Know-How

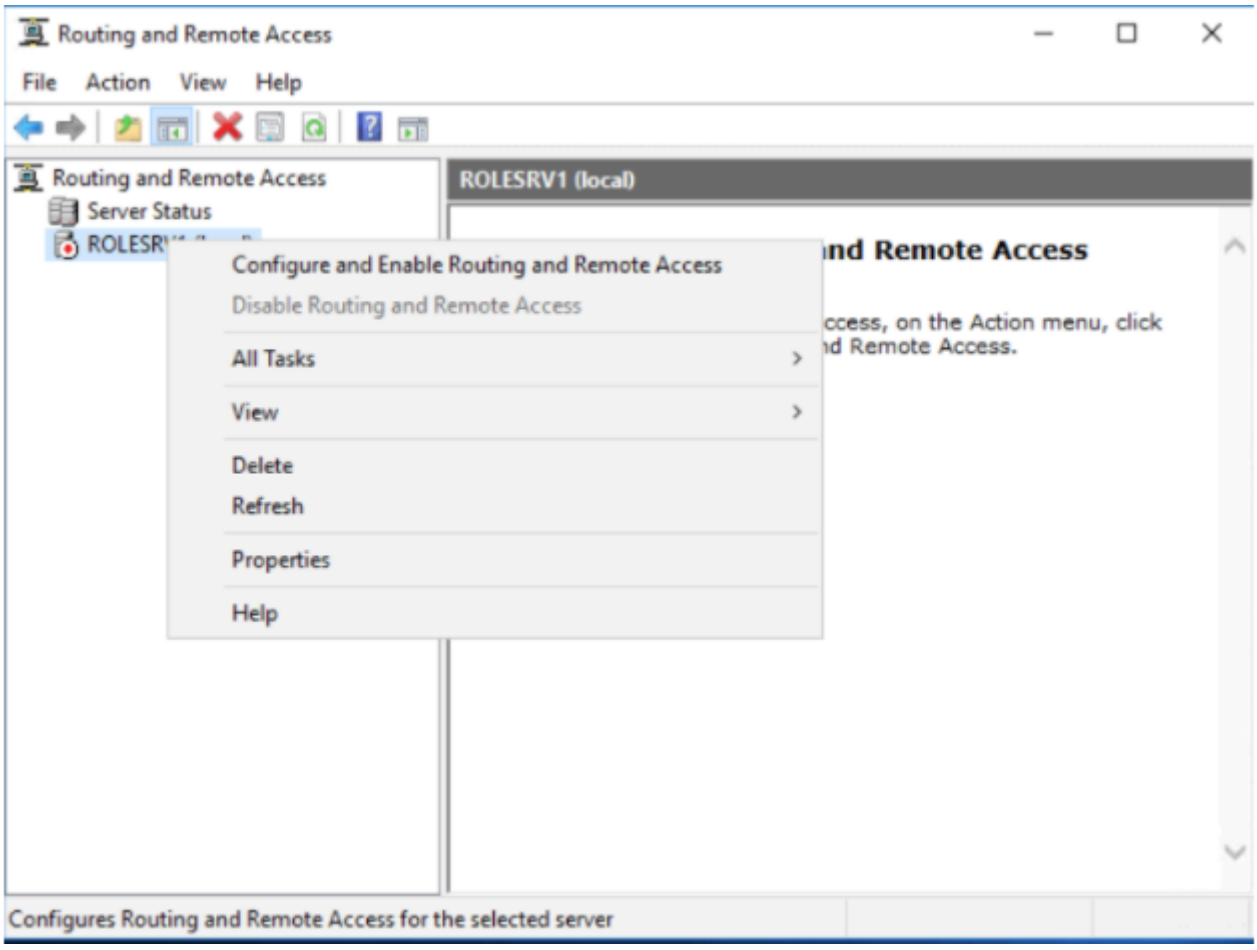
- Open-VPN mit RAS Windows Server
- VPS als Gateway zum Hosting / übergehen DynDNS

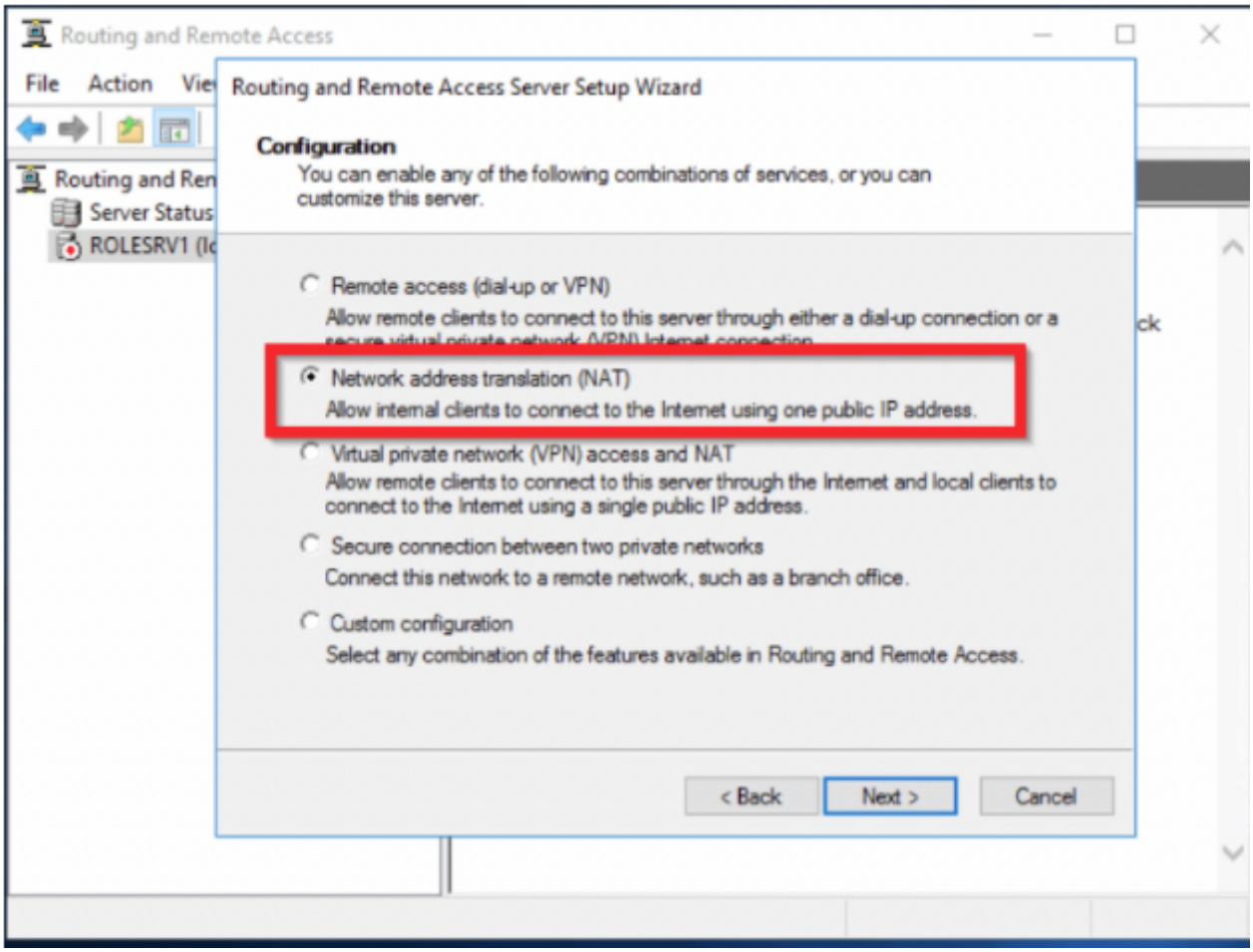
Open-VPN mit RAS Windows Server

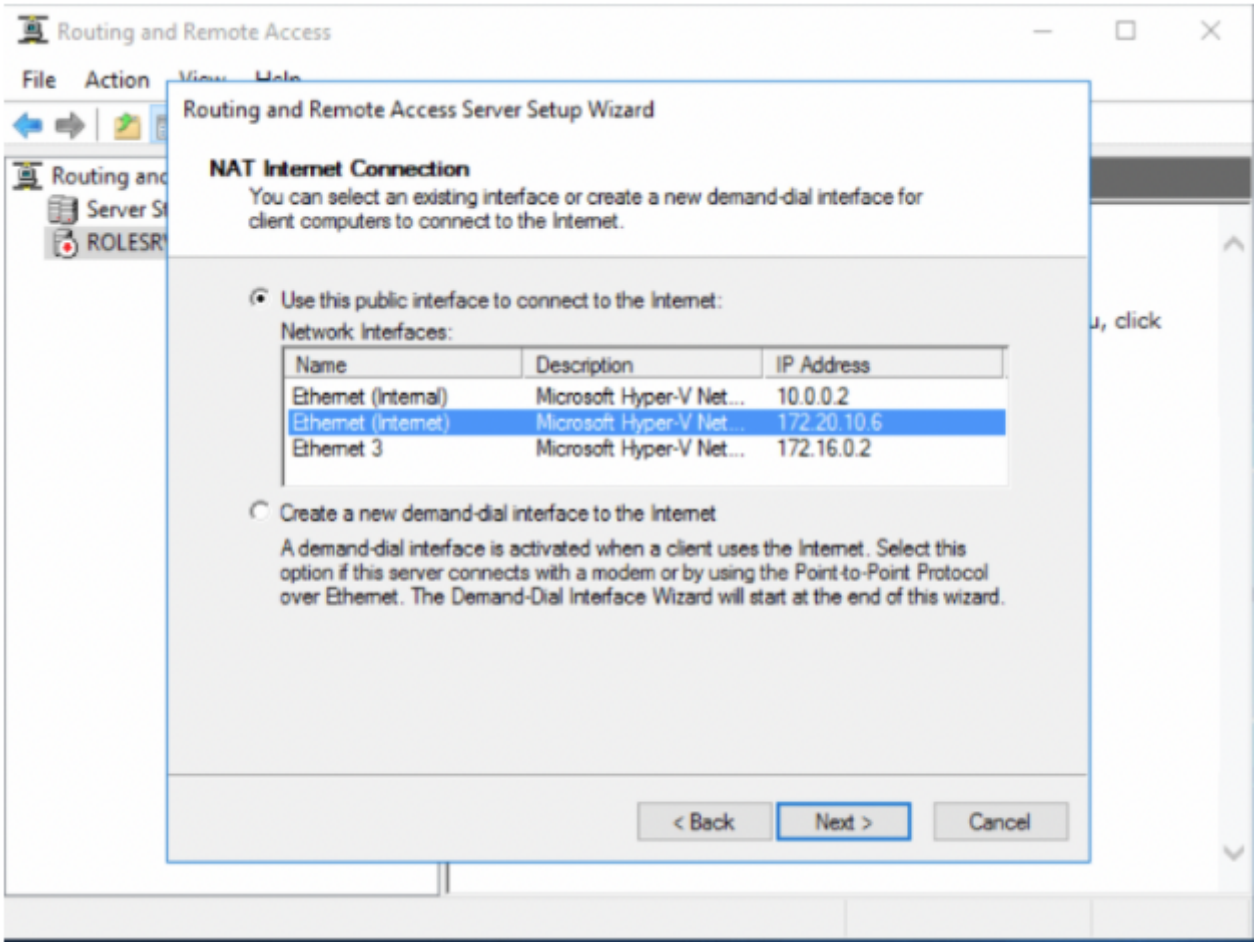
> Netzwerkadapter und TAP-Adapter bridgen führt zu einer Neuvergabe von lokalen IP-Adressen!!!! Erreichbarkeit geht dadurch verloren!

Damit die Option "redirect gateway def1" richtig funktioniert, und der Traffic über die Ethernetschnittstelle geht, muss im Server Manager "Remote Acess" installiert werden.

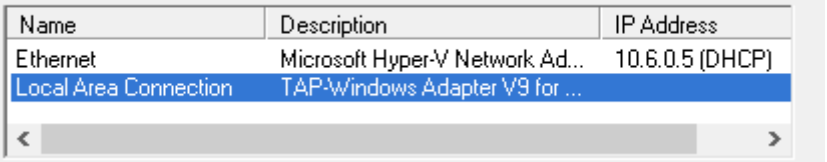
Konfiguration erfolgt folgendermaßen:




Routing and Remote Access
File Action Vie
Routing and Ren
Server Status
ROLESRV1 (lo
Routing and Remote Access Server Setup Wizard
Configuration
You can enable any of the following combinations of services, or you can customize this server.
Remote access (dial-up or VPN)
Allow remote clients to connect to this server through either a dial-up connection or a secure virtual private network (VPN) Internet connection.
Network address translation (NAT)
Allow internal clients to connect to the Internet using one public IP address.
Virtual private network (VPN) access and NAT
Allow remote clients to connect to this server through the Internet and local clients to connect to the Internet using a single public IP address.
Secure connection between two private networks
Connect this network to a remote network, such as a branch office.
Custom configuration
Select any combination of the features available in Routing and Remote Access.
< Back
Next >
Cancel


Routing and Remote Access
File Action View Help
Routing and
Server St
ROLESR
Routing and Remote Access Server Setup Wizard
NAT Internet Connection
You can select an existing interface or create a new demand-dial interface for client computers to connect to the Internet.
Use this public interface to connect to the Internet:
Network Interfaces:
Name
Description
IP Address
Ethernet (Internal)
Microsoft Hyper-V Net...
10.0.0.2
Ethernet (Internet)
Microsoft Hyper-V Net...
172.20.10.6
Ethernet 3
Microsoft Hyper-V Net...
172.16.0.2
Create a new demand-dial interface to the Internet
A demand-dial interface is activated when a client uses the Internet. Select this option if this server connects with a modem or by using the Point-to-Point Protocol over Ethernet. The Demand-Dial Interface Wizard will start at the end of this wizard.
< Back
Next >
Cancel

Network Interfaces:



Name	Description	IP Address
Ethernet	Microsoft Hyper-V Network Ad...	10.6.0.5 (DHCP)
Local Area Connection	TAP-Windows Adapter V9 for ...	

VPS als Gateway zum Hosting / übergehen DynDNS

VPN-Server aufsetzen

Server auf den neusten Stand bringen

```
sudo apt update && sudo apt upgrade -y
```

Open-VPN und easy-rsa installieren

```
sudo apt install openvpn easy-rsa -y
```

Easy-RSA Umgebung einrichten

```
make-cadir ~/openvpn-ca
cd ~/openvpn-ca
./easyrsa clean-all
./easyrsa build-ca
```

Server-Zerti erstellen

```
./easyrsa gen-req server nopass
./easyrsa sign-req server server
```

DH und TLS-Auth

```
./easyrsa gen-dh
openvpn --genkey --secret ta.key
```

Client-Zerti

```
./easyrsa gen-req client nopass
./easyrsa sign-req client client
```

Alles kopieren und OpenVPN Config erstellen in /etc/OpenVPN

```
port 1194
proto udp
dev tun

ca ca.crt
cert server.crt
key server.key
dh dh.pem

tls-auth ta.key 0

server 10.8.0.0 255.255.255.0
ifconfig-pool-persist ipp.txt

push "redirect-gateway def1 bypass-dhcp"
push "dhcp-option DNS 1.1.1.1"
push "dhcp-option DNS 8.8.8.8"

keepalive 10 120
cipher AES-256-CBC
user nobody
group nogroup
persist-key
persist-tun
status openvpn-status.log
log-append /var/log/openvpn.log
verb 3
explicit-exit-notify 1
```

Starten und in systemctl aktivieren

```
sudo systemctl enable openvpn@server
sudo systemctl start openvpn@server
sudo systemctl status openvpn@server
```

Firewall und IP-Forwarding

> Firewall auf Hosterseite nicht vergessen!

```
# IP-Forwarding aktivieren
echo 1 > /proc/sys/net/ipv4/ip_forward
sudo sed -i 's/#net.ipv4.ip_forward=1/net.ipv4.ip_forward=1/' /etc/sysctl.conf
sudo sysctl -p
```

```
# NAT über iptables
iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -o eth0 -j MASQUERADE
sudo apt install iptables-persistent -y
sudo netfilter-persistent save
```

Client-Konfiguration

OpenVPN-Config für den Client:

```
client
dev tun
proto udp
remote YOUR.SERVER.IP 1194
resolv-retry infinite
nobind
persist-key
persist-tun
remote-cert-tls server
cipher AES-256-CBC
verb 3
key-direction 1

ca ca.crt
cert client1.crt
key client1.key
tls-auth ta.key 1
```

Befehl zum Kopieren über SSH

```
pscp user@vps-ip:/root/openvpn-ca/ta.key C:\Users\DeinBenutzer\Downloads\
pscp user@vps-ip:/root/openvpn-ca/pki/ca.crt C:\Users\DeinBenutzer\Downloads\
pscp user@vps-ip:/root/openvpn-ca/pki/issued/client.crt C:\Users\DeinBenutzer\Downloads\
pscp user@vps-ip:/root/openvpn-ca/pki/private/client.key C:\Users\DeinBenutzer\Downloads\
```

IP-Tables-Regeln setzen

```
# Weiterleitung von Port 80 an 10.8.0.5:80
sudo iptables -t nat -A PREROUTING -p tcp -d 85.215.196.99 --dport 80 -j DNAT --to-destination 10.8.0.5:80

# Erlauben, dass die Pakete auch rausgehen dürfen
sudo iptables -t nat -A POSTROUTING -j MASQUERADE
sudo netfilter-persistent save
```