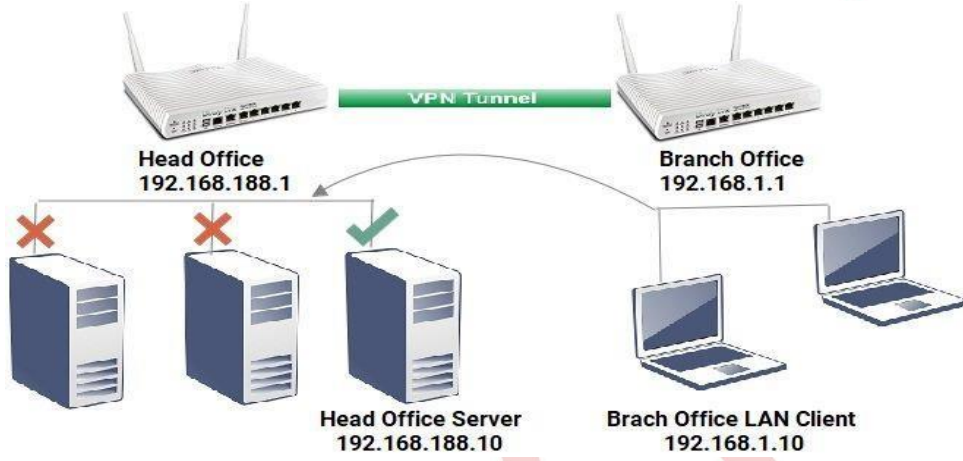


Uzak VPN Ağının Belirli IP'ye Erişimini Kısıtlama

VPN, Local network ile Remote network arasında güvenli bir bağlantı sağlar. VPN kurulduktan sonra, Remote Network Local Networkteki tüm cihazlara fiziksel olarak bağlanmış gibi erişebilir. Ancak, yalnızca belirli bir sunucuya erişmek için Remote Network için VPN'i kurarsak? Bu makale, Routerin nasıl yapılandırılacağını ve Remote VPN kullanıcılarının sadece aşağıdaki senaryo için belirli bir Local sunucu ile nasıl kısıtlanacağını gösterecektir.



DrayOS

Bunu başarmanın iki yolu vardır: VPN Configuration ve Firewall Rules.

1.Yöntem 1: VPN Yapılandırması ile

- Branch Office'de Vigor Router'ın LAN-LAN VPN profilinde, Remote Network IP'sini tüm ağdan sadece sunucunun IP'sine çevirin.

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	192.168.188.10	<input type="checkbox"/> IPsec VPN with the Same Subnets	
Remote Network Mask	255.255.255.255	<input type="checkbox"/> Change default route to this VPN tunnel (Only active if one single WAN is up)	
Local Network IP	192.168.1.0		
Local Network Mask	255.255.255.0		
<input type="button" value="More"/>			

- Head Office'deki Vigor Router'ın LAN-LAN VPN profilinde, Local Network IP'sini tüm ağdan sadece sunucunun IP'sine değiştirin.

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	192.168.1.0	<input type="checkbox"/> IPsec VPN with the Same Subnets	
Remote Network Mask	255.255.255.0	<input type="checkbox"/> Change default route to this VPN tunnel (Only active if one single WAN is up)	
Local Network IP	192.168.188.10		
Local Network Mask	255.255.255.255		
<input type="button" value="More"/>			

3. VPN kurulduğunda, Branch Office Router, yönlendirme bilgisine sadece sunucunun IP 192.168.188.10/32 bilgisine sahip olacak, böylece Branch Office'teki istemciler sadece sunucuya erişebilecektir.

Diagnostics >> View Routing Table

IPv4

Key	Destination	Gateway	Interface
*	0.0.0.0/ 0.0.0.0	via 192.168.239.1	WAN2
C~	192.168.1.0/ 255.255.255.0	directly connected	LAN1
C	192.168.239.0/ 255.255.255.0	directly connected	WAN2
S~	192.168.188.10/ 255.255.255.255	via 192.168.239.16	VPN-1

| Refresh |

2.Yöntem 2: Firewall Kuralı'na Göre

- Branch Office'deki bağlantıyı sınırlandırmak için genel merkez Router'indeki firewall kuralını oluşturabiliriz. İlk önce **Objects Setting >> IP Object'e** gidin, serverin IP'si için bir IP Object profili oluşturmak için uygun bir indexe tıklayın:
- Nesneyi tanımlamak için Name girin
- Interface için "LAN / DMZ / RT / VPN" seçeneğini seçin
- Address Type için "Single Address" seçeneğini seçin ve ardından server IP adresini 192.168.188.10 olarak girin.
- Kaydetmek için OK'a tıklayın.

Objects Setting >> IP Object

Profile Index : 1

Name:	server
Interface:	LAN/DMZ/RT/VPN ▾
Address Type:	Single Address ▾
Mac Address:	00 :00 :00 :00 :00 :00
Start IP Address:	192.168.188.10 <input type="button" value="Select"/>
End IP Address:	0.0.0.0 <input type="button" value="Select"/>
Subnet Mask:	
Invert Selection:	<input type="checkbox"/>

1. Şube VPN Network'ü için bir IP Object profili oluşturmak üzere başka bir uygun indexe tıklayın, □ Name girin.
 - Interface için "LAN/DMZ/RT/VPN" seçin.
 - Address Type için "Subnet Address" seçeneğini seçin ve ardından 192.168.1.0 IP adresini ve 255.255.255.0 Subnet Mask'ını girin.
 - Kaydetmek için OK'a tıklayın.

Objects Setting >> IP Object

Profile Index : 2

Name:	branchvpn
Interface:	LAN/DMZ/RT/VPN ▾
Address Type:	Subnet Address ▾
Mac Address:	00 : 00 : 00 : 00 : 00 : 00
Start IP Address:	192.168.1.0 <input type="button" value="Select"/>
End IP Address:	0.0.0.0 <input type="button" value="Select"/>
Subnet Mask:	255.255.255.0
Invert Selection:	<input type="checkbox"/>

2. Firewall >> Filter Setup >> Filter Set 2 (Default Data Filter)'e git, paketleri Branch Office'den sunucuya geçirmek üzere Firewall kuralını düzenlemek için mevcut bir profile tıkla.

Firewall kuralını etkinleştir.

Profil Name girin.

Direction: LAN/DMZ/RT/VPN → LAN/DMZ/RT/VPN

Source IP: Branch VPN networkü için oluşturduğumuz IP nesnesini seçin.

Destination IP: Local server için oluşturduğumuz IP nesnesini seçin

(İsteğe bağlı) Service Type: Burada VPN networkünün sunucuya belirli bir porttan erişmesini istiyorsanız belirtin.

Filter: Pass Immediately

Filter Set 2 Rule 2		
<input checked="" type="checkbox"/>	Check to enable the Filter Rule	
	Comments	passBranch1
	Index(1-15) in Schedule Setup	
	Clear sessions when schedule ON	<input type="checkbox"/> Enable
Direction		
		LAN/DMZ/RT/VPN -> LAN/DMZ/RT/VPN ▾
Source IP		
		branchvpn <input type="button" value="Edit"/>
Destination IP		
		server <input type="button" value="Edit"/>
Service Type		
		Any <input type="button" value="Edit"/>
Fragments		
		Don't Care ▾
Application		
	Action/Profile	Pass Immediately ▾
	Filter	
	Branch to Other Filter Set	None ▾
	Sessions Control	0 / 60000
	MAC Bind IP	Non-Strict ▾
	Quality of Service	None ▾
	User Management	None ▾
	APP Enforcement	None ▾
	URL Content Filter	None ▾
	Web Content Filter	None ▾
	DNS Filter	None ▾
	Syslog	<input type="checkbox"/>

3. Paketleri şubeden diğer IP adreslerine engellemek için bir IP Filter kuralı oluşturmak için (Index number, step 3'den bir büyük olmalıdır) bir başka Index'e tıklayın.

- Bu Firewall kuralını etkinleştir.
- Profile Name gir.
- **Direction:** LAN/DMZ/RT/VPN → LAN/DMZ/RT/VPN
- **Source IP:** Şube VPN networkü için oluşturduğumuz IP nesnesini seçin.
- **Destination IP:** Any
- **Filter:** Block Immediately

○

Filter Set 2 Rule 3

Check to enable the Filter Rule

Comments: blockBranch1

Index(1-15) in Schedule Setup: [] [] [] [] [] [] [] [] [] [] [] [] [] [] []

Clear sessions when schedule ON: Enable

Direction: LAN/DMZ/RT/VPN -> LAN/DMZ/RT/VPN

Source IP: branchvpn

Destination IP: Any

Service Type: Any

Fragments: Don't Care

Application: Action/Profile: Block Immediately

Filter: Block Immediately

Branch to Other Filter Set: None

Sessions Control: 0 / 60000

MAC Bind IP: Non-Strict

Quality of Service: None

User Management: None

APP Enforcement: None

URL Content Filter: None

Web Content Filter: None

DNS Filter: None

Syslog:

Ve bu gerekli yapılandırmayla. Filtrelenen trafik olup olmadığını görmek için, **Diagnostics >> Syslog Explorer** sayfasındaki Firewall loglarını kontrol edebiliriz.

Diagnostics >> Syslog Explorer

Web Syslog		USB Syslog	
<input checked="" type="checkbox"/> Enable Web Syslog		Export Refresh Clear	
Syslog Type: Firewall		Display Mode: Stop record when full	
Time	Message		
2017-08-29 11:57:43	[FILTER][Block][LAN/RT/VPN->LAN/RT/VPN, 0:10:42][@S:R=2:3, 192.168.1.10->192.168.188.11][ICMP][HLen=20, TLen=60, Type=8, Code=0]		
2017-08-29 11:57:38	[FILTER][Block][LAN/RT/VPN->LAN/RT/VPN, 0:10:37][@S:R=2:3, 192.168.1.10->192.168.188.11][ICMP][HLen=20, TLen=60, Type=8, Code=0]		

LINUX

Bunu başarmanın iki yolu vardır: VPN Configuration ve Firewall kuralları.

1. Yöntem 1: VPN Yapılandırması ile

- Şubedeki Vigor Router'ın LAN-LAN VPN profilinde, Remote IP / Subnet Mask'ı tüm ağdan sadece sunucunun IP'sine çevirin.

Local IP / Subnet Mask : 192.168.1.1 255.255.255.0/24

Add Save Profile Number Limit : 16

Remote IP / Subnet Mask	IP	Subnet Mask
	192.168.188.10	255.255.255.255

Route / NAT Mode : Route

- Head Office'deki Vigor Router'ın LAN-LAN VPN profilinde, Local IP / Subnet Maskını tüm ağdan sadece sunucunun IP'sine değiştirin.

Local IP / Subnet Mask : 192.168.188.10 255.255.255.255/32

Add Save Profile Number Limit :

Remote IP / Subnet Mask	IP	Subnet Mask
	192.168.1.1	255.255.255.0

- VPN kurulduğunda, Branch Office Router, yönlendirme bilgisine sadece Server'in IP 192.168.188.10/32 bilgisine sahip olacak, böylece Branch Office'teki Client'ler sadece Server'e erişebilecektir.

Diagnostics >> Routing Table >> Routing Table

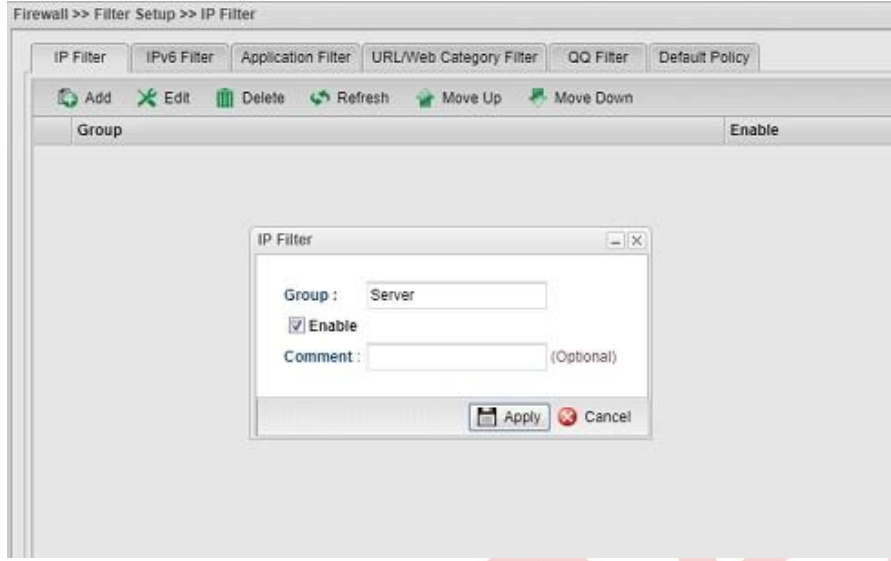
Routing Table IPv6 Routing Table

Refresh Legend U=Up,G=Gateway,H=Host

	Search Destination	Search Gateway	Search Genmask	Search Flags	Search Metric	Search Iface
1	192.168.66.1	0.0.0.0	255.255.255.255	UH	0	ppp1000
2	192.168.188.10	0.0.0.0	255.255.255.255	UH	0	ppp1000
3	192.168.39.0	0.0.0.0	255.255.255.0	U	0	wan-wan2
4	192.168.1.0	0.0.0.0	255.255.255.0	U	0	lan-lan1
5	default	192.168.39.1	0.0.0.0	UG	0	wan-wan2

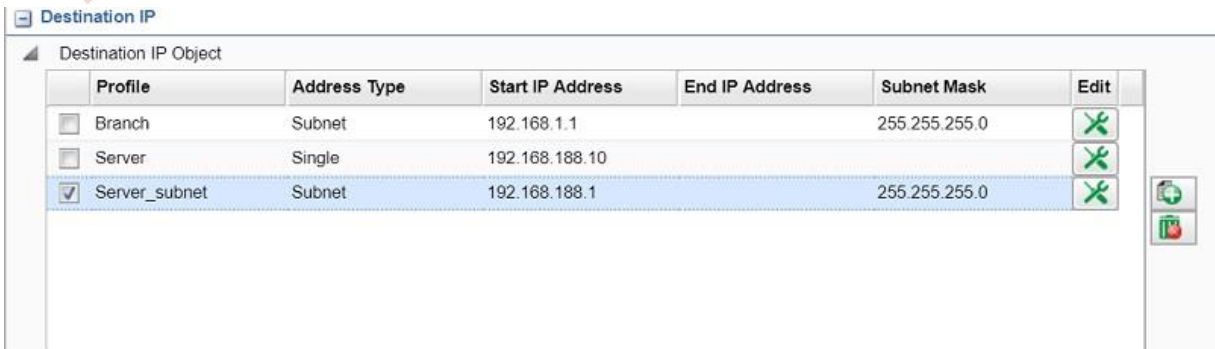
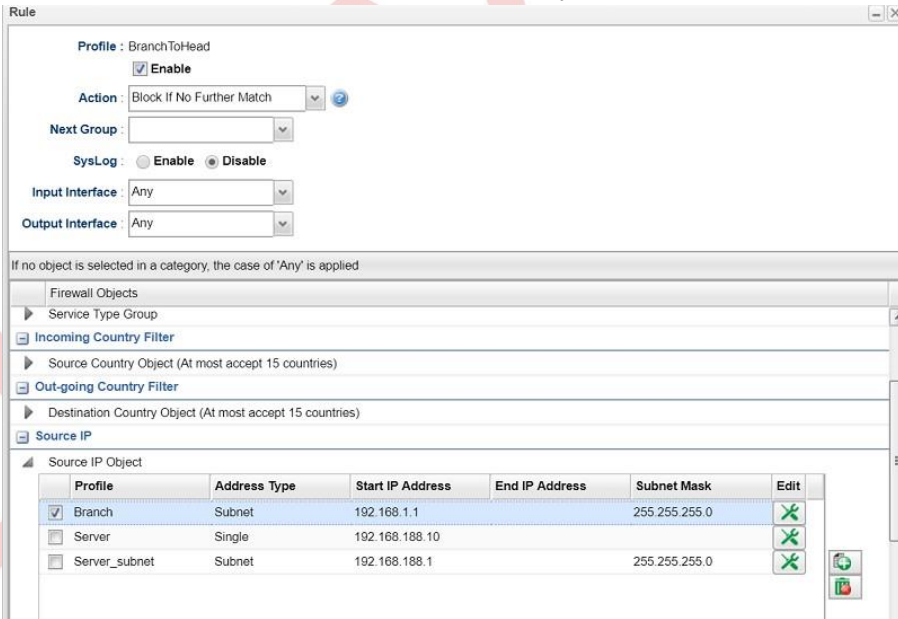
Yöntem 2 :Firewall Kuralı'na Göre

1. Brach ofisindeki bağlantıyı sınırlandırmak için merkez Router'de firewall kuralını oluşturabiliriz. Önce, Firewall >> Filter Setup >> IP Filter bölümüne gidin, yeni bir grup oluşturmak için Add'e tıklayın.



2. Filtre grubunda, aşağıdaki gibi yeni bir kural ekleyin: □ Profile Name girin.

- Etkinleştirmeyi denetleyin.
- Action için “Block if No Further Match”i seçin.
- Source IP’de Branch Office networkü için bir nesne ekleyin ve onu seçin
- Destination IP’de, Head Office networkü için bir nesne ekleyin ve onu seçin.



- İkinci kuralı aşağıdaki gibi ekleyin □
 - Profile Name girin.
 - Etkinleştirmeyi denetleyin.
 - Action olarak "Accept"i seçin.
 - Source IP'de Branch Office Network'ü için bir nesne ekleyin ve onu seçin □ Destination IP'de, Server'in IP'si için bir nesne ekleyin ve onu seçin.

Rule

Profile : Accept

Enable

Action : Accept

Next Group :

SysLog : Enable Disable

Input Interface : Any

Output Interface : Any

If no object is selected in a category, the case of 'Any' is applied

Firewall Objects

Advanced Setting

Service Protocol

Service Type Object

Service Type Group

Incoming Country Filter

Source Country Object (At most accept 15 countries)

Out-going Country Filter

Destination Country Object (At most accept 15 countries)

Source IP

Source IP Object

Profile	Address Type	Start IP Address	End IP Address	Subnet Mask	Edit
<input checked="" type="checkbox"/> Branch	Subnet	192.168.1.1		255.255.255.0	
<input type="checkbox"/> Server	Single	192.168.188.10			
<input type="checkbox"/> Server_subnet	Subnet	192.168.188.1		255.255.255.0	

Destination IP Object

Profile	Address Type	Start IP Address	End IP Address	Subnet Mask	Edit
<input type="checkbox"/> Branch	Subnet	192.168.1.1		255.255.255.0	
<input checked="" type="checkbox"/> Server	Single	192.168.188.10			
<input type="checkbox"/> Server_subnet	Subnet	192.168.188.1		255.255.255.0	

Gerekli yapılandırma bu şekildedir.