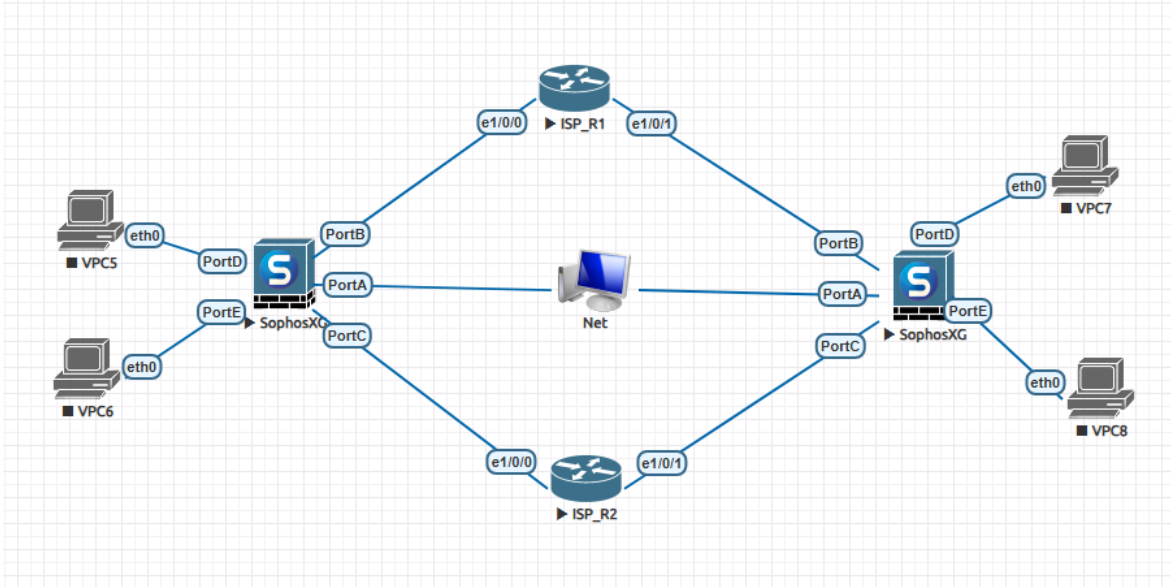


# SD-WAN

Günümüz işlerin büyük bir kısmı network/internet üzerinden gerçekleştirildiği için kurumlarda internet bağlantısının yedekliliğinin önemi de artmıştır. Bazen de birden fazla internet hattına sahip olduğu durumlarda internet trafiğinin bu hatlar arasında dengelenerek kullanılması istenebiliyor. Bu yazıda Sophos FW kullanılan kurumlarda internet hattının yedekliliğinin nasıl sağlanacağı açıklanmaya çalışılacaktır. Bu süreçte kullanılacak topoloji aşağıdaki gibidir.



Bu süreçte routerlar ve FW'lar üzerinde kullanılacak portlara sadece ip adresleri verildi. Ek olarak FW'ların iç bacaklarındaki networkler için Static Route tanımları eklendi. Tanımlar sonrasında FW'larda WAN portlarının Gateway'lerine erişim erişmediğini kontrol edebilmek için "Network -> WAN Management -> Status" yolu takip edilebilir. Bu tanımlar yapıldıktan sonra SD-WAN konfigürasyonuna başlanabilir.

Network									
Feedback	How-to guides	Log viewer	Help	admin@Site					
Interfaces	Zones	WAN link manager	DNS	DHCP	IPv6 router advertisement	Cellular WAN	IP tunnels	Neighbors (ARP-NDP)	Dynamic DNS
IPv4 gateway									
Name	IP address	Interface	Type	Activate on failure of	Weight	Status	Usage	Manage	
ISP_1	10.10.10.1	PortB_ISP_1 - 10.10.10.2/255.255.255.0	Active	N/A	1	●	Q		
ISP_2	10.10.20.1	PortC_ISP_2 - 10.10.20.2/255.255.255.0	Active	N/A	1	●	Q		

SD-WAN konfigürasyonu için ilk olarak "Routing -> SD-WAN Profiles -> Add" yolu takip edilerek SD-WAN profili oluşturulmalıdır.

- "Name" kısmıyla oluşturulacak profile bir isim tanımlanmalıdır.
- "Routing Strategies" kısmıyla profil tanımına eklenecek WAN linkleri arasında yük dengeleme işlemi mi yapılmak istendiği yoksa ilk ayakta olan WAN bağlantısı üzerinden mi bütün trafiğin gönderileceği belirlenmelidir.
  - o "Load Balance Method" yük dengeleme yapılmak isteniyorsa bu durumda yük dengeleme kriterinin oturma bazlı mı yapılacağı yoksa Round-Robin algoritmasına göre otomatize mi yapılacağı belirtilmelidir.

- “Gateways” kısmıyla profil tanımında kullanılacak WAN portları belirtilmelidir (Lab için Internal1trafiğini ISP1’den, Internal2 trafiğini ISP2’den çıkarmak istiyoruz. Bu nedenle profile tanımında birisi seçiliyor).
- “Gateways Weight” kısmıyla seçile WAN portları arasında birisinin daha yoğun kullanılması istendiği durumunda ayarlanan alandır.

Routing [Feedback](#) [How-to guides](#) [Log viewer](#)

SD-WAN routes **SD-WAN profiles** Gateways Static routes BGP OSPF OSPFv3 Information Upst

Name \* INTERNAL1\_to\_ISP1

Description Enter Description

Routing strategy ☐ First available gateway Routes traffic based on first available gateway if SLA is turned off. ☒ Load balancing Load-balances traffic among all available gateways or those meeting the SLA.

Load balancing method ☐ Round-robin ☒ Session persistence type Source IP address

Gateways \*

Select gateways type to search... Create

☒ ISP\_1 ☐ ISP\_2

Assigned gateways ISP\_1

Gateway weights 1 ISP\_1 1 [1 - 100] ISP\_1

- “SLA” kısmı WAN bağlantıları üzerindeki Latency, Jitter ve Packet Loss gibi kriterler göz önünde bulundurularak hatların kalitesi ölçülmek istendiğinde kullanılıyor.
- “SLA Strategy” kısmıyla hatlar arasındaki kalite durumunun otomatize şekilde ölçülerek mi yoksa özel olarak belirtilen değerler göz önünde bulundurularak mı hatlar arasında geçiş yapılacağı belirleniyor.
  - o “Custom SLA” kısmıyla özel olarak Latency, Jitter ve Packet Loss değerleri tanımlanarak hatlar arasında geçişlerin yapılması sağlanabiliyor.
- “Health-Check” kısmıyla port ayakta olsa dahi bir hedef adrese erişimin belirli sıklıklarda kontrol edilmesi ve bu hedefe erişim kesildiği durumda trafiğini yedek hatta geçirilmesi sağlanıyor.
  - o Burada profile içerisinde **tanımlı WAN portlarının tamamından hedef olarak tanımlanan adrese erişim sağlanamadığı durumda** profilden diğer adreslere erişim sağlanıyor olsa dahi profile tanımlı kullanılamayacaktır (Status ledi kırmızı yanar). Bu nedenle mümkünse burada tanımlanacak hedef adresler dikkatli ve birden fazla olacak şekilde tanımlanmalıdır.
- “Protocol” kısmıyla hedef adrese erişimin hangi protokol kullanılarak yapılmak istendiği belirtiliyor.
- “Probe Target” kısmıyla hedef olarak gösterilen ip adreslerinin ne sıklıkta kontrol edileceği belirtilmelidir.
- “Health Check Attempts” kısmıyla hedef ip adresine ne kadar süre erişilemediği takdirde trafiklerin yedeklenen diğer hatta geçiş yapacağı belirlenmektedir.

Routing [Feedback](#) [How-to guides](#) [Log viewer](#) [Help](#) [admin@](#)

SD-WAN routes **SD-WAN profiles** Gateways Static routes BGP OSPF OSPFv3 Information Upstream proxy

SLA ☒

SLA strategy ☐ Best quality Routes traffic through the best-performing gateway. It only load-balances if two or more gateways have the best SLA performance. ☒ Custom SLA Routes traffic through the first gateway meeting the SLA. For load balancing, it uses all gateways meeting the SLA. If no gateway meets the SLA, the configured routing strategy applies.

Custom SLA

Maximum latency ☒ 250 [1-60000 ms]

Maximum jitter ☒ 50 [1-60000 ms]

Maximum packet loss ☒ 2 [0-100 %]

Recommended SLA values

Health check ☒

Protocol ☒ Ping ☐ TCP

Probe target [+](#)

IP address 10.10.10.1 Port -

Health check attempts Interval between checks 2 [1-3600 seconds] Response time-out 2 [1-10 seconds]

Action Deactivate gateway after: 3 [1-10 consecutive failures] Activate gateway after: 5 [1-10 consecutive responses]

Sample size for SLA 30 [5-100 samples]

Save Cancel [Sophos Assistant](#)

General web traffic  
Latency: 250 ms  
Jitter: 50 ms  
Packet loss: 2 %

Media (example: video, IP telephony)  
Latency: 150 ms  
Jitter: 30 ms  
Packet loss: 1 %

Office 365  
Latency: 250 ms  
Jitter: 50 ms  
Packet loss: 5 %

Profile tanımları yapıldıktan sonra her durumları “Routing -> SD-WAN Profile” yolu takip edilerek kontrol edilebilir. Eğer ki Healt-Check kısmında belirtilen ip adresine belirtilen WAN bağlantılarından birisiyle bile erişiliyorsa bu durumda profilin en solunda yeşil işaret bulunacaktır. Bir anlamı bu işaretler Profile tanımının belirtilen WAN bağlantılarının çalışır durumda olduğunu gösterir.

Routing [Feedback](#) [How-to guides](#) [Log viewer](#) [Help](#) [admin@Site1](#)

SD-WAN routes **SD-WAN profiles** Gateways Static routes BGP OSPF OSPFv3 Information Upstream proxy

Logs

	#	Name	Gateway	Health check	ID	Status	Usage	Manage
<input type="checkbox"/>	1	INTERNAL1 to ISP1	ISP_1	On	#1		0	
<input type="checkbox"/>	2	INTERNAL2 to ISP2	ISP_2	On	#2		0	

SD-WAN profili tanımlandıktan sonra bu profile tanımları bir SD-WAN Routing Policy tanımına bağlanması gerekiyor. Bu işlem için “Routing -> SD-WAN Routes -> Add” yolu takip edilir. Burada;

- “Name” kısmıyla SD-WAN politikasına bir isim verilmelidir.
- “Rule Position” kısmıyla oluşturulacak politikanın konumu belirtilmelidir.
- “Incoming Interface” kısmıyla trafiğin geleceği arayüz seçimi yapılmalıdır.
- “DSCP Marking” kısmıyla QoS yapılmak isteniyorsa trafiklere DSCP bitlerinin eklenmesi sağlanabiliyor.
- “Source Networks” kısmıyla trafiğin geleceği arayüzdeki hangi kaynak ip adresine sahip paketlere bu politikanın uygulanacağı belirtilmelidir.
- “Destination Networks” kısmıyla paketler hangi hedef ip adreslerine gönderilmek istendiğinde bu politikanın kullanılacağı belirtilmelidir.
- “Services” kısmıyla hangi protokoller kullanılırken bu politikanın kullanılacağı seçilmelidir.
- “Application Objects” kısmıyla hangi uygulama trafiklerinin (port bazlı değil de uygulama bazlı) bu politika ile eşleşeceği belirtilmelidir.
- “User or Group” kısmıyla hangi kullanıcı ve grupların bu politikayı kullanacağı seçilebiliyor.

Routing Feedback How

**SD-WAN routes** SD-WAN profiles Gateways Static routes BGP OSPF OSPFv3 Information

Name \* INTERNAL1\_to\_ISP1\_POLICY Description Enter Description Route position Top

Traffic selector

Incoming interface PortD\_INTERNAL\_1-192.168.10.1

Source networks Internal1 Ntw Add new item

Application object Any Add new item

DSCP marking Select DSCP marking

Destination networks Any Add new item

User or groups Any Add new item

Services Any Add new item

- “Link Selection Setting” kısmıyla üst kısımda belirtilen nitelikteki trafiklerin bir port seçilerek mi yoksa SD-WAN profil tanımlarından birisiyle mi eşleştirileceği belirtilemelidir.
  - o “Select SD-WAN Profile” kısmıyla SD-WAN routing politikasının eşleşeceği SD-WAN profil tanımı seçilmelidir.

### Link selection settings

- ☒ Select SD-WAN profile i ☐ Primary and Backup gateways

Select SD-WAN profile \*

INTERNAL1\_to\_ISP1

☐ Route only through specified gateways i

Save

Cancel

Routing Feedback How-to guides Log viewer Help admin@Site1

**SD-WAN routes** SD-WAN profiles Gateways Static routes BGP OSPF OSPFv3 Information Upstream proxy \*\*\*

Current precedence for routing: Static route, SD-WAN route, VPN route.  
Policy route also applies to system-generated and reply traffic. To learn how to change the configuration, go to the [online help](#).

**IPv4** **IPv6**

IPv4 SD-WAN route Watch: How to use SD-WAN routes

	#	Name	Interface	Source	Destination	Services	Application	ID	Active
	1	INTERNAL1_to_ISP2_POLICY in 0.0.0.0, out 0.0.0.0	PortD_INTERNAL_2	Internal2 Ntw	Any	Any service	Any application	#2	<span>●</span>
	2	INTERNAL1_to_ISP1_POLICY in 0.0.0.0, out 1.69 KB	PortD_INTERNAL_1	Internal1 Ntw	Any	Any service	Any application	#1	<span>●</span>

Add Delete

Bu tanımlar yapıldıktan sonra trafikler internet ortamına çıkarılmak üzere “Rules and Policies -> Add Firewall Rule” yolu takip edilerek politika yazılması gerekiyor. Buradaki politika için ayrıca açıklama yapılmadı. Kaynak ip adresi dışında her şey “any” olarak bırakılabilir. Ek olarak da internet çıkışı için bu politikalara uygun bir NAT kuralı oluşturup uygulanması yeterli olacaktır.

NAT politikası Firewall Rule kısmındaki bir politika içerisinde oluşturulabileceği gibi “Rules and Policies -> NAT Rule -> Add” yolu izlenerek de oluşturulabilir.

- NAT kuralı oluşturulurken dikkat edilmesi gereken noktalardan birisi de "" kısmının MASQ olarak seçilmesi gerekmektedir. Bu seçenek kaynak ip adreslerinin maskelenerek WAN bacağındaki ip bilgisine NAT'lanmasını ve bu Public ip adresiyle internete çıkmasını sağlayacaktır.

Edit firewall rule

Feedback

Ho

Add NAT rule

Rule status

Rule name \*

INTERNAL1\_to\_SD-WAN\_NAT\_RULE

Description

Rule position

Top

Translation settings

Select the matching criteria and translation settings for source, destination, and services.

All matching criteria of the firewall, including users and schedule, apply to its linked NAT rule. Can't edit these in the NAT rule.

Original source \*

Any

Add new item

Original destination \*

Any

Add new item

Original service \*

Any

Add new item

Translated source (SNAT)

MASQ

Translated destination (DNAT)

Original

Translated service (PAT)

Original

Interface matching criteria

Inbound interface \*

Any

Add new item

Outbound interface \*

Any

Add new item

Override source translation (SNAT) for specific outbound interfaces

Create loopback rule

Create reflexive rule

Sophos Assistant

Rules and policies

Feedback

How-to guides

Log viewer

Help

admin@Site1

Firewall rules

NAT rules

SSL/TLS inspection rules

IPv4

IPv6

Disable filter

Watch: How to use NAT

Add NAT rule

Disable

Delete

NAT type	Status	Rule ID	Hide linked NAT rule					
#	Name	Original	Translated	Interface	ID	Usage		
1	INTERNAL2_to_SD-WAN_NA Firewall rule ID: 6	Source: Internal2.Nw Service: Any service Destination: Any host	Source: MASQ Service: Original Destination: Original	Inbound: Any interface Outbound: Any interface Last used: Unused	#4	0		
2	INTERNAL1_to_SD-WAN_NA Firewall rule ID: 5	Source: Internal1.Nw Service: Any service Destination: Any host	Source: MASQ Service: Original Destination: Original	Inbound: Any interface Outbound: Any interface Last used: Unused	#3	0		
3	Auto added NAT rule for MTA Firewall rule ID: 1	Source: Any host Service: SMTP:SMTP(S) Destination: Any host	Source: MASQ Service: Original Destination: Original	Inbound: Any interface Outbound: Any interface Last used: Unused	#1	0		
4	Default SNAT IPv4	Source: Any host Service: Any service Destination: Any host	Source: MASQ Service: Original Destination: Original	Inbound: Any interface Outbound: PortB_ISP_1... Last used: 2025-06-01 15:33:45	#2	45		

Showing 4 of 4. Selected 0

Burada Sophos zerine yeni çalışmaya başladığım için emin olmadığım konulardan birisi de ayrıca her iki WAN portu için de Static Route yazmama gerek olup olmadığı. Normalde WAN portlarını (ISP\_1 ve ISP\_2 portları) ayarlarken Default Gateway olarak routerların ip adresleri tanımlandığı için ayrıca Static Route yazmaya gerek olmadığını düşünüyorum (Port altında Gateway adresi olarak tanımlanamazdı Static Route tanımına ihtiyaç olacaktır).

Firewall Policy ve NAT politikaları da oluşturulduktan sonra Site1 FW (Sol taraftaki Sophos FW) üzerinde yapılması gereken işlemler tamamlanmıştır. Artık test için Site2 FW (Sağ taraftaki Sophos FW) üzerindeki tanımlara geçilebilir.

**SOPHOS** FW

Search

MONITOR & ANALYZE

Control center

Current activities

Reports

Zero-day protection

Diagnostics

PROTECT

**Rules and policies**

Intrusion prevention

Web

Applications

Wireless

Email

Web server

Active threat response

CONFIGURE

Remote access VPN

Site-to-site VPN

Network

Routing

Authentication

System services

SYSTEM

Sophos Central

Profiles

Hosts and services

Administration

Backup & firmware

Certificates

### Add firewall rule

Feedback How-to guides Lc

☒ Rule status

Rule name \* INTERNAL1\_to\_SD-WAN

Action Accept

☒ Log firewall traffic  
Logs traffic matching this firewall rule, on the appliance (by default) or on the configured syslog server.

Description Enter Description

Rule position Top

Rule group None

Source

Select the source zones, networks, and devices.  
The rule applies to traffic from these sources during the scheduled time period.

Source zones \* LAN

Source networks and devices \* Internal1 Ntw

During scheduled time All the time

Destination and services

Select the destination zones, networks, devices, and services.  
The rule applies to traffic to these destinations.

Destination zones \* WAN

Destination networks \* Any

Services \* Any

Save Cancel

Sophos Assistant

Rules and policies

Feedback

How-to guides

Log viewer

Help

admin@Site1

Firewall rules

NAT rules

SSL/TLS inspection rules

IPv4

IPv6








Disable filter

Test your policies

Add firewall rule

Disable

Delete

Rule type	Source zone	Destination zone	Status	Rule ID	Add Filter	Reset filter		
#	Name	Source	Destination	What	ID	Action	Feature and service	
<input checked="" type="checkbox"/>	1	 INTERNAL2 to SD-WAN in 840 B, out 1.64 KB	LAN, Internal2 Ntw	WAN, Any host	Any service	#6	Accept	IPS, IAV, Intrusion Prevention, Anti-Malware, Anti-Spyware, Anti-Fraud, Anti-DDoS
<input checked="" type="checkbox"/>	2	 INTERNAL1 to SD-WAN in 3.75 KB, out 8.81 KB	LAN, Internal1 Ntw	WAN, Any host	Any service	#5	Accept	IPS, IAV, Intrusion Prevention, Anti-Malware, Anti-Spyware, Anti-Fraud, Anti-DDoS
<input checked="" type="checkbox"/>	 Traffic to Internal Zones in 0 B, out 0 B	To LAN, WIFI, VPN, DMZ. Firewall rules with the destination zone as LAN, WIFI, VPN, DMZ would be added to this group on the first match basis if user selects automatic grouping option...						
<input checked="" type="checkbox"/>	 Traffic to WAN in 0 B, out 0 B	Outbound traffic to WAN. Firewall rules with the destination zone as WAN would be added to this group on the first match basis if user selects automatic grouping option. This is the d...						
<input checked="" type="checkbox"/>	 Traffic to DMZ in 0 B, out 0 B	Inbound traffic to DMZ. Firewall rules with the destination zone as DMZ would be added to this group on the first match basis if user selects automatic grouping option. This is the d...						
<input checked="" type="checkbox"/>	6	 Auto added firewall policy for MTA in 0 B, out 0 B	Any zone, Any host	Any zone, Any host	SMTP, SMTP(S)	#1	Accept	IPS, IAV, Intrusion Prevention, Anti-Malware, Anti-Spyware, Anti-Fraud, Anti-DDoS
<input checked="" type="checkbox"/>	7	 Drop all in 0 B, out 0 B	Any zone, Any host	Any zone, Any host	Any service	#0	Drop	IPS, IAV, Intrusion Prevention, Anti-Malware, Anti-Spyware, Anti-Fraud, Anti-DDoS

Site2 FW üzerinde sadece WAN Zone'dan LAN Zone'a doğru politika tanımlanması yeterli olacaktır. Site2 FW üzerinde de WAN portlarını ayarlarken Default gateway olarak routerların ip bilgileri tanımlandığı için ayrıca Static Route tanımlı yapmaya gerek kalmayacaktır.

SOPHOS

FW

Search

MONITOR & ANALYZE

Control center

Current activities

Reports

Zero-day protection

Diagnostics

PROTECT

Rules and policies

Intrusion prevention

Web

Rules and policies

Feedback

How-to guides

Log viewer

Help

admin@Site2

Firewall rules

NAT rules

SSL/TLS inspection rules

IPv4

IPv6

Disable filter

Test your policies

Add firewall rule

Disable

Delete

Rule type

Source zone

Destination zone

Status

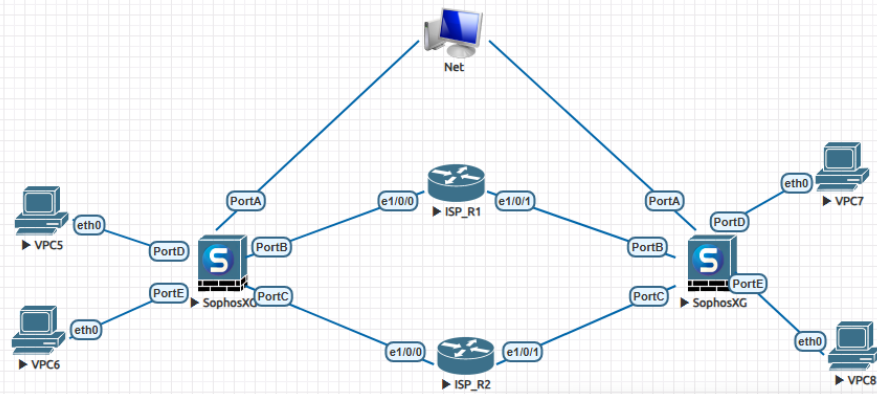
Rule ID

Add Filter

Reset filter

#	Name	Source	Destination	What	ID	Action	Feature and service
1	test in 1.46 KB, out 1.76 KB	WAN, Any host	LAN, Any host	Any service	#5	Accept	IPS, IAV, Intrusion Prevention, Anti-Malware, Anti-Spyware, Anti-Fraud, Anti-DDoS
	Traffic to Internal Zones in 0 B, out 0 B	To LAN, WIFI, VPN, DMZ. Firewall rules with the destination zone as LAN, WIFI, VPN, DMZ would be added to this group on the first match basis if user selects automatic grouping option...					

Günün sonunda VPC'ler arasında Trace atıldığında çıktı aşağıdaki gibi olacaktır. SD-WAN tanımlı yapmadan önce test ettiğimde PC'lere trace atarken ISP\_1 hattından, Site2 FW'un iç bacağına verilen ip adresine Trace attığımda ISP\_2 üzerinden gidiyordu. SD-WAN konfigürasyonu sonrasında VPC5 her koşulda ISP\_1 hattını, VPC6 her koşulda ISP\_2 hattını kullanmaya başladı.



```

VPCS>
VPCS>
VPCS>
VPCS> ip 192.168.10.50 192.168.10.1
Checking for duplicate address...
VPCS : 192.168.10.50 255.255.255.0 gateway 192.168.10.1

VPCS> trace 192.168.30.50
trace to 192.168.30.50, 8 hops max, press Ctrl+C to stop
 1 192.168.10.1 0.238 ms 0.161 ms 0.193 ms
 2 10.10.10.1 3.084 ms 1.339 ms 1.182 ms
 3 10.10.30.2 1.519 ms 1.441 ms 0.948 ms
 4 *192.168.30.50 0.945 ms (ICMP type:3, code:3, Destination port unreachable)

VPCS> trace 192.168.40.50
trace to 192.168.40.50, 8 hops max, press Ctrl+C to stop
 1 192.168.10.1 0.317 ms 0.187 ms 0.126 ms
 2 10.10.10.1 3.805 ms 1.353 ms 0.698 ms
 3 10.10.30.2 0.449 ms 0.618 ms 0.519 ms
 4 *192.168.40.50 0.780 ms (ICMP type:3, code:3, Destination port unreachable)

VPCS>

```

```

VPCS>
VPCS>
VPCS>
VPCS> ip 192.168.20.50 192.168.20.1
Checking for duplicate address...
VPCS : 192.168.20.50 255.255.255.0 gateway 192.168.20.1

VPCS> trace 192.168.30.50
trace to 192.168.30.50, 8 hops max, press Ctrl+C to stop
 1 192.168.20.1 0.261 ms 0.187 ms 0.150 ms
 2 10.10.20.1 3.812 ms 1.540 ms 1.545 ms
 3 10.10.40.2 0.598 ms 0.400 ms 0.697 ms
 4 *192.168.30.50 1.157 ms (ICMP type:3, code:3, Destination port unreachable)

VPCS> trace 192.168.40.50
trace to 192.168.40.50, 8 hops max, press Ctrl+C to stop
 1 192.168.20.1 0.316 ms 0.189 ms 0.190 ms
 2 10.10.20.1 3.138 ms 1.336 ms 1.149 ms
 3 10.10.40.2 1.461 ms 0.446 ms 0.394 ms
 4 *192.168.40.50 0.912 ms (ICMP type:3, code:3, Destination port unreachable)

VPCS>

```