

# Little Big Topo

Eine gesamte Topologie über die Inhalte der 4. und 5. Klasse Netzwerktechnik

**Autor:** Albin Gashi

## Inhaltsverzeichnis

1	Einleitung .....	2
1.1	Umsetzung .....	2
1.2	Netzplan .....	3
2	Standort Wien .....	4
2.1	FortiGate .....	5
2.2	Active Directory .....	8
2.2.1	OUs, Benutzer und Gruppen .....	8
2.2.2	Berechtigungen auf dem DFS-Share .....	9
2.2.3	Group Policy Objects .....	11
2.2.4	Public-Key-Infrastructure .....	11
2.2.5	Jump-Server und PAW .....	12
2.2.6	IPAM .....	12
2.2.7	Device Hardening .....	13
3	Standort Heidleberg .....	14
3.1	pfSense .....	15
3.2	Active Directory .....	16
4	Konfiguration .....	16

# 1 Einleitung

Dieses Portfolio bietet einen detaillierten Einblick in die *Little Big Topo*, ein Abschlussprojekt im Fach Netzwerktechnik der HTL 3 Rennweg. Sie bündelt alle Inhalte der 4. und 5. Klasse Netzwerktechnik sowie dem Sub-Fach Operating System (OS).

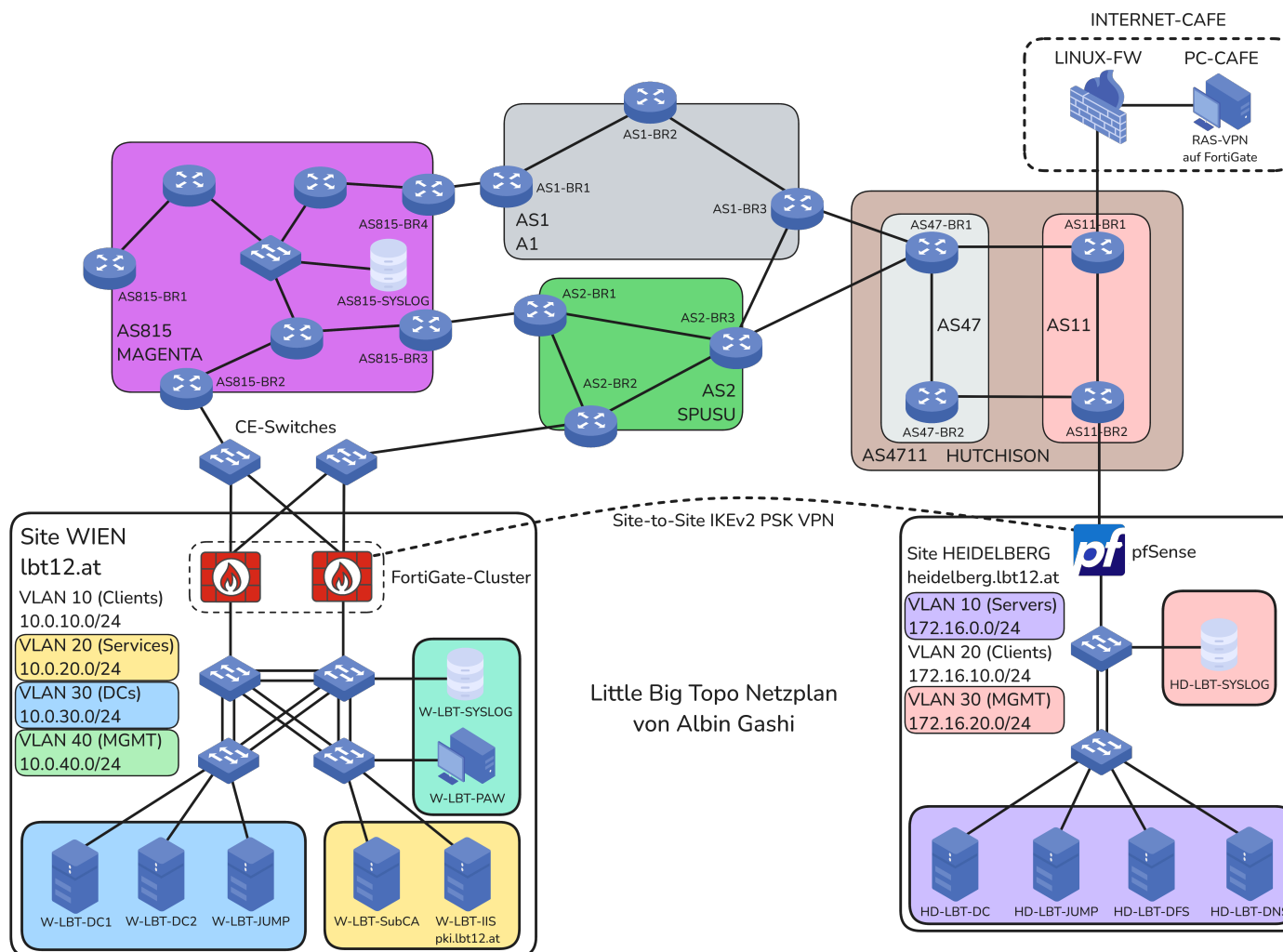
Das Dokument wurde mit [Typst](#) verfasst und basiert auf folgende Vorlage:

<https://codeberg.org/typst/htl3r>

## 1.1 Umsetzung

Die Umsetzung der *Little Big Topo* erfolgte über GNS3 und VMWare. Hierbei wurde der Bereich Netzwerktechnik in GNS3 und der Bereich Betriebssysteme in VMware realisiert. Um die Rechenleistung auszubalancieren wurden die virtuellen Maschinen auf zwei PCs aufgeteilt und mittels lokalen GNS3-Servern miteinander verbunden.

## 1.2 Netzplan



## 2 Standort Wien

Standort Wien bildet den zentralen Knotenpunkt des Unternehmens. Auf diesem Ort laufen die wichtigsten Dienste des Active-Directories. Zu diesen zählen eine PKI in Kombination mit IIS, DHCP, ein mithilfe von AGDLP umgesetzter Share und IPAM.

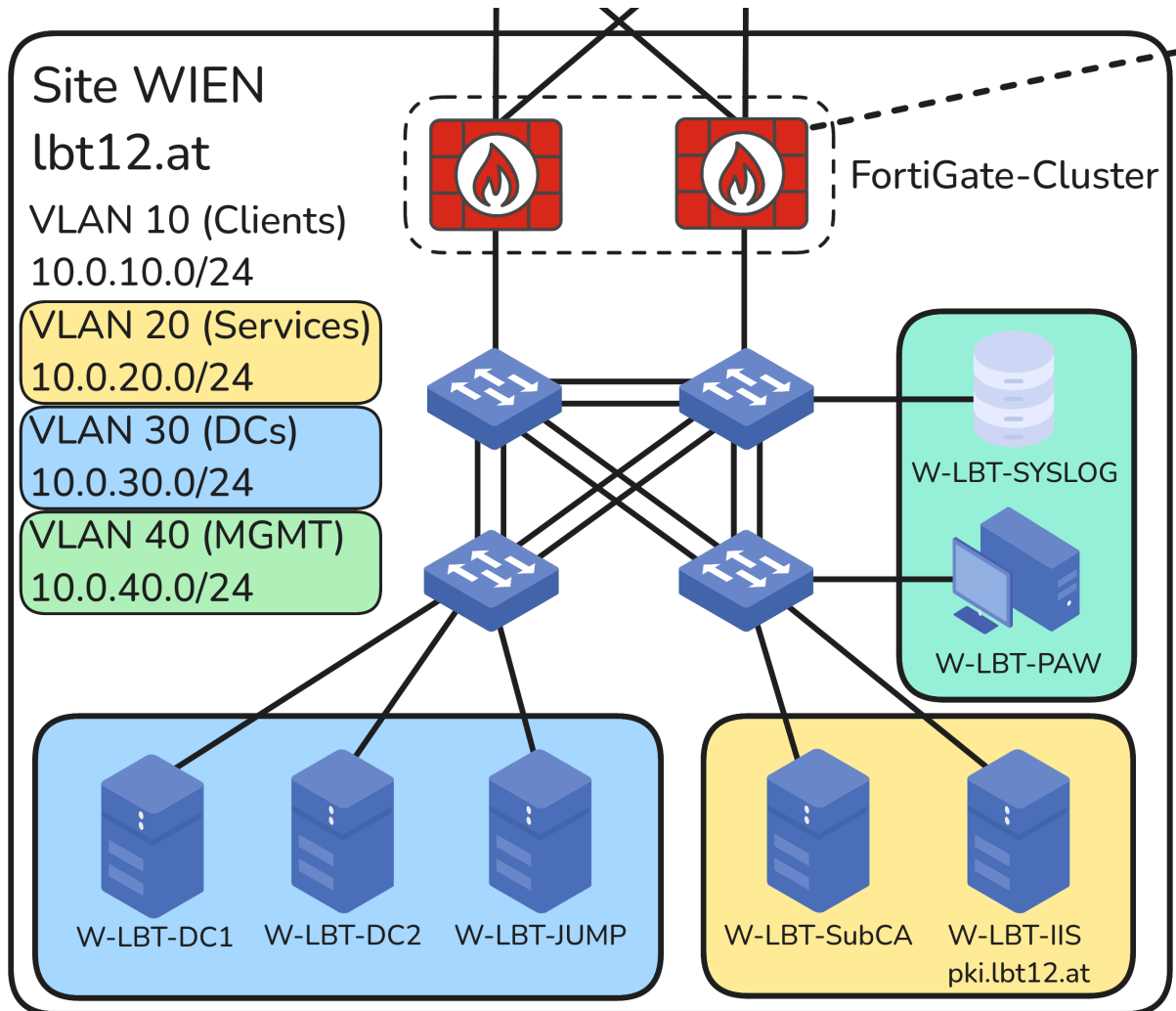


Abbildung 1: Aufbau des Standortes Wien

Das Netzwerk ist in vier VLANs mikrosegmentiert:

VLAN	Name	Description
10	CLIENTS	Alle Mitarbeiter-PCs
20	SERVICES	Für Services wie PKI & IIS
30	DC	Alle Domain-Controller inklusive JUMP-Server
40	MGMT	Management VLAN mit SYSLOG-Server und PAW

Tabelle 1: Mikrosegmentierung des Standorts Wien

## 2.1 FortiGate

An jeweils beiden Core-Switches ist eine FortiGate angeschlossen, die als HA-Cluster geformt ist. Hier stellt sich nun die Frage: an welchem Interface terminiert der Site-to-Site VPN? Hierfür wurde an der FortiGate ein Loopback-Interface konfiguriert und mithilfe von BGP an die beiden autonomen Systeme propagiert. Dadurch erreicht die pfSense über ihre ISP-Anbindung das Loopback Interface einer der beiden FortiGate, auch im Falle eines Ausfalls.

In einem HA-Cluster existieren Primary und Secondary Rollen. Die Secondary-FortiGate spricht über die Heartbeat-Ports mit der Primary-Rolle und aktualisiert damit die Konfiguration.

```
FGVM02TM25000701 login: secondary's external files are not in sync with the primary's, sequence:0. (type CERT_LOCAL)
secondary's external files are not in sync with the primary's, sequence:1. (type CERT_LOCAL)
secondary's external files are not in sync with the primary's, sequence:2. (type CERT_LOCAL)
secondary's external files are not in sync with the primary's, sequence:3. (type CERT_LOCAL)
secondary's external files are not in sync with the primary's, sequence:4. (type CERT_LOCAL)
secondary succeeded to sync external files with primary
```

Abbildung 2: Die Secondary-FortiGate beim synchronisieren der Konfiguration

Die FortiGate übernehmen das Inter-VLAN-Routing der Mikrosegmentierung. Hierfür wurden an einem Trunk-Interface die VLANs angelegt. Im folgenden Abbild sind die konfigurierten Interfaces zu sehen. An erster Stelle ist auch das vorher erwähnte Loopback-Interface aufgelistet.

```
W-LBT-FG # sh sys int
name      Name.
Loopback0 static 0.0.0.0 0.0.0.0 12.12.12.12 255.255.255.255 up disable loopback
W-LBT-CLIENTS static 0.0.0.0 0.0.0.0 10.0.10.254 255.255.255.0 up disable vlan
W-LBT-DC static 0.0.0.0 0.0.0.0 10.0.30.254 255.255.255.0 up disable vlan
W-LBT-MCD-VPN static 0.0.0.0 0.0.0.0 169.254.1.1 255.255.255.255 up disable tunnel
W-LBT-MGMT static 0.0.0.0 0.0.0.0 10.0.40.254 255.255.255.0 up disable vlan
W-LBT-SERVICES static 0.0.0.0 0.0.0.0 10.0.20.254 255.255.255.0 up disable vlan
W_to_HD static 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 up disable tunnel
fortilink static 0.0.0.0 0.0.0.0 10.255.1.1 255.255.255.0 up disable aggregate
l2t.root static 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 up disable tunnel
naf.root static 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 up disable tunnel
port1 dhcp 0.0.0.0 0.0.0.0 192.168.122.148 255.255.255.0 up disable physical
port2 static 0.0.0.0 0.0.0.0 12.3.0.2 255.255.255.0 up disable physical
port3 static 0.0.0.0 0.0.0.0 12.2.0.2 255.255.255.0 up disable physical
```

Abbildung 3: Die Interfaces der FortiGate W-LBT-FG

Sehen wir uns nun die BGP-Konfiguration an. Als AS-Nummer wurde 99 gewählt. Wie vorhin erwähnt, wird das Netz 12.12.12.12 via BGP an die Nachbarn von AS815 und AS2 verteilt.

```
W-LBT-FG # sh router bgp
config router bgp
  set as 99
  set router-id 12.12.12.12
  config neighbor
    edit "12.3.0.1"
      set next-hop-self enable
      set remote-as 815
    next
    edit "12.2.0.1"
      set next-hop-self enable
      set remote-as 2
    next
  end
  config network
    edit 1
      set prefix 12.12.12.12 255.255.255.255
    next
  end
```

Abbildung 4: BGP-Konfiguration an der FortiGate W-LBT-FG

Am Border-Router vom ISP Magenta sehen wir die BGP-Route in der ROuting-Tabelle aufscheinen.

```
AS815-BR2#show ip route bgp | include 12.
      12.0.0.0/8 is variably subnetted, 9 subnets, 2 masks
B      12.12.12.12/32 [20/0] via 12.3.0.2, 00:01:20
AS815-BR2#
```

Abbildung 5: BGP-Konfiguration an der FortiGate W-LBT-FG

Nun kann auch der VPN konfiguriert werden. Dafür werden für beide IKEv2 Phasen entsprechende Konfigurationen angelegt.

```
W-LBT-FG # sh vpn ipsec phase1-interface
config vpn ipsec phase1-interface
  edit "W_to_HD"
    set interface "Loopback0"
    set ike-version 2
    set local-gw 12.12.12.12
    set peertype any
    set net-device disable
    set proposal aes256-sha512
    set dhgrp 14
    set remote-gw 12.0.0.2
    set psksecret ENC r7sWCKIdn37wSsU2
    KvGrUT8ZwC/VAWgk0c++YQrQK6U99KNJssFMgEqSet
  next
```

Abbildung 6: IKEv2 Phase1-Konfiguration an der FortiGate W-LBT-FG

```
W-LBT-FG # sh vpn ipsec phase2-interface
config vpn ipsec phase2-interface
  edit "VIENNA-T0-HD"
    set phase1name "W_to_HD"
    set proposal aes256-sha512
    set dhgrp 14
    set src-subnet 10.0.30.0 255.255.255.0
    set dst-subnet 172.16.0.0 255.255.255.0
  next
  edit "W-LBT-MCD-VPN"
    set phase1name "W-LBT-MCD-VPN"
    set proposal aes128-sha1 aes256-sha1 aes
    set comments "VPN: W-LBT-MCD-VPN (Create
  next
```

Abbildung 7: IKEv2 Phase2-Konfiguration an der FortiGate W-LBT-FG

Zur guter Letzt dürfen Policies nicht fehlen. Besonders bei Inter-VLAN-Routing sind diese essenziell, um den Traffic zwischen den VLANs aufs nötigste zu limitieren. Die letzte Policy ist besonders für Jump-Server und PAW relevant, da dies den VLAN-übergreifenden Traffic nur mit der MAC-Adresse der PAW auf die MAC-Adresse des Jump-Servers zulässt (siehe Abschnitt 2.2.5). Des Weiteren sind für die Internet-Policy Malware- und Webfilter sowie SSL- und Signature-Based-Inspection konfiguriert. Dies wird beim Testen mit einem EICAR-File relevant.

Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Security Profiles
W-LBT-DC-to-SERVICES	Domain Controller (W-LBT-DC)	SERVICES (W-LBT-SERVICES)	W-LBT-DC address	W-LBT-SERVICES address	always	Windows AD	ACCEPT	Disabled	no-inspection
W-LBT-SERVICES-to-DC	SERVICES (W-LBT-SERVICES)	Domain Controller (W-LBT-DC)	W-LBT-SERVICES address	W-LBT-DC address	always	Windows AD	ACCEPT	Disabled	no-inspection
W-LBT-CLIENTS-to-DC	CLIENTS (W-LBT-CLIENTS)	Domain Controller (W-LBT-DC)	W-LBT-CLIENTS address	W-LBT-DC address	always	Windows AD DHCP	ACCEPT	Disabled	no-inspection
W-LBT-DC-to-CLIENTS	CLIENTS (W-LBT-CLIENTS)	Domain Controller (W-LBT-DC)	W-LBT-DC address	W-LBT-CLIENTS address	always	Windows AD DHCP	ACCEPT	Disabled	no-inspection
HD-Servers_to_W-DC	W_to_HD	Domain Controller (W-LBT-DC)	HD-LBT-SERVERS	W-LBT-DC address	always	ALL_ICMP Windows AD	ACCEPT	Disabled	no-inspection
W-DC-to-HD-SERVERS	Domain Controller (W-LBT-DC) to_W-LBT (port4)	W_to_HD	W-LBT-DC address	HD-LBT-SERVERS	always	Windows AD ALL_ICMP	ACCEPT	Disabled	no-inspection
W-LBT-to-INET	CLIENTS (W-LBT-CLIENTS) Domain Controller (W-LBT-DC) SERVICES (W-LBT-SERVICES)	INTERNET (port1)	W-LBT-CLIENTS address W-LBT-DC address W-LBT-SERVICES address	all	always	ALL	ACCEPT	Enabled	W-LBT-MALWARE W-LBT-Webfilter W-LBT-SBD W-LBT-SSL-Inspection
VPN-to-Lo0	to_ISP1 (port2) to_ISP2 (port3)	Loopback0	all	all	always	BGP ESP IKE PING	ACCEPT	Disabled	no-inspection
W-LBT-DC-to_MGMT	Domain Controller (W-LBT-DC)	Management (W-LBT-MGMT)	W-LBT-DC address	W-LBT-MGMT address	always	PROMETHEUS SYSLOG	ACCEPT	Enabled	no-inspection
vpn_W-LBT-MCD-VPN_remote_0	W-LBT-MCD-VPN	CLIENTS (W-LBT-CLIENTS)	W-LBT-MCD-VPN_range	W-LBT-CLIENTS address	always	ALL	ACCEPT	Enabled	no-inspection
W-LBT-PAW-to-JUMP	CLIENTS (W-LBT-CLIENTS)	Domain Controller (W-LBT-DC)	W-LBT-PAW	W-LBT-DC address	always	RDP	ACCEPT	Disabled	no-inspection

Abbildung 8: Policies an der FortiGate W-LBT-FG

## 2.2 Active Directory

### 2.2.1 OUs, Benutzer und Gruppen

Für die OU-Struktur wurde sich an die Mikrosegmentierung der VLANs orientiert. Dabei werden Server in Services und Domain Controllers eingeteilt. Für die Gruppen wird in Global und Domain Local unterschieden. Die Benutzer werden entsprechend ihren Abteilungen zugeteilt (inkl. Protected Users). In W-LBT-DC1 und wW-LBT-DC2 (siehe Abschnitt 4) werden die Powershell-Scripts für das automatische Anlegen der Benutzer, Gruppen und OUs sowie die Konfiguration der Domain-Controller aufgelistet.



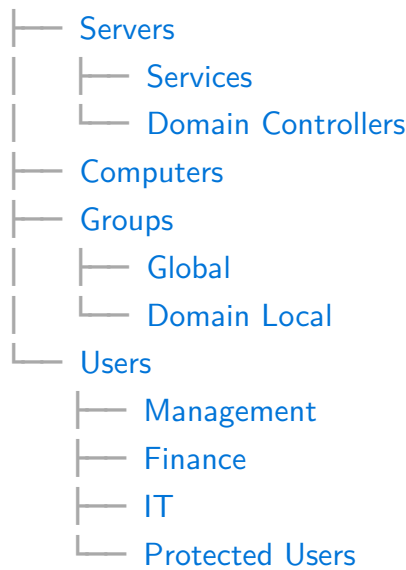


Abbildung 9: Die OU-Struktur von lbt12.at und heidelberg.lbt12.at

Benutzername	Name	Gruppe
smueller	Sarah Müller	IT, Protected Users
mschmidt	Markus Schmidt	Management
lweber	Lena Weber	Finanzen

Tabelle 2: Die Benutzer der Domäne lbt12.at

### 2.2.2 Berechtigungen auf dem DFS-Share

Den Usern wurde mittels AGDLP Berechtigungen auf dem DFS-Share erteilt. Dabei erhält jede globale Gruppe eine Domain Local Gruppe mit spezifischen Berechtigungen wie Read oder Write.

```
PS C:\Users\Administrator> get-acl \\W-LBT-IIS\Share\1_Finzen | Format-Table -wrap

Directory: \\W-LBT-IIS\Share

Path      Owner      Access
-----
1_Finzen  BUILTIN\Administrators LBT12\DL_1_Finzen_R Allow ReadAndExecute, Synchronize
          LBT12\DL_1_Finzen_M Allow Modify, Synchronize
          LBT12\DL_2_Management_R Allow ReadAndExecute, Synchronize
          LBT12\DL_3_IT_R Allow ReadAndExecute, Synchronize
          LBT12\DL_3_IT_M Allow Modify, Synchronize
          LBT12\Administrator Allow FullControl
          BUILTIN\Administrators Allow FullControl
          NT AUTHORITY\SYSTEM Allow FullControl
```

Abbildung 10: Befehlsausgabe von *Get-ACL* für den Finanzen-Ordner

```
PS C:\Users\Administrator> get-acl \\W-LBT-IIS\Share\2_Management | Format-Table -wrap

Directory: \\W-LBT-IIS\Share

Path      Owner      Access
-----
2_Management BUILTIN\Administrators LBT12\DL_2_Management_R Allow ReadAndExecute, Synchronize
          LBT12\DL_2_Management_M Allow Modify, Synchronize
          LBT12\DL_3_IT_R Allow ReadAndExecute, Synchronize
          LBT12\DL_3_IT_M Allow Modify, Synchronize
          LBT12\Administrator Allow FullControl
          BUILTIN\Administrators Allow FullControl
          NT AUTHORITY\SYSTEM Allow FullControl
```

Abbildung 11: Befehlsausgabe von *Get-ACL* für den Management-Ordner

```
PS C:\Users\Administrator> get-acl \\W-LBT-IIS\Share\3_IT | Format-Table -wrap

Directory: \\W-LBT-IIS\Share

Path Owner      Access
-----
3_IT BUILTIN\Administrators LBT12\DL_3_IT_R Allow ReadAndExecute, Synchronize
          LBT12\DL_3_IT_M Allow Modify, Synchronize
          LBT12\Administrator Allow FullControl
          BUILTIN\Administrators Allow FullControl
          NT AUTHORITY\SYSTEM Allow FullControl
```

Abbildung 12: Befehlsausgabe von *Get-ACL* für den IT-Ordner

### 2.2.3 Group Policy Objects

In der folgenden Tabelle werden alle implementierten GPOs und ihre Funktion aufgelistet:

GPO	Funktion	verknüpft
DriveMount	Mountet den DFS-Share automatisch an den Clients an	lbt12.at
LastUserNotShown	Am Login-Screen der Mitarbeiter-PCs werden keine anderen User angezeigt	lbt12.at
DesktopWallpaper	Setzt für alle PCs ein einheitliches Desktop-Wallpaper	lbt12.at
LogonScreen	Setzt für alle PCs ein einheitliches Login-Wallpaper	lbt12.at
PasswordPolicy	Setzt für alle Benutzer eine Mindestlänge und Komplexität für Passwörter voraus	lbt12.at
LocalFirewall	Aktiviert die Lokale Firewall an den PCs und blockiert ICMP	lbt12.at
AutoCertEnroll	Installiert automatisch an allen Clients die Root- und Sub-CA-Zertifikate	lbt12.at
Audits	Setzt Advanced Audit Policies für besseres Logging im Event Viewer	lbt12.at
CredentialGuard	Aktiviert den Credential Guard für PAW und DCs	DCs, PAW
PAW_AppLocker	Limitiert bestimmte Apps (z.B. Powershell) für die PAW-Workstation	PAW

Tabelle 3: Die Benutzer der Domäne lbt12.at

### 2.2.4 Public-Key-Infrastructure

Auf dem Standort Wien wird eine Two-Tier-PKI betrieben. Dabei ist die Root-CA vom Netzwerk vollkommen abgekoppelt und die Sub-CA übernimmt die Aufgaben der Zertifikats-

ausstellungen. Mithilfe eines IIS-Webserver werden den PCs über dem Verzeichnis <https://pki.lbt12.at/CertEnroll> die Zertifikate bereitgestellt. Des Weiteren wird mittels GPO allen Mitarbeiter-PCs automatisch die Root- und Sub-CA-Zertifikate installiert. Der Webserver ist mit einem SSL-Zertifikat ausgestattet.

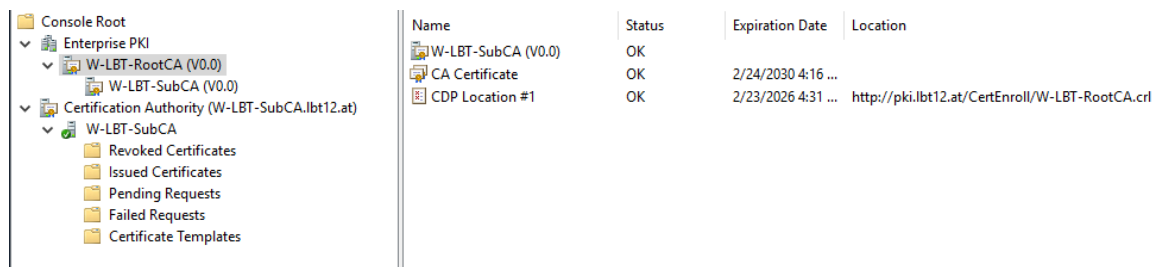


Abbildung 13: Auszug aus der PKIView von W-LBT-SubCA

## 2.2.5 Jump-Server und PAW

Der Standort Wien wird über einen Jump-Server administriert, der nur durch eine Priviledged Access Workstation (kurz PAW) über RDP erreichbar ist. Die PAW befindet sich im Management-VLAN, dass vom Internet abgekoppelt ist. Zusätzlich wird an der FortiGate über Inter-VLAN-Routing nur die MAC-Adresse der PAW zugelassen, um zum Jump-Server zu gelangen. Auf der PAW werden über AppLocker Dienste wie Powershell gesperrt, um die weitere Sicherheit zu gewährleisten.

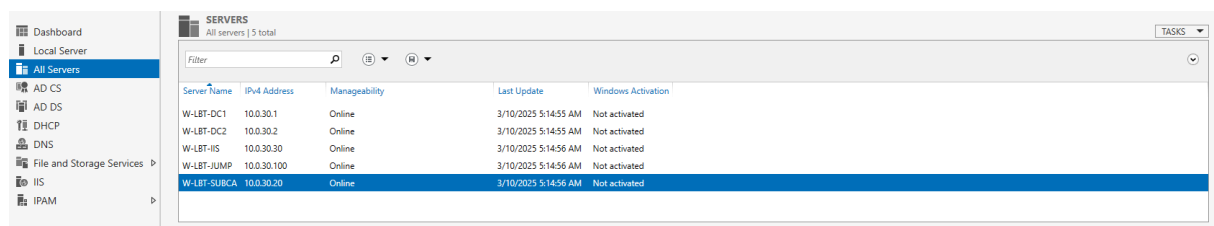
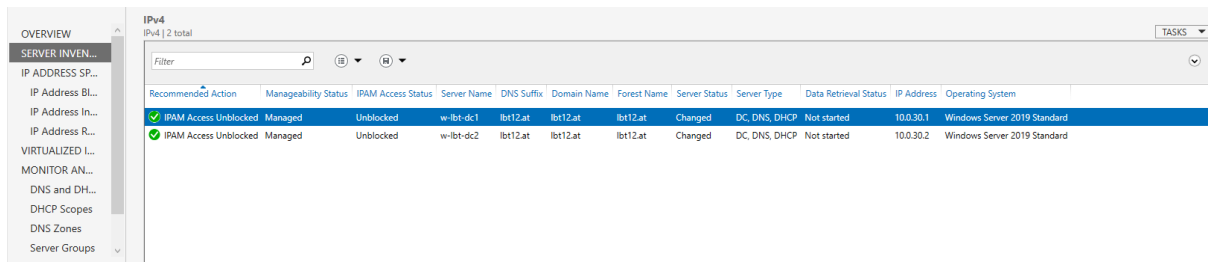


Abbildung 14: Auszug aus dem Server-Manager von W-LBT-JUMP

## 2.2.6 IPAM

Zur besseren Übersicht auf das Unternehmensnetzwerk wurde am JUMP-Server IPAM implementiert.



Recommended Action	Manageability Status	IPAM Access Status	Server Name	DNS Suffix	Domain Name	Forest Name	Server Status	Server Type	Data Retrieval Status	IP Address	Operating System
IPAM Access Unblocked	Managed	Unblocked	w-lbt-dc1	lbt12.at	lbt12.at	lbt12.at	Changed	DC, DNS, DHCP	Not started	10.0.30.1	Windows Server 2019 Standard
IPAM Access Unblocked	Managed	Unblocked	w-lbt-dc2	lbt12.at	lbt12.at	lbt12.at	Changed	DC, DNS, DHCP	Not started	10.0.30.2	Windows Server 2019 Standard

Abbildung 15: Auszug aus dem IPAM-Dashboard von W-LBT-JUMP

## 2.2.7 Device Hardening

Trotz der Mikrosegmentierungen müssen die Geräte selbst ebenfalls gehärtet werden. Dabei wurden die Domain-Controller sowie die PAW näher betrachtet. Als erstes wurde ein Credential Guard implementiert, wie es auch bei GPOs in Abschnitt 2.2.3 aufgelistet ist. Dafür wurden die virtuellen Maschinen mit TPM verschlüsselt und anschließend der Credential Guard angewendet.

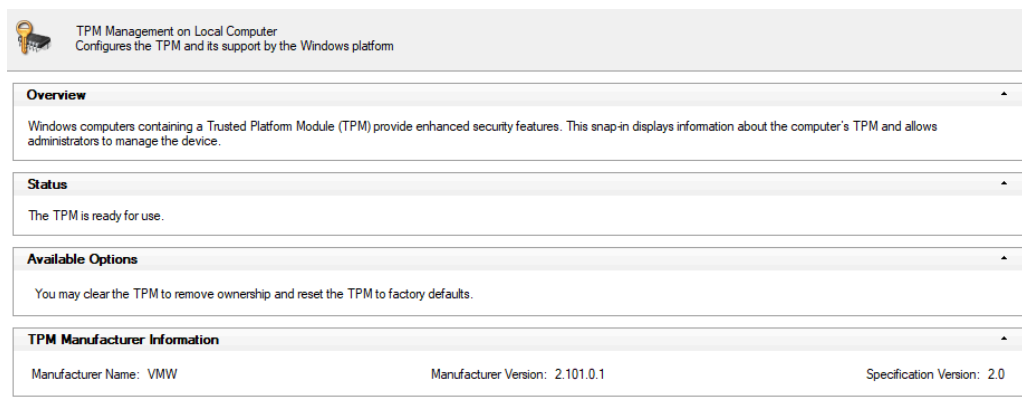


Abbildung 16: Das aktivierte TPM auf der PAW

Zusätzlich wurde für die PAW eine Local Administrator Password Solution angewendet. Nach der Installation und der Implementierung der GPO wurde es auf dem Jump-Server mit folgenden Befehlen getestet:

```
PS C:\Users\Administrator.LBT12> Get-AdmPwdPassword -ComputerName "W-LBT-PAW"
ComputerName      DistinguishedName      Password      ExpirationTimestamp
-----
W-LBT-PAW         CN=W-LBT-PAW,OU=Special Accounts,OU=Vienna... 4(3Y54$+e-    4/27/2025 3:52:26 AM
PS C:\Users\Administrator.LBT12>
```

Abbildung 17: Ausgabe des Administratorpassworts von der PAW

### 3 Standort Heidelberg

Der Standort Heidelberg bildet mit einer Child-Domain eine weitere administrative Organisationseinheit im Unternehmen LBT12. Sie besitzt eine pfSense als Firewall und verbindet sich mit dem Standort Wien über einen plattformübergreifenden Site-to-Site VPN via PSK.

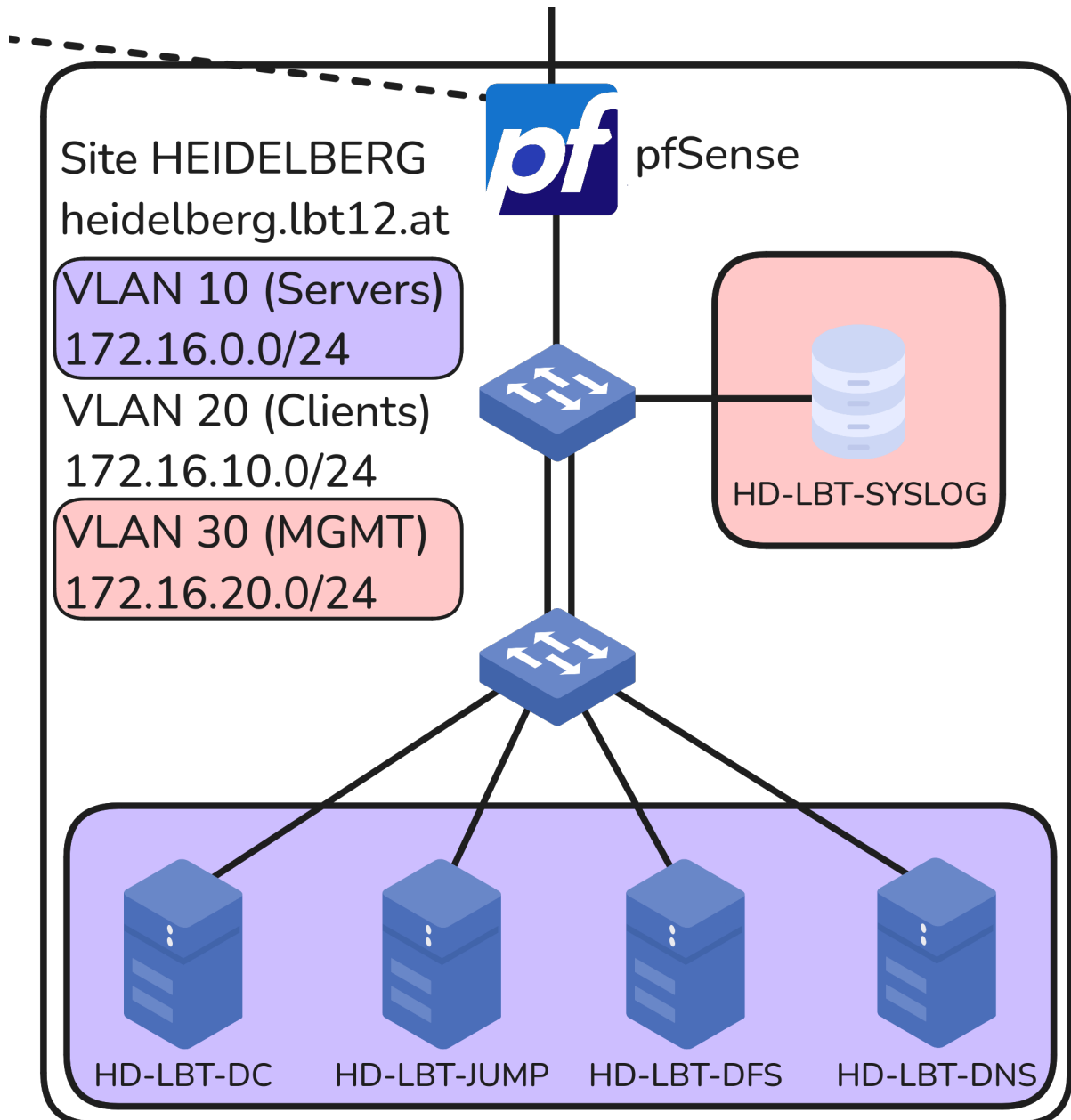


Abbildung 18: Aufbau des Standortes Heidelberg

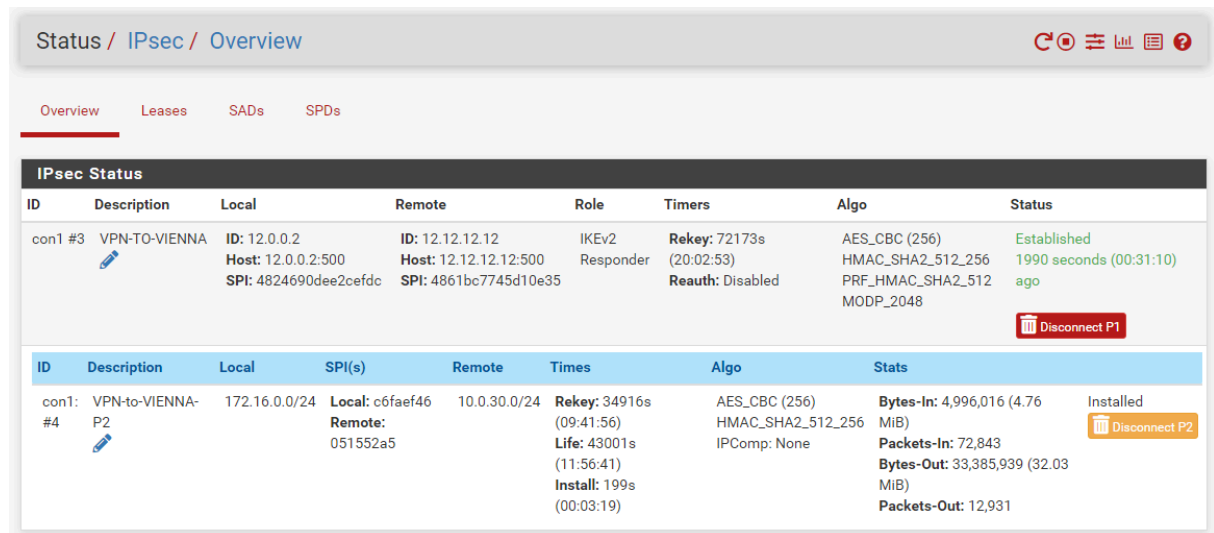
Die Geräte des Standorts wurden in VLANs segmentiert und über die pfSense mittels Inter-VLAN-Routing verbunden.

VLAN	Name	Description
10	CLIENTS	Alle Mitarbeiter-PCs
20	SERVERS	Alle Server der Site Heidelberg
30	MGMT	SYSLOG, RSPAN und Netflow

Tabelle 4: VLANs des Standort Heidelberg

### 3.1 pfSense

Als Firewall am Standort Heidelberg wurde eine pfSense implementiert. Sie führt, wie am Standort Wien, ebenfalls das Inter-VLAN-Routing durch. Gemeinsam mit der FortiGate baut sie den Site-to-Site VPN für die Site-Replikation auf.



IPsec Status							
ID	Description	Local	Remote	Role	Timers	Algo	Status
con1 #3	VPN-TO-VIENNA	ID: 12.0.0.2 Host: 12.0.0.2:500 SPI: 4824690dee2cefdc	ID: 12.12.12.12 Host: 12.12.12.12:500 SPI: 4861bc7745d10e35	IKEv2 Responder	Rekey: 72173s (20:02:53) Reauth: Disabled	AES_CBC (256) HMAC_SHA2_512_256 PRF_HMAC_SHA2_512 MODP_2048	Established 1990 seconds (00:31:10) ago <span>Disconnect P1</span>
ID	Description	Local	SPI(s)	Remote	Times	Algo	Stats
con1: #4	VPN-to-VIENNA-P2	172.16.0.0/24	Local: c6faef46 Remote: 051552a5	10.0.30.0/24	Rekey: 34916s (09:41:56) Life: 43001s (11:56:41) Install: 199s (00:03:19)	AES_CBC (256) HMAC_SHA2_512_256 IPComp: None	Bytes-In: 4,996,016 (4.76 MiB) Packets-In: 72,843 Bytes-Out: 33,385,939 (32.03 MiB) Packets-Out: 12,931 Installed <span>Disconnect P2</span>

Abbildung 19: Auszug aus dem pfSense-Dashboard für den IPsec-VPN

## 3.2 Active Directory

In Heidelberg wird ein Domain Controller mit einem Jump-Server zur besseren Administration betrieben. Zusätzlich dazu steht ein BIND9-Server als DNS-Forwarder inklusive Caching bereit. Der DFS-Server repliziert den Share des Standort Wien.

```
PS C:\Users\Administrator> Get-ADReplicationSite

Description           :
DistinguishedName     : CN=Wien,CN=Sites,CN=Configuration,DC=lbt12,DC=at
InterSiteTopologyGenerator : CN=NTDS Settings,CN=W-LBT-DC1,CN=Servers,CN=Wien,CN=Sites,CN=Configuration,DC=lbt12,DC=at
ManagedBy            :
Name                  : Wien
ObjectClass            : site
ObjectGUID            : 84464450-946c-4c38-8c07-e9cb6acc8fac
ReplicationSchedule    : System.DirectoryServices.ActiveDirectory.ActiveDirectorySchedule
UniversalGroupCachingRefreshSite :
```

Abbildung 20: Befehlsausgabe von *Get-ADReplicationSite* für den Site-Link WIEN-HEIDELBERG

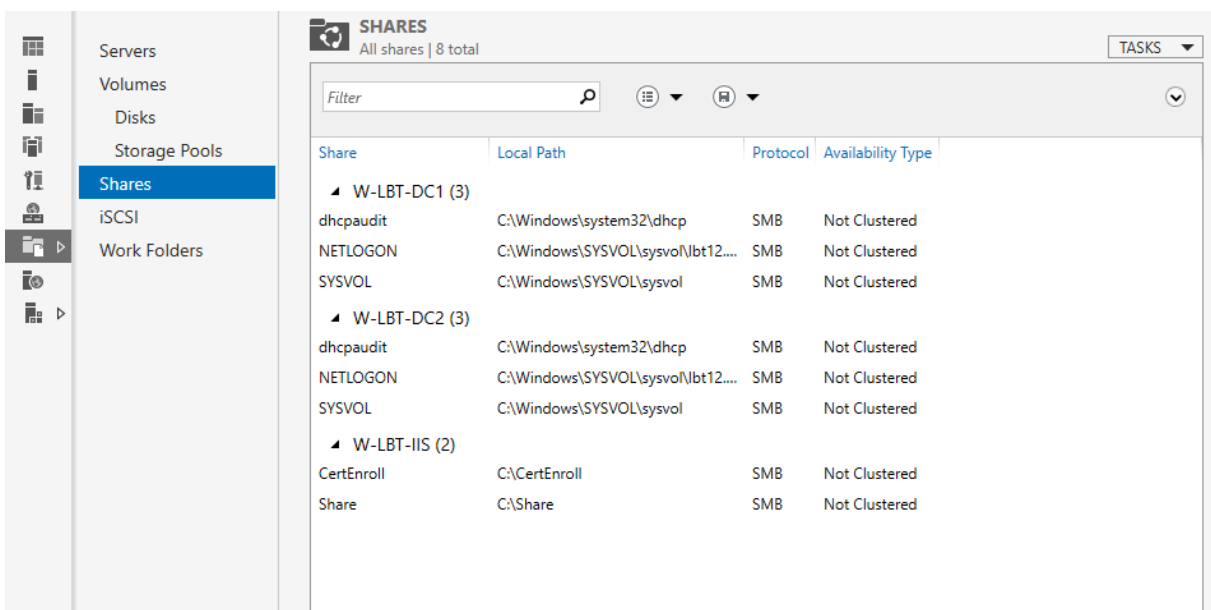


Abbildung 21: Die Shares der Active-Directory-Struktur im Überblick

## 4 Konfiguration

Alle Scripts sind auf <https://github.com/gjashni/LBT> zu finden.