APPLICATION NOTE 004

Double WeOS 1-1 NAT Rules with Proxy ARP

How to use the same subnet on both sides of a routed link.

Application Note Network Layout

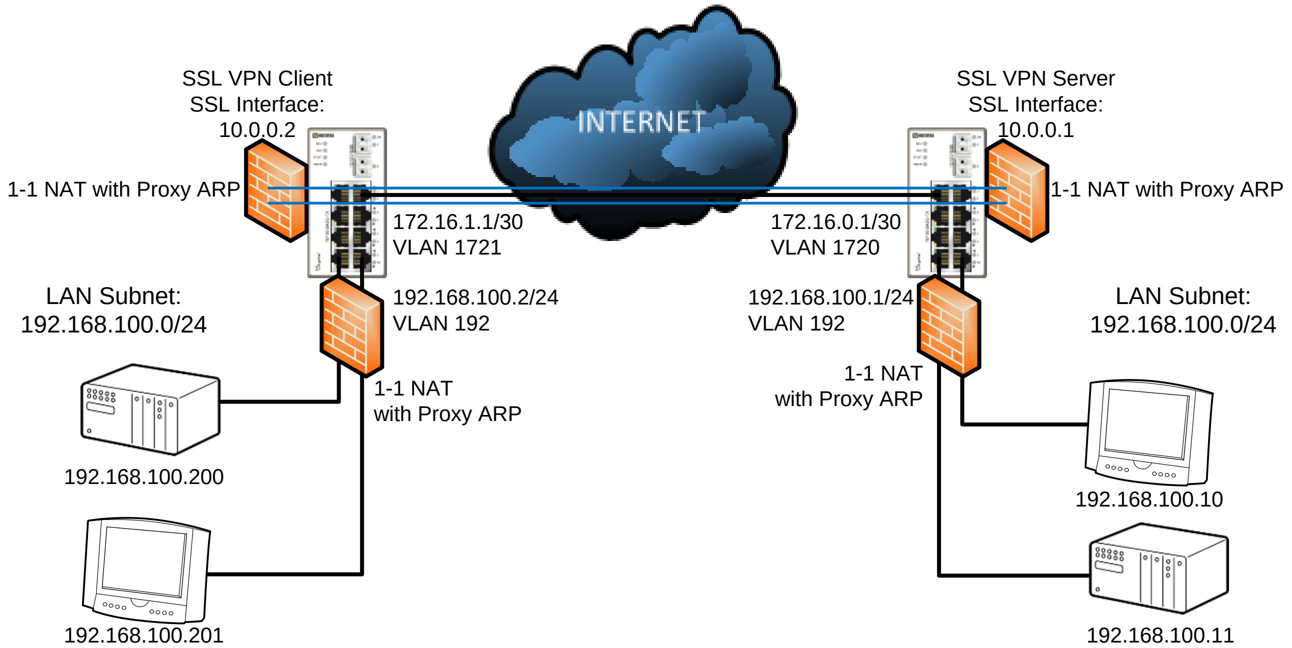
This Application Note shows how to handle the situation where the same subnet needs to be connected together over a routed network, but without the possibility to configure Default Gateways on the connected equipment.

Background

The 1-1 NAT with Proxy ARP functionality of the WeOS firewall can be used for handling the situation where the connected equipment can not configure a Default Gateway.
An SSL VPN tunnel is used to securely link the two parts of the same network together.
This also generates two new interfaces, SSL, that can be used for setting up a second 1-1 NAT rule on each side of the tunnel.
The equipment on both sides of the tunnel must have unique IP-addresses in the subnet.
Please Note! This is not the recommended way to design new networks this solution is mainly for existing networks that are limited in its possibilities to introduce routing.

All configuration in this Application Note is done using WeOS version 4.16.0.

The communication works in this way:
If the HMI at 192.168.100.10 wants to send traffic to the PLC at 192.168.100.200 on the other side of the tunnel it will only have to use the 192.168.100.200 IP-address.
When it sends out the ARP asking for 192.168.100.200 the Lynx at 192.168.100.1 will answer the ARP as it is part of its 1-1 NAT rule using Proxy ARP. The traffic is then forwaded to the VPN Client’s SSL interface, 10.0.0.2, on the other side of the tunnel which also has a 1-1 NAT rule with Proxy ARP. This rule will then pass the traffic out to 192.168.100.200 on the VPN Client’s internal LAN.
The source addresses are never changed for the LAN to LAN communication so ARPs for the reply traffic are picked up by the nearest Lynx through the Proxy ARP function.

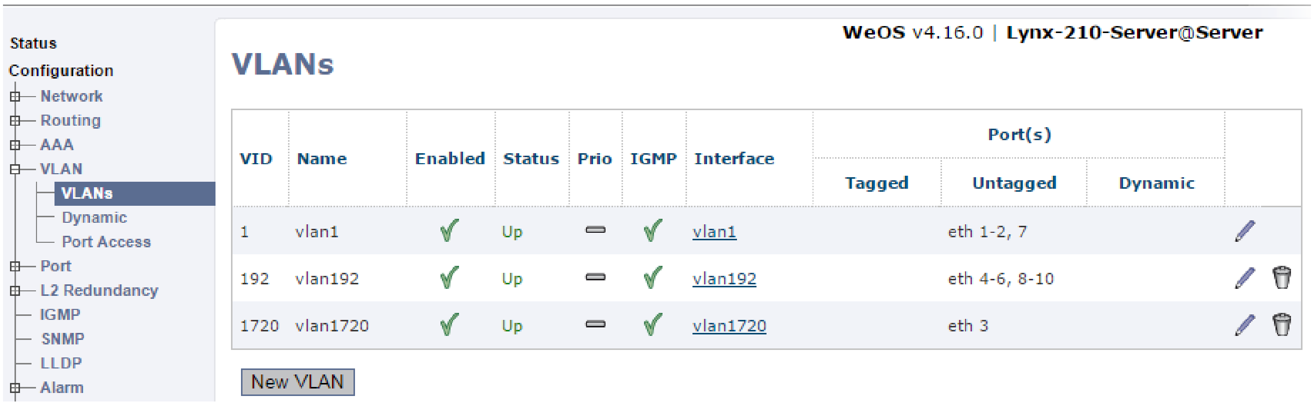


Configuration

VLAN

First setup the VLANs needed.

Server: VLAN 192 is the internal LAN and VLAN 1720 is the external WAN connection.

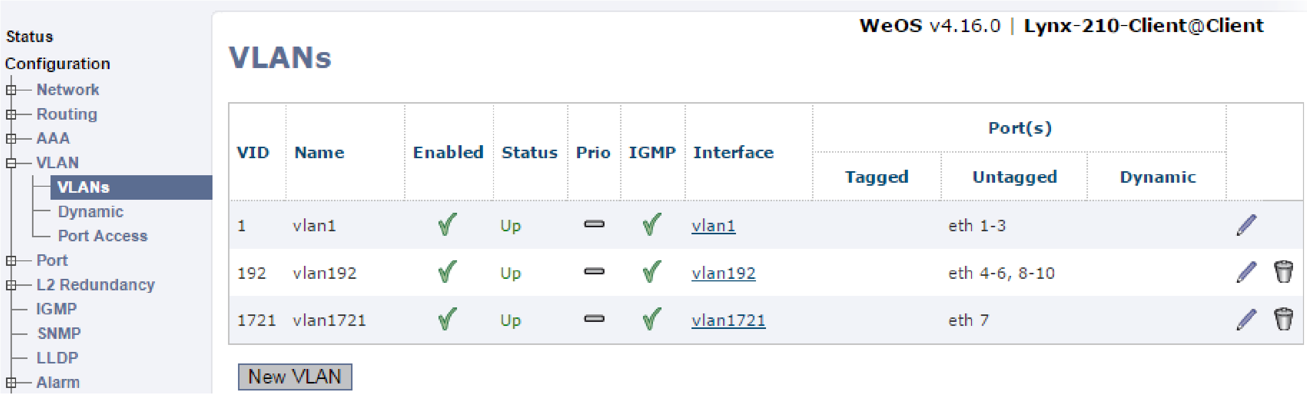


WeOS v4.16.0 | Lynx-210-Server@Server

VLANs

VID	Name	Enabled	Status	Prio	IGMP	Interface	Port(s)			
							Tagged	Untagged	Dynamic	
1	vlan1	✓	Up	−	✓	vlan1		eth 1-2, 7		✎
192	vlan192	✓	Up	−	✓	vlan192		eth 4-6, 8-10		✎ 🗑
1720	vlan1720	✓	Up	−	✓	vlan1720		eth 3		✎ 🗑

Client: VLAN 192 is the internal LAN and VLAN 1721 is the external WAN connection.



WeOS v4.16.0 | Lynx-210-Client@Client

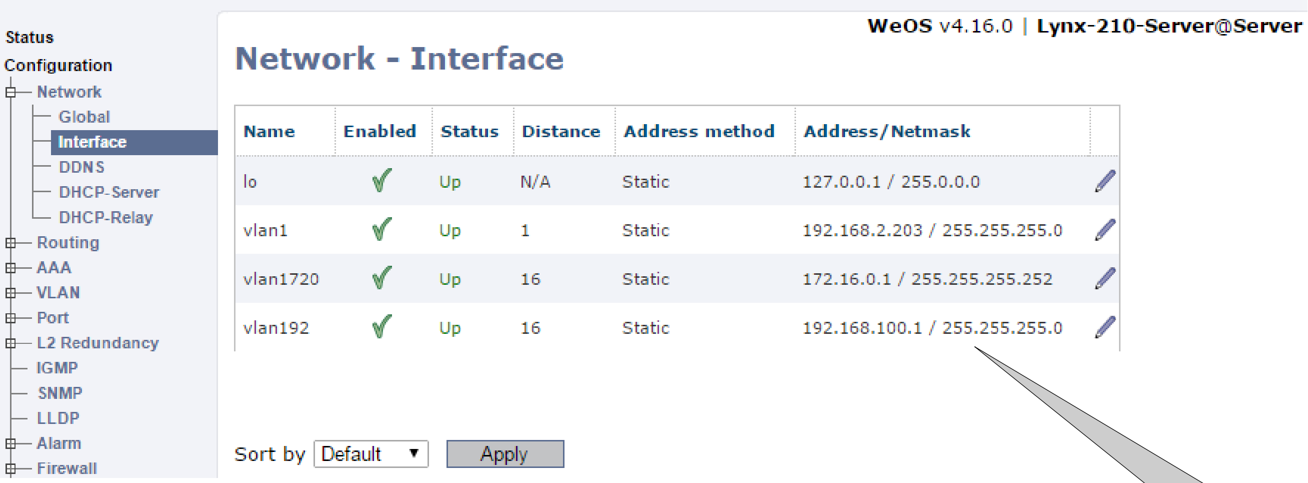
VLANs

VID	Name	Enabled	Status	Prio	IGMP	Interface	Port(s)			
							Tagged	Untagged	Dynamic	
1	vlan1	✓	Up	−	✓	vlan1		eth 1-3		✎
192	vlan192	✓	Up	−	✓	vlan192		eth 4-6, 8-10		✎ 🗑
1721	vlan1721	✓	Up	−	✓	vlan1721		eth 7		✎ 🗑

Interface

Then configure IP-addresses for the interfaces.

Server:



WeOS v4.16.0 | **Lynx-210-Server@Server**

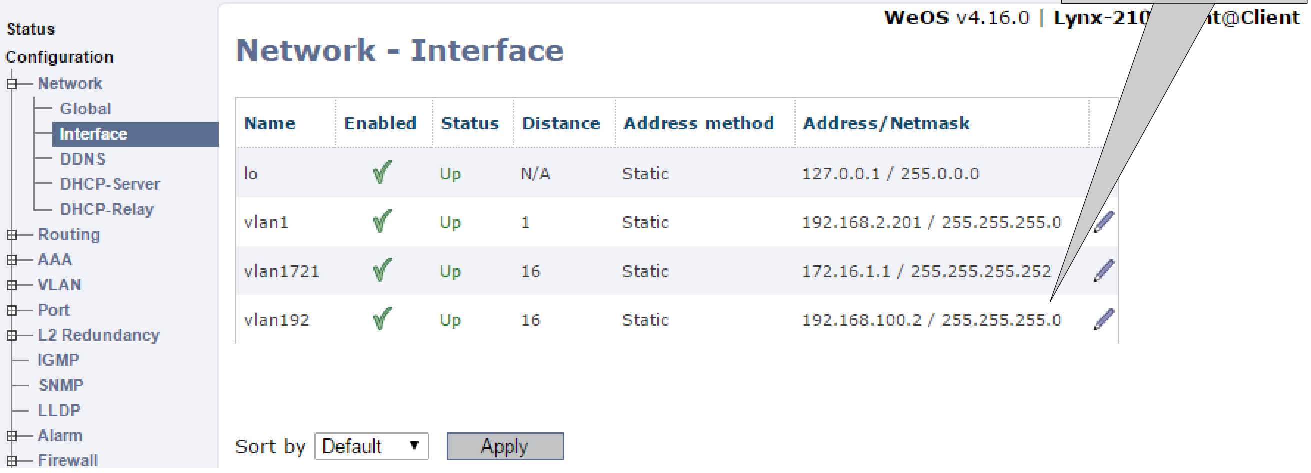
Network - Interface

Name	Enabled	Status	Distance	Address method	Address/Netmask	
lo	✓	Up	N/A	Static	127.0.0.1 / 255.0.0.0	✎
vlan1	✓	Up	1	Static	192.168.2.203 / 255.255.255.0	✎
vlan1720	✓	Up	16	Static	172.16.0.1 / 255.255.255.252	✎
vlan192	✓	Up	16	Static	192.168.100.1 / 255.255.255.0	✎

Sort by Default ▾ Apply

VLAN 192 has the same subnet on both units.

Client:



WeOS v4.16.0 | **Lynx-210 t@Client**

Network - Interface

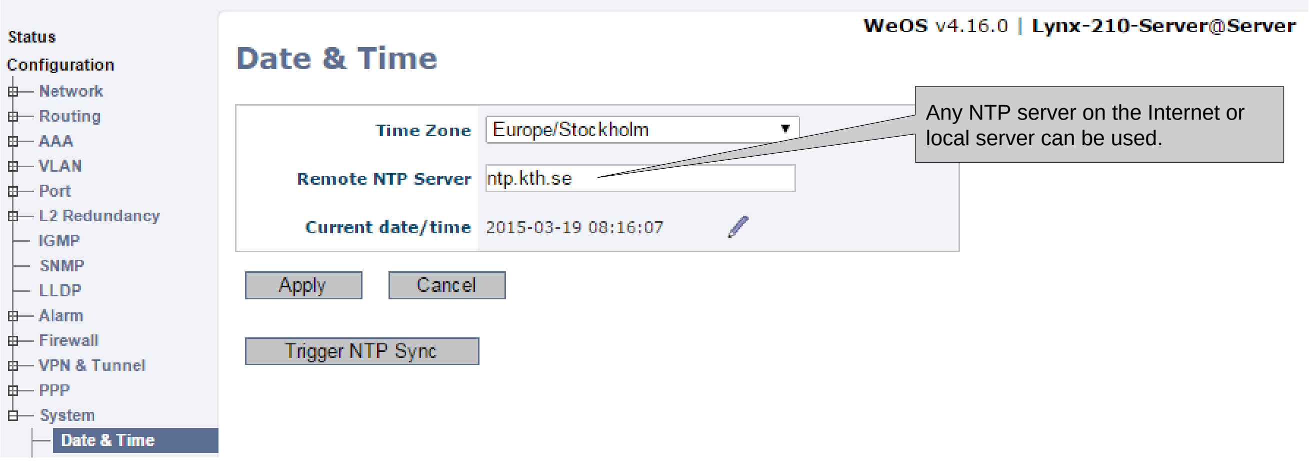
Name	Enabled	Status	Distance	Address method	Address/Netmask	
lo	✓	Up	N/A	Static	127.0.0.1 / 255.0.0.0	
vlan1	✓	Up	1	Static	192.168.2.201 / 255.255.255.0	✎
vlan1721	✓	Up	16	Static	172.16.1.1 / 255.255.255.252	✎
vlan192	✓	Up	16	Static	192.168.100.2 / 255.255.255.0	✎

Sort by Default ▾ Apply

Certificates

In order for the SSL VPN certificates to work properly the switches will have to have the correct time set. To make sure this is the case it is best to synchronize the time with a time server. If this can not be achieved make sure the time is as accurate as possible.

Server and Client:



WeOS v4.16.0 | Lynx-210-Server@Server

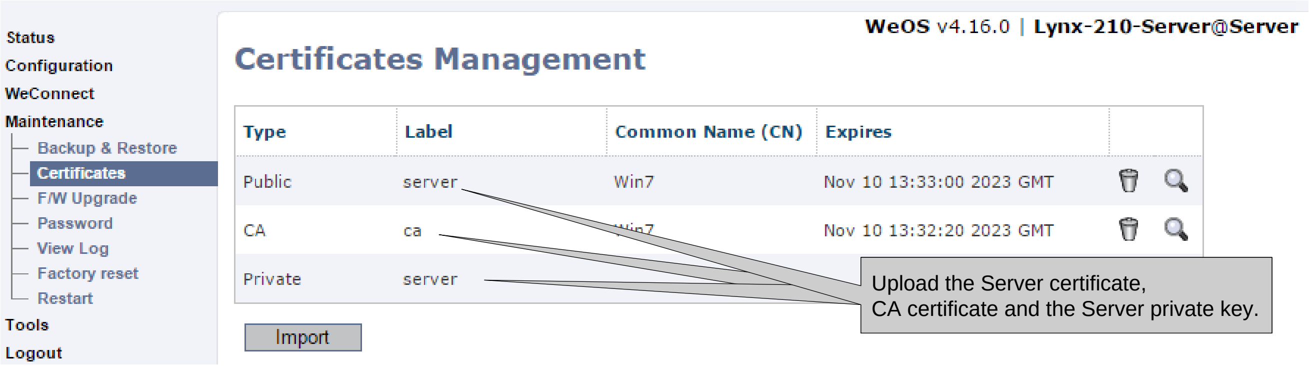
Date & Time

Time Zone	Europe/Stockholm
Remote NTP Server	ntp.kth.se
Current date/time	2015-03-19 08:16:07

Any NTP server on the Internet or local server can be used.

Upload the certificates for the SSL VPN to each switch.
Please Note! How to generate the certificates for the SSL VPN Tunnel is described in Tech Note 003 Self Signed Certificates.

Server:



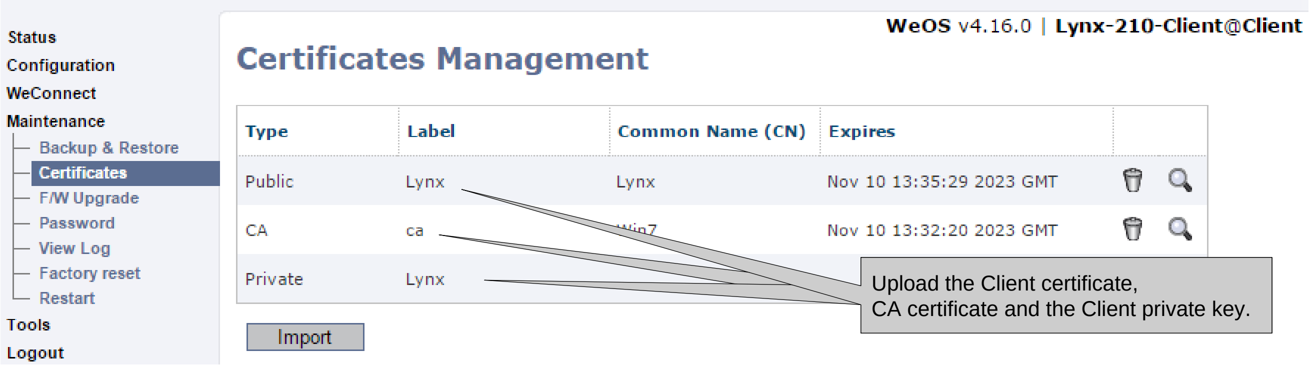
WeOS v4.16.0 | Lynx-210-Server@Server

Certificates Management

Type	Label	Common Name (CN)	Expires
Public	server	Win7	Nov 10 13:33:00 2023 GMT
CA	ca	Win7	Nov 10 13:32:20 2023 GMT
Private	server		

Upload the Server certificate,
CA certificate and the Server private key.

Client:



WeOS v4.16.0 | Lynx-210-Client@Client

Certificates Management

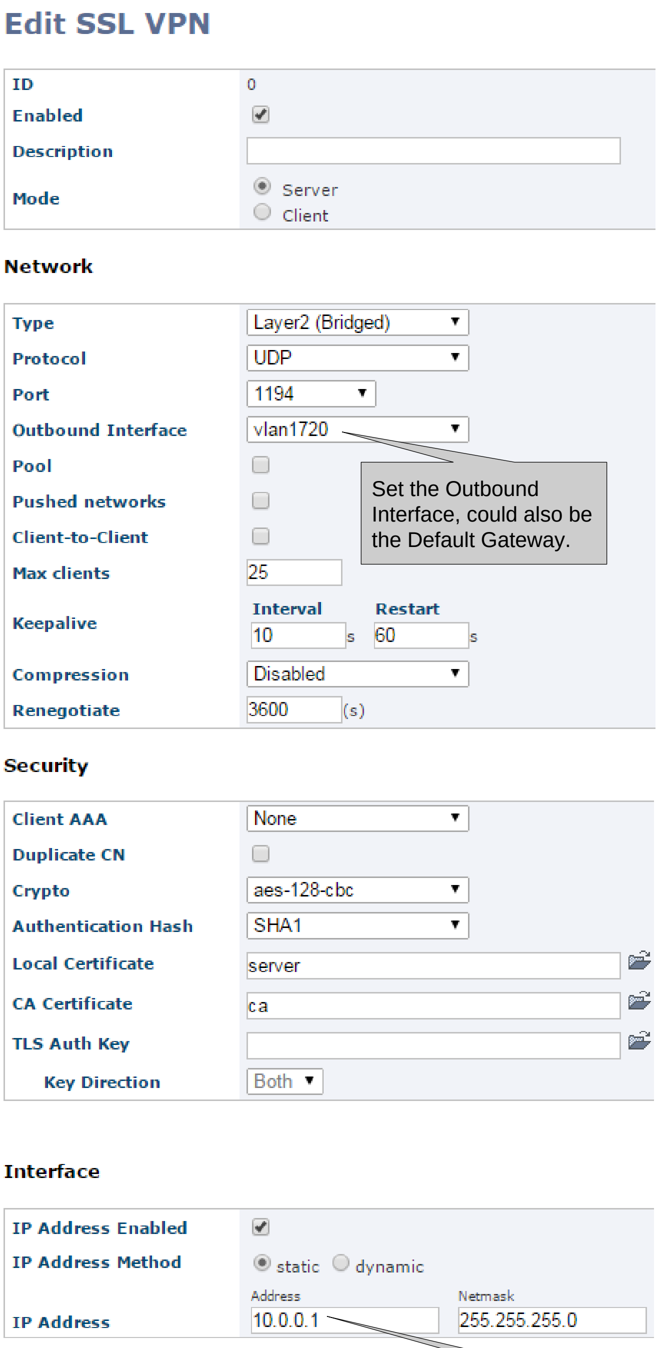
Type	Label	Common Name (CN)	Expires
Public	Lynx	Lynx	Nov 10 13:35:29 2023 GMT
CA	ca	Win7	Nov 10 13:32:20 2023 GMT
Private	Lynx		

Upload the Client certificate,
CA certificate and the Client private key.

SSL VPN Tunnel

After the certificates have been uploaded configure the SSL VPN tunnel.

Server:



Edit SSL VPN

ID	0
Enabled	☑
Description	
Mode	● Server ○ Client

Network

Type	Layer2 (Bridged)
Protocol	UDP
Port	1194
Outbound Interface	vlan1720
Pool	☐
Pushed networks	☐
Client-to-Client	☐
Max clients	25
Keepalive	Interval 10 s Restart 60 s
Compression	Disabled
Renegotiate	3600 (s)

Set the Outbound Interface, could also be the Default Gateway.

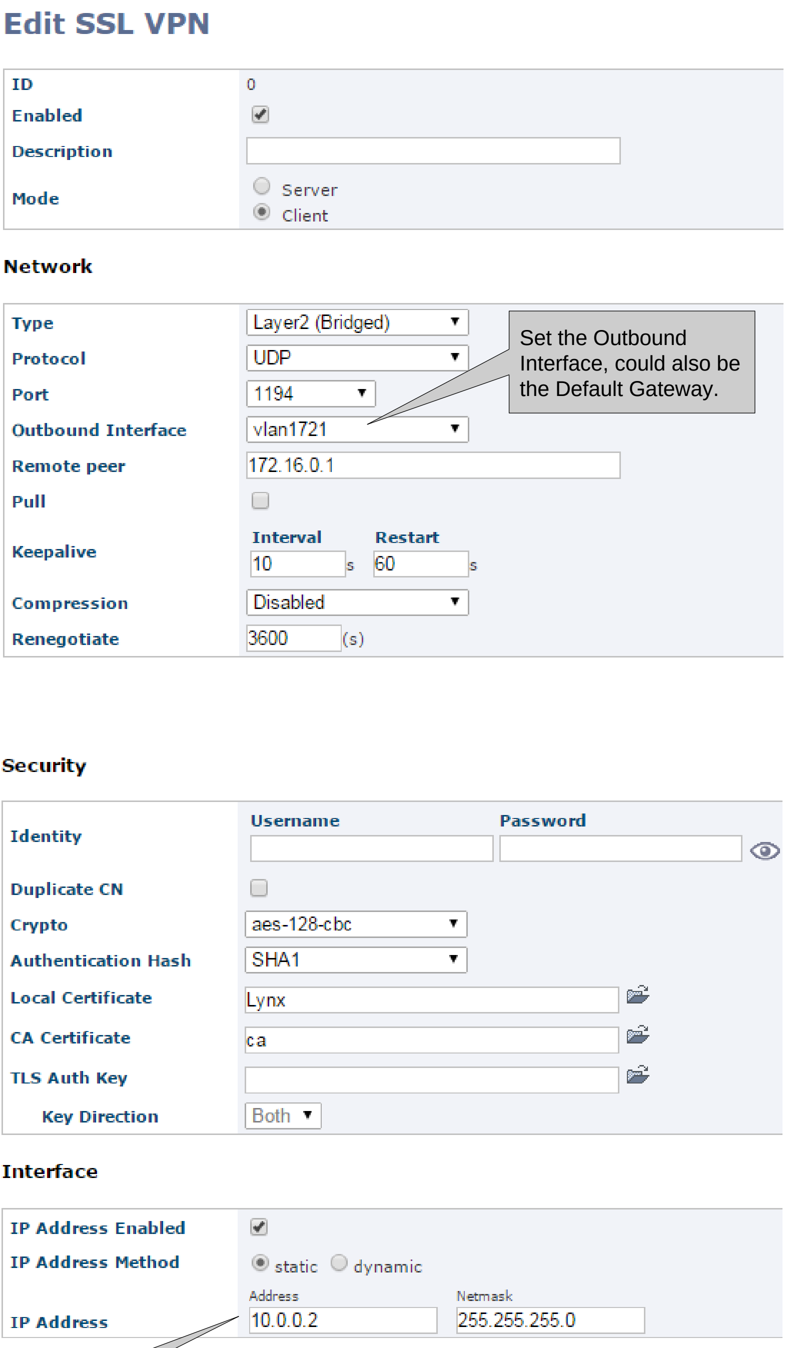
Security

Client AAA	None
Duplicate CN	☐
Crypto	aes-128-cbc
Authentication Hash	SHA1
Local Certificate	server
CA Certificate	ca
TLS Auth Key	
Key Direction	Both

Interface

IP Address Enabled	☑
IP Address Method	● static ○ dynamic
IP Address	Address 10.0.0.1 Netmask 255.255.255.0

Client:



Edit SSL VPN

ID	0
Enabled	☑
Description	
Mode	○ Server ● Client

Network

Type	Layer2 (Bridged)
Protocol	UDP
Port	1194
Outbound Interface	vlan1721
Remote peer	172.16.0.1
Pull	☐
Keepalive	Interval 10 s Restart 60 s
Compression	Disabled
Renegotiate	3600 (s)

Set the Outbound Interface, could also be the Default Gateway.

Security

Identity	Username Password
Duplicate CN	☐
Crypto	aes-128-cbc
Authentication Hash	SHA1
Local Certificate	Lynx
CA Certificate	ca
TLS Auth Key	
Key Direction	Both

Interface

IP Address Enabled	☑
IP Address Method	● static ○ dynamic
IP Address	Address 10.0.0.2 Netmask 255.255.255.0

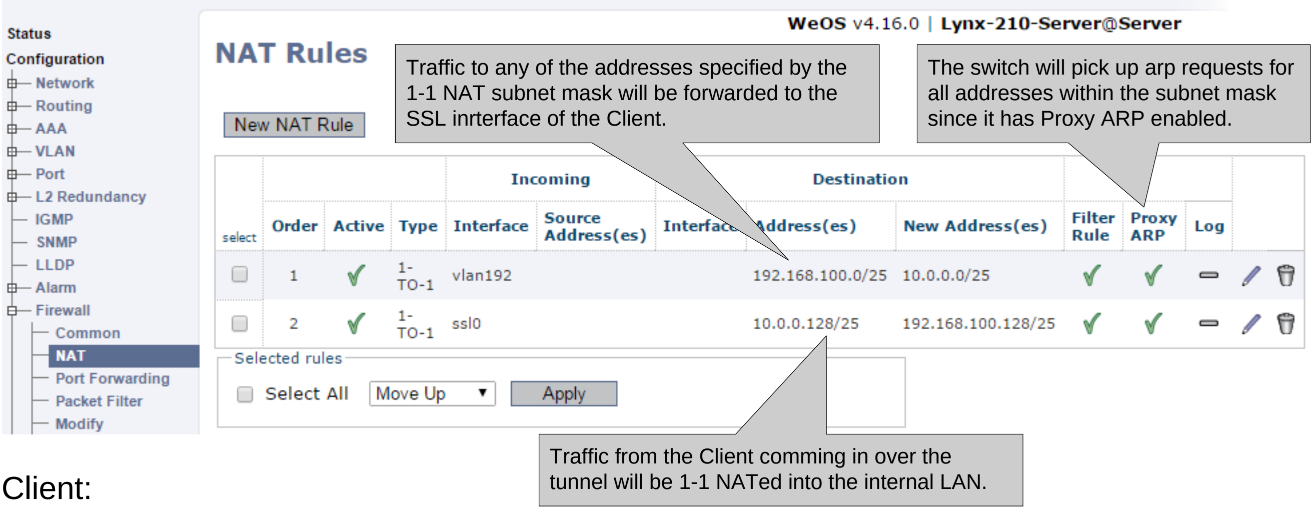
Configure an IP-address for the SSL interface.

Firewall

Finally enable the Firewall and setup the 1-1 NAT rules needed.
Depending on how the IP-address plan of the exsisting network is made the 1-1 NAT rules can be setup in different ways.
The 1-1 NAT addresses can be subnetted again to divide the network into smaller sections which will decrease the amount of 1-1 NAT rules needed. If this is possible depends on how the IP-addresses are divided between the two sides of the tunnel.
If this is not possible, individual 1-1 NAT rules needs to be setup for each unit that shall communicate over the tunnel.

This example show how the 192.168.100.0/24 network has been split in two by using a /25 subnet mask for the 1-1 NAT rules. So IP-addresses up to 192.168.100.126 are on the server side and IP-addresses from 192.168.100.129 are on the client side.

Server:



NAT Rules

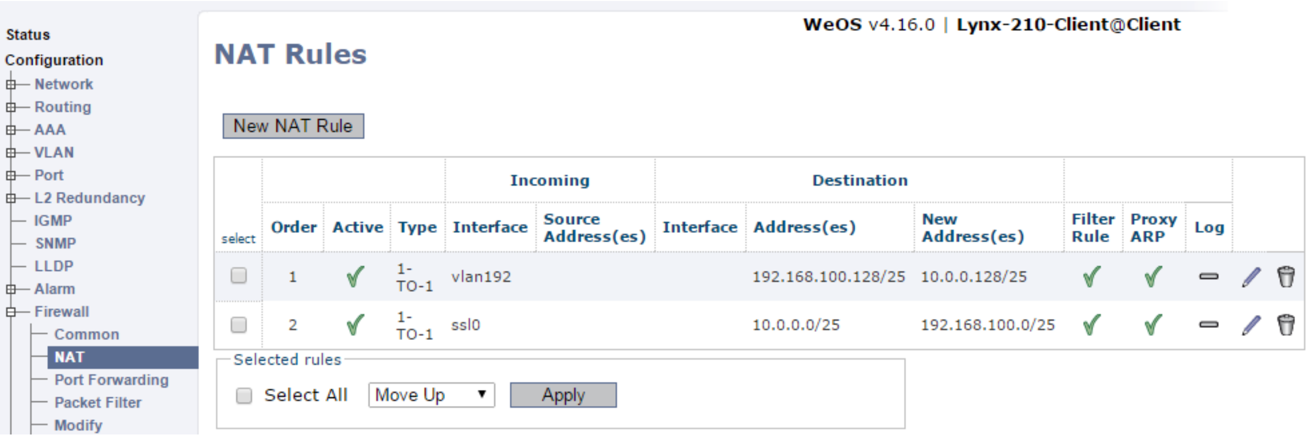
				Incoming		Destination					
select	Order	Active	Type	Interface	Source Address(es)	Interface	Address(es)	New Address(es)	Filter Rule	Proxy ARP	Log
□	1	✓	1-TO-1	vlan192			192.168.100.0/25	10.0.0.0/25	✓	✓	−
□	2	✓	1-TO-1	ssl0			10.0.0.128/25	192.168.100.128/25	✓	✓	−

Traffic to any of the addresses specified by the 1-1 NAT subnet mask will be forwarded to the SSL inrterface of the Client.

The switch will pick up arp requests for all addresses within the subnet mask since it has Proxy ARP enabled.

Traffic from the Client comming in over the tunnel will be 1-1 NATed into the internal LAN.

Client:

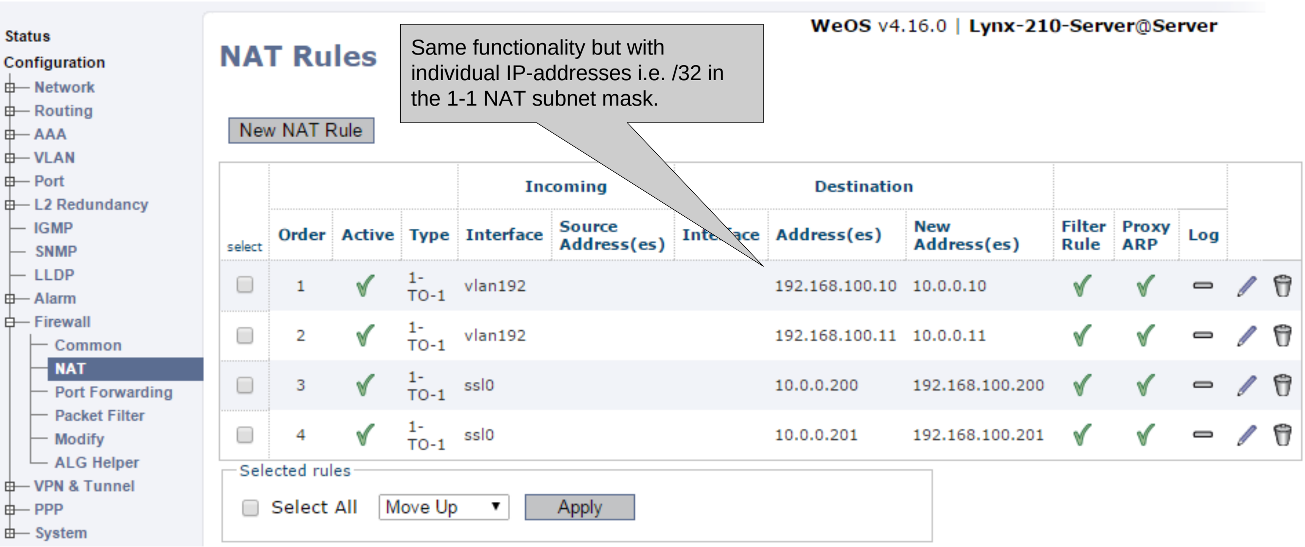


NAT Rules

				Incoming		Destination					
select	Order	Active	Type	Interface	Source Address(es)	Interface	Address(es)	New Address(es)	Filter Rule	Proxy ARP	Log
□	1	✓	1-TO-1	vlan192			192.168.100.128/25	10.0.0.128/25	✓	✓	−
□	2	✓	1-TO-1	ssl0			10.0.0.0/25	192.168.100.0/25	✓	✓	−

This is the example of how individual 1-1 NAT rules are configured.

Server:



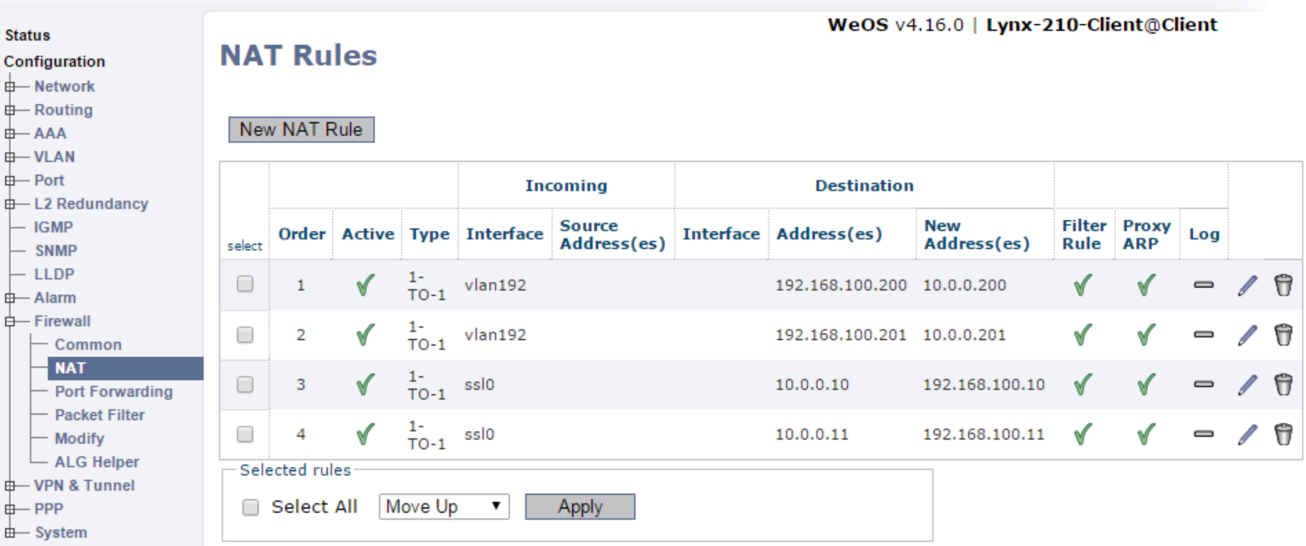
WeOS v4.16.0 | **Lynx-210-Server@Server**

NAT Rules

Same functionality but with individual IP-addresses i.e. /32 in the 1-1 NAT subnet mask.

				Incoming		Destination						
select	Order	Active	Type	Interface	Source Address(es)	Interface	Address(es)	New Address(es)	Filter Rule	Proxy ARP	Log	
□	1	✓	1-TO-1	vlan192			192.168.100.10	10.0.0.10	✓	✓	▬	✎ 🗑
□	2	✓	1-TO-1	vlan192			192.168.100.11	10.0.0.11	✓	✓	▬	✎ 🗑
□	3	✓	1-TO-1	ssl0			10.0.0.200	192.168.100.200	✓	✓	▬	✎ 🗑
□	4	✓	1-TO-1	ssl0			10.0.0.201	192.168.100.201	✓	✓	▬	✎ 🗑

Client:



WeOS v4.16.0 | **Lynx-210-Client@Client**

NAT Rules

				Incoming		Destination						
select	Order	Active	Type	Interface	Source Address(es)	Interface	Address(es)	New Address(es)	Filter Rule	Proxy ARP	Log	
□	1	✓	1-TO-1	vlan192			192.168.100.200	10.0.0.200	✓	✓	▬	✎ 🗑
□	2	✓	1-TO-1	vlan192			192.168.100.201	10.0.0.201	✓	✓	▬	✎ 🗑
□	3	✓	1-TO-1	ssl0			10.0.0.10	192.168.100.10	✓	✓	▬	✎ 🗑
□	4	✓	1-TO-1	ssl0			10.0.0.11	192.168.100.11	✓	✓	▬	✎ 🗑

Now all the neccessary configurations are made for these two parts of the same subnet to be able to communicate over the routed link between them.

Revision history for version 1.0

Revision	Rev by	Revision note	Date
00	ML	First version	150319
01			
02			
03			
04			
05			
06			
07			

HEAD OFFICE

Sweden
Westermo
SE-640 40 Stora Sundby
Tel: +46 (0)16 42 80 00
Fax: +46 (0)16 42 80 01
info@westermo.se
www.westermo.com

Sales Units

Westermo Data Communications

China
sales.cn@westermo.com
www.cn.westermo.com

France
infos@westermo.fr
www.westermo.fr

Germany
info@westermo.de
www.westermo.de

North America
info@westermo.com
www.westermo.com

Singapore
sales@westermo.com.sg
www.westermo.com

Sweden
info.sverige@westermo.se
www.westermo.se

United Kingdom
sales@westermo.co.uk
www.westermo.co.uk

Other Offices

For complete contact information, please visit our website at www.westermo.com/contact or scan the QR code with your mobile phone.