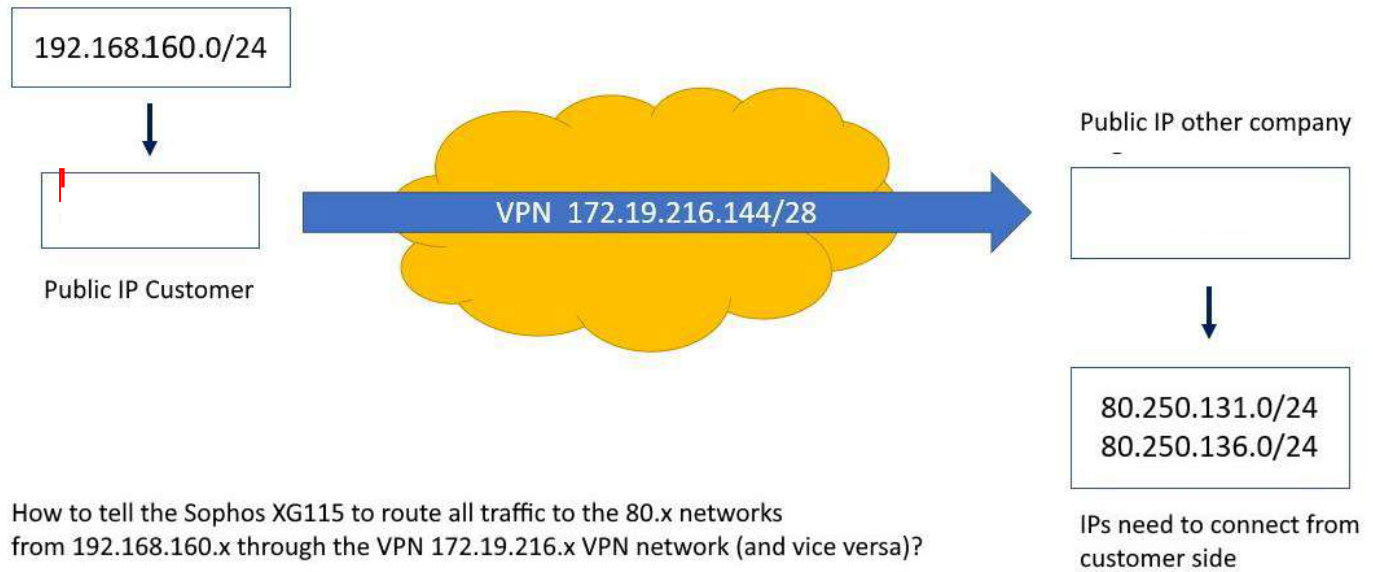


What we have and what we need

LOCAL Network (Sophos 192.168.160.1)



How to tell the Sophos XG115 to route all traffic to the 80.x networks from 192.168.160.x through the VPN 172.19.216.x VPN network (and vice versa)?

VPN Settings

IPsec connections

[Show additional properties](#)

[Add](#) [Delete](#) [Wizard](#)

☐	Name	Group name	Policy	Connection type	Status	Connection	Manage
☐	VPN_M...	-	_VPN	Site-to-site		i	edit stop delete

General settings

Name:

Description:

IP version: ☒ IPv4 ☐ IPv6 ☐ Dual

Connection type:

Gateway type:

☒ Activate on save

☐ Create firewall rule

Encryption

Policy:

Authentication type:

[Change preshared key](#)

Gateway settings

Local gateway	Remote gateway
Listening interface: Port2 - 192.168.161.20	Gateway address: 1
Local ID type: IP address	Remote ID type: IP address
Local ID:	Remote ID:
Local subnet: _LAN Add new item	Remote subnet: _aaS_131 _aaS_136 Add new item
☐ Network Address Translation (NAT) You must first create these subnets in "Hosts and services".	

Networks:

_aaS_131	= 80.250.131.0 / 24
_aaS_136	= 80.250.136.0 / 24
_LAN	= 172.19.216.144 / 28
_LAN_Range_24	= 172.19.216.144 / 28
Internal Network BG	= 192.168.160.0 / 24
Internal_Network_BG_Range	= 192.168.160.0 / 24

Firewall Rule

ON

Rule status

Rule name *

II VPN_Mainz

Action

Accept

☒ Log firewall traffic

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

Description

Auto created Firewall Rule

Rule group

VPN

Source

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

Source zones *

Any

Add new item

Source networks and devices *

Internal Network BG

LAN

aaS_131

aaS_136

Add new item

During scheduled time

All the time

Select to apply the rule to a specific time period and day of the week.

Destination and services

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

Destination zones *

Any

Add new item

Destination networks *

Internal Network BG

LAN

aaS_131

aaS_136

Add new item

Services *

Any

Add new item

Services are traffic types based on a combination of protocols and ports.

NAT Rule Inbound

☐ OFF Rule status

Rule name *

DNAT VPN eingehend

Description

Translation settings

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

Original source *

aaS_131

aaS_136

Add new item

Original destination *

LAN_Range_24

Add new item

Original service *

Any

Add new item

Translated source (SNAT)

Original

Translated destination (DNAT)

Internal_Network_BG_Range

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 ?

Advanced settings

Load balancing method

One-to-one

Nat Rule Outbound

OFF

Rule status

Rule name *

SNAT_VPN_ausgehend

Description

Translation settings

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

Original source *

Internal_Network_BG_Range

Add new item

Original destination *

_aaS_131

_aaS_136

Add new item

Original service *

Any

Add new item

Translated source (SNAT)

Aareon IP

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

Advanced settings

Load balancing method

Select