

VPN- & Security-Policy mit MS-AD

Projekt «Globale Ablösung Forefront TMG bei Wey Technology»

Martin Volkart, Geschäftsführer, IMV Informatik GmbH

Manuel Fraefel, System Engineer, Studerus AG



Agenda

Vorstellung Martin Volkart / IMV Informatik GmbH

Wey Technology Projekt TMG to Firewall

TMG to Firewall Migration, welche Rollen sind möglich

Tech.Part 1 Firewall AD Anbindung Konfiguration

Tech.Part2 VPN to VPN static Routing

Wer ist IMV Informatik GmbH



- Gegründet 1997
- Neuhausen am Rheinfal
- 8 Mitarbeiter
- Systemintegrator KMU
- Region SH / CH Nord
- Zyxel, Microsoft, HP/HP
- Schulungen
- Consulting in
Grossumgebungen



Wer ist Martin Volkart

- El. Ing HTL
- Geschäftsführer IMV
- >150 Microsoft Zertifizierungen
- MCT seit 1997
- Dozent
Expertenschulungen

Projekte mit

- AD / Exchange / Office 365
- Azure / VOIP / HyperV
- Microsoft TMG



Der Kunde: WEY Technology AG



Filialstandorte in

- Frankfurt
- London
- Paris
- Mailand
- Singapore
- New York
- Moskau



Massgeschneiderte Produkte
"Made in Switzerland"



Projekt Ausgangslage





Ziel des Projekts

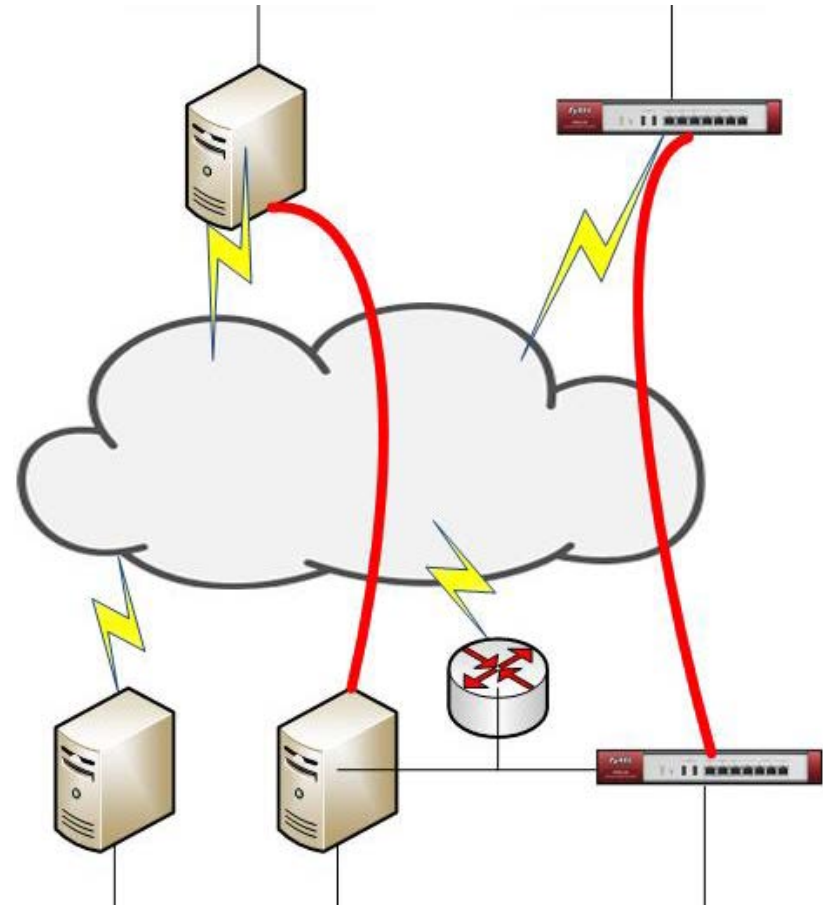
Da TMG nicht mehr unterstützt wird, muss dieser abgelöst werden. Dabei muss die bestehende Funktionalität erhalten bleiben.

Role	TMG bisher	Firewall neu
Security Policy	JA	JA
Site-to-Site VPN	JA	JA
Client-to-Site VPN mit MS-AD Authentication	JA	JA
2 ISP am Hauptsitz	(JA)	JA
Routing LAN/DMZ,WLAN	JA	JA
Web-Proxy HTTPS	JA	NEIN

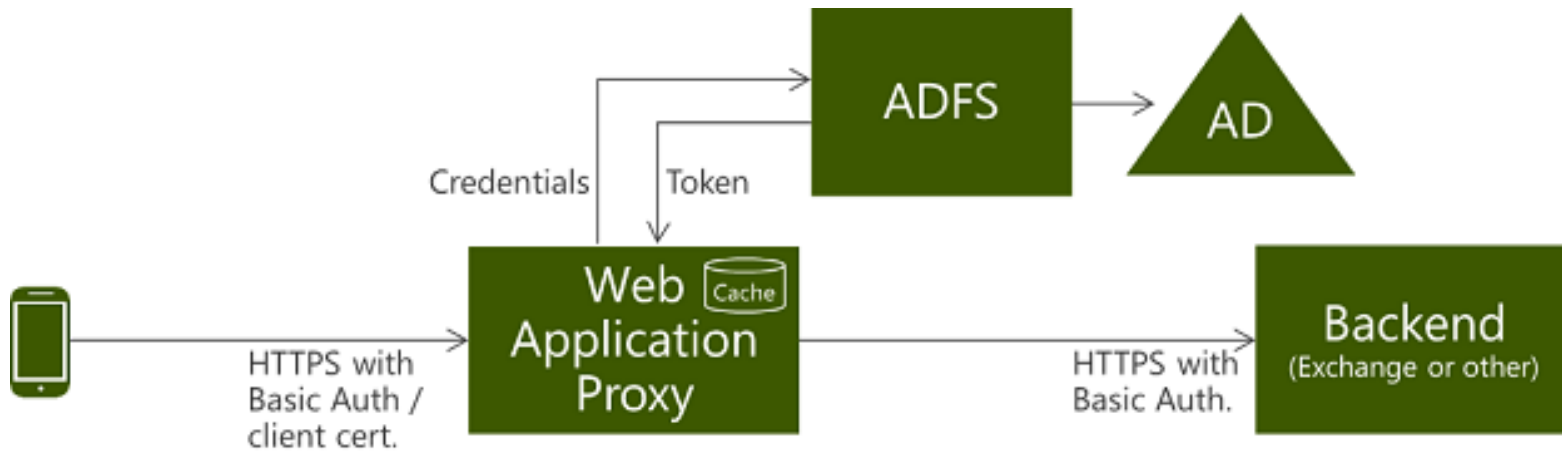
Migration (Part 1)



1. HQ Schweiz mit USG 1100 auf separater IP in Betrieb nehmen
2. Alle Rollen TMG zu Firewall verschieben
3. Filiale um Filiale migrieren
 - a. Vorkonfigurierte USG 110 versenden
 - b. VPN TMG/TMG ersetzen durch USG/USG
 - c. Routing zwischen den Filialen anpassen
4. Migration veröffentlichter Dienste von TMG nach USG



Migration (Part 2)



Aufbau Web App Proxy für Preauthenticated Access

- ADFS schon vorhanden, aber Upgrade notwendig
- Web App Proxy hinzugefügt
- ADFS Federation zu O365 aktualisiert
- Exchange Published

Agenda

Vorstellung Martin Volkart / IMV Informatik GmbH

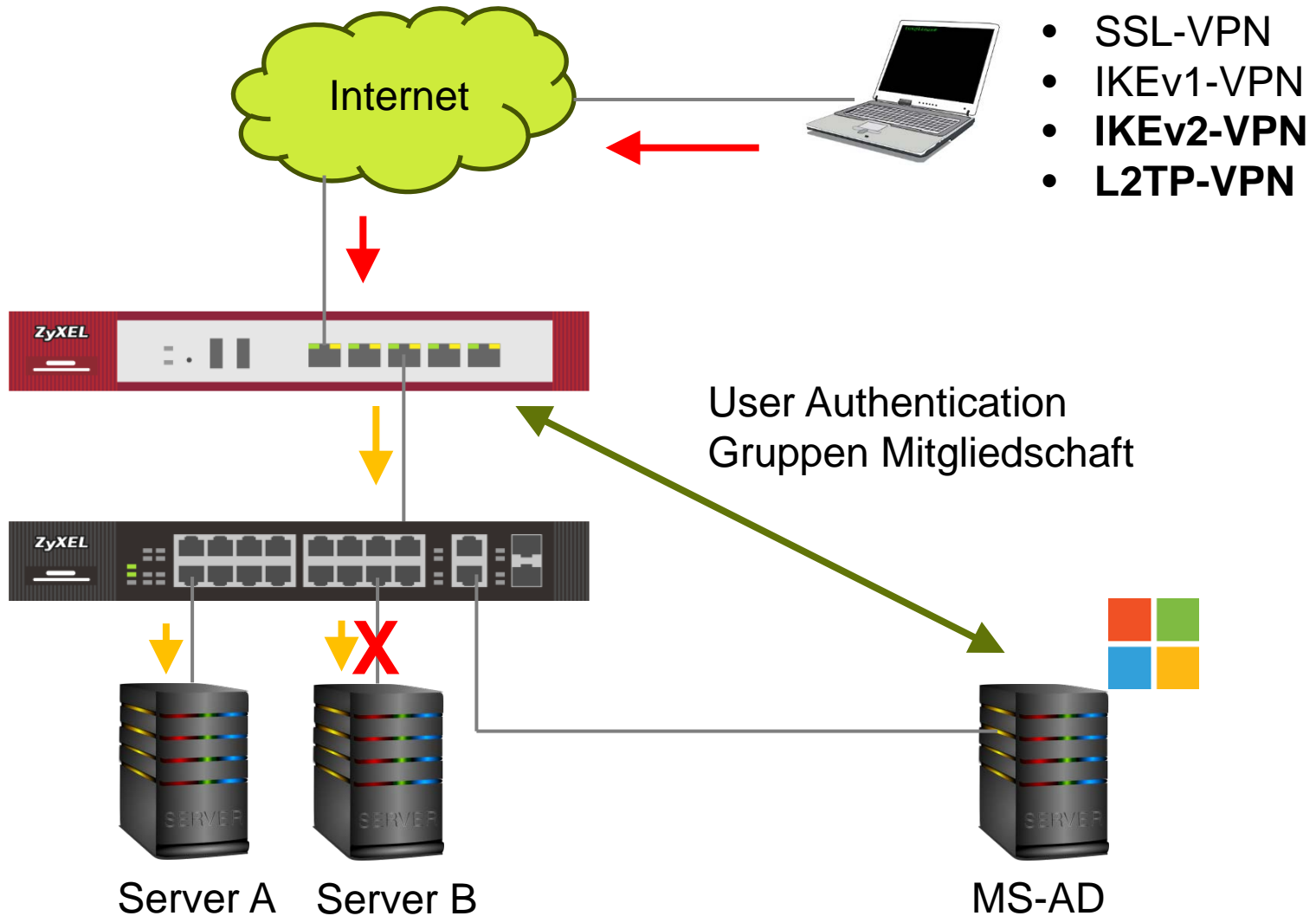
Wey Technology Projekt TMG to Firewall

TMG to Firewall Migration, welche Rollen sind möglich

Tech.Part 1 Firewall AD Anbindung Konfiguration

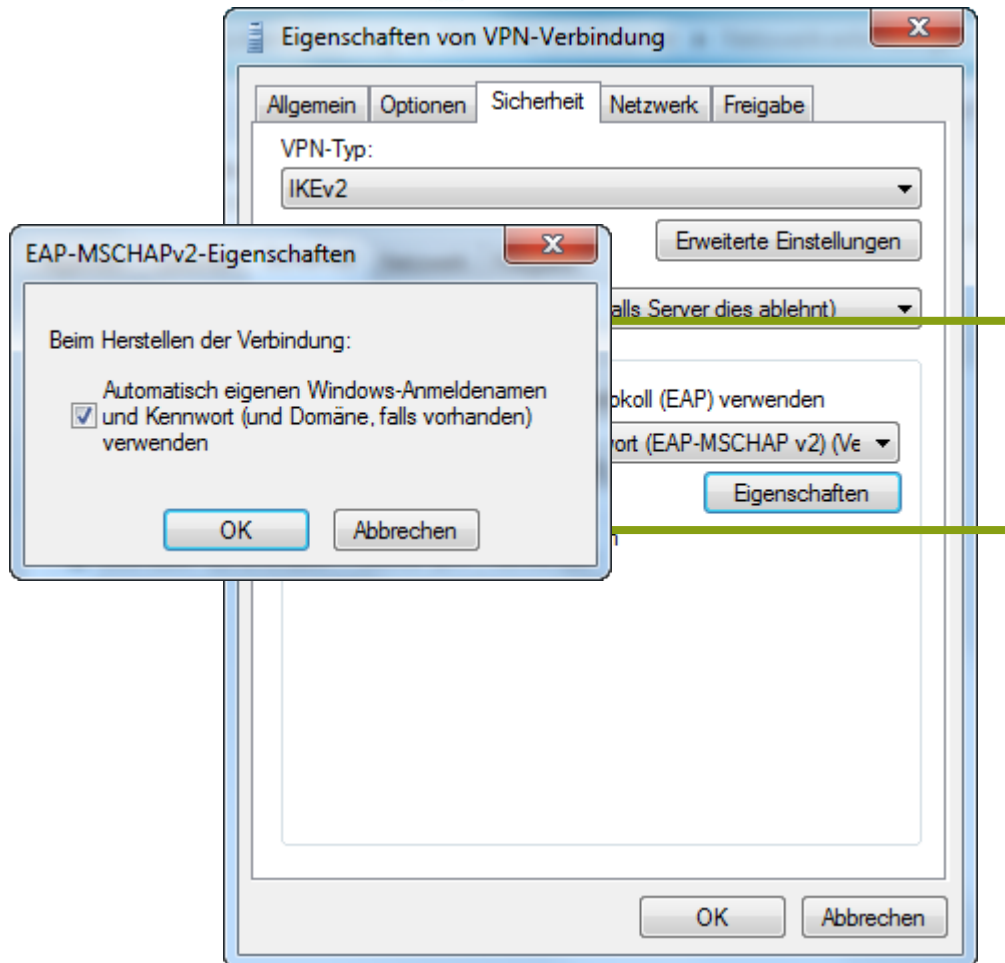
Tech.Part2 VPN to VPN static Routing

MS-AD Anbindung der Firewall - Overview



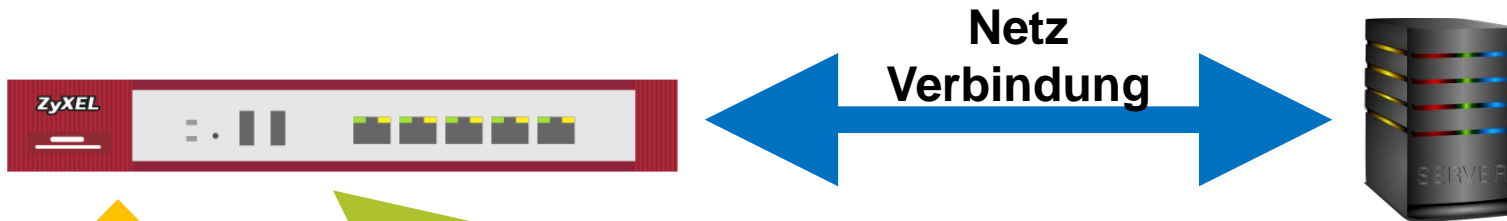
MS-AD Anbindung der Firewall – Win Client

- IKEv2-VPN





Firewall-Konfiguration Basis für MS-AD



1

Host Name

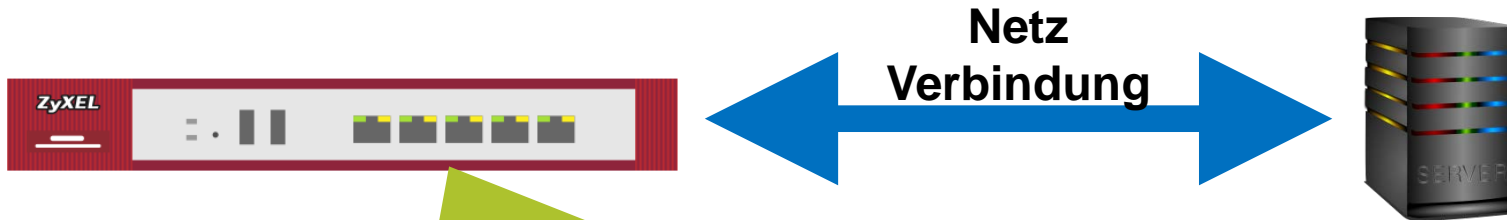
General Settings

System Name:	<input type="text" value="fw01"/>	(Optional)
Domain Name:	<input type="text" value="studeruslab.local"/>	(Optional)

Note:
In windows AD authentication case, please make sure the system name is shorter than 15 characters.
The long system name will make AD authentication fail.



Firewall-Konfiguration Basis für MS-AD



2

Edit Domain Zone Forwarder 1

Domain Zone: studeruslab.local

DNS Server

DNS Server(s) from ISP

wan1_ppp

First DNS Server: N/A

Second DNS Server: N/A

Third DNS Server: N/A

Public DNS Server

172.27.2.40

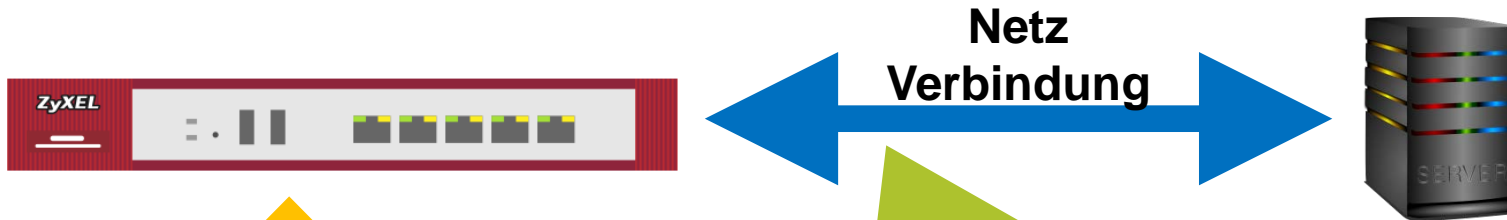
Query via: auto

Private DNS Server

OK Cancel



Firewall-Konfiguration Basis für MS-AD



3

Network Tool

Network Tool:

PING IPv4

Domain Name or IP Address:

studeruslab.local

 Advance

Test

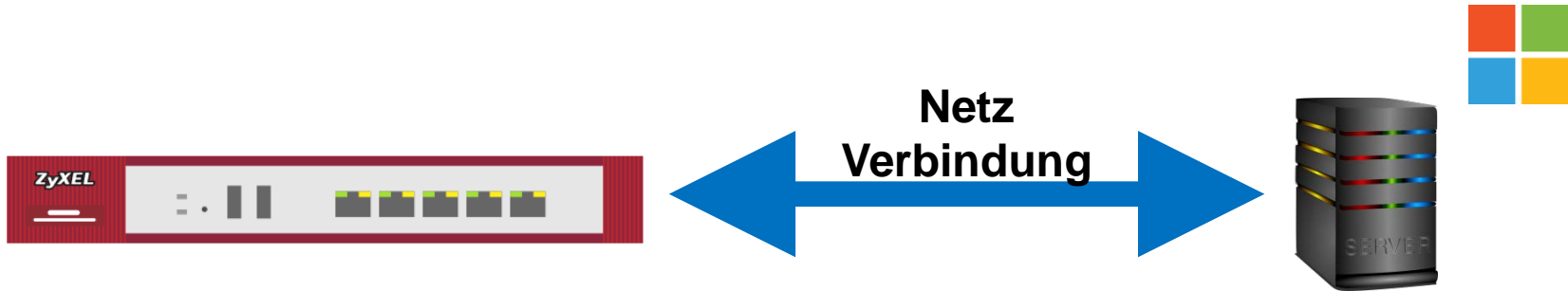
Stop

Reset

```
# ping studeruslab.local -n -c 3
PING studeruslab.local (172.27.2.40) 56(84) bytes of data.
64 bytes from 172.27.2.40: icmp_seq=1 ttl=127 time=0.449 ms
64 bytes from 172.27.2.40: icmp_seq=2 ttl=127 time=0.382 ms
64 bytes from 172.27.2.40: icmp_seq=3 ttl=127 time=0.410 ms

--- studeruslab.local ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.382/0.413/0.449/0.036 ms
```

Firewall-Konfiguration Basis für MS-AD



1. Firewall Host/Domain Eintrag für MS-AD Domain
2. Firewall DNS Zone Forwarder für MS-AD Domain
3. Ping Test auf die AD Domain in Ordnung
4. Optional Firewall Auth. Server-Zertifikat für PEAP (SSL)

Firewall MS-AD Anbindungseinstellungen



LDAP
Verbindung



1

Edit Active Directory MFR_TESTLAN_2012R2

General Settings

Name:

Description: (Optional)

Server Settings

Server Address: (IP or FQDN)


Backup Server Address: (IP or FQDN)(Optional)

Port: (1-65535)

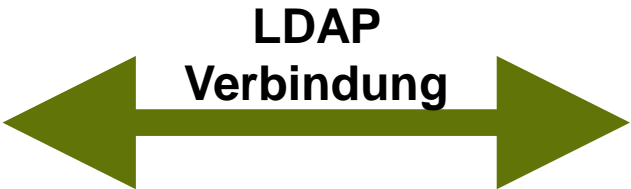
Base DN:

Use SSL

Search time limit: (1-300 seconds)

Case-sensitive User Names 

Firewall MS-AD Anbindungseinstellungen



Active Directory Users and Computers		Name	Type
<ul style="list-style-type: none"> Active Directory Users and Computers <ul style="list-style-type: none"> Saved Queries studeruslab.local <ul style="list-style-type: none"> Builtin Computers Domain Controllers ForeignSecurityPrincipals Formation LostAndFound Managed Service Accounts Program Data Radius_Test_abi System test_mfr Users NTDS Quotas TPM Devices sru_users 		<ul style="list-style-type: none"> Builtin Computers ForeignSecurityPrincipals Managed Service Accounts Program Data System Users Infrastructure LostAndFound NTDS Quotas TPM Devices Domain Controllers Formation Radius_Test_abi test_mfr sru_users 	<ul style="list-style-type: none"> builtinDomain Container Container Container Container Container Container infrastructureUpdate lostAndFound msDS-QuotaContainer msTPM-InformationO... Organizational Unit Organizational Unit Organizational Unit Organizational Unit Organizational Unit

Firewall MS-AD Anbindungseinstellungen



LDAP
Verbindung



2

Server Authentication

Bind DN:
Password:
Retype to Confirm:

cn=Administrator,cn=Users,dc=studeruslab,dc=local

Alternative Login Name Attribute: (Optional)
Group Membership Attribute:

Firewall MS-AD Anbindungseinstellungen



LDAP
Verbindung



2

Server Authentication

Bind DN:

Password:

Retype to Confirm:

User Login Settings

Login Name Attribute:

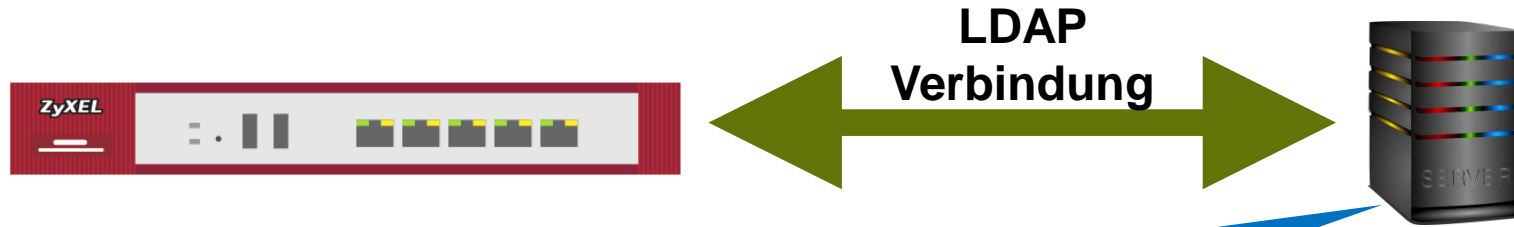
Alternative Login Name Attribute: (Optional)

Group Membership Attribute:

userPrincipalName



Firewall MS-AD Anbindungseinstellungen



2

Manuel Fraefel Properties [?] [X]

Published Certificates	Member Of	Password Replication	Dial-in	Object	
Security	Environment	Sessions	Remote control		
Remote Desktop Services Profile		COM+	Attribute Editor		
General	Address	Account	Profile	Telephones	Organization

User logon name:

User logon name (pre-Windows 2000):

Firewall MS-AD Anbindungseinstellungen



Configuration Validation

Please enter an existing user account in this server to validate the above settings.

Username:

Returned User Attributes:

```
dn: CN=Manuel Fraefel,OU=test_mfr,DC=studeruslab,DC=local
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: Manuel Fraefel
sn: Fraefel
givenName: Manuel
distinguishedName: CN=Manuel Fraefel,OU=test_mfr,DC=studeruslab,DC=local
instanceType: 4
whenCreated: 20170809155707.0Z
whenChanged: 20170809155707.0Z
displayName: Manuel Fraefel
```

Firewall MS-AD Anbindungseinstellungen



Auth.Option



General Settings

Name: default

+ Add Edit Remove Move

#	Method List
1	group MFR_TESTLAN_2012R2
2	local

Zugangsprüfung erst gegen MS-AD und dann gegen die lokale DB der Firewall

Authentication Method

Configuration

+ Add Edit Remove Object References

#	Method Name	Method List
1	default	local

Page 1 of 1 Show 50 items

Firewall MS-AD Anbindungseinstellungen



Login TEST



Enter User Name/Password and click to login.

User Name:

Password:

One-Time Password: (Optional)
 (max. 63 alphanumeric, printable characters and no spaces)

Login

mfr, You now have logged in.

Click the logout button to terminate the access session.
 You could renew your lease time by clicking the Renew button.
 For security reason you must login in again after 23 hours 59 minutes.

User-defined lease time (max 1440 minutes):

Updating lease time automatically

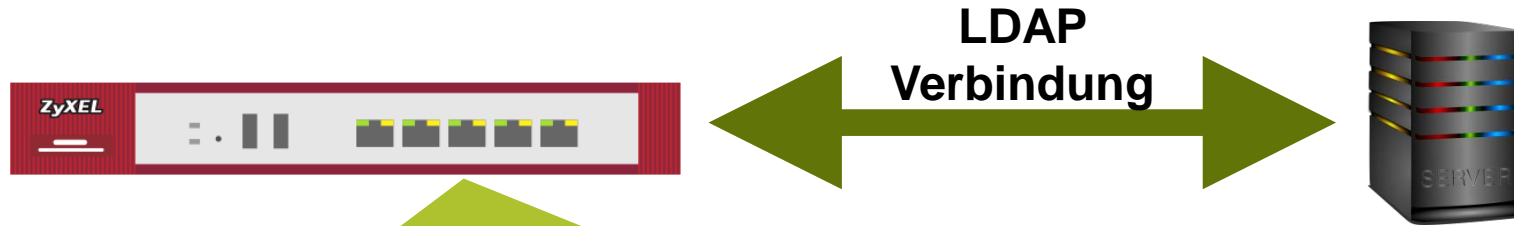
Remaining time before lease timeout (hh:mm:ss):

Remaining time before auth. timeout (hh:mm:ss):

Logout



Firewall MS-AD Anbindungseinstellungen

**3**

Domain Authentication for MSChap

 Enable

User Name:

manuel 

User Password:

●●●●●●●●●●

Retype to Confirm:

●●●●●●●●●●

Realm:

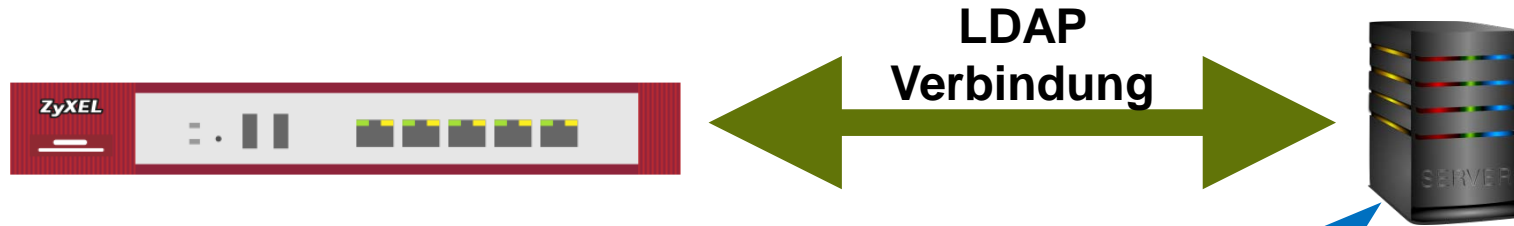
studeruslab.local

NetBIOS Name:

studeruslab

Achtung: Primary-Gruppe «Domain Admin»

Firewall MS-AD Anbindungseinstellungen

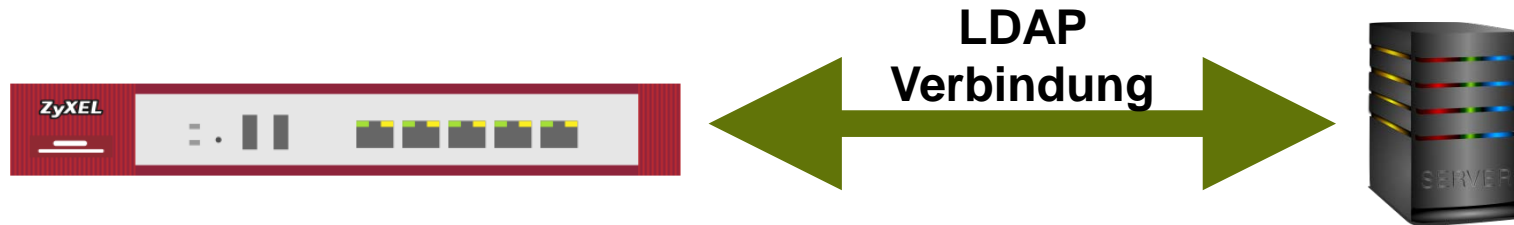


3

A screenshot of the 'Active Directory Users and Computers' console. The left pane shows the tree structure: Active Directory Users and Computers > Saved Queries > studeruslab.local > Builtin > Computers. The right pane shows a table with the following data:

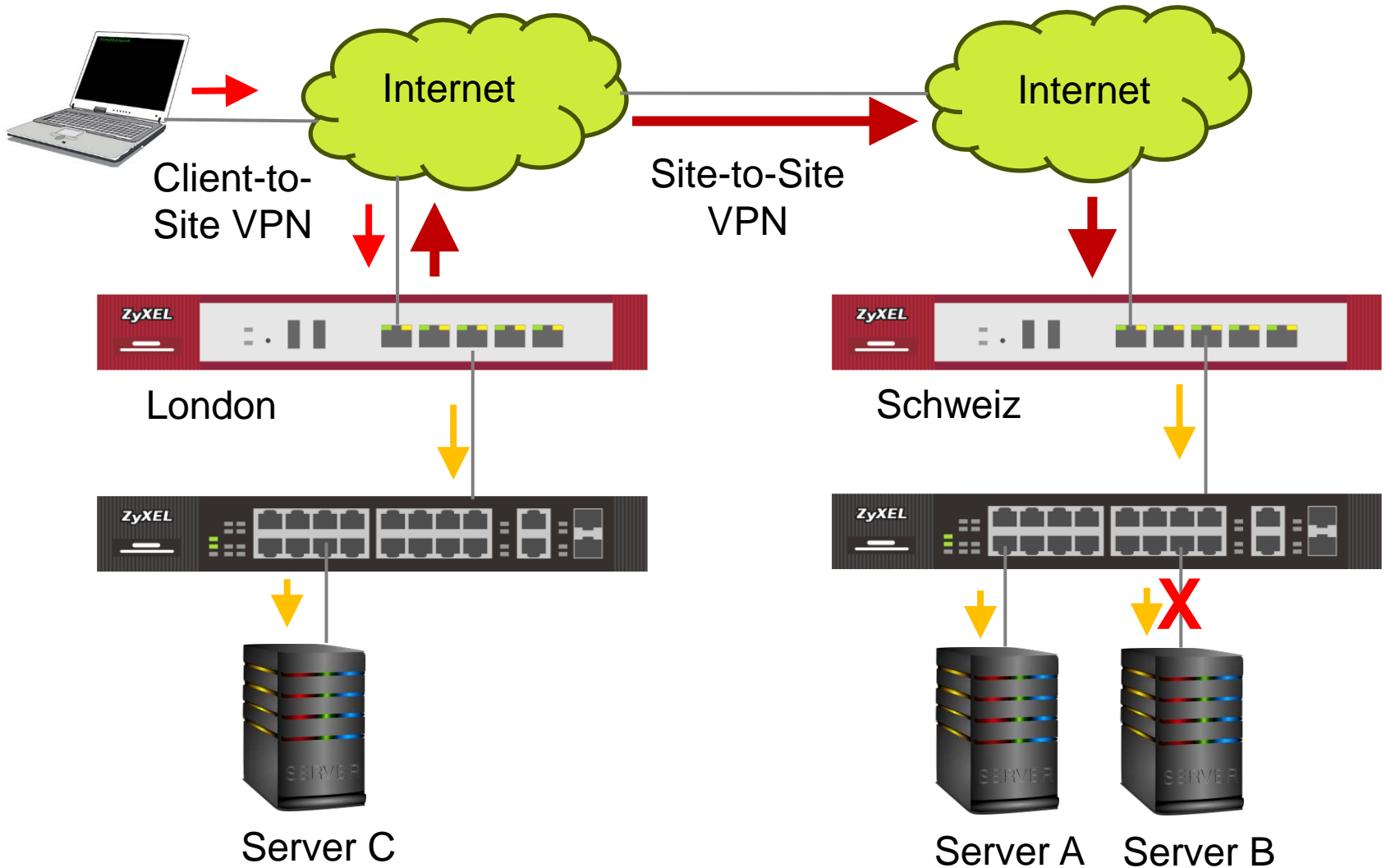
Name	Type
fw01	Computer

Firewall MS-AD Anbindungseinstellungen

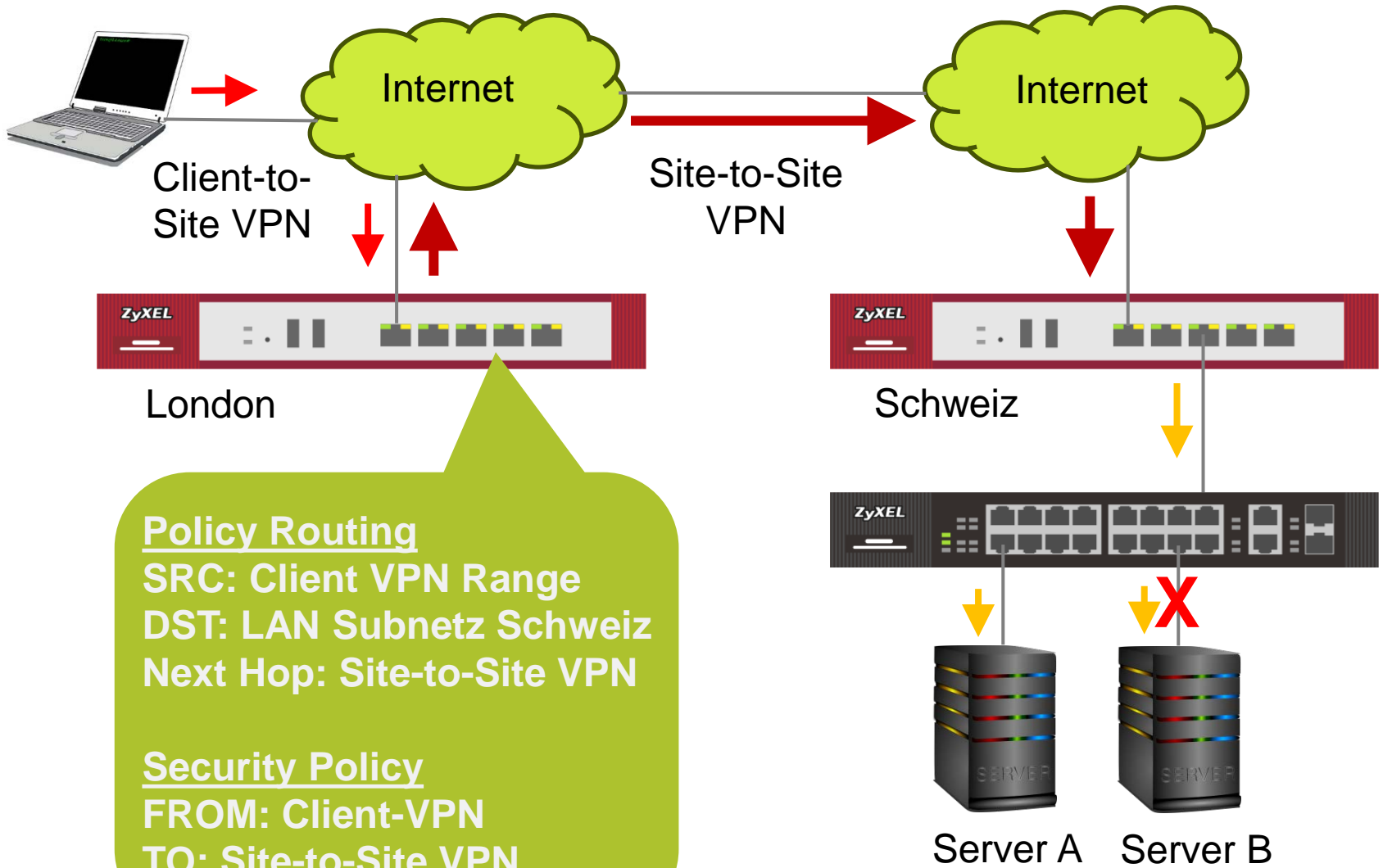


1. Eintrag AD-Server / IP AD Backup-Server (IP bevorzugt)
BASE DN Einstiegspunkt der LDAP-Abfrage
Standard Port 389, SSL verschlüsselt Port 636
2. BIND DN, LDAP Pfad für autorisierten User der Firewall-Attribute für sAM User und AD-Gruppen-Abfrage
3. Erweiterte Autorisierung für IKEv2 EAP-MSChapv2 und optional L2TP EAP-MSChapv2-Abfrage

Client VPN – 1 Site-to-Site Hop - Overview



Client VPN – 1 Site-to-Site Hop – Route 1



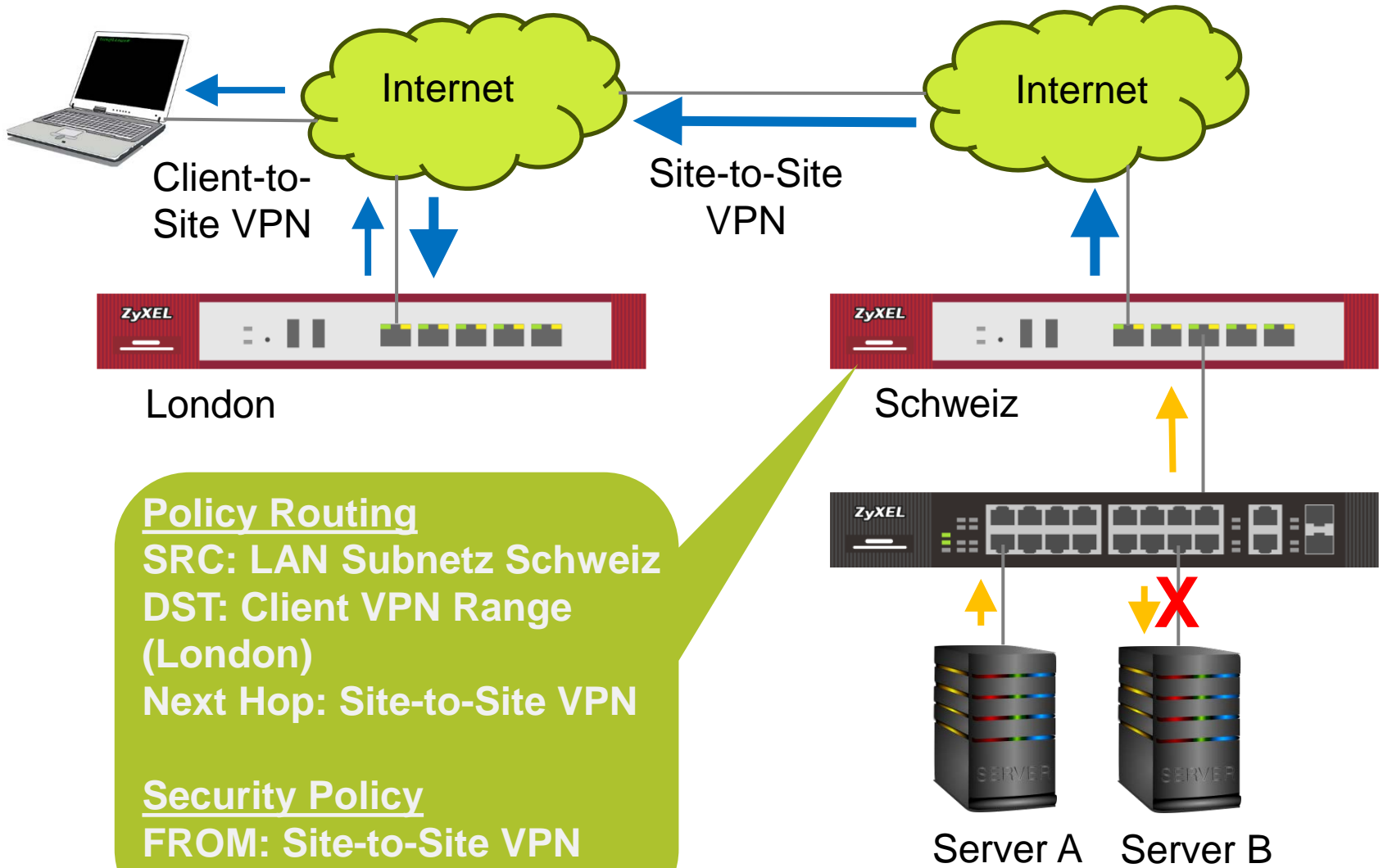
Policy Routing

SRC: Client VPN Range
 DST: LAN Subnetz Schweiz
 Next Hop: Site-to-Site VPN

Security Policy

FROM: Client-VPN
 TO: Site-to-Site VPN

Client VPN – 1 Site-to-Site Hop – Route 2



Policy Routing
 SRC: LAN Subnetz Schweiz
 DST: Client VPN Range (London)
 Next Hop: Site-to-Site VPN

Security Policy
 FROM: Site-to-Site VPN
 TO: LAN Subnetz Schweiz

Fragen?

TE
FO17



STUDERUS
TECHNOLOGY
FORUM