

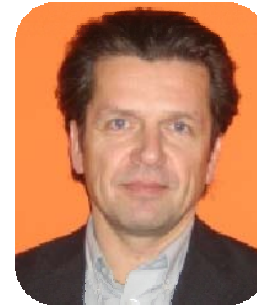
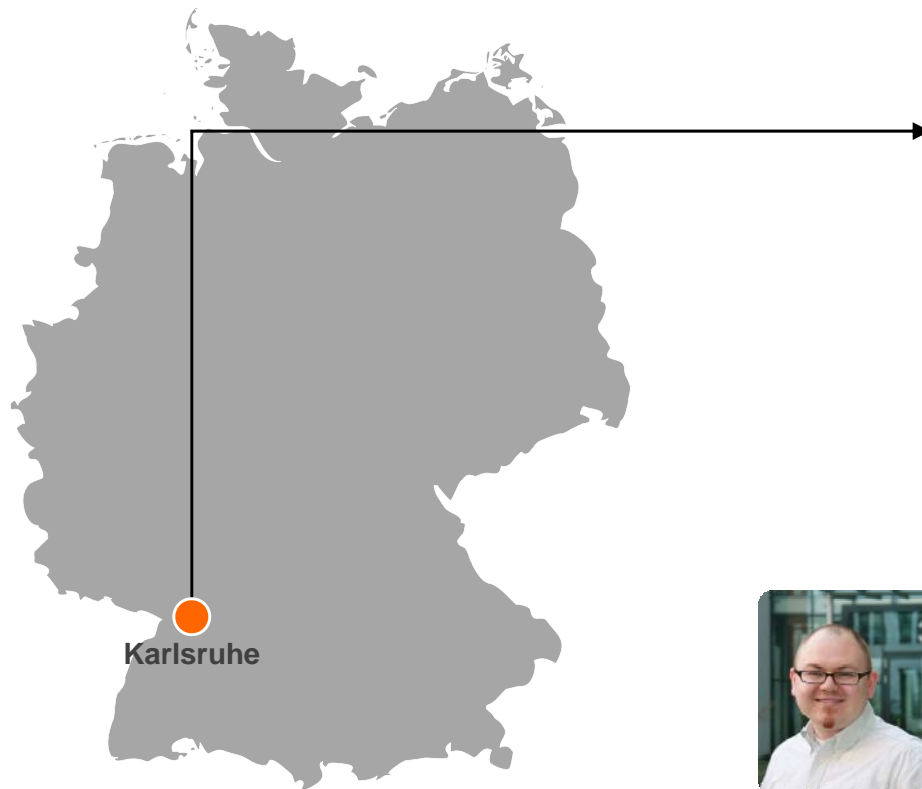


Simplifying Email, Web & Network Protection

## **Astaro Security Gateway Tips & Tricks for Customers**

# **VPN**

# Today's Webinar Team



**Lutz Linzenmeier**  
Head of Pre-Sales EMEA  
Astaro AG



**Christian Louis**  
Pre-Sales Engineer EMEA  
Astaro AG



**Nils Schiele**  
Senior Support Engineer  
Astaro AG

## Site-to-Site VPN

- ▶ **Best practise** (PSK/RSA/Certificates, Certificate management)
- ▶ **Topologies** (Site-to-Center, Hub-and-Spoke, Fully Meshed)
- ▶ **SSL-VPN – how to configure properly**
- ▶ **NAT in a VPN tunnel**

## Remote Access VPN

- ▶ **SSL: How to redirect all traffic into the tunnel**
- ▶ **SSL: Fix IP addresses for remote access user**
- ▶ **IPSec: CA-DN-Mode**
- ▶ **IPsec: PSK and XAUTH**
- ▶ **Advantages and disadvantages: SSL-VPN vs. IPsec-VPN**

# Connection establishment IPsec

```
13:15:56.226802 IP vpn2.isakmp > vpn1.isakmp: isakmp: phase 1 I ident
13:15:56.227960 IP vpn1.isakmp > vpn2.isakmp: isakmp: phase 1 R ident
13:15:56.228009 IP vpn1.isakmp > vpn2.isakmp: isakmp: phase 1 I ident
13:15:56.237995 IP vpn2.isakmp > vpn1.isakmp: isakmp: phase 1 I ident
13:15:56.241201 IP vpn2.isakmp > vpn1.isakmp: isakmp: phase 1 R ident
13:15:56.247543 IP vpn1.isakmp > vpn2.isakmp: isakmp: phase 1 R ident
13:15:56.251959 IP vpn1.isakmp > vpn2.isakmp: isakmp: phase 1 I ident
13:15:56.252549 IP vpn2.isakmp > vpn1.isakmp: isakmp: phase 1 I ident [E]
```

```
2009:12:04-13:15:56 vpn1 pluto[7155]: packet from 172.20.1.82:500: ignoring Vendor ID payload [strongSwan 4.2.3]
2009:12:04-13:15:56 vpn1 pluto[7155]: packet from 172.20.1.82:500: ignoring Vendor ID payload [Cisco-Unity]
2009:12:04-13:15:56 vpn1 pluto[7155]: packet from 172.20.1.82:500: received Vendor ID payload [XAUTH]
2009:12:04-13:15:56 vpn1 pluto[7155]: packet from 172.20.1.82:500: received Vendor ID payload [Dead Peer Detection]
2009:12:04-13:15:56 vpn1 pluto[7155]: packet from 172.20.1.82:500: received Vendor ID payload [RFC 3947]
2009:12:04-13:15:56 vpn1 pluto[7155]: packet from 172.20.1.82:500: ignoring Vendor ID payload [draft-ietf-ipsec-nat-t-ike-03]
2009:12:04-13:15:56 vpn1 pluto[7155]: packet from 172.20.1.82:500: ignoring Vendor ID payload [draft-ietf-ipsec-nat-t-ike-02]
2009:12:04-13:15:56 vpn1 pluto[7155]: packet from 172.20.1.82:500: ignoring Vendor ID payload [draft-ietf-ipsec-nat-t-ike-02_n]
2009:12:04-13:15:56 vpn1 pluto[7155]: packet from 172.20.1.82:500: ignoring Vendor ID payload [draft-ietf-ipsec-nat-t-ike-00]
2009:12:04-13:15:56 vpn1 pluto[7155]: "S_REF_cSoDpMaWpB_0" #2: responding to Main Mode
2009:12:04-13:15:56 vpn1 pluto[7155]: "S_REF_cSoDpMaWpB_0" #2: NAT-Traversal: Result using RFC 3947: no NAT detected
2009:12:04-13:15:56 vpn1 pluto[7155]: "S_REF_cSoDpMaWpB_0" #1: ignoring Vendor ID payload [strongSwan 4.2.3]
2009:12:04-13:15:56 vpn1 pluto[7155]: "S_REF_cSoDpMaWpB_0" #1: ignoring Vendor ID payload [Cisco-Unity]
2009:12:04-13:15:56 vpn1 pluto[7155]: "S_REF_cSoDpMaWpB_0" #1: received Vendor ID payload [XAUTH]
2009:12:04-13:15:56 vpn1 pluto[7155]: "S_REF_cSoDpMaWpB_0" #1: received Vendor ID payload [Dead Peer Detection]
2009:12:04-13:15:56 vpn1 pluto[7155]: "S_REF_cSoDpMaWpB_0" #1: received Vendor ID payload [RFC 3947]
2009:12:04-13:15:56 vpn1 pluto[7155]: "S_REF_cSoDpMaWpB_0" #1: enabling possible NAT-traversal with method 3
2009:12:04-13:15:56 vpn1 pluto[7155]: "S_REF_cSoDpMaWpB_0" #2: Peer ID is ID_IPV4_ADDR: '172.20.1.82'
2009:12:04-13:15:56 vpn1 pluto[7155]: "S_REF_cSoDpMaWpB_0" #2: sent MR3, ISAKMP SA established
2009:12:04-13:15:56 vpn1 pluto[7155]: "S_REF_cSoDpMaWpB_0" #1: NAT-Traversal: Result using RFC 3947: no NAT detected
2009:12:04-13:15:56 vpn1 pluto[7155]: "S_REF_cSoDpMaWpB_0" #3: responding to Quick Mode
2009:12:04-13:15:56 vpn1 pluto[7155]: "S_REF_cSoDpMaWpB_0" #1: Peer ID is ID_IPV4_ADDR: '172.20.1.82'
2009:12:04-13:15:56 vpn1 pluto[7155]: "S_REF_cSoDpMaWpB_0" #1: ISAKMP SA established
2009:12:04-13:15:56 vpn1 pluto[7155]: "S_REF_cSoDpMaWpB_0" #4: initiating Quick Mode PSK+ENCRYPT+TUNNEL+UP {using isakmp#1}
2009:12:04-13:15:56 vpn1 pluto[7155]: "S_REF_cSoDpMaWpB_0" #3: Dead Peer Detection (RFC 3706) enabled
2009:12:04-13:15:56 vpn1 pluto[7155]: "S_REF_cSoDpMaWpB_0" #3: IPsec SA established {ESP=>0x8f4a9c39 <0x5174092d DPD}
2009:12:04-13:15:56 vpn1 pluto[7155]: "S_REF_cSoDpMaWpB_0" #4: Dead Peer Detection (RFC 3706) enabled
2009:12:04-13:15:56 vpn1 pluto[7155]: "S_REF_cSoDpMaWpB_0" #4: sent QI2, IPsec SA established {ESP=>0x8f4a9c3a <0x5174092e DPD}
```

# Connection establishment SSL



```
2009:12:04-13:28:24 vpn1 openvpn[7533]: Re-using SSL/TLS context
2009:12:04-13:28:24 vpn1 openvpn[7533]: LZO compression initialized
2009:12:04-13:28:24 vpn1 openvpn[7533]: Control Channel MTU parms [ L:1556 D:140 EF:40 FR:0 ET:0 FI:0 ]
2009:12:04-13:30:47.849658 IP vpn1.https > vpn2.53396: P 969:1085(116) ack 281 win 5792 <nop,nop,timestamp 892681 1165669>
2009:12:04-13:30:47.850117 IP vpn2.53396 > vpn1.https: P 281:305(24) ack 1085 win 8576 <nop,nop,timestamp 1165669 892681>
2009:12:04-13:30:47.850222 IP vpn1.https > vpn2.53396: P 1085:1201(116) ack 305 win 5792 <nop,nop,timestamp 892681 1165669>
2009:12:04-13:30:47.850607 IP vpn2.53396 > vpn1.https: P 305:333(28) ack 1201 win 8576 <nop,nop,timestamp 1165670 892681>
2009:12:04-13:30:47.850723 IP vpn1.https > vpn2.53396: P 1201:1317(116) ack 333 win 5792 <nop,nop,timestamp 892681 1165670>
2009:12:04-13:30:47.851354 IP vpn2.53396 > vpn1.https: P 333:357(24) ack 1317 win 8576 <nop,nop,timestamp 1165670 892681>
2009:12:04-13:30:47.851510 IP vpn1.https > vpn2.53396: P 1317:1549(232) ack 357 win 5792 <nop,nop,timestamp 892682 1165670>
2009:12:04-13:30:47.851796 IP vpn2.53396 > vpn1.https: P 357:381(24) ack 1549 win 9648 <nop,nop,timestamp 1165670 892682>
=ehaag@asta 13:30:47.851898 IP vpn1.https > vpn2.53396: P 1549:1665(116) ack 381 win 5792 <nop,nop,timestamp 892682 1165670>
2009:12:04-13:30:47.852463 IP vpn2.53396 > vpn1.https: P 381:405(24) ack 1665 win 9648 <nop,nop,timestamp 1165670 892682>
2009:12:04-13:30:47.852565 IP vpn1.https > vpn2.53396: P 1665:1781(116) ack 405 win 5792 <nop,nop,timestamp 892682 1165670>
2009:12:04-13:30:47.852919 IP vpn2.53396 > vpn1.https: P 405:433(28) ack 1781 win 9648 <nop,nop,timestamp 1165670 892682>
2009:12:04-13:30:47.853067 IP vpn1.https > vpn2.53396: P 1781:1897(116) ack 433 win 5792 <nop,nop,timestamp 892682 1165670>
2009:12:04-13:30:47.853438 IP vpn2.53396 > vpn1.https: P 433:457(24) ack 1897 win 9648 <nop,nop,timestamp 1165670 892682>
2009:12:04-13:30:47.853550 IP vpn1.https > vpn2.53396: P 1897:2129(232) ack 457 win 5792 <nop,nop,timestamp 892682 1165670>
2009:12:04-13:30:47.854001 IP vpn2.53396 > vpn1.https: P 457:481(24) ack 2129 win 10720 <nop,nop,timestamp 1165670 892682>
2009:12:04-13:30:47.854112 IP vpn1.https > vpn2.53396: P 2129:2245(116) ack 481 win 5792 <nop,nop,timestamp 892682 1165670>
2009:12:04-13:30:47.856808 IP vpn2.53396 > vpn1.https: P 481:505(24) ack 2245 win 10720 <nop,nop,timestamp 1165671 892682>
2009:12:04-13:30:47.857597 IP vpn1.https > vpn2.53396: P 2245:2361(116) ack 505 win 5792 <nop,nop,timestamp 892683 1165671>
2009:12:04-13:30:47.857627 IP vpn2.53396 > vpn1.https: P 505:533(28) ack 2361 win 10720 <nop,nop,timestamp 1165671 892683>
2009:12:04-13:30:47.858227 IP vpn1.https > vpn2.53396: P 2361:2477(116) ack 533 win 5792 <nop,nop,timestamp 892683 1165671>
2009:12:04-13:30:47.858250 IP vpn2.53396 > vpn1.https: P 533:557(24) ack 2477 win 10720 <nop,nop,timestamp 1165671 892683>
2009:12:04-13:30:47.858976 IP vpn1.https > vpn2.53396: P 2477:2556(79) ack 557 win 5792 <nop,nop,timestamp 892683 1165671>
2009:12:04-13:30:47.859005 IP vpn2.53396 > vpn1.https: P 557:581(24) ack 2556 win 10720 <nop,nop,timestamp 1165672 892683>
2009:12:04-13:30:47.896356 IP vpn1.https > vpn2.53396: . ack 581 win 5792 <nop,nop,timestamp 892693 1165672>
2009:12:04-13:30:47.896404 IP vpn2.53396 > vpn1.https: P 581:1057(476) ack 2556 win 10720 <nop,nop,timestamp 1165681 892693>
2009:12:04-13:30:47.896702 IP vpn1.https > vpn2.53396: . ack 1057 win 6432 <nop,nop,timestamp 892693 1165681>
2009:12:04-13:30:47.896706 IP vpn2.53396 > vpn1.https: P 2556:2580(24) ack 1057 win 6432 <nop,nop,timestamp 892693 1165681>
2009:12:04-13:30:47.897120 IP vpn1.https > vpn2.53396: P 1057:1173(116) ack 2580 win 10720 <nop,nop,timestamp 1165681 892693>
2009:12:04-13:30:47.897263 IP vpn2.53396 > vpn1.https: P 2580:2628(48) ack 1173 win 6432 <nop,nop,timestamp 892693 1165681>
2009:12:04-13:30:47.897742 IP vpn1.https > vpn2.53396: P 1173:1289(116) ack 2628 win 10720 <nop,nop,timestamp 1165681 892693>
2009:12:04-13:30:47.897852 IP vpn2.53396 > vpn1.https: P 2628:2676(48) ack 1289 win 6432 <nop,nop,timestamp 892693 1165681>
2009:12:04-13:30:47.898243 IP vpn1.https > vpn2.53396: P 1289:1405(116) ack 2676 win 10720 <nop,nop,timestamp 1165681 892693>
2009:12:04-13:30:47.898453 IP vpn2.53396 > vpn1.https: P 2676:2700(24) ack 1405 win 6432 <nop,nop,timestamp 892693 1165681>
2009:12:04-13:30:47.898933 IP vpn1.https > vpn2.53396: P 1405:1521(116) ack 2700 win 10720 <nop,nop,timestamp 1165682 892693>
2009:12:04-13:30:47.899053 IP vpn2.53396 > vpn1.https: P 2700:2724(24) ack 1521 win 6432 <nop,nop,timestamp 892693 1165682>
2009:12:04-13:30:47.899306 IP vpn1.https > vpn2.53396: P 1521:1637(116) ack 2724 win 10720 <nop,nop,timestamp 1165682 892693>
2009:12:04-13:30:47.899508 IP vpn2.53396 > vpn1.https: P 2724:2748(24) ack 1637 win 6432 <nop,nop,timestamp 892694 1165682>
2009:12:04-13:30:47.899721 IP vpn1.https > vpn2.53396: P 1637:1753(116) ack 2748 win 10720 <nop,nop,timestamp 1165682 892694>
2009:12:04-13:30:47.899964 IP vpn2.53396 > vpn1.https: P 2748:2772(24) ack 1753 win 6432 <nop,nop,timestamp 892694 1165682>
2009:12:04-13:30:47.900390 IP vpn1.https > vpn2.53396: P 1753:1869(116) ack 2772 win 10720 <nop,nop,timestamp 1165682 892694>
2009:12:04-13:30:47.900541 IP vpn2.53396 > vpn1.https: P 2772:2796(24) ack 1869 win 6432 <nop,nop,timestamp 892694 1165682>
2009:12:04-13:30:47.900814 IP vpn1.https > vpn2.53396: P 1869:1985(116) ack 2796 win 10720 <nop,nop,timestamp 1165682 892694>
2009:12:04-13:30:47.900917 IP vpn2.53396 > vpn1.https: P 2796:2820(24) ack 1985 win 6432 <nop,nop,timestamp 892694 1165682>
2009:12:04-13:30:47.901101 IP vpn1.https > vpn2.53396: P 1985:2101(116) ack 2820 win 10720 <nop,nop,timestamp 1165682 892694>
2009:12:04-13:30:47.901286 IP vpn2.53396 > vpn1.https: P 2820:2844(24) ack 2101 win 6432 <nop,nop,timestamp 892694 1165682>
2009:12:04-13:30:47.901758 IP vpn1.https > vpn2.53396: P 2101:2217(116) ack 2844 win 10720 <nop,nop,timestamp 1165682 892694>
2009:12:04-13:30:47.901861 IP vpn2.53396 > vpn1.https: P 2844:2868(24) ack 2217 win 6432 <nop,nop,timestamp 892694 1165682>
2009:12:04-13:30:47.902051 IP vpn1.https > vpn2.53396: P 2217:2333(116) ack 2868 win 10720 <nop,nop,timestamp 1165682 892694>
2009:12:04-13:30:47.902264 IP vpn2.53396 > vpn1.https: P 2868:2892(24) ack 2333 win 6432 <nop,nop,timestamp 892694 1165682>
2009:12:04-13:30:47.902714 IP vpn1.https > vpn2.53396: P 2333:2449(116) ack 2892 win 10720 <nop,nop,timestamp 1165683 892694>
2009:12:04-13:30:47.903512 IP vpn2.53396 > vpn1.https: P 2892:2916(24) ack 2449 win 6432 <nop,nop,timestamp 892695 1165683>
2009:12:04-13:30:47.903541 IP vpn1.https > vpn2.53396: P 2449:2681(232) ack 2916 win 10720 <nop,nop,timestamp 1165683 892695>
2009:12:04-13:30:47.903717 IP vpn2.53396 > vpn1.https: P 2916:2940(24) ack 2681 win 7504 <nop,nop,timestamp 892695 1165683>
2009:12:04-13:30:47.904129 IP vpn1.https > vpn2.53396: P 2681:2730(49) ack 2940 win 10720 <nop,nop,timestamp 1165683 892695>
2009:12:04-13:30:47.911357 IP vpn2.53396 > vpn1.https: P 2940:2964(24) ack 2730 win 7504 <nop,nop,timestamp 892696 1165683>
2009:12:04-13:30:47.951186 IP vpn1.https > vpn2.53396: . ack 2964 win 10720 <nop,nop,timestamp 1165695 892696>
```

```
VPN_CA/emailAddress
OvXd
EF_VZUReXJcDP'
bit key
authentication
bit key
authentication
1024 bit RSA
93
```

# Overhead/Latencies



## ▶ IPsec

```
vpn1:/root # ping -c 1 -I 10.10.10.10 192.168.1.1
PING 192.168.1.1 (192.168.1.1) from 10.10.10.10 : 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=0.728 ms

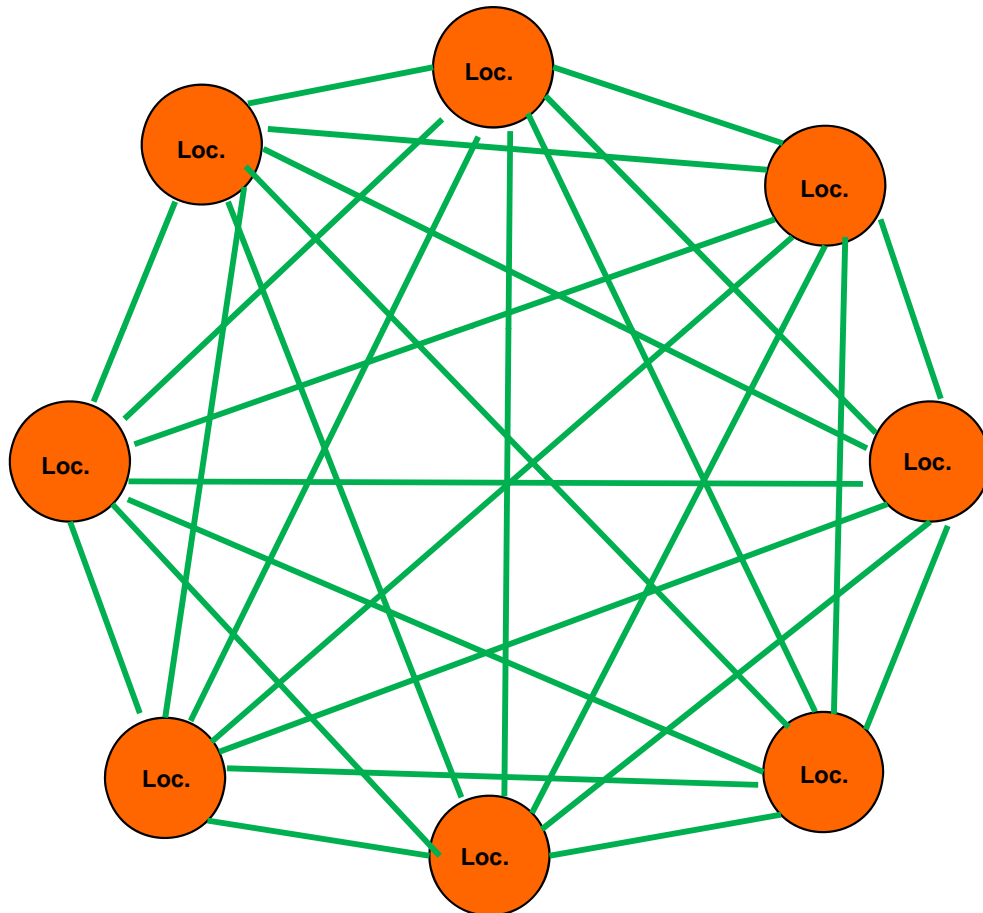
13:18:47.933520 IP vpn1 > vpn2: ESP (spi=0x8f4a9c3a,seq=0x3), length 132
13:18:47.933884 IP vpn2 > vpn1: ESP (spi=0x5174092e,seq=0x3), length 132
```

## ▶ SSL

```
vpn1:/root # ping -c 1 -I 10.10.10.10 192.168.1.1
PING 192.168.1.1 (192.168.1.1) from 10.10.10.10 : 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=0.728 ms

15:48:33.395149 length 197: vpn1.https > vpn2.53396: P 1402869499:1402869630(131) ack 1468021704 win 9648
15:48:33.396348 length 197: vpn2.53396 > vpn1.https: P 1:132(131) ack 131 win 12864
15:48:33.396507 length 66: vpn1.https > vpn2.53396: . ack 132 win 9648
```

# VPN Topologies Fully Meshed



The number of connections in a full mesh:

$$n(n - 1) / 2$$

$n$  = number of nodes (branches)

**Examples:**

$$n=8 \\ (8 \times 7) / 2 = \underline{28}$$

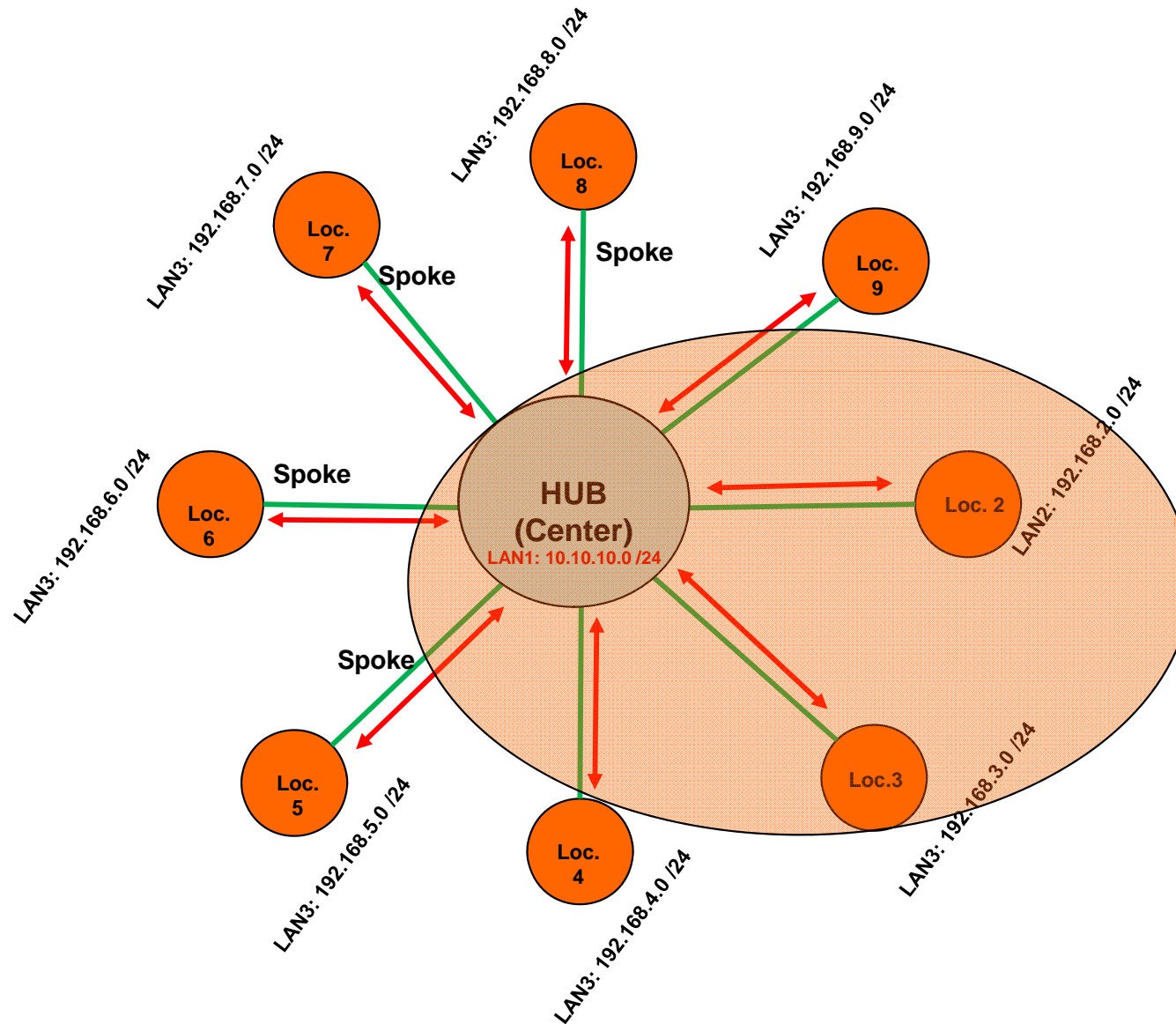
$$n=50 \\ (50 \times 49) / 2 = \underline{1225}$$

$$n=100 \\ (100 \times 99) / 2 = \underline{4950}$$

# VPN Topologies Hub and Spoke

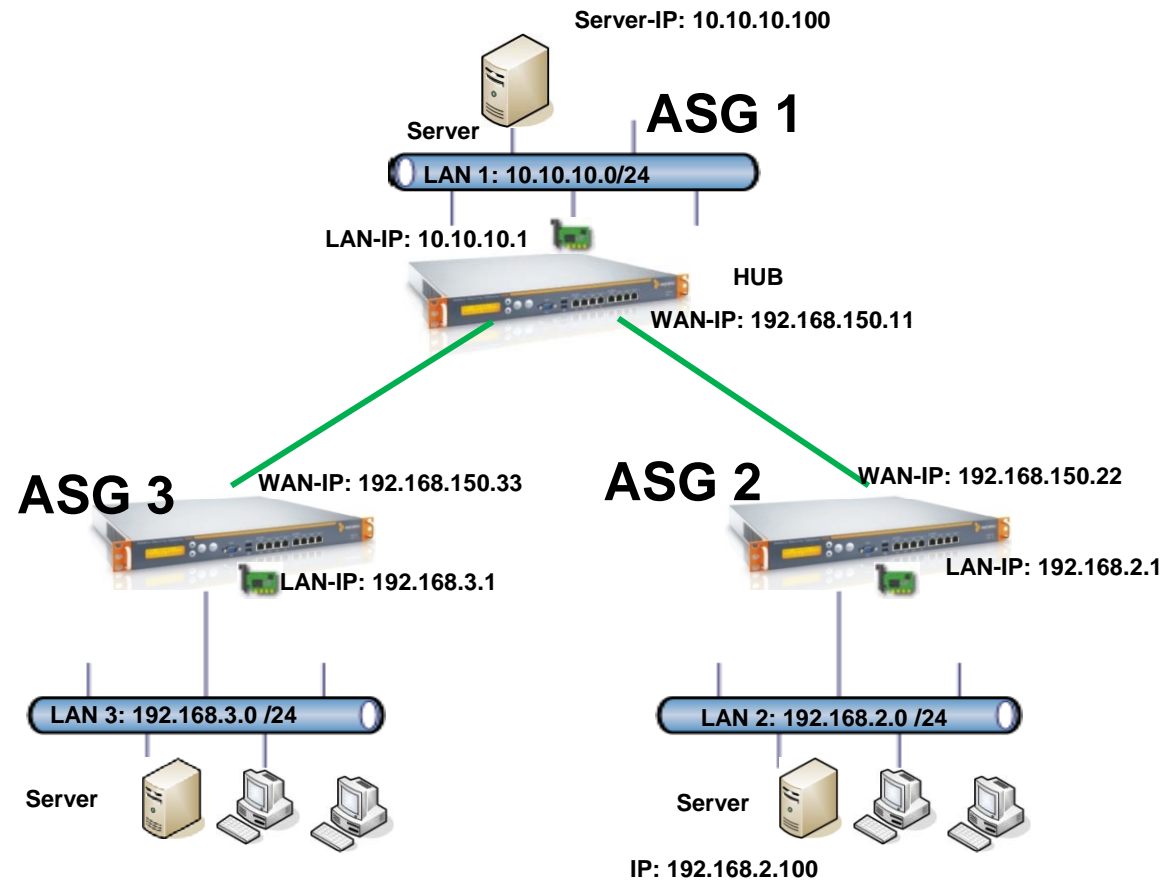
## Communication „Site to Center“

DEMO



# VPN Topologies Hub and Spoke

## Communication „Site to Center“

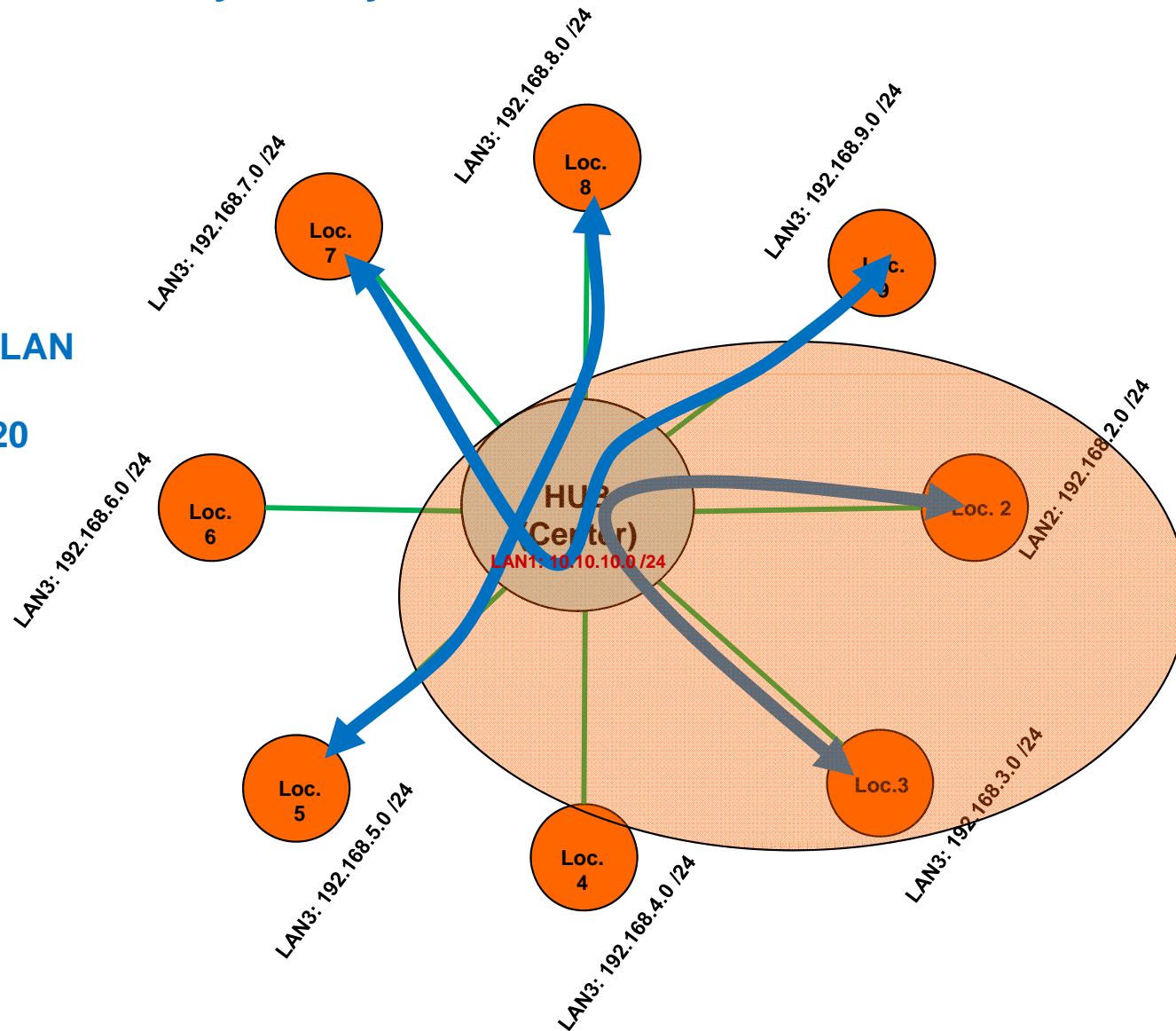


# VPN Topologies Hub and Spoke

Communication „any to any“

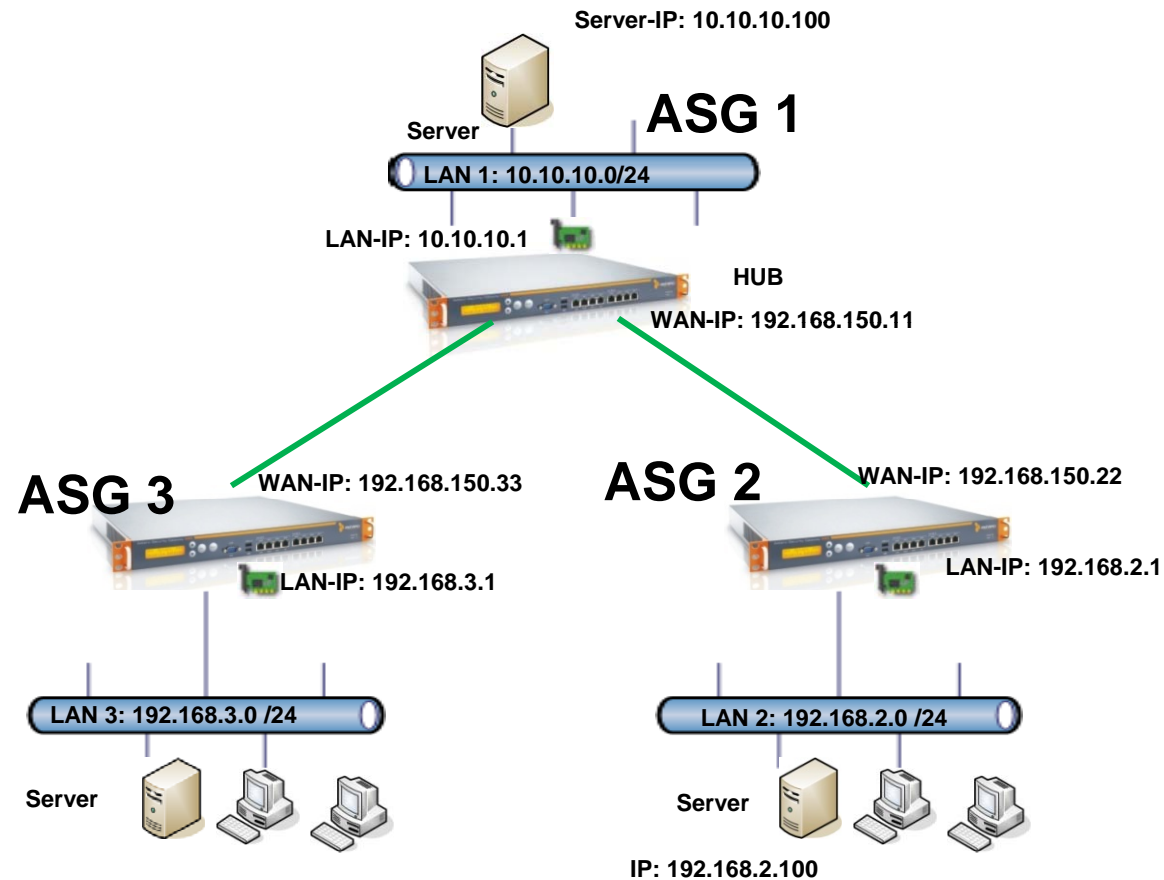
DEMO

Higher-ranking LAN  
„SupraNet“  
192.168.0.0/20



# VPN Topologies Hub and Spoke

Communication „any to any“



Higher-ranking LAN  
„SupraNet“  
192.168.0.0/20

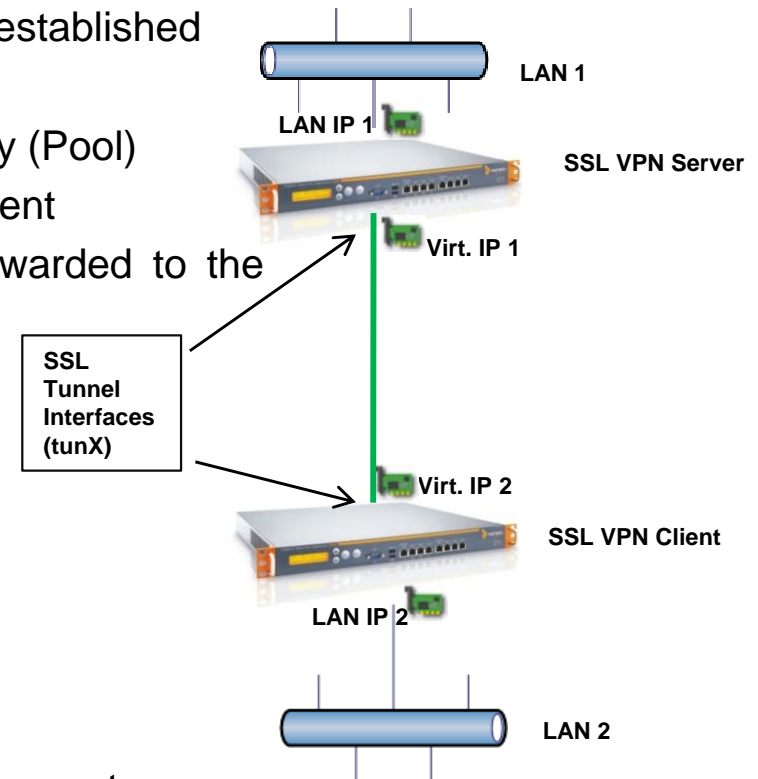
## Best practise IPSec Site2Site

- ▶ **First step: Create the remote gateway**
- ▶ **Gateway type:**
  - ▶ **Initiate Connection: ASG initializes VPN to the other tunnel endpoint actively**
  - ▶ **Respond only: ASG is waiting for the connection initialized by the other tunnel endpoint**
    - ▶ **e.g. for dial up connections, dynamical IP without DynDNS**
- ▶ **Avoid PSK!**
  - ▶ **Functional limitations**
  - ▶ **Security aspects**
- ▶ **Use RSA or X.509 certificates**
  - ▶ **X.509 certificates contain a RSA public key**
  - ▶ **Recommended type: „local X.509 certificate“**
  - ▶ **Exchange certificates vice versa with the other tunnel endpoint**
    - ▶ **Download always as PEM (not PKCS#12, contains private key!)**
    - ▶ **„advanced – local X509 cert“ defines the certificate**
    - ▶ **DPD and NAT-T should be activated normally**

# Configure SSL VPN Site2Site properly

DEMO

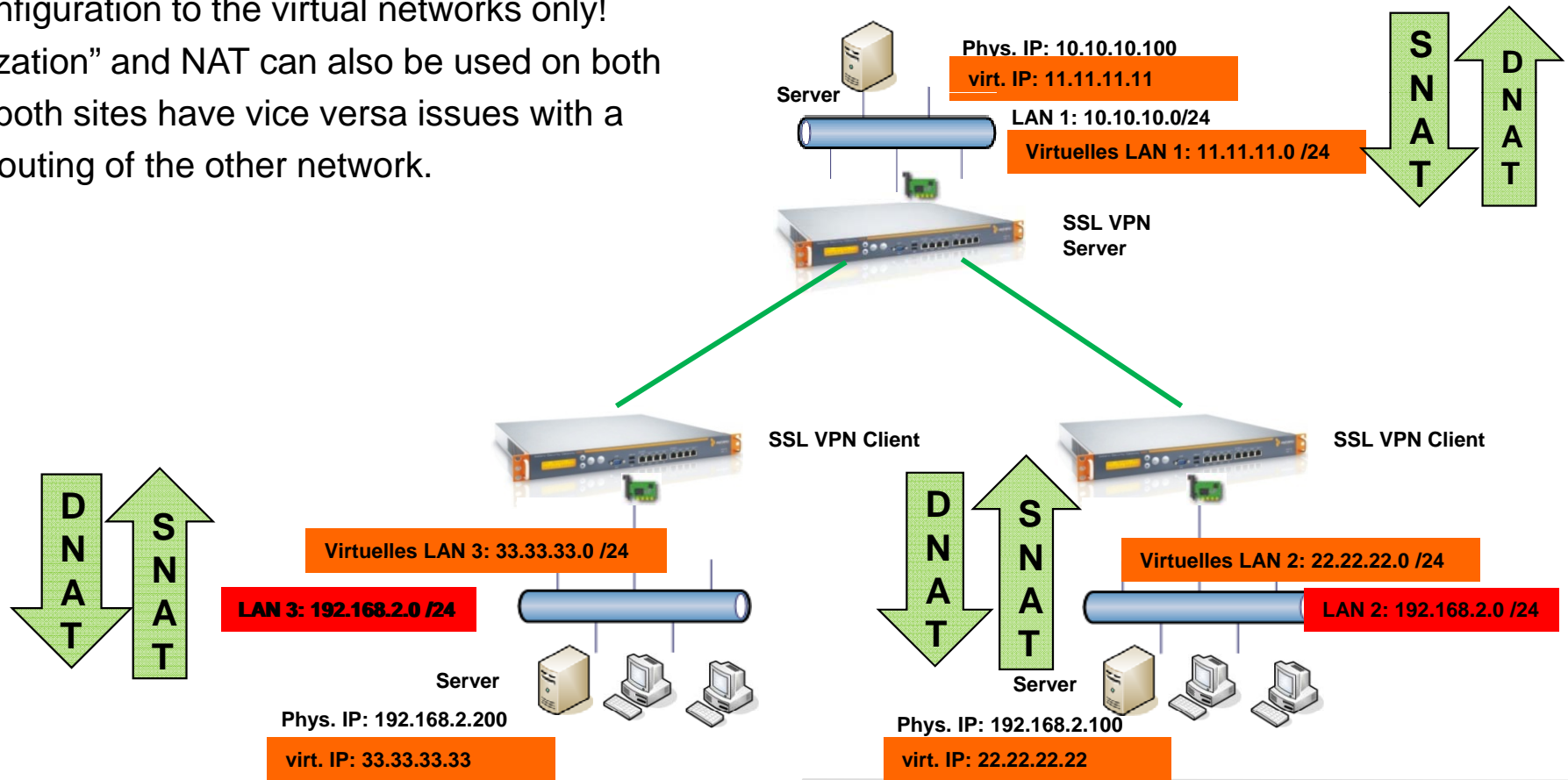
- ▶ Client - Server principle
  - ▶ Server in “respond only” mode, client in “initiate only” mode
  - ▶ The same ASG can play the role of server and client for multiple connections during the same time.
- ▶ Based on OpenVPN , but with Astaro specific configuration files
  - ▶ Very simple and fast setup/rollout
- ▶ Between the tunnel endpoints always a transfer network gets established
  - ▶ Per Default IP-Adressen aus dem “SSL VPN Pool”
  - ▶ Client-IP can be changed per connection, Server globally (Pool)
  - ▶ Trick: Client IP = ASG IP internal -> ping comes from client
- ▶ Many changes in server configuration are automatically forwarded to the clients (tunnels are stopped and restarted):
  - ▶ “local network”
  - ▶ static virtual IP
  - ▶ server virtual IP Pool
  - ▶ but **not**:
    - ▶ Encryption settings
    - ▶ Port/Protocol settings
    - ▶ Override hostname setting
  - ▶ Requires: Not just to download a new APC file, but to generate a new connection!



# NAT in a VPN tunnel

- ▶ Requirement
  - ▶ Hide remote LAN IPs because of overlapping with other remote LANs
  - ▶ Hide remote LAN IPs because of overlapping with local LANs
- ▶ “Hiding” has to happen at one (remote) site
- ▶ Hide the “real” network behind a virtual network:
  - ▶ DNAT for incoming traffic, e.g. access to remote server
  - ▶ SNAT as “Pseudo-Masquerading” for outgoing access to the central LAN
- ▶ VPN configuration to the virtual networks only!
- ▶ “Virtualization” and NAT can also be used on both sites, if both sites have vice versa issues with a proper routing of the other network.

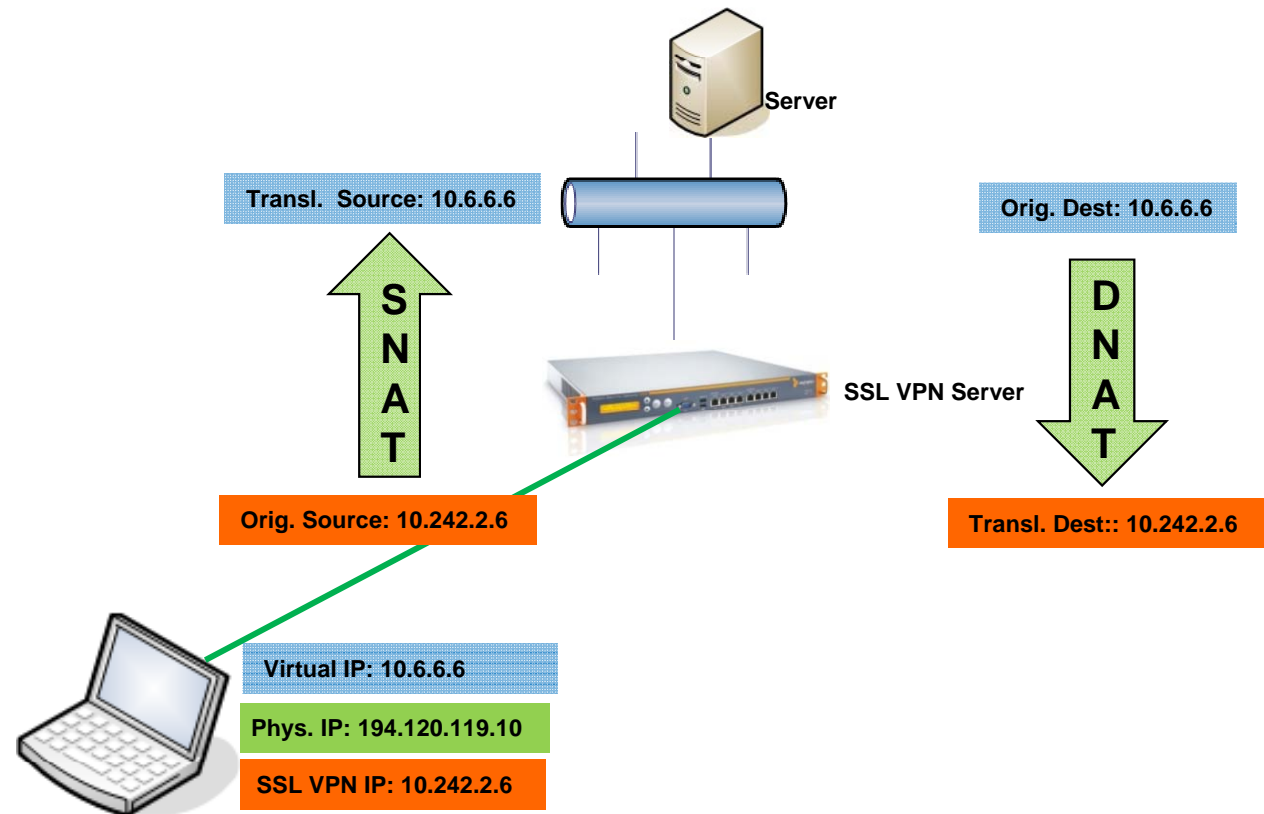
**DEMO**



## SSL VPN: Remote User with static IP

- ▶ **SSL VPN Client gets ALWAYS a dynamical IP address**
- ▶ “use static remote access IP” does not influence it for SSL VPN!
- ▶ Workaround: SNAT and DNAT
  - ▶ Each user gets a virtual IP address
  - ▶ This address is *not* dynamical
  - ▶ Depending on the scenario *pure* SNAT or *pure* DNAT or SNAT & DNAT rules are needed
- ▶ **From point of view of the LAN the SSL User has a fix IP address now!**

### DEMO



## SSL VPN: Push all traffic into the tunnel

- ▶ **Avoid “split tunneling”**
  - ▶ To assure that a user can not have access to confidential data in the headquarter network and surf the Internet during the same time
  - ▶ Otherwise worms, trojans, spyware, monitorware, exploits can reach the central network though the user PC.
- ▶ It s implemented as a feature in the ASC Client, but not in the SSL VPN client
- ▶ Can be realized (with some limitations) also on the SSL VPN client based on a kind of workaround:
- ▶ ***Use the network definition “ANY” instead of the internal networks in your “Local Network” configuration vor SSL VPN! (Do not forget: MASQUERADING rules, Proxy rules etc.)***
  - ▶ ALL traffic of the users will be pushed into the tunnel based on the automatically created routing settings on the client.
  - ▶ Attention: Users with some networking knowhow are able to circumvent these settings.

**DEMO**

## IPSec VPN: Mode "CA DN match"

- ▶ **IPSec RAS for many user with X.509 certificates**
  - ▶ Mode „X.509“: all certificates have to be stored on the ASG under „Certificate Management“!
- ▶ Effort to integrate user with certificates of external CAs
- ▶ Solution: Mode „CA DN match“
  - ▶ Just import once the CA as verification CA
  - ▶ ASC clients authenticate/connect with user certificate of this CA
  - ▶ In IPSec connection a „DN Mask“ is used, which has to match the „incoming“ certificates → Remote access groups are possible
  - ▶ *No auto packetfilter* → Firewall rules are depending on the peer IP address
  - ▶ Important for ASC configuration: Folder CA\_Certs has to contain the CA certificates of the verification CA and of the ASG CA!
  - ▶ No auto IP address assignment

**DEMO**

## IPSec VPN: PSK and XAUTH

- ▶ **Limitations while using PSK**
  - ▶ Dynamical IP addresses of the remote site
    - ▶ C2S: all user have the same PSK!
    - ▶ S2S: just a single „Respond Only“ Gateway with PSK possible
  - ▶ No tunnel status in remote access overview
  - ▶ No assignment of virtual remote access IP addresses
  
- ▶ **Remote access VPN: PSK should always be combined with XAUTH!**
  - ▶ Additional user specific authentication („password“)
  - ▶ Offers the option to use backend authentication server, incl. OTP

**DEMO**

## SSL VPN vs. IPSec-VPN

	IPSec VPN	SSL VPN
Complexity of the protocol	0	+
Scalability/Performance	+	0
Protocoll overhead and latencies	+	+ -
Interoperabililty with other vendors	+	-
Security aspects	+ -	0
Supported authentication methods	+	0
Usability in different scenarios	0	+
„Client Push“ possibility	-	+
Changes are not influencing other tunnels	+	-
Easy to roll out and use	0	+++

# Thank you for your attendance!

Web: [www.astaro.com](http://www.astaro.com)

Mail: [info@astaro.com](mailto:info@astaro.com)

Tel: +49(0)721 255 16 0

Astaro Up2date-Blog: <http://up2date.astaro.com>

User Bulletin Board: <http://www.astaro.org>

Knowledgebase: <http://www.astaro.com/kb>