

Dokumentationsbuch

Little Big Topo Team 4

durch

David Koch
Julian Burger

unter Anleitung von

Christian Schöndorfer
Clemens Kussbach

Wien, 12.03.2025

Inhaltsverzeichnis

1 Einführung	5
1.1 Ausgangssituation	5
1.2 Firma Backstory	5
1.3 Topologie	5
1.4 Verwendete Geräte & Software	6
2 Backbone	8
2.1 Namenskonvention	8
2.2 Addressbereiche	8
2.3 Autonome Systeme	9
2.3.1 AS20	9
2.3.2 AS100	10
2.3.3 AS666	10
2.4 Dynamisches Routing	12
2.4.1 Authentifizierung	12
2.5 Statisches Routing	13
3 Firewalls	14
3.1 FortiGate	14
3.1.1 Grundkonfiguration	14
3.1.2 Interfaces	14
3.1.3 Lizenzierung	16
3.1.4 Policies	16
3.1.5 HA Cluster	17
3.1.6 NAT	18
3.1.7 DHCP	19
3.1.8 VPNs	20
3.1.9 Captive Portal	20
3.1.10 SSL Inspection	21
3.1.11 Traffic Shaping	21
3.1.12 Webfilter	23
3.1.13 BGP	24
3.1.14 Sonstiges	24
3.2 PfSense	25
3.3 Cisco Router	26

3.3.1 FlexVPN	26
3.3.2 MPLS Overlay VPN	27
4 Standorte	28
4.1 Wien Favoriten	28
4.1.1 VLANs	29
4.1.2 Geräte	29
4.1.3 Features	30
4.2 Langenzersdorf	32
4.2.1 VLANs	32
4.2.2 Geräte	33
4.2.3 Features	34
4.3 Kebapci	36
4.4 Praunstraße	36
4.4.1 Private VLANs	37
4.5 Flex-Standorte	38
4.5.1 EIGRP	39
4.6 Armut-Standorte	39
4.7 Viktor-Standort	39
4.7.1 Linux-Firewall	40
5 Active Directory	42
5.1 Überblick	42
5.2 Geräte	42
5.2.1 Domain Controller	42
5.2.2 Jump Server	43
5.2.3 CA + PKI	43
5.2.4 NPS	43
5.2.5 Workstations	43
5.3 PowerShell Konfiguration	44
5.4 Users & Computers	46
5.5 PKI	47
5.5.1 CA Konfiguration	47
5.5.2 IIS Konfiguration	49
5.6 NPS	49
5.7 DFS	50
5.8 GPOs	50
5.8.1 Security Baseline	50
5.8.2 LAPS	50

A Gesamte logische Topologie	51
B Cisco-Gerät Grundkonfiguration	53
Abkürzungsverzeichnis	54
Glossar	56
Literaturverzeichnis	57

1 Einführung

Dies ist die Dokumentation des „Little Big Topo“-Projekts der 5ten Klasse Informationstechnologie im Ausbildungszweig Netzwerktechnik der HTL Rennweg. In den folgenden Kapiteln wird ein Überblick über die eingesetzten Konzepte und die für ihre Umsetzung nötigen Konfigurationsschritte geboten.

1.1 Ausgangssituation

Die „Little Big Topo“ ist eine Aufgabenstellung, die den Entwurf und die Umsetzung einer Topologie, die alle mögliche Features, die in den letzten zwei Jahren im Rahmen des NWT-Unterrichts gelernt worden sind, umfasst.

1.2 Firma Backstory

Gartenbedarfs GmbH

CEO: Huber „Huber“ Huber

Verkauft u.a. die Rasensprengerköpfe „Sprühkönig“ und „Sprengmeister“ als auch den Stoff „Huberit“.

Die Mitarbeiter der Gartenbedarfs GmbH gehen gerne in ihren Mittagspausen u.a. zu Kebapci fressen, aber die Gartenbedarfs GmbH ist heimlich mit Kebapci geschäftlich und infrastrukturtechnisch verwickelt, da Kebapci als Front für die Schwarzarbeit und Geldwäsche der Gartenbedarfs GmbH genutzt wird.

1.3 Topologie

Die gesamte Topologie besteht insgesamt aus 40 Netzwerkgeräten und 28 Endgeräten. Alle Geräte innerhalb der Topologie werden auf zwei Echtgeräten virtualisiert.

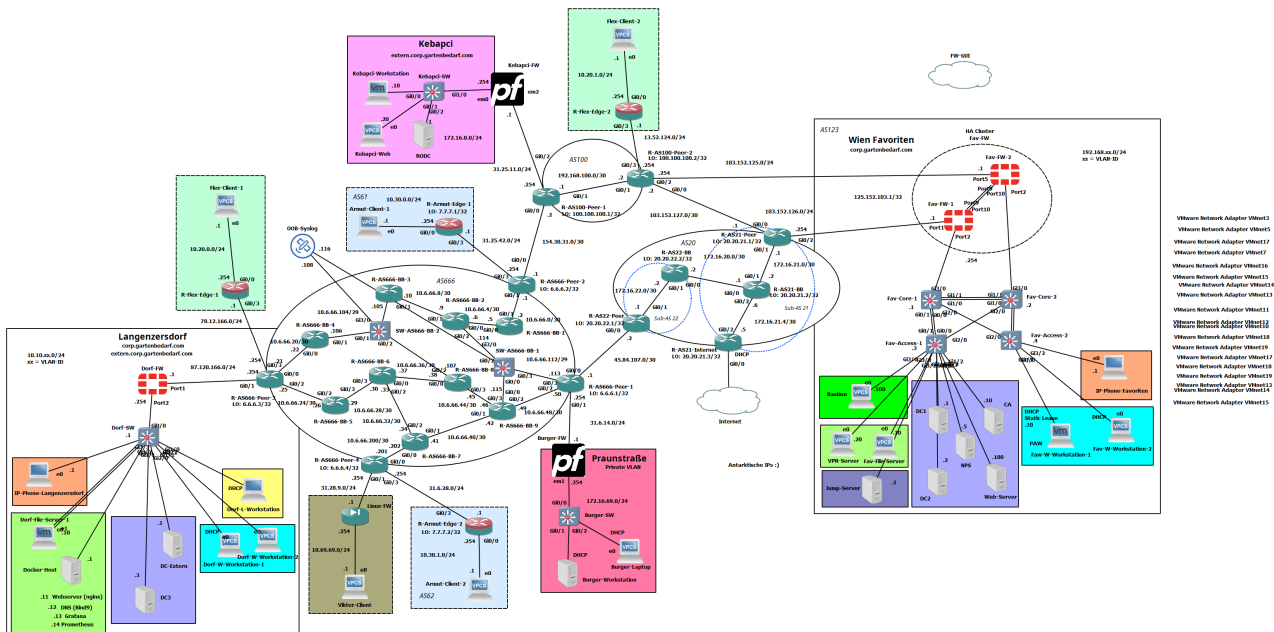


Abbildung 1.1: Der logische Topologieplan (v9)

(Für eine größere Ansicht des logischen Topologieplans siehe Appendix A)

Der Zugang ins Internet ist durch die Anbindung einer NAT^[1]-Cloud an AS^[2]20 bzw. AS21 ermöglicht worden.

1.4 Verwendete Geräte & Software

Für den Aufbau der Topologie wurde folgende Software verwendet:

- GNS3 v2.2.53
- VMware Workstation 17
- Cisco vIOS Switch & Router Images
- PfSense Linux Firewalls
- FortiGateVM
- VPCS

Die physischen Geräte, auf denen die Topologie läuft, sind zwei OptiPlex Tower Plus 7020 Desktop-PCs im Raum 076. Auf Arbeitsplatz 3 läuft die GNS3-VM mit den Netzwerkgeräten, auf Arbeitsplatz 4 laufen in VMware Workstation alle Endgeräte.

^[1]Network Address Translation: Die Veränderung einer privaten IP-Adresse auf eine öffentliche, um die von ihr geschickten Daten im Internet routbar zu machen.

^[2]Autonomes System: TODO

Um die zwei miteinander zu verbinden, wurde in GNS die IP-Adresse von Arbeitsplatz 4 als Remote-Server eingetragen und nach einem erfolgreichen Verbindungsaufbau werden VMnet Adapter in GNS3 verwendet, um die Endgeräte in die bestehende GNS-Topologie einzubinden und eine Konnektivität zwischen den Geräten herzustellen.

Zur Erstellung der Dokumentation wurden Typst und die Online-Plattform Draw.IO verwendet.

2 Backbone

2.1 Namenskonvention

Alle Geräte im Backbone sind nach der folgenden Namenskonvention benannt:

[SW/R]-AS[Nr]-[BB/Peer/Internet]-[Nr]

Beispiele mit Erklärung:

- R-AS100-Peer-2: Der zweite eBGP-Peering Router im AS 100
- SW-AS666-BB-1: Der erste Switch im Backbone von AS 666

2.2 Addressbereiche

Zwischen den AS's werden als public IPs die für die Antarktis vorgesehenen IP-Ranges genutzt, somit sollte es auch bei einem Anschluss ans echte Internet keinen Overlap geben. Den einzigen Overlap, den es bei der Umsetzung gegeben hat, war mit einem Starlink-Adressbereich.

Public-Peering-Adressbereiche:

- Zwischen AS100 (R-AS100-Peer-1) und AS666 (R-AS666-Peer-2): 154.30.31.0/30
- Zwischen AS666 (R-AS666-Peer-1) und AS20 (R-AS22-Peer): 45.84.107.0/30
- Zwischen AS20 (R-AS21-Peer) und AS100 (R-AS100-Peer-2): 103.152.127.0/30

Bei den Firewall-PoPs^[1]:

- R-AS100-Peer-1 zu Kebapci-FW: 31.25.11.0/24
- R-AS666-Peer-3 zu Dorf-FW: 87.120.166.0/24
- R-AS21-Peer zu Fav-FW-1: 103.152.126.0/24
- R-AS100-Peer-2 zu Fav-FW-2: 103.152.125.0/24
- R-AS666-Peer-1 zu Burger-FW: 31.6.14.0/24
- R-AS666-Peer-3 zu R-Flex-Edge-1: 78.12.166.0/24
- R-AS100-Peer-2 zu R-Flex-Edge-2: 13.52.124.0/24
- R-AS666-Peer-2 zu R-Armut-Edge-1: 31.25.42.0/24
- R-AS666-Peer-4 zu R-Armut-Edge-2: 31.6.28.0/24

^[1]Point of Presence: TODO

Öffentliches Loopback für eine problemlose Kombination von HA-Clustering und VPN-Endpoint:

- Fav-FW: 125.152.103.1/32

2.3 Autonome Systeme

Das Backbone besteht aus drei AS's.

2.3.1 AS20

Besteht aus den Sub-AS's 21 & 22, insgesamt 5 Router (2 in 21 und 3 in 22):

- R-AS21-Peer
- R-AS21-BB
- R-AS21-Internet
- R-AS22-Peer
- R-AS22-BB

Nutzt ein MPLS Overlay, OSPF^[1] Underlay

BGP^[2] Features:

- R-AS21-BB dient als Route-Reflector
- R-AS21-Internet teilt seine Default Route ins Internet den anderen Peers mit

Netzadresse	Subnetzprefix	Verbundene Geräte		
		Hostname	Adresse	Interface
172.16.20.0	30	R-AS21-BB	.1	Gig0/0
		R-AS22-BB	.2	Gig0/0
172.16.21.0	30	R-AS21-Peer	.1	Gig0/1
		R-AS21-BB	.2	Gig0/1
172.16.21.4	30	R-AS21-Internet	.5	Gig0/2
		R-AS21-BB	.6	Gig0/2
172.16.22.0	30	R-AS22-Peer	.1	Gig0/1
		R-AS22-BB	.2	Gig0/1

TODO: Loopback

^[1]Open Shortest Path First: Ein dynamisches Link-State Routingprotokoll

^[2]Border Gateway Protocol: TODO

2.3.2 AS100

Besteht aus insgesamt nur 2 Routern:

- R-AS100-Peer-1
- R-AS100-Peer-2

Braucht kein Overlay/Underlay, nur iBGP weil das AS aus lediglich zwei Routern besteht.

BGP Features:

- Distribution Lists (Traffic von Burger-FW wird auf allen Border-Routern blockiert)

Netzadresse	Subnetzprefix	Verbundene Geräte		
		Hostname	Adresse	Interface
192.168.100.0	30	R-AS100-Peer-1	.1	Gig0/1
		R-AS100-Peer-2	.2	Gig0/1

TODO: Loopback

2.3.3 AS666

Besteht aus 13 Routern und 2 L2-Switches:

- R-AS666-Peer-1
- R-AS666-Peer-2
- R-AS666-Peer-3
- R-AS666-Peer-4
- R-AS666-BB-1
- R-AS666-BB-2
- R-AS666-BB-3
- R-AS666-BB-4
- R-AS666-BB-5
- R-AS666-BB-6
- R-AS666-BB-7
- R-AS666-BB-8
- R-AS666-BB-9
- SW-AS666-BB-1
- SW-AS666-BB-2

Nutzt ein OSPF Underlay mit MPLS als Overlay.

BGP Features:

- Pfadmanipulation mittels Local Preference von 100 auf 300 -> Traffic für den Standort Favoriten innerhalb AS666 immer über R-AS666-Peer-2 an AS100 ausschicken statt AS20
- Prefix-List die alle Bogon-Adressen enthält auf die eBGP-Neighbors inbound angewendet werden, um Bogons zu blockieren

Unter anderem steht in AS666 ein OOB-Syslog-Server, welcher von den Routern XXX, YYY und ZZZ diverse Logs zu den Protokollen LDP bzw. MPLS, OSPF und BGP gesammelt und gespeichert hat. Bei der Konfiguration von den Debug-Befehlen auf den Routern bleiben diese leider nach einem Neustart des Geräts nicht bestehen, also mussten sie nach jedem (Neu-)Start erneut eingegeben werden. Folgende Debug-Befehle wurden hierbei verwendet:

- fd dfd
- fd fd
- hghghgh

Netzadresse	Subnetzprefix	Verbundene Geräte		
		Hostname	Adresse	Interface
10.6.66.0	30	R-AS666-Peer-2	.1	Gig0/1
		R-AS666-BB-1	.2	Gig0/1
10.6.66.4	30	R-AS666-BB-1	.5	Gig0/0
		R-AS666-BB-2	.6	Gig0/0
10.6.66.8	30	R-AS666-BB-2	.9	Gig0/1
		R-AS666-BB-3	.10	Gig0/1
10.6.66.20	30	R-AS666-Peer-3	.21	Gig0/0
		R-AS666-BB-4	.22	Gig0/0
10.6.66.24	30	R-AS666-Peer-3	.25	Gig0/2
		R-AS666-BB-5	.26	Gig0/2
10.6.66.28	30	R-AS666-BB-5	.29	Gig0/3
		R-AS666-BB-6	.30	Gig0/3
10.6.66.32	30	R-AS666-BB-6	.33	Gig0/2
		R-AS666-BB-7	.34	Gig0/2
10.6.66.36	30	R-AS666-BB-6	.37	Gig0/0
		R-AS666-BB-8	.38	Gig0/0
10.6.66.40	30	R-AS666-BB-7	.41	Gig0/1
		R-AS666-BB-9	.42	Gig0/1
10.6.66.44	30	R-AS666-BB-8	.45	Gig0/3
		R-AS666-BB-9	.46	Gig0/3

10.6.66.48	30	R-AS666-BB-9	.49	Gig0/2
		R-AS666-Peer-1	.50	Gig0/2
10.6.66.104	29	R-AS666-BB-3	.105	Gig0/0
		R-AS666-BB-4	.106	Gig0/1
		R-AS666-BB-8	.107	Gig0/2
10.6.66.112	29	R-AS666-Peer-1	.113	Gig0/3
		R-AS666-BB-2	.114	Gig0/2
		R-AS666-BB-9	.115	Gig0/0
10.6.66.200	30	R-AS666-Peer-4	.201	Gig0/0
		R-AS666-BB-7	.202	Gig0/0

TODO: Loopback

2.3.3.1 OOB Syslog

TODO

2.4 Dynamisches Routing

Für den automatischen Routenaustausch innerhalb von den Backbone-Netzwerken werden die dynamischen Routingprotokolle OSPF und RIP^[1] verwendet. Für den externen Routenaustausch zwischen ASen wird BGP verwendet.

2.4.1 Authentifizierung

Jegliche Instanzen von OSPF und RIP im AS666 nutzen Authentifizierung für ihre Updates.

OSPF:

- Key-String: ciscocisco
- Algorithmus: hmac-sha-512

```
1 key chain 1
2 key 1
3 key-string ciscocisco
4 cryptographic-algorithm hmac-sha-512
```

^[1]Routing Information Protocol: Ein dynamisches Distance-Vektor Routingprotokoll

```
5 ex
6
7 int g0/1
8 ip ospf authentication key-chain 1
9 ex
```

Quellcode 2.1: Authenticated OSPF-Updates mittels Key-Chain

RIP:

- Key-String: ganzgeheim123!
- Algorithmus: dsa-2048

```
1 key chain 2
2 key 1
3 key-string ganzgeheim123!
4 cryptographic-algorithm hmac-sha-384
5 ex
6
7 int tunnel1
8 ip rip authentication key-chain 2
9 ex
```

Quellcode 2.2: Authenticated RIP-Updates mittels Key-Chain

BGP:

- Key-String: BeeGeePeel?
- Algorithmus: ecdsa-384

2.5 Statisches Routing

Damit Traffic zu den Firewalls vom Standort Wien Favoriten findet, wird nicht nur die Loopback-Adresse von den Fav-FWs von R-AS21-Peer und R-AS100-Peer-2 advertised, sondern es wird auf den zwei Geräten ebenfalls eine statische Route konfiguriert, weil sie sonst die Loopback-Adresse nicht finden/erreichen können.

Alternative: Firewalls der Kunden haben ein BGP-Peering mit Border-Routern im Backbone, um ihr Loopback per eBGP bekanntzugeben.

Es wird ebenfalls eine statische Route auf R-AS21-Internet verwendet, um allen anderen Geräten in der Topologie einen Zugang zum Internet per NAT-Cloud zu ermöglichen.

3 Firewalls

3.1 FortiGate

Die Firma Fortinet ist einer der Weltmarktführer im Bereich Firewalls mit ihrer Reihe an FortiGate-Firewalls. Sie bieten nicht nur physische Modelle, sondern auch virtuelle Instanzen. In der Topologie werden insgesamt drei solcher virtuellen FortiGates eingesetzt, um eine industriennahe Firewall-Implementierung mit SOTA-Features erreichen.

In der Topologie sind insgesamt drei FortiGate-Firewalls zu finden:

- Fav-FW-1 und Fav-FW-2 am Standort Wien Favoriten
- Dorf-FW am Standort Langenzersdorf

Für die Addressbereiche der Peering- oder der Standort-Netzwerke siehe Abschnitt 2 und Abschnitt 4.

Bei der Umsetzung der hier aufgelisteten Features wurde immer nur die CLI verwendet. Das Web-Dashboard dient nur der Überprüfung und der Veranschaulichung der Konfiguration.

3.1.1 Grundkonfiguration

```
1 config system global
2     set hostname Fav-FW-1
3     set admintimeout 30
4     set timezone 26
5 end
```

Quellcode 3.1: Grundkonfiguration der Fav-FW-1

3.1.2 Interfaces

Bevor die Implementierung von den Firewall-Features auf der FortiGate stattfinden kann, müssen – wie auf allen anderen Netzwerkgeräten auch – zuerst die Netzwerkinterfaces konfiguriert werden.

```
1  config system interface
2      edit port3
3          set desc "Used to enroll VM license 00B"
4          set mode static
5          set ip 192.168.0.100 255.255.255.0
6          set allowaccess ping http https
7      next
8      edit port1
9          set desc "to_R_AS21_Peer"
10         set mode static
11         set ip 103.152.126.1 255.255.255.0
12         set role wan
13         set allowaccess ping
14     next
15 ...
16 edit "Dorf_VPN_GW_LB"
17     set vdom root
18     set ip 125.152.103.1 255.255.255.255
19     set allowaccess ping
20     set type loopback
21 next
22 edit VLAN_10
23     set desc "Linux Clients"
24     set vdom root
25     set interface port2
26     set type vlan
27     set vlanid 10
28     set mode static
29     set ip 192.168.10.254 255.255.255.0
30     set allowaccess ping
31 next
32 ...
33 end
```

Quellcode 3.2: Interface-Konfigurationsbeispiele auf Fav-FW-1

3.1.3 Lizenzierung

3.1.4 Policies

Eines der wichtigsten Werkzeuge, die eine FortiGate – wie viele andere Firewalls auch – bietet, sind Policies. Standardmäßig lässt eine FortiGate-Firewall keinerlei Datenverkehr durch, ein „implicit deny“ wird verwendet. Es müssen durch den/die zuständige Netzwerkadministrator/in beim Einsatz einer FortiGate die nötigen Firewall-Policies „geschnitzt“ werden, um den Datenverkehr auf das nötige Minimum einzuschränken, ohne dabei die Funktionalität des (bestehenden) Netzwerks zu beeinträchtigen.

```
1  config firewall policy
2      edit 20
3          set name "Windows_Clients_to_Servers"
4          set srcintf VLAN_20
5          set dstintf VLAN_200
6          set srcaddr all
7          set dstaddr all
8          set action accept
9          set schedule "always"
10         set service "ALL"
11     next
12 end
```

Quellcode 3.3: Interface-Konfigurationsbeispiele auf Fav-FW-1

```
1  config firewall policy
2      edit 24
3          set name "Windows_PAW_to_Jump"
4          set srcintf VLAN_20
5          set dstintf VLAN_210
6          set srcaddr "PAW"
7          set dstaddr all
8          set action accept
9          set schedule "always"
10         set service "RDP"
11     next
12 end
```

Quellcode 3.4: Interface-Konfigurationsbeispiele auf Fav-FW-1


```
1  config firewall policy
2      edit 150
3          set name "Bastion_to_Windows_Devices"
4          set srcintf VLAN_150
5          set dstintf VLAN_20 VLAN_200
6          set srcaddr "Bastion"
7          set dstaddr all
8          set action accept
9          set schedule "always"
10         set service "SSH"
11     next
12 end
```

Quellcode 3.5: Interface-Konfigurationsbeispiele auf Fav-FW-1

3.1.5 HA Cluster

Ein High Availability Cluster besteht aus zwei oder mehr FortiGate und dient der Ausfallsicherheit durch die automatisierte Konfigurationsduplikation zwischen den Geräten. Bei einem erfolgreichen Clustering verhalten sich die Geräte im Cluster so, als wären sie ein Einziges.

Vorraussetzungen:

- Zwei oder mehr FortiGate-Firewalls mit HA-Unterstützung
- Mindestens eine Point-to-Point Verbindung zwischen den Firewalls

Folgende Konfigurationsoptionen müssen gesetzt werden, um ein HA-Clustering zu erzielen:

- Clustering-Mode (Active-Passive oder Active-Active)
- Group-ID
- Group-Name
- Passwort
- Heartbeat-Interfaces (Die Point-to-Point Interfaces, die für die HA-Kommunikation genutzt werden sollen)

```
1  config system ha
2      set mode a-a
3      set group-id 1
4      set group-name Koch_Burger_LBT_Cluster
5      set password ganzgeheim123!
6      set hbdev port9 10 port10 20
7      set override enable
```

```
8      set priority 200
9  end
```

Quellcode 3.6: Konfiguration des HA Clusters auf Fav-FW-1

Nachdem auf beiden Geräten die richtige Konfiguration vorgenommen worden ist, beginnen sie die gegenseitige Synchronisation ihrer gesamten Konfigurationen.

Zur Überprüfung können folgende Befehle verwendet werden:

- fd fd fd
- fd fd fd

3.1.6 NAT

Damit die alle Client-PCs als auch manche Server der Standorte Wien Favoriten und Langenzersdorf die öffentlichen Adressen im LBT-Netzwerk sowie das Internet erreichen können, braucht es eine Art von NAT bzw. PAT.

```
1  config firewall policy
2      edit 1
3          set name "non-VPN-PAT-to-Outside"
4          set srcintf "port2" "VLAN_10" "VLAN_20" "VLAN_21" "VLAN_30" "VLAN_31"
           "VLAN_100" "VLAN_150" "VLAN_200" "VLAN_210"
5          set dstintf "port1"
6          set srcaddr "all"
7          set dstaddr "Langenzersdorf_REMOTE" "Kebapci_REMOTE"
8          set dstaddr-negate enable
9          set action accept
10         set schedule "always"
11         set service "ALL"
12         set utm-status enable
13         set inspection-mode proxy
14         set logtraffic all
15         set webfilter-profile "webprofile"
16         set profile-protocol-options default
17         set ssl-ssh-profile custom-deep-inspection
18         set nat enable
19         set ippool enable
20         set poolname "NAT_Public_IP_Pool"
21         set logtraffic all
```

```
22     next
23 end
```

Quellcode 3.7: Die non-VPN-Traffic PAT-to-Outside Firewall-Policy

3.1.7 DHCP

Für die automatische Zuweisung von IP-Adressen an die Client-Computer wurde auf der FortiGate DHCP konfiguriert. Da manche Clients trotz automatischer IP-Zuweisung dauerhaft die gleiche IP brauchen, z.B. für bestimmte Firewall-Policies, wird zum DHCP-Pool dazu ein Static-Lease für die PAW erstellt.

```
1  config sys dhcp server
2      edit 1
3          set status enable
4          set lease-time 86400
5          set vci-match disable
6          set interface VLAN_20
7          set dns-server1 192.168.200.1
8          set dns-server2 192.168.200.2
9          set domain "corp.gartenbedarf.com"
10         set default-gateway 192.168.20.254
11         set netmask 255.255.255.0
12         config ip-range
13             edit 1
14                 set start-ip 192.168.20.10
15                 set end-ip 192.168.20.15
16             next
17         end
18         config reserved-address
19             edit 1
20                 set type mac
21                 set ip 192.168.20.10
22                 set mac 01:23:45:67:89:AB
23                 set action assign
24                 set description "Static Lease .10 for PAW (Workstation-1)"
25             next
26         end
27     next
```

28 end

Quellcode 3.8: DHCP-Server-Konfiguration für VLAN 20 (inkl. Static Lease)

3.1.8 VPNs

Alle VPNs auf den FortiGate sind PSK-basiert.

3.1.8.1 Site-to-Site IPsec VPN

für loopback bgp verteilung: Abschnitt 3.1.13.

3.1.8.2 RAS-VPN

3.1.9 Captive Portal

Bevor die Windows Clients (in VLAN 20) externe Hosts und Dienste erreichen können, müssen sie sich über ein sogenanntes „Captive Portal“ bei der Firewall authentifizieren. Für die Authentifizierung wird der AD-integrierte NPS-Server genutzt, als Protokoll wird hierbei RADIUS verwendet.

Um eine „Captive Portal“-Authentifizierung auf einer FortiGate-Firewall zu konfigurieren, AAAAAA:

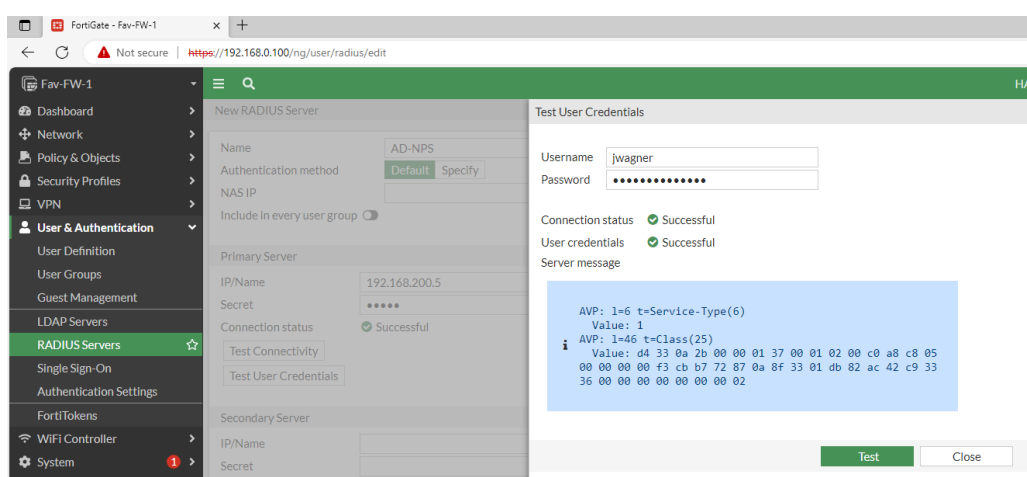


Abbildung 3.1: Die erfolgreiche Authentifizierung mit AD-Benutzer über RADIUS

3.1.10 SSL Inspection

HTTPS-Traffic verläuft zwischen den Endgeräten TLS-verschlüsselt, wodurch die Firewalls nicht den Datenverkehr auf Schadsoftware oder andere unerwünschte Inhalten überprüfen können. Die Lösung zu diesem Problem ist die sogenannte „SSL Inspection“, der Datenverkehr wird von der Firewall entschlüsselt (Original-Zertifikat wird entfernt), geprüft und anschließend wieder verschlüsselt (neues Zertifikat wird eingefügt).

AAAAAAAAAAAAa

3.1.11 Traffic Shaping

Verschiedene Arten von Datenverkehr sollten im Netzwerk unterschiedlich priorisiert werden, da beispielsweise ein VoIP-Telefonat oder ein Livestream eine stabilere Verbindung braucht als das Laden einer statischen Website. Um diese Priorisierung zu ermöglichen, wird das Feature „Traffic Shaping“ eingesetzt: Der Datenverkehr wird geshaped (umgeformt), sodass bei einem VoIP-Telefonat immer eine bestimmte (Rest-)Bandbreite garantiert ist.

Für die Standorte Wien Favoriten und Langenzersdorf ist folgendes Shaping vorgesehen:

- VoIP-Telefonate bekommen die höchste Prioritätsstufe und haben eine garantierte Bandbreite von 300kbps.
- Youtube-Streaming bekommt die mittlere Prioritätsstufe und hat eine garantierte Bandbreite von 1500kbps (Hat aber Nachrang bei wenig Bandbreite und aktivem VoIP-Traffic!).
- Der restliche Datenverkehr bekommt die niedrigste Prioritätsstufe und hat somit die restliche Bandbreite, es wird hierbei keine Bandbreite garantiert.

Traffic Shaping muss eigenen Firewall-Policies zugewiesen werden, damit es aktiv ist. Bevor es jedoch zugewiesen wird, sollten die Shaping-Stufen konfiguriert werden. Standardmäßig sind die Stufen `high-priority`, `medium-priority` und `low-priority` vorkonfiguriert, ihre Parameter können jedoch angepasst werden.

```
1 # voip high prio (medium band)
2 # youtube medium prio (viel band)
3 # rest low prio (der rest? band)
4 config firewall shaper traffic-shaper
5     edit high-priority
6         set per-policy enable
7         set priority high
8         set bandwidth-unit kbps
9         set guaranteed-bandwidth 300
```

```
10      set maximum-bandwidth 1000000
11      next
12      edit medium-priority
13          set per-policy enable
14          set priority medium
15          set bandwidth-unit kbps
16          set guaranteed-bandwidth 1500
17          set maximum-bandwidth 1000000
18      next
19      edit low-priority
20          set per-policy enable
21          set priority low
22          set bandwidth-unit kbps
23          set maximum-bandwidth 1000000
24      next
25  end
```

Quellcode 3.9: Die Konfiguration der Traffic-Shaping-Stufen

Shaping-Policies gehören konfigurationstechnisch nicht zu den „normalen“ Policies, sie müssen mit dem Befehl `config firewall shaping-policy` erstellt werden:

```
1  config firewall shaping-policy
2      edit 1
3          set name VOIP
4          set status enable
5          set ip-version 4
6          set service FINGER H323
7          set srcaddr "IP-Phone-Langenzersdorf"
8          set dstaddr "IP-Phone-Favoriten"
9          set dstintf VLAN_42
10         set traffic-shaper high-priority
11     next
12     edit 2
13         set name YT
14         set status enable
15         set ip-version 4
16         set srcaddr "Dorf-L-Workstations" "Dorf-W-Workstations"
17         set srcintf VLAN_10 VLAN_20
18         set dstintf port1
```

```
19      set internet-service enable
20      set internet-service-name Google-Web
21      # YTs app ID
22      set application 16040
23      set traffic-shaper medium-priority
24  next
25 end
```

Quellcode 3.10: Die Shaping-Policies, die auf den Shaping-Stufen aufbauen

3.1.12 Webfilter

Ein Webfilter ist eine Art der DPI, bei welcher HTTP(S)-Packets auf die abgefragte URL untersucht und je nach Webfilter-Policy blockiert bzw. akzeptiert werden. Somit lassen sich z.B. unerlaubte Inhalte blockieren, damit die Client-PCs im Firmennetzwerk keinen Zugriff auf ablenkende Inhalte während der Arbeitszeit haben.

Je nach Standort werden unterschiedliche Websites blockiert. Während in Wien X (ehem. Twitter) und die Website der HTL Spengergasse blockiert sind, sind in Langenzersdorf ebenfalls X aber dazu die Website der HTL Rennweg blockiert.

```
1  config webfilter urlfilter
2      edit 1
3          set name "webfilter"
4          config entries
5              edit 1
6                  set url "*x.com"
7                  set type wildcard
8                  set action block
9              next
10             edit 2
11                 set url "www.spengergasse.at"
12                 set type simple
13                 set action block
14             next
15         end
16     next
17 end
```

Quellcode 3.11: URL-Filter für X.com und www.spengergasse.at

```
1 config webfilter profile
2     edit "webprofile"
3         config web
4             set urlfilter-table 1
5         end
6         config ftgd-wf
7         end
8     next
9 end
```

Quellcode 3.12: Das Webfilter-Profil für die Aktivierung der URL-Filter

3.1.13 BGP

3.1.14 Sonstiges

3.1.14.1 Adressobjekte und Adressgruppen

3.1.14.2 Lokale Benutzer

3.2 PfSense

Eine PfSense-Firewall ist eine kostenlose und software-basierte Alternative zu herkömmlichen Hardware-Firewalls von Herstellern wie Cisco oder Fortinet.

3.3 Cisco Router

Um die Anforderungen einer FlexVPN-Verbindung zu erfüllen, wurden kleinere Standorte erstellt, welche als Firewall lediglich einen Cisco Router haben, da Features wie FlexVPN Cisco-proprietär sind.

3.3.1 FlexVPN

FlexVPN ist Ciscos Lösung um die Aufsetzung von VPNs zu vereinfachen und deckt fast alle VPN-Arten ab, unter anderem z.B. site-to-site, hub-and-spoke (inklusive spoke-to-spoke) und remote access VPNs. Ein weiteres Feature von FlexVPN ist, dass es IKEv2 für alle VPN-Arten nutzt und somit eine gewisse Sicherheit voraussetzt.

In unserer Topologie wird ein PSK-basierter site-to-site FlexVPN mit „Smart Defaults“ genutzt, welcher über einen GRE-Tunnel läuft. Er verbindet die privaten Addressbereiche der „Flex“-Standorte.

„Smart Defaults“ bieten vordefinierte Werte für die IKEv2-Konfiguration, die auf den Best Practices basieren. Sie beinhalten alles bis auf die folgenden IKEv2-Konfigurationen:

- IKEv2 profile
- IKEv2 keyring

Das heißt, dass folgende Konfigurationen übersprungen werden können:

- IKEv2 proposal
- IKEv2 policy
- IPSec transform-set
- IPSec profile

```
1  crypto ikev2 keyring mykeys
2  peer R-Flex-Edge-2
3  address 13.52.124.1
4  pre-shared-key IchMussFlexen!
5  ex
6
7  crypto ikev2 profile default
8  match identity remote address 13.52.124.1 255.255.255.255
9  authentication local pre-share
10 authentication remote pre-share
```

```
11 keyring local mykeys
12 dpd 60 2 on-demand
13 ex
14
15 crypto ipsec profile default
16 set ikev2-profile default
17 ex
18
19 int tun0
20 ip address 10.20.69.1 255.255.255.0
21 tunnel source g0/3
22 tunnel destination 13.52.124.1
23 tunnel protection ipsec profile default
24 ex
```

Quellcode 3.13: FlexVPN-Konfiguration auf R-Flex-Edge-1

3.3.2 MPLS Overlay VPN

Falls der Kunde bzw. Standortinhaber die privaten Addressbereiche seiner Standorte per VPN verknüpft haben möchte aber auf seinen Edge-Routern oder Firewalls keinen eigenen VPN-Tunnel konfigurieren möchte, kann vom Betreiber des Backbones ein MPLS Overlay VPN eingesetzt werden.

In unserer Topologie ist diese Art von VPN im AS666 – zwischen den Border-Routern R-AS666-Peer-2 und R-AS666-Peer-4 – realisiert. Folgende Konfigurationsschritte sind für einen MPLS Overlay VPN nötig:

- Im Backbone wird MPLS zur Datenübertragung verwendet.
- Die Border-Router haben VRFs für die Abkapselung der Routen bei Verbindung der Standorte.
- Die Edge-Router der Standorte peeren mit den Border-Routern über eBGP.
- In der BGP-Konfiguration der Border-Router werden die Edge-Router in der Addressfamilie „VPNv4“ als Nachbarn angegeben.

4 Standorte

4.1 Wien Favoriten

Wien Favoriten ist der Hauptstandort der Gartenbedarfs GmbH und somit auch der größte in der gesamten Topologie.

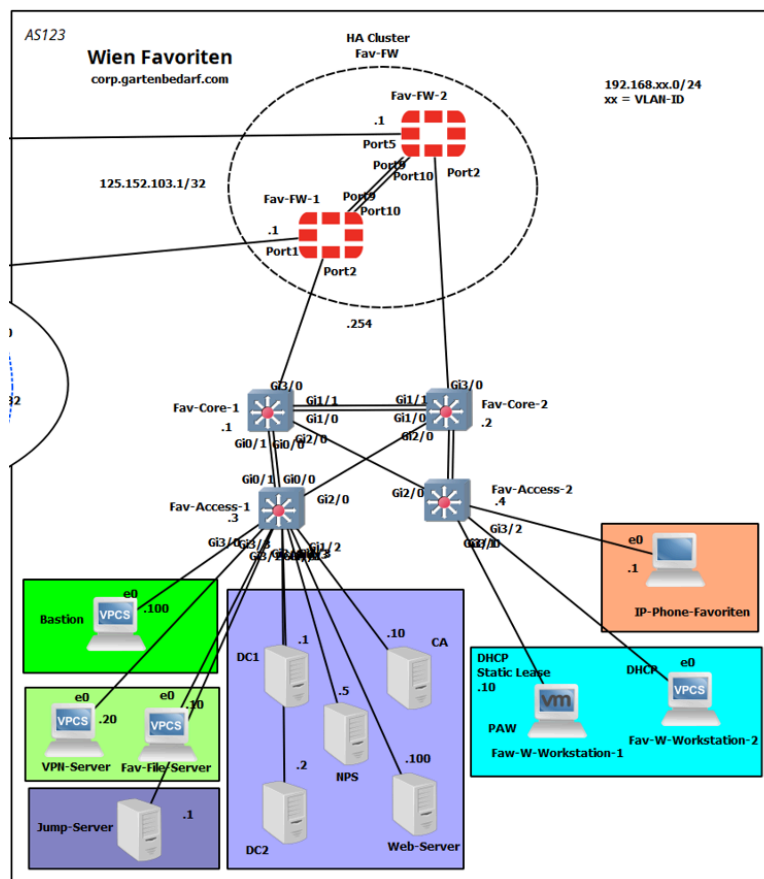


Abbildung 4.1: Der Standort Wien Favoriten

Der private Adressbereich an diesem Standort entspricht dem Subnetz 192.168.xx.0/24.
xx = VLAN-ID, falls das Gerät keinem spezifischen VLAN zugewiesen ist, dann ist xx = 0

4.1.1 VLANs

ID	Bezeichnung
20	Windows Clients
30	Switch Management
31	Switch R-SPAN Mirroring
42	VoIP-Geräte
100	Ubuntu Server (ohne Bastion)
150	Bastion
200	Windows Server
210	Jump Server
666	Blackhole

4.1.2 Geräte

- 2x FortiGate
 - Fav-FW-1 (192.168.xx.254)
 - Fav-FW-2 (192.168.xx.253)
- 4x L3-Switch
 - Fav-Core-1 (192.168.30.1)
 - Fav-Core-2 (192.168.30.2)
 - Fav-Access-1 (192.168.30.3)
 - Fav-Access-2 (192.168.30.4)
- 1x IP-Phone
 - IP-Phone-Favoriten (192.168.42.1)
- 3x Ubuntu-Server
 - Bastion (192.168.150.100)
 - Fav-File-Server (192.168.100.10)
 - VPN-Server (192.168.100.20)
- 6x Windows-Server
 - DC1 (192.168.200.1) (Core)
 - DC2 (192.168.200.2) (Core)
 - NPS (192.168.200.5) (Core)
 - CA (192.168.200.10) (Core)
 - Web-Server (192.168.200.100) (GUI)
 - Jump-Server (192.168.210.1) (GUI)

- 2x Windows-Client
 - Fav-W-Workstation-1 (DHCP -> Static Lease für 192.168.20.10) (PAW)
 - Fav-W-Workstation-2 (DHCP)

4.1.3 Features

Folgende Features wurden im Rahmen dieses Standorts implementiert:

4.1.3.1 FortiGates

Siehe Abschnitt 3.1.

4.1.3.2 Switches

- PVST+
- Management-Interface auf VLAN 30, IPs siehe oben
- VTP für die automatische Verteilung von VLAN-Informationen
- Bei redundanten Verbindungen untereinander EtherChannel mittels LACP aggregieren (inklusive Load-Balancing)
- Switchport Security (Hardening)
 - Gehärteter PVST+ Prozess
 - Root-, Loop, BPDU-Guard
 - DHCP Snooping, Dynamic ARP inspection (DAI)
 - Blackhole VLAN auf ungenutzten Interfaces

4.1.3.3 Bastion

TODO

4.1.3.4 Fav-File-Server

- SMB-Share
- Synchronisiert seine Dateien mit Dorf-File-Server mittels lsyncd
- Erhält R-SPAN Daten der Fav-Switches und verarbeitet diese mittels T-Shark und speichert das auf einem Log-Share ab

4.1.3.5 VPN-Server

Ein WireGuard VPN-Server dient am Standort Wien Favoriten als alternativer RAS-VPN-Endpunkt zum RAS-VPN auf den FortiGate-Firewalls.

4.1.3.6 Active Directory

Am Standort Wien Favoriten stehen als AD-integrierte Endgeräte eine CA, zwei DCs, ein Jump-Server, ein Web-Server, ein NPS und mehrere Windows Workstations (darunter eine PAW).

Für nähere Informationen siehe Abschnitt 5.

4.2 Langenzersdorf

Langenzersdorf ist der Nebenstandort der Gartenbedarfs GmbH und ist der zweitgrößte Standort in der Topologie.

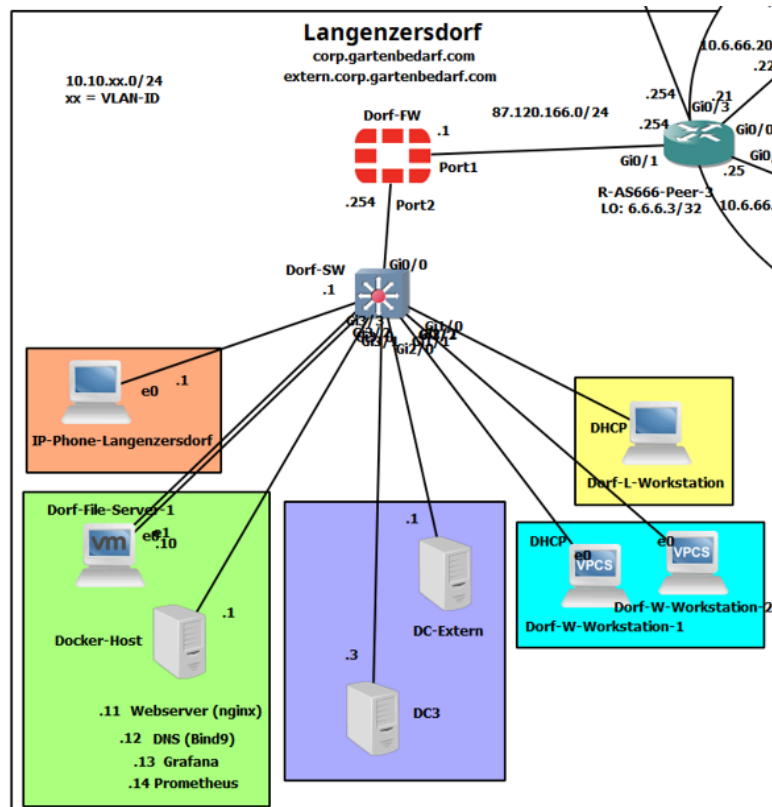


Abbildung 4.2: Der Standort Langenzersdorf

Der private Adressbereich an diesem Standort entspricht dem Subnetz 10.10.xx.0/24.

xx = VLAN-ID, falls das Gerät keinem spezifischen VLAN zugewiesen ist, dann ist xx = 0

4.2.1 VLANs

ID	Bezeichnung
10	Linux Clients
20	Windows Clients

30	Switch Management
31	Switch Mirroring
42	VoIP-Geräte
100	Ubuntu Server
200	Windows Server
666	Blackhole

4.2.2 Geräte

- 1x FortiGate
 - Dorf-FW (10.10.xx.254)
- 1x L3-Switch
 - Dorf-SW (10.10.30.1)
- 1x IP-Phone
 - IP-Phone-Langenzersdorf (10.10.42.1)
- 2x Ubuntu-Server
 - Dorf-File-Server (quasi Syslog) (10.10.100.1)
 - Docker-Host (10.10.100.10 & Docker-Container)
 - NGINX Webserver (10.10.100.11)
 - Bind9 DNS-Server (10.10.100.12)
 - Grafana (10.10.100.13)
 - Prometheus (10.10.100.14)
- 2x Windows-Server
 - DC-Extern (10.10.200.1) (Core)
 - DC3 (10.10.200.3) (Core)
- 1x Linux-Client
 - Dorf-L-Workstation (DHCP)
- 2x Windows-Client
 - Dorf-W-Workstation-1 (DHCP)
 - Dorf-W-Workstation-2 (DHCP)

4.2.3 Features

4.2.3.1 FortiGate

Siehe Abschnitt 3.1.

4.2.3.2 Switch

- Management-Interface auf VLAN 30, IP siehe oben.
- Folgende Switchport Security (Hardening) Features sind konfiguriert:
 - Root-, Loop, BPDU-Guard
 - DHCP Snooping, Dynamic ARP inspection (DAI)
 - Blackhole VLAN auf unused Interfaces
 - Spanning-Tree deaktiviert
- Spiegelt Traffic mittels SPAN an den Dorf-File-Server.

4.2.3.3 Dorf-File-Server

- Hostet einen SMB-Share.
- Synchronisiert seine Dateien mit Fav-File-Server mittels lsyncd.
- Erhält SPAN-Daten des Dorf-Switches und verarbeitet diese mittels T-Shark und speichert das auf einem Log-Share ab.

4.2.3.4 Docker-Host

Hostet folgende Services innerhalb von Docker-Containern mit eigenen IPs (siehe oben): NGINX, Bind9, Grafana und Prometheus.

4.2.3.5 Active Directory

Am Standort Langenzersdorf stehen als AD-integrierte Endgeräte eine CA, zwei DCs, ein Jump-Server, ein Web-Server, ein NPS und mehrere Windows Workstations (darunter eine PAW).

Für nähere Informationen siehe Abschnitt 5. TODO

- DC3 und DC-Extern nutzen beide Windows Server Core
- Hosten die AD-Domäne corp.gartenbedarf.com bzw. extern.corp.gartenbedarf.com
- Linux Workstations
 - WIP
- Windows Workstations

- Sind Teil der corp.gardenbedarf.com Domäne
- Sind in einem private VLAN (20 bzw. 21) und können sich nicht gegenseitig erreichen

4.3 Kebapci

fdfdfdfdfd

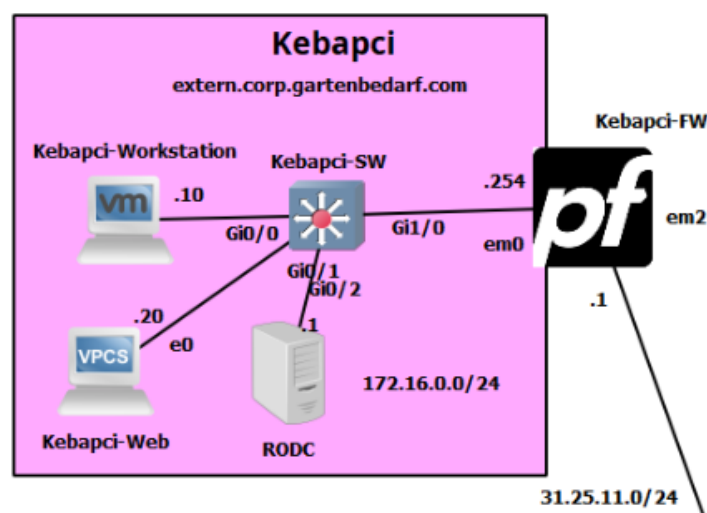


Abbildung 4.3: Der Standort „Kebapci“

4.4 Praunstraße

Der Standort Praunstraße symbolisiert ein kleines Heimnetzwerk, welches von einem Mitarbeiter der Gartenbedarfs GmbH für das Home-Office verwendet wird. Hier ist lediglich ein Internetzugriff gegeben, über welchen beispielsweise gesurft und eine RAS-VPN-Verbindung zum Firmenstandort Wien Favoriten aufgebaut werden kann.

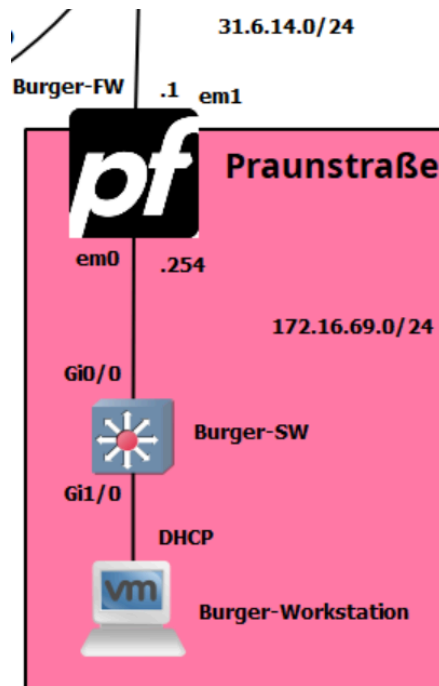


Abbildung 4.4: Der Standort Praunstraße

4.4.1 Private VLANs

Da der hier ansässige Mitarbeiter ein großes Bewusstsein für die Cybersicherheit hat, hat er auf seinem Switch private VLANs konfiguriert, damit sich die Endgeräte innerhalb seines Netzwerks nicht untereinander erreichen können.

```
1  vtp mode transparent
2
3  vlan 100
4  name BURGER-LAN-ISOLATED
5  private-vlan isolated
6  ex
7
8  vlan 10
9  name BURGER-LAN
10 private-vlan primary
11 private-vlan association add 100
12 ex
```

```
13
14 ...
15
16 int range gig 0/1 - 2
17 switchport mode private-vlan host
18 switchport private-vlan host-association 10 100
19 exit
20
21 int gig 0/0
22 switchport mode private-vlan promiscuous
23 switchport private-vlan mapping 10 100
24 exit
```

Quellcode 4.1: Private VLANs auf Burger-SW

4.5 Flex-Standorte

Die Flex-Standorte dienen lediglich der Implementierung eines FlexVPN-Tunnels. Deswegen bestehen sie jeweils nur aus zwei Geräten: Einem Cisco Router als „Firewall“ und einem VPCS^[1] für Ping-Tests.

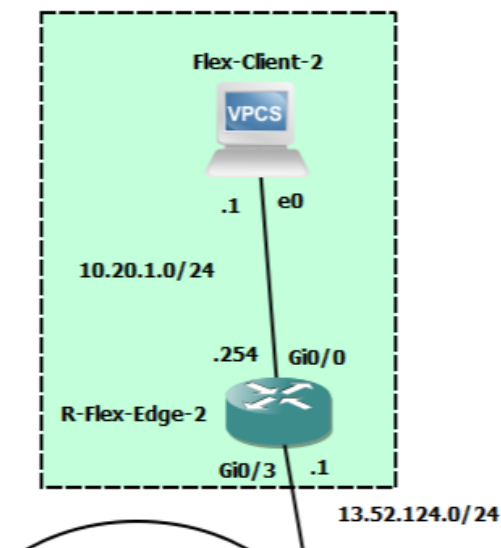


Abbildung 4.5: Der zweite Flex-Standort

^[1]Virtual PC Simulator: Ein in GNS3 vorinstalliertes Gerät bzw. Programm, welches einen simplen Client-PC simuliert.

4.5.1 EIGRP

Damit sich die Endgeräte der Flex-Standorte erreichen können, müssen die Edge-Router vom gegenüberliegenden Netzwerk wissen. Für diesen Routenaustausch wird das Routingprotokoll EIGRP verwendet, da es simpel zu konfigurieren ist und im Vergleich zu anderen Distance-Vektor-Protokollen moderner gestaltet ist (im Vergleich zu RIP z.B.).

```
1 router eigrp 100
2 no auto-summary
3 network 10.20.0.0 0.0.0.255
4 network 10.20.69.0 0.0.0.255
5 ex
```

Quellcode 4.2: EIGRP-Konfiguration auf R-Flex-Edge-2

4.6 Armut-Standorte

Beide Armut-Standorte sind miteinander über einen MPLS Overlay VPN über das Backbone-Netz von AS666 verbunden. Für weitere Informationen siehe Abschnitt 3.3.2.

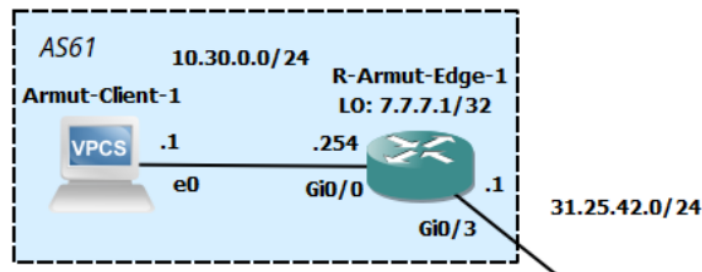


Abbildung 4.6: Der erste Armut-Standort

4.7 Viktor-Standort

Der „Viktor-Standort“ ist der zweite Home-Office-Standort der Topologie (nach Praunstraße) und wird statt einem Edge-Router oder einer Firewall durch eine Ubuntu-basierte Linux-Firewall vom öffentlichen Netz abgegrenzt.

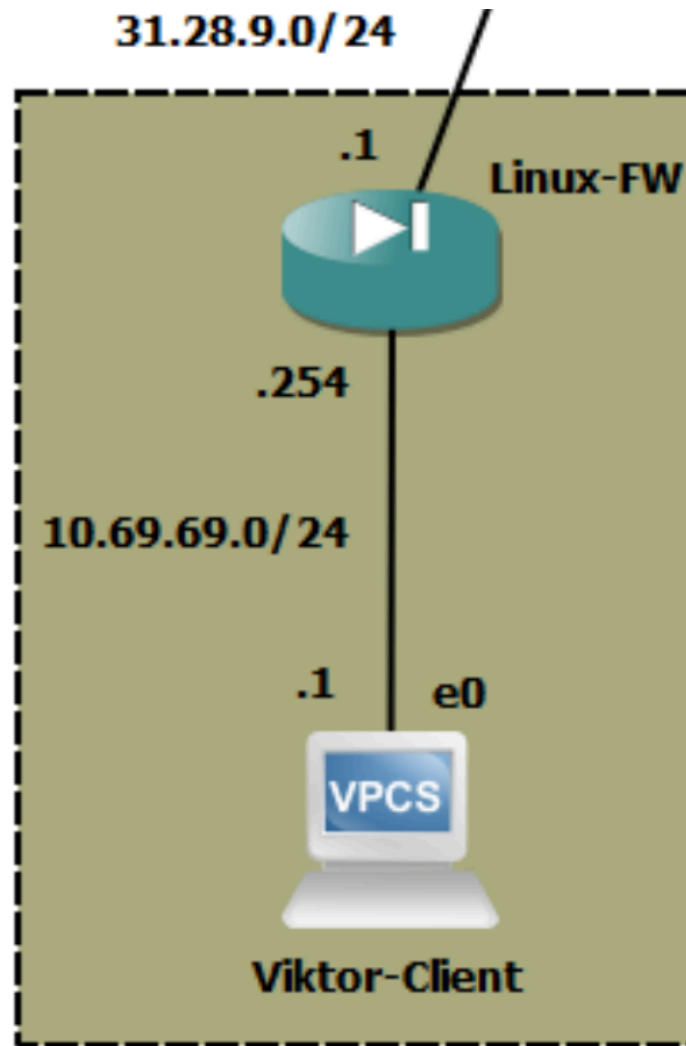


Abbildung 4.7: Der Viktor-Standort

4.7.1 Linux-Firewall

Wie zuvor erwähnt ist die Linux-Firewall am Viktor Standort eine Ubuntu 22.04 VM. Sie regelt den Datenverkehr zwischen dem Viktor-Client und dem öffentlichen Netz, wobei sie lediglich ICMP-Anfragen (und deren Rückantworten) erlaubt.

Für die Konfiguration der Netzwerkkarte wird folgende Netplan-Config verwendet:

```
1 network:
2   version: 2
3   renderer: networkd
```



```
4   ethernets:
5     ens33:
6       dhcp4: false
7       match:
8         macaddress: 00:0c:29:32:ea:ca
9       set-name: outside
10      addresses:
11        - 31.28.9.1/24
12      gateway4: 31.28.9.254
13      nameservers:
14        addresses: [8.8.8.8, 8.8.4.4]
15    ens37:
16      dhcp4: false
17      match:
18        macaddress: 00:0c:29:32:ea:d4
19      set-name: Viktor-LAN
20      addresses:
21        - 10.69.69.254/24
```

Quellcode 4.3: Netplan-Konfiguration für die Netzwerkadapter der Linux-Firewall

Alle anderen Ubuntu-basierten Computer in der Topologie werden ebenfalls mittels Netplan (und somit mit ähnlichen Konfigurationsdateien zu der in der Abbildungen oben) konfiguriert.

Damit ein Ubuntu-Gerät zu einer Linux-Firewall wird, muss IP-Routing/Forwarding eingeschaltet und darauf die nötigen iptables-Regeln erstellt werden. Zur Aktivierung von IP-Routing (ACHTUNG: nicht persistent!) können folgende Befehle verwendet werden:

```
1 sysctl -w net.ipv4.ip_forward=1
2 sysctl -p
```

Quellcode 4.4: Aktivierung nicht-persistentes IP-Routing unter Ubuntu

Anschließend können z.B. folgende iptables-Regeln gesetzt werden, um einen statischen NAT (PAT) nach außen zu starten und nur ICMP-Datenverkehr durchzulassen:

```
1 sysctl -w net.ipv4.ip_forward=1
2 sysctl -p
```

Quellcode 4.5: iptables-Regeln der Linux-FW

5 Active Directory

5.1 Überblick

Root-Domain: corp.gartenbedarf.com

Sonstige Domains: extern.corp.gartenbedarf.com

Streckt sich über die Standorte Wien Favoriten, Langenzersdorf und Kebapci, wobei beide Root-DCs in Favoriten stehen.

5.2 Geräte

5.2.1 Domain Controller

Name	IP-Adresse	FQDN	FSMO-Rollen	RO
DC1	192.168.200.1	dc1.corp.gartenbedarf.com	DNM, PDC	
DC2	192.168.200.2	dc2.corp.gartenbedarf.com	SM, RIDPM, IM	
DC3	10.10.200.3	dc3.corp.gartenbedarf.com	-	
DC-Extern	10.10.200.1	dc.extern.corp.gartenbedarf.com	-	
RODC	172.16.0.10	rodc.extern.crop.gartenbedarf.com	-	X

- RODC ist Read-Only
- SSH-Server ist an und PowerShell-Remoting ist erlaubt
- Schicken mittels Windows-Prometheus-Exporter Daten an den Grafana Server in Langenzersdorf
- Root-DCs dienen als NTP-Server

5.2.2 Jump Server

Name	IP-Adresse	FQDN
Jump-Server	192.168.210.1	jump.corp.gartenbedarf.com

- Kann per RDP und SSH auf die DCs zugreifen (wird von FW mittels Policies geregelt!)

5.2.3 CA + PKI

Name	IP-Adresse	FQDN
Certificate Authority	192.168.200.10	ca.corp.gartenbedarf.com
IIS-Server	192.168.200.100	web.corp.gartenbedarf.com

Die PKI besteht aus einem AD-CS Server und einem IIS-Server. Der IIS-Server stellt die CRLs und zur Verfügung und dient ebenso zum Testen der ausgestellten Zertifikate.

5.2.4 NPS

Name	IP-Adresse	FQDN
NPS-Server	192.168.200.5	nps.corp.gartenbedarf.com

5.2.5 Workstations

Name	IP-Adresse	FQDN	PAW
Fav-W-Workstation-1	DHCP, Static Lease 192.168.20.10	favwork1.corp.gartenbedarf.com	X
Fav-W-Workstation-2	DHCP	favwork2.corp.gartenbedarf.com	
Dorf-W-Workstation-1	DHCP	dorfwork1.corp.gartenbedarf.com	
Dorf-W-Workstation-2	DHCP	dorfwork2.corp.gartenbedarf.com	

- Die Fav-W-Workstation-1 ist eine Privileged Access Workstation (PAW), und kann u.a. deswegen folgende besondere Sachen:
 - Auf den Jump-Server per RDP und SSH zugreifen

5.3 PowerShell Konfiguration

Alle Domain-Controller wurden grundlegend mittels PowerShell-Skripts konfiguriert. Lediglich GUI-Exklusive Teile wie z.B.: NPS und IIS wurde im GUI erledigt. GPOs wurde aus Bequemlichkeitsgründen ebenfalls im GUI konfiguriert. Natürlich kann man sich im Nachhinein die GPOs exportieren und per PowerShell einspielen.

Die Grundkonfiguration sieht hierbei wie folgt aus:

```
scripts/windows/Favoriten-DC1-part1.ps1
```

```
1  Rename-Computer DC1
2
3  Rename-NetAdapter -Name "Ethernet0" `
4      -NewName "LAN"
5
6  New-NetIPAddress -InterfaceAlias "LAN" `
7      -IPAddress "192.168.200.1" `
8      -PrefixLength 24 `
9      -DefaultGateway "192.168.200.254"
10 Set-DnsClientServerAddress -InterfaceAlias "LAN" `
11     -ServerAddresses ("1.1.1.1", "1.0.0.1")
12
13 Set-TimeZone -Id "W. Europe Standard Time"
14 Enable-PSRemoting
15
16 Add-WindowsCapability -Online -Name "OpenSSH.Client~~~~0.0.1.0"
17 Add-WindowsCapability -Online -Name "OpenSSH.Server~~~~0.0.1.0"
18 Start-Service sshd
19 Set-Service -Name sshd -StartupType "Automatic"
20 New-ItemProperty -Path "HKLM:\SOFTWARE\OpenSSH" `
21     -Name DefaultShell `
22     -Value "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" `
23     -PropertyType String `
24     -Force
25 Restart-Service sshd
26
27 Restart-Computer
```

Quellcode 5.1: DC1 Grundkonfiguration

Diese Konfiguration ist sieht auf allen DCs fast gleich aus.

Als nächstes wird ein Forest auf DC1 erstellt und die Replication-Sites angelegt:

```
scripts/windows/Favoriten-DC1-part2.ps1
1  Install-WindowsFeature AD-Domain-Services -IncludeManagementTools
2  Import-Module ADDSDeployment
3
4  $SecureStringPassword = (ConvertTo-SecureString "Ganzgeheim123!" -AsPlainText
   -Force)
5
6  Install-ADDSForest -DomainName "corp.gartenbedarf.com" `
7      -DomainMode "WinThreshold" `
8      -ForestMode "WinThreshold" `
9      -SafeModeAdministratorPassword $SecureStringPassword `
10     -InstallDNS `
11     -Force
12
13 # Sites
14 New-ADReplicationSite -Name "Favoriten"
15 New-ADReplicationSite -Name "Langenzersdorf"
16 New-ADReplicationSite -Name "Kebapci"
17
18 New-ADReplicationSubnet -Name "192.168.200.0/24" -Site "Favoriten"
19 New-ADReplicationSubnet -Name "192.168.210.0/24" -Site "Favoriten"
20 New-ADReplicationSubnet -Name "192.168.20.0/24" -Site "Favoriten"
21 New-ADReplicationSubnet -Name "10.10.200.0/24" -Site "Langenzersdorf"
22 New-ADReplicationSubnet -Name "10.10.20.0/24" -Site "Langenzersdorf"
23 New-ADReplicationSubnet -Name "172.16.0.0/24" -Site "Kebapci"
24
25 New-ADReplicationSiteLink -Name "Favoriten-To-Langenzersdorf" `
26     -SitesIncluded ("Favoriten", "Langenzersdorf") `
27     -ReplicationFrequencyinMinutes 20
28
29 New-ADReplicationSiteLink -Name "Langenzersdorf-To-Kebapci" `
30     -SitesIncluded ("Langenzersdorf", "Kebapci") `
31     -ReplicationFrequencyinMinutes 20
32
33 Move-ADDirectoryServer -Identity "DC1" -Site "Favoriten"
```

Quellcode 5.2: DC1 erweiterte Konfiguration

Natürlich ist auf allen DCs Win-RM aktiviert um diese mittels Jump-Server administrieren zu können:

```
scripts/windows/Favoriten-DC1-part2.ps1
35 New-NetFirewallRule -DisplayName "WinRM HTTPS" `
36     -Direction Inbound `
37     -LocalPort 5985 `
38     -Protocol TCP `
39     -Action Allow `
40     -RemoteAddress "192.168.210.1"
```

Quellcode 5.3: Win-RM Konfiguration

5.4 Users & Computers

Innerhalb des ADs existieren folgende Benutzer:

Name	Logon	Password	Groups
Alex Taub	ataub	Ganzgeheim123!	Sales
Jonas Wagner	jwagner	Ganzgeheim123!	Sales
Sabine Rauch	srauch	Ganzgeheim123!	Management
Thomas Koch	tkoch	Ganzgeheim123!	Sales

Die Gruppen sind dann Weiter nach AGDLP wie folgt unterteilt:

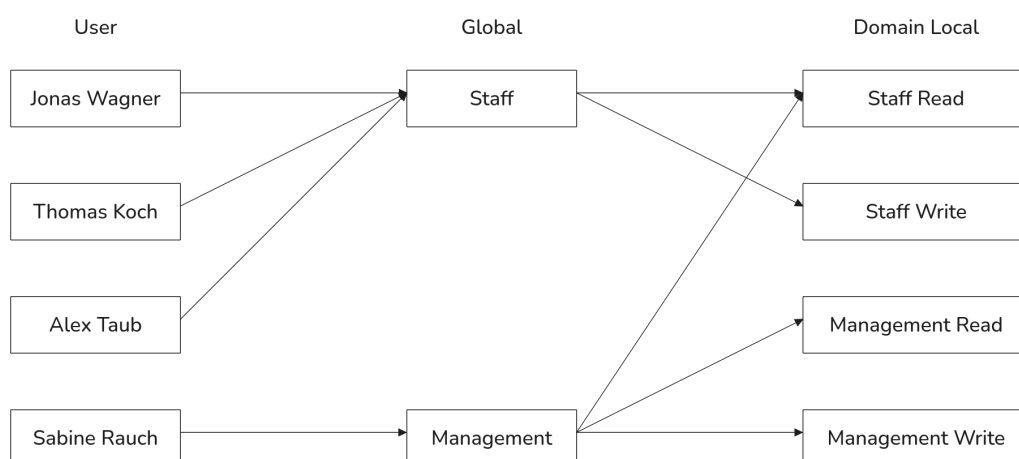


Abbildung 5.1: AGDLP

Die Domain-Locals finden auf einem DFS share anwendung, welcher zwei Verzeichnisse beinhaltet:

- Management
- Sales

Welche Gruppen wie Zugriff haben ist selbsterklärend.

5.5 PKI

1-tier PKI

Name	IP-Adresse	FQDN
CA	192.168.200.10	ca.corp.gartenbedarf.com

Autoenrollment der Zertifikate per GPO für:

- Clients
- VPN

Natürlich dazu auch passende Templates, sowie templates für Sub-CA (notwendig fürs Captive-Portal) und IIS.

5.5.1 CA Konfiguration

Die CA wurde ausschließlich mit der PowerShell aufgesetzt:

```
scripts/windows/Favoriten-CA-part2.ps1
1 $SecureStringPassword = (ConvertTo-SecureString "Ganzgeheim123!" -AsPlainText
  -Force)
2 $DomainAdministratorCredentials = New-Object -TypeName
  System.Management.Automation.PSCredential `
3     -ArgumentList ("Administrator@corp.gartenbedarf.com",
  $SecureStringPassword)
4
5 Add-Computer -DomainName "corp.gartenbedarf.com" `
6     -Credential $DomainAdministratorCredentials `
7     -Restart
8
9 $CAPolicyContent = @"
```

```
scripts/windows/Favoriten-CA-part2.ps1
```

```
10 [Version]
11 Signature="$Windows NT$"
12 [PolicyStatementExtension]
13 Policies=InternalPolicy
14 [InternalPolicy]
15 OID= 1.2.3.4.1455.67.89.5
16 Notice="Legal Policy Statement"
17 URL=http://pki.corp.5cn.at/cps.txt
18 [Certsrv_Server]
19 RenewalKeyLength=2048
20 RenewalValidityPeriod=Years
21 RenewalValidityPeriodUnits=10
22 LoadDefaultTemplates=0
23 AlternateSignatureAlgorithm=1
24 "@
25 $CAPolicyContent > C:\Windows\CAPolicy.inf
26
27 Install-WindowsFeature Adcs-Cert-Authority -IncludeManagementTools
28 Install-AdcsCertificationAuthority -CAType EnterpriseRootCa `
29     -CryptoProviderName "RSA#Microsoft Software Key Storage Provider" `
30     -KeyLength 2048 `
31     -HashAlgorithmName SHA256 `
32     -CACommonName "Gartenbedarf Root CA" `
33     -CADistinguishedNameSuffix "DC=corp,DC=gartenbedarf,DC=com" `
34     -ValidityPeriod Years `
35     -ValidityPeriodUnits 10
36 Certutil -setreg CA\CRLPeriodUnits 1
37 Certutil -setreg CA\CRLPeriod "Weeks"
38 Certutil -setreg CA\CRLDeltaPeriodUnits 1
39 Certutil -setreg CA\CRLDeltaPeriod "Days"
40 Certutil -setreg CA\CRLOverlapPeriodUnits 12
41 Certutil -setreg CA\CRLOverlapPeriod "Hours"
42 Certutil -setreg CA\ValidityPeriodUnits 5
43 Certutil -setreg CA\ValidityPeriod "Years"
44 Certutil -setreg CA\AuditFilter 127
45
46 Certutil -setreg CA\CACertPublicationURLs "1:C:
    \Windows\system32\CertSrv\CertEnroll\%1_%3%4.crt\n2:ldap://"
```



```
scripts/windows/Favoriten-CA-part2.ps1
```

```
CN=%7,CN=AIA,CN=Public Key Services,CN=Services,%6%11\n2:http://pki.corp.
gartenbedarf.com/CertEnroll/%1_%3%4.crt"
47 Certutil -setreg CA\CRLPublicationURLs "65:C:
\Windows\system32\CertSrv\CertEnroll\%3%8%9.crl\n79:ldap:///
CN=%7%8,CN=%2,CN=CDP,CN=Public Key Services,CN=Services,%6%10\n6:http://pki.
corp.gartenbedarf.com/CertEnroll/%3%8%9.crl\n65:file://\
\WEB.corp.gartenbedarf.com\CertEnroll\%3%8%9.crl"
48
49 Copy-Item -Path 'C:
\Windows\System32\CertSrv\CertEnroll\CA.corp.gartenbedarf.com_Gartenbedarf
Root CA.crt' `
50     -Destination '\\WEB.corp.gartenbedarf.com\C$\CertEnroll'
51
52 New-NetFirewallRule -DisplayName "WinRM HTTPS" `
53     -Direction Inbound `
54     -LocalPort 5985 `
55     -Protocol TCP `
56     -Action Allow `
57     -RemoteAddress "192.168.210.1"
58
59 Restart-Computer
```

Quellcode 5.4: CA Konfiguration und Setup

5.5.2 IIS Konfiguration

Der IIS-Server wurde mittels GUI erstellt und beinhaltet folgende Features:

- Directory Browsing (Nur für CertEnroll-Directory)
- HTTPS (mittels Cert-Template)
- URL-Double-Escaping, notwendig für CA

5.6 NPS

NPS wurde als Radius-Server für das Captive-Portal verwendet und kann auf alle Domain-User zugreifen. Dadurch kann ein jeder AD-User, um das Internet zu browsen, seinen eigenen Benutzer verwenden. Die Abfragen wurden mittels NPS-Policy auf die FortiGate begrenzt und gelten ebenfalls auch nur für das VLAN der Workstations.

5.7 DFS

Es wurde ein DFS angelegt, welches zwei Shares kombiniert:

- Management -> DC1
- Sales -> DC2

Der Kombinierte DFS Share trägt den Namen „Staff“ und wird mittels GPO on Logon gemounted. Auf den Verzeichnissen im DFS liegen Permissions nach AGDLP-Konzept.

5.8 GPOs

- Desktophintergrund setzen und Veränderung verbieten
- Last logged in User nicht anzeigen
- Mount Drive
- PWD Security-Richtlinie
- Removable Media verbieten
- Registry-Zugriff einschränken
- PKI-Zertifikate automatisch enrollen

5.8.1 Security Baseline

Natürlich wurde auch die Windows Security Baseline eingespielt. Die dazugehörigen GPOs kann man sich einfach vom Internet ziehen: <https://www.microsoft.com/en-us/download/details.aspx?id=55319>

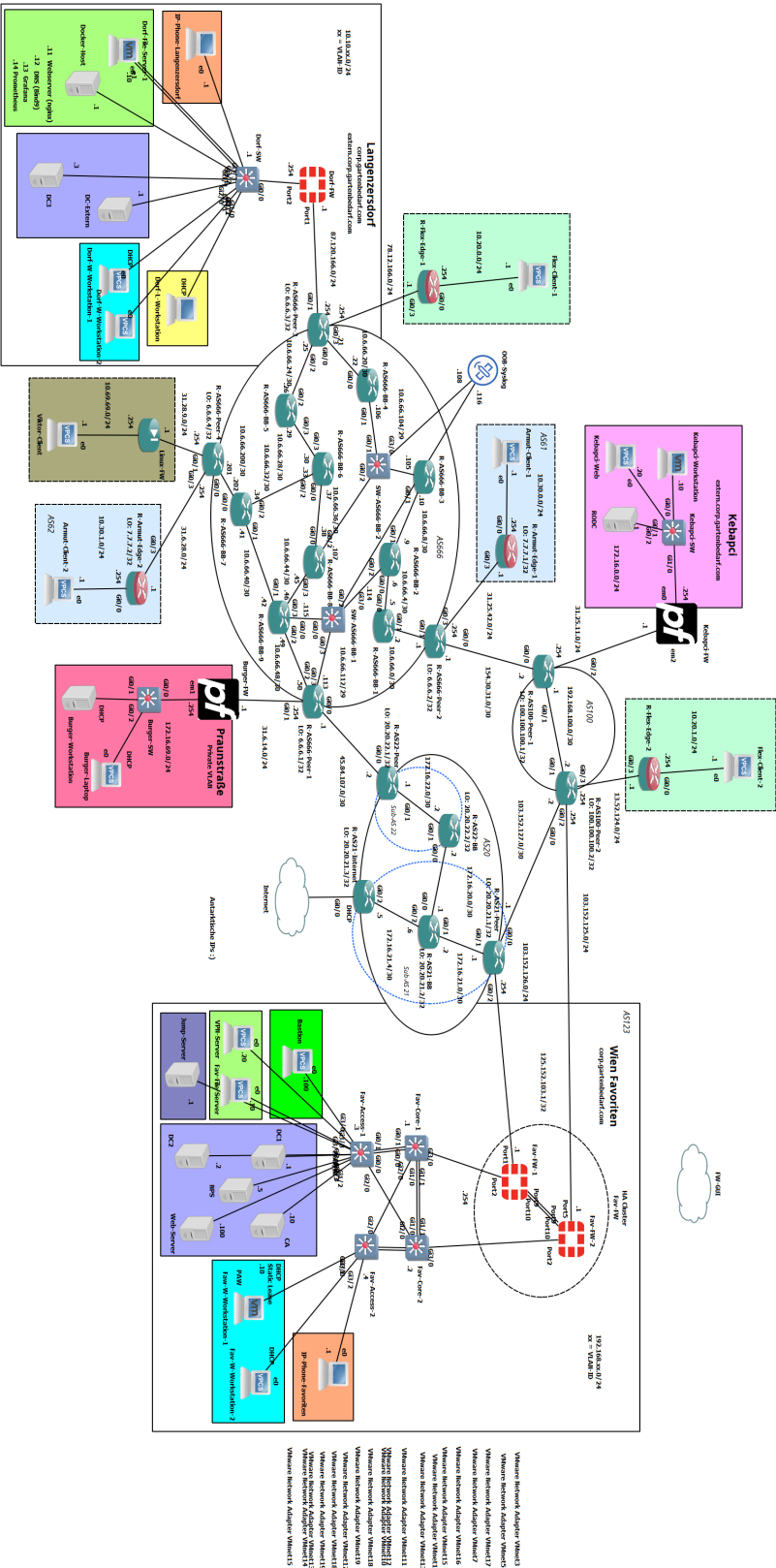
TODO: Heruntergeladene Objekte auflisten

5.8.2 LAPS

LAPS wurde ebenfalls angewandt, hiermit werden die Passwörter der Lokalen Administratoren ebenfalls vom AD verwaltet, heruntergeladen werden kann sich der Installer vom Internet: <https://www.microsoft.com/en-us/download/details.aspx?id=46899>>

Auf den DCs wurden die GPOs draufgespielt und auf Computer in einer bestimmte OU namens „LAPS“ angewandt. Diese OU wurde speziell für diesen Zweck erstellt.

A Gesamte logische Topologie



B Cisco-Gerät Grundkonfiguration

```
1  ! David Koch & Julian Burger 5CN
2  ! Little Big Topo
3  ! BASE
4  ! =====
5
6  en
7  conf t
8  hostname BASE
9  no ip domain-lookup
10 ip domain name 5CN
11 banner motd *!!!KEEP OUT - Property of Koch & Burger!!!*
12 service password-encryption
13 username cisco priv 15
14 username cisco algorithm-type scrypt secret cisco
15 crypto key generate rsa usage-keys modulus 1024
16 ip ssh version 2
17
18 line vty 0 15
19 login local
20 logging synchronous
21 exec-timeout 0 0
22 transport input telnet ssh
23 exit
24
25 line con 0
26 logging synchronous
27 exec-timeout 0 0
28 exit
29
30 ! config goes here
31
32 end
33 wr
```

Abkürzungsverzeichnis

AS: Autonomes System <i>S.: 6, 12</i>	<i>Glossar (S. 56)</i>
BB: Backbone <i>Nicht Referenziert</i>	
BGP: Border Gateway Protocol <i>S.: 9, 10, 11, 12, 13</i>	<i>Glossar (S. 56)</i>
FW: Firewall <i>Nicht Referenziert</i>	<i>Glossar (S. 56)</i>
HA: High Availability <i>S.: 17</i>	
IP: Internet Protocol <i>Nicht Referenziert</i>	
MPLS: Multi-Protocol Label Switching <i>S.: 9, 10</i>	
NAT: Network Address Translation <i>S.: 6, 13</i>	<i>Glossar (S. 56)</i>
OSPF: Open Shortest Path First <i>S.: 9, 10, 12</i>	<i>Glossar (S. 56)</i>
PoP: Point of Presence <i>S.: 8</i>	<i>Glossar (S. 56)</i>
RIP: Routing Information Protocol <i>S.: 12</i>	<i>Glossar (S. 56)</i>

SOTA: State of the Art
Nicht Referenziert

Glossar (S. 56)

VPCS: Virtual PC Simulator
S.: 38

Glossar (S. 56)

Glossar

Autonomes System: TODO

Border Gateway Protocol: TODO

Firewall: Ein Netzwerkgerät das zur sicheren Trennung von Netzwerk dient. Wird meist zur Abgrenzung eines privaten Netzwerks zum Internet verwendet.

Network Address Translation: Die Veränderung einer privaten IP-Adresse auf eine öffentliche, um die von ihr geschickten Daten im Internet routbar zu machen.

Open Shortest Path First: Ein dynamisches Link-State Routingprotokoll

Point of Presence: TODO

Routing Information Protocol: Ein dynamisches Distance-Vektor Routingprotokoll

State of the Art: Der neuste Stand der Technik

Virtual PC Simulator: Ein in GNS3 vorinstalliertes Gerät bzw. Programm, welches einen simplen Client-PC simuliert.

Literaturverzeichnis

Allianz SE, 2024. „Cyber attacks on critical infrastructure“. [Online]

Verfügbar unter: <https://commercial.allianz.com/news-and-insights/expert-risk-articles/cyber-attacks-on-critical-infrastructure.html>

[Zugriff am 19.12.2024].

Canonical Group Ltd., 2024. *Cloud-init documentation*. [Online]

Verfügbar unter: <https://cloudinit.readthedocs.io/en/latest/index.html>

[Zugriff am 14.12.2024].

Cybersecurity & Infrastructure Security Agency (USA), 2024. *Defending OT Operations Against Ongoing Pro-Russia Hactivist Activity*. [Online]

Verfügbar unter: <https://www.cisa.gov/sites/default/files/2024-05/defending-ot-operations-against-ongoing-pro-russia-hactivist-activity-508c.pdf>

[Zugriff am 19.12.2024].

Die neue NIS-2-Richtlinie, 2025. . [Online]

Verfügbar unter: <https://www.nis.gv.at/nis-2-richtlinie.html>

[Zugriff am 2024].

Engrie, M., 2021. *ESP32 meets Raspberry Pi*. [Online]

Verfügbar unter: https://data.engrie.be/ESP32/ESP32_-_Part_12_-_ESP32_meets_Raspberry_Pi.pdf

[Zugriff am 13.12.2024].

Exabeam, 2024. „9 Lateral Movement Techniques and Defending Your Network“. [Online]

Verfügbar unter: <https://www.exabeam.com/explainers/what-are-ttps/9-lateral-movement-techniques-and-defending-your-network/>

[Zugriff am 19.12.2024].

Fortinet Inc., 2024a. *Lateral Movement Definition*. [Online]

Verfügbar unter: <https://www.fortinet.com/resources/cyberglossary/lateral-movement>

[Zugriff am 19.12.2024].

Fortinet Inc., 2024b. *Sichere Betriebstechnologie*. [Online]

Verfügbar unter: <https://www.fortinet.com/de/solutions/enterprise-midsize-business/ot-security>

[Zugriff am 19.12.2024].

Fortinet Inc., 2025. *VDOM overview*. [Online]

Verfügbar unter: <https://docs.fortinet.com/document/fortigate/7.6.1/administration-guide/597696/vdom-overview>

[Zugriff am 5.1.2025].

Informationstechnik (BSI), 2014. *Die Lage der IT-Sicherheit in Deutschland 2014*. [Online]

Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile

[Zugriff am 23.12.2024].

IPC2U GmbH, 2017. *Detailed description of the Modbus TCP protocol with command examples*. [Online]

Verfügbar unter: <https://ipc2u.com/articles/knowledge-base/detailed-description-of-the-modbus-tcp-protocol-with-command-examples/>

[Zugriff am 23.12.2024].

Irazabal, J.-M. und Blozis, S., 2003. „AN10216-01 (I²C Manual)“. [Online]

Verfügbar unter: <https://www.nxp.com/docs/en/application-note/AN10216.pdf>

[Zugriff am 13.12.2024].

KWOCO Automation Co., L., 2024. *Welche SPS wird in der Industrie am häufigsten eingesetzt? Die wichtigsten SPS erklärt*. [Online]

Verfügbar unter: <https://kwoco-plc.com/de/most-used-plc-in-industry/>

[Zugriff am 23.12.2024].

Lukas Milevski, 2011. *STUXNET AND STRATEGY – A Special Operation in Cyberspace?*. [Online]

Verfügbar unter: https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-63/jfq-63_64-69_Milevski.pdf?ver=Jy0SW9E8UBbatlrmrw-egQ%3D%3D

[Zugriff am 24.12.2024].

MITRE ATT&CK, 2023. *TA0109*. [Online]

Verfügbar unter: <https://attack.mitre.org/tactics/TA0109/>

[Zugriff am 19.12.2024].

NIS2 Richtlinie, 2025. . [Online]

Verfügbar unter: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj?locale=de>

[Zugriff am 27.12.2022].

Pahl, A. und Dickmann, S., 2022. *Analysis of sensor disturbances caused by IEMI*. Aachen, Germany: Apprimus. [Online]

Verfügbar unter: <https://doi.org/10.15488/12572>.

Patrick Beuth, 2020. „Die erste Cyberwaffe und ihre Folgen“. [Online]
Verfügbar unter: <https://www.spiegel.de/netzwelt/web/die-erste-cyberwaffe-und-ihre-folgen-a-a0ed08c9-5080-4ac2-8518-ed69347dc147>
[Zugriff am 24.12.2024].

Ruddy, K., 2021. „How Automated Provisioning Tools Pave the Way to Multi-Cloud Adoption“. [Online]
Verfügbar unter: <https://www.hashicorp.com/blog/how-automated-provisioning-tools-pave-the-way-to-multi-cloud-adoption>
[Zugriff am 14.12.2024].

Siemens AG, 2024. *Automatisierung passiert nicht automatisch*. [Online]
Verfügbar unter: <https://www.siemens.com/de/de/unternehmen/konzern/geschichte/specials/175-jahre/simatic.html>
[Zugriff am 23.12.2024].

Thiago Alves, 2022. *OpenPLC Overview*. [Online]
Verfügbar unter: <https://autonomylogic.com/docs/openplc-overview/>
[Zugriff am 23.12.2024].