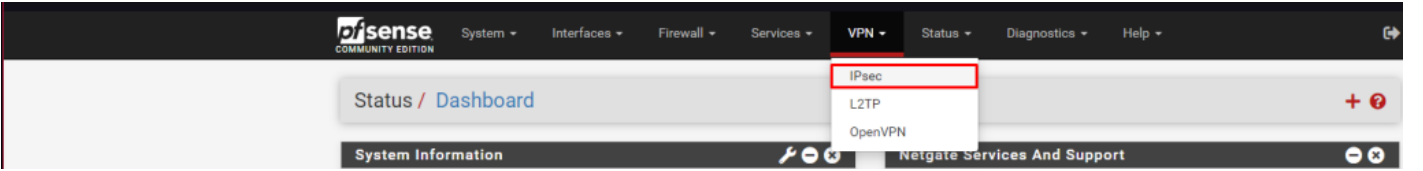


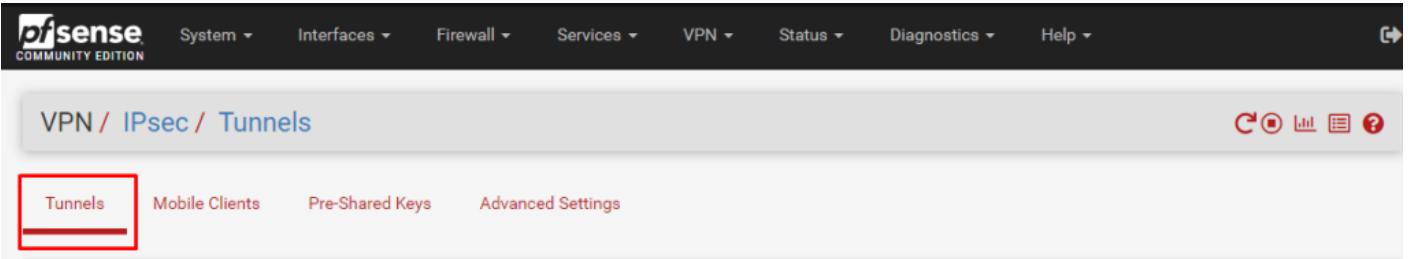
# PFSENSE İLE NSX EDGE ARASINDA IPSEC YAPILANDIRMASI

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

## pfSense UTM Tanımları:

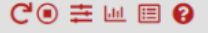


VPN altında IPsec sekmesine giriş yapıyoruz.



Tunnels butonuna geçiş yapıyoruz. Önce Faz1 ayarlarını yapıyoruz.

## VPN / IPsec / Tunnels / Edit Phase 1

[Tunnels](#) [Mobile Clients](#) [Pre-Shared Keys](#) [Advanced Settings](#)

## General Information

Description

Edge to Pfsense

A description may be entered here for administrative reference (not parsed).

Disabled

☐

Set this option to disable this phase1 without removing it from the list.

IKE ID

1

## IKE Endpoint Configuration

Key Exchange version

IKEv1

Select the Internet Key Exchange protocol version to be used. Auto uses IKEv2 when initiator, and accepts either IKEv1 or IKEv2 as responder.

Internet Protocol

IPv4

Select the Internet Protocol family.

Interface

[Redacted]

Dış interface ya da ip adresini seçiyorsunuz

Select the interface for the local endpoint of this phase1 entry.

Remote Gateway

[Redacted]

Uzak uçtaki dış ip adresi yazıyorsunuz

Enter the public IP address or host name of the remote gateway. ⓘ

interface kısmına public ip ve remote gateway kısmına karşı tarafın public ip adresini yazıyoruz.

### Phase 1 Proposal (Authentication)

**Authentication Method**

Mutual PSK

Must match the setting chosen on the remote side.

**Negotiation mode**

Main

Aggressive is more flexible, but less secure.

**My identifier**

My IP address

**Peer identifier**

Peer IP address

**Pre-Shared Key**

••••••••••

 oluşturduğunuz key i giriyorsunuz

Enter the Pre-Shared Key string. This key must match on both peers.  
This key should be long and random to protect the tunnel and its contents. A weak Pre-Shared Key can lead to a tunnel compromise.

Generate new Pre-Shared Key

### Phase 1 Proposal (Encryption Algorithm)

**Encryption Algorithm**

AES

Algorithm

128 bits

Key length

SHA1

Hash

14 (2048 bit)

DH Group

Delete

Edge 'in desteklediği şifreleme algoritmasını görseldeki gibi ayarlıyoruz.  
Note: Blowfish, 3DES, CAST128, MD5, SHA1, and DH groups 1, 2, 5, 22, 23, and 24 provide weak security and should be avoided.

**Add Algorithm**

+ Add Algorithm

### Expiration and Replacement

**Life Time**

28800

Yaşam süresi aynı bırakıyoruz

Hard IKE SA life time, in seconds, after which the IKE SA will be expired. Must be larger than Rekey Time and Reauth Time. Cannot be set to the same value as Rekey Time or Reauth Time. If left empty, defaults to 110% of whichever timer is higher (reauth or rekey)

**Reauth Time**

25920

Time, in seconds, before an IKE SA is torn down and recreated from scratch, including authentication. This can be disruptive unless both sides support make-before-break and overlapping IKE SA entries. Cannot be set to the same value as Life Time. Supported by IKEv1 and IKEv2. Leave blank to use a default value of 90% Life Time when using IKEv1. Enter a value of 0 to disable.

**Rand Time**

2880

A random value up to this amount will be subtracted from Rekey Time/Reauth Time to avoid simultaneous renegotiation. If left empty, defaults to 10% of Life Time. Enter 0 to disable randomness, but be aware that simultaneous renegotiation can lead to duplicate security associations.

Görseldeki gibi Edge 'e uygun algrotima yapısını ve key i ekliyoruz.

**Advanced Options**

Child SA Start Action

Default

Set this option to force specific initiation/responder behavior for child SA (P2) entries

Child SA Close Action

Default

Set this option to control the behavior when the remote peer unexpectedly closes a child SA (P2)

NAT Traversal

Auto

Set this option to enable the use of NAT-T (i.e. the encapsulation of ESP in UDP packets) if needed, which can help with clients that are behind restrictive firewalls.

Gateway duplicates

☐ Enable this to allow multiple phase 1 configurations with the same endpoint. When enabled, pfSense does not manage routing to the remote gateway and traffic will follow the default route without regard for the chosen interface. Static routes can override this behavior.

Custom IKE/NAT-T Ports

Remote IKE Port

Remote NAT-T Port

UDP port for IKE on the remote gateway. Leave empty for default automatic behavior (500/4500).

UDP port for NAT-T on the remote gateway.

Dead Peer Detection

☒ Enable DPD

Check the liveness of a peer by using IKEv2 INFORMATIONAL exchanges or IKEv1 R\_U\_THERE messages. Active DPD checking is only enforced if no IKE or ESP/AH packet has been received for the configured DPD delay.

Delay

10

Delay between sending peer acknowledgement messages. In IKEv2, a value of 0 sends no additional messages and only standard messages (such as those to rekey) are used to detect dead peers.

Max failures

5

Number of consecutive failures allowed before disconnecting. This only applies to IKEv1; in IKEv2 the [retransmission timeout](#) is used instead.

Save

Değişiklik yapmadan save butonuna basabilirsiniz.

Save butonu basarak devam ediyoruz.

**pfSense** COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

VPN / IPsec / Tunnels

Tunnels Mobile Clients Pre-Shared Keys Advanced Settings

**IPsec Tunnels**

	ID	IKE	Remote Gateway	Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Actions
<input checked="" type="checkbox"/>	1	V1	192.168.1.100	main	AES (128 bits)	SHA1	14 (2048 bit)	Edge_to_Pfsense	

Show Phase 2 Entries (1)

Faz 2 ayarları için butona tıklıyoruz

+ Add P1

Delete P1s

Faz 2 ayarların ageçiyoruz.

**pfSense** COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

VPN / IPsec / Tunnels / Edit Phase 2

Tunnels Mobile Clients Pre-Shared Keys Advanced Settings

### General Information

**Description**   
A description may be entered here for administrative reference (not parsed).

**Disabled** ☐ Disable this phase 2 entry without removing it from the list.

**Mode**

**Phase 1** Edge\_to\_Pfsense (IKE ID 1)

**P2 reqid** 1

### Networks

**Local Network**   / 24   
Type  
Local network component of this IPsec security association.

**NAT/BINAT translation**   / 0   
Type  
If NAT/BINAT is required on this network specify the address to be translated

**Remote Network**   / 24   
Type  
Remote network component of this IPsec security association.

local network kısmına lokal ip network ve remote network kısmına karşı tarafın lokal network'ünü ekliyoruz.

### Phase 2 Proposal (SA/Key Exchange)

**Protocol**   
Encapsulating Security Payload (ESP) is encryption, Authentication Header (AH) is authentication only.

**Encryption Algorithms** ☒ AES

☐ AES128-GCM

☐ AES192-GCM

☐ AES256-GCM

☐ Blowfish

☐ 3DES

☐ CAST128

Note: Blowfish, 3DES, and CAST128 provide weak security and should be avoided.

**Hash Algorithms** ☐ MD5 ☒ SHA1 ☐ SHA256 ☐ SHA384 ☐ SHA512 ☐ AES-XCBC

Note: Hash is ignored with GCM algorithms. MD5 and SHA1 provide weak security and should be avoided.

**PFS key group**

Note: Groups 1, 2, 5, 22, 23, and 24 provide weak security and should be avoided.

Algoartima ve protokol görseldeki gibi ayarlıyoruz.

**Expiration and Replacement**

Life Time

3600

Hard Child SA life time, in seconds, after which the Child SA will be expired. Must be larger than Rekey Time. Cannot be set to the same value as Rekey Time. If left empty, defaults to 110% of Rekey Time. If both Life Time and Rekey Time are empty, defaults to 3960.

Rekey Time

3240

Time, in seconds, before a Child SA establishes new keys. This works without interruption. Cannot be set to the same value as Life Time. Leave blank to use a default value of 90% Life Time. If both Life Time and Rekey Time are empty, defaults to 3600. Enter a value of 0 to disable, but be aware that when rekey is disabled, connections can be interrupted while new Child SA entries are negotiated.

Rand Time

360

A random value up to this amount will be subtracted from Rekey Time to avoid simultaneous renegotiation. If left empty, defaults to 10% of Life Time. Enter 0 to disable randomness, but be aware that simultaneous renegotiation can lead to duplicate security associations.

**Keep Alive**

Automatically ping host

Sends an ICMP echo request inside the tunnel to the specified IP Address. Can trigger initiation of a tunnel mode P2, but does not trigger initiation of a VTI mode P2.

Keep Alive

☐ Enable periodic keep alive check

Periodically checks to see if the P2 is disconnected and initiates when it is down. Does not send traffic inside the tunnel. Works for VTI and tunnel mode P2 entries. For IKEv2 without split connections, this only needs enabled on one P2.

Save

Değişiklik yapmadan save butonuna basıyoruz.

**disense**  
COMMUNITY EDITION

























System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾






Firewall / Rules / WAN

Floating **WAN** LAN IPsec

Aliases  
NAT  
**Rules**  
Schedules  
Traffic Shaper  
Virtual IPs

**Rules (Drag to Change Order)**

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0 / 0 B	IPv4 TCP	18	*	172	3389 (MS RDP)	*	none	NAT	  
<input type="checkbox"/>	✓	0 / 0 B	IPv4 TCP	17	*	LAN	*	*	none	IPsec- Local	  
<input type="checkbox"/>	✓	0 / 0 B	IPv4 TCP	37	*	195	500 (ISAKMP)	*	none	IPSEC	  
<input type="checkbox"/>	✓	0 / 0 B	IPv4 TCP	37	*	195	4500 (IPsec NAT-T)	*	none	IPSEC	  
<input type="checkbox"/>	✓	0 / 0 B	IPv4 TCP	18	*	*	*	*	none	Hakki EV	  
<input type="checkbox"/>	✓	0 / 0 B	IPv4 TCP	19	*	*	*	*	none	VPN	  
<input type="checkbox"/>	✓	2 / 289 KiB	IPv4 TCP	94	*	*	*	*	none	VPN	  
<input type="checkbox"/>	✗	0 / 39 KiB	IPv4 TCP	*	*	*	*	*	none	Default Deny	  

 Add  Add  Delete  Save  Separator

Firewall kurallarını ekliyoruz.

pfSense COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

Firewall / Rules / WAN

Floating WAN LAN IPsec

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	0 / 0 B	IPv4 TCP	Remote ip adresi	*	LAN net	*	*	none		IPsec-Local	

pfSense COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

Firewall / Rules / WAN

Floating WAN LAN IPsec

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	0 / 0 B	IPv4 TCP	Remote Public ip	*	Public ip	500 (ISAKMP)	*	none		IPSEC	
<input type="checkbox"/>	0 / 0 B	IPv4 TCP	Remote Public ip	*	Public ip	4500 (IPsec NAT-T)	*	none		IPSEC	

pfSense COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

Firewall / Rules / IPsec

Floating WAN LAN IPsec

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	0 / 0 B	IPv4 TCP	Remote local ip adresi	*	LAN net	*	*	none		IPsec_ Local Rule	

Add Add Delete Save Separator

pfSense COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

VPN / IPsec / Tunnels

Tunnels Mobile Clients Pre-Shared Keys Advanced Settings

Yaptığımız ipsec yapılandırmasını aktif etmek için resimdeki simgeye tıklıyoruz

**pfSense** COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Status / IPsec / Overview

Overview Leases SADs SPDs

### IPsec Status

ID	Description	Local	Remote	Role	Timers	Algo	Status
con1 #2	Edge_to_Pfsense	ID: 105-155-105-100 Host: 105-155-105-100:500 SPI: cb7670237f432086	ID: 37-9-2-100-500 Host: 37-9-2-100-500:500 SPI: 6ffbb5f2a032ae07	IKEv1 Responder	Reauth: 21103s (05:51:43)	AES_CBC (128) HMAC_SHA1_96 PRF_HMAC_SHA1 MODP_2048	Established 4571 seconds (01:16:11) ago <a href="#">Disconnect P1</a>

ID	Description	Local	SPI(s)	Remote	Times	Algo	Stats
con1_1: #4	Edge_to_Pfsense	172.20.1.1/24	Local: c186bac0 Remote: c3034585	172.20.1.1	Rekey: 1245s (00:20:45) Life: 1704s (00:28:24) Install: 1896s (00:31:36)	AES_CBC (128) HMAC_SHA1_96 MODP_2048 IPComp: None	Bytes-In: 134,820 (132 KiB) Packets-In: 2,247 Bytes-Out: 224,160 (219 KiB) Packets-Out: 1,868 Installed <a href="#">Disconnect P2</a>

Connetc/disconnect butonlarından ipsec bağlantımızı aktif/pasif yapabiliyoruz.

## NSX Edge Tanımları:

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

Edge Gateways

EXPORT EDGE GATEWAYS

Name	Status	Scope	Distributed Routing	Used NICs	External Networks	Org VDC Networks	HA State
TeletekDEMO_	Normal	TeletekDEMO_	Disabled	5	1	4	Disabled

Ekrandaki mavi yazılı kısma çift tıklayarak devam ediyoruz.

All Edge Gateways > TeletekDEMO\_

TeletekDEMO\_ SERVICES OPEN IN VDC CONTEXT

### General

Name	TeletekDEMO_
Description	-
Status	Normal
Distributed Routing	Disabled
FIPS Mode	Disabled
Edge Gateway Configuration	Large
High Availability	Disabled
Syslog Server Settings	-

### Scope

Organization Virtual Data Center	TeletekDEMO_
Organization	TeletekDEMO_

Yeni açılan sayfada "SERVICES" kısmına çift tıklıyoruz.



## Firewall Rules

Enabled ☒[+](#) [x](#) [+](#) [+](#)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

[+](#) [x](#) [x](#)

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

Revision #2

Created 29 April 2024 21:41:42 by Teletek

Updated 19 July 2024 01:39:20 by Teletek