

# SOPHOS İLE NSX EDGE ARASINDA IPSEC YAPILANDIRMASI

- [SOPHOS İLE NSX EDGE ARASINDA IPSEC YAPILANDIRMASI](#)

# SOPHOS İLE NSX EDGE ARASINDA IPSEC YAPILANDIRMASI

Sopshos UTM ile NSX Edge firewall ipsec bağlantısı için arasında faz1 ve faz2 uygun yapılan şekilde yapılandırmanız gerekmektedir.

**Sophos UTM Tanımları:**

**SOPHOS** UTM 9 | admin | ? | C | ⚙️

search IPsec

Dashboard Management Definitions & Users Interfaces & Routing Network Services Network Protection Web Protection Email Protection Advanced Protection Endpoint Protection Wireless Protection Webserver Protection RED Management Site-to-site VPN Amazon VPC **IPsec** SSL Certificate Management Remote Access Logging & Reporting Support Log off

Connections Remote Gateways **Policies** Local RSA Key Advanced Debug

+ New IPsec Policy...

search Find

Display: 10 1-10 of 10

Action	Sort by: Name asc
<input type="checkbox"/> Edit Delete Clone	<b>AES-256</b> Compression off, not using strict policy. IKE Settings: AES 256 / MD5 / Group 5: MODP 1536 Lifetime: 7800 seconds IPsec Settings: AES 256 / MD5 / Null (None) Lifetime: 3600 seconds
<input type="checkbox"/> Edit Delete Clone	<b>AES-256 PFS</b> Compression off, not using strict policy. IKE Settings: AES 256 / MD5 / Group 5: MODP 1536 Lifetime: 7800 seconds IPsec Settings: AES 256 / MD5 / Group 5: MODP 1536 Lifetime: 3600 seconds
<input type="checkbox"/> Edit Clone	<b>L2TP-over-IPsec</b> [Policy used for L2TP-over-IPsec] Compression off, not using strict policy. IKE Settings: AES 128 / SHA2 256 / Group 14: MODP 2048 Lifetime: 28800 seconds IPsec Settings: AES 128 / SHA2 256 (96 bit) / Null (None) Lifetime: 3600 seconds
<input type="checkbox"/> Edit Delete Clone	<b>Microsoft Windows</b> Compression off, not using strict policy. IKE Settings: 3DES / SHA1 / Group 14: MODP 2048 Lifetime: 28800 seconds IPsec Settings: 3DES / MD5 / Null (None) Lifetime: 3600 seconds
<input type="checkbox"/> Edit Delete Clone	<b>Novell BorderManager</b> Compression off, using strict policy. IKE Settings: 3DES / SHA1 / Group 2: MODP 1024 Lifetime: 14400 seconds IPsec Settings: 3DES / MD5 / Group 2: MODP 1024 Lifetime: 3600 seconds
<input type="checkbox"/> Edit Delete Clone	<b>TripleDES</b> Compression off, not using strict policy. IKE Settings: 3DES / MD5 / Group 5: MODP 1536 Lifetime: 7800 seconds IPsec Settings: 3DES / MD5 / Null (None) Lifetime: 3600 seconds
<input type="checkbox"/> Edit Delete Clone	<b>TripleDES PFS</b> Compression off, not using strict policy. IKE Settings: 3DES / MD5 / Group 5: MODP 1536 Lifetime: 7800 seconds IPsec Settings: 3DES / MD5 / Group 5: MODP 1536 Lifetime: 3600 seconds
<input type="checkbox"/> Edit Delete Clone	<b>demopolicy</b> Compression off, not using strict policy. IKE Settings: AES 128 / SHA1 / Group 5: MODP 1536 Lifetime: 28800 seconds IPsec Settings: AES 128 / SHA1 / Group 5: MODP 1536 Lifetime: 3600 seconds

New IPsec Policy seçerek yeni bir policy oluşturuyoruz.

+ New IPsec Policy...

search

Edit IPsec Policy

Name: demopolicy

IKE encryption algorithm: AES 128

IKE authentication algorithm: SHA1

IKE SA lifetime: 28800

IKE DH group: Group 5: MODP 1536

IPsec encryption algorithm: AES 128

IPsec authentication algorithm: SHA1

IPsec SA lifetime: 3600

IPsec PFS group: Group 5: MODP 1536

Strict policy: ☐

Compression: ☐

Comment:

Save

Cancel

Sophos UTM üzerinde görseldeki şekilde Faz1 ve Faz2 yapılandırmasını gerçekleştiriyoruz.

search

IPsec

Dashboard

Management

Definitions & Users

Interfaces & Routing

Network Services

Network Protection

Web Protection

Email Protection

Advanced Protection

Endpoint Protection

Wireless Protection

Webserver Protection

RED Management

Site-to-site VPN

Amazon VPC

IPsec

SSL

Certificate Management

Connections

Remote Gatew...

Policies

Local RSA Key

Advanced

Debug

+ New Remote Gateway...

search

Find

Display: 10

☐

Action

☐

Edit

Delete

Clone

Sort by: Name asc

demo\_remote 37

VPN ID is IP Address, authenticated via Preshared key.

New Remote Gateway ekliyoruz.

Connections Remote Gatew... Policies Local RSA Key Advanced Debug

+ New Remote Gateway...  Find << >>

Display: 10 1-1 of 1

Edit Remote Gateway

Name: demo\_remote

Gateway type: Initiate connection

Gateway: 37.9.203.107

Authentication type: Preshared key

Key: .....

Repeat: .....

VPN ID type: IP address

VPN ID (optional):

Remote networks: 172.2.0.0/24   
DND DND  
DND DND  
DND DND

Comment:

+ Advanced

✓ Save ✗ Cancel

☐ Action

Sort by: Name asc

☐ Edit

Delete

Clone

demo\_remote 37.9.203.107

VPN ID is IP Address, authenticated via Preshared key.

Uzak uç public , local ip ve Preshared key tanımlarımızı giriyoruz.

search IPsec

Dashboard Management Definitions & Users Interfaces & Routing Network Services Network Protection Web Protection Email Protection Advanced Protection Endpoint Protection Wireless Protection Webserver Protection RED Management Site-to-site VPN Amazon VPC IPsec SSL Certificate Management

Connections Remote Gateways Policies Local RSA Key Advanced Debug

+ New IPsec Connection... search Find << >>

Open Live Log Display: 10 1-1 of 1

☐ Action ☐ Edit ☒ Demo\_IPsec External demo\_remote demopolicy [Auto Firewall is on and strict routing is not in use.] ☐ Delete ☐ Clone Sort by: Name asc

New IPsec Connection seçiyoruz.

IPsec

Connections Remote Gateways Policies Local RSA Key Advanced Debug

+ New IPsec Connection... search Find << >>

Open Live Log Display: 10 1-1 of 1

Edit IPsec Connection

Name: Demo\_IPsec

Remote gateway: demo\_remote

Local interface: External

Policy: demopolicy

Local Networks

172.20.0.0/24	DND	DND	DND	DND
DND	DND	DND	DND	DND
DND	DND	DND	DND	DND
DND	DND	DND	DND	DND

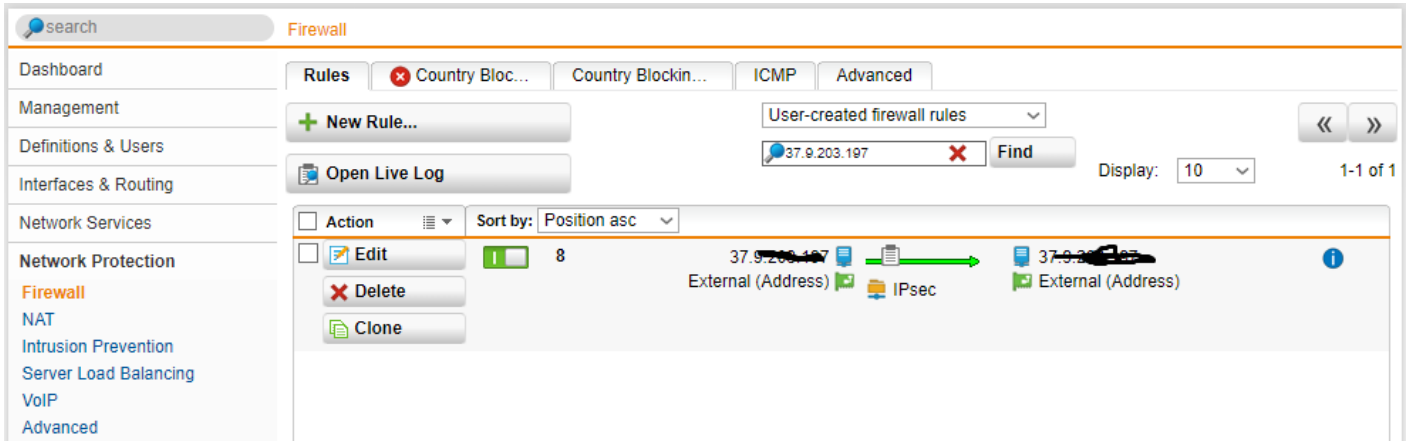
☒ Automatic firewall rules  
☐ Strict routing  
☐ Bind tunnel to local interface

Comment:

Save Cancel

☐ Action ☐ Edit ☒ Demo\_IPsec External demo\_remote demopolicy [Auto Firewall is on and strict routing is not in use.] ☐ Delete ☐ Clone Sort by: Name asc

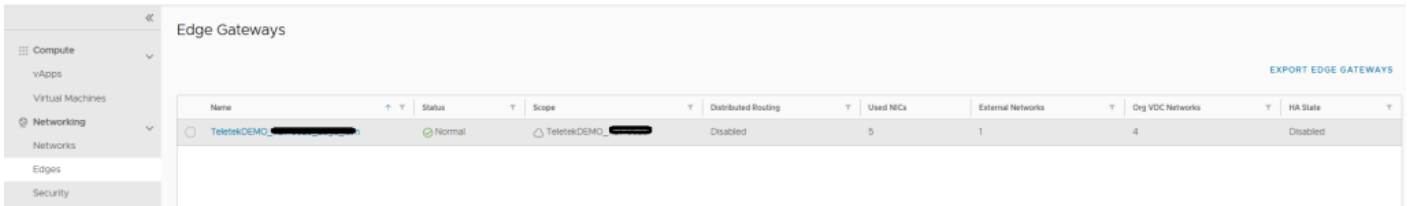
Local ip adresimiz ile birlikte tanımladığımız remote gateway local interface policy yi seçiyoruz.



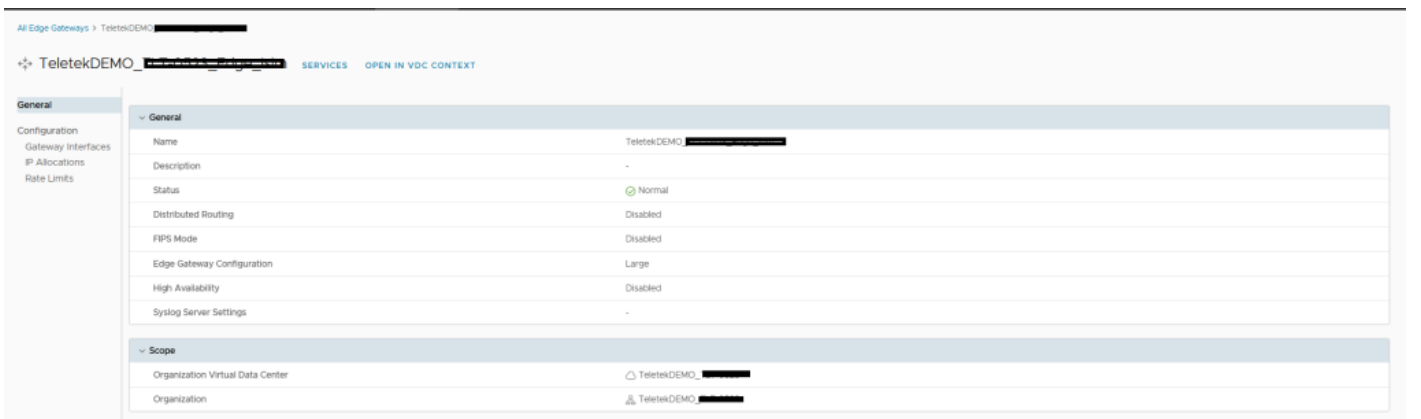
Son olarak Firewall'dan karşılıklı Ipsec kuralımızı tanımlıyoruz.

## NSX Edge Tanımları:

Vmware Cloud Director 'de VDC 'ye giriş yaptıktan sonra sol kısımda Edges kısmını göreceksiniz.



Ekrandaki mavi yazılı kısmına çift tıklayarak devam ediyoruz.



Yeni açılan sayfada "SERVICES" kısmına çift tıklıyoruz.

## Firewall Rules

Enabled ☒   Show only user defined rules ☐

Firewall tabında Firewal Rules >> Enabled kısmını aktif ediyoruz

## IPsec VPN

## IPsec VPN Configuration

Activation Status Global Configuration Logging Settings

## IPsec VPN Sites

Site Name	Local Endpoint	Local Subnets	Peer Endpoint	Peer Subnets	Site Enabled
Teletek-test-Ark...	37	172	195	172	<input checked="" type="checkbox"/>

VPN >> IPsec VPN Configuration >> Ipsec VPN Sites " + " işareti basarak yeni yapılandırma oluşturuyoruz. Aşağıdaki örneklerdeki gibi ayarlarımızı ekliyoruz.



# Edit IPsec VPN

Enabled

Enable perfect forward secrecy (PFS)

Name

Teletek-test-Ankara

Local Id \*

37.██████████

Local Endpoint \*

37.██████████

SELECT

Local Subnets \*

172.2██████████

Subnets should be entered in CIDR format with comma as separator.

Peer Id \*

195.██████████

Peer Endpoint \*

195.155.195.192

Endpoint should be a valid IP, FQDN or any.

Peer Subnets \*

172.2██████████

Subnets should be entered in CIDR format with comma as separator.

Extension

DISCARD

KEEP

## Edit IPsec VPN



Extension could be passthroughSubnets=192.168.1.0/24, 192.168.2.0

Encryption Algorithm

AES

Authentication

PSK

Change Shared Key



Pre-Shared Key

.....

Display Shared Key



The global pre-shared key (PSK) is shared by all the sites whose peer endpoint is set to 'any'. If a global PSK is already set, changing the PSK to an empty value and saving it has no effect on the existing setting.

Diffie-Hellman Group

DH5

Digest Algorithm

SHA1

IKE Option

IKEv1

IKE Responder Only



Session Type

Policy Based Session

DISCARD

KEEP