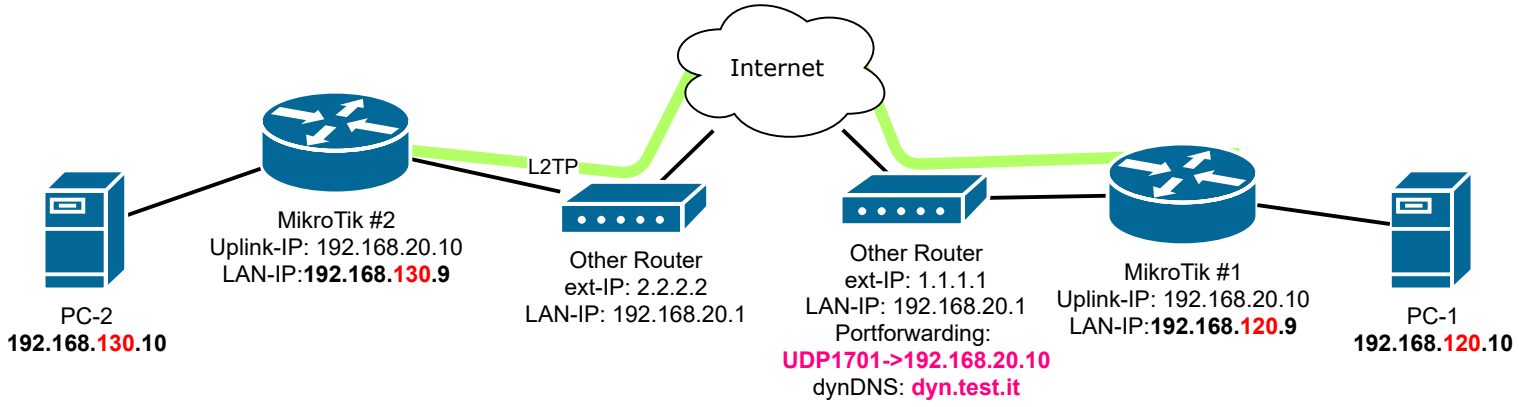
Site-2-Site VPN with NATed-Routers



Step 1: L2TP-Tunnel

 # add PPP-Interface
```
/interface l2tp-client
add connect-to=dyn.test.it disabled=no \
  name=l2tp-SITE1 password=pass123456 \
  user=User1
```

 # add Route
```
/ip route add distance=1 \
  dst-address=192.168.120.0/24 \
  gateway=172.16.2.1
```

 # add PPP-User
```
/ppp profile
add change-tcp-mss=yes name=l2tp-enc \
  use-encryption=required
/ppp secret
  add local-address=172.16.2.1 \
  password=pass123456 profile=l2tp-enc \
  remote-address=172.16.2.2 name=User1
```

 # add Route
```
/ip route add distance=1 \
  dst-address=192.168.130.0/24 \
  gateway=172.16.2.2
```

At this point everything ist fully functional except the **weak encryption used by L2TP**.
Thus an IPSec-Tunnel should be established inside this L2TP-Tunnel

Step 2: Establish IPSec-Tunnel inside L2TP-Tunnel

```
/ip ipsec profile
add dh-group=modp2048 enc-algorithm=aes-256 \
  hash-algorithm=sha256 name=enc \
  nat-traversal=no proposal-check=strict
/ip ipsec proposal
add auth-algorithms=sha256 name=enc \
 enc-algorithms=aes-128-gcm pfs-group=modp2048
/ip ipsec peer
add address=172.16.2.1/32 name=peer#1 \
  local-address=172.16.2.2 profile=enc

/ip ipsec identity
add peer=peer#1 secret=ips-pass-123456
/ip ipsec policy
add dst-address=192.168.120.0/24 peer=peer#1 \
  src-address=192.168.130.0/24 proposal=enc \
  tunnel=yes
```

```
/ip ipsec profile
add dh-group=modp2048 enc-algorithm=aes-256 \
  hash-algorithm=sha256 name=enc \
  nat-traversal=no proposal-check=strict
/ip ipsec proposal
add auth-algorithms=sha256 name=enc \
  enc-algorithms=aes-128-gcm pfs-group=modp2048
/ip ipsec peer
add address=172.16.2.2/32 name=peer#1 \
  local-address=172.16.2.1 profile=enc \
  passive=yes
/ip ipsec identity
add peer=peer#1 secret=ips-pass-123456
/ip ipsec policy
add dst-address=192.168.130.0/24 peer=peer#1 \
  src-address=192.168.120.0/24 proposal=enc \
  tunnel=yes
```

DISABLE Routes (from Step 1 are disabled, because the IPSec Policies shoud do the routing

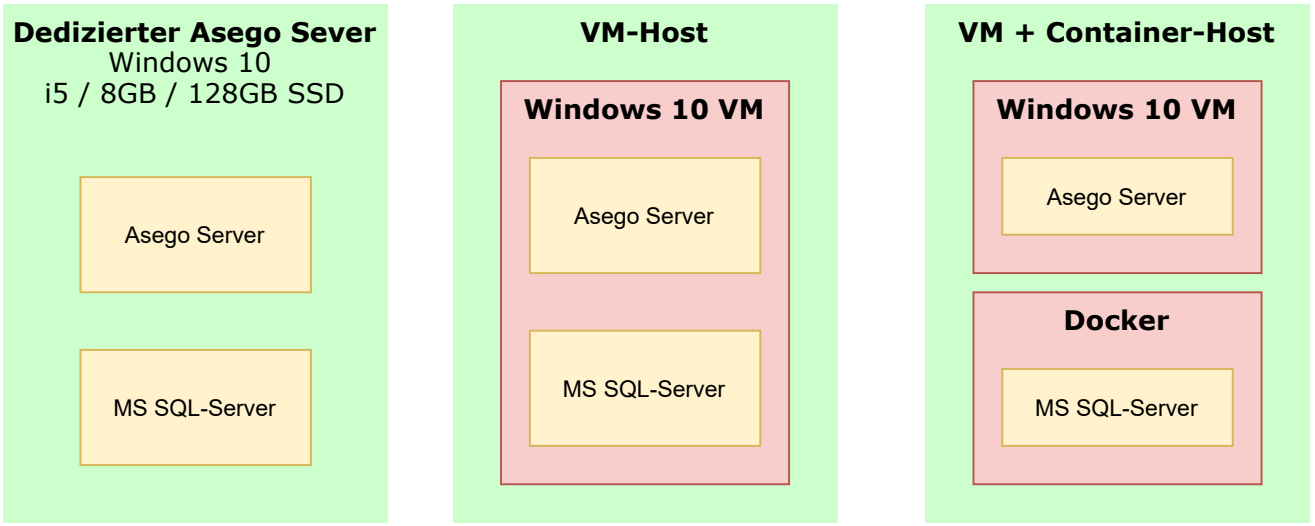
Now the Connection between **192.168.120.0**/24 and **192.168.130.0**/24 should be operational through the IPSec-Tunnel.
But ist is not: CIFS Browsing is not possible anymore, Ping still works. (Maybe MTU-Problem)

To analyze it I did the following
1. Set up everything as above.
2. Disable IPSect Peers and Policies on both sides
3. Start three continous Ping tasks
   - from Router1 to PC2: 192.168.120.9: PING 192.168.130.10 (Interface: Bridge/IF, where 192.168.120.9 is connected)
   - from Router2 to PC1: 192.168.130.9: PING 192.168.120.10 (Interface: Bridge/IF, where 192.168.130.9 is connected)
   - from PC2 to PC1: 192.168.130.10: PING 192.168.120.10
   - Browse CIFS-Ressource on PC1: net use z: \\192.168.120.10\folder1
   Result:
   - Everything looks fine - All three PING-Tasks getting Response and I can browse through the files.
4. Enable IPSec-Peer on both sides
   Result:
   - Got active Peer, Initiator is Mikrotik#2, responder Mikrotik#1 (which has set passive=yes)
5. Enable IPSec-Policy on both sides
   Result:
   - some Pings got lost, after some seconds everything looks fine
   - Two active Security-Associations on both Sides

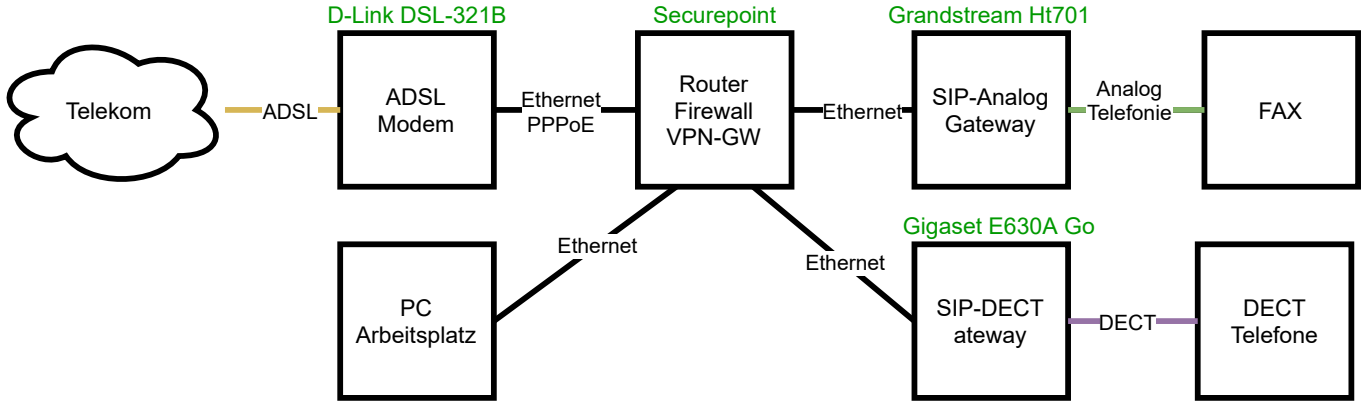
At this Point CIFS-Browsing is not possible anymore.

The only Idea i have is the MTU:
When i check the MTU size from Client (Mikrotik#2) to Server (Mikrotik#1) using:
/ping 192.168.120.9 src-address=192.168.130.9 do-not-fragment count=1 size=1450
I get a mazimum Size of **MTU: 1450**
But on the way back from Server (Mikrotik#1) to Client (Mikrotik#1) using:
/ping 192.168.130.9 src-address=192.168.120.9 do-not-fragment count=1 size=1390
I get **MTU: 1390** (Maybe due to the DST-Nat?)

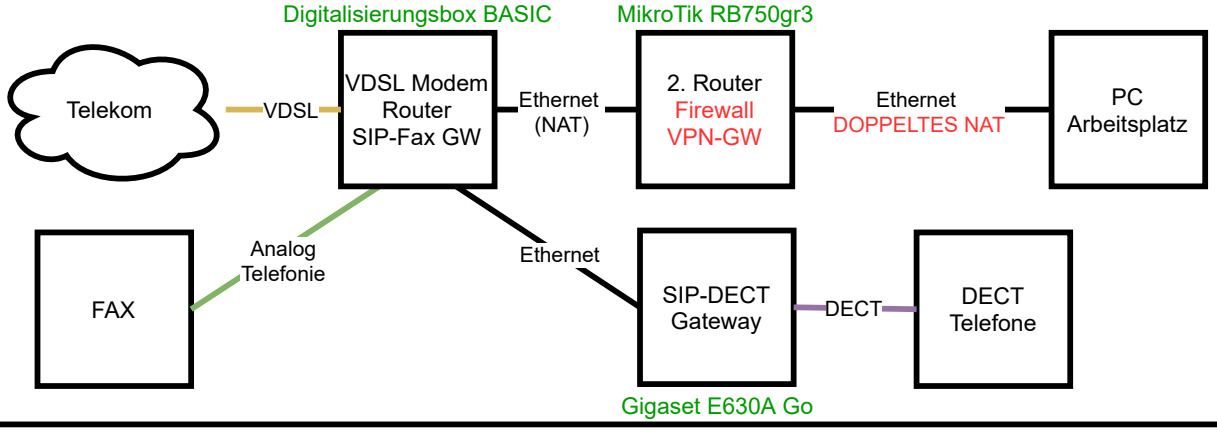
My Question now:
Where can/must I set the MTU to 1390?
Or is ther another option to configure a site-2-site VPN?


Dedizierter Asego Sever
Windows 10
i5 / 8GB / 128GB SSD
Asego Server
MS SQL-Server
VM-Host
Windows 10 VM
Asego Server
MS SQL-Server
VM + Container-Host
Windows 10 VM
Asego Server
Docker
MS SQL-Server

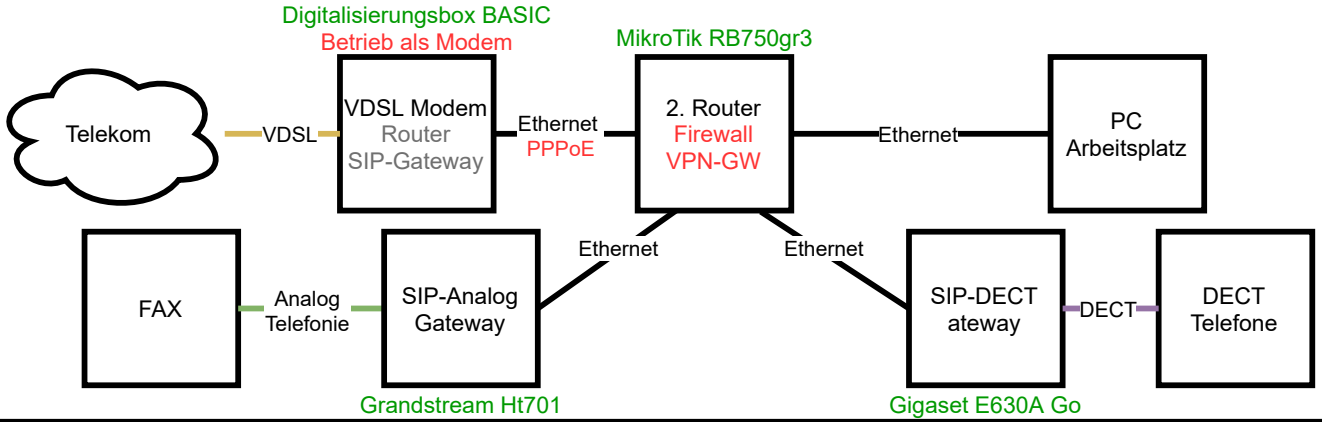
Aktueller Stand - VDSL so nicht möglich



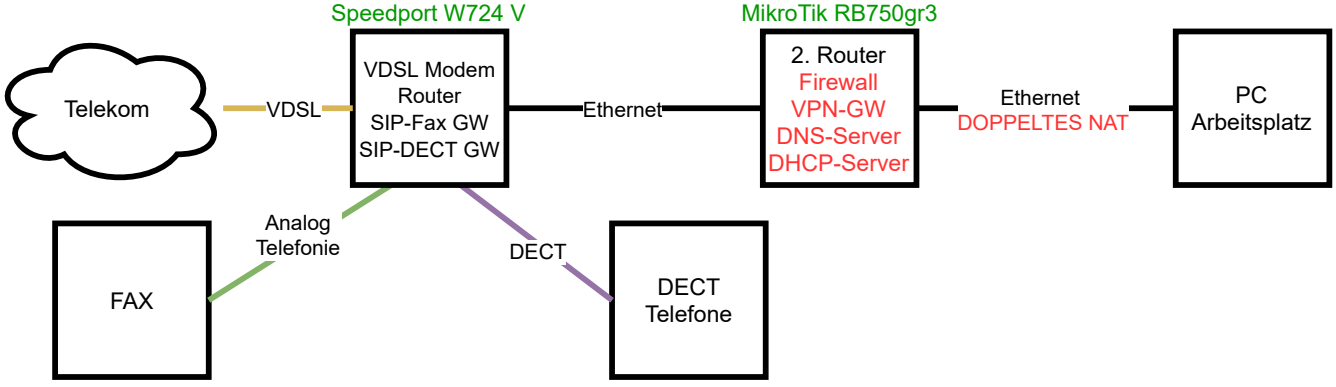
Alternative 1: Digitalisierungsbox Basic als Router und Sip-Fax Gateway

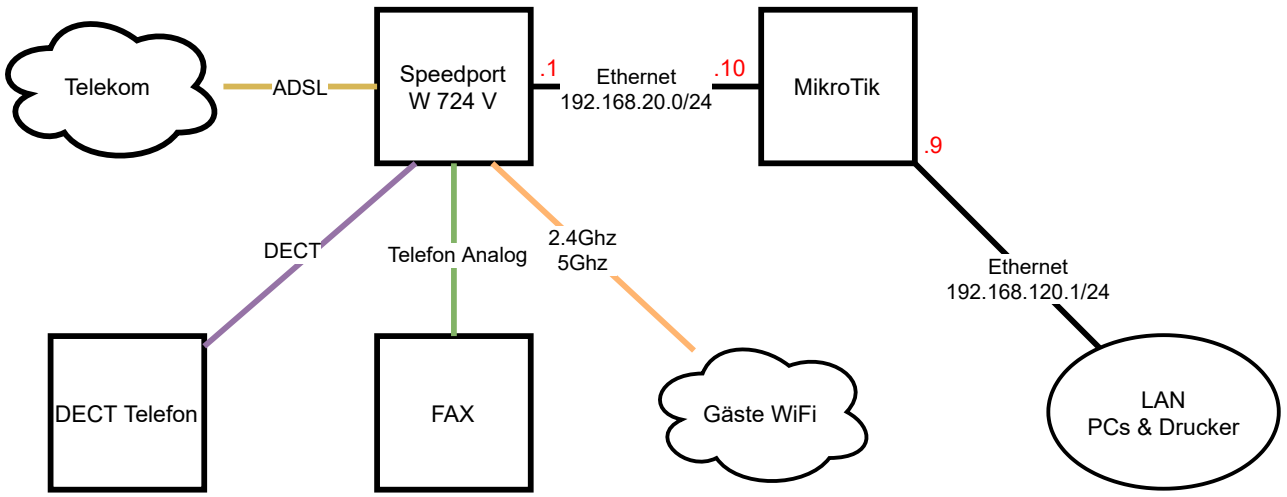


Alternative 2: Digitalisierungsbox Basic im Modembetrieb (Siehe Anleitung Seite 16 oben)



Speedport 724: DSL-Modem + WiFi-Gastnetz + Fax-Gateway + DECT-Gateway
Mikrotik Router: VPN-Gateway, DNS-Server, DHCP-Server





Speedport 724: DSL-Modem + WiFi-Gastnetz + Fax-Gateway + DECT-Gateway
Mikrotik Router: VPN-Gateway, DNS-Server, DHCP-Server