



## LAN Subnet için Outgoing WAN'ı Belirleyin

Router'in birden fazla WAN arayüzü varsa, trafiği Route Policy ile dengeleyebiliriz. Örneğin, LAN1'den gelen trafik kaynağının WAN1 üzerinden gönderilmesini ve LAN2'den gelen trafiğin WAN2 üzerinden gönderilmesini sağlayabiliriz.



## **DrayOS**

1. LAN1'den WAN1'e gitmek üzere trafik için bir Route Policy oluşturun: a. Profili etkinleştirin.

b. Source IP Subnet'i seçin ve LAN1 Subnet'inin IP aralığını girin.

Load-Balance/Route Policy

- c. WAN1 olarak Interface'i seçin.
- d. Failover'i WAN2'ye etkinleştir, böylece WAN1 bağlantısı başarısız olduğunda trafik WAN2 üzerinden gönderilebilir.
- e. Policy'i kaydetmek için OK 'a tıklayın.

Criteria			
Protocol	Any 🔻		
Source IP	Any		
	Src IP Range		
	Src IP Subnet		
	Network: 192.168.	.1.0 Mask: 255.255.255.0 /	24 🔻
Destination IP	Any		
	Dest IP Range		
	Dest IP Subnet		
Destination Port	Apv		
	Dest Port Start	Dest Port End	
	- Dest Port Start	N	
Send via if Criteria Match	ied		
Interface	• WAN/LAN	WAN1 •	
	O VPN	VPN 1.??? •	
Sateway	<ul> <li>VPN</li> <li>Default Gateway</li> </ul>	VPN 1.??? •	
Sateway	<ul> <li>VPN</li> <li>Default Gateway</li> <li>Specific Gateway</li> </ul>	VPN 1.??? •	
Sateway More Options A Packet Forwarding to W	VPN Default Gateway Specific Gateway /AN via Force NAT Force Routing	VPN 1, 222 •	
Sateway More Options A Packet Forwarding to V @ Failover to	VPN Default Gateway Specific Gateway /AN via Force NAT Force Routing WAN/LAN	VPN 1, 222 •	
Sateway More Options ▲ Packet Forwarding to W ☞ Failover to	VPN Default Gateway Specific Gateway VAN via Force NAT Force Routing WAN/LAN VPN VPN VPN VPN	VPN 1, 222 •	
Sateway More Options A Packet Forwarding to W S Failover to	VPN Default Gateway Specific Gateway VAN via Force NAT Force Routing WAN/LAN VPN VPN Route Policy Ind	VPN 1, 222 •	
Sateway More Options A Packet Forwarding to W Ø Failover to	VPN Default Gateway Specific Gateway Force NAT Force Routing WAN/LAN VPN VPN Route Policy Gateway M	VPN 1, 222 • AN2 • N 1, 227 • ex 1 • Default Gateway	
Sateway More Options ▲ Packet Forwarding to ₩ @ Failover to	VPN Default Gateway Specific Gateway Force NAT Force Routing WAN/LAN VPN Route Policy Gateway Specific Gateway Specific Gateway	N1.222 • N1.222 • ex 1 • Default Gateway Specific Gateway 0.0.0	
Sateway More Options Packet Forwarding to W Failover to Failoack	VPN Default Gateway Specific Gateway Force NAT Force Routing WAN/LAN VPN Route Policy Gateway Seteway	WI2	
Sateway More Options  Packet Forwarding to W Failover to Failback New sessions affe once that interfac Existing sessions a	VPN Default Gateway Specific Gateway Force NAT Force Routing WAN/LAN Route Policy Route Policy Cateway Cted by this Policy will be sel frected by this Policy will rei	VPN 1,222    N1.222   N1.222  Ex1  Default Gateway  Specific Gateway  D.0.0  nt via the original interface main on the failovered interface	
Sateway More Options  Packet Forwarding to W Failover to Failback New sessions affe once that interfat Existing sessions	VPN Default Gateway Specific Gateway Force NAT Force Routing WAN/LAN VPN VPN Route Policy Ind Gateway Cted by this Policy will be sel rersumes service affected by this Policy will rer	AN2   AN2  AN2  AN2  AN2  AN2  AN2  AN2	High
Sateway More Options  Packet Forwarding to W Failover to Failback New sessions affe once that interfat Existing sessions a Cc Priority: 200	VPN Default Gateway Specific Gateway Force NAT Force Routing WAN/LAN VPN Conternation Gateway Conternation Conternatio	AN2 N 1.??? • ex 1 • Default Gateway Specific Gateway D.0.00 nt via the original interface main on the failovered interface	High
Sateway More Options  Packet Forwarding to W Failover to Failback New sessions affe once that interfac Existing sessions Prionty: 200 250	VPN  Default Gateway  Specific Gateway  VAN via  Force NAT  Force Routing  WAN/LAN VV  NVPN Route Policy Md Gateway  Cted by this Policy will be server ensumes service affected by this Policy will ref	VPN 1,222 •	High



- Benzer şekilde, LAN2'deki trafiğin WAN2 üzerinden gitmesini sağlamak için başka bir Route Policy oluşturun: a. Profili etkinleştirin.
  - b. Source IP Subnet'i seçin ve LAN2'nin IP aralığını girin.
  - c. WAN2 olarak Interface'i seçin.
  - d. Failover'i WAN1 olarak etkinleştirin, böylece trafik WAN2 bağlantısı başarısız olduğunda WAN1 üzerinden gönderilebilir.

netfast

e. Policy'i kaydetmek için Tamam'ı tıklayın.

2			
C Enable			
Criteria			
Protocol	Any 🔻		
Source IP	Any		
	Src IP Range	9	
	Src IP Subne	et	
	Network: 192	2.168.2.0 Mask: 255.255.255.0/24 🔹	
Destination IP	Any		
	Dest IP Rang	je -	
	Dest IP Subr	net	
Destination Port	. Δηγ	indoinve	
90 MAY 10 LO CONTROL OF LOCAL AND A	Dest Port St	art Dest Port End	
		N	
Send via if Criteria Matched			
Sena via il citteria materica			
Interface	WAN/LAN	WAN2 •	
	O VPN	VPN 1.??? •	
Gateway	Default Gates	way	
	Specific Gate	way	
More Ontions			
more options =			
Packet Forwarding to WAN	via 💿 Force NAT		
	Force Routin	g	
🕑 Failover to	WAN/LAN	WAN1 T	
	O VPN	VPN 1.??? •	
	Route Policy	Index 1 🔻	
	Gateway	Default Gateway	
		Specific Gateway 0.0.0.0	
🗍 Failback			
Failback . New sessions affecte	d by this Policy will b	e sent via the original interface	
Failback . New sessions affecte once that interface of Evicting sessions offections.	d by this Policy will b esumes service	e sent via the original interface	
Failback . New sessions affecte once that interface r . Existing sessions affe	d by this Policy will b esumes service icted by this Policy w	e sent via the original interface ill remain on the failovered interface	
Failback . New sessions affecte once that interface r . Existing sessions affe	d by this Policy will b esumes service Incted by this Policy w	e sent via the original interface ill remain on the failovered interface	
Failback . New sessions affecte once that interface r . Existing sessions affe Low	d by this Policy will b esumes service icted by this Policy w	e sent via the original interface ill remain on the failovered interface <b>High</b>	
<ul> <li>Failback         <ul> <li>New sessions affected once that interface restrictions that interface restrictions affected by the sessions affected by the session of the session of</li></ul></li></ul>	ed by this Policy will b esumes service incted by this Policy w	e sent via the original interface ill remain on the failovered interface High	
Failback New sessions affecte once that interface r Existing sessions affe Priority: 200 Low	d by this Policy will b esumes service incted by this Policy w	e sent via the original interface ill remain on the failovered interface High 150 0 0	





3. LAN istemcisinin hangi yolu kullandığını doğrulamak için "tracert" komutunu kullanabiliriz.Bu komut ile LAN2 subnetlerinden gelen trafiğin WAN2 arayüzüne gönderildiğini görebiliriz.

Traci	ng ra	oute	to go	oogle	-pub	lic-	dns-a.google.com	[8.8.8]
over	a max	cimur	of a	30 ho	ps :			
1	<1	ms	<1	ms	<1	MS	192.168.2.1	
2	<1	ms	<1	ms	<1	ms	192.168.92.2	

## LİNUX

- 1. LAN1'den WAN1'i alacak trafik için bir Route Policy oluşturun. Routing >> Policy Route'a gidin, yeni bir policy kuralı eklemek için Add'e tıklatın ve kuralı aşağıdaki gibi yapılandırın:
  - a. Profil adını girin
  - b. Bu kuralı etkinleştir
  - c. "Interface" için Source Type'ı seçin, ardından LAN1'i seçin
  - d. Out-going Rule 'User Defined' olarak ve Out-going Inteface'i WAN1 olarak ayarlayın
  - e. (İsteğe bağlı) WAN1 başarısız olduğunda bir sonraki kurala uyması için Failover'i Next Rule olarak etkinleştirin.
  - f. (İsteğe bağlı) WAN1 yeniden bağlandığında, Router, Failover arayüzündeki oturumu derhal sonlandıracak ve trafiği WAN1'e gönderecek şekilde, Failback'i etkinleştirin.
  - g. Yapılandırmayı kaydetmek için Apply'a tıklayın.

Profile :		LAN1			
V Enable					
Priority :		Normal	~		
Protocol		ALL	~		
Source					
Source Type :		Interface	>		
Interface :		lan1	~		
Destination					
Destination Type :		Any	~		
Route Rule					
Out-going Rule :		User Defined	~		
Out-going Interface		wan1	~		
Out-going (Gateway) :			(	Optional)	
Mode		NAT	~		
Use IP Alias :		⊖ Enable			
Failover to Next Rule :		Enable      Disable			
when interface down					
O when target	ping	Fail for 3	Y	seconds	
Failback (Quick Recover) :		Enable      Disable			

Yukarıdaki yapılandırma ile router, LAN1'den WAN1'e olan trafiği gönderecektir. Ve Failover to Next Rule etkin olduğu için, WAN1 mevcut olmadığında, router bir sonraki kuralı izleyecektir, aksi durumda , Default Route uygulanacaktır.

2. Benzer şekilde, LAN2'den gelen trafiğin WAN2'yi alması için bir Policy Rule ekleyin.

Profile :		LAN2			
🔽 Enable					
Priority		Normal	~		
Protocol :		ALL	~		
Source				-	
Source Type :		Interface	*		
Interface :		lan2	~		
Destination	1				
Destination Type :		Any	*		
Route Rule					
Out-going Rule :		User Defined	~		
Out-going Interface		wan2	*		
Out-going (Gateway)			(0	Optional)	
Mode		NAT	*		
Use IP Alias :		O Enable   Disable			
Failover to Next Rule :		Enable      Disable			
• when target	ping	Fail of for 3		seconds	
Failback (Quick Recover)		Enable O Disable		5001103	

NOT: Vigor3900 / 2960, ping algılaması başarısız olduğunda Failover yapmayı da destekler. Failover , ping algılama ile yapılandırılmışsa, Router hedefi pinglemeye devam eder ve koşulu yerine getirdiğinde failover işlemini gerçekleştirir. Koşul, bir aralık için ping Fail/Success/Latency olabilir.





	100	
Profile :	ping	
V Enable		
Priority :	Normal	~
Protocol	ALL	*
Source		
Source Type :	Interface	*
Interfa <mark>ce</mark> :	lan1	*
Destination		
Destination Type	Any	*
Route Rule		
Out-going Rule :	User Defined	*
Out-going Interface	wan1	*
Out-going (Gateway) :		(Optional)
Mode :	NAT	~
Use IP Alias :	⊖ Enable ) ● Disat	ble
Failover to Next Rule :	Enable      Disat	ble
🔿 when interface down		
(a) when target 10.0.0.10	ping Fail 🗸 for 3	3 v seconds
Failback (Quick Recover)	Enable O Disat	ble

3. Default Route Yapılandırın Routing >> Default Route. Default Route, Policy Rule eşleşmediğinde izlenecek kuraldır. Default Route belirli bir WAN arayüzüne veya "default pool" olarak ayarlayabilirsiniz. "Auto Failover to Active WANs" seçeneğini etkinleştirmek, mevcut WAN bağlantısı koptuğunda oturumları diğer etkin WAN bağlantılarıyla değiştirir.

efault Route		
WAN Profile/Loadbalance Pool Name :	default_pool	~
Auto Failover to Active WANs :	Enable Ois	able
Load Balance Mode :	Session Based	~





4. Default Pool konfigürasyonu, Routing >> Load Balance Pool'dadır. Varsayılan olarak, her WAN arayüzü aynı ağırlığa sahiptir. Böylece Default Route uygulandığında, Router mevcut tüm WAN arayüzlerini eşit olarak kullanır.

Profile :	default_pool				
Mode :	Load Balance 👻				
	🚯 Add  🛗 Save	Add 🛗 Save			
	Interface	Weight			
	wan1	1	Ŵ		
	wan2	1	Ŵ		
Interface :	wan3	4	Ŵ		
	wan4	1	Ŵ		
	wan5	1	Ŵ		
	usb1	1	Ē		
	usb2	1	Ô		
e range of V ample of set in1 bandwid in2 bandwid ggested: wa	Veight is 1~255. ting load balance weight: #th:30M/30M #th:100M/100M an1 weight=3, wan2 weight=10 (ma	ax weight value : 255)			

5. Failover arayüzü olarak belirli bir WAN arayüzü kullanmak istiyorsanız, lütfen başka bir Policy Rule oluşturun. Örneğin, LAN2 için WAN1 üzerinden internete gitmek için ikinci bir kural oluşturabilirsiniz.

P	olicy Rule										
1	🕼 Add 🔀	Edit 🔟 I	Delete 🛛 👻 M	ove Up 🛛 🌏 Mov	e Down 🕻 🔓	Rename A	uto Refresh :	1 Minute 💉	🗢 Refresh	Proti	e Number
	Profile	Enable	Protocol	Source	Source Port	Destination	Destinatio	Out-going Rule	Mode	Failover t	Failb
1	LAN1	true	ALL	192,168,1,1/24	1	Any	82	wan1	NAT	Enable	Disable
2	LAN2	true	ALL	192.168.2.1/24	<u>9</u> ;	Any	8 <u>6</u> 6)	wan2	NAT	Enable	Disable
3	LAN2_backup	true	ALL	192.168.2.1/24	**	Any		wan1	NAT	Enable	Disable
•						111					1
						1					1

Şimdi, aynı Source'e sahip, ancak farklı Out-going Rule ile ilgili iki policy kuralı varsa. İlk önce daha küçük dizin numarasına sahip olan geçerli olacaktır. Eğer WAN2 mevcutsa, LAN2'den gelen trafik her zaman WAN2 üzerinden gerçekleşir. Yalnızca WAN2 kapalı olduğunda, "Failover to Next Rule" etkin olduğundan, bir sonraki kural uygulanacaktır; Böylece trafik WAN1'e gönderilecektir.