

Little Big Topo Dokumentation

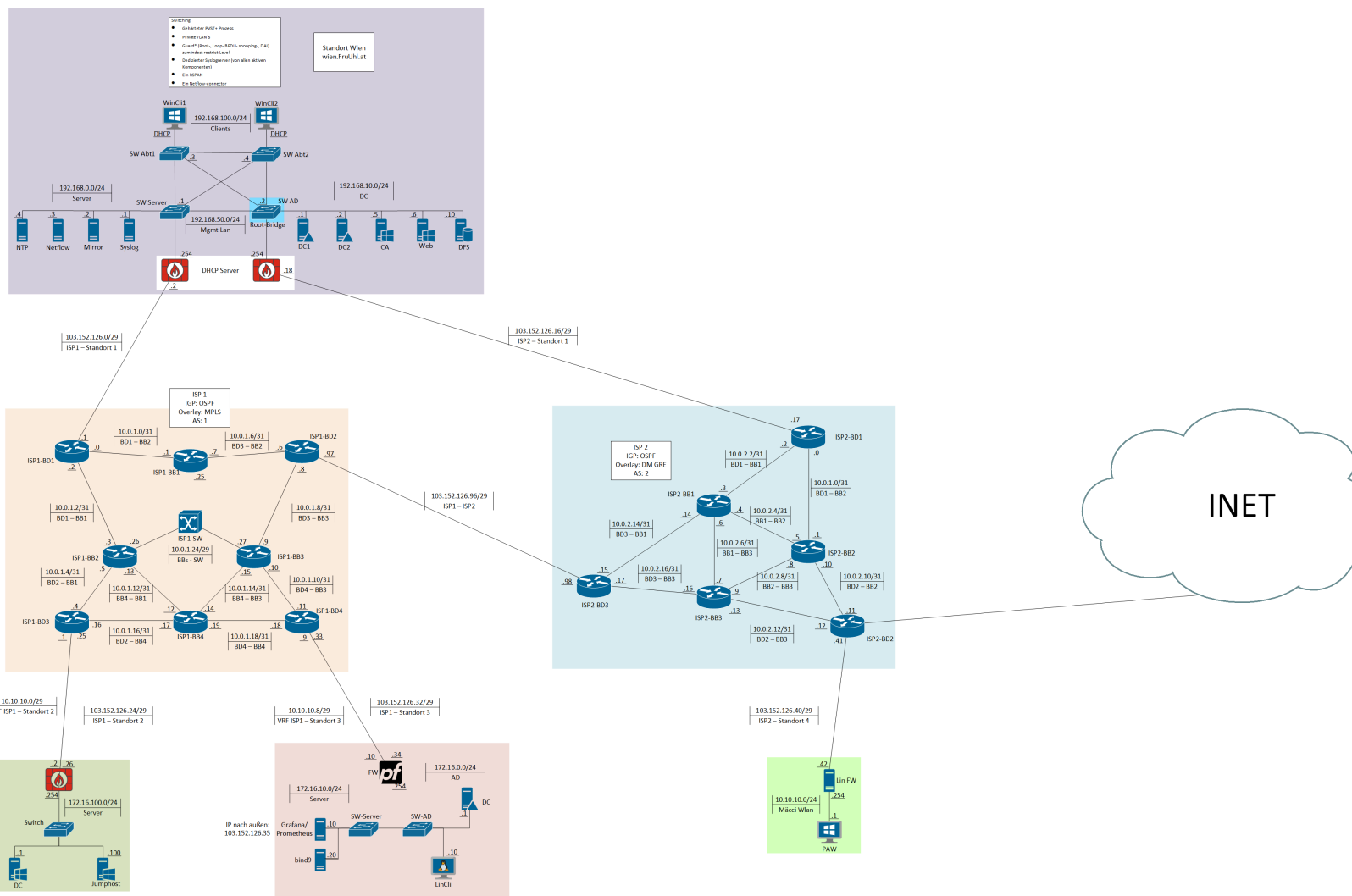
Projekttitle: Little Big Topo
Auftraggeber: SDO, KUS
Auftragnehmer: Linus Frühstück, Bastian Uhlig
Schuljahr: 2024/25 **Klasse:** 5CN

VERSION	DATUM	AUTOR/IN	ÄNDERUNG
v1.0	12.03.2025	Bastian Uhlig	Erstellung des Dokuments
v1.1	12.03.2025	Linus Frühstück	ISP1
v1.2	13.03.2025	Linus Frühstück	ISP2
v1.3	13.03.2025	Bastian Uhlig	AD Dokumentation
v1.4	13.03.2025	Linus Frühstück	Firewalls

Inhaltsverzeichnis

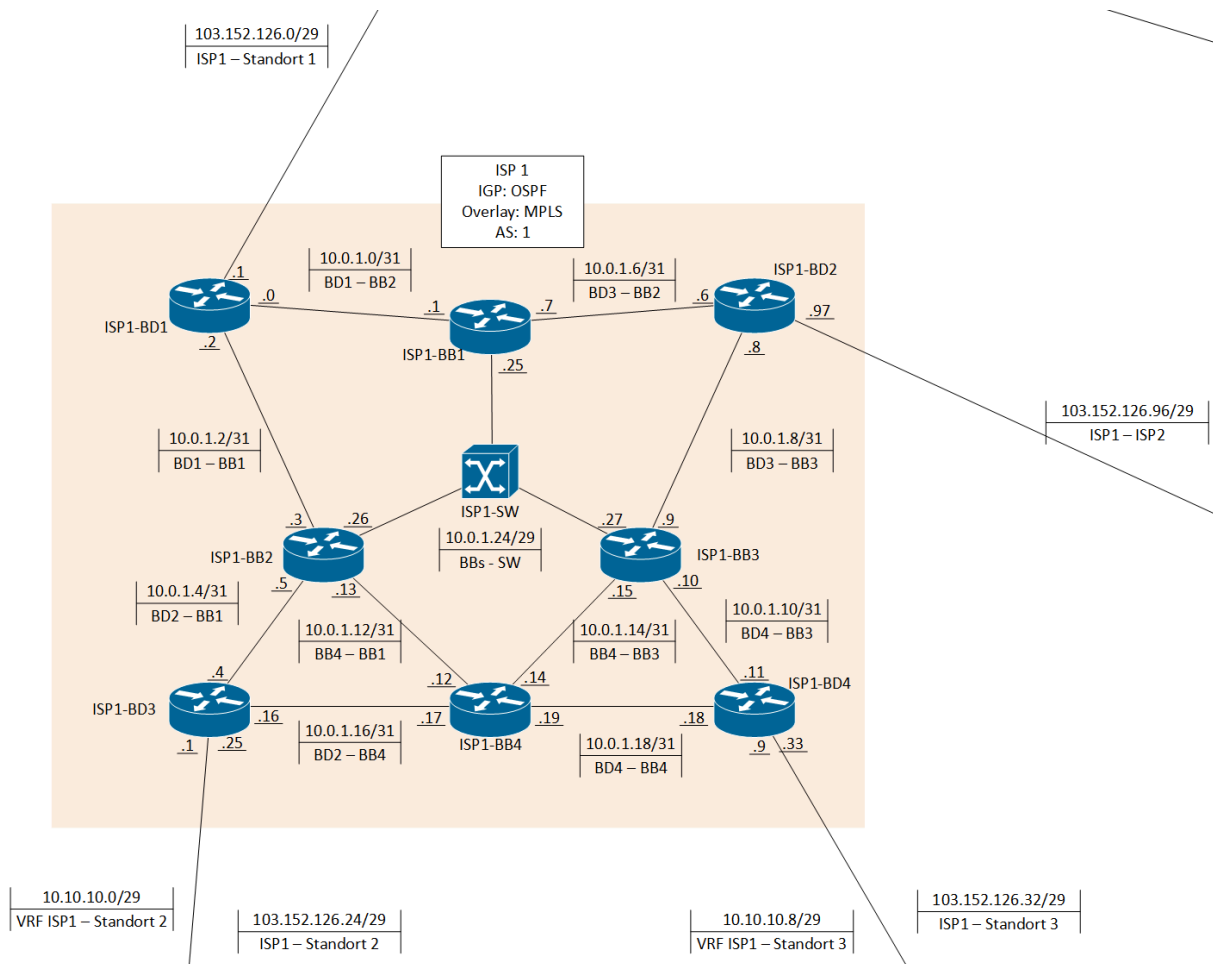
1	Netzplan	3
2	ISP 1	4
2.1	Plan	4
2.2	Allgemeine Informationen	4
2.3	Grundkonfig	5
2.4	Interfaces	6
2.5	Bogon Block ACL	7
2.6	OSPF	8
2.7	BGP	9
2.8	VRF	9
3	ISP 2	11
3.1	Plan	11
3.2	Allgemeine Informationen	12
3.3	Grundkonfig	12
3.4	Interfaces	12
3.5	Bogon Block ACL	13
3.6	OSPF	14

3.7 BGP	15
3.8 DMVPN	15
4 Standort Wien	17
4.1 Plan	17
4.2 Allgemeine Informationen	18
4.3 Windows	18
4.3.1 Gruppen	19
4.3.2 OUs	19
4.3.3 Screenshots	19
4.3.3.1 Sites	19
4.4 Switching	19
4.4.1 Spanning Tree	20
4.4.2 RSPAN	20
4.4.3 Netflow	20
4.4.4 Syslog	20
4.4.5 Authentication	20
4.5 Features FG Wien	21
5 Standort Rennweg	21
5.1 Plan	21
5.2 Allgemeine Informationen	22
5.3 Features FG Rennweg	22
6 Standort Graz	23
6.1 Plan	23
6.2 Allgemeine Informationen	24
6.3 Features PF Graz	24



2 ISP 1

2.1 Plan



2.2 Allgemeine Informationen

- 4 Border Router
- 3 Backbone Router
- 1 Switch

IGP: OSPF

Overlay Netz : MPLS

Netz: 10.0.1.0 - 10.0.1.18 /31

Loopbacks für BGP: 10.0.1.101 - 10.0.1.104 /32

Bogon Filter auf den public Interfaces

Ein VRF auf Border 3 & Border 4 um Standort Rennweg mit Graz zu verbinden. Dazu werden die privaten Netzze der beiden Standorte mit OSPF verteilt und anschließend über BGP weiterverteilt.

2.3 Grundkonfig

Die Grundkonfiguration ist auf allen Geräten gleich.

```
1  !----- bash
2  ! Name des Geräts
3  !-----
4
5  ! Grundkonfiguration (Basic Configuration)
6
7  en                ! Enter enable mode
8  conf t            ! Enter global configuration mode
9  hostname Name_des_Geraets ! Set the hostname of the device
10
11 ip domain-name Lil-BT_FRU_UHL ! Define the domain name
12 username cisco priv 15 algo sc sec cisco
13 ! Create a local user "cisco" with privilege level 15 (full access)
14 ! 'algo sc sec' specifies password encryption (scrypt)
15 ! Password is set to 'cisco'
16
17 no ip domain-lo ! (This command is to disable domain lookup)
18 crypto key generate rsa us mod 1024
19
20 ! Generate an RSA key for SSH with a 1024-bit modulus
21 ip ssh version 2 ! Enforce SSH version 2 for secure remote access
22 service password-enc ! Enable encryption of plaintext passwords
23 mpls ip ! Enable MPLS (Multiprotocol Label Switching) on the device
24
25 ! Configure Virtual Terminal (VTY) lines for remote access
26 line vty 0 924
27 logging sync ! Synchronize log messages with command output
```

```

28 transport input ssh ! Allow only SSH for remote access (no Telnet)
29 login local ! Use local user authentication
30 exec-time 0 ! Disable automatic timeout
31 exit
32
33 ! Configure Console line settings
34 line con 0
35 logg sync ! Synchronize log messages with command output
36 no login ! Allow console access without login
37 exec-time 0 ! Disable automatic timeout
38 exit
39
40 end

```

2.4 Interfaces

Hier als Beispiel die Interfaces des Border Router 1.

```

1  !----- bash
2  ! Interfaces Konfiguration
3  !-----
4
5  conf t ! In den globalen Konfigurationsmodus wechseln
6
7  ! GigabitEthernet0/0 - Verbindung zu ISP1-BB1
8  int g0/0
9
10  desc to_ISP1-BB1 ! Beschreibung der Schnittstelle
11  ip add 10.0.1.0 255.255.255.254 ! IP-Adresse mit einer /31-
    Subnetzmaske (Point-to-Point)
12  mpls ip ! MPLS aktivieren
13  ip ospf authentication key-chain OSPF ! OSPF-Authentifizierung mit
    einer Key-Chain
14  no shut ! Schnittstelle aktivieren
15
16 exit
17
18 ! GigabitEthernet0/1 - Verbindung zu ISP1-BB2
19 int g0/1

```

```

20
21  desc to_ISP1-BB2  ! Beschreibung der Schnittstelle
22  ip add 10.0.1.2 255.255.255.254 ! IP-Adresse mit einer /31-
    Subnetzmaske (Point-to-Point)
23  mpls ip ! MPLS aktivieren
24  ip ospf authentication key-chain OSPF ! OSPF-Authentifizierung mit
    einer Key-Chain
25  no shut ! Schnittstelle aktivieren
26
27  exit
28
29  ! GigabitEthernet0/2 - Verbindung zu Standort 1
30  int g0/2
31
32  desc to_Standort1 ! Beschreibung der Schnittstelle
33  ip add 103.152.126.1 255.255.255.248 ! IP-Adresse mit einer /29-
    Subnetzmaske (6 nutzbare Hosts)
34  mpls ip ! MPLS aktivieren
35  ip access-group BLOCK_PRIVATE_AND_LOOPBACK in ! ACL zur Blockierung
    von privaten und Loopback-Adressen im eingehenden Verkehr
36  no shut ! Schnittstelle aktivieren
37
38  exit
39
40  ! Loopback1 - Loopback für BGP
41  int lo1
42
43  desc loopback_for_BGP ! Beschreibung der Loopback-Schnittstelle
44  ip add 10.0.1.101 255.255.255.255 ! IP-Adresse für die Loopback-
    Schnittstelle (/32-Subnetzmaske)
45  no shut ! Schnittstelle aktivieren
46
47  end

```

2.5 Bogon Block ACL

```

1  conf t
2
3  ip access-list extended BLOCK_PRIVATE_AND_LOOPBACK

```

bash

```

4      deny ip 10.0.0.0 0.255.255.255 any # Blockiert den gesamten
      10.0.0.0/8-Bereich (privates Netzwerk)
5      deny ip 172.16.0.0 0.15.255.255 any # Blockiert den 172.16.0.0/12-
      Bereich (privates Netzwerk)
6      deny ip 192.168.0.0 0.0.255.255 any # Blockiert den 192.168.0.0/16-
      Bereich (privates Netzwerk)
7      deny ip 127.0.0.0 0.255.255.255 any # Blockiert den gesamten
      127.0.0.0/8-Bereich (Loopback-Adressen)
8      permit ip any any # Erlaubt allen anderen Traffic
9  end

```

2.6 OSPF

Über OSPF werden die Netzze zwischen den Routern synchronisiert und die Loopbacks für BGP verteilt. Der Austausch findet zwischen allen Routern statt und ist verschlüsselt.

```

1  ! Keychains-Konfiguration für OSPF-Authentifizierung bash
2  conf t
3
4  key chain OSPF # Erstellt eine Keychain für OSPF
5      key 1 # Definiert den ersten Schlüssel in der Keychain
6          cryptographic-algorithm hmac-sha-512 # Setzt den
          Verschlüsselungsalgorithmus auf HMAC-SHA-512
7          key-string OSPFSECRETKEY # Legt den geheimen Schlüssel für die
          Authentifizierung fest
8  end
9
10 ! OSPF-Routing-Protokoll Konfiguration
11 conf t
12
13 router ospf 1 # Erstellt den OSPF-Prozess mit der ID 1
14     router-id 10.0.1.0 # Setzt die OSPF-Router-ID auf 10.0.1.0
15
16     network 10.0.1.0 0.0.0.1 area 1 # Fügt das Netz 10.0.1.0/31 in Area
17     1 hinzu
18     network 10.0.1.2 0.0.0.1 area 1 # Fügt das Netz 10.0.1.2/31 in Area
19     1 hinzu
20

```



```
19      network 10.0.1.101 0.0.0.0 area 1 # Fügt die Loopback-Schnittstelle
      10.0.1.101 in Area 1 hinzu
20 end # Beendet den Konfigurationsmodus
```

2.7 BGP

Es gibt eine BGP Beziehung zwischen allen den Border Routern. Die Loopbacks werden als Source genommen damit man nicht von einem Physischen Interface abhängig ist. Es werden auch die public Netze über BGP bekanntgegeben.

```
1  ! BGP-Konfiguration bash
2  conf t
3
4  router BGP 1 # Aktiviert den BGP-Prozess mit der AS-Nummer 1
5      network 103.152.126.0 mask 255.255.255.248 # Fügt das Netzwerk
      103.152.126.0/29 in die BGP-Routing-Tabelle ein
6
7      neighbor 10.0.1.102 remote-as 1 # Definiert einen BGP-Nachbarn
      (10.0.1.102) mit der AS-Nummer 1
8      neighbor 10.0.1.102 update-source lo1 # Setzt die Quelle für BGP-
      Updates auf die Loopback-Schnittstelle lo1
9
10     neighbor 10.0.1.103 remote-as 1 # Definiert einen weiteren BGP-
      Nachbarn (10.0.1.103) mit der AS-Nummer 1
11     neighbor 10.0.1.103 update-source lo1 # Setzt auch hier die Quelle
      für BGP-Updates auf lo1
12
13     neighbor 10.0.1.104 remote-as 1 # Definiert einen weiteren BGP-
      Nachbarn (10.0.1.104) mit der AS-Nummer 1
14     neighbor 10.0.1.104 update-source lo1 # Setzt die Quelle für BGP-
      Updates auf lo1
15 end # Verlasse den Konfigurationsmodus
```

2.8 VRF

```
1  ! VRF-Konfiguration bash
2  conf t
3
4  ip vrf rennweg-graz # Erstellt eine VRF mit dem Namen "rennweg-graz"
```

```

5      rd 1:10 # Definiert den Route Distinguisher (RD) für die VRF
6      route-target export 1:10 # Setzt den Route Target (RT) für den
Export auf 1:10
7      route-target export 1:20 # Setzt den Route Target (RT) für den
Export auf 1:20
8      route-target import 1:10 # Setzt den Route Target (RT) für den
Import auf 1:10
9      route-target import 1:20 # Setzt den Route Target (RT) für den
Import auf 1:20
10     end
11
12     ! Schnittstellen-Konfiguration für VRF
13     int g0/2
14         desc vrf_to_Standort2 # Beschreibung der Schnittstelle
15         ip vrf forward rennweg-graz # Weist die Schnittstelle der VRF
"rennweg-graz" zu
16         ip add 10.10.10.1 255.255.255.248 # IP-Adresse und Subnetzmaske für
die Schnittstelle
17         mpls ip # Aktiviert MPLS auf der Schnittstelle
18         no shut # Aktiviert die Schnittstelle
19     exit
20
21     ! Distribution List
22     ip prefix-list BLOCK_NET seq 10 deny 192.168.53.0/24 # Blockiert das
Netzwerk 192.168.53.0/24
23     ip prefix-list BLOCK_NET seq 20 permit 0.0.0.0/0 le 32 # Erlaubt alle
anderen IPs
24
25     ! OSPF mit VRF und Prefix-Filter
26     router ospf 10 vrf rennweg-graz # Aktiviert OSPF in der VRF "rennweg-
graz"
27         redistribute connected subnets # Redistribuiert verbundene Netzwerke
und Subnetze
28         distribute-list prefix BLOCK_NET in # Wendet die Prefix-List
"BLOCK_NET" auf eingehende Routen an
29         network 10.10.10.0 0.0.0.7 area 1 # Definiert das OSPF-Netzwerk in
Area 1
30     end
31
32     ! BGP-Konfiguration für VRF
33     router BGP 1

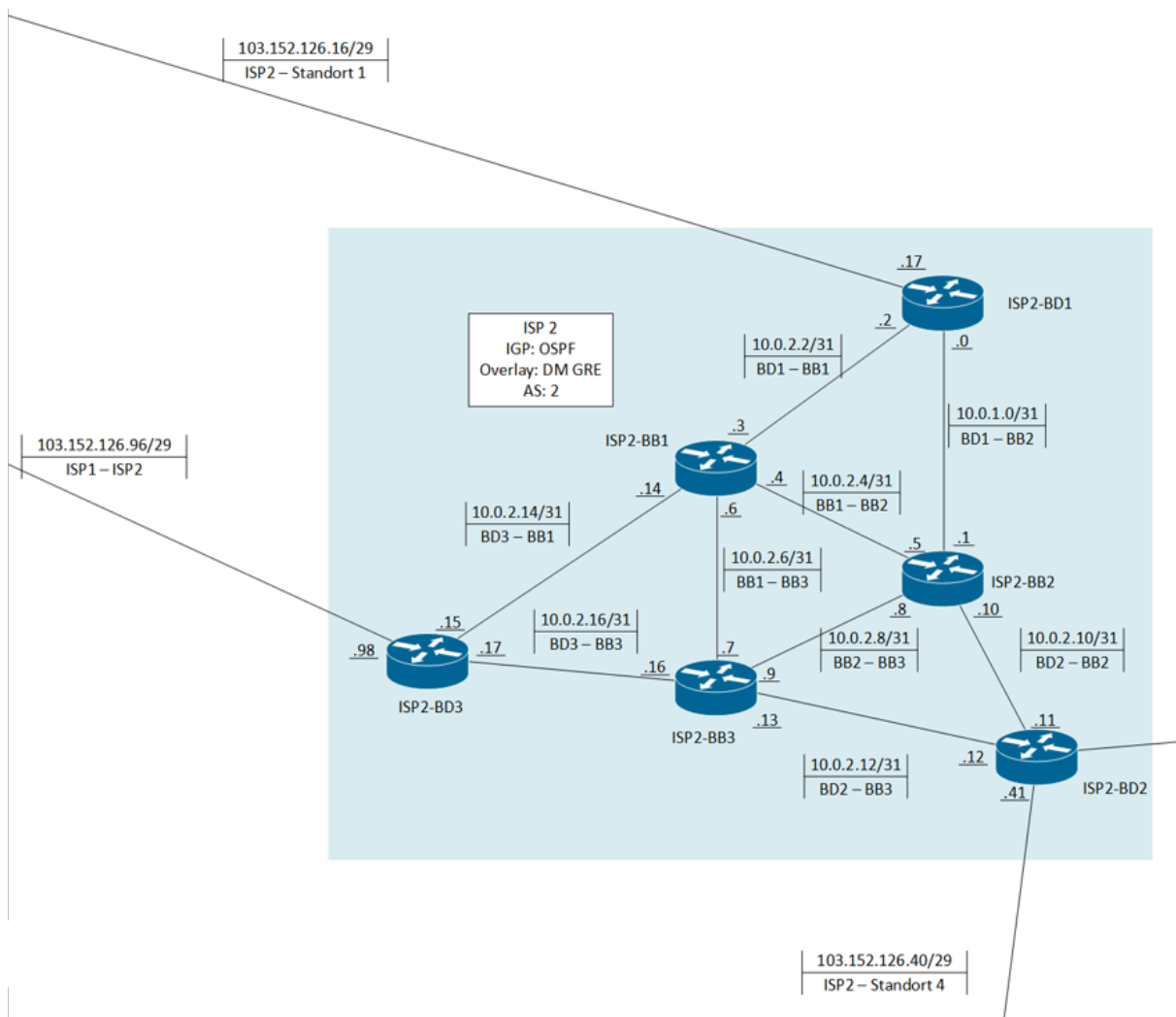
```

```

34 address-family vpnv4 # Aktiviert das vpnv4 Adressfamilien-Protokoll
35     nei 10.0.1.104 activate # Aktiviert den BGP-Nachbarn 10.0.1.104
    für vpnv4
36     nei 10.0.1.104 send-community extended # Aktiviert das Senden
    von erweiterten Communities zu diesem Nachbarn
37
38 address-family ipv4 vrf rennweg-graz # Aktiviert die IPv4-
    Adressenfamilie für die VRF "rennweg-graz"
39     redistribute ospf 10 # Redistribuiert OSPF-Routen in BGP
40 end
  
```

3 ISP 2

3.1 Plan



3.2 Allgemeine Informationen

- 3 Border Router
- 3 Backbone Router

IGP: OSPF

Overlay Netz : DMVPN

Netz: 10.0.2.0 - 10.0.2.16 /31

Loopbacks für BGP: 10.0.2.101 - 10.0.2.103 /32

Loopbacks für den DMVPN: 10.0.2.111 - 10.0.2.113 /32

Bogon Filter auf den public Interfaces

Eine default Route, die via BGP weitergegeben wird.

3.3 Grundkonfig

Siehe ISP1

3.4 Interfaces

```
1  !Interfaces bash
2  conf t
3
4  ! Interface zur Verbindung mit ISP2-BB2
5  int g0/0
6      desc to_ISP2-BB2
7      ip add 10.0.2.0 255.255.255.254 ! Setzt die IP-Adresse mit
        einer /31-Subnetzmaske
8      ip ospf authentication key-chain OSPF ! Aktiviert die OSPF-
        Authentifizierung
9      no shut ! Aktiviert das Interface
10 exit
11
12 ! Interface zur Verbindung mit ISP2-BB1
13 int g0/1
```

```

14     desc to_ISP2-BB1
15     ip add 10.0.2.2 255.255.255.254 ! Setzt die IP-Adresse mit
    einer /31-Subnetzmaske
16     ip ospf authentication key-chain OSPF ! Aktiviert die OSPF-
    Authentifizierung
17     no shut ! Aktiviert das Interface
18 exit
19
20 ! Interface zur Verbindung mit Standort1
21 int g0/2
22     desc to_Standort1
23     ip add 103.152.126.17 255.255.255.248 ! Setzt die IP-Adresse mit
    einer /29-Subnetzmaske
24     ip access-group BLOCK_PRIVATE_AND_LOOPBACK in ! Filtert privaten und
    Loopback-Traffic
25     no shut ! Aktiviert das Interface
26 exit
27
28 ! Loopback-Interface für BGP
29 int lo1
30     desc loopback_for_BGP
31     ip add 10.0.2.101 255.255.255.255 ! Setzt eine /32-IP für BGP
32     no shut ! Aktiviert das Interface
33 exit
34
35 ! Loopback-Interface für Tunnel
36 int lo2
37     desc for_tunnel
38     ip add 10.0.2.111 255.255.255.255 ! Setzt eine /32-IP für
    Tunnelverbindungen
39     no shut ! Aktiviert das Interface
40 exit

```

3.5 Bogon Block ACL

Siehe ISP 1

3.6 OSPF

Es gibt zwei OSPF Prozesse. Der erste ist um die Netzte zwischen den Routern für OSPF zu aktivieren und die Loopbacks für die Tunnel auszutauschen. Der zweite Prozess dient dazu, über das DMVPN die Loopbacks für BGP auszutauschen.

```

1  ! Keychains-Konfiguration für OSPF-Authentifizierung
2  conf t
3
4  key chain OSPF # Erstellt eine Keychain für OSPF
5      key 1 # Definiert den ersten Schlüssel in der Keychain
6          cryptographic-algorithm hmac-sha-512 # Setzt den
        Verschlüsselungsalgorithmus auf HMAC-SHA-512
7          key-string OSPFSECRETKEY # Legt den geheimen Schlüssel für die
        Authentifizierung fest
8  end
9
10 !OSPF
11 conf t
12
13 ! OSPF-Prozess 1 - Primärer OSPF-Router für Area 1
14 router ospf 1
15 router-id 10.0.2.0 ! Setzt die eindeutige Router-ID für OSPF 1
16
17     network 10.0.2.0 0.0.0.1 area 1 ! Fügt das Netzwerk 10.0.2.0/31 zu
        Area 1 hinzu
18     network 10.0.2.2 0.0.0.1 area 1 ! Fügt das Netzwerk 10.0.2.2/31 zu
        Area 1 hinzu
19     network 10.0.2.111 0.0.0.0 area 1 ! Fügt die Loopback-Adresse
        10.0.2.111/32 zu Area 1 hinzu
20
21 exit
22
23 ! OSPF-Prozess 2 - Zweiter OSPF-Prozess für Area 2
24 router ospf 2
25 router-id 10.0.2.111 ! Setzt die eindeutige Router-ID für OSPF 2
26
27     network 101.100.12.0 0.0.0.255 area 2 ! Fügt das Netzwerk
        101.100.12.0/24 zu Area 2 hinzu

```

```

28      network 10.0.2.101 0.0.0.0 area 2  ! Fügt die Loopback-Adresse
      10.0.2.101/32 zu Area 2 hinzu
29
30  end

```

3.7 BGP

Siehe ISP 1

3.8 DMVPN

Es gibt einen DMVPN zwischen den drei Border Routern. Dieser dient als Overlay Netzwerk. Der VPN ist verschlüsselt das gleiche gilt auch für den OSPF Prozess, der über das Overlay läuft.

```

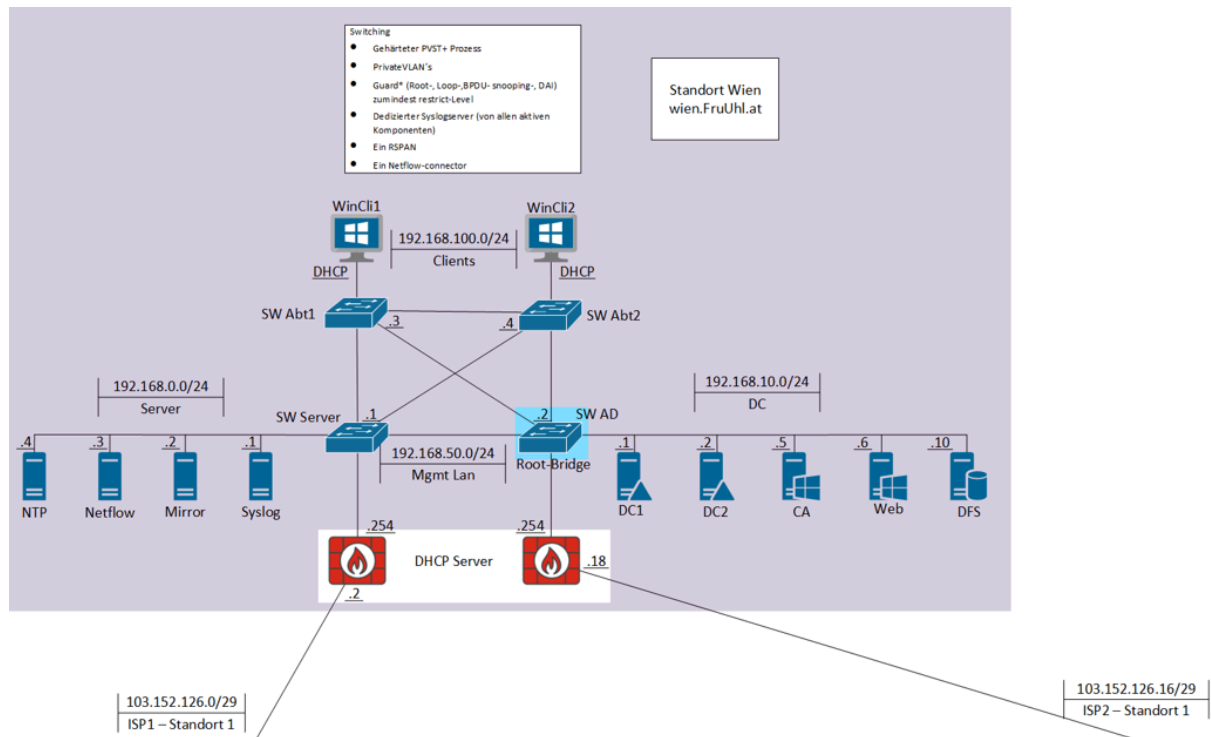
1  !Tunnel bash
2  int tun1
3      desc multipoint_tunnel  ! Beschreibung des Tunnels
4      ip add 101.100.12.1 255.255.255.0  ! IP-Adresse und Subnetzmaske für
      das Tunnelinterface
5      tunnel mode gre multipoint  ! GRE-Tunnel im Multipoint-Modus
6      tunnel source lo2  ! Quelle des Tunnels ist Loopback 2
7      no ip redirects  ! Deaktiviert ICMP-Redirects für Sicherheit
8      ip mtu 1440  ! Setzt die maximale Übertragungsgröße für den Tunnel
9      ip nhrp authentication cisco123  ! NHRP-Authentifizierung mit
      Passwort
10     ip nhrp map multicast dynamic  ! Erlaubt dynamisches Multicast-
      Mapping über NHRP
11     ip nhrp network-id 1  ! Setzt die Netzwerk-ID für NHRP
12     no shut  ! Aktiviert das Interface
13  exit
14
15  !VPN
16  crypto isakmp policy 10
17     encryption aes 256  ! Starke AES-256-Verschlüsselung
18     lifetime 86400  ! Lebensdauer des Schlüssels auf 24 Stunden gesetzt
19     hash sha512  ! SHA-512 für starke Integritätsprüfung
20     group 5  ! Diffie-Hellman Gruppe 5 für Schlüsselaustausch
21     authentication pre-share  ! Pre-Shared Key zur Authentifizierung

```

```
22 exit
23
24 crypto isakmp key cisco123! address 0.0.0.0 ! Setzt den Pre-Shared Key
    für alle IP-Adressen
25
26 crypto ipsec transform-set 5CN esp-sha512-hmac esp-aes 256
27     mode transport ! Transportmodus für IPSec
28 exit
29
30 crypto ipsec profile IPSEC_PROF
31     set transform-set 5CN ! Verwendet das zuvor erstellte Transform-Set
32 exit
33
34 int tun1
35     no ip split-horizon ! Deaktiviert Split-Horizon, um Routing-Probleme
        zu vermeiden
36     ip nhrp shortcut ! Aktiviert NHRP-Shortcuts für schnellere
        Paketweiterleitung
37     tunn protection ipsec profile IPSEC_PROF ! Schützt den Tunnel mit
        IPSec
        ip ospf network point-to-multipoint ! Setze das Netz auf OSPF point
38 to multipoint. Dadurch das die Loopbacks für BGP über die Tunnel
        bekanntgegeben werden muss das gesetzt werden. Sonst flappt der Tunnel
39     ip ospf authentication key-chain OSPF ! OSPF-Authentifizierung mit
        einer Key-Chain
40 end
```


4 Standort Wien

4.1 Plan



Hostname	IP-Adresse
<i>DC-Netzwerk</i>	<i>192.168.10.0/24</i>
DC1	192.168.10.1
DC2	192.168.10.2
CA	192.168.10.5
Web	192.168.10.6
DFS	192.168.10.10
<i>Server-Netzwerk</i>	<i>192.168.0.0/24</i>
Syslog	192.168.0.1
Mirror	192.168.0.2

Hostname	IP-Adresse
Netflow	192.168.0.3
NTP	192.168.0.4
<i>Management-Netzwerk</i>	<i>192.168.50.0/24</i>
SW Server	192.168.50.1
SW AD	192.168.50.2
SW Abt1	192.168.50.3
SW Abt2	192.168.50.4
<i>Client-Netzwerk</i>	<i>192.168.100.0/24</i>
Client 1	DHCP
Client 2	DHCP

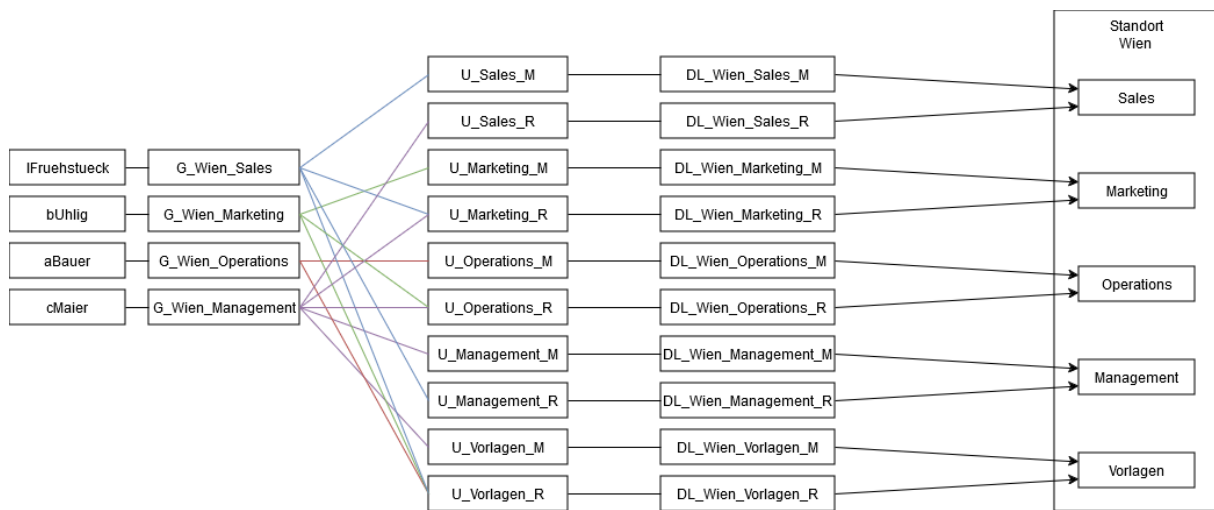
4.2 Allgemeine Informationen

Dies ist der Hauptstandort mit den wichtigsten Active-Directory Komponenten. Auch einige Server-Dienste sind hier angesiedelt, sowie ein HA-Cluster für den Uplink und switching.

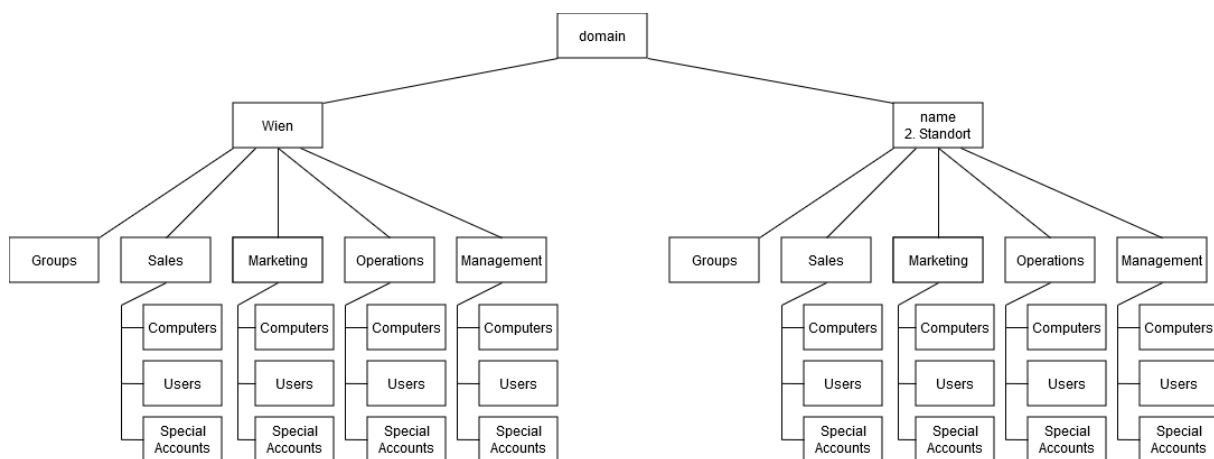
4.3 Windows

Dies ist der Hauptstandort der Domain wien.FruUhl.at. Hier befinden sich die beiden Domaincontroller DC1 und DC2, sowie der Certificate Authority Server CA. Der Web-server ist sowohl als CDP in Verwendung sowie als Radius-Server zur Authentifizierung bei den Switches des Netzwerkes. Auf dem DFS-Server befinden sind Freigaben für Benutzer, darunter abteilungsweite Shares und die Ablageorte für Roaming-Profiles. Das Active-Directory Gruppen-Prinzip ist nach AGUDLP aufgebaut, die OUs nach Business Unit Model.

4.3.1 Gruppen



4.3.2 OUs



4.3.3 Screenshots

TODO: Screenshot der CA - pkiview.msc

4.3.3.1 Sites

4.4 Switching

Die verschiedenen Netzwerke werden mittels VLANs unterteilt. Hierbei gibt es 5 unterschiedliche:

VLAN	Name
1	Server
10	DC
50	Management
100	Clients
200	RSPAN

4.4.1 Spanning Tree

Auf allen Switches ist per-vlan Spanning Tree konfiguriert, wobei der AD-Switch die Root-Bridge für alle VLANs ist. Zwischen den Switches sind auf den Trunk-Ports immer nur die zwingend notwendigen VLANs erlaubt, beispielsweise ist das RSPAN Netzwerk nur auf den Core-Layer Switches erlaubt.

4.4.2 RSPAN

Das RSPAN-Vlan existiert nur auf den Core-Layer Switches. über dieses wird jeglicher Traffic aus dem AD-Netzwerk gespiegelt und auf den Mirror-Server geleitet, auf welchem mit tshark der Traffic aufgezeichnet und abgespeichert wird.

4.4.3 Netflow

Auf dem AD Switch ist ein Flow-Exporter konfiguriert, welcher mittels Netflow allen Traffic aus dem AD-Netzwerk auf den Netflow-Server leitet. Dieser wertet die Daten aus und stellt sie in einem Dashboard dar.

4.4.4 Syslog

Alle Switches sind konfiguriert, ihre Log-Daten an den Syslog-Server zu senden. Dort wird dieser mittels Kiwi Syslog aufgezeichnet.

4.4.5 Authentication

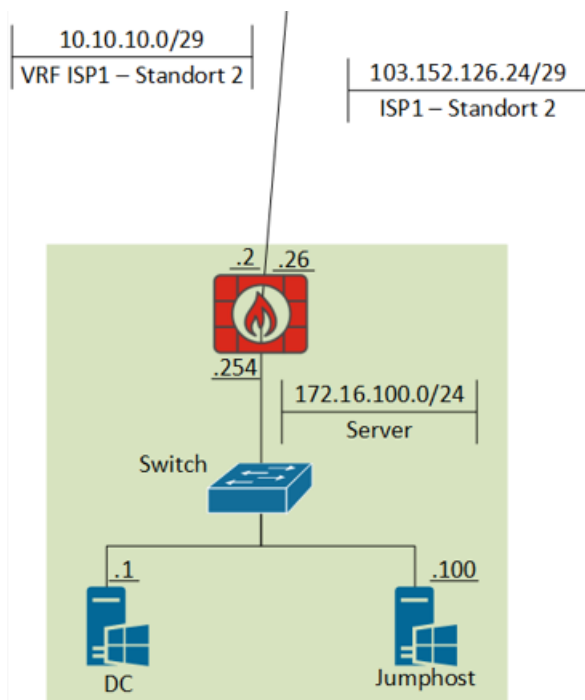
Die Switches sind mittels Radius-Server authentifiziert. Der Radius-Server ist auf dem WEB-Server installiert und konfiguriert, da ein GUI benötigt wird, und dieser Server der einzige mit GUI ist.

4.5 Features FG Wien

- HA Cluster
- NAT/PAT
- Granulare Policies
- Traffic Shaping
- Captive Portal
- DHCP
- Subinterfaces
- Site2Site VPN mit anderer FortiGate
 - (FG Rennweg)
- Site2Site VPN mit PfSense
 - (PF Graz)
- RAS VPN zu WinCli auf IPsec Basis
- Redundanter ISP

5 Standort Rennweg

5.1 Plan



Hostname	IP-Adresse
<i>Server-Netzwerk</i>	<i>172.16.100.0/24</i>
DC	172.16.100.1
Jumphost	172.16.100.100

5.2 Allgemeine Informationen

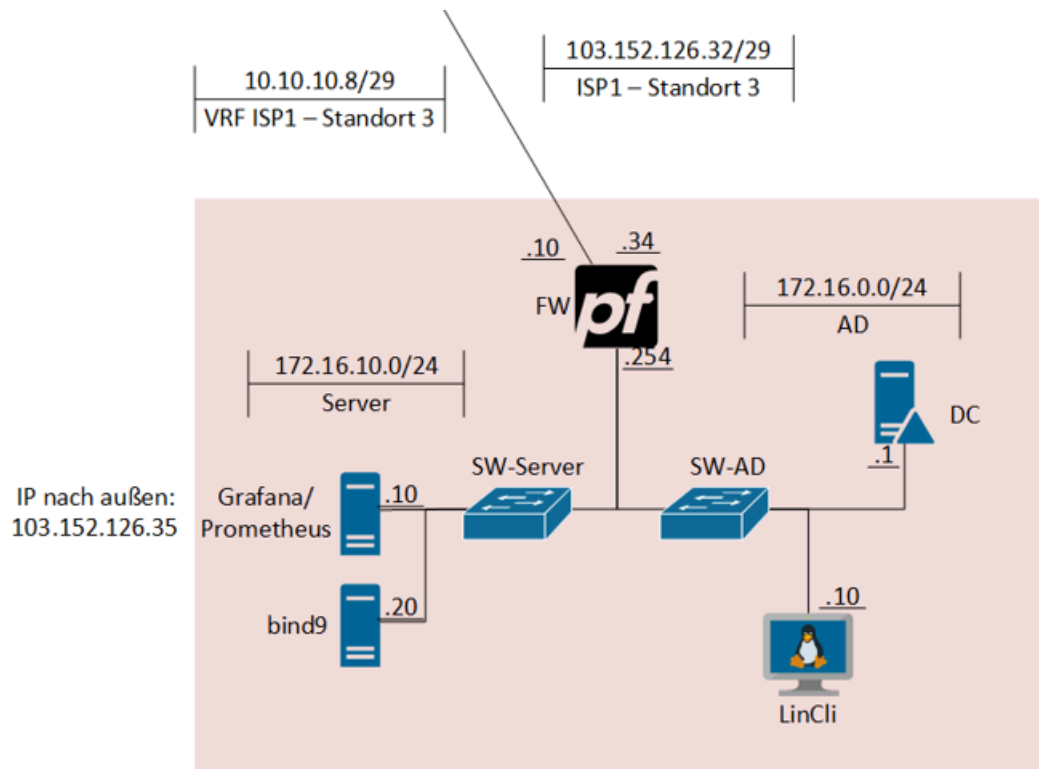
Rennweg ist eine 2. Site der wien.FruUhl.at Domain. Der Domaincontroller hier ist ein Read-Only Domaincontroller. Der Jumphost ist für die Administration des Servers zuständig, denn nur über ihn kann eine RDP-Session aufgebaut werden.

5.3 Features FG Rennweg

- NAT/PAT
- Site2Site VPN mit anderer FortiGate
 - (FG Wien)
- OSPF um private Netzze für VRF bekanntzugeben
- Distribution Listen um Netze nicht via OSPF zu teilen

6 Standort Graz

6.1 Plan



Hostname	IP-Adresse
<i>AD-Netzwerk</i>	<i>172.16.0.0/24</i>
DC	172.16.0.1
LinCli	172.16.0.10
<i>Server-Netzwerk</i>	<i>172.16.10.0/24</i>
Grafana	172.16.10.10 - 103.152.126.35 nach außen
bind9	172.16.10.20

6.2 Allgemeine Informationen

Graz ist eine Sub-Domain der wien.FruUhl.at Domain. Auf dem Standort befindet sich weiters ein Active Directory gejointer Linux Client. Der DNS-Server bind9 wird als caching Forwarder verwendet und auf dem Grafana-Dashboard sind Statistiken der Serverauslastung zu sehen, welche mittels Prometheus gesammelt werden. Der Server wird auch statisch nach außen genattet, womit er public erreichbar ist.

6.3 Features PF Graz

- NAT/PAT
- Subinterfaces
- Site2Site VPN mit FortiGate
 - (FG Wien)
- OSPF um private Netzze für VRF bekanntzugeben
- Distribution Listen um Netze nicht via OSPF zu teilen
- Static NAT
 - Grafana Server
- WireGuard RAS VPN für WinCli