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 **4**
1.1 Firma Backstory 4
1.2 Topologie 4
1.3 Verwendete Geräte & Software 5

2 Backbone **7**
2.1 Namenskonvention 7
2.2 Addressbereiche 7
2.3 Autonome Systeme 8
2.3.1 AS20 8
2.3.2 AS100 9
2.3.3 AS666 9
2.4 Dynamisches Routing 11
2.4.1 Authentifizierung 11
2.5 Statisches Routing 12

3 Firewalls **13**
3.1 FortiGate 13
3.1.1 Grundkonfiguration 13
3.1.2 Interfaces 13
3.1.3 Lizensierung 15
3.1.4 Policies 15
3.1.5 HA Cluster 15
3.1.6 NAT 16
3.1.7 DHCP 17
3.1.8 VPNs 17
3.1.9 Captive Portal 17
3.1.10 SSL Inspection 17
3.1.11 Traffic Shaping 18
3.1.12 Webfilter 20
3.2 PfSense 21
3.3 Cisco Router 22
3.3.1 FlexVPN 22
3.3.2 MPLS Overlay VPN 23

4 Standorte **24**
4.1 Wien Favoriten 24
4.2 Langenzersdorf 24
4.3 Kebapci 25
4.4 Praunstraße 25
4.5 Flex-Standorte 25
4.6 Armut-Standorte 26

5 Active Directory **27**
5.1 Überblick 27
5.2 Geräte 27
5.2.1 Domain Controller 27
5.2.2 Jump Server 28
5.2.3 CA + PKI 28
5.2.4 NPS 28
5.2.5 Workstations 28
5.3 PowerShell Konfiguration 29
5.4 Users & Computers 31
5.5 PKI 32
5.5.1 CA Konfiguration 32
5.5.2 IIS Konfiguration 34
5.6 NPS 34
5.7 DFS 35
5.8 GPOs 35
5.8.1 Security Baseline 35
5.8.2 LAPS 35

Abkürzungsverzeichnis **36**

Glossar **38**

Literaturverzeichnis **38**

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

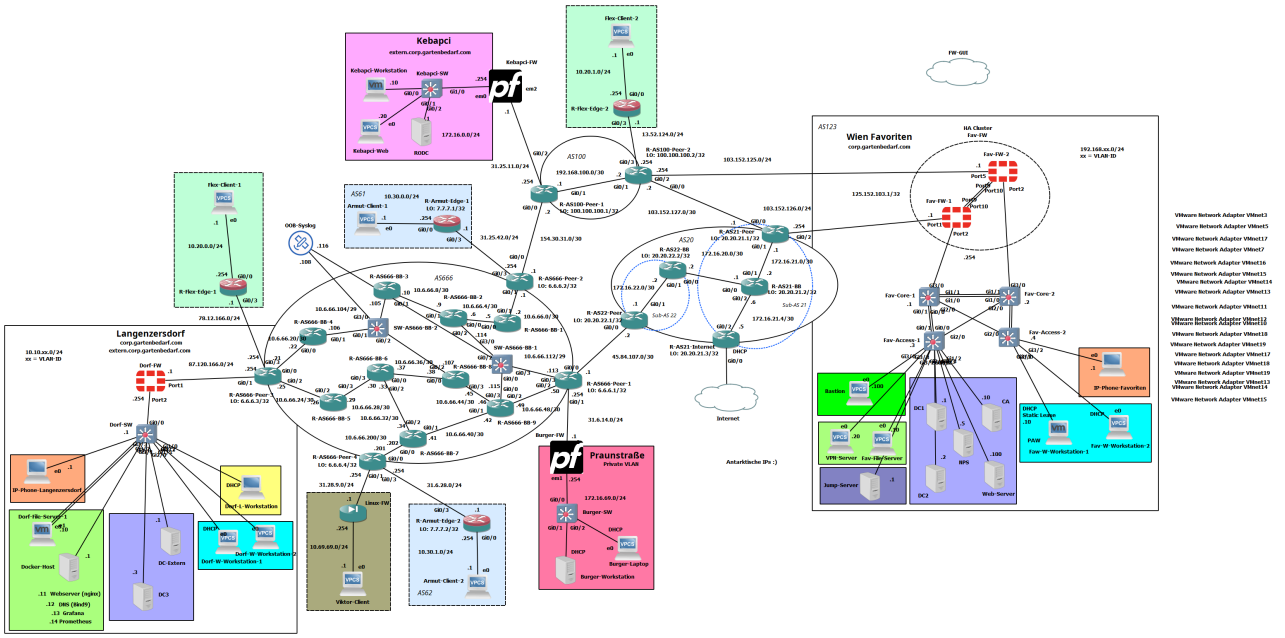

Abbildung 1.1: Der logische Topologieplan (v9)

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

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:

- fdfdfd
- fdfd
- hghgghgh

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 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
5 ex
6
7 int g0/1
```

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

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

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      set override enable
```

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

3.1.7 DHCP

3.1.8 VPNs

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:

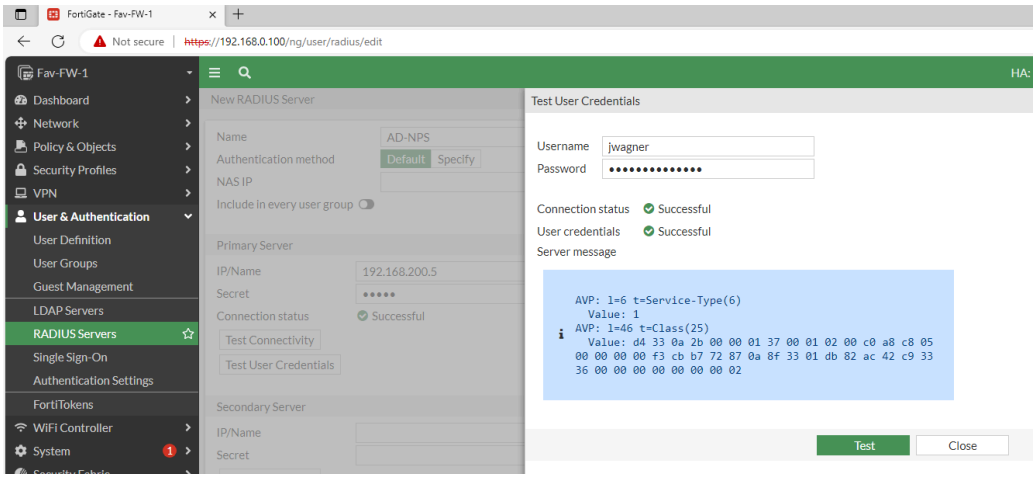

Abbildung 3.1: Die erfolgreiche Authentifizierung mit AD-Benutzer über RADIUS

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).

AAAAAAAAAAa

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 einen garantiere Bandbreite von 300kbps.
- Youtube-Streaming bekommt die mittlere Prioritätsstufe und hat einen 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-priorty` 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 3.5: Die Konfiguration der Traffic-Shaping-Stufen

```
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 3.6: 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 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 3.7: 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 3.8: Das Webfilter-Profile für die Aktivierung der URL-Filter

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

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
```

scripts/cisco/R-Flex-Edge-1

```
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 3.9: 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 Routern XXX und YYY — realisiert. Folgende Konfigurationsschritte sind für einen MPLS Overlay VPN nötig:

- Im Backbone wird MPLS zur Datenübertragung verwendet
- Die Border-Router haben VRFs für die Verbindung der Standorte
- Die Edge-Router der Standorte peeren mit den Border-Routern über BGP
- 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.

4.2 Langenzersdorf

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

4.3 Kebapci

4.4 Praunstraße

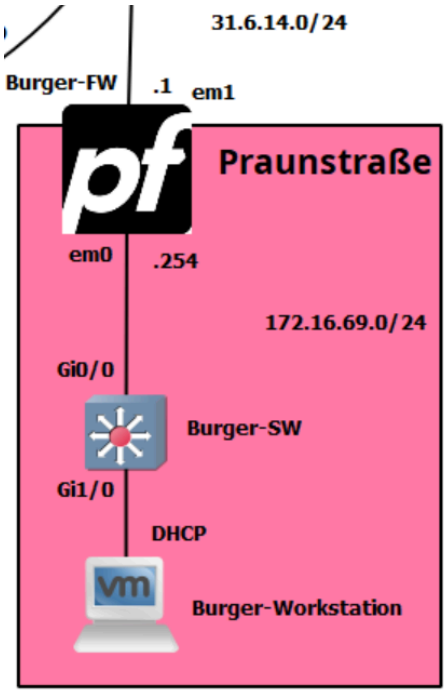

Abbildung 4.1: Der Standort Praunstraße

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.

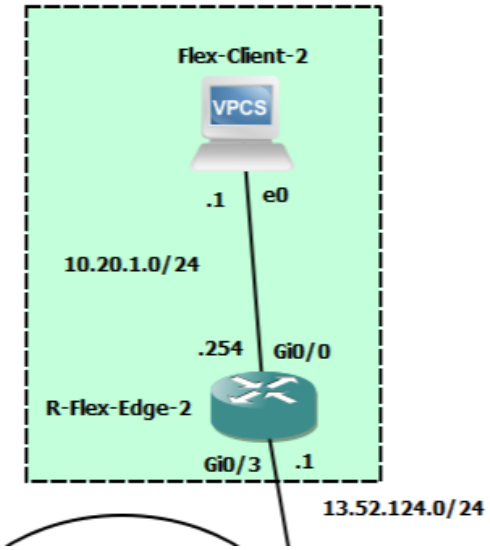

Abbildung 4.2: Der zweite Flex-Standort

```
scripts/cisco/R-Flex-Edge-2
69  router eigrp 100
70  no auto-summary
71  network 10.20.1.0 0.0.0.255
72  network 10.20.69.0 0.0.0.255
73  ex
```

Quellcode 4.1: EIGRP-Konfiguration auf R-Flex-Edge-2

4.6 Armut-Standorte

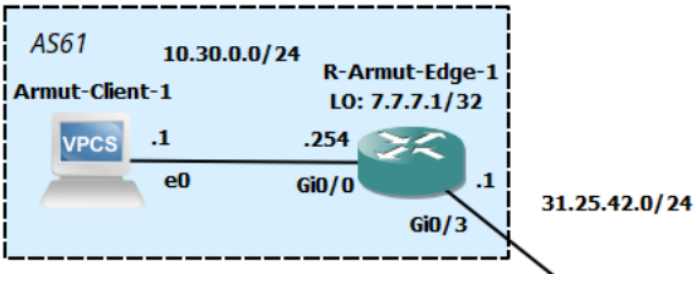

Abbildung 4.3: Der erste Armut-Standort

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

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 Priviliged 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-Scripts konfiguriert. Lediglich GUI-Exclusive 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 wiefolgt 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 wiefolgt unterteilt:

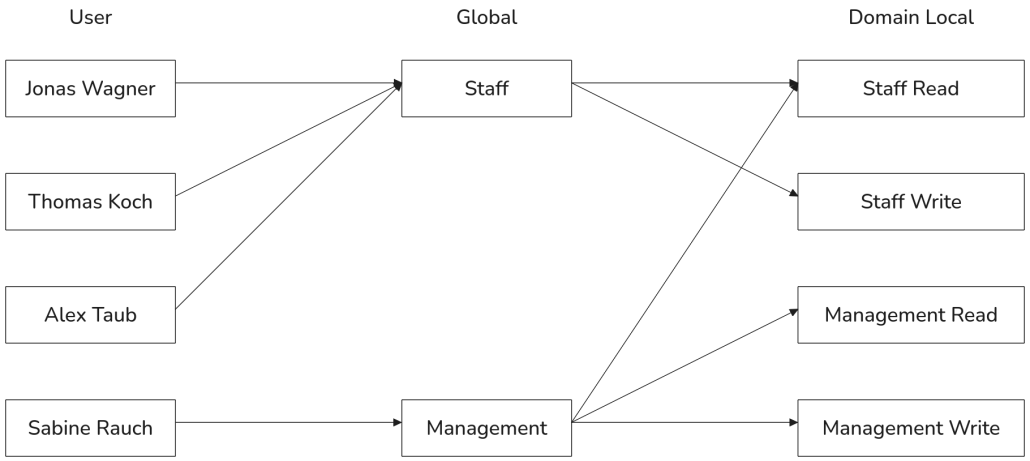

Abbildung 5.1: AGDLP

Die Domain-Locals finden auf einem DFS share anwendung, welcher zwei Verzeichnise 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

```
[Version]
Signature="$Windows NT$"
[PolicyStatementExtension]
Policies=InternalPolicy
[InternalPolicy]
OID= 1.2.3.4.1455.67.89.5
Notice="Legal Policy Statement"
URL=http://pki.corp.5cn.at/cps.txt
[Certsrv_Server]
RenewalKeyLength=2048
RenewalValidityPeriod=Years
RenewalValidityPeriodUnits=10
LoadDefaultTemplates=0
AlternateSignatureAlgorithm=1
"@
$CAPolicyContent > C:\Windows\CAPolicy.inf

Install-WindowsFeature Adcs-Cert-Authority -IncludeManagementTools
Install-AdcsCertificationAuthority -CAType EnterpriseRootCa `
    -CryptoProviderName "RSA#Microsoft Software Key Storage Provider" `
    -KeyLength 2048 `
    -HashAlgorithmName SHA256 `
    -CACommonName "Gartenbedarf Root CA" `
    -CADistinguishedNameSuffix "DC=corp,DC=gartenbedarf,DC=com" `
    -ValidityPeriod Years `
    -ValidityPeriodUnits 10
Certutil -setreg CA\CRLPeriodUnits 1
Certutil -setreg CA\CRLPeriod "Weeks"
Certutil -setreg CA\CRLDeltaPeriodUnits 1
Certutil -setreg CA\CRLDeltaPeriod "Days"
Certutil -setreg CA\CRLOverlapPeriodUnits 12
Certutil -setreg CA\CRLOverlapPeriod "Hours"
Certutil -setreg CA\ValidityPeriodUnits 5
Certutil -setreg CA\ValidityPeriod "Years"
Certutil -setreg CA\AuditFilter 127

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 Verzeichnisen 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 angewand, 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&gt

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.

Abkürzungsverzeichnis

AS: Autonomes System *Glossar (S. 38)*
S.: 11

OSPF: Open Shortest Path First *Glossar (S. 38)*
S.: 8, 9, 11

RIP: Routing Information Protocol *Glossar (S. 38)*
S.: 11

BGP: Border Gateway Protocol *Glossar (S. 38)*
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. 38)*
Nicht Referenziert

SOTA: State of the Art *Glossar (S. 38)*
Nicht Referenziert

PoP: Point of Presence *Glossar (S. 38)*
S.: 7

HA: High Availabity
S.: 15

VPCS: Virtual PC Simulator *Glossar (S. 38)*
S.: 25

NAT: Network Address Translation *Glossar (S. 38)*
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.