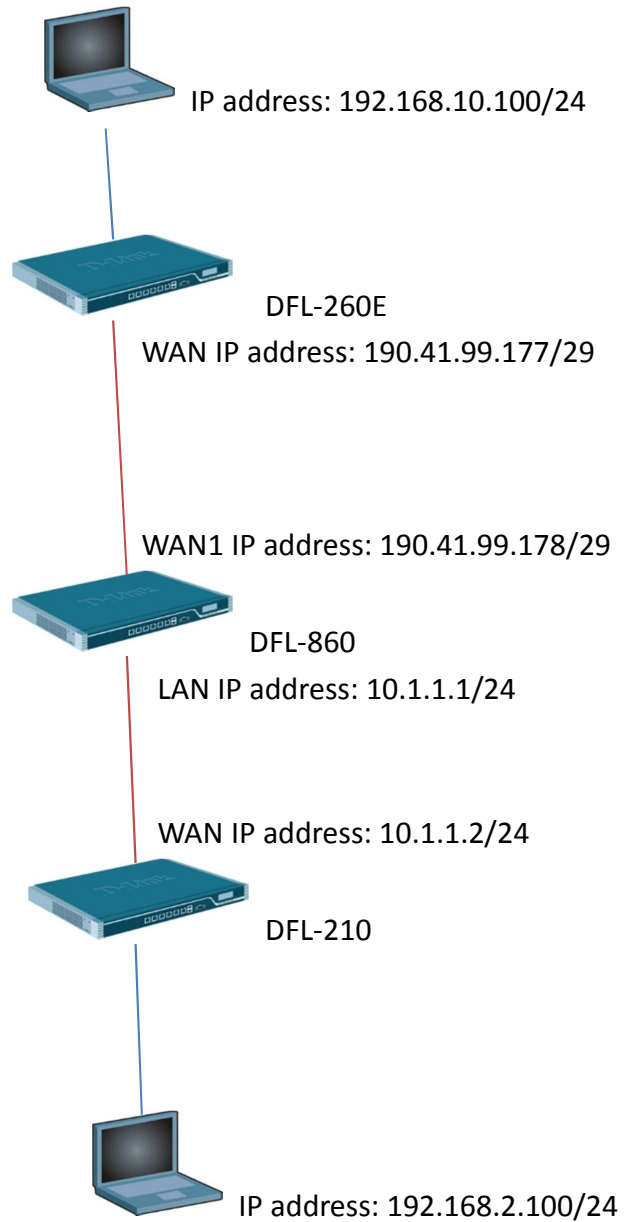


How to setup IPsec NAT traversal on DFL-860

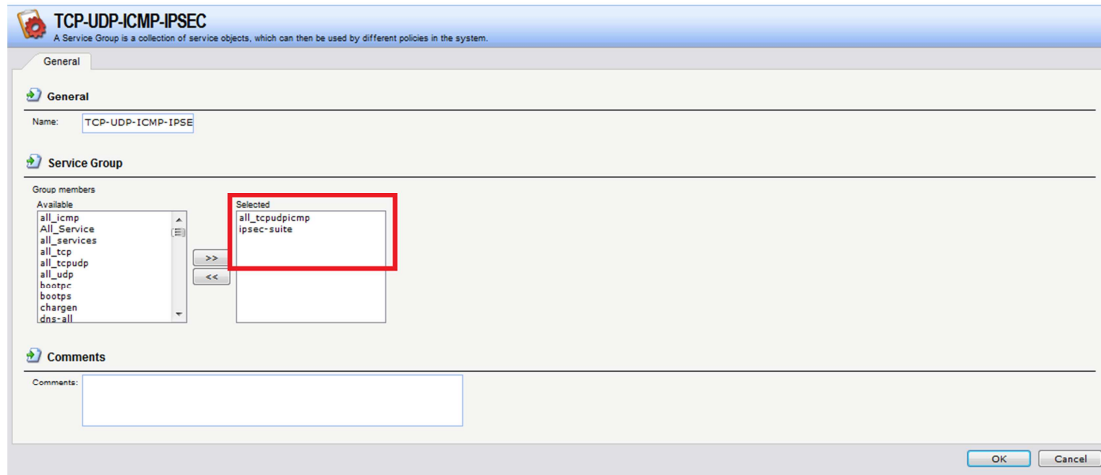
Topology:



(1) We need to add a new service “TCP-UDP-ICMP-IPSEC”.

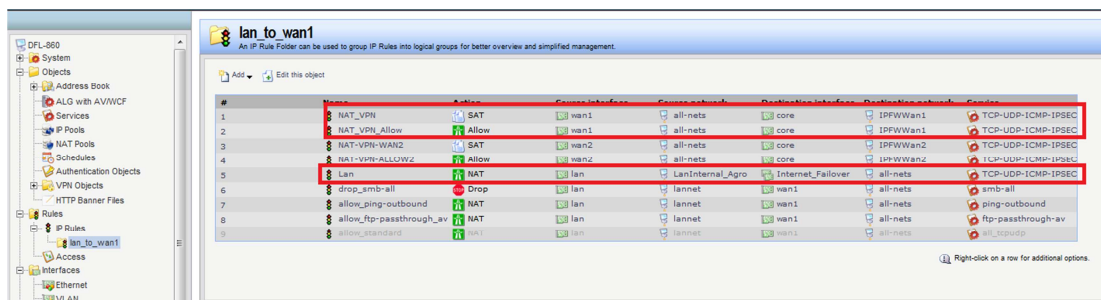


(2) Choose “all_tcpudpicmp” and “ipsec-suite”. “ipsec-suite” has IP protocol 50, 51 and UDP port 500 and 4500.



(3) Because IPsec traffic is bidirectional. We need use new service “TCP-UDP-ICMP-IPSEC” for LAN to WAN rules and WAN to LAN rules. Because DFL-860 just do IPsec NAT traversal therefore we need to use SAT+ALLOW rule make IPsec traffic transmit to DFL-210.

DFL-260E IPsec remote endpoint is IP address 190.41.99.178.



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

General Log Settings NAT SAT Multiplex SAT SLB SAT SLB Monitors

General

Name: NAT_VPN

Action: SAT

Service: **TCP-UDP-ICMP-IP**

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.

Source: Interface: wan1 Network: all-nets

Destination: core IPFWwan1

Comments

(4) IsaServer = IP address 10.1.1.2/24

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

General Log Settings NAT SAT Multiplex SAT SLB SAT SLB Monitors

General

Translate the

Source IP

Destination IP

to:

New IP Address: **IsaServer**

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

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

General Log Settings NAT SAT Multiplex SAT SLB SAT SLB Monitors

General

Name: Lan

Action: NAT

Service: **TCP-UDP-ICMP-IP**

Schedule: (None)

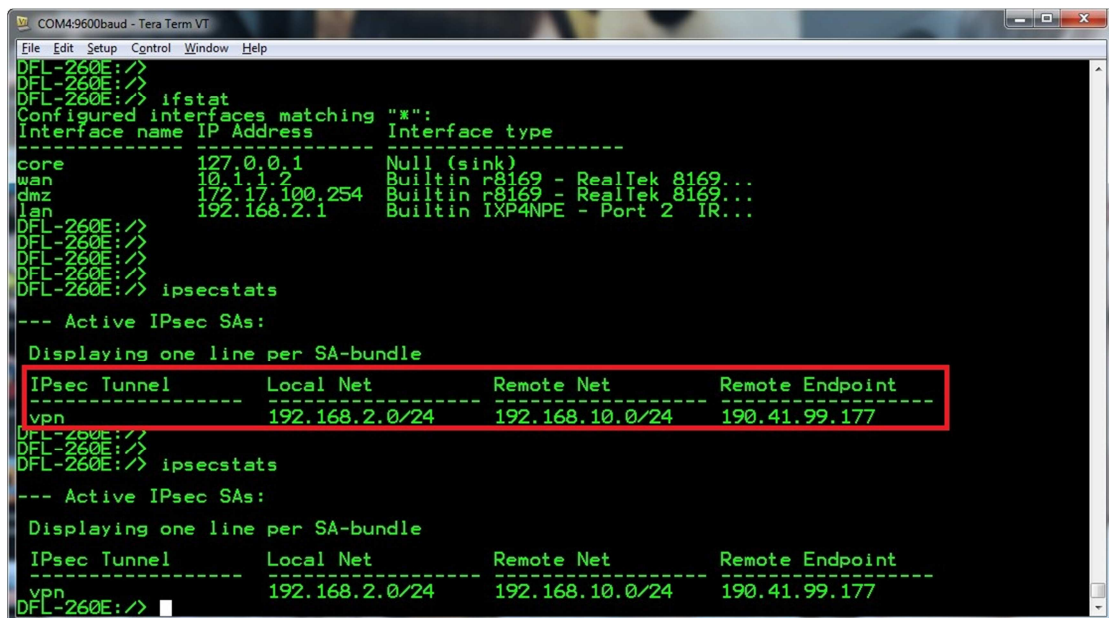
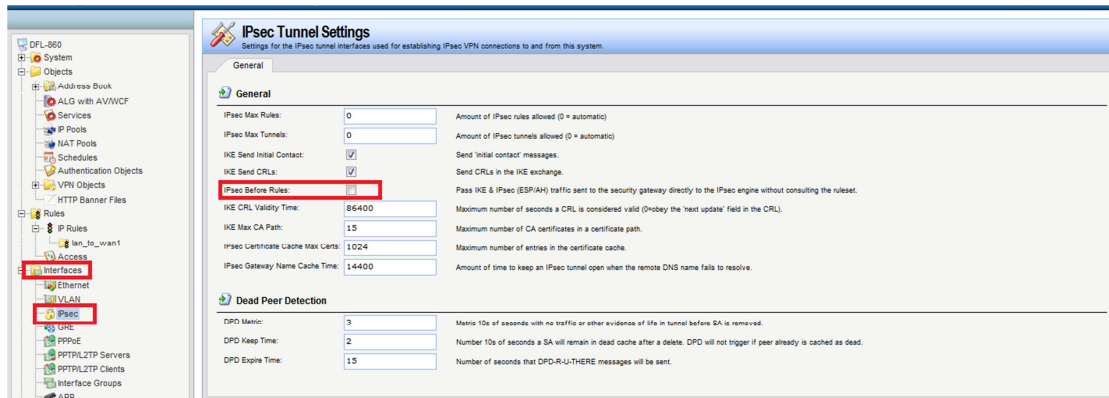
Address Filter

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

Source: Interface: lan Network: LanInternal_Agro

Destination: Internet_Failover all-nets

(5) Go to advanced settings. Disable "IPSec before rule".



END