

DrayTek'den Palo Alto'ya IPSec VPN Tüneli Oluşturma

Draytek

VPN and Remote Access >>LAN to LAN'a gidin ve indexlerden herhangi birine tıklayın.

Bu bölümde aşağıdaki parametreleri yapılandıracağız:

- Profil Adı: VPN_DR_PA
- Profili etkinleştir
- Call Direction: Dial-Out'u seçin
- Tunnel Mode: Always on'u seçin
- VPN Dial-Out Through: Önce WAN1'i seçin ve WAN bağlantı noktasının IP adresini seçin.

Profile Index : 2
1. Common Settings

Profile Name <input type="text" value="VPN_DR_PA"/> <input checked="" type="checkbox"/> Enable this profile VPN Dial-Out Through WAN1 First 1-113.190.242. Netbios Naming Packet <input checked="" type="radio"/> Pass <input type="radio"/> Block Multicast via VPN <input type="radio"/> Pass <input checked="" type="radio"/> Block (for some IGMP,IP-Camera,DHCP Relay..etc.)	Call Direction <input type="radio"/> Both <input checked="" type="radio"/> Dial-Out <input type="radio"/> Dial-in Tunnel Mode <input type="radio"/> GRE Tunnel <input checked="" type="checkbox"/> Always on Idle Timeout -1 second(s) <input type="checkbox"/> Enable PING to keep IPsec tunnel alive PING to the IP
--	--

Dial-Out Ayarlarını Yapılandırma

Bu bölümde aşağıdaki parametreleri yapılandıracağız:

- Type of server I am calling : IPSec Tüneli IKEv1'i seçin
- VPN için Sunucu IP/Ana Bilgisayar Adı: Palo Alto'nun WAN IP adresini girin.
- IKE Kimlik Doğrulama Yöntemi: Pre-shared Key'I seçin ve yanındaki kutuya parolayı girin. (Palo Alto tarafı için aynı şifreyi girmek için bu şifreyi unutmayın)
- IPSec Güvenlik Yöntemi: High(ESP) kutusunu işaretleyin ve kimlik doğrulamalı 3DES'i seçin.
- Ardından Advanced'e tıklayın,

2. Dial-Out Settings

Type of Server I am calling <input type="radio"/> PPTP <input checked="" type="radio"/> IPsec Tunnel <input type="text" value="IKEv1"/> <input type="radio"/> IPsec EAP <input type="radio"/> L2TP with IPsec Policy <input type="text" value="None"/> <input type="radio"/> SSL Tunnel Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89) 113.161.93 Server Port (for SSL Tunnel): 443	Username <input type="text" value="???"/> Password <input type="text" value="Max: 15 characters"/> PPP Authentication PAP/CHAP/MS-CHAP/MS-CHAPv2 VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off IKE Authentication Method <input checked="" type="radio"/> Pre-Shared Key IKE Pre-Shared Key <input type="text" value="*****"/> <input type="radio"/> Digital Signature(X.509) Peer ID <input type="text" value="None"/> Local ID <input checked="" type="radio"/> Alternative Subject Name First <input type="radio"/> Subject Name First Local Certificate <input type="text" value="None"/> IPsec Security Method <input type="radio"/> Medium(AH) <input checked="" type="radio"/> High(ESP) 3DES with Authentication Advanced Schedule Profile <input type="text" value="None"/> <input type="text" value="None"/> <input type="text" value="None"/> <input type="text" value="None"/>
--	---

IKE Advanced ayarlar paneli görünür, aşağıdaki parametrelerle yapılandıracağız.

- IKE phase 1 modu (IKEv1): main modu seçin
- IKE phase 1 proposal: 3DES_MD5_G2'yi seçin
- IKE ifade 2 proposal: 3DES_MD5'i seçin
- IKE phase 1 key lifetime: 28800
- IKE phase 2 key lifetime: 3600
- Perfect Forward Secret: disable seçin.
- Kaydetmek için Tamam'ı tıklayın.

IKE advanced settings

IKE phase 1 mode(IKEv1) ☒ Main mode ☐ Aggressive mode

IKE phase 1 proposal 3DES_MD5_G2

IKE phase 2 proposal 3DES_MD5

IKE phase 1 key lifetime 28800 (900 ~ 86400)

IKE phase 2 key lifetime 3600 (600 ~ 86400)

Perfect Forward Secret ☒ Disable ☐ Enable

Local ID

OK Close

Note:
If you select "Auto" as IKE phase 1 proposal, router will send the following proposals sequentially to negotiate with the remote site:
1. AES256_(SHA256/SHA1/MD5)_G14
2. AES256_(SHA1/MD5)_G5
3. AES192_(SHA1/MD5)_G14
4. AES128_(SHA1/MD5)_G5
5. 3DES_(SHA1/MD5)_G5

G1= Group1, 786 bit / G2= Group2, 1024 bit / G5= Group5, 1536 bit / G14= Group14, 2048 bit

TCP/IP Ağ Ayarlarını Yapılandırma

Bu bölümde aşağıdaki parametreleri yapılandıracağız:

- Uzak Ağ IP'si: Palo Alto'nun LAN IP'sini yazın
- Uzak Ağ Maskesini seçin
- Yerel Ağ IP'si: Draytek'in LAN IP'sini girin
- Yerel Ağ Maskesini seçin
- Tamam'ı tıklayın.

5. TCP/IP Network Settings

My WAN IP	0.0.0.0	RIP Direction	Disable
Remote Gateway IP	0.0.0.0	From first subnet to remote network, you have to do	Route
Remote Network IP	10.146.41.1	<input type="checkbox"/> IPsec VPN with the Same Subnets	
Remote Network Mask	255.255.255.0 / 24	<input type="checkbox"/> Change default route to this VPN tunnel (Only active if one single WAN is up)	
Local Network IP	192.168.4.1		
Local Network Mask	255.255.255.0 / 24		
	More		

LAN-to-LAN Profilleri paneline geri dönün ve yeni oluşturulan dizin profili için Etkinleştir'i seçin ve bu profili etkinleştirmek için Tamam'a tıklayın.

Palo Alto PA-220**Zone Oluştur**

VPN bağlantıları için zone oluşturmamız gerekiyor.

Oluşturmak için Network > Zones'e gidin.

Ekle'ye tıklayın ve aşağıdaki bilgilere göre oluşturun:

- İsim: VPN
- Type: Layer3
- Tamam'ı tıklayın.

Zone

Name: VPN

Log Setting: None

Type: Layer3

Interfaces

Zone Protection

Zone Protection Profile: None

Enable Packet Buffer Protection

User Identification ACL

Enable User Identification

Include List

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

Add Delete

Users from these addresses/subnets will be identified.

Exclude List

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

Add Delete

Users from these addresses/subnets will not be identified.

OK Cancel

Yapılandırma değişikliklerini kaydetmek için Kabul Et ve Tamam'a tıklayın.

Adres Nesnesi Oluştur

Palo Alto ve Draytek cihazlarının 2 LAN katmanını için Adres Nesnesi oluşturacağız.

Oluşturmak için Object > Adresler'e gidin.

Ekle'ye tıklayın ve aşağıdaki parametrelere göre oluşturun.

Palo Alto LAN'ı:

- İsim: PA_LAN
- Type: IP Netmask
- Tamam'ı tıklayın.

Address

Name PA_LAN

Description

Type IP Netmask 10.146.41.0/24 [Resolve](#)

Enter an IP address or a network using the slash notation (Ex. 192.168.80.150 or 192.168.80.0/24). You can also enter an IPv6 address or an IPv6 address with its prefix (Ex. 2001:db8:123:1::1 or 2001:db8:123:1::/64)

Tags

OK Cancel

Draytek_LAN:

- İsim: Draytek_LAN
- Type: IP Netmask
- Tamam'ı tıklayın.

Address

Name Draytek_LAN

Description

Type IP Netmask 192.168.4.0/24 [Resolve](#)

Enter an IP address or a network using the slash notation (Ex. 192.168.80.150 or 192.168.80.0/24). You can also enter an IPv6 address or an IPv6 address with its prefix (Ex. 2001:db8:123:1::1 or 2001:db8:123:1::/64)

Tags

OK Cancel

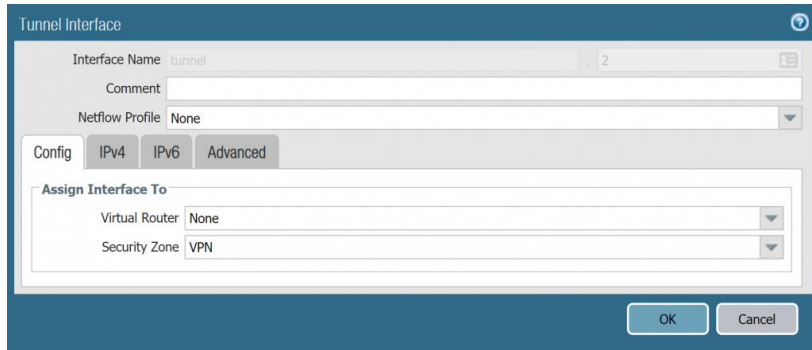
Yapılandırma değişikliklerini kaydetmek için Kabul Et ve Tamam'a tıklayın.

Tunnel Interface Oluştur

Oluşturmak için Network > Interface > Tunnel'e gidin.

Ekle'ye tıklayın ve aşağıdaki bilgilere göre oluşturun:

- Interface Name: tunnel – 2
- Virtual Router: Yok
- Security Zone: VPN
- Tamam'ı tıklayın.



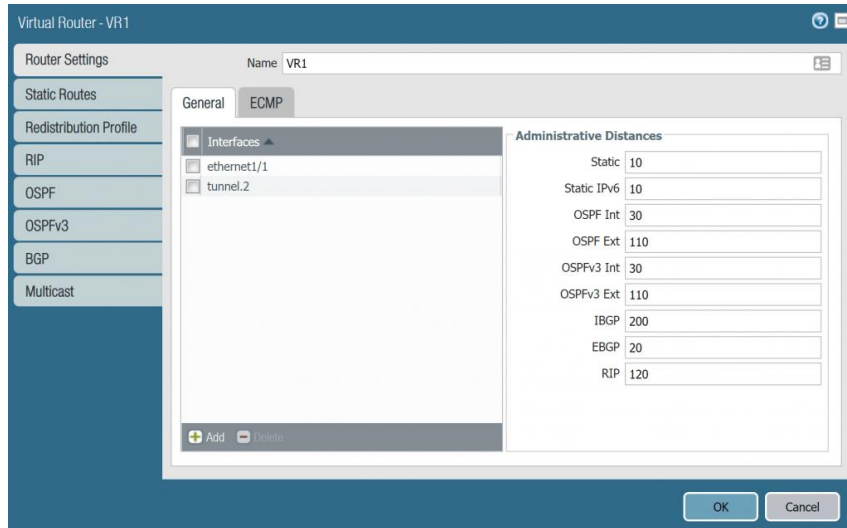
Yapılandırma değişikliklerini kaydetmek için Kabul Et ve Tamam'a tıklayın.

Virtual Routers Oluşturun

Sanal Yönlendiriciler oluşturmak için Network > Virtual Routers > Ekle'ye gidin ve aşağıdaki bilgilere göre yapılandırın.

Router Sekme Ayarları:

- İsim: VR1
- General : Ekle'ye tıklayın ve vlan portlarını (LAN portu), ethernet1/1 (internet portu) ve tünel.2'yi (VPN bağlantısı için kullanılan tünel) seçin.



Static Route > IPv4:

Statik yollar eklemek için Ekle'ye tıklayın ve aşağıdaki bilgileri doldurun:

- İsim: VPN_PA_2_Draytek
- Destination: Draytek_LAN
- Interface: tunnel.2
- 2 kez Tamam'ı tıklayın.

Virtual Router - Static Route - IPv4

Name

VPN_PA_2_Draytek

Destination

Draytek_LAN

Interface

tunnel.2

Next Hop

None

Admin Distance

10 - 240

Metric

10

Route Table

Unicast

☐ Path Monitoring

Failure Condition

☒ Any ☐ All

Preemptive Hold Time (min)

2

<input type="checkbox"/>	Name	Enable	Source IP	Destination IP	Ping Interval(sec)	Ping Count
--------------------------	------	--------	-----------	----------------	--------------------	------------

+ Add

- Delete

OK

Cancel

Yapılandırma değişikliklerini kaydetmek için Kabul Et ve Tamam'a tıklayın.

IKE Kripto Oluştur

VPN bağlantısı için IKE Crypto yani Phrase 1 oluşturacağız.

Oluşturmak için Network > IKE Crypto'ya gidin ve Ekle'ye tıklayın ve aşağıdaki bilgilere göre oluşturun:

- İsim: VPN_PA_2_Draytek_Phase1
- DH Grubu: grup2
- Şifreleme: 3des
- Kimlik doğrulama: md5
- Key Lifetime :Seconds – 28800
- Tamam'ı tıklayın

The screenshot shows the 'IKE Crypto Profile' configuration window. The 'Name' field is 'VPN_PA_2_Draytek_Phase1'. The 'DH Group' section has 'group2' selected. The 'Encryption' section has '3des' selected. The 'Authentication' section has 'md5' selected. The 'Timers' section shows 'Key Lifetime' set to 'Seconds' and '28800', and 'Ikev2 Authentication Multiple' set to '0'. The 'Minimum lifetime = 3 mins' is also displayed. The 'OK' and 'Cancel' buttons are at the bottom right.

Yapılandırma değişikliklerini kaydetmek için Kabul Et ve Tamam'a tıklayın.

IPSec Crypto'yu yapılandırın

IPSec Crypto oluşturmak için Network > IPSec Crypto'ya gidin ve Ekle'ye tıklayın.

Aşağıdaki parametrelere göre yapılandırın:

- İsim: VPN_PA_2_Draytek_Phase2
- IPSec Protokolü: ESP
- Şifreleme: 3des
- Kimlik doğrulama: md5
- DH Grubu: no-pfs
- Lifetime: Second – 3600
- Tamam'ı tıklayın

IPSec Crypto Profile

Name: VPN_PA_2_Draytek_Phase2

IPSec Protocol: ESP

Encryption

☒ 3des

Authentication

☒ md5

DH Group: no-pfs

Lifetime: Seconds 3600

Minimum lifetime = 3 mins

☐ Enable

Lifesize: MB [1 - 65535]

Recommended lifesize is 100MB or greater

OK Cancel

Yapılandırma değişikliklerini kaydetmek için Kabul Et ve Tamam'a tıklayın.

IKE Gateway oluşturun

Oluşturmak için Network > IKE Gateways'e gidin ve Ekle'ye tıklayın.

Aşağıdaki parametrelere göre yapılandırın

Genel:

- İsim: VPN_PA_2_Draytek_IKE
- Sürüm: IKEv1 only mode
- Adres Türü: IPv4
- Arayüz: ethernet1/1 (Palo Alto'nun WAN portu)
- Yerel IP Adresi: Yok
- Peer Adres : 113.190.242.x
- Kimlik Doğrulama: Pre-shared key
- Pre-shared key : bağlantı şifresini girin (bu şifre Draytek'te ayarlanan şifre ile aynı olmalıdır)
- Pre-shared keyi onaylayın: bağlantı parolasını yeniden girin.

IKE Gateway

General Advanced Options

Name VPN_PA_2_Draytek_IKE

Version IKEv1 only mode

Address Type ☒ IPv4 ☐ IPv6

Interface ethernet1/1

Local IP Address None

Peer IP Address Type ☒ IP ☐ FQDN ☐ Dynamic

Peer Address 113.190.242

Authentication ☒ Pre-Shared Key ☐ Certificate

Pre-shared Key

Confirm Pre-shared Key

Local Identification None

Peer Identification None

OK Cancel

Gelişmiş seçenekler:

- Exchange Mode: select main
- IKE Kripto Profili: VPN_PA_2_Draytek_Phase1
- Tamam'ı tıklayın.

The screenshot shows the 'IKE Gateway' configuration window with the 'Advanced Options' tab selected. The 'Common Options' section has two unchecked checkboxes: 'Enable Passive Mode' and 'Enable NAT Traversal'. The 'IKEv1' section has a dropdown for 'Exchange Mode' set to 'main', a dropdown for 'IKE Crypto Profile' set to 'VPN_PA_2_Draytek_Phrase1', and an unchecked checkbox for 'Enable Fragmentation'. The 'Dead Peer Detection' section is checked, with 'Interval' and 'Retry' both set to '5'. At the bottom right are 'OK' and 'Cancel' buttons.

Yapılandırma değişikliklerini kaydetmek için Kabul Et ve Tamam'a tıklayın.

IPSec Tünelleri Oluşturun

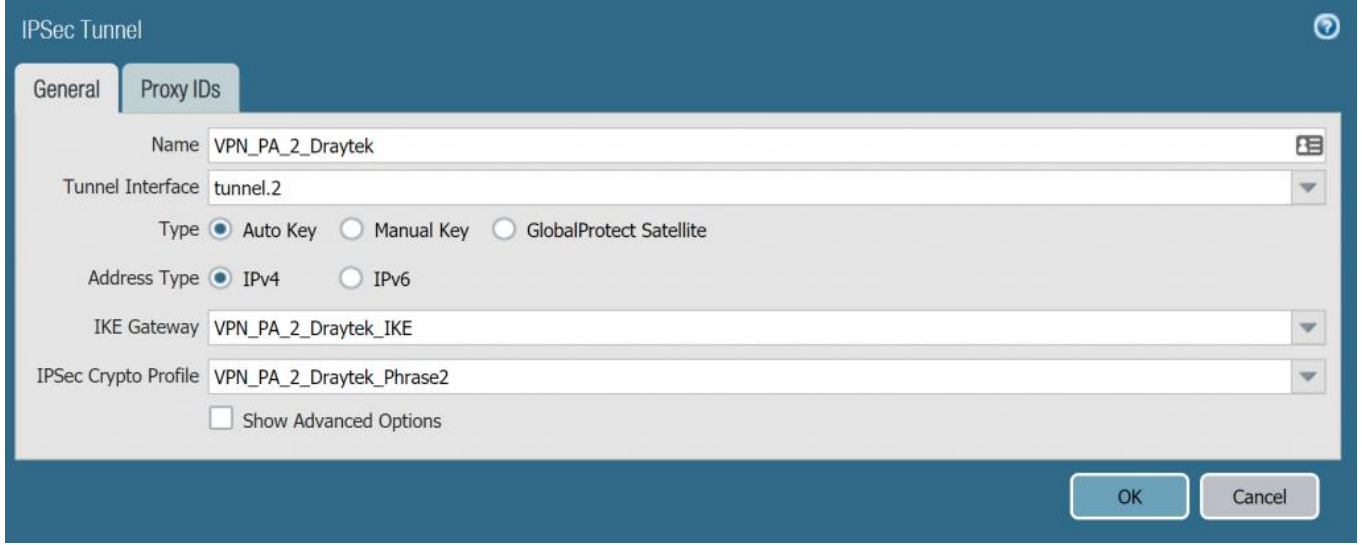
Şimdi Draytek cihazı ile VPN bağlantısı oluşturmaya başlayacağız.

Oluşturmak için Network > IPSec Tunnels'e gidin ve Ekle'ye tıklayın.

Aşağıdaki bilgilerle oluşturun.

General Sekmesi:

- İsim: VPN_PA_2_Draytek
- Tünel Arayüzü: tunnel.2
- Tür: Auto Key
- Adres Türü: IPv4
- IKE Gateway: VPN_PA_2_Draytek_IKE
- IPSec Kripto Profili: VPN_PA_2_Draytek_Phrase2



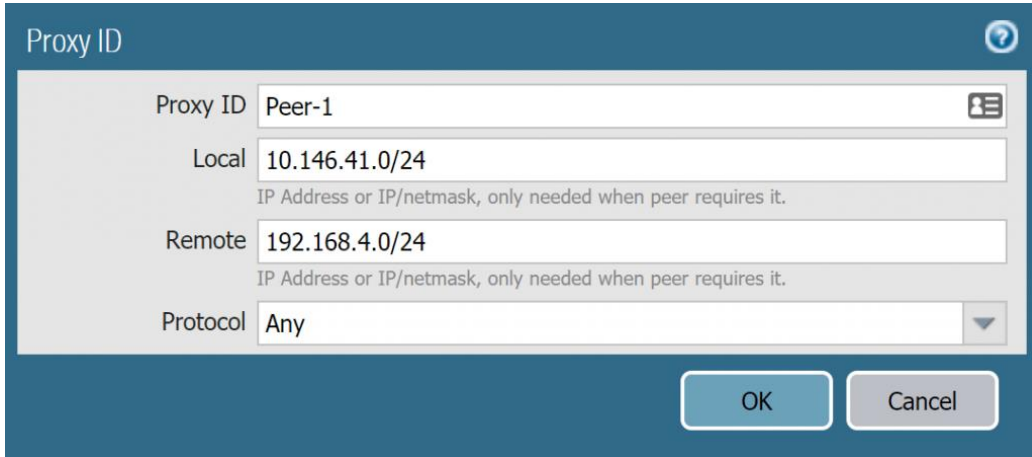
The image shows the 'IPSec Tunnel' configuration window with the 'General' tab selected. The 'Name' field is 'VPN_PA_2_Draytek'. The 'Tunnel Interface' is 'tunnel.2'. The 'Type' is 'Auto Key'. The 'Address Type' is 'IPv4'. The 'IKE Gateway' is 'VPN_PA_2_Draytek_IKE'. The 'IPSec Crypto Profile' is 'VPN_PA_2_Draytek_Phase2'. There is a checkbox for 'Show Advanced Options' which is unchecked. At the bottom right are 'OK' and 'Cancel' buttons.

Field	Value
Name	VPN_PA_2_Draytek
Tunnel Interface	tunnel.2
Type	Auto Key
Address Type	IPv4
IKE Gateway	VPN_PA_2_Draytek_IKE
IPSec Crypto Profile	VPN_PA_2_Draytek_Phase2

Proxy IDs Sekmesi:

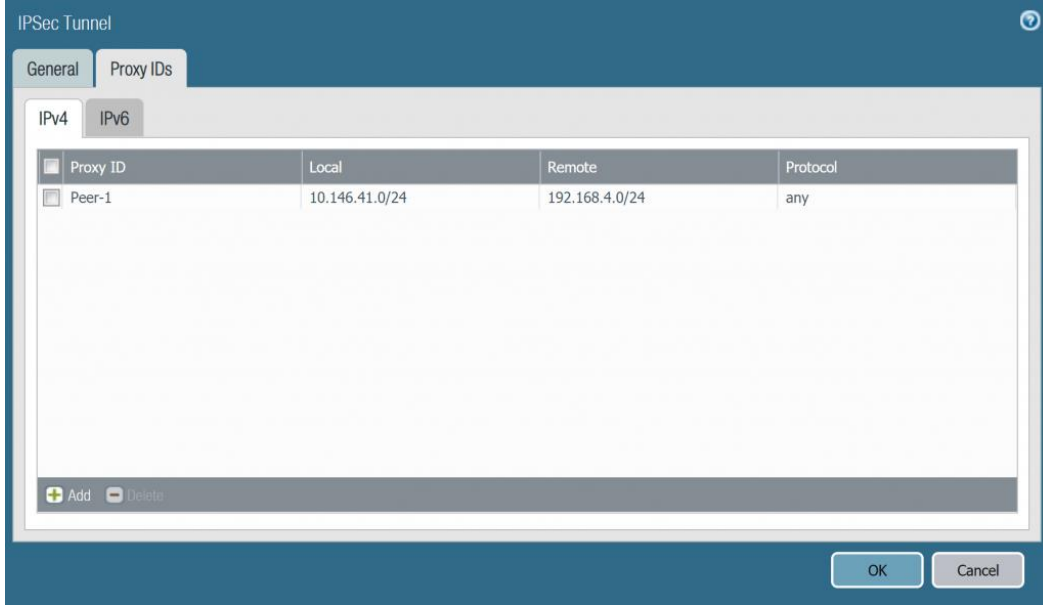
Ekle'ye tıklayın ve aşağıdaki bilgileri yapılandırın:

- Proxy ID: Peer-1
- Local: 10.146.41.0/24
- Remote: 192.168.4.0/24
- Protokol: Any
- 2 kez Tamam'ı tıklayın.



The image shows the 'Proxy ID' configuration window. The 'Proxy ID' field is 'Peer-1'. The 'Local' field is '10.146.41.0/24'. The 'Remote' field is '192.168.4.0/24'. The 'Protocol' field is 'Any'. Below the 'Local' and 'Remote' fields, there is a note: 'IP Address or IP/netmask, only needed when peer requires it.' At the bottom right are 'OK' and 'Cancel' buttons.

Field	Value
Proxy ID	Peer-1
Local	10.146.41.0/24
Remote	192.168.4.0/24
Protocol	Any



IPsec Tünellerini oluşturduktan sonra yeni oluşturduğumuz tünele tıklıyoruz ve bu tüneli etkinleştirmek için Enable tıklıyoruz.

Yapılandırma değişikliklerini kaydetmek için Kabul Et ve Tamam'a tıklayın.

Policy Oluştur

Palo Alto'nun LAN katmanından gelen trafiğin Draytek'in LAN katmanından geçmesi için tersi yönde bir policy oluşturmamız gerekiyor.

Policy oluşturmak için Policies > Security'e gidin ve Ekle'ye tıklayın.

Aşağıdaki bilgilerle Palo Alto'nun LAN katmanından gelen trafiğin Draytek'in LAN katmanından geçmesine izin veren bir policy oluşturun:

General Sekmesi:

- İsim: VPN_PA_Draytek
- Kural Türü: universal (default)

Security Policy Rule

General Source User Destination Application Service/URL Category Actions

Name: VPN_PA_Draytek

Rule Type: universal (default)

Description:

Tags:

Group Rules By Tag: None

Audit Comment:

[Audit Comment Archive](#)

OK Cancel

Source Sekmesi:

- Source Zone: Ekle'ye tıklayın ve Trust-Layer3'ü seçin (Bu, LAN katmanının bölgesidir)
- Source Address: Ekle'ye tıklayın ve PA_LAN'ı seçin (PA_LAN, daha önce oluşturduğumuz Adres Nesnesidir)

Security Policy Rule

General Source User Destination Application Service/URL Category Actions

Any

Source Zone

Trust-Layer3

Any

Source Address

PA_LAN

+ Add - Delete

+ Add - Delete

Negate

OK Cancel

Destination Sekmesi:

- Destination Zone: VPN
- Destination Address: Draytek-LAN (başlangıçta oluşturulan Adres Objesidir)

The screenshot shows the 'Security Policy Rule' configuration window with the 'Destination' tab selected. The window has tabs for General, Source, User, Destination, Application, Service/URL Category, and Actions. The 'Destination' tab contains two main sections: 'Destination Zone' and 'Destination Address'. In the 'Destination Zone' section, 'VPN' is selected. In the 'Destination Address' section, 'Draytek_LAN' is selected. There are 'Add' and 'Delete' buttons for each section. A 'Negate' checkbox is at the bottom. 'OK' and 'Cancel' buttons are at the bottom right.

Actions Sekmesi:

- Action: Allow'u seçin.
- Tamam'ı tıklayın.

The screenshot shows the 'Security Policy Rule' configuration window with the 'Actions' tab selected. The window has tabs for General, Source, User, Destination, Application, Service/URL Category, and Actions. The 'Actions' tab contains three main sections: 'Action Setting', 'Log Setting', and 'Other Settings'. In the 'Action Setting' section, 'Allow' is selected in the 'Action' dropdown, and 'Send ICMP Unreachable' is unchecked. In the 'Log Setting' section, 'Log at Session End' is checked, and 'Log Forwarding' is set to 'None'. In the 'Other Settings' section, 'Schedule' and 'QoS Marking' are both set to 'None', and 'Disable Server Response Inspection' is unchecked. 'OK' and 'Cancel' buttons are at the bottom right.

Ardından, Ekle'yi tıklatacağız ve trafiğin Draytek'in LAN katmanından Palo Alto'nun LAN katmanına aşağıdaki bilgilerle gitmesine izin veren bir policy oluşturacağız:

General Sekmesi:

- İsim: VPN_Draytek_2_PA
- Kural Türü: universal (default)

The screenshot shows the 'Security Policy Rule' configuration window with the 'General' tab selected. The 'Name' field is filled with 'VPN_Draytek_2_PA'. The 'Rule Type' dropdown is set to 'universal (default)'. The 'Description' field is empty. The 'Tags' dropdown is empty. The 'Group Rules By Tag' dropdown is set to 'None'. The 'Audit Comment' field is empty. At the bottom right, there are 'OK' and 'Cancel' buttons. A link for 'Audit Comment Archive' is visible below the 'Audit Comment' field.

General	Source	User	Destination	Application	Service/URL Category	Actions
<p>Name: VPN_Draytek_2_PA</p> <p>Rule Type: universal (default)</p> <p>Description:</p> <p>Tags:</p> <p>Group Rules By Tag: None</p> <p>Audit Comment:</p> <p>Audit Comment Archive</p> <p>OK Cancel</p>						

Source Sekmesi:

- Source Zone: Ekle'ye basın ve VPN'i seçin
- Source Address: Ekle'ye tıklayın ve Draytek_LAN'ı seçin (Draytek_LAN, daha önce oluşturduğumuz Adres Nesnesidir)

Security Policy Rule

General Source User Destination Application Service/URL Category Actions

Any

Source Zone ▲

VPN

Source Address ▲

Draytek_LAN

Add Delete

Add Delete

Negate

OK Cancel

Destination Sekmesi:

- Destination Zone: Trust-Layer3 (LAN katmanının bölgesi)
- Destination Address: PA-LAN (Başlangıçta oluşturulan Adres Objesidir)

Security Policy Rule

General Source User Destination Application Service/URL Category Actions

select

Destination Zone ▲

Trust-Layer3

Destination Address ▲

PA_LAN

Add Delete

Add Delete

Negate

OK Cancel

Action Sekmesi:

- Action: Allow'u seçin.
- Tamam'ı tıklayın.

Security Policy Rule

General Source User Destination Application Service/URL Category Actions

Action Setting

Action: Allow

☐ Send ICMP Unreachable

Log Setting

☐ Log at Session Start

☒ Log at Session End

Log Forwarding: None

Profile Setting

Profile Type: None

Other Settings

Schedule: None

QoS Marking: None

☐ Disable Server Response Inspection

OK Cancel

Sonuç

Sonuçları Palo Alto cihazında kontrol etmek için Network > IPSec Tunnels'e gidin.

Tünelde 2 durum noktası ve yeşil IKE Gateway göreceğiz, bu da VPN bağlantısının başarıyla kurulduğu anlamına gelir.

Name	Status	Type	Interface	Local IP	Peer Address	Status	Interface	Virtual Router	Virtual System	Security Zone	Status
S2S-DYNM-DACL-IPsec-Tunnel	Tunnel Info	Auto Key	ethernet1/1			IKE Info	tunnel.10	VR1 (Show Routes)	vsys1	VPN	
VPN_PA_2_Draytek	Tunnel Info	Auto Key	ethernet1/1		113.190.242	IKE Info	tunnel.2	VR1 (Show Routes)	vsys1	VPN	

Draytek cihazına geçin, VPN and Remote Access > Connection Management bölümüne giderek VPN bağlantısının başarılı olup olmadığını kontrol edebilirsiniz.

VPN bağlantısının kurulduğunu, bağlantının durumunu, ne zaman bağlandığını vb. göreceksiniz.

VPN Connection Status

All VPN Status		LAN-to-LAN VPN Status			Remote Dial-in User Status				
VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate(bps)	Rx Pkts	Rx Rate(Kbps)	UpTime	
1 (VPN_DQCD9)	IPsec Tunnel 3DES-MD5 Auth	203.205.26. via WAN1	172.16.20.1/20	37106	712	168464	1528	30:7:15	Drop
2 (VPN_DR_PA)	IPsec Tunnel 3DES-MD5 Auth	113.161.93. via WAN1	10.146.41.1/24	0	0	223	1120	0:11:40	Drop

xxxxxxx : Data is encrypted.
xxxxxxx : Data isn't encrypted.