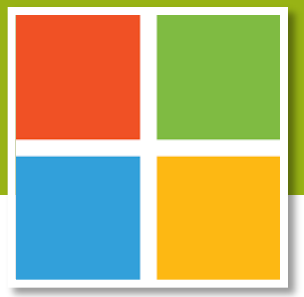
Track T4

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



STUDERUS
network technologies

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

STUDERUS
network technologies

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

STUDERUS
network technologies

Der Kunde: WEY Technology AG

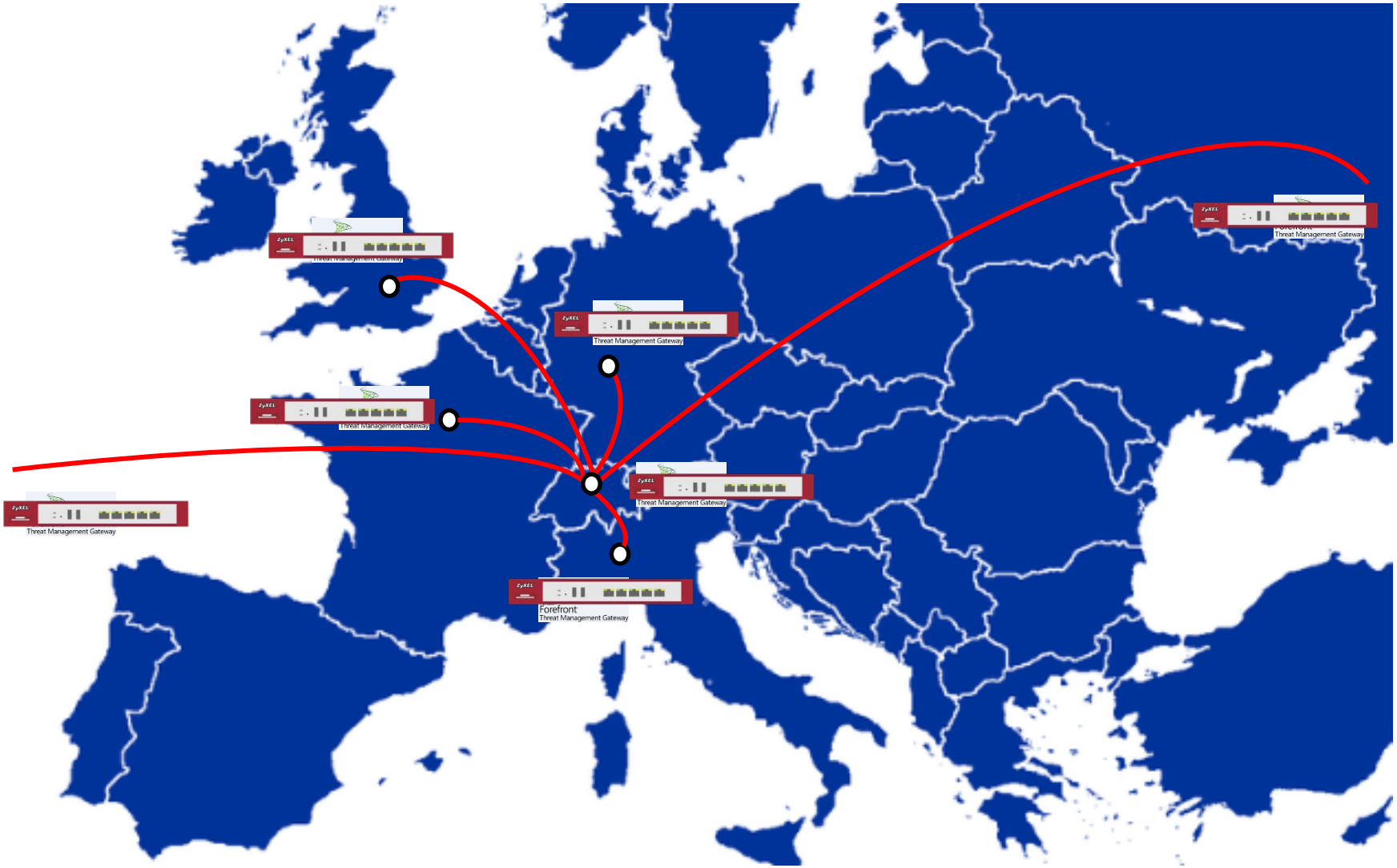
Filialstandorte in

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

Massgeschneiderte Produkte
"Made in Switzerland"

STUDERUS
network technologies

Projekt Ausgangslage



STUDERUS
network technologies

Ziel des Projekts

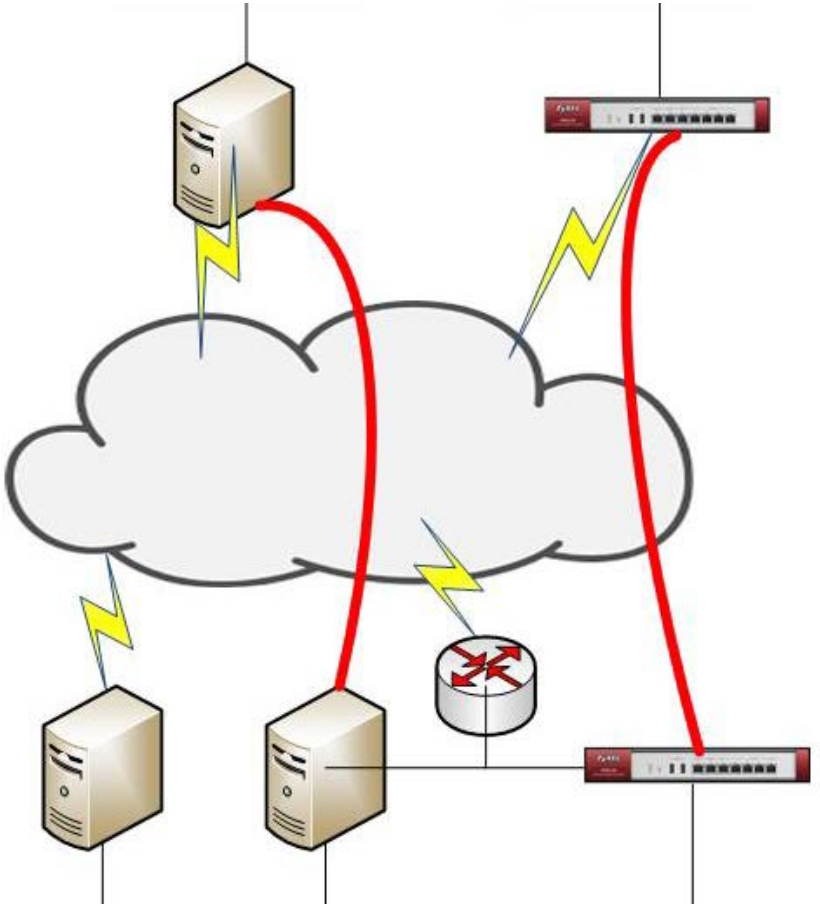
Da TMG nicht mehr unterstützt wird, muss dieser abgelöst werden. Dabei muss die bestehende Funktionalität erhalten bleiben.

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

STUDERUS
network technologies

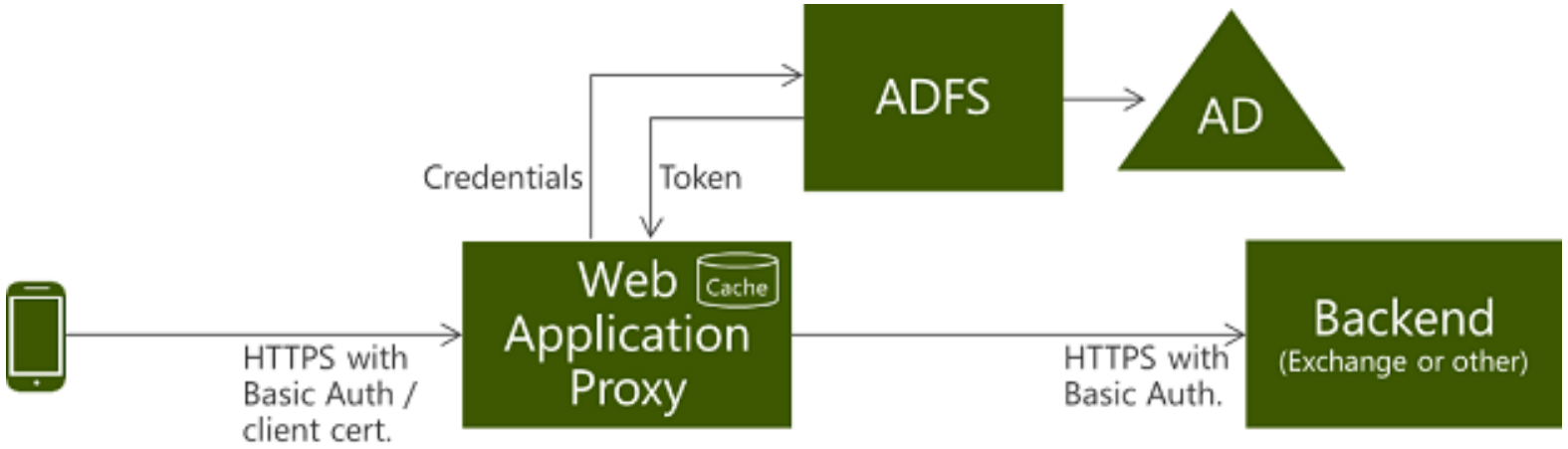
Migration (Part 1)

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



STUDERUS
network technologies

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

STUDERUS
network technologies

Agenda

Vorstellung Martin Volkart / IMV Informatik GmbH

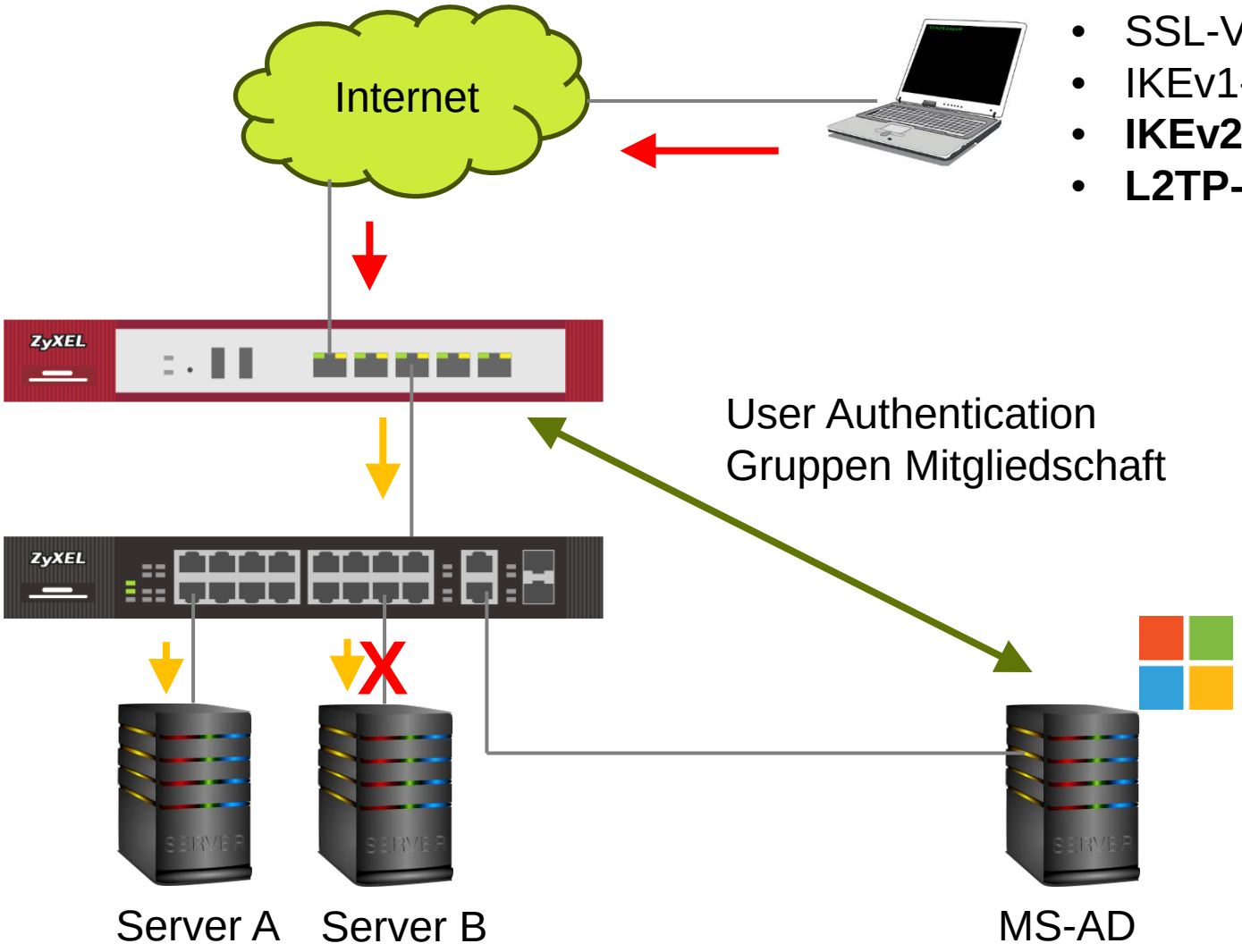
Wey Technology Projekt TMG to Firewall

TMG to Firewall Migration, welche Rollen sind möglich

Tech.Part 1 Firewall AD Anbindung Konfiguration

Tech.Part2 VPN to VPN static Routing

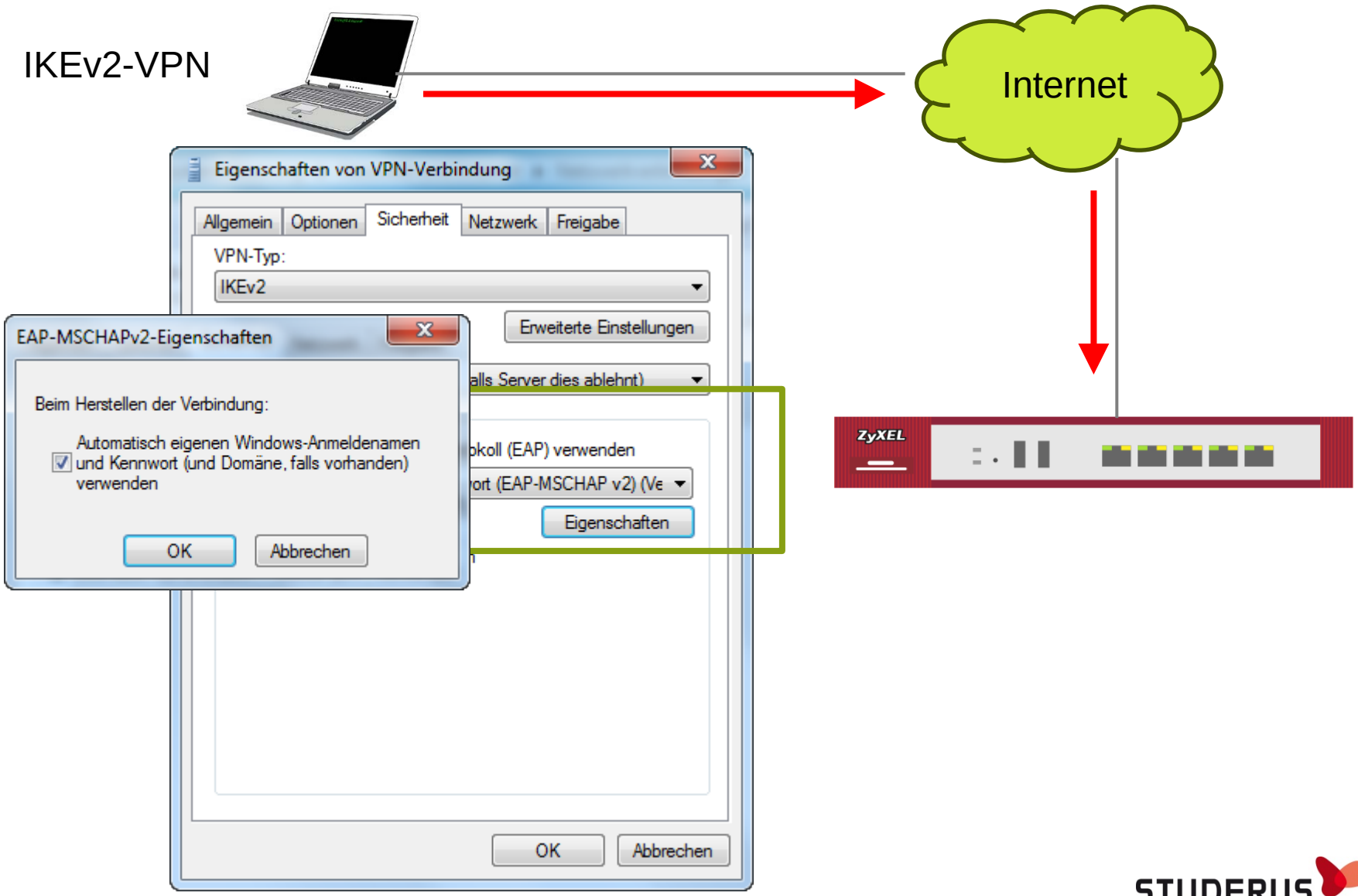
MS-AD Anbindung der Firewall - Overview



- SSL-VPN
- IKEv1-VPN
- **IKEv2-VPN**
- **L2TP-VPN**

MS-AD Anbindung der Firewall – Win Client

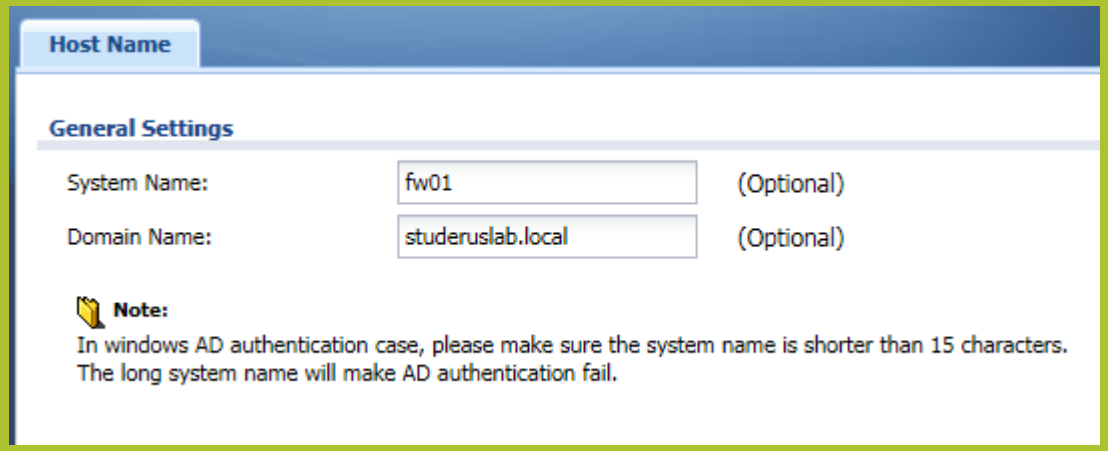
- IKEv2-VPN



Firewall-Konfiguration Basis für MS-AD

Netz
Verbindung

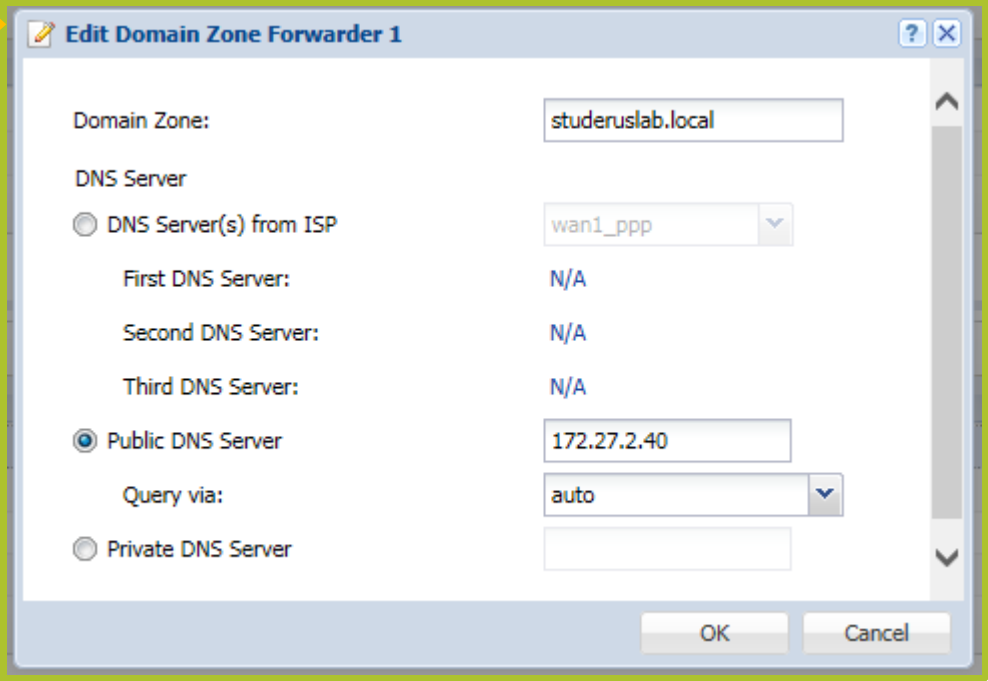
1



Firewall-Konfiguration Basis für MS-AD

Netz
Verbindung

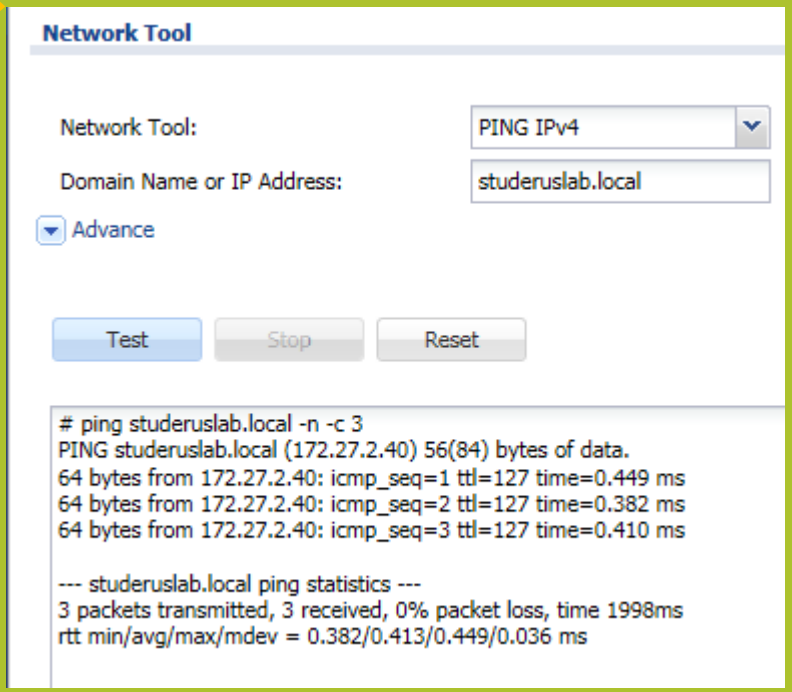
2



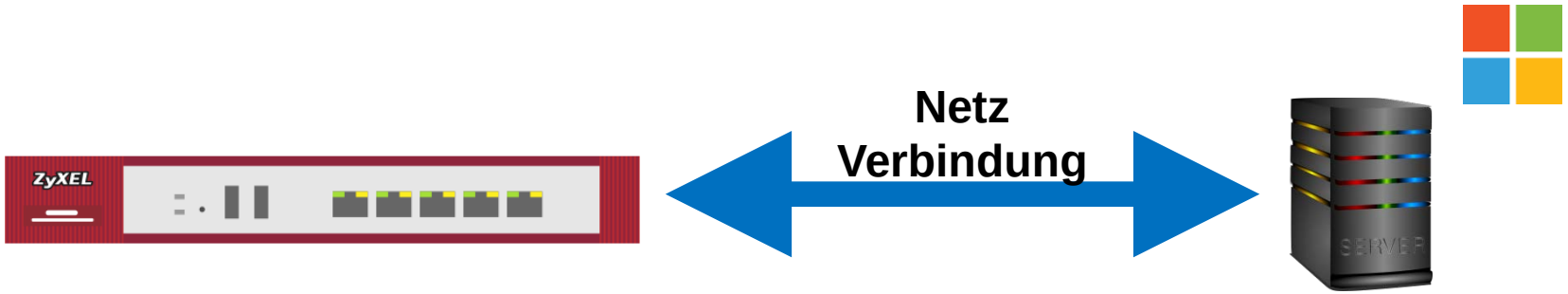
Firewall-Konfiguration Basis für MS-AD

Netz
Verbindung

3



Firewall-Konfiguration Basis für MS-AD

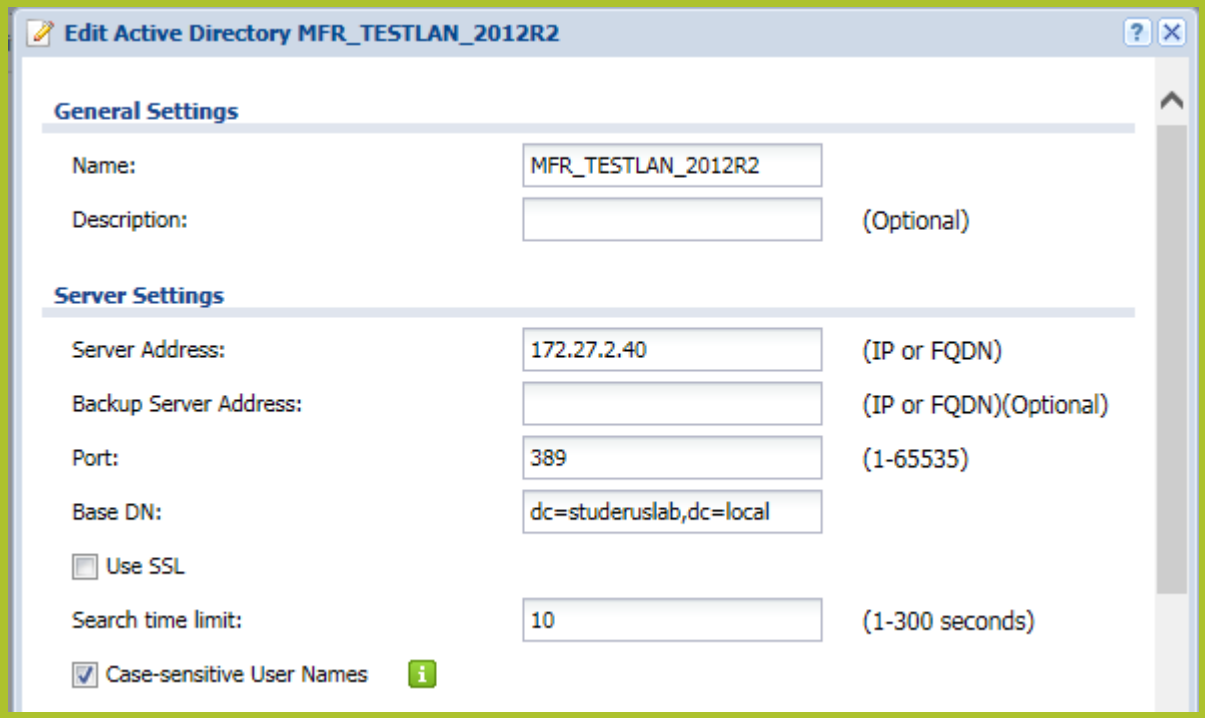


1. Firewall Host/Domain Eintrag für MS-AD Domain
2. Firewall DNS Zone Forwarder für MS-AD Domain
3. Ping Test auf die AD Domain in Ordnung
4. Optional Firewall Auth. Server-Zertifikat für PEAP (SSL)

Firewall MS-AD Anbindungseinstellungen

LDAP Verbindung

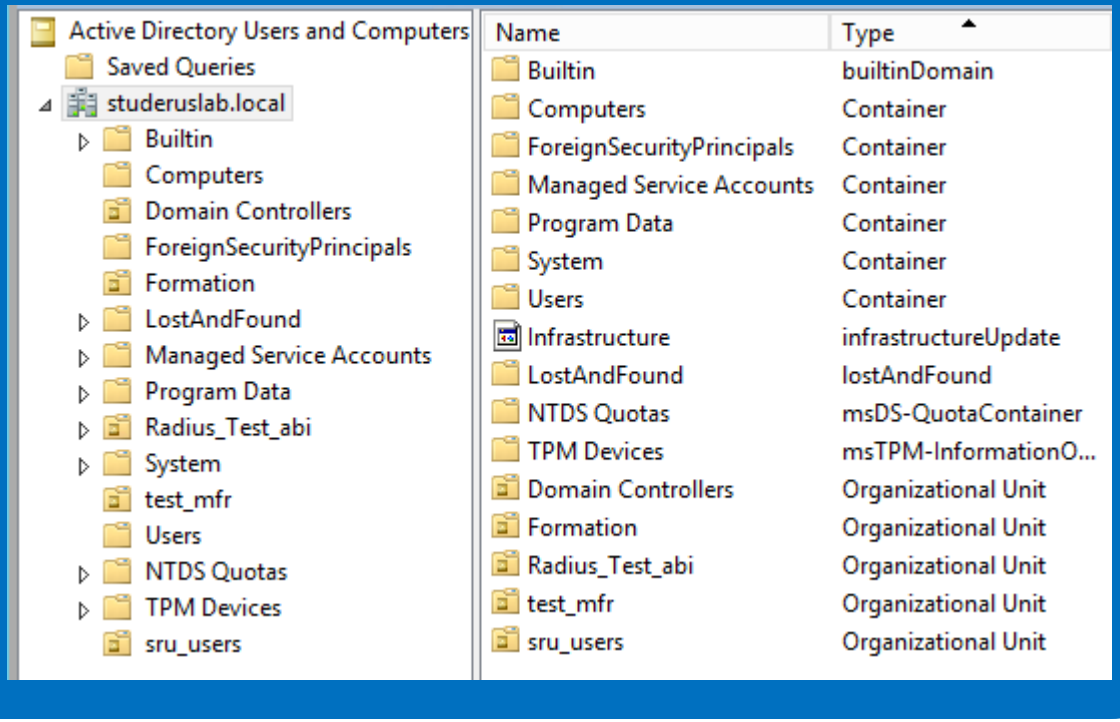
1



Firewall MS-AD Anbindungseinstellungen

LDAP Verbindung

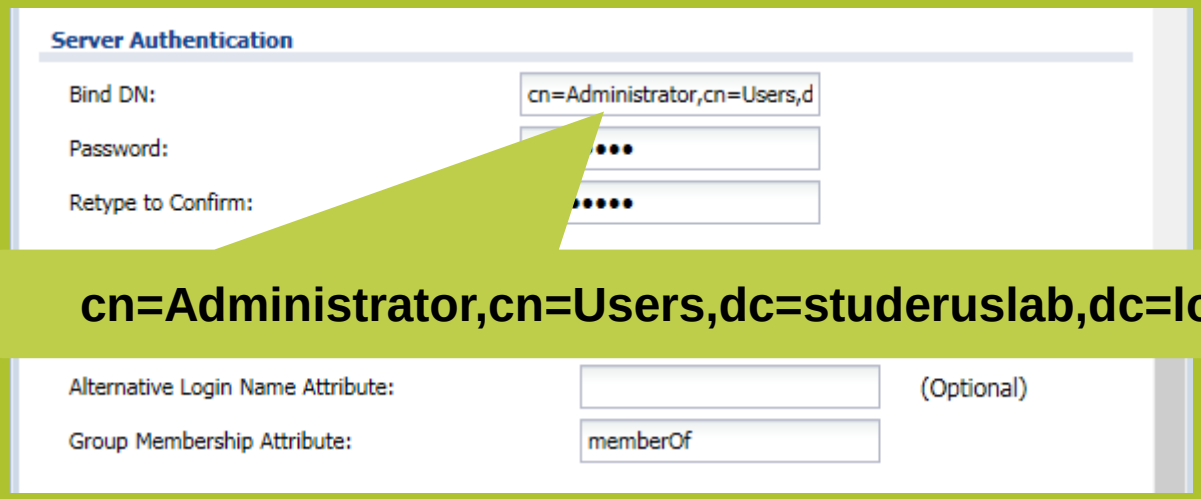
1



Firewall MS-AD Anbindungseinstellungen

LDAP
Verbindung

2



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

Firewall MS-AD Anbindungseinstellungen

LDAP
Verbindung

2

Server Authentication

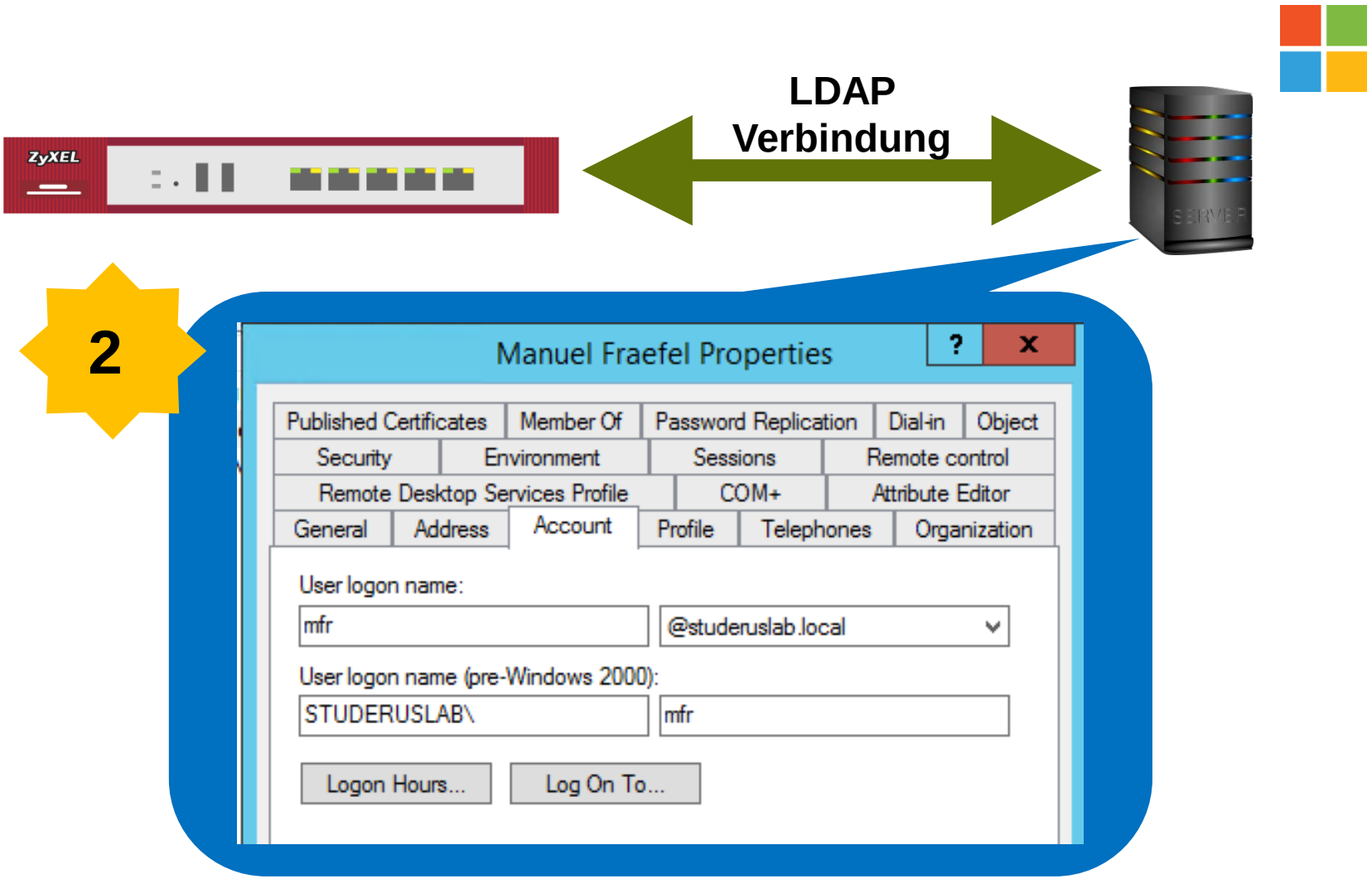
Bind DN:	cn=Administrator,cn=Users,d
Password:	••••••••
Retype to Confirm:	••••••••

User Login Settings

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

userPrincipalName

Firewall MS-AD Anbindungseinstellungen



Firewall MS-AD Anbindungseinstellungen

LDAP TEST

Configuration Validation

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

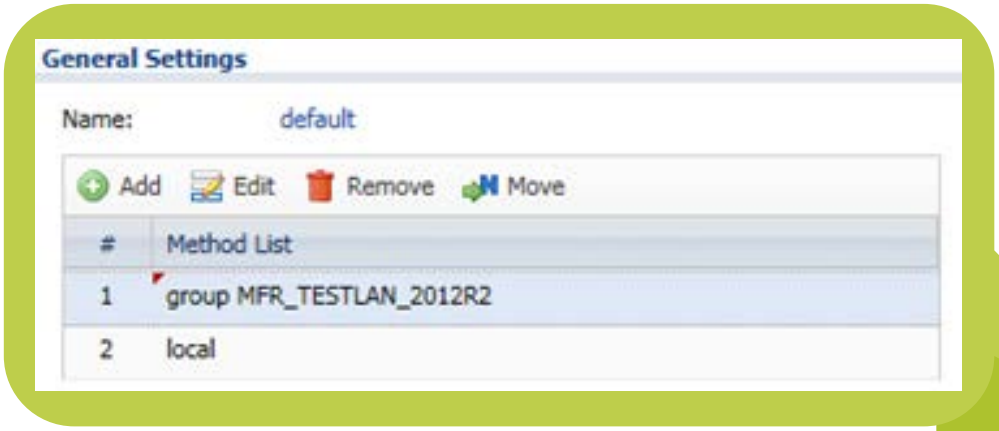
Username: mfr Test

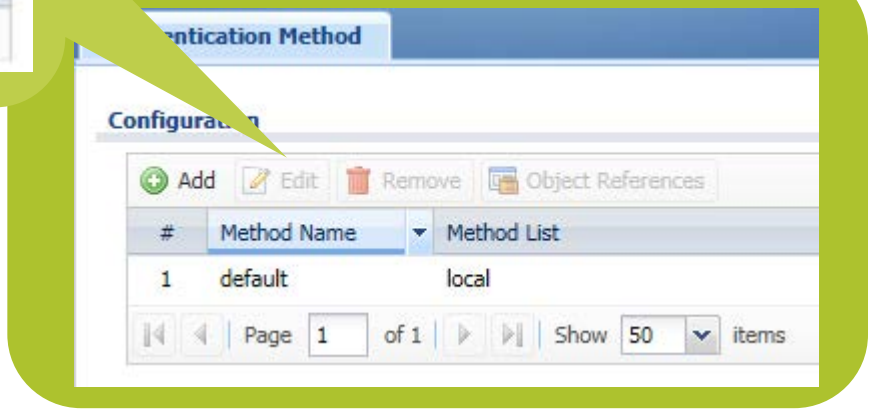
Returned User Attributes:

```
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

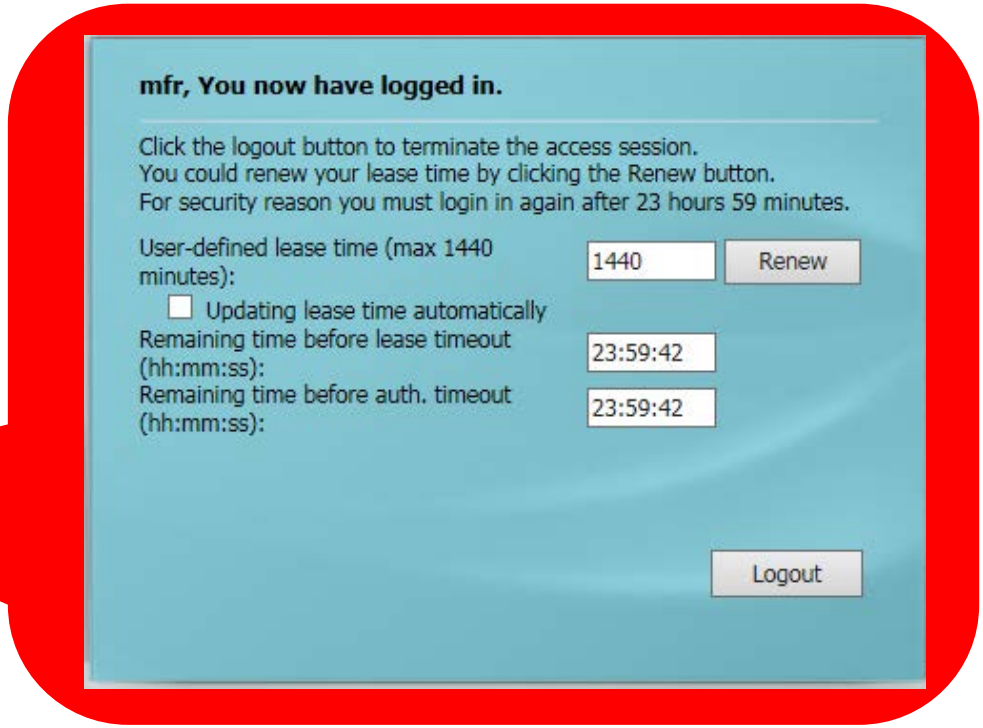




Zugangsprüfung erst gegen MS-AD und dann gegen die lokale DB der Firewall

Firewall MS-AD Anbindungseinstellungen

Login TEST



Firewall MS-AD Anbindungseinstellungen

LDAP Verbindung

3

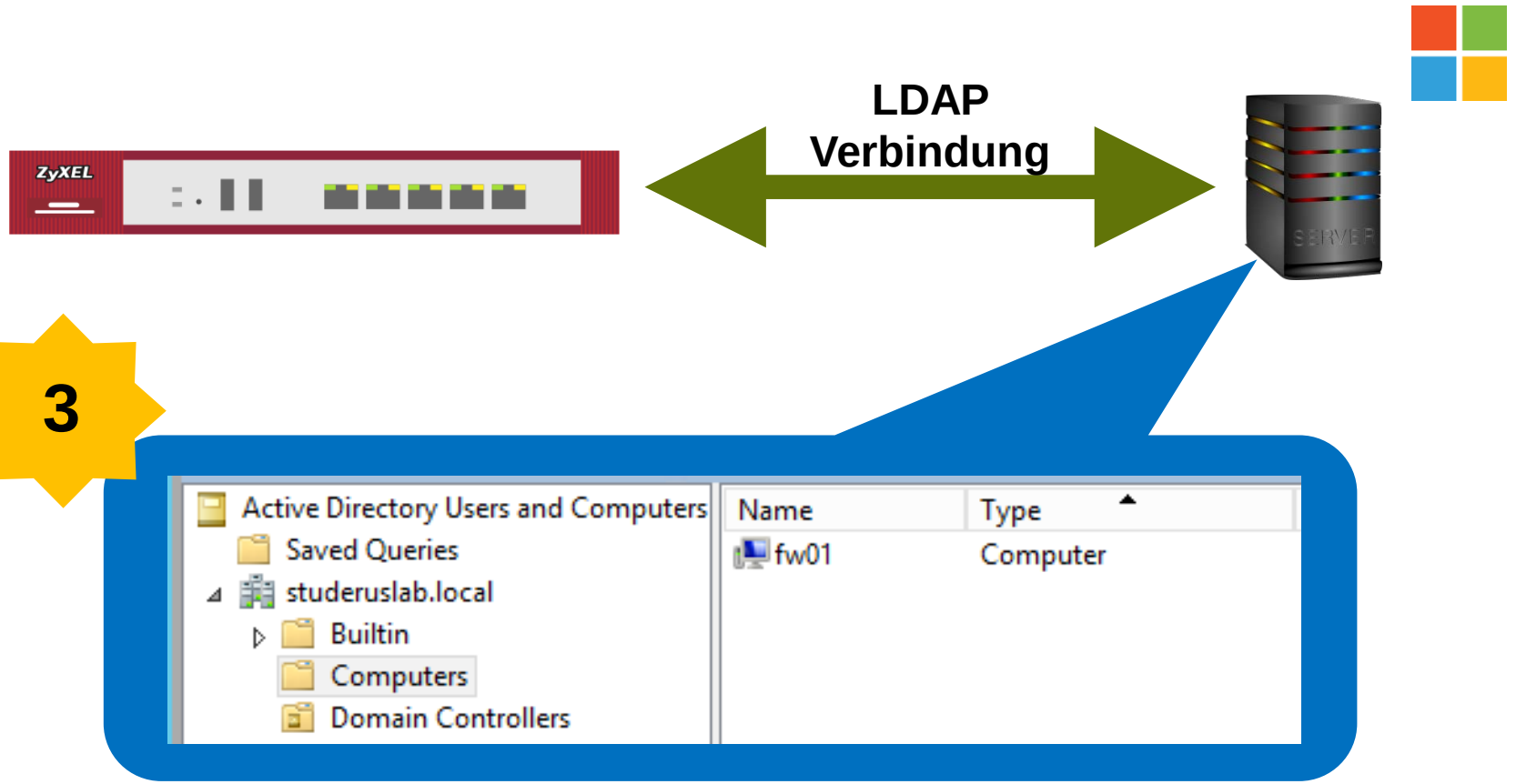
Domain Authentication for MSChap

Enable

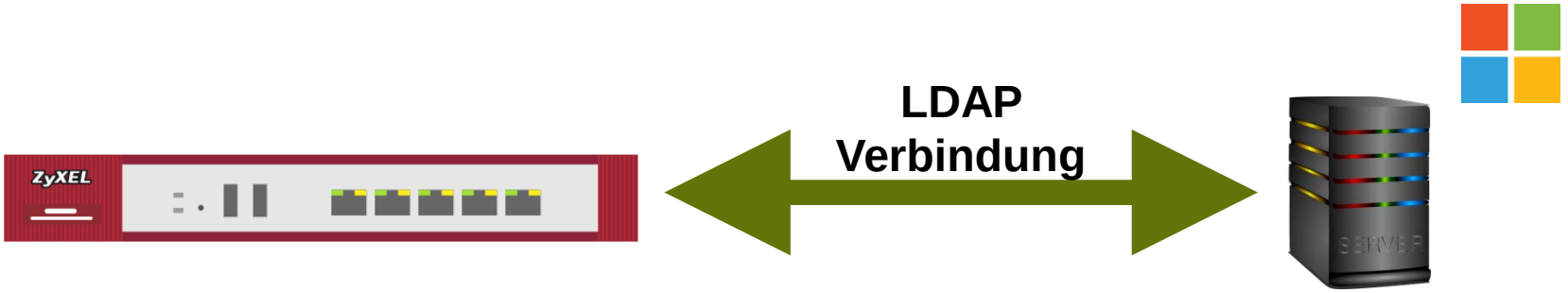
User Name:	manuel
User Password:	••••••••••••••••
Retype to Confirm:	••••••••••••••••
Realm:	studeruslab.local
NetBIOS Name:	studeruslab

Achtung: Primary-Gruppe «Domain Admin»

Firewall MS-AD Anbindungseinstellungen

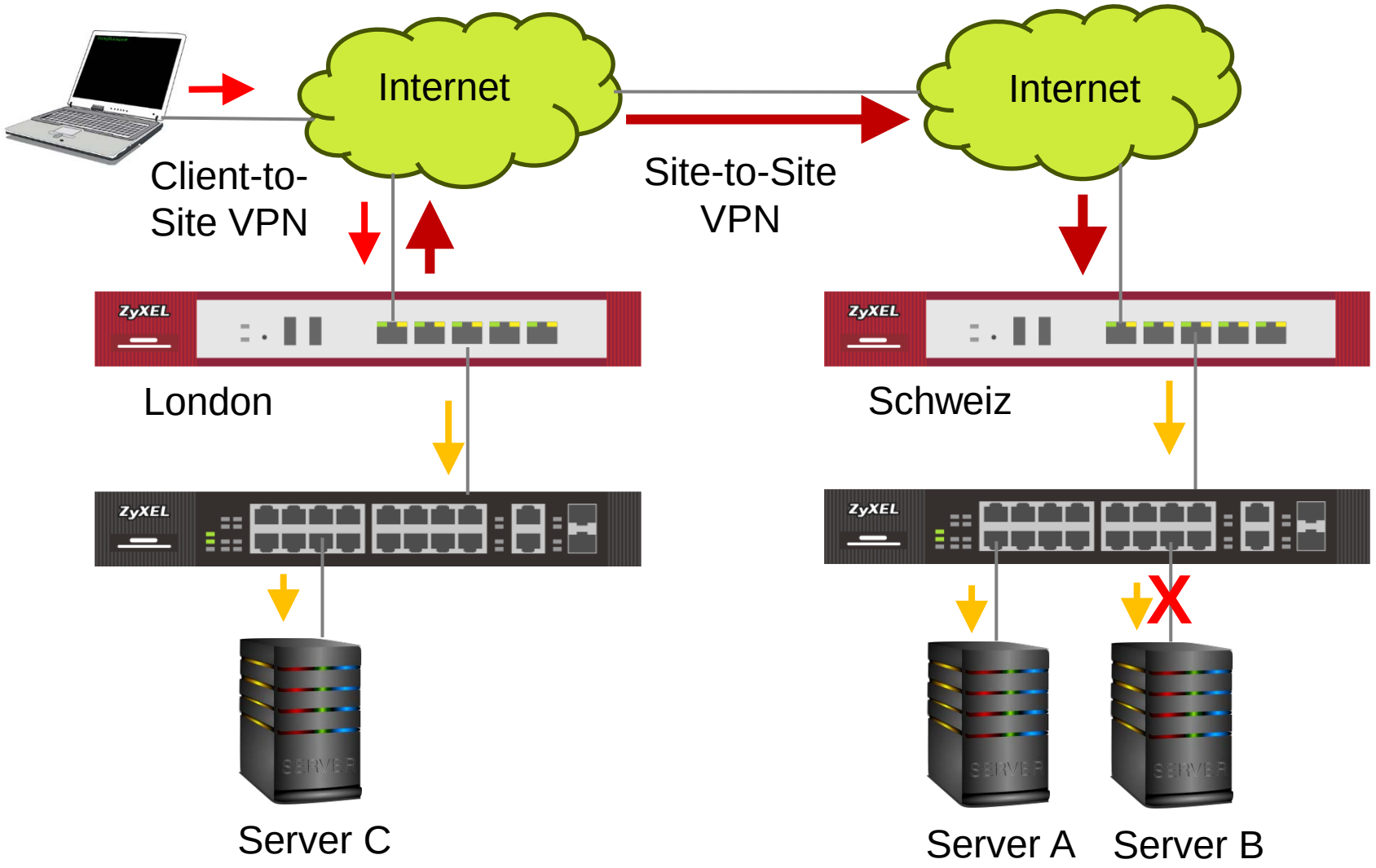


Firewall MS-AD Anbindungseinstellungen

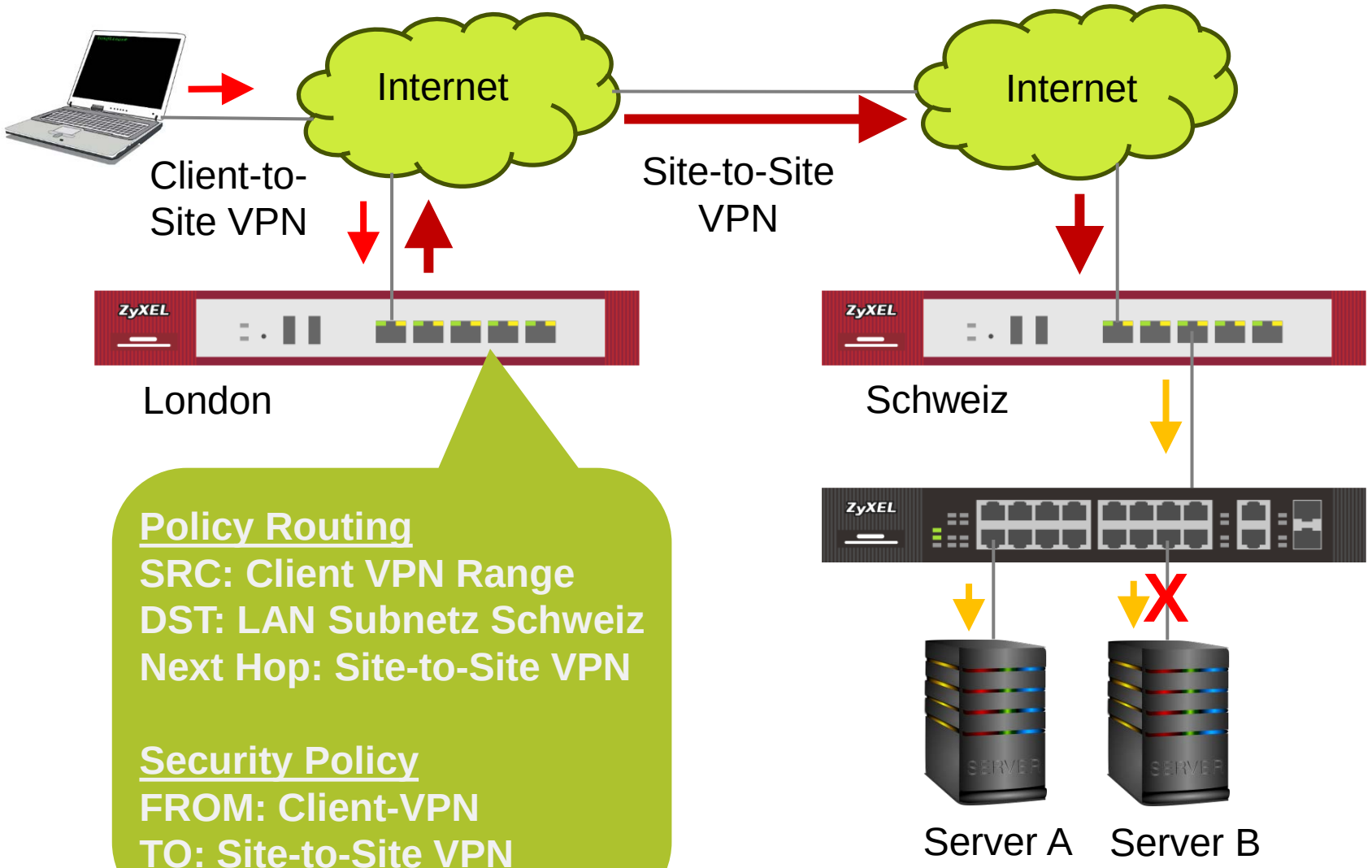


1. Eintrag AD-Server / IP AD Backup-Server (IP bevorzugt)
   BASE DN Einstiegspunkt der LDAP-Abfrage
   Standard Port 389, SSL verschlüsselt Port 636
2. BIND DN, LDAP Pfad für autorisierten User der Firewall-Attribute für sAM User und AD-Gruppen-Abfrage
3. Erweiterte Autorisierung für IKEv2 EAP-MSChapv2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

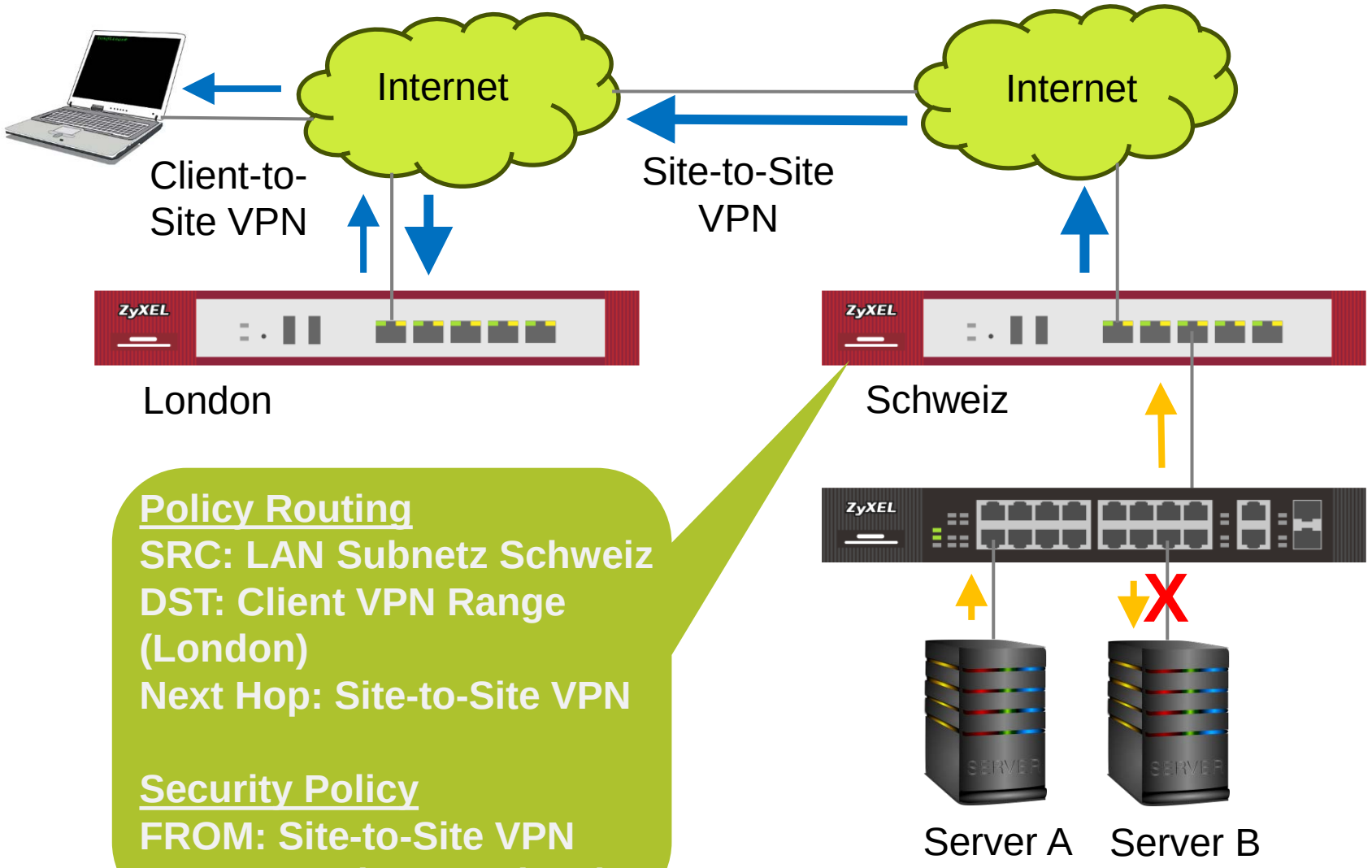
Client VPN – 1 Site-to-Site Hop - Overview



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



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

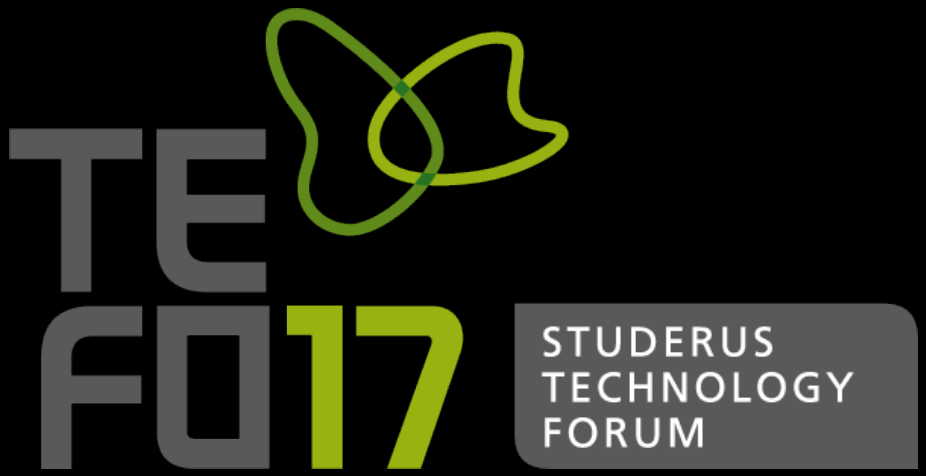


Fragen an die Referenten

TE FO17

Fragen?

STUDERUS
network technologies


TE
FO17
STUDERUS
TECHNOLOGY
FORUM