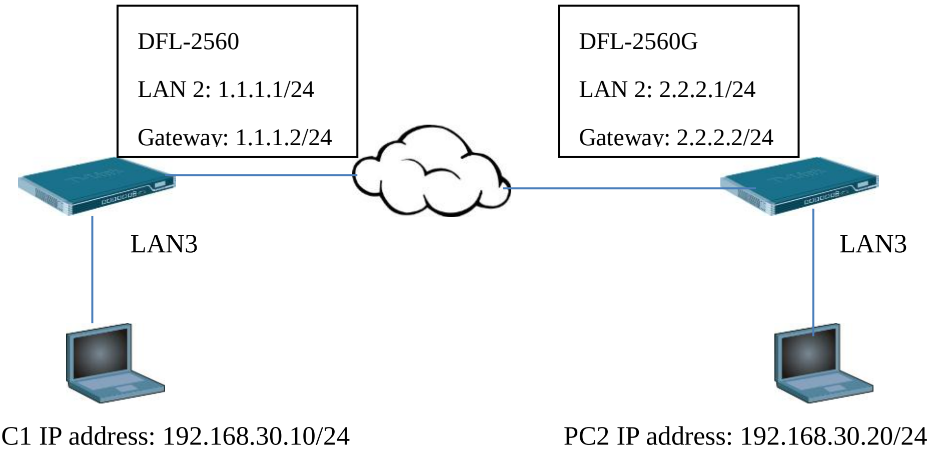
How to set up an overlapping network with IPSec tunnel in DFL unit

Before the scenario hands-on, we assume that the readers already along with following abilities:

1. The simple routing concept
2. The basic concept for IPSEC interface
3. The concept of overlapping network issue. If you need mode information, please refer the following

Scenario summary:

DFL-210/800/1600/2500/860/260 must use f/w:v2.26.00 or later



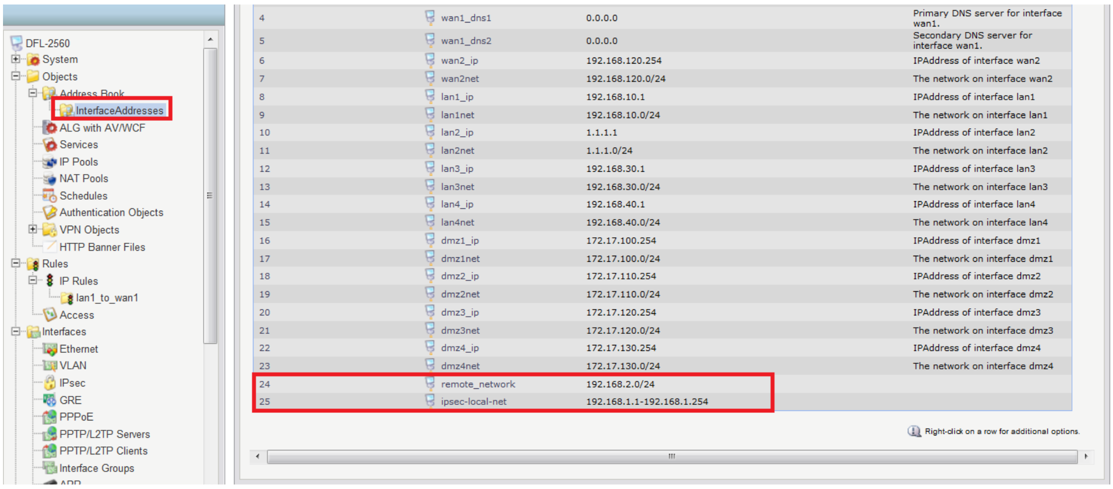
Object:

PC1 and PC2 can access each other with IPSec tunnel.

DFL-2560

Step1. Set the IP address for LAN, Wan and other network objects respectively.

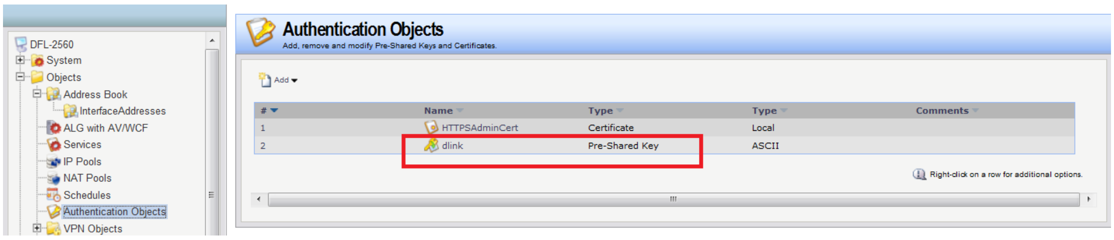
Remote network = the opposite virtual network



4	wan1_dns1	0.0.0.0	Primary DNS server for interface wan1.
5	wan1_dns2	0.0.0.0	Secondary DNS server for interface wan1.
6	wan2_ip	192.168.120.254	IPAddress of interface wan2
7	wan2net	192.168.120.0/24	The network on interface wan2
8	lan1_ip	192.168.10.1	IPAddress of interface lan1
9	lan1net	192.168.10.0/24	The network on interface lan1
10	lan2_ip	1.1.1.1	IPAddress of interface lan2
11	lan2net	1.1.1.0/24	The network on interface lan2
12	lan3_ip	192.168.30.1	IPAddress of interface lan3
13	lan3net	192.168.30.0/24	The network on interface lan3
14	lan4_ip	192.168.40.1	IPAddress of interface lan4
15	lan4net	192.168.40.0/24	The network on interface lan4
16	dmz1_ip	172.17.100.254	IPAddress of interface dmz1
17	dmz1net	172.17.100.0/24	The network on interface dmz1
18	dmz2_ip	172.17.110.254	IPAddress of interface dmz2
19	dmz2net	172.17.110.0/24	The network on interface dmz2
20	dmz3_ip	172.17.120.254	IPAddress of interface dmz3
21	dmz3net	172.17.120.0/24	The network on interface dmz3
22	dmz4_ip	172.17.130.254	IPAddress of interface dmz4
23	dmz4net	172.17.130.0/24	The network on interface dmz4
24	remote_network	192.168.2.0/24	
25	ipsec-local-net	192.168.1.1-192.168.1.254	

Right-click on a row for additional options.

Step2. Create a pre-shared key for IPSEC interface.



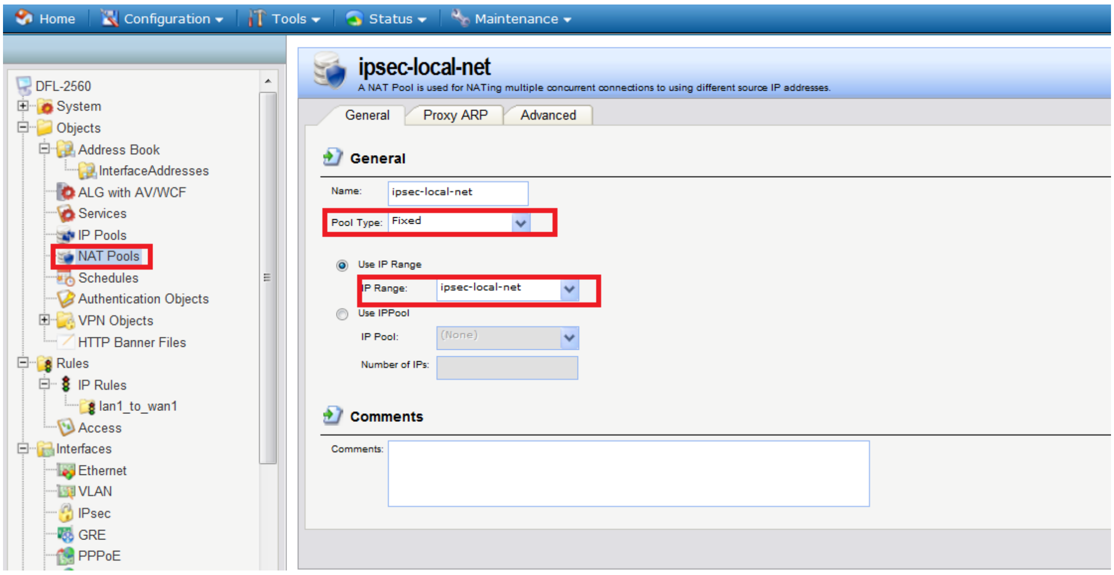
Authentication Objects

Add, remove and modify Pre-Shared Keys and Certificates.

#	Name	Type	Type	Comments
1	HTTPSAdminCert	Certificate	Local	
2	dlink	Pre-Shared Key	ASCII	

Right-click on a row for additional options.

Step3. Create a NAT POOL object as the screenshot below.



ipsec-local-net

A NAT Pool is used for NATing multiple concurrent connections to using different source IP addresses.

General

Name: ipsec-local-net

Pool Type: Fixed

● Use IP Range

IP Range: ipsec-local-net

○ Use IPPool

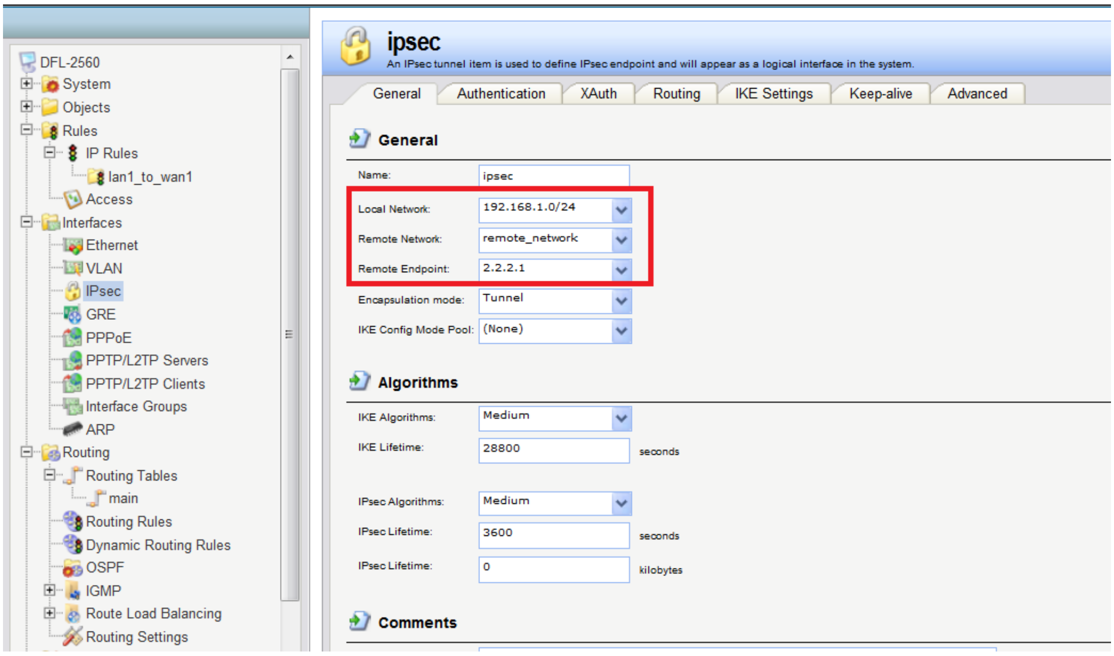
IP Pool: (None)

Number of IPs:

Comments

Comments:

Step4. Create an IPSEC interface as the following screenshots.



ipsec

An IPsec tunnel item is used to define IPsec endpoint and will appear as a logical interface in the system.

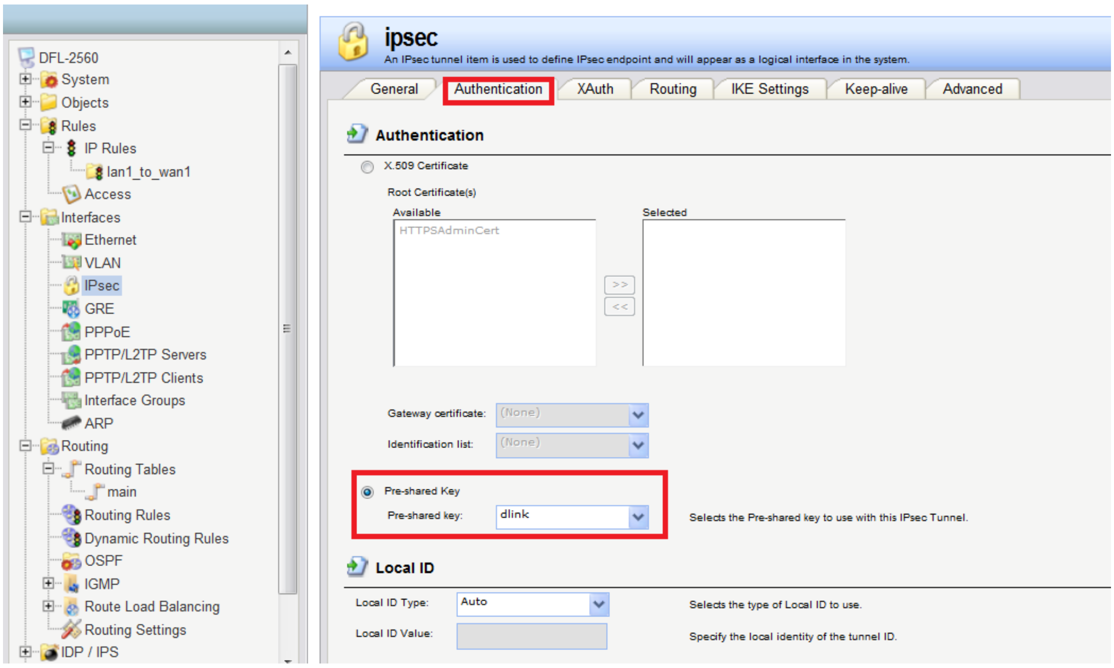
General

Name: ipsec
Local Network: 192.168.1.0/24
Remote Network: remote_network
Remote Endpoint: 2.2.2.1
Encapsulation mode: Tunnel
IKE Config Mode Pool: (None)

Algorithms

IKE Algorithms: Medium
IKE Lifetime: 28800 seconds
IPsec Algorithms: Medium
IPsec Lifetime: 3600 seconds
IPsec Lifetime: 0 kilobytes

Comments



ipsec

An IPsec tunnel item is used to define IPsec endpoint and will appear as a logical interface in the system.

Authentication

○ X.509 Certificate

Root Certificate(s)

Available: HTTPSAdminCert
Selected:

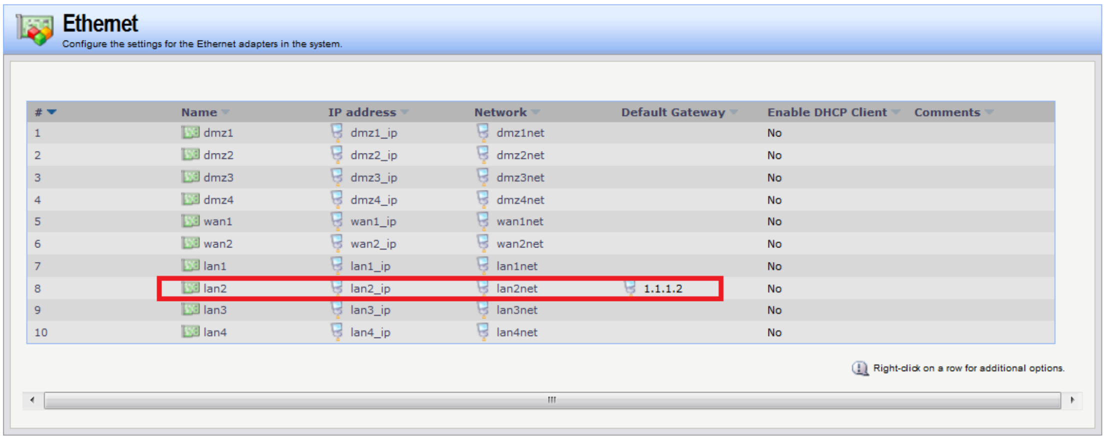
Gateway certificate: (None)
Identification list: (None)

● Pre-shared Key
Pre-shared key: dlink
Selects the Pre-shared key to use with this IPsec Tunnel.

Local ID

Local ID Type: Auto
Selects the type of Local ID to use.
Local ID Value:
Specify the local identity of the tunnel ID.

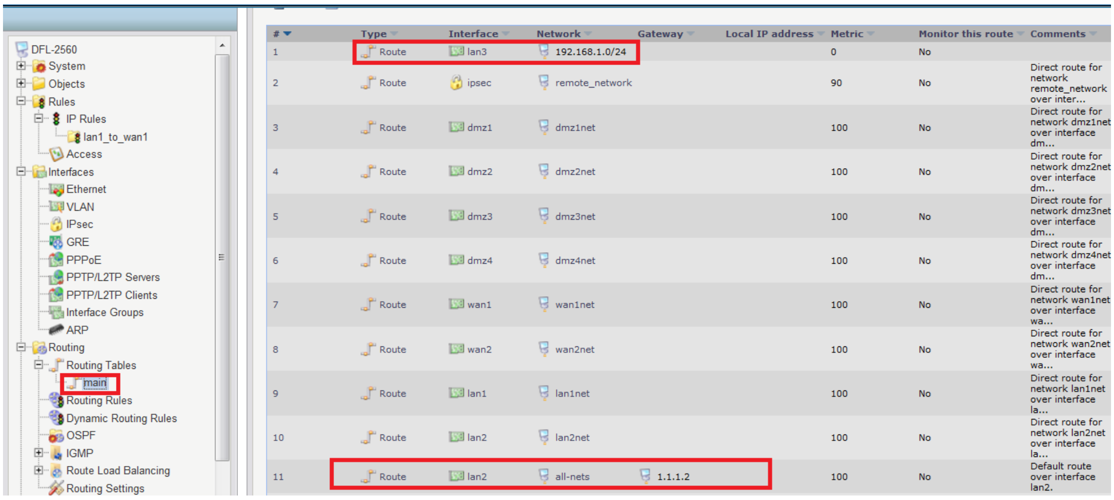
Step5. Add a routing entry for the virtual LAN net and add default gateway for the LAN2.



Ethernet
Configure the settings for the Ethernet adapters in the system.

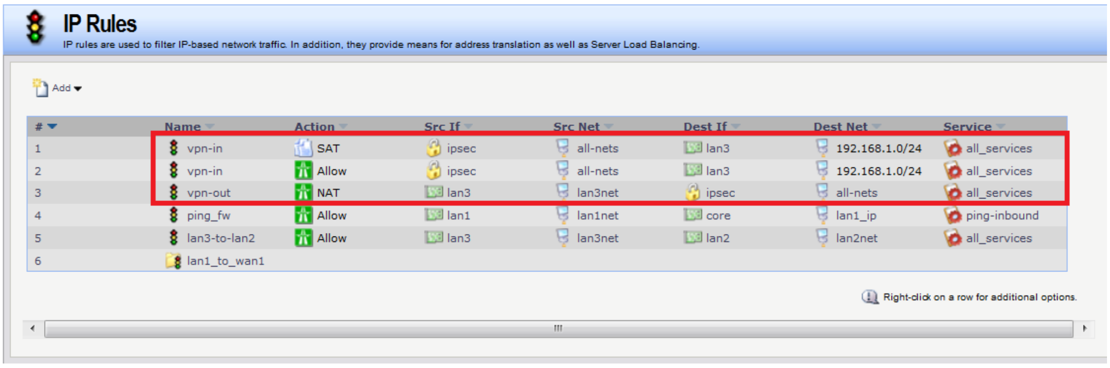
#	Name	IP address	Network	Default Gateway	Enable DHCP Client	Comments
1	dmz1	dmz1_ip	dmz1net		No	
2	dmz2	dmz2_ip	dmz2net		No	
3	dmz3	dmz3_ip	dmz3net		No	
4	dmz4	dmz4_ip	dmz4net		No	
5	wan1	wan1_ip	wan1net		No	
6	wan2	wan2_ip	wan2net		No	
7	lan1	lan1_ip	lan1net		No	
8	lan2	lan2_ip	lan2net	1.1.1.2	No	
9	lan3	lan3_ip	lan3net		No	
10	lan4	lan4_ip	lan4net		No	

Right-click on a row for additional options.



#	Type	Interface	Network	Gateway	Local IP address	Metric	Monitor this route	Comments
1	Route	lan3	192.168.1.0/24			0	No	
2	Route	ipsec	remote_network			90	No	Direct route for network remote_network over inter...
3	Route	dmz1	dmz1net			100	No	Direct route for network dmz1net over interface dm...
4	Route	dmz2	dmz2net			100	No	Direct route for network dmz2net over interface dm...
5	Route	dmz3	dmz3net			100	No	Direct route for network dmz3net over interface dm...
6	Route	dmz4	dmz4net			100	No	Direct route for network dmz4net over interface dm...
7	Route	wan1	wan1net			100	No	Direct route for network wan1net over interface wa...
8	Route	wan2	wan2net			100	No	Direct route for network wan2net over interface wa...
9	Route	lan1	lan1net			100	No	Direct route for network lan1net over interface la...
10	Route	lan2	lan2net			100	No	Direct route for network lan2net over interface la...
11	Route	lan2	all-nets	1.1.1.2		100	No	Default route over interface lan2.

Step6. Create one SAT and one Allow rule as the following screenshots for the IPSEC in bound traffic.

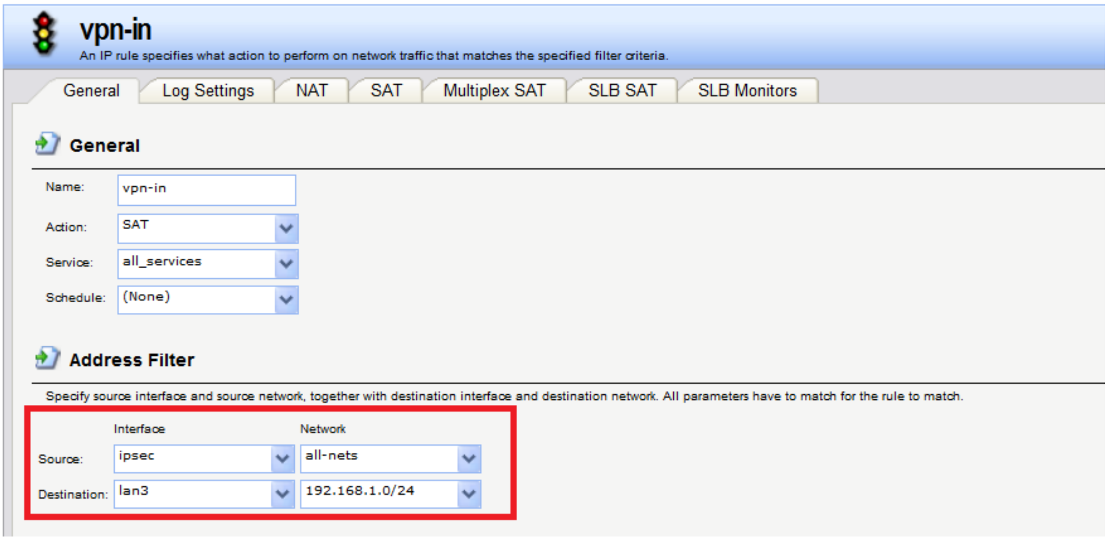


IP Rules
IP rules are used to filter IP-based network traffic. In addition, they provide means for address translation as well as Server Load Balancing.
Add

#	Name	Action	Src If	Src Net	Dest If	Dest Net	Service
1	vpn-in	SAT	ipsec	all-nets	lan3	192.168.1.0/24	all_services
2	vpn-in	Allow	ipsec	all-nets	lan3	192.168.1.0/24	all_services
3	vpn-out	NAT	lan3	lan3net	ipsec	all-nets	all_services
4	ping_fw	Allow	lan1	lan1net	core	lan1_ip	ping-inbound
5	lan3-to-lan2	Allow	lan3	lan3net	lan2	lan2net	all_services
6	lan1_to_wan1						

Right-click on a row for additional options.

SAT rule:



vpn-in

An IP rule specifies what action to perform on network traffic that matches the specified filter criteria.

General

Name: vpn-in

Action: SAT

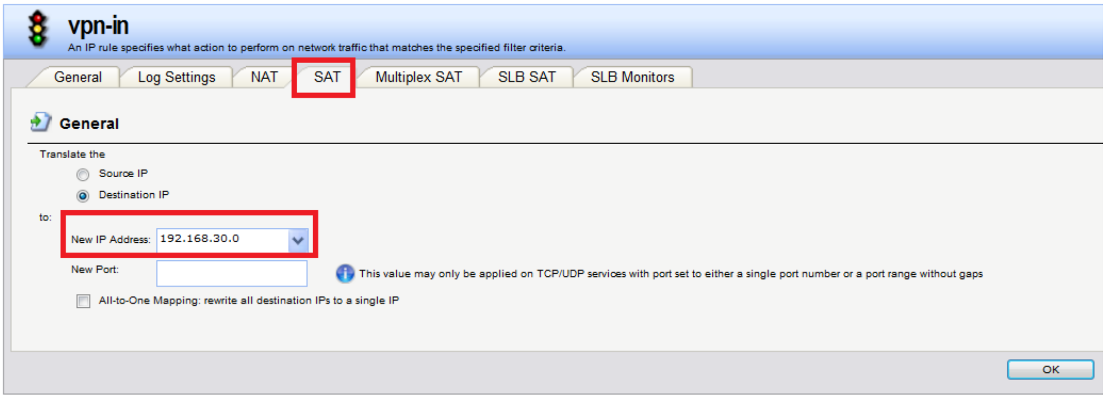
Service: all_services

Schedule: (None)

Address Filter

Specify source interface and source network, together with destination interface and destination network. All parameters have to match for the rule to match.

	Interface	Network
Source:	ipsec	all-nets
Destination:	lan3	192.168.1.0/24



vpn-in

An IP rule specifies what action to perform on network traffic that matches the specified filter criteria.

General

Translate the

○ Source IP

● Destination IP

to:

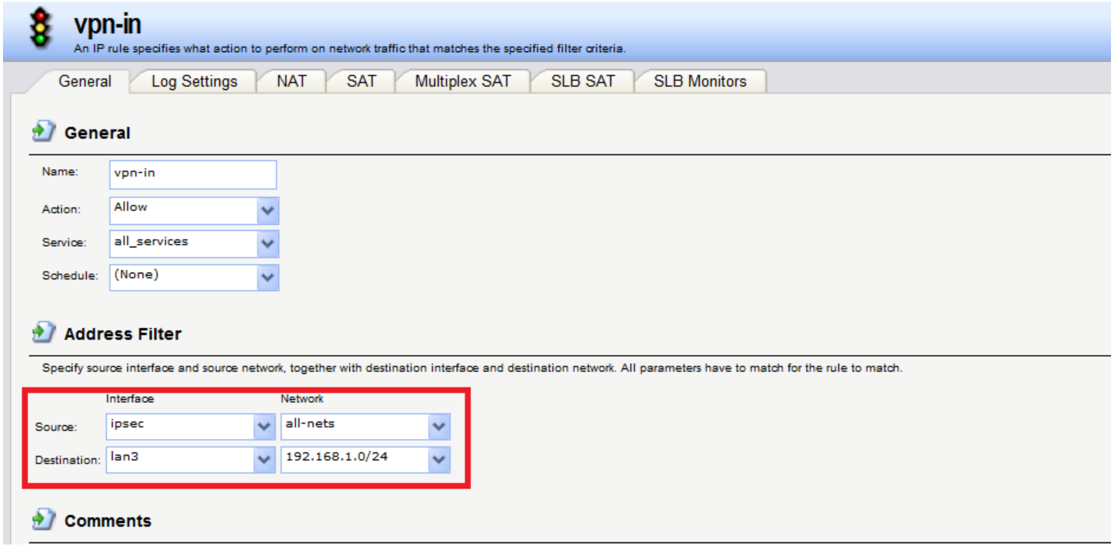
New IP Address: 192.168.30.0

New Port:

This value may only be applied on TCP/UDP services with port set to either a single port number or a port range without gaps

□ All-to-One Mapping: rewrite all destination IPs to a single IP

Allow rule:



vpn-in

An IP rule specifies what action to perform on network traffic that matches the specified filter criteria.

General

Name: vpn-in

Action: Allow

Service: all_services

Schedule: (None)

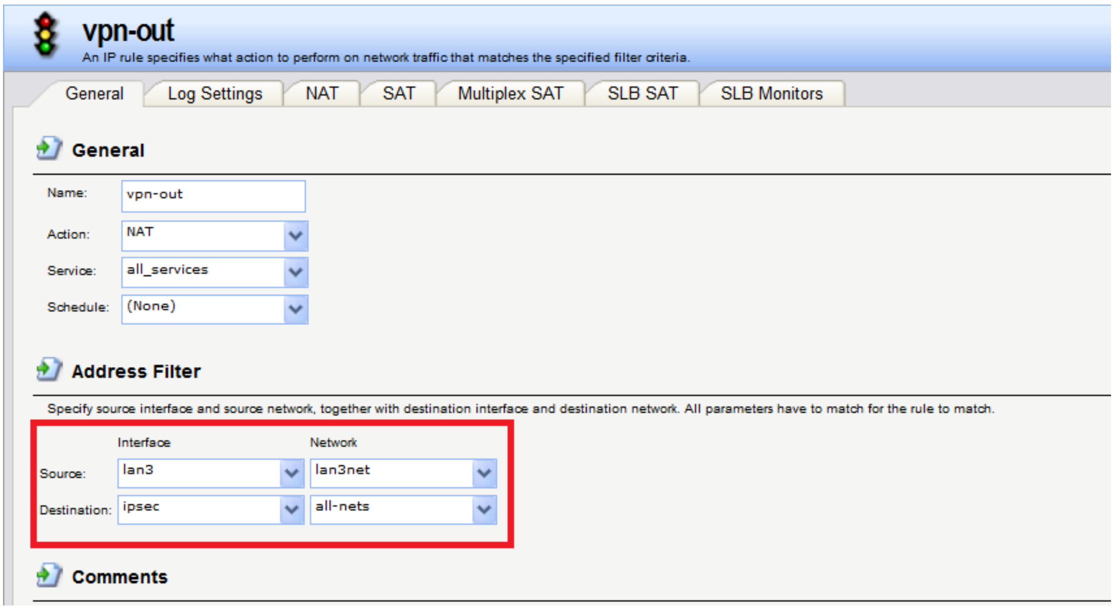
Address Filter

Specify source interface and source network, together with destination interface and destination network. All parameters have to match for the rule to match.

	Interface	Network
Source:	ipsec	all-nets
Destination:	lan3	192.168.1.0/24

Comments

Step7. Create a NAT rule as the following screenshots for the IPSEC out bound traffic.



vpn-out

An IP rule specifies what action to perform on network traffic that matches the specified filter criteria.

General

Name: vpn-out

Action: NAT

Service: all_services

Schedule: (None)

Address Filter

Specify source interface and source network, together with destination interface and destination network. All parameters have to match for the rule to match.

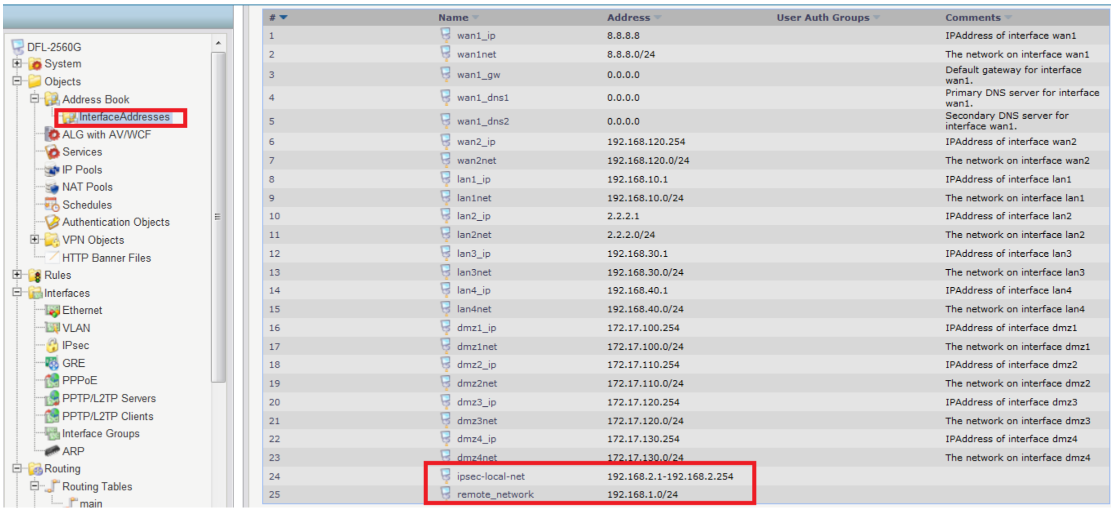
	Interface	Network
Source:	lan3	lan3net
Destination:	ipsec	all-nets

Comments

DFL-2560G

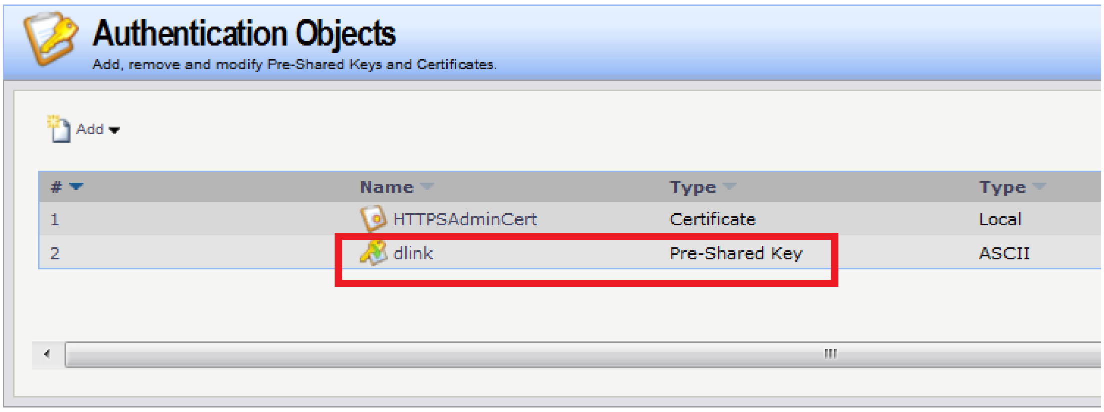
Step1. Set the IP address for LAN, Wan and other network objects respectively.

Remote network = the opposite virtual network



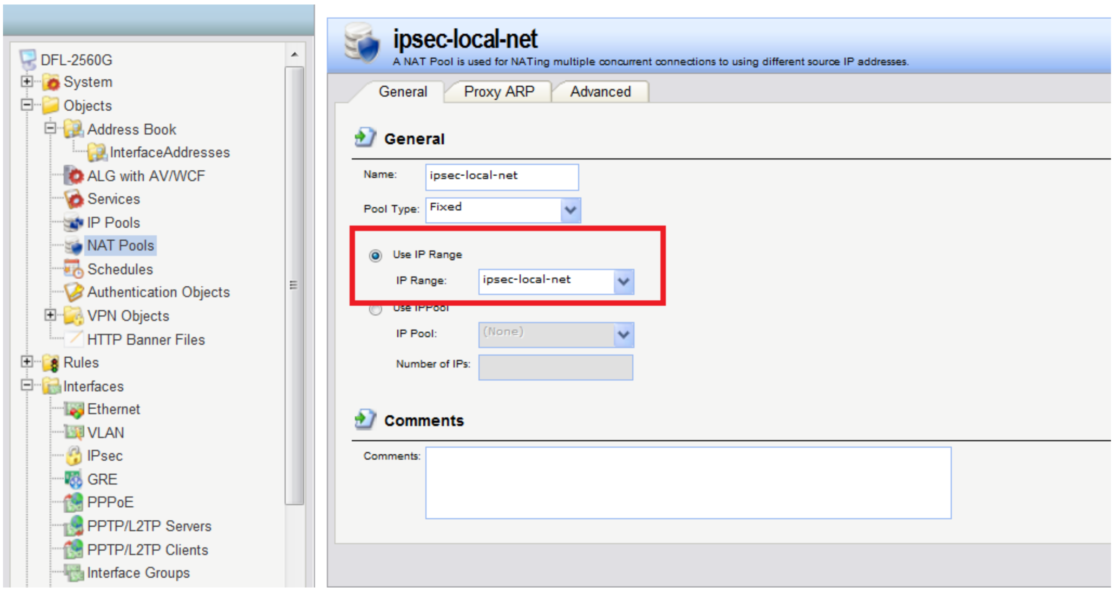
#	Name	Address	User Auth Groups	Comments
1	wan1_ip	8.8.8.8		IPAddress of interface wan1
2	wan1net	8.8.8.0/24		The network on interface wan1
3	wan1_gw	0.0.0.0		Default gateway for interface wan1.
4	wan1_dns1	0.0.0.0		Primary DNS server for interface wan1.
5	wan1_dns2	0.0.0.0		Secondary DNS server for interface wan1.
6	wan2_ip	192.168.120.254		IPAddress of interface wan2
7	wan2net	192.168.120.0/24		The network on interface wan2
8	lan1_ip	192.168.10.1		IPAddress of interface lan1
9	lan1net	192.168.10.0/24		The network on interface lan1
10	lan2_ip	2.2.2.1		IPAddress of interface lan2
11	lan2net	2.2.2.0/24		The network on interface lan2
12	lan3_ip	192.168.30.1		IPAddress of interface lan3
13	lan3net	192.168.30.0/24		The network on interface lan3
14	lan4_ip	192.168.40.1		IPAddress of interface lan4
15	lan4net	192.168.40.0/24		The network on interface lan4
16	dmz1_ip	172.17.100.254		IPAddress of interface dmz1
17	dmz1net	172.17.100.0/24		The network on interface dmz1
18	dmz2_ip	172.17.110.254		IPAddress of interface dmz2
19	dmz2net	172.17.110.0/24		The network on interface dmz2
20	dmz3_ip	172.17.120.254		IPAddress of interface dmz3
21	dmz3net	172.17.120.0/24		The network on interface dmz3
22	dmz4_ip	172.17.130.254		IPAddress of interface dmz4
23	dmz4net	172.17.130.0/24		The network on interface dmz4
24	ipsec-local-net	192.168.2.1-192.168.2.254		
25	remote_network	192.168.1.0/24		

Step2. Create a pre-shared key for IPSEC interface.



#	Name	Type	Type
1	HTTPSAdminCert	Certificate	Local
2	dlink	Pre-Shared Key	ASCII

Step3. Create a NAT POOL object as the screenshot below.



Name: ipsec-local-net

Pool Type: Fixed

● Use IP Range

IP Range: ipsec-local-net

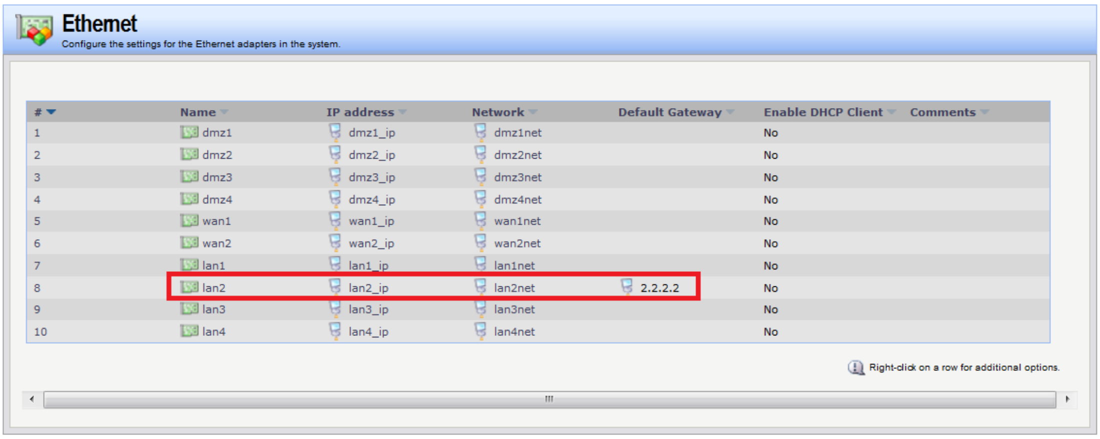
○ Use IPPool

IP Pool: (None)

Number of IPs:

Comments:

Step4. Add a routing entry for the virtual LAN net and add default gateway for the LAN2.

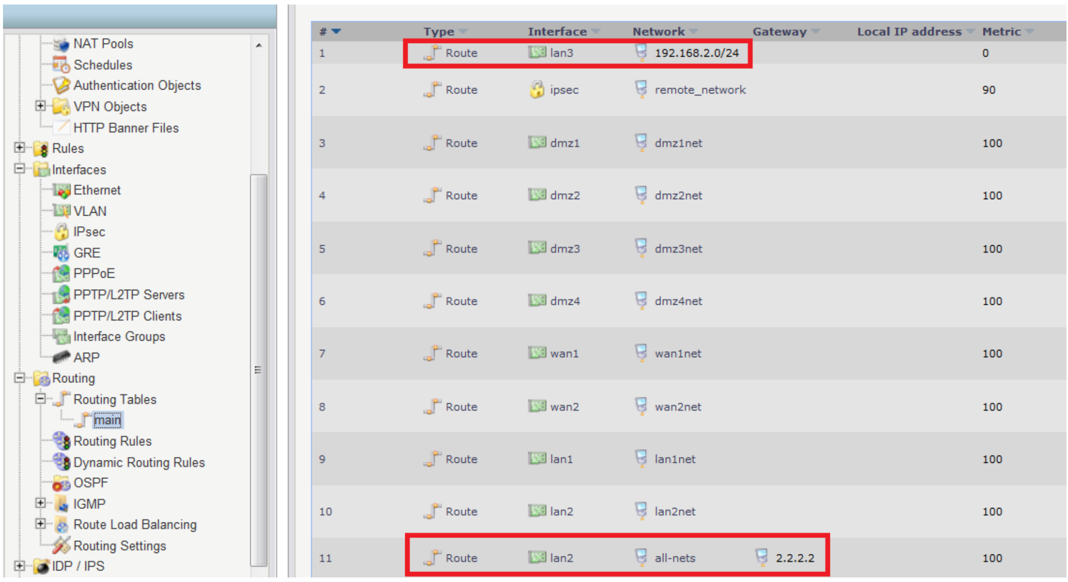


Ethernet

Configure the settings for the Ethernet adapters in the system.

#	Name	IP address	Network	Default Gateway	Enable DHCP Client	Comments
1	dmz1	dmz1_ip	dmz1net		No	
2	dmz2	dmz2_ip	dmz2net		No	
3	dmz3	dmz3_ip	dmz3net		No	
4	dmz4	dmz4_ip	dmz4net		No	
5	wan1	wan1_ip	wan1net		No	
6	wan2	wan2_ip	wan2net		No	
7	lan1	lan1_ip	lan1net		No	
8	lan2	lan2_ip	lan2net	2.2.2.2	No	
9	lan3	lan3_ip	lan3net		No	
10	lan4	lan4_ip	lan4net		No	

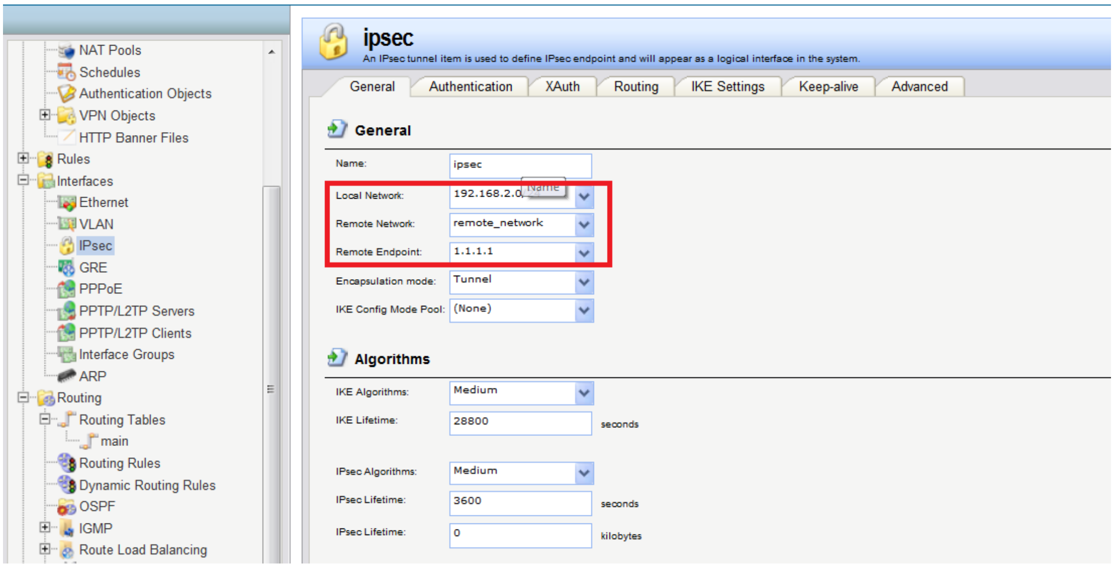
Right-click on a row for additional options.



#	Type	Interface	Network	Gateway	Local IP address	Metric
1	Route	lan3	192.168.2.0/24			0
2	Route	ipsec	remote_network			90
3	Route	dmz1	dmz1net			100
4	Route	dmz2	dmz2net			100
5	Route	dmz3	dmz3net			100
6	Route	dmz4	dmz4net			100
7	Route	wan1	wan1net			100
8	Route	wan2	wan2net			100
9	Route	lan1	lan1net			100
10	Route	lan2	lan2net			100
11	Route	lan2	all-nets	2.2.2.2		100

\

Step5. Create an IPSEC interface as the following screenshots.



ipsec

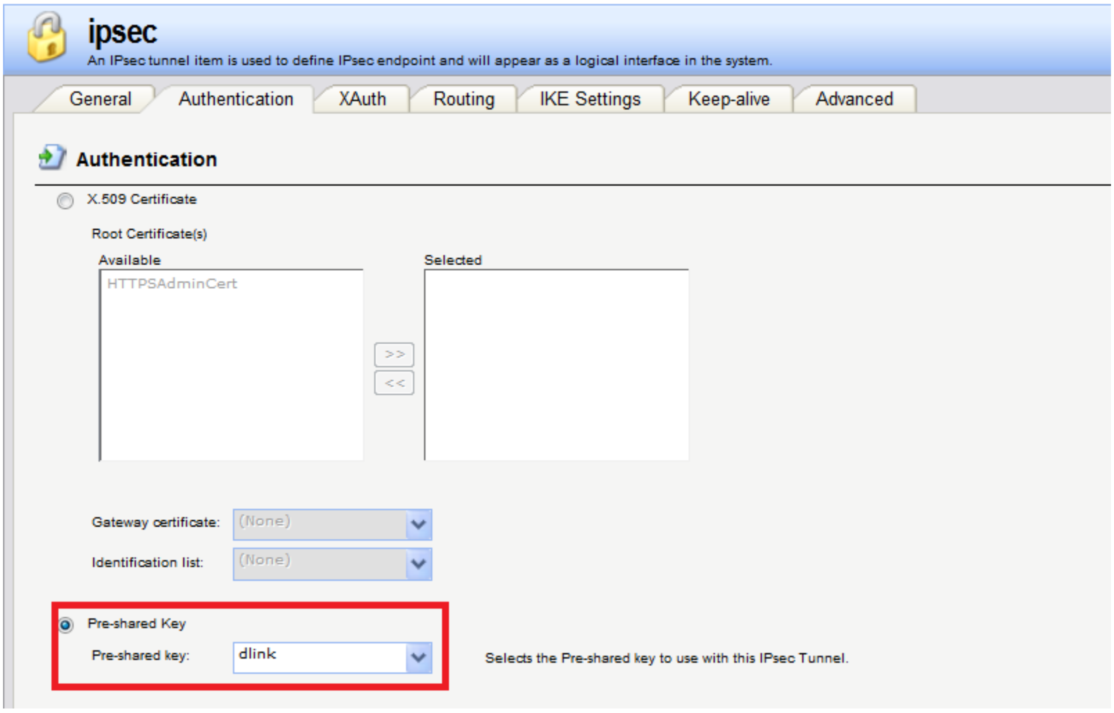
An IPsec tunnel item is used to define IPsec endpoint and will appear as a logical interface in the system.

General

Name:	ipsec	
Local Network:	192.168.2.0/24	
Remote Network:	remote_network	
Remote Endpoint:	1.1.1.1	
Encapsulation mode:	Tunnel	
IKE Config Mode Pool:	(None)	

Algorithms

IKE Algorithms:	Medium	
IKE Lifetime:	28800	seconds
IPsec Algorithms:	Medium	
IPsec Lifetime:	3600	seconds
IPsec Lifetime:	0	kilobytes



ipsec

An IPsec tunnel item is used to define IPsec endpoint and will appear as a logical interface in the system.

Authentication

○ X.509 Certificate

Root Certificate(s)

Available: HTTPSAdminCert

Selected:

Gateway certificate: (None)

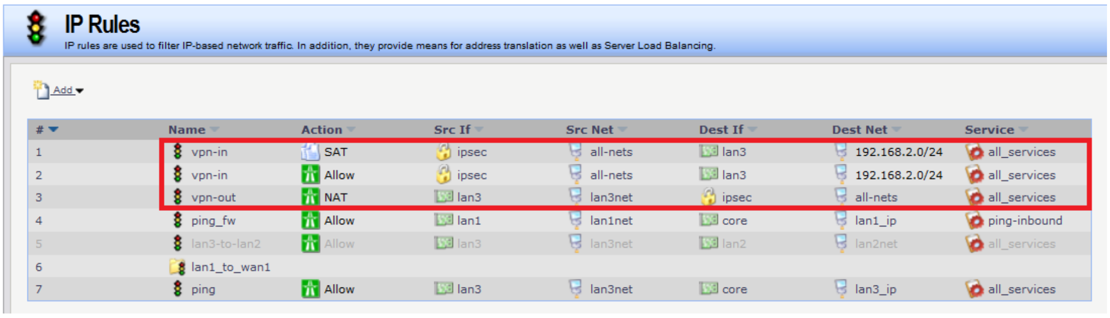
Identification list: (None)

● Pre-shared Key

Pre-shared key: dlink

Selects the Pre-shared key to use with this IPsec Tunnel.

Step6. Create one SAT and one Allow rule as the following screenshots for the IPSEC in bound traffic.

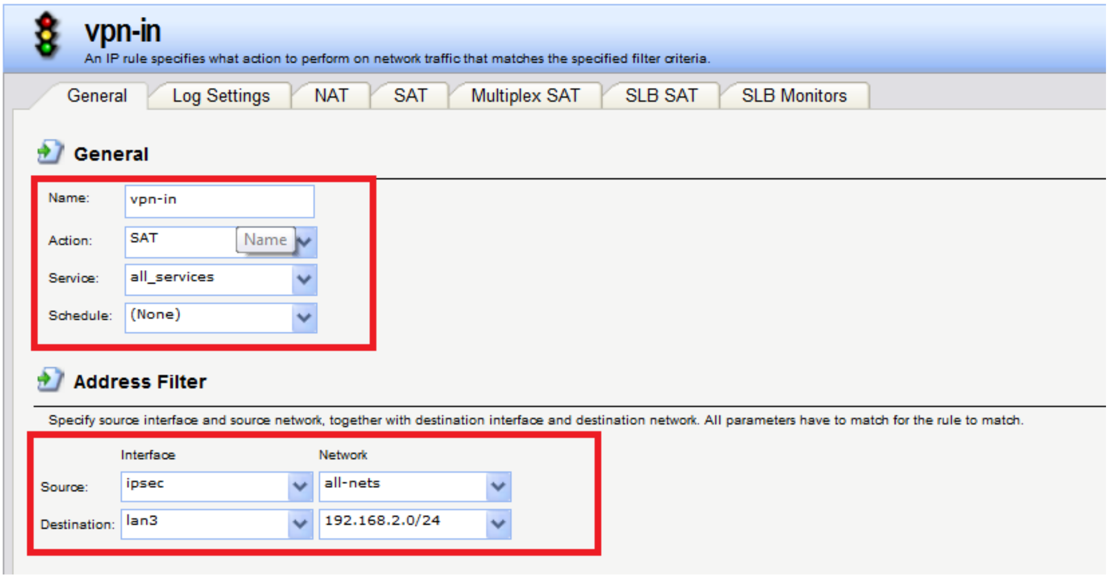


IP Rules

IP rules are used to filter IP-based network traffic. In addition, they provide means for address translation as well as Server Load Balancing.

#	Name	Action	Src If	Src Net	Dest If	Dest Net	Service
1	vpn-in	SAT	ipsec	all-nets	lan3	192.168.2.0/24	all_services
2	vpn-in	Allow	ipsec	all-nets	lan3	192.168.2.0/24	all_services
3	vpn-out	NAT	lan3	lan3net	ipsec	all-nets	all_services
4	ping_fw	Allow	lan1	lan1net	core	lan1_ip	ping-inbound
5	lan3-to-lan2	Allow	lan3	lan3net	lan2	lan2net	all_services
6	lan1_to_wan1						
7	ping	Allow	lan3	lan3net	core	lan3_ip	all_services

SAT rule:



vpn-in

An IP rule specifies what action to perform on network traffic that matches the specified filter criteria.

General

Name: vpn-in

Action: SAT

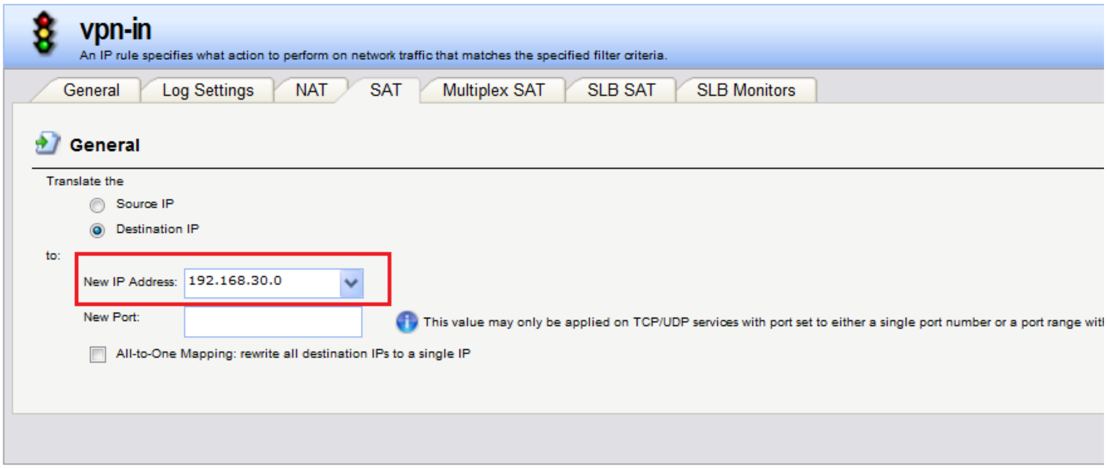
Service: all_services

Schedule: (None)

Address Filter

Specify source interface and source network, together with destination interface and destination network. All parameters have to match for the rule to match.

	Interface	Network
Source:	ipsec	all-nets
Destination:	lan3	192.168.2.0/24



vpn-in

An IP rule specifies what action to perform on network traffic that matches the specified filter criteria.

General

Translate the

○ Source IP

● Destination IP

to:

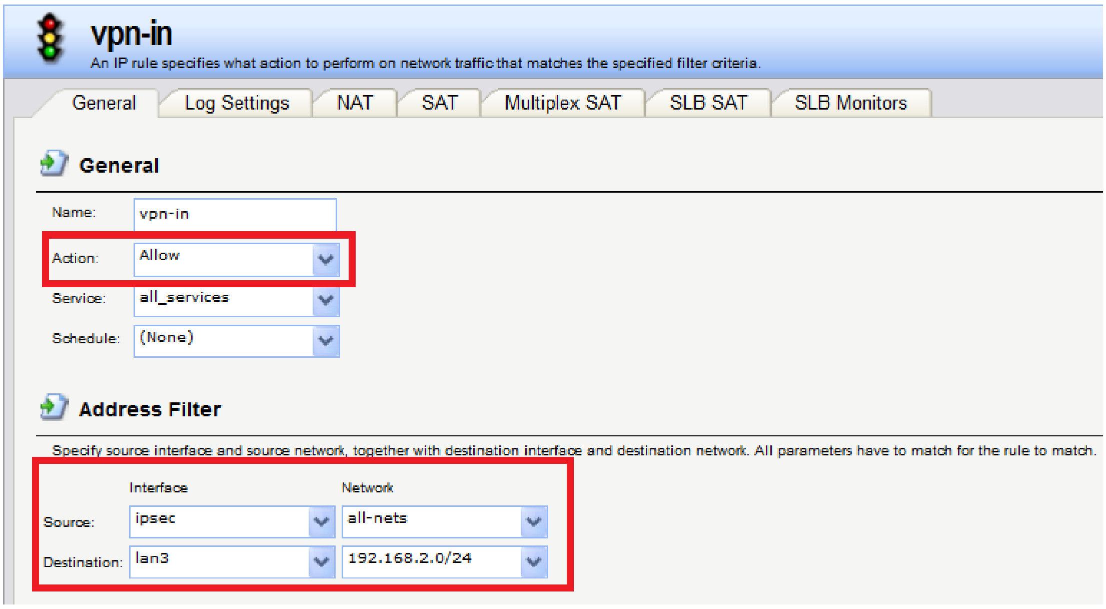
New IP Address: 192.168.30.0

New Port:

This value may only be applied on TCP/UDP services with port set to either a single port number or a port range wit

□ All-to-One Mapping: rewrite all destination IPs to a single IP

Allow rule:



vpn-in

An IP rule specifies what action to perform on network traffic that matches the specified filter criteria.

General

Name: vpn-in

Action: Allow

Service: all_services

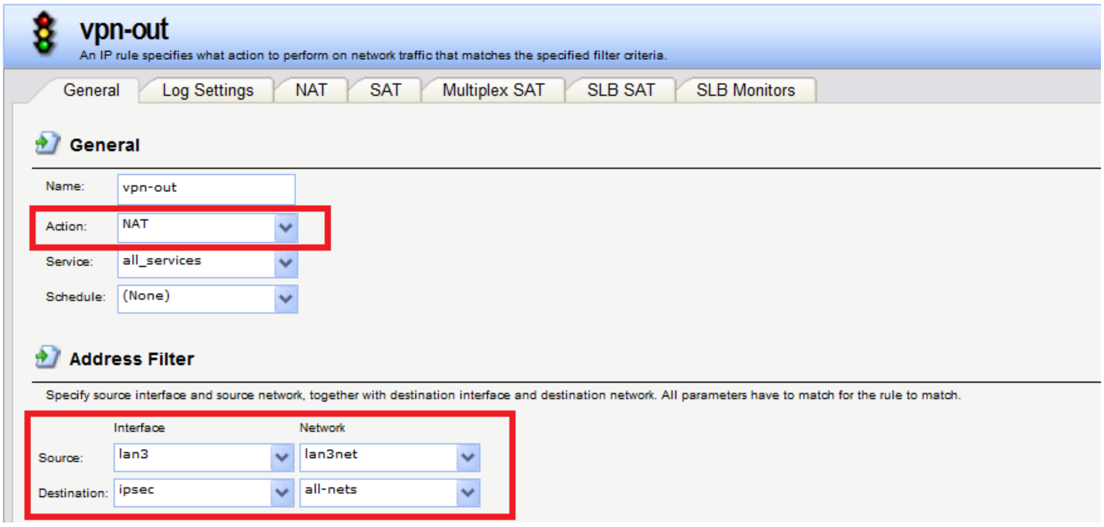
Schedule: (None)

Address Filter

Specify source interface and source network, together with destination interface and destination network. All parameters have to match for the rule to match.

	Interface	Network
Source:	ipsec	all-nets
Destination:	lan3	192.168.2.0/24

Step7. Create a NAT rule as the following screenshots for the IPSEC out bound traffic.



vpn-out

An IP rule specifies what action to perform on network traffic that matches the specified filter criteria.

General

Name: vpn-out

Action: NAT

Service: all_services

Schedule: (None)

Address Filter

Specify source interface and source network, together with destination interface and destination network. All parameters have to match for the rule to match.

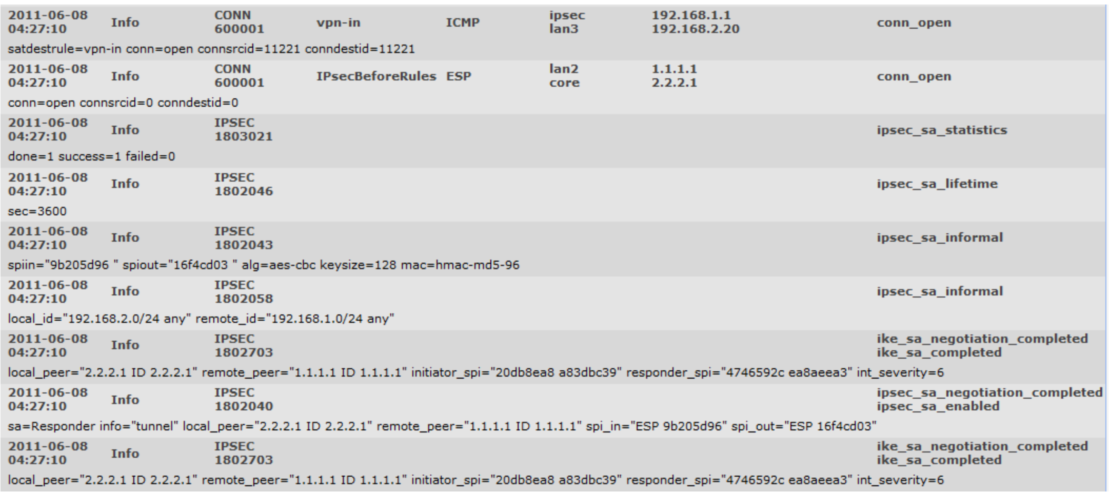
	Interface	Network
Source:	lan3	lan3net
Destination:	ipsec	all-nets

Result:

PC1 can access PC2 with 192.168.2.20.

PC2 can access PC1 with 192.168.1.10

Note that the log page below is captured on DFL-2560G



```
2011-06-08  Info  CONN     vpn-in           ICMP  ipsec  192.168.1.1    conn_open
04:27:10          600001                          lan3   192.168.2.20
satdestrule=vpn-in conn=open connsrcid=11221 conndestid=11221
2011-06-08  Info  CONN     IPsecBeforeRules ESP   lan2   1.1.1.1        conn_open
04:27:10          600001                          core   2.2.2.1
conn=open connsrcid=0 conndestid=0
2011-06-08  Info  IPSEC                                                 ipsec_sa_statistics
04:27:10          1803021
done=1 success=1 failed=0
2011-06-08  Info  IPSEC                                                 ipsec_sa_lifetime
04:27:10          1802046
sec=3600
2011-06-08  Info  IPSEC                                                 ipsec_sa_informal
04:27:10          1802043
spiin="9b205d96 " spiout="16f4cd03 " alg=aes-cbc keysize=128 mac=hmac-md5-96
2011-06-08  Info  IPSEC                                                 ipsec_sa_informal
04:27:10          1802058
local_id="192.168.2.0/24 any" remote_id="192.168.1.0/24 any"
2011-06-08  Info  IPSEC                                                 ike_sa_negotiation_completed
04:27:10          1802703                                               ike_sa_completed
local_peer="2.2.2.1 ID 2.2.2.1" remote_peer="1.1.1.1 ID 1.1.1.1" initiator_spi="20db8ea8 a83dbc39" responder_spi="4746592c ea8aeea3" int_severity=6
2011-06-08  Info  IPSEC                                                 ipsec_sa_negotiation_completed
04:27:10          1802040                                               ipsec_sa_enabled
sa=Responder info="tunnel" local_peer="2.2.2.1 ID 2.2.2.1" remote_peer="1.1.1.1 ID 1.1.1.1" spi_in="ESP 9b205d96" spi_out="ESP 16f4cd03"
2011-06-08  Info  IPSEC                                                 ike_sa_negotiation_completed
04:27:10          1802703                                               ike_sa_completed
local_peer="2.2.2.1 ID 2.2.2.1" remote_peer="1.1.1.1 ID 1.1.1.1" initiator_spi="20db8ea8 a83dbc39" responder_spi="4746592c ea8aeea3" int_severity=6
```

END