuzu tanımlamak için create new butonuna tıklıyorum.

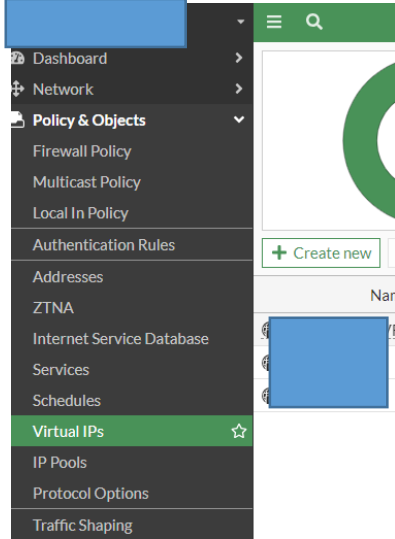


Karşıma gelen ekrandan Type seçeneğinden Fixed Port Range seçeneğini seçiyorum. External kısmına merkez çevrilecek ip bloğumu internal kısmına ise mevcut olan ip bloğumun bilgileri giriyorum.

New Dynamic IP Pool

Name	mrk-new-ip
Comments	Write a comment... 0/255
Type	Fixed Port Range
External IP Range ⓘ	10.135.1-10.135.254
Internal IP Range ⓘ	192.168.0.1-192.168.0.254
Ports Per User	<input type="checkbox"/>
ARP Reply	<input checked="" type="checkbox"/>

Sonraki adımda ip çevrim işlemlerinin yapılması için Policy & Object altından Virtual IPs tıklıyorum ve oradan yeni bir tanım için create new butonuna tıklıyorum.



Karşıma gelen ekrandan tanımlamalarımı yapıyorum. Interface VPN i seçiyorum. External kısmına çevrilecek ip bloğu Map to kısmına ise mevcut local ip bloğumu tanımlıyorum.

New Virtual IP

VIP type

IPv4


Name

Mrk-Nat-Ip

Comments


Write a comment... 0/255

Color

 Change

Network


Interface

 Mrk-Şube

Type

Static NAT

FQDN

External IP address/range 

10.1.35.1-10.1.35.254

Map to

IPv4 address/range

192.168.0.1 - 192.168.0.254

☐ Optional Filters

☐ Port Forwarding

Sonraki adımda VPN için merkezden şube ye şubeden de merkeze doğru firewall policy oluşturuyorum. Burada dikkat etmem gereken husus NAT açık ve Ip Pool Configuration seçeneğinden de üst adımlarda oluşturduğumuz ip havuzunun seçilmesidir.

New Policy

ID

0

Name ⓘ

Mrk-Şube

Type

Standard ZTNA

Incoming Interface

lan

Outgoing Interface

Mrk-Şube

Source

LAN

Negate Source

IP/MAC Based Access Control ⓘ

Destination

Şube

Negate Destination

Schedule

always

Service

ALL

Action

ACCEPT DENY

Inspection Mode

Flow-based Proxy-based

Firewall/Network Options

NAT

IP Pool Configuration

Use Outgoing Interface Address Use Dynamic IP Pool

Preserve Source Port

Protocol Options

PROT default

Security Profiles

AntiVirus

Web Filter

DNS Filter

Application Control

IPS

File Filter

SSL Inspection

SSL no-inspection

Logging Options

Log Allowed Traffic

Security Events

All Sessions

Advanced

WCCP

Exempt from Captive Portal

Comments

Write a comment... 0/1023

Enable this policy

OK

Cancel

Sonraki adımda tekrar bir policy daha oluştuyorum. Dikkat etmem gerekenler Nat Kapalı tutuyorum. Destination kısmında virtual ip de oluşturmuş olduğumuz kuralı seçiyoruz.

New Policy

ID

0

Name ⓘ

Şube-Mrk

Type

Standard ZTNA

Incoming Interface

Mrk-Şube

Outgoing Interface

Ian

Source

Şube

Negate Source

IP/MAC Based Access Control ⓘ

Destination

Mrk-Nat-Ip

Negate Destination

Schedule

always

Service

Action

✓ ACCEPT ✗ DENY

Inspection Mode

Flow-based Proxy-based

Firewall/Network Options

NAT

Protocol Options

PROT default

Security Profiles

AntiVirus

Web Filter

DNS Filter

Application Control

IPS

File Filter

SSL Inspection

SSL no-inspection

Logging Options

Log Allowed Traffic

Security Events All Sessions

Advanced

WCCP

Exempt from Captive Portal

Comments

Write a comment... 0/1023

Enable this policy

Additional In

API P

Online G

Relevan

Video T

Consoli

Hot Que

Join the

OK

Cancel

Merkez firewall cihazımla işlemlerimi tamamladıktan sonra Aynı işlemleri Şube cihazımda da gerçekleştiriyorum.

Şube cihazımda Ipsec Vpn kuruyorum.

Edit VPN Tunnel

Name

Hosab - Su Depo

Comments

Comments0/255

Network

Remote Gateway : Static IP Address (95.173.10.48) , Interface : wan1

Edit

Authentication

Authentication Method : Pre-shared Key

IKE Version : 1 , Mode : Main (ID protection)

Edit

Phase 1 Proposal

Algorithms : 3DES-SHA1

Diffie-Hellman Group : 2

Edit

XAUTH

Type : Disabled

Edit

Phase 2 Selectors

Name	Local Address	Remote Address	
Hosab - Su Depo	10.1.36.0/255.255.255.0	10.1.35.0/255.255.255.0	<div><div>+</div>Add</div> <div>Edit</div>

Sonrasında Statik rota oluştuyorum.

New Static Route

Destination

Subnet

Internet Service

10.1.35.0/24

Interface

Şube-Mrk

+

Administrative Distance

200

Comments

Write a comment...0/255

Status

Enabled

Disabled

Advanced Options

Şube cihazında Adres tanımlamalarımı gerçekleştiriyorum. Merkez çevrilecek ip bloğunu giriyorum.

New Address


Category

Address Multicast Address

Name

Merkez

Color

 Change


Type

Subnet ▼

IP/Netmask

10.1.35.0/24

Interface

 Şube-Mrk ▼

Static route configuration

☐

Comments

Write a comment... 0/255

İkinci adres tanımlamada şube local network ü tanımlıyorum.

New Address


Category

Address Multicast Address

Name

Şube

Color

 Change


Type

Subnet ▼

IP/Netmask

192.168.0.0/24

Interface

 lan ▼

Static route configuration

☐

Comments

Write a comment... 0/255

Sonraki adımda şub için ip pool tanımlamamı gerçekleştiriyorum.

The screenshot shows the 'Edit Dynamic IP Pool' configuration page. The left sidebar contains a menu with 'IP Pools' highlighted. The main content area has the following fields:

- Name: şube-new-ip
- Comments: Write a comment... (0/255)
- Type: Fixed Port Range
- External IP Range: 10.1.36.1-10.1.36.254
- Internal IP Range: 192.168.0.1-192.168.0.254
- Ports Per User: ☐
- ARP Reply: ☒

Sonraki adımda Virtuals IPs tanımlamamı gerçekleştiriyorum.

The screenshot shows the 'Edit Virtual IP' configuration page. The left sidebar contains a menu with 'Virtual IPs' highlighted. The main content area has the following fields:

- VIP type: IPv4
- Name: Şube-Nat-Ip
- Comments: Write a comment... (0/255)
- Color: Change
- Network:
 - Interface: Şube-Mrk
 - Type: Static NAT
 - External IP address/range: 10.1.36.1-10.1.36.254
 - Map to:
 - IPv4 address/range: 192.168.0.1 - 192.168.0.254
- ☐ Optional Filters
- ☐ Port Forwarding

Sonraki adımda yine kurallarımı oluřturuyorum. Yukarıdaki adımların aynısını řube cihazım için gerekleřtirim.

New Policy

ID

0

Name ⓘ

řube-Mrk

Type

Standard ZTNA

Incoming Interface

lan + x

Outgoing Interface

řub-Mrk + x

Source

LAN + x

Negate Source

☐

IP/MAC Based Access Control ⓘ

+

Destination

řube-Nat-Ip + x

Negate Destination

☐

Schedule

always v

Service

+

Action

☒ ACCEPT ☐ DENY

Inspection Mode

Flow-based Proxy-based

Firewall/Network Options

NAT

☒

IP Pool Configuration

Use Outgoing Interface Address Use Dynamic IP Pool

řube-new-ip + x

Preserve Source Port

☐

Protocol Options

PROT default v

Security Profiles

AntiVirus

☐

Web Filter

☐

DNS Filter

☐

Application Control

☐

IPS

☐

File Filter

☐

SSL Inspection

SSL no-inspection v

Logging Options

Log Allowed Traffic

☒

Security Events

All Sessions

Advanced

WCCP

☐

Exempt from Captive Portal

☐

Comments

Write a comment... 0/1023

Enable this policy

☒

OK

Cancel

Aynı şekilde çapraz kuralımı da oluştuyorum. Çapraz kuralımı oluştururken

Nat kapalı ve destination kısmında Virtual ip kuralım seçili

New Policy

ID

0

Name

Mrk-Şube

Type

Standard ZTNA

Incoming Interface

Şube-Mrk

Outgoing Interface

Ian

Source

Merkez

Negate Source

IP/MAC Based Access Control

Destination

Şube-Nat-Ip

Negate Destination

Schedule

always

Service

ALL

Action

ACCEPT DENY

Inspection Mode

Flow-based Proxy-based

Firewall/Network Options

NAT

IP Pool Configuration

Use Outgoing Interface Address Use Dynamic IP Pool

Preserve Source Port

Protocol Options

PROT default

Security Profiles

AntiVirus

Web Filter

DNS Filter

Application Control

IPS

File Filter

SSL Inspection

SSL no-inspection

Logging Options

Log Allowed Traffic

Security Events All Sessions

Advanced

WCCP

Exempt from Captive Portal

Comments

Write a comment... 0/1023

Enable this policy

Additional Information

API Preview

Online Guides

Relevant Docs

Video Tutorials

Consolidated

Hot Questions

Join the Discussion

OK

Cancel

Son olarak Vpn ayağa kalkması için iki cihazımda da IPsec motoru ile ilgili vpn sağ tuş yapıp Bring up tıklamak.

The screenshot displays the FortiGate IPsec Monitor interface. On the left, a sidebar menu shows 'IPsec Monitor' selected. The main panel is titled 'IPsec' and contains a table of active tunnels. The table has columns for Name, Remote Gateway, Peer ID, and Incoming Data. The first tunnel listed is 'TT_APN'. A context menu is open over the 'TT_APN' row, with the 'Bring Up' option highlighted. Other options in the menu include 'Reset Statistics', 'Bring Down', 'Locate on VPN Map', 'Show Matching Logs', 'Entire Tunnel', 'Phase 2 Selector: Hosab - Su Depo', 'Phase 2 Selector: Hosab - Su Deposu 2', and 'All Phase 2 Selectors'.

Name	Remote Gateway	Peer ID	Incoming Data
TT_APN			84.67 MB
TURCELL			284.07 MB