Höhere Technische Bundeslehranstalt Wien 3, Rennweg

Höhere Abteilung für Mechatronik
Höhere Abteilung für Informationstechnologie
Fachschule für Informationstechnik

Dokumentationsbuch

Little Big Topo
Team 4

durch

David Koch

Julian Burger

unter Anleitung von

Christian Schöndorfer

Clemens Kussbach

Wien, 29.01.2025

Inhaltsverzeichnis

1 Einführung

AAAAAAAAAAA

1.1 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 futtern, ABER die Gartenbedarfs GmbH ist heimlich mit Kebapci geschäftlich und infrastrukturtechnisch verwickelt, da Kepabci als Front für die Schwarzarbeit und Geldwäsche der Gartenbedarfs GmbH genutzt wird.

1.2 Topologie

40 Netzwerkgeräte 28 Endgeräte

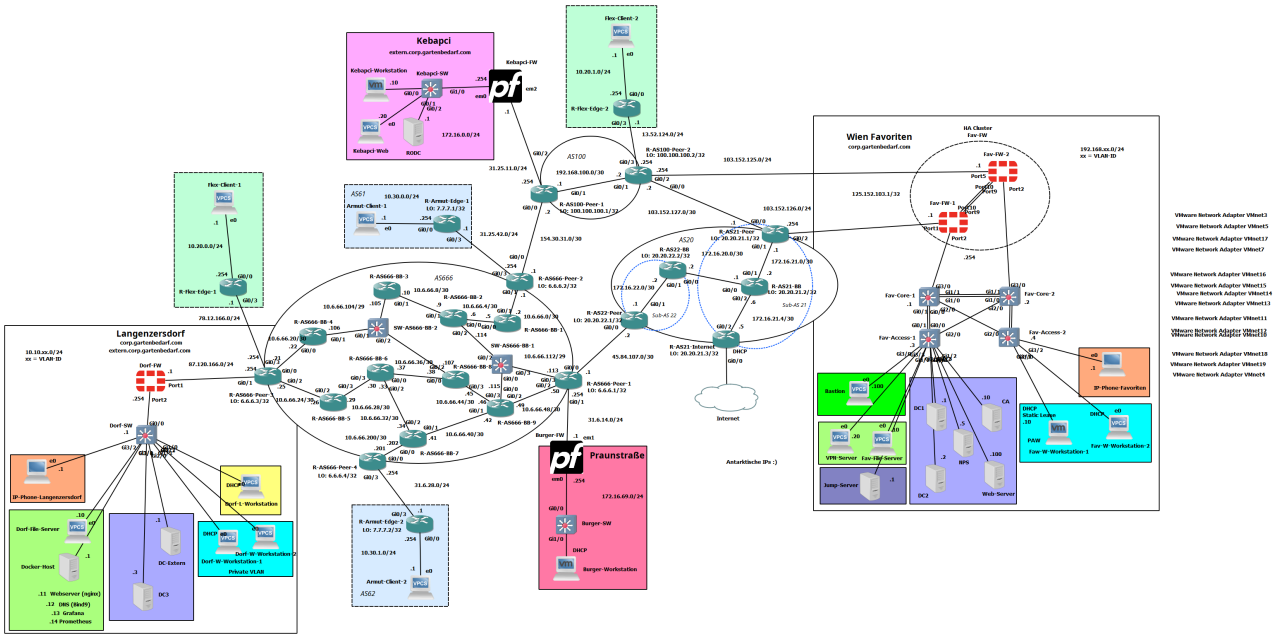

Abbildung 1.1: Der logische Topologieplan (v7)

Der Zugang ins Internet ist durch die Anbindung einer NAT-Cloud an AS20 bzw. AS21 ermöglicht worden.

1.3 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.

Um die zwei miteinander zu verbinden, wurde in GNS die IP-Addresse 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

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

2.4 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[2] wird BGP verwendet.

2.4.1 Authentifizierung

Jegliche Instanzen von OSPF, RIP und BGP 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
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
```

[1] *Routing Information Protocol*: Ein dynamisches Distance-Vektor Routingprotokoll
[2] *Autonomes System*: TODO

```
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: BeeGeePee!?
- 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[1]-Cloud zu ermöglichen.

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

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 industrienahe 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

scripts/fortinet/Fav-FW-1.conf

```
6   config system global
7       set hostname Fav-FW-1
8       set admintimeout 30
9       set timezone 26
10  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.

scripts/fortinet/Fav-FW-1.conf

```
20   config system interface
21       edit port3
22           set desc "Used to enroll VM license OOB"
23           set mode static
24           set ip 192.168.0.100 255.255.255.0
25           set allowaccess ping http https
26       next
27       edit port1
28           set desc "to_R_AS21_Peer"
29           set mode static
30           set ip 103.152.126.1 255.255.255.0
31           set role wan
32           set allowaccess ping
33       next
…                                          …
61       edit VLAN_20
62           set desc "Windows Clients"
63           set vdom root
64           set interface port2
65           set type vlan
66           set vlanid 20
67           set mode static
68           set ip 192.168.20.254 255.255.255.0
69           set allowaccess ping
70       next
…                                          …
151  end
```

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

3.1.3 Lizensierung

3.1.4 Policies

3.1.5 HA Cluster

Ein High Availabity Cluster besteht aus zwei oder mehr FortiGates 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)

scripts/fortinet/Fav-FW-1.conf

```
12  config system ha
13      set mode a-a
14      set group-id 1
15      set group-name Koch_Burger_LBT_Cluster
16      set password ganzgeheim123!
17      set hbdev port9 10 port10 20
18  end
```

Quellcode 3.3: 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:

BILD

Zur Überprüfung können folgende Befehle verwendet werden:

- fdfdfd
- fdfdfdf

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 3.4: Das UDP-Packet für den DoS-Angriff auf die S7-1200

3.1.7 DHCP

3.1.8 VPNs

3.1.9 Captive Portal

3.1.10 SSL Inspection

3.1.11 Traffic Shaping

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 Websiten 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 3.5: Das UDP-Packet für den DoS-Angriff auf die S7-1200

```
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 3.6: Das UDP-Packet für den DoS-Angriff auf die S7-1200

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 FlexVPN Cisco-proprietär ist.

3.3.1 FlexVPN

scripts/cisco/R-Flex-Edge-1

```
42  crypto ikev2 keyring mykeys
43  peer R-Flex-Edge-2
44  address 13.52.124.1
45  pre-shared-key IchMussFlexen!
46  ex
47
48  crypto ikev2 profile default
49  match identity remote address 13.52.124.1 255.255.255.255
50  authentication local pre-share
51  authentication remote pre-share
52  keyring local mykeys
53  dpd 60 2 on-demand
54  ex
55
56  crypto ipsec profile default
57  set ikev2-profile default
58  ex
59
60  int tun0
61  ip address 10.20.69.1 255.255.255.0
62  tunnel source g0/3
63  tunnel destination 13.52.124.1
64  tunnel protection ipsec profile default
65  ex
```

Quellcode 3.7: FlexVPN-Konfiguration auf R-Flex-Edge-1

4 Standorte

4.1 Wien Favoriten

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

4.2 Langenzersdorf

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

4.3 Kebapci

4.4 Praunstraße

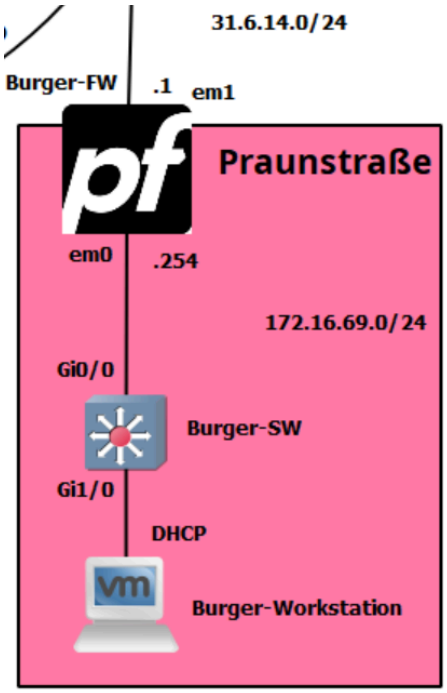

Abbildung 4.1: Der Standort Praunstraße

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.

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

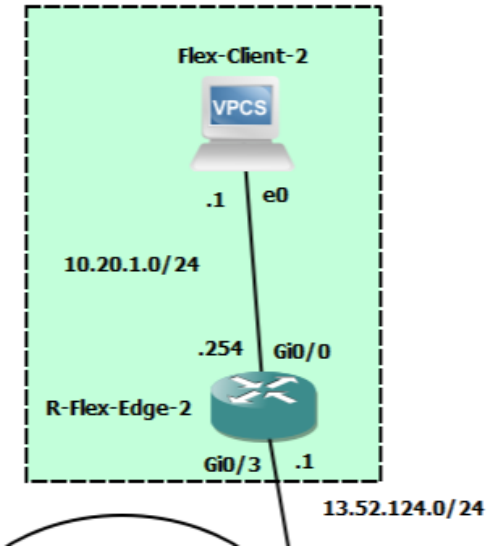

Abbildung 4.2: Der zweite Flex-Standort

4.6 Armut-Standorte

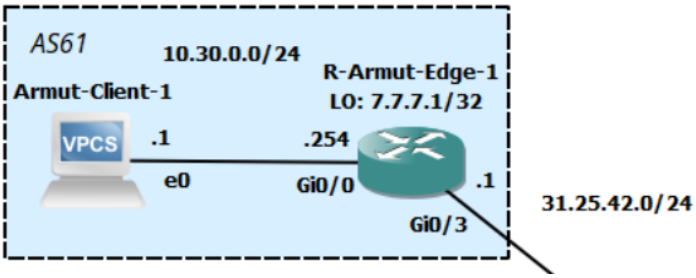

Abbildung 4.3: Der erste Armut-Standort

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

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

- RODC ist Read-Only (duh)
- 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

Bezeichnung	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, NPS, Web-Server, ...

5.2.4 Workstations

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

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

5.3 Users & Computers

AGDLP

OUs

5.4 PKI

1-tier PKI

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

Autoenrollment der Zertifikate per GPO für:

- Clients
- VPN

5.5 NPS

5.6 IPAM

5.7 GPOs

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

Abkürzungsverzeichnis

AS: Autonomes System *Glossar (S. 29)*
S.: 11

OSPF: Open Shortest Path First *Glossar (S. 29)*
S.: 8, 9, 11

RIP: Routing Information Protocol *Glossar (S. 29)*
S.: 11

BGP: Border Gateway Protocol *Glossar (S. 29)*
S.: 8, 9, 10, 11, 12

IP: Internet Protocol
Nicht Referenziert

BB: Backbone
Nicht Referenziert

MPLS: Multi-Protocol Label Switching
S.: 8, 9

FW: Firewall *Glossar (S. 29)*
Nicht Referenziert

SOTA: State of the Art *Glossar (S. 29)*
Nicht Referenziert

PoP: Point of Presence *Glossar (S. 29)*
S.: 7

HA: High Availabity
S.: 15

VPCS: Virtual PC Simulator *Glossar (S. 29)*
S.: 22

NAT: Network Address Translation *Glossar (S. 29)*
S.: 12

Glossar

Autonomes System: TODO

Open Shortest Path First: Ein dynamisches Link-State Routingprotokoll

Routing Information Protocol: Ein dynamisches Distance-Vektor Routingprotokoll

Border Gateway Protocol: TODO

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

State of the Art: Der neuste Stand der Technik

Point of Presence: TODO

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

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

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 Hacktivist Activity*. [Online]
Verfügbar unter: https://www.cisa.gov/sites/default/files/2024-05/defending-ot-operations-against-ongoing-pro-russia-hacktivist-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 (I^2C 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]