

Little Big Topo

Autoren: Lukas Freudensprung, Morris Tichy

Inhaltsverzeichnis

1. Topologie	7
1.1. Avenger-HQ	7
1.2. Wakanda	8
1.3. Sanctum Sanctorum	8
1.4. NewYork	8
1.5. Hawkeye Farm	8
1.6. Stark Tower, Bifröst und S.H.I.E.L.D	8
1.7. Verbindung der Standorte mittels VPN	9
2. ISP	9
2.1. ISP Overlay + Underlay	9
2.1.1. Underlay	9
2.1.2. Overlay	9
2.1.3. Überprüfung	10
2.1.4. BGP	10
2.1.5. Überprüfung	10
2.2. Theorie	11
2.2.1. Szenario	11
2.2.2. Konfiguration	11
2.3. Distribution List	12
2.3.1. Konfiguration	12
2.4. Bogons blocken	12
2.5. Hub-and-Spoke FlexVPN	13
2.5.1. Konfiguration	13
3. Switching	17
3.1. Private VLANs	17
3.1.1. Theorie	17
3.1.2. Konzept	17
3.1.3. Konfiguration	17
3.1.4. Überprüfung	18
3.2. RSPAN	19

3.2.1. Konfiguration	19
3.3. Spanningtree	20
3.3.1. RSTP aktivieren	20
3.3.2. Root Guard	20
3.3.3. Loop Guard	20
3.3.4. BPDU Guard	21
4. Firewalls	21
4.1. Anti Virus	21
4.1.1. Konfiguration des AV Profiles	21
4.1.2. Custom-Deep-Inspection	22
4.1.3. Überprüfung	23
4.2. Data Leak Prevention	23
4.2.1. Konfiguration Block Exe Datein	23
4.2.2. Firewall Policy	24
4.2.3. Überprüfung	24
4.3. Intrusion Prevention System	24
4.3.1. Konfiguration	25
4.3.2. Überprüfung	25
4.4. Webfilter	25
4.4.1. Theorie	25
4.4.2. Überprüfung	26
4.5. Fortigate Bogons	26
4.5.1. Konfiguration	27
4.6. FortiGate HA-Cluster	28
4.6.1. Was ist ein HA-Cluster?	28
4.6.2. Konfiguration eines HA-Clusters	29
4.6.3. Überprüfung	29
4.7. Site-to-Site-VPN PSK	30
4.7.1. Theorie	30
4.7.2. Konfiguration	30
4.7.2.1. VPN Erstellen	30
4.7.2.2. Statische Route für den Tunnel	31
4.7.2.3. Policy für den VPN	31
4.8. NPS FortiGate Captive Portal	32
4.8.1. NPS Konfiguration	32
4.8.2. Connection Request Policies	32
4.8.3. Network Policies	33
4.8.4. Vendor Specific Attributes	34

4.8.5. FortiGate Konfiguration	35
4.8.6. Überprüfung	36
4.9. Statischer NAT	37
4.9.1. Theorie	37
4.9.2. Konfiguration	37
4.9.2.1. Erstellen der VIP	37
4.9.2.2. Zuweisen in der Policy	37
4.10. PfSense	38
4.10.1. Plattformübergreifender VPN	38
5. Active Directory	39
5.1. Active Directory Directory Services	39
5.1.1. DC1	39
5.1.2. DC2	40
5.1.3. WinCLI1	41
5.1.4. WinCLI2	41
5.1.5. DC3	42
5.1.6. DC4	43
5.1.7. RODC	43
5.2. Active Directory Sites und Services	44
5.2.1. Standorte	44
5.2.2. Site-Links	45
5.2.3. Server in Standorte verschieben	45
5.3. Active Directory Users und Computers	46
5.3.1. OU Struktur	46
5.3.2. User und Gruppen	48
5.4. Distributed File System	49
5.4.1. Konfiguration	50
5.4.2. Ordnerstruktur erstellen	51
5.4.3. AGDLP	52
5.4.4. DFS verwalten	52
5.4.5. GPO DriveMapPolicy	55
5.4.6. Überprüfung	56
5.5. IIS	56
5.5.1. Web Server IIS Role installieren	57
5.5.2. CertEnroll Folder erstellen und Share	57
5.5.3. NTFS Berechtigungen festlegen	59
5.5.4. CertEnroll Virtual Directory erstellen auf IIS	60
5.5.5. Double Escaping auf IIS Server aktivieren	61

5.5.6. CNAME erstellen	61
5.6. Certificate Authority	62
5.6.1. CA Policy.inf erstellen	63
5.6.2. Post Installation Timer Konfiguration	63
5.6.3. AIA konfigurieren	63
5.6.4. CDP konfigurieren	64
5.6.5. CA Certificate AIA veröffentlichen	64
5.6.6. CA Certificate CDP veröffentlichen	64
5.6.7. Web Server Security Group	65
5.6.8. Webserver Certificate Template erstellen	67
5.6.9. CA für Zertifikatsausstellung konfigurieren	68
5.6.10. Request SSL Certificate	69
5.6.11. Enable SSL	72
5.6.12. Web Server Certificate Test	74
5.7. Hardening	75
5.7.1. GPOs	75
5.7.1.1. GPO Desktop Hintergrund	75
5.7.1.2. GPO Lock/Logon Screen	78
5.7.1.3. GPO Last signed in user not shown	80
5.7.1.4. GPO Password Security Settings	82
5.7.1.5. GPO Lokale Firewall Einstellungen (per PS-Skript)	83
5.7.1.6. GPO Account Sperrung	85
5.7.1.7. GPO Software Installation	87
5.7.2. Credential Guard	87
5.7.2.1. Nutzen/Vorteil	88
5.7.2.2. Requirements	88
5.7.2.3. Wichtig!	89
5.7.2.4. Default Enablement	90
5.7.2.5. GPO Konfiguration	90
5.7.2.6. Überprüfung	91
5.7.3. Protected Users Security Group	92
5.7.3.1. Wichtig!	92
5.7.3.2. Requirements	92
5.7.3.3. Device Protection für Protected Users	92
5.7.3.4. Domain Controller Protection für Protected Users	93
5.7.3.5. Konfiguration	93
5.7.4. Windows Security Baseline	94
5.7.4.1. Was ist eine Security Baseline?	94

5.7.4.2. Warum werden Security Baselines benötigt?	95
5.7.4.3. Policy Analyzer	95
5.7.4.4. Konfiguration	95
5.7.5. Advanced Security Audit Policies	100
5.7.5.1. Nutzen/Vorteil	100
5.7.5.2. GPO Konfiguration	100
5.7.5.3. Überprüfung	100
6. Linux	101
6.1. Bind9 Forwarder	101
6.1.1. Checkliste	101
6.1.2. Forwarder Konfigurieren	102
6.1.2.1. Konfiguration überprüfen	102
6.2. Metasploit Scan	102
6.2.1. Nmap Scan	103
6.3. Prometheus/Grafana	104
6.3.1. Theorie	104
6.3.1.1. Was ist Prometheus?	104
6.3.1.2. Was ist Grafana?	105
6.3.2. Installation	105
6.3.2.1. Grundkonfiguration Prometheus Server	105
6.3.2.2. Installation Prometheus	106
6.3.2.3. Überprüfen des Web-Zugriffs	107
6.3.2.4. Installation Grafana	107
6.3.2.5. Node Explorer Ubuntu	108
6.3.3. Dashboard einrichten	108
6.3.4. Alerts	109
6.3.5. Alert Manager	111
6.3.6. Testen	112
6.4. Wireguard VPN	113
6.4.1. WG-Client	113
6.4.2. WG-Server	113
6.4.2.1. Netzwerkkonfiguration	113
6.4.3. Wireguard Installation	114
6.4.3.1. Server	114
6.4.4. Wireguard starten	115
6.4.5. Überprüfung	115
6.5. Syslog Server Linux	116
6.5.1. Setup	116

6.5.2. Konfiguration	116
6.6. Linux Firewall mit iptables	117
6.6.1. Konfiguration	117
6.7. Apparmor	118
6.7.1. Konfiguration des TFTP-Servers	119
6.7.2. Überprüfung	119

1. Topologie

Unsere Topologie besteht aus den drei ISPs: Start Tower, Bifröst und S.H.I.E.L.D., die die fünf Standorte miteinander verbinden. Die Namen der Standorte sowie der ISPs sind von dem Marvel Universum inspiriert.

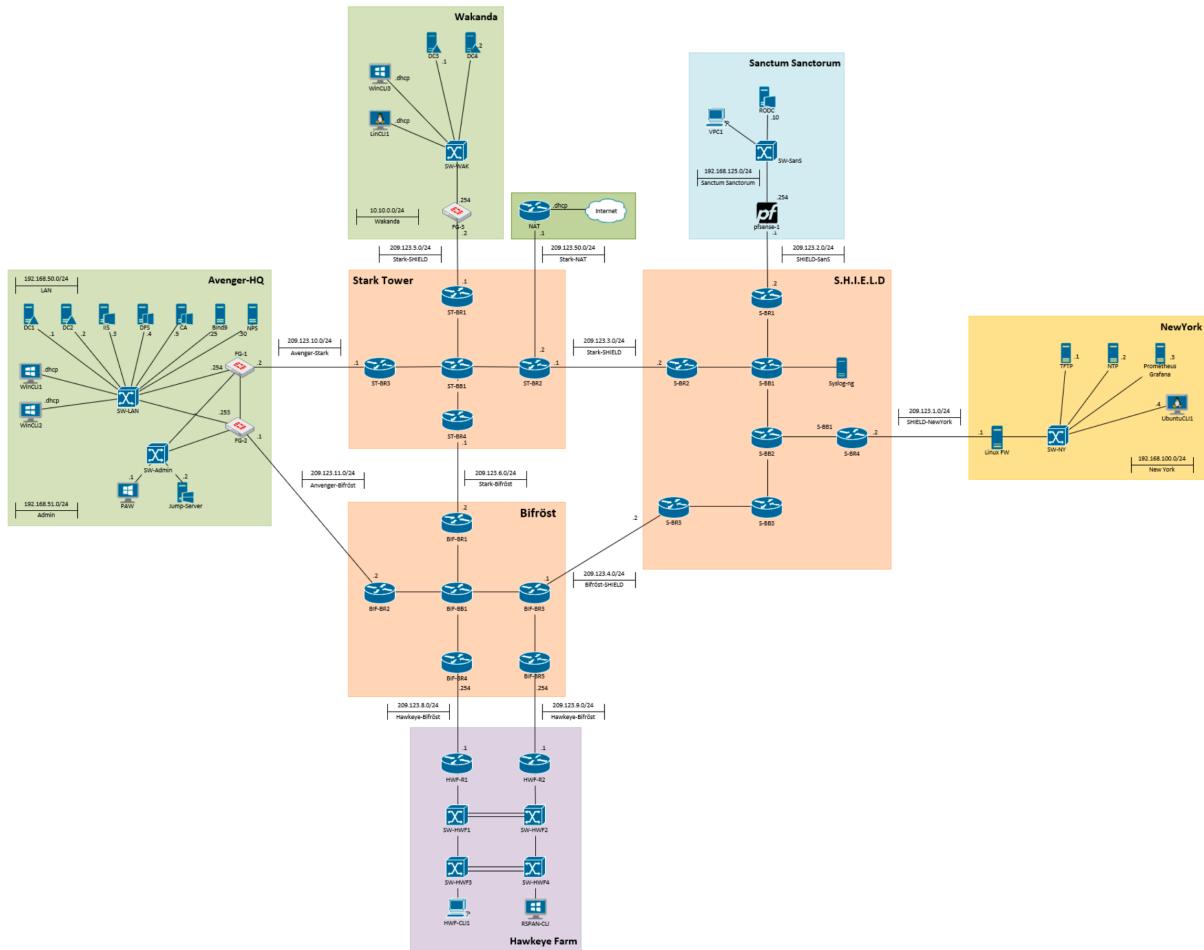


Abbildung 1: Topologie

1.1. Avenger-HQ

Avenger-HQ ist der zentrale Windows-Standort mit der Forest-Root-Domäne AvengerHQ.at und wird durch einen redundanten **FortiGate-HA-Cluster** abgesichert. Er umfasst unter anderem die beiden Domänencontroller **DC1** und **DC2** sowie einen **DFS- und Bind9-Server**. Zudem gibt es eine **1-Tier-PKI** mit einem **IIS-Webserver**, der über ein Webserver-Zertifikat HTTPS bereitstellt. Außerdem wurde ein **NPS**, für die Internetzugriffseinschränkung, eingerichtet. Für Testzwecke sind die Windows-Clients **WinCLI1** und **WinCLI2** integriert.

1.2. Wakanda

Wakanda ist der zweite Windows-Standort und hat die Subdomäne Wakanda.AvengerHQ.at. Der Standort wird durch eine **FortiGate-Firewall** abgesichert und umfasst die beiden Domänencontroller **DC3** und **DC4** sowie die beiden Clients **WinCLI3** und **LinCLI1**.

1.3. Sanctum Sanctorum

Sanctum Sanctorum ist ein sicherheitskritischer Standort mit minimaler Infrastruktur. Daher wird dort ausschließlich ein **Read-Only Domain Controller (RODC)** betrieben. Eine **pfSense-Firewall** schützt den Standort vor externen Bedrohungen. Zusätzlich wurden auf dem Switch Private Isolated VLANs konfiguriert, um die interne Sicherheit weiter zu erhöhen. Zur Erprobung der Private VLANs wurde der Client **VPC1** integriert.

1.4. NewYork

NewYork ist der zentrale Linux-Standort und wird durch eine **Linux-Firewall** mit IPTables abgesichert. Der Standort umfasst unter anderem den Monitoring-Server **Prometheus/Grafana** sowie einen **NTP- und TFTP Server**. Der Ubuntu Client **LinCLI1** wird zur Datenüberwachung von Prometheus und Grafana verwendet.

1.5. Hawkeye Farm

Die Hawkeye Farm ist ein rein Cisco-proprietärer Standort und verfügt über eine redundante Firewall, die mittels IP SLA und HSRP abgesichert ist. Der Standort umfasst ein komplexes Switching, das folgende Funktionen integriert: VLANs, VTP, RSTP, EtherChannel sowie Sicherheitsmaßnahmen wie Port-Security, verschiedene Guards und ein gehärtetes PVST+.

Für Testzwecke sind der VPC VPNC1 und der Windows-Client RSPAN-CLI integriert.

1.6. Stark Tower, Bifröst und S.H.I.E.L.D

Der ISP besteht aus den Standorten Stark Tower, Bifröst und S.H.I.E.L.D.. Als Underlay kommt OSPF zum Einsatz, während für die interne Adjazenzbildung iBGP verwendet wird. Zur Anbindung der ISPs untereinander dient eBGP.

Als Overlay wurde MPLS implementiert. Zusätzlich wurde am ISP Stark Tower ein Hub-and-Spoke-FlexVPN eingerichtet, um den Datenverkehr zu verschlüsseln.

1.7. Verbindung der Standorte mittels VPN

Zwischen den Standorten Avenger-HQ und Wakanda wurde ein Site-to-Site-VPN eingerichtet. Dieses VPN wird über IPsec realisiert und verbindet die beiden FortiGate Firewalls. Weiters sind die FortiGate Firewalls von Avenger-HQ mit der Pfsense von Sanctum Sanctorum über ein VPN verbunden. Auf der Linux Firewall wurde ein Wireguard VPN eingerichtet, der Usern aus Wakanda erlaubt sich mit dem Monitoring-Server (Prometheus & Grafana) in NewYork zu verbinden.

2. ISP

2.1. ISP Overlay + Underlay

Wie auch schon oben erwähnt wurde, wurde für die ISP-Topologie ein Overlay und ein Underlay erstellt. Genaueres zu den beiden Begriffen wird im Folgenden erklärt.

2.1.1. Underlay

Das physische oder grundlegende Netzwerk (z.B. Router, Switches), das Daten transportiert. In unserem Fall wurde OSPF konfiguriert.

ISP-Router

```
1 router ospf 30
2 router-id 10.0.3.14
3 network 10.0.3.12 0.0.0.3 area 30
4 network 10.0.3.8 0.0.0.3 area 30
5 exit
```

2.1.2. Overlay

Ein virtuelles Netzwerk, das auf dem Underlay-Netzwerk aufbaut und zusätzliche Funktionen wie VPNs oder SD-WAN ermöglicht. In unserem Fall wurde MPLS konfiguriert.

ISP-Router

```
1 ip cef
2 mpls ip
```

2.1.3. Überprüfung

ST-BB1#sh mpls forwarding-table						
Local Label	Outgoing Label	Prefix or Tunnel Id	Bytes Switched	Outgoing interface	Next Hop	
20	Pop Label	1.1.1.4/32	8555	Gi0/0	10.0.1.2	
21	Pop Label	1.1.1.3/32	19120	Gi0/1	10.0.1.6	
22	Pop Label	1.1.1.2/32	8134	Gi0/3	10.0.1.14	
23	No Label	1.1.1.1/32	11958	Gi0/2	10.0.1.10	

Abbildung 2: MPLS Forward-Table

2.1.4. BGP

BGP ist ein Routing-Protokoll, das für den Austausch von Routing-Informationen zwischen verschiedenen Autonomen Systemen (AS) verwendet wird. Im und zwischen den ISP wurde BGP konfiguriert. Folgender Codeabschnitt zeigt diese Konfiguration.

ISP-Router

```

1 router BGP 2
2 network 209.123.6.0 m 255.255.255.0
3 neighbor 2.2.2.2 remote-as 2
4 neighbor 2.2.2.2 update-source lo1
5 neighbor 2.2.2.3 remote-as 2
6 neighbor 2.2.2.3 update-source lo1
7 neighbor 2.2.2.4 remote-as 2
8 neighbor 2.2.2.4 update-source lo1
9 neighbor 2.2.2.5 remote-as 2
10 neighbor 2.2.2.5 update-source lo1
11 neighbor 209.123.6.1 remote-as 1
12 neighbor 209.123.6.1 update-source gi0/1
13 exit

```

2.1.5. Überprüfung

Mithilfe von **sh ip bgp sum** kann überprüft werden, ob die Verbindung zwischen den zwei ISP aufgebaut wurde.

```
ST-BR4#sh ip bgp sum
BGP router identifier 1.1.1.4, local AS number 1
BGP table version is 14, main routing table version 14
12 network entries using 1728 bytes of memory
12 path entries using 1008 bytes of memory
6/5 BGP path/bestpath attribute entries using 960 bytes of memory
3 BGP AS-PATH entries using 72 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 3768 total bytes of memory
BGP activity 12/0 prefixes, 13/1 paths, scan interval 60 secs

Neighbor      V      AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
1.1.1.1        4      1     8       8       14      0     0 00:04:05      1
1.1.1.2        4      1    12      9       14      0     0 00:04:03      8
1.1.1.3        4      1     8       9       14      0     0 00:03:57      1
209.123.6.2    4      2    13     12       14      0     0 00:04:47      1
```

Abbildung 3: BGP Verbindung

2.2. Theorie

BGP Path Manipulation ist eine Technik, die von Angreifern verwendet wird, um den Datenverkehr über das Internet zu manipulieren. BGP Path Manipulation kann dazu verwendet werden, um Datenverkehr über einen bestimmten Pfad zu leiten oder um Datenverkehr zu blockieren.

2.2.1. Szenario

In unserem Beispiel sagen wir, dass aufgrund des höheren Datendurchsatzes von AS2 wir die Route zu 209.123.2.0 über AS2 leiten wollen und nicht nur über AS3. Wir konfigurieren daher auf dem ST-BR1 Router eine Route Map, die den Pfad zu 209.123.2.0 über AS2 leitet.

2.2.2. Konfiguration

```
1 ip prefix-list route_T0_SHIELD permit 209.123.2.0/24
2
3 route-map T0_SHIELD permit 10
4   match ip address prefix-list route_T0_SHIELD
5   set local-preference 200
6
7 router bgp 1
8   neighbor 209.123.6.2 route-map T0_SHIELD in
```

```
B      209.123.1.0/24 [200/0] via 209.123.3.2, 00:13:02
B      209.123.2.0/24 [200/0] via 209.123.3.2, 00:13:02
```

Abbildung 4: Route vor der Manipulation

```
B      209.123.1.0/24 [200/0] via 209.123.3.2, 00:16:11
B      209.123.2.0/24 [20/0] via 209.123.6.2, 00:00:02
```

Abbildung 5: Route nach der Manipulation

2.3. Distribution List

Wir verwenden die Distribution List aus folgendem Grund. Wir sagen, das der ISP Bifröst schneller ist als der ISP SHIELD und deshalb lernen wir die Route von 209.123.1.0/24 über den ISP Bifröst.

2.3.1. Konfiguration

```
1 ip access-list standard Set_NoTransit
2 deny ip 209.123.1.0 0.0.0.255
3 permit any
4
5 router bgp 1
6 address-family ipv4
7 neighbor 209.123.3.2 distribute-list Set_NoTransit out
```

Danach sollte die Route nur mehr von AS2 gelernt werden.

2.4. Bogons blocken

Auf dem ISP Border-Router **BIF-BR3** wurde auf dem outside Interface In und Out, mithilfe einer Access-List, Bogons blockiert. Die Konfiguration sieht wie folgt aus:

```
1 ip access-list extended BLOCK_BOGONS
2 deny ip 0.0.0.0 0.255.255.255 any
3 deny ip 10.0.0.0 0.255.255.255 any
4 deny ip 100.64.0.0 0.63.255.255 any
5 deny ip 127.0.0.0 0.255.255.255 any
6 deny ip 169.254.0.0 0.0.255.255 any
7 deny ip 172.16.0.0 0.15.255.255 any
8 deny ip 192.0.2.0 0.0.0.255 any
9 deny ip 192.88.99.0 0.0.0.255 any
10 deny ip 192.168.0.0 0.0.255.255 any
11 deny ip 198.18.0.0 0.1.255.255 any
12 deny ip 198.51.100.0 0.0.0.255 any
13 deny ip 203.0.113.0 0.0.0.255 any
14 deny ip 224.0.0.0 31.255.255.255 any
15 permit ip any any
16
17 int gi0/0
```

```
18 ip access-group BLOCK_BOGONS in
19 ip access-group BLOCK_BOGONS out
20 exit
```

2.5. Hub-and-Spoke FlexVPN

Die FlexVPN-Technologie nutzt IKEv2 zur sicheren Verbindung zwischen den Routern. Dabei wird auf dem Hub-Router ein dynamisches Virtual Tunnel Interface (dVTI) und auf den Spoke-Routern ein statisches VTI verwendet.

2.5.1. Konfiguration

Im Stark Tower wurde eine Hub-and-Spoke FlexVPN-Architektur implementiert, bei der der Hub-Router über FlexVPN mit drei Spoke-Routern verbunden ist. Zwischen dem Hub und den Spokes befindet sich der Backbone-Router ST-BB1.

- Hub-Router: ST-BR1
- Spoke-Router: ST-BR2 (Spoke 1), ST-BR3 (Spoke 2), ST-BR4 (Spoke 3)

Hub

```
1 interface Loopback2
2 ip address 172.16.1.254 255.255.255.255
3 exit
4
5 crypto ikev2 keyring IKEV2_KEYRING
6 peer SPOKE_ROUTERS
7 address 0.0.0.0
8 pre-shared-key local cisco123
9 pre-shared-key remote cisco123
10 exit
11
12 crypto ikev2 authorization policy IKEV2_AUTHORIZATION
13 route set interface
14 route set access-list FLEXVPN_ROUTES
15 exit
16
17 ip access-list standard FLEXVPN_ROUTES
18 permit any
19 exit
20
21 crypto ikev2 profile IKEV2_PROFILE
22 match identity remote address 10.0.1.14
23 match identity remote address 10.0.1.2
24 match identity remote address 10.0.1.4
```

```
25 identity local address 10.0.1.10
26 authentication remote pre-share
27 authentication local pre-share
28 keyring local IKEV2_KEYRING
29 aaa authorization group psk list FLEXVPN_LOCAL IKEV2_AUTHORIZATION
30 virtual-template 1
31 exit
32
33 crypto ipsec profile IPSEC_PROFILE
34 set ikev2-profile IKEV2_PROFILE
35 exit
36
37 interface Virtual-Template1 type tunnel
38 ip unnumbered Loopback2
39 tunnel protection ipsec profile IPSEC_PROFILE
40 exit
```

Spoke 1

```
1 crypto ikev2 keyring IKEV2_KEYRING
2 peer ST-BR1
3 address 10.0.1.10
4 pre-shared-key local cisco123
5 pre-shared-key remote cisco123
6 exit
7 exit
8
9 aaa new-model
10 aaa authorization network FLEXVPN_LOCAL local
11
12 crypto ikev2 authorization policy IKEV2_AUTHORIZATION
13 route set interface
14 route set access-list FLEXVPN_ROUTES
15 exit
16
17 ip access-list standard FLEXVPN_ROUTES
18 permit 209.123.3.0 0.0.0.255
19 exit
20
21 crypto ikev2 profile IKEV2_PROFILE
22 match identity remote address 10.0.1.10
23 identity local address 10.0.1.14
24 authentication local pre-share
25 authentication remote pre-share
26 keyring local IKEV2_KEYRING
27 aaa authorization group psk list FLEXVPN_LOCAL IKEV2_AUTHORIZATION
28 exit
29
30 crypto ipsec profile IPSEC_PROFILE
31 set ikev2-profile IKEV2_PROFILE
32 exit
```

```
33
34 interface tunnel 0
35 ip address 172.16.1.1 255.255.255.0
36 tunnel source gi0/3
37 tunnel dest 10.0.10.1
38 tunnel protection ipsec profile IPSEC_PROFILE
39 exit
```

Spoke 2

```
1 crypto ikev2 keyring IKEV2_KEYRING
2 peer ST-BR1
3 address 10.0.1.10
4 pre-shared-key local cisco123
5 pre-shared-key remote cisco123
6 exit
7 exit
8
9 aaa new-model
10 aaa authorization network FLEXVPN_LOCAL local
11
12 crypto ikev2 authorization policy IKEV2_AUTHORIZATION
13 route set interface
14 route set access-list FLEXVPN_ROUTES
15 exit
16
17 ip access-list standard FLEXVPN_ROUTES
18 permit 209.123.10.0 0.0.0.255
19 exit
20
21 crypto ikev2 profile IKEV2_PROFILE
22 match identity remote address 10.0.1.10
23 identity local address 10.0.1.2
24 authentication local pre-share
25 authentication remote pre-share
26 keyring local IKEV2_KEYRING
27 aaa authorization group psk list FLEXVPN_LOCAL IKEV2_AUTHORIZATION
28 exit
29
30 crypto ipsec profile IPSEC_PROFILE
31 set ikev2-profile IKEV2_PROFILE
32 exit
33
34 interface tunnel 0
35 ip address 172.16.1.2 255.255.255.0
36 tunnel source gi0/1
37 tunnel dest 10.0.1.10
38 tunnel protection ipsec profile IPSEC_PROFILE
39 exit
```

Spoke 3

```
1 crypto ikev2 keyring IKEV2_KEYRING
2 peer ST-BR1
3 address 10.0.1.10
4 pre-shared-key local cisco123
5 pre-shared-key remote cisco123
6 exit
7 exit
8
9 aaa new-model
10 aaa authorization network FLEXVPN_LOCAL local
11
12 crypto ikev2 authorization policy IKEV2_AUTHORIZATION
13 route set interface
14 route set access-list FLEXVPN_ROUTES
15 exit
16
17 ip access-list standard FLEXVPN_ROUTES
18 permit 209.123.6.0 0.0.0.255
19 exit
20
21 crypto ikev2 profile IKEV2_PROFILE
22 match identity remote address 10.0.1.10
23 identity local address 10.0.1.4
24 authentication local pre-share
25 authentication remote pre-share
26 keyring local IKEV2_KEYRING
27 aaa authorization group psk list FLEXVPN_LOCAL IKEV2_AUTHORIZATION
28 exit
29
30 crypto ipsec profile IPSEC_PROFILE
31 set ikev2-profile IKEV2_PROFILE
32 exit
33
34 interface tunnel 0
35 ip address 172.16.1.3 255.255.255.0
36 tunnel source gi0/0
37 tunnel dest 10.0.1.10
38 tunnel protection ipsec profile IPSEC_PROFILE
39 exit
```

3. Switching

3.1. Private VLANs

3.1.1. Theorie

Ein Private VLAN erweitert normale VLANs, indem es den Datenverkehr zwischen bestimmten Ports einschränkt. Es gibt drei Haupttypen von PVLAN-Ports: Promiscuous, Community und Isolated. Der Promiscuous Port kann mit allen anderen PVLAN-Ports kommunizieren (z. B. ein Gateway oder Router). Community Ports können untereinander und mit dem Promiscuous Port kommunizieren, aber nicht mit Isolated Ports oder anderen Community Groups. Isolated Ports dürfen nur mit dem Promiscuous Port kommunizieren, nicht untereinander oder mit Community Ports. Das erhöht die Sicherheit, indem bestimmte Geräte voneinander getrennt bleiben.

3.1.2. Konzept

In dem Standort Sanctum Sanctorum gibt es einen RODC und einen Client (VPCS). Diese sind durch Private Isolated VLANs von einander getrennt und kommen daher nur zu ihrem Gateway, der pfsense, über den Promiscuous Port.

3.1.3. Konfiguration

SW-Sans

```
1 # Konfiguration des Switches und der Private VLANs
2
3 en
4 conf t
5 ho SW-SanS
6 no ip domain-lookup
7 usern cisco priv 15
8 usern cisco al sc se cisco
9 ip domain-name 5CN
10 crypto key ge rsa us m 1024
11 ip ssh v 2
12
13 line vty 0 924
14 transport input ssh
15 login local
16 exit
17
18 line con 0
19 exec-time 0 0
20 exit
21
```

```
22 vtp mode transparent
23
24 # Private Isolated VLAN erstellen
25 vlan 100
26 name isolated-vlan-100
27 private-vlan isolated
28 exit
29
30 # Primary VLAN erstellen
31 vlan 10
32 name primary-vlan-10
33 private-vlan primary
34 private-vlan association add 100
35 exit
36
37 # Promiscuous Port konfigurieren
38 int gi0/0
39 des TO_pfSense2
40 switchport mode private-vlan promiscuous
41 switchport private-vlan mapping 10 100
42 exit
43
44 # Isolated Ports konfigurieren
45 int gi0/1
46 des TO_RODC
47 switchport mode private-vlan host
48 switchport private-vlan host-association 10 100
49 exit
50
51 int gi0/2
52 des TO_PC2
53 switchport mode private-vlan host
54 switchport private-vlan host-association 10 100
55 exit
```

3.1.4. Überprüfung

In folgendem Screenshot ist zu sehen, wie PC2 versucht den RODC mit der IP Adresse 192.168.125.1 zu erreichen. Da PC2 nur mit dem Promiscuous Port kommunizieren darf kann er nur die IP Adresse 192.168.125.254 (pfSense) pingen.

```

Welcome to Virtual PC Simulator, version 0.6.2
Dedicated to Daling.
Build time: Apr 10 2019 02:42:20
Copyright (c) 2007-2014, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file

PC2> ip 192.168.125.2/24 192.168.125.254
Checking for duplicate address...
PC1 : 192.168.125.2 255.255.255.0 gateway 192.168.125.254

PC2> ping 192.168.125.1
host (192.168.125.1) not reachable

PC2>
PC2> ping 192.168.125.254
84 bytes from 192.168.125.254 icmp_seq=1 ttl=64 time=4.583 ms
84 bytes from 192.168.125.254 icmp_seq=2 ttl=64 time=4.555 ms
84 bytes from 192.168.125.254 icmp_seq=3 ttl=64 time=4.858 ms
84 bytes from 192.168.125.254 icmp_seq=4 ttl=64 time=8.209 ms
84 bytes from 192.168.125.254 icmp_seq=5 ttl=64 time=6.683 ms

```

Abbildung 6: Test Ping von PC2

3.2. RSPAN

RSPAN wird verwendet um den gesamten Traffic eines VLANs auf einem Switch zu spiegeln und an einen anderen Switch zu senden. Dies ermöglicht es, den Traffic mit einem Sniffer zu analysieren, ohne den normalen Betrieb des Netzwerks zu beeinträchtigen.

3.2.1. Konfiguration

In unserem Fall wurde bei der Hawkeye Farm ein RSPAN eingerichtet, um den Traffic auf HWF-CLI2 zu spiegeln. Dazu werden die Switches SW-HWF3 und SW-HWF4 verwendet.

SW3:

```

1  vlan 100
2  remote-span
3  exit

```

```
4
5 monitor session 1 source interface gi 0/0
6 monitor session 1 destination remote vlan 100
```

SW4:

```
1 vlan 100
2 remote-span
3 exit
4
5 monitor session 1 source remote vlan 100
6 monitor session 1 destination interface gi 0/0
```

3.3. Spanningtree

SpanningTree wird verwendet, um Schleifen in einem Netzwerk zu verhindern. Es wird auf Layer 2 Switches eingesetzt und berechnet den besten Pfad zu einem Ziel. Dabei werden redundante Verbindungen deaktiviert, um Schleifen zu vermeiden. SpanningTree ist ein Protokoll, das auf dem IEEE 802.1D-Standard basiert und in verschiedenen Varianten wie STP, RSTP und MSTP verfügbar ist.

3.3.1. RSTP aktivieren

```
1 # RSTP aktivieren
2 spanning-tree mode rapid-pvst
3 # Eindeutige Bridge ID durch die erweiterte System ID gewährleisten
4 spanning-tree extend system-id
5
6 spanning-tree vlan 10 root primary
7 spanning-tree vlan 30 root secondary
```

3.3.2. Root Guard

```
1 # Verhindert unbeabsichtigte Root Bridge-Übernahmen
2 interface GigabitEthernet0/1
3 spanning-tree guard root
```

3.3.3. Loop Guard

```
1 # Erkennt unidirektionale Link-Fehler
2 interface GigabitEthernet0/1
```

3 spanning-tree guard loop

3.3.4. BPDU Guard

```

1 # Verhindert unerwünschte Spanning Tree Topologie-Änderungen
2 spanning-tree portfast bpduguard default
3 interface GigabitEthernet0/1
4 spanning-tree bpduguard enable
5 spanning-tree portfast edge

```

```

Switch(config)#do sh spanning-tree summary
Switch is in rapid-pvst mode
Root bridge for: VLAN0001
Extended system ID           is enabled
Portfast Default              is disabled
Portfast Edge BPDU Guard Default is enabled
Portfast Edge BPDU Filter Default is disabled
Loopguard Default             is enabled
PVST Simulation Default       is enabled but inactive in rapid-pvst mode
Bridge Assurance               is enabled
EtherChannel misconfig guard   is enabled
Configured Pathcost method used is short
UplinkFast                     is disabled
BackboneFast                   is disabled

```

Abbildung 7: Anzeige der Aktivierten Guards

4. Firewalls

4.1. Anti Virus

4.1.1. Konfiguration des AV Profiles

Das AV Profile wird so konfiguriert, dass alle Dateien blockiert werden, die als Virus erkannt werden. Der folgende Code zeigt die Konfiguration des AV Profiles.

```

1 config antivirus profile
2   edit „AV_SVAL“
3     set feature-set proxy
4     config http
5       set av-scan block
6       set outbreak-prevention block
7     end
8     config ftp
9       set av-scan block
10      set outbreak-prevention block

```

```

11      end
12  config imap
13      set av-scan block
14      set outbreak-prevention block
15      set executables virus
16  end
17  config pop3
18      set av-scan block
19      set outbreak-prevention block
20      set executables virus
21  end
22  config smtp
23      set av-scan block
24      set outbreak-prevention block
25      set executables virus
26  end
27  config cifs
28      set av-scan block
29      set outbreak-prevention block
30  end
31 next
32 end

```

4.1.2. Custom-Deep-Inspection

Anschließend muss die custom deep inspection konfiguriert werden. Dafür muss auf den Ziel Clients das FortiGate Zertifikat installiert werden. Im Firefox-Browser wird das wie folgt gemacht:

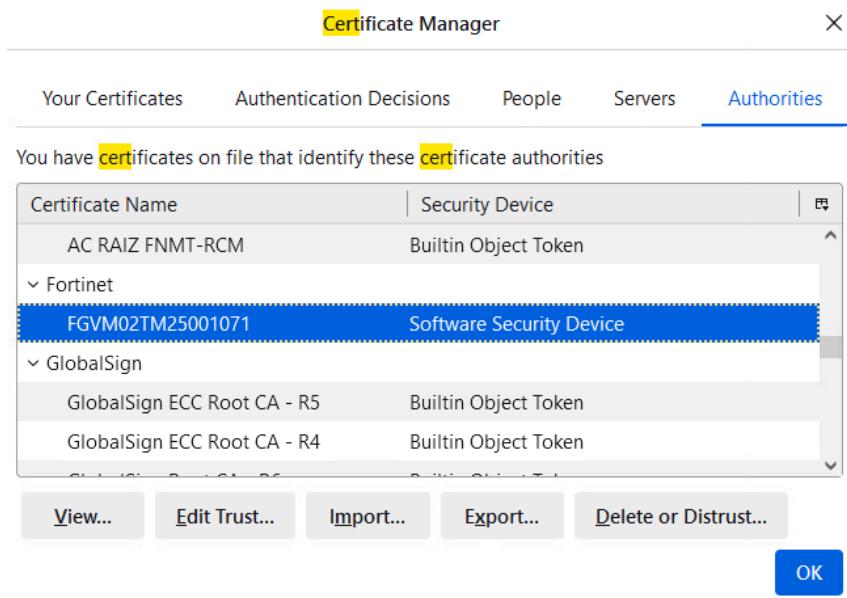


Abbildung 8: FireFox Zertifikat installieren

4.1.3. Überprüfung

Damit der AV nun getestet werden kann, wird eine Datei von der Website [www.eicar.org](https://secure.eicar.org/eicar.com.txt) installiert. Diese Datei ist ein Testvirus und wird von den meisten AV-Programmen erkannt. Wenn der AV funktioniert, wird die Datei blockiert und der Benutzer sieht folgenden Output.

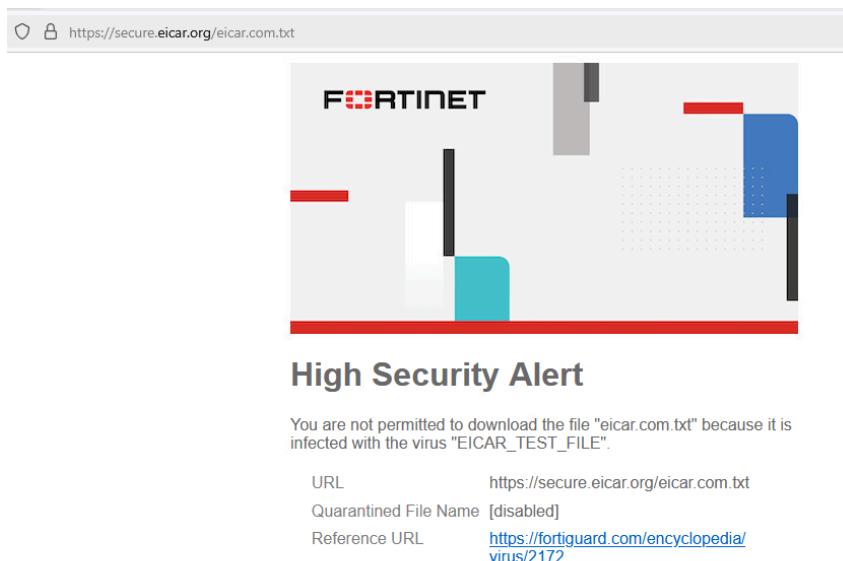


Abbildung 9: AV blockiert File

4.2. Data Leak Prevention

Data Leak Prevention (DLP) ist eine Technologie, die den unautorisierten Transfer von sensiblen Daten verhindert. DLP-Systeme überwachen den Datenverkehr und blockieren oder alarmieren, wenn sie sensible Daten erkennen. DLP-Systeme können auf verschiedenen Ebenen des OSI-Modells arbeiten, um Daten zu schützen. DLP-Systeme können auf der Anwendungsschicht arbeiten, um Daten in E-Mails oder Webseiten zu schützen.

4.2.1. Konfiguration Block Exe Datein

```
1 config dlp filepattern
2   edit 3
3     set name "case3-exe"
4     config entries
5       edit "exe"
6         set filter-type type
7         set file-type exe
8       next
9     end
```

```
10      next
11  end
```

4.2.2. Firewall Policy

```
1 config firewall policy
2   edit 9
3     set dlp-profile "profile-case3-type-size"
4   next
5 end
```

4.2.3. Überprüfung

Um zu überprüfen, ob die DLP-Konfiguration korrekt ist, geben Sie den folgenden Befehl ein:

```
1 show full-configuration dlp profile
```

Damit wir die Konfiguration der .exe Datei überprüfen können, wird putty.exe installiert. Wie man auf dem Screenshot sehen kann wird dieser blockiert.



Attention

The file "putty.exe" has been blocked due to its file type and/or properties.

URL <https://the.earth.li/~sgtatham/putty/0.83/wa64/putty.exe>

Abbildung 10: Blocked by FortiGate

4.3. Intrusion Prevention System

Ein Intrusion Prevention System (IPS) ist eine Technologie, die den unautorisierten Zugriff auf ein Netzwerk verhindert. IPS-Systeme überwachen den Datenverkehr und blockieren oder alarmieren, wenn sie verdächtige Aktivitäten erkennen. IPS-Systeme können auf verschiedenen Ebenen des OSI-Modells arbeiten, um Daten zu schützen. IPS-Systeme können auf der Anwendungsschicht arbeiten, um Daten in E-Mails oder Webseiten zu schützen.

4.3.1. Konfiguration

In der FortiGate GUI wird unter **Security Profiles > Intrusion Prevention** eine neues IPS-Profil erstellt. In diesem Profil werden Regeln definiert, die den Datenverkehr überwachen und blockieren oder alarmieren, wenn verdächtige Aktivitäten erkannt werden. Es wird dabei eine Signatur erstellt.

Dieses Profil wird dann anschließend der Firewall Policy zugewiesen, um den Datenverkehr zu überwachen.

4.3.2. Überprüfung

Um die Funktionalität des IPS zu testen, kann ein Angriff simuliert werden. Dazu kann ein Angriffssignatur in das Profil eingefügt werden.

Unter **Logs & Reports > System Events** werden die Events von IPS angezeigt.

Intrusion Prevention		
Top Attack	Action	Count
Eicar.Virus.Test.File	Detected	2
2 events		

Abbildung 11: System Events

4.4. Webfilter

4.4.1. Theorie

Der Web-Filter der FortiGate ist zuständig, um den Client auf gewisse Website den Zugriff zu verweigern oder zu gewähren. Man kann dabei bestimmte URLs blocken. Die Konfiguration könnte so aussehen. Dazu gehen wir in Security-Profiles auf **Webfilter**. Das folgende Beispiel blockiert Instagram und Facebook.

URL	Type	Action	Status
instagram.com	Wildcard	Block	Enable
facebook.com	Wildcard	Block	Enable

Abbildung 12: URL Filter

4.4.2. Überprüfung

Falls Clients dann versuchen auf die Website zu gelangen sehen sie Folgenden Alert.

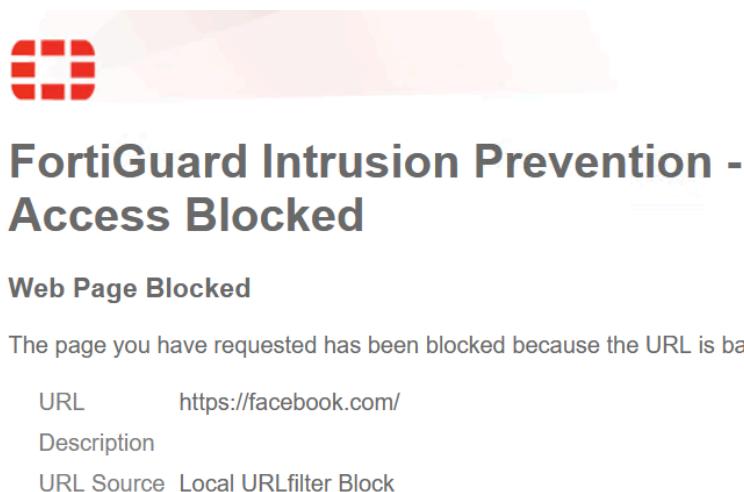


Abbildung 13: Access Block

In der FortiGate kann dann unter **Log & Reports > Security Events** das Events angezeigt werden, welches durch den Alert geloggt wurde.

4.5. Fortigate Bogons

Bogon sind private Adressen, die im öffentlichen Netz geblockt werden sollen. Auf der FortiGate werden daher eine local-in-policy erstellt die dazu dienen diese Adressen zu blockieren. Folgender Code blockiert diese Adressen.

4.5.1. Konfiguration

```
1 config firewall address
2     edit "Bogon_0.0.0.0/8"
3         set subnet 0.0.0.0 255.0.0.0
4     next
5     edit "Bogon_10.0.0.0/8"
6         set subnet 10.0.0.0 255.0.0.0
7     next
8     edit "Bogon_100.64.0.0/10"
9         set subnet 100.64.0.0 255.192.0.0
10    next
11    edit "Bogon_127.0.0.0/8"
12        set subnet 127.0.0.0 255.0.0.0
13    next
14    edit "Bogon_169.254.0.0/16"
15        set subnet 169.254.0.0 255.255.0.0
16    next
17    edit "Bogon_172.16.0.0/12"
18        set subnet 172.16.0.0 255.240.0.0
19    next
20    edit "Bogon_192.0.0.0/24"
21        set subnet 192.0.0.0 255.255.255.0
22    next
23    edit "Bogon_192.0.2.0/24"
24        set subnet 192.0.2.0 255.255.255.0
25    next
26    edit "Bogon_192.168.0.0/16"
27        set subnet 192.168.0.0 255.255.0.0
28    next
29    edit "Bogon_198.18.0.0/15"
30        set subnet 198.18.0.0 255.254.0.0
31    next
32    edit "Bogon_198.51.100.0/24"
33        set subnet 198.51.100.0 255.255.255.0
34    next
35    edit "Bogon_203.0.113.0/24"
36        set subnet 203.0.113.0 255.255.255.0
37    next
38    edit "Bogon_224.0.0.0/4"
39        set subnet 224.0.0.0 240.0.0.0
40    next
41    edit "Bogon_240.0.0.0/4"
42        set subnet 240.0.0.0 240.0.0.0
43    next
44    edit "Bogon_255.255.255.255/32"
45 set subnet 255.255.255.255 255.255.255.255
46    next
47 end
```

```

1 Dieser Codeabschnitt legt die Adressen die später blockiert werden sollen
2 fest
3
4 config firewall addrgrp
5     edit "Bogon_Addresses"
6         set member "Bogon_0.0.0.0/8" "Bogon_10.0.0.0/8"
7             "Bogon_100.64.0.0/10" "Bogon_127.0.0.0/8" "Bogon_169.254.0.0/16"
8             "Bogon_172.16.0.0/12" "Bogon_192.0.0.0/24" "Bogon_192.0.2.0/24"
9             "Bogon_192.168.0.0/16" "Bogon_198.18.0.0/15" "Bogon_198.51.100.0/24"
10            "Bogon_203.0.113.0/24" "Bogon_224.0.0.0/4" "Bogon_240.0.0.0/4"
11            "Bogon_255.255.255.255/32"
12        next
13    end

```

Hier werden Adress-Gruppen für die Bogons erstellt. Anschließend werden sie der Policy zugewiesen.

```

1 config firewall local-in-policy
2     edit 1
3         set intf "VLAN 10 HA"
4         set srcaddr "Bogon_Addresses"
5         set dstaddr "all"
6         set service "PING"
7         set schedule "always"
8     next
9     edit 2
10        set intf "VLAN 20 HA"
11        set srcaddr "Bogon_Addresses"
12        set dstaddr "all"
13        set service "PING"
14        set schedule "always"
15    next
16 end

```

Falls nun eine private Adresse im AS auftaucht und diese Adresse versucht die FortiGate zu erreichen wird diese geblockt.

4.6. FortiGate HA-Cluster

4.6.1. Was ist ein HA-Cluster?

Ein HA-Cluster (High Availability Cluster) ist ein System, das aus zwei oder mehr Rechnern besteht, die zusammenarbeiten, um eine hohe Verfügbarkeit von Diensten zu gewährleisten. Ein HA-Cluster kann so konfiguriert werden, dass er automatisch auf einen anderen Rechner umschaltet, wenn einer der Rechner ausfällt. Dies wird als Failover bezeichnet. Ein HA-Cluster

kann auch so konfiguriert werden, dass er Lasten zwischen den Rechnern verteilt, um die Leistung zu verbessern. Dies wird als Load Balancing bezeichnet.

Es gibt bei der FortiGate zwei verschiedene Arten von HA-Clustern:

- Active-Passive: Hier ist nur ein Gerät aktiv und das andere Gerät ist im Standby-Modus.
(failover)
- Active-Active: Hier sind beide Geräte aktiv und teilen sich die Last. (load-balancing)

4.6.2. Konfiguration eines HA-Clusters

Die beiden FortiGate sind mithilfe eines Kabels verbunden. Man nennt dieses das Heartbeat-Interface, darüber läuft der Traffic zwischen den beiden Geräten.

```
1 # Auf FG1
2 config system ha
3     set mode a-a
4     set group-name HA_Cluster
5     set password admin
6     set hbdev port4 50
7 end
```

```
1 # Auf FG2
2 config system ha
3     set mode a-a
4     set group-name HA_Cluster
5     set password admin
6     set hbdev port4 60
7 end
```

Es kann vorkommen, dass nach der Konfiguration die zwei Nodes nicht synchronized sind. Daher muss folgender Befehl ausgeführt werden.

```
1 execute ha synchronize all
```

4.6.3. Überprüfung

Falls, alles richtig funktioniert sehen wir in der GUI folgendes.

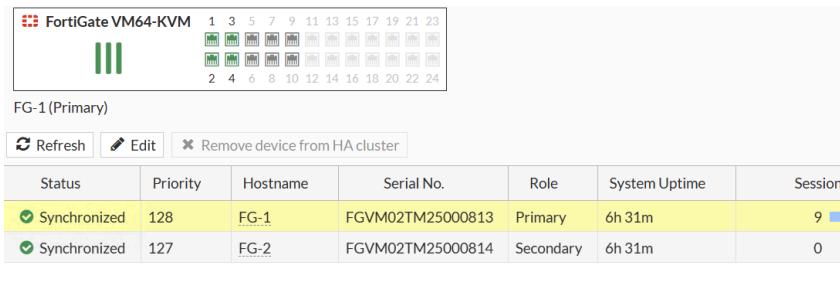


Abbildung 14: Synchronisation von den Cluster-Nodes

4.7. Site-to-Site-VPN PSK

4.7.1. Theorie

Ein Site-to-Site VPN mit PSK (Pre-Shared Key) ermöglicht die sichere Verbindung zwischen zwei Standorten über das Internet. Dabei verwenden beide FortiGate-Firewalls einen gemeinsamen geheimen Schlüssel für die Authentifizierung.

4.7.2. Konfiguration

4.7.2.1. VPN Erstellen

```

1 config vpn ipsec phasel-interface
2   edit "T0_FG2" # Name der Phase-1-Schnittstelle
      set interface "VLAN10" # Das physischeInterface, über das der
3       VPN-Tunnel aufgebaut wird
      set remote-gw 209.123.5.2 # Die öffentliche IP-Adresse des
4       entfernten VPN-Gateways
      set psksecret admin # Der Pre-Shared Key für die
5       Authentifizierung
      set proposal aes128-sha256 # Verschlüsselungs-Algorithmus für
6       Phase 1
      next
8 end
9 config vpn ipsec phase2-interface
10   edit "T0_FG2" # Name der Phase-2-Schnittstelle
11     set phasename "toFG2" # Verknüpft der Phase-Konfiguration
12     set proposal aes128-sha256 # Verschlüsselungs-Algorithmus für
13      Phase 2
14       set src-subnet 192.168.50.0 255.255.255.0 # Das lokale Subnetz,
15       das über den Tunnel erreichbar sein soll
           set dst-subnet 10.0.0.0 255.255.255.0 # Das Ziel-Subnetz auf der
             Gegenseite des VPN-Tunnels
             next

```

16 end

4.7.2.2. Statische Route für den Tunnel

Es wird eine Statische Route benötigt damit der Traffic über den VPN-Tunnel geht.

```
1 config router static
2   edit 1
3     set device "T0_FG2"
4     set dstaddr "T0_FG2_remote" # Gruppe aller remoten Adressen
5   next
6 end
```

4.7.2.3. Policy für den VPN

Eine Policy wird für den VPN-Tunnel konfiguriert.

```
1 config firewall policy
2   edit 1
3     set name "T0_FG2_local" # Regel für ausgehenden Traffic
4     set srcintf "port4" # Lokales Interface
5     set dstintf "T0_FG2_zone" # VPN-Zielinterface
6     set action accept # Erlaubt Traffic
7     set srcaddr "T0_FG1_local" # Lokale Adressen
8     set dstaddr "T0_FG2_remote" # Remote-Adressen
9     set schedule "always" # Immer aktiv
10    set service "ALL" # Alle Dienste erlaubt
11    set logtraffic all # Traffic loggen
12  next
13 end
14 config firewall policy
15   edit 2
16     set name "T0_FG1_remote" # Regel für eingehenden Traffic
17     set srcintf "T0_FG1_zone" # VPN-Interface
18     set dstintf "port4" # Lokales Interface
19     set action accept # Erlaubt Traffic
20     set srcaddr "T0_FG2_remote" # Remote-Adressen
21     set dstaddr "T0_FG1_local" # Lokale Adressen
22     set schedule "always" # Immer aktiv
23     set service "ALL" # Alle Dienste erlaubt
24     set logtraffic all # Traffic loggen
25  next
26 end
```

4.8. NPS FortiGate Captive Portal

Mithilfe des NPS Dienstes unter Windows sollen sich die AD-User auf einer FortiGate oder um ins Internet zu gelangen authentifizieren. Diese Datei beschreibt die Konfiguration des NPS Dienstes und der FortiGate.

4.8.1. NPS Konfiguration

Nachdem der NPS Server grundkonfiguriert wurde und der Network Policy Server installiert ist, wird zuerst ein neuer Radius-Client erstellt. **NPS > Radius Client und Server > Radius Clients > Neu**. Hier wird die IP-Adresse der FortiGate und ein gemeinsames Passwort einge tragen.

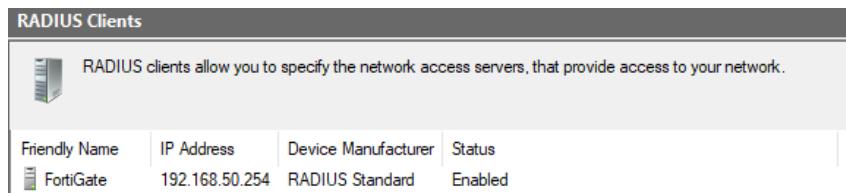


Abbildung 15: Radius Client Konfiguration

1. Hinzufügen der FortiGate zu den ‚RADIUS Clients‘ in der MS NPS-Konfiguration (wählen Sie ‚RADIUS Clients‘ und wählen Sie ‚Neu‘).
2. Geben Sie die Details des FortiGate RADIUS-Clients ein:
 - Versichern Sie sich, dass das Kästchen ‚Enable this RADIUS client‘ aktiviert ist.
 - Geben Sie den ‚Friendly name‘, die IP-Adresse und das Passwort ein (das gleiche Passwort, das auf der FortiGate konfiguriert wurde).
 - Der Rest kann auf den Standardwerten belassen werden.

4.8.2. Connection Request Policies

1. Erstellen Sie eine ‚Connection Request Policy‘ für die FortiGate (wählen Sie ‚Connection Request Policies‘ und wählen Sie ‚Neu‘).
2. Geben Sie den ‚Policy name‘ an und wählen Sie ‚Weiter‘.
3. Unter ‚Specify Conditions‘ wählen Sie ‚Add...‘ und wählen Sie ‚Client IPv4 Address‘ und geben Sie die IP-Adresse der FortiGate an.

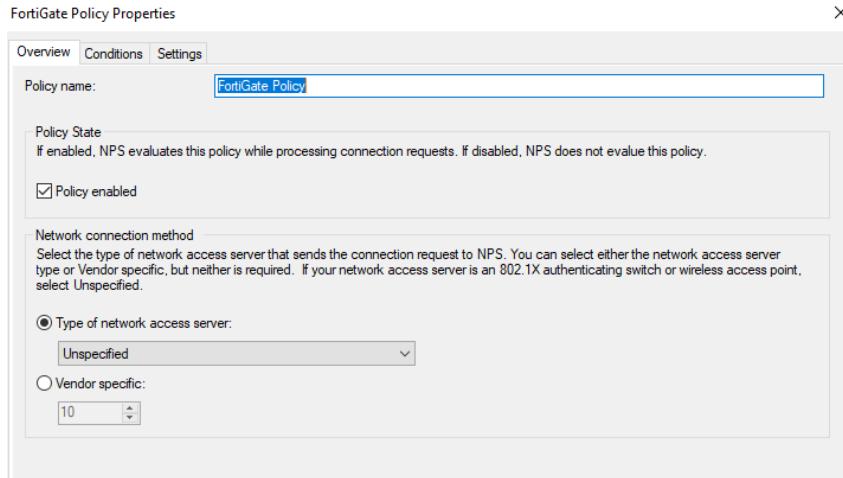


Abbildung 16: Connection Request Policy

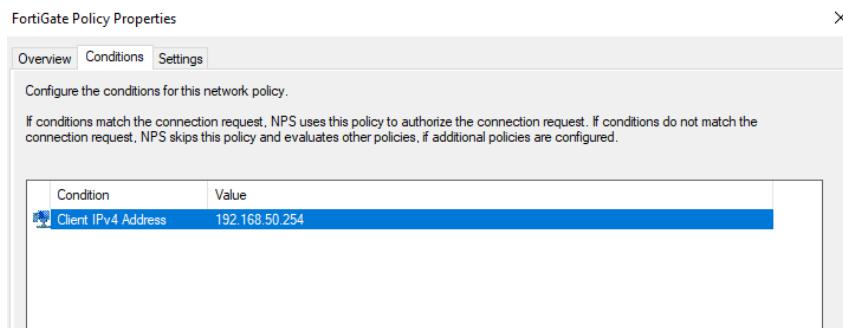


Abbildung 17: Connection Request Policy

4.8.3. Network Policies

1. Erstelle eine ‚Network Policy‘ für Zugriffsanfragen, die von der FortiGate kommen (wählen Sie ‚Network Policies‘ und wählen Sie ‚Neu‘). NPS -> Policies -> Network Policies.
2. Geben Sie den ‚Policy name‘ an und wählen Sie ‚Weiter‘.

Adding Network Policy with AD authentication.

Hinzufügen einer Netzwerkrichtlinie mit AD-Authentifizierung.

1. Unter ‚Specify Conditions‘ wählen Sie ‚Add...‘ und wählen Sie ‚Windows Groups‘ wählen Sie ‚Add Groups...‘ und geben Sie den AD-Gruppennamen ein.

Wenn Sie fertig sind, bestätigen Sie die Einstellungen mit ‚OK‘ und ‚Hinzufügen...‘.

- Geben Sie die Zugriffsberechtigung an und wählen Sie ‚Weiter‘

- Der Rest kann auf den Standardwerten belassen werden.

The screenshot shows the 'Network Policies' configuration screen. It displays a table of policies:

Policy Name	Status	Processing Order	Access Type	Source
FortiGate Policy	Enabled	1	Grant Access	Unspecified
Connections to Microsoft Routing and Remote Access server	Enabled	999998	Deny Access	Unspecified
Connections to other access servers	Enabled	999999	Deny Access	Unspecified

Below the table, under 'FortiGate Policy', the 'Conditions - If the following conditions are met:' section is shown, containing a single condition: 'Windows Groups AvangerHQ\Domain Users'. The 'Settings - Then the following settings are applied:' section lists the following values:

Setting	Value
Authentication Method	MS-CHAP v1 OR MS-CHAP v1 (User can change password after it has expired) OR MS-CHAP v...
Access Permission	Grant Access
Framed-Protocol	PPP
Service-Type	Framed
Ingnore User Dial-In Properties	False

Abbildung 18: Funktionsbereite Network Policy

4.8.4. Vendor Specific Attributes

The screenshot shows the 'Configure Settings' dialog for 'Vendor Specific' attributes. On the left, a sidebar lists settings categories: RADIUS Attributes (selected), Standard, Vendor Specific, Routing and Remote Access, Multilink and Bandwidth Allocation Protocol (BAP), IP Filters, Encryption, and IP Settings. The main pane displays instructions: 'NPS applies settings to the connection request if all of the network policy conditions and constraints for the policy are matched.' Below this, it says 'Configure the settings for this network policy. If conditions and constraints match the connection request and the policy grants access, settings are applied.' A 'Settings:' section on the left contains a 'Vendor Specific' checkbox which is checked. To the right, there is a table titled 'Attributes:' with columns 'Name', 'Vendor', and 'Value'. Buttons at the bottom include 'Add...', 'Edit...', and 'Remove'. Navigation buttons at the bottom right are 'Previous', 'Next', 'Finish', and 'Cancel'.

Abbildung 19: Vendor Specific Attributes

1. Drücken Sie auf ‚Add...‘ und wählen Sie ‚Vendor-Specific‘
2. Wählen Sie ‚Add...‘ und geben Sie die Vendor Code ‚12356‘ ein und Yes. It conforms.
3. Dürcken sie nun auf Configure Attribute und geben Sie die Attribute ein. vendor: 12356, attribute: 1, as string: Domain_User.
4. Überprüfen der Konfiguration und Finish

4.8.5. FortiGate Konfiguration

Nachdem der NPS Server konfiguriert wurde, wird die FortiGate konfiguriert. Dazu wird ein neuer Radius-Server erstellt. **User & Device > Radius Servers > Neu**. Hier wird die IP-Adresse des NPS Servers und das gemeinsame Passwort eingetragen. Unter Test Connectivity kann die Verbindung getestet werden und mit Test Credentials kann ein Anmeldevorgang simuliert werden.

The screenshot shows the configuration of a new Radius server named "NPSRadius". The "Authentication method" is set to "Default". Under "Primary Server", the IP/Name is "192.168.50.30" and the secret is masked as "*****". A successful connection status is indicated. Buttons for "Test Connectivity" and "Test User Credentials" are visible.

Name	NPSRadius
Authentication method	Default Specify
NAS IP	
Include in every user group	<input checked="" type="checkbox"/>
Primary Server	
IP/Name	192.168.50.30
Secret	*****
Connection status	✓ Successful
Test Connectivity	
Test User Credentials	

Abbildung 20: Radius Server Konfiguration in der FortiGate

Anschließend wird eine neue User Group erstellt die als Remote Server den NPS Server einge-tragen hat. **User & Device > User Groups > Neu**. Hier wird der Name der Gruppe und der NPS Server eingetragen. Daraufhin wird unter dem jeweiligen Port ein neues Captive Portal erstellt.

The screenshot shows the 'Network' configuration section of a FortiGate device. Under 'Security mode', 'Captive Portal' is selected. In the 'User access' section, 'Restricted to Groups' is chosen. A list of exempt sources is shown, including 'NPSRadius' and three other entries represented by '+' icons. At the bottom, there are tabs for 'Original Request' and 'Specific URL'.

Abbildung 21: Captive Portal Konfiguration

4.8.6. Überprüfung

Wenn alle Konfigurations schritte durchgeführt wurden, sollte sich ein AD-User auf der FortiGate oder im Internet authentifizieren können. Folgendes sollte passieren:

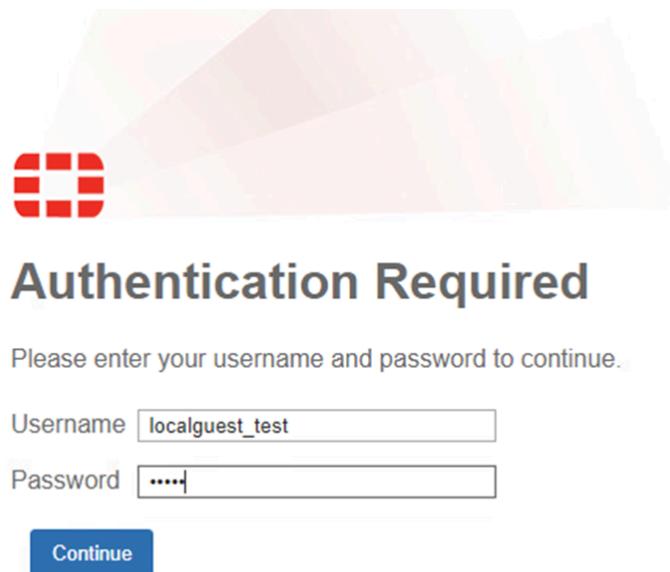


Abbildung 22: Login Screen

4.9. Statischer NAT

4.9.1. Theorie

Eine statische NAT (Destination NAT oder DNAT) auf einer FortiGate-Firewall wird verwendet, um eingehenden Datenverkehr von einer öffentlichen IP-Adresse an eine private IP-Adresse im internen Netzwerk weiterzuleiten. Dies wird oft für Webserver, Mailserver oder andere interne Dienste genutzt.

4.9.2. Konfiguration

4.9.2.1. Erstellen der VIP

```

1 config firewall vip
2   edit "VIP_Webserver"
3     set extip 209.123.50.10      # Öffentliche IP-Adresse
4     set mappedip 192.168.50.100   # Interne IP des Servers
5     set extintf "VLAN10"         # WAN-Schnittstelle
6     set portforward enable      # Portweiterleitung aktivieren
7     set protocol tcp
8     set extport 80                # Öffentlicher Port (HTTP)
9     set mappedport 80             # Interner Port
10    next
11 end

```

4.9.2.2. Zuweisen in der Policy

```

1 config firewall policy
2   edit 10                      # ID der neuen Regel (automatisch
3     nummeriert)
4     set name "Allow_HTTP_NAT"
5     set srcintf "LAN"            # Eingehendes Interface (WAN)
6     set dstintf "VLAN10"         # Ziel-Interface (LAN)
7     set srcaddr "VIP_Webserver"  # Erlaubt von überall
8     (anpassen, falls gewünscht)
9     set dstaddr "all"           # Die erstellte VIP als Ziel
10    set action accept          # Erlauben des Verkehrs
11    set schedule "always"
12    set service "HTTP"          # Nur HTTP-Verkehr erlauben
13    set logtraffic all         # Logging aktivieren
14    next
15 end

```

4.10. Pfsense

Die Pfsense wird auf dem Standort Sanctum Sanctorum eingesetzt. Sie dient als Firewall und Router und schützt das interne Netzwerk vor unerwünschtem Datenverkehr. Die Pfsense bietet eine Vielzahl von Funktionen und kann durch zusätzliche Pakete erweitert werden. Sie wird über eine Web-Oberfläche konfiguriert und kann auch über die Kommandozeile bedient werden.

4.10.1. Platformübergreifender VPN

Zwischen dem FortiGate-HA Cluster und der Pfsense wird ein VPN-Tunnel eingerichtet. Dieser Tunnel wird über IPsec realisiert und ermöglicht eine sichere Kommunikation zwischen den beiden Standorten. Die Konfiguration erfolgt auf beiden Seiten und beinhaltet die Angabe der IP-Adressen, der Pre-Shared Key und der Verschlüsselungseinstellungen.

Zuerst werden die IP-Adressen unter **Interfaces** zugewiesen.

General Configuration	
Enable	<input checked="" type="checkbox"/> Enable interface
Description	OPT2 Enter a description (name) for the interface here.
IPv4 Configuration Type	Static IPv4
IPv6 Configuration Type	None
MAC Address	xx:xx:xx:xx:xx:xx This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: xx:xxxx:xxxx or leave blank.
MTU	If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS	If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.
Speed and Duplex	Default (no preference, typically autoselect) Explicitly set speed and duplex mode for this interface. WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.
Static IPv4 Configuration	
IPv4 Address	192.168.125.254
IPv4 Upstream gateway	None
	+ Add a new gateway

Abbildung 23: Interface anlegen

In der nachfolgenden Abbildung sehen sie die Konfiguration des VPN-Tunnels auf der Pfsense. Dies passiert unter **VPN -> IPsec -> Tunnels**.

IPsec Tunnels									
	ID	IKE	Remote Gateway	Auth/Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Actions
<input type="checkbox"/>	1	Disable	V2	OPT1 209.123.10.1	Mutual PSK	AES (128 bits)	SHA256	5 (1536 bit)	Pfsense1_TO_FG-2
+ Show Phase 2 Entries (1)									
+ Add P1									

Abbildung 24: VPN Tunnel

Anschließend muss noch eine Rule für den VPN erstellt werden. Diese erlaubt standardmäßig den gesamten Traffic.

Firewall / Rules / IPsec										
Floating	WAN	LAN	OPT1	OPT2	IPsec					
Rules (Drag to Change Order)										
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<input type="checkbox"/>	0/0 B	IPv4 *	*	*	*	*	*	*	none	
+ Add										

Abbildung 25: Regel festlegen

5. Active Directory

5.1. Active Directory Services

5.1.1. DC1

Grundkonfiguration

```

1 Rename-Computer -NewName "DC1"
2
3 # Netzwerkkonfiguration
4 Get-NetAdapter Ethernet0 | Rename-NetAdapter -NewName "LAN"
5 New-NetIPAddress -InterfaceAlias "LAN" -IPAddress "192.168.50.1" -
6 PrefixLength 24 -DefaultGateway "192.168.50.254"
7 Set-DnsClientServerAddress -InterfaceAlias "LAN" -ServerAddresses
8 ("192.168.50.1", "192.168.50.2")
9
10 # Zeitzone setzen
11 Set-TimeZone -Id "W. Europe Standard Time"
12
13 Restart-Computer

```

Forest Root Domäne AvengerHQ.at erstellen

```

1 # Features installieren
2 Install-WindowsFeature -Name "AD-Domain-Services" -IncludeManagementTools
3 Install-WindowsFeature -Name "DNS" -IncludeManagementTools
4
5 # Domäne erstellen
Install-ADDSForest -CreateDnsDelegation:$false -DatabasePath "C:
\Windows\NTDS" -DomainMode "WinThreshold" -DomainName "AvengerHQ.at" -
DomainNetbiosName "AvengerHQ" -ForestMode "WinThreshold" -InstallDns:$true
6 -LogPath "C:\Windows\NTDS" -NoRebootOnCompletion:$true -
SafeModeAdministratorPassword (ConvertTo-SecureString "Supergeheim123!" -
AsPlainText -Force) -SysvolPath "C:\Windows\SYSVOL" -Force:$true
7
8 Restart-Computer

```

5.1.2. DC2

Grundkonfiguration

```

1 Rename-Computer -NewName "DC2"
2
3 # Netzwerkkonfiguration
4 Get-NetAdapter Ethernet0 | Rename-NetAdapter -NewName "LAN"
New-NetIPAddress -InterfaceAlias "LAN" -IPAddress "192.168.50.2" -
5 PrefixLength 24 -DefaultGateway "192.168.50.254"
Set-DnsClientServerAddress -InterfaceAlias "LAN" -ServerAddresses
6 ("192.168.50.1", "192.168.50.2")
7
8 # Zeitzone setzen
9 Set-TimeZone -Id "W. Europe Standard Time"
10
11 Restart-Computer

```

AvengerHQ.at beitreten

```

1 # Features installieren
2 Install-WindowsFeature -Name "AD-Domain-Services" -IncludeManagementTools
3 Install-WindowsFeature -Name "DNS" -IncludeManagementTools
4
5 # Domäne beitreten
Install-ADDSDomainController -DomainName "AvengerHQ.at" -Sitetename Default-
First-Site-Name -Credential (Get-Credential "AvengerHQ.at\Administrator")
6 -SafeModeAdministratorPassword (ConvertTo-SecureString "Supergeheim123!" -
AsPlainText -Force) -InstallDNS -Confirm:$false
7

```

```
8 # DNS zurück ändern
Set-DnsClientServerAddress -InterfaceAlias "LAN" -ServerAddresses
9 ("192.168.50.2", "192.168.50.1")
```

5.1.3. WinCLI1

Grundkonfiguration

```
1 Rename-Computer -NewName "WinCLI1"
2
3 # Netzwerkkonfiguration
4 Get-NetAdapter Ethernet0 | Rename-NetAdapter -NewName "LAN"
5
6 # Firewallregeln setzen
7 Set-NetFirewallRule -Name "FPS-ICMP4-ERQ-In" -Enabled True -Profile
8 Domain,Private,Public
9 Set-NetFirewallRule -Name "FPS-ICMP4-ERQ-Out" -Enabled True -Profile
10 Domain,Private,Public
11 # Zeitzone setzen
12 Set-TimeZone -Id "W. Europe Standard Time"
13 Restart-Computer
```

AvengerHQ.at beitreten

```
1 Add-Computer -DomainName AvengerHQ.at -Credential (Get-Credential) -
2 Restart
```

5.1.4. WinCLI2

Grundkonfiguration

```
1 Rename-Computer -NewName "WinCLI2"
2
3 # Netzwerkkonfiguration
4 Get-NetAdapter Ethernet0 | Rename-NetAdapter -NewName "LAN"
5
6 # Firewallregeln setzen
7 Set-NetFirewallRule -Name "FPS-ICMP4-ERQ-In" -Enabled True -Profile
8 Domain,Private,Public
9 Set-NetFirewallRule -Name "FPS-ICMP4-ERQ-Out" -Enabled True -Profile
10 Domain,Private,Public
11 # Zeitzone setzen
```

```
11 Set-TimeZone -Id "W. Europe Standard Time"  
12  
13 Restart-Computer
```

AvengerHQ.at beitreten

```
1 Add-Computer -DomainName "AvengerHQ.at" -Credential (Get-Credential) -  
Restart
```

5.1.5. DC3

Grundkonfiguration

```
1 Rename-Computer -NewName "DC3"  
2  
3 # Netzwerkkonfiguration  
4 Get-NetAdapter Ethernet0 | Rename-NetAdapter -NewName "Wakanda"  
5 New-NetIPAddress -InterfaceAlias "Wakanda" -IPAddress "10.10.0.1" -  
PrefixLength 24 -DefaultGateway "10.10.0.254"  
6 Set-DnsClientServerAddress -InterfaceAlias "Wakanda" -ServerAddresses  
("10.10.0.1", "10.10.0.2")  
7  
8 # Zeitzone setzen  
9 Set-TimeZone -Id "W. Europe Standard Time"  
10  
11 Restart-Computer
```

Child Domäne Wakanda.AvengerHQ.at erstellen

```
1 # Features installieren  
2 Install-WindowsFeature -Name "AD-Domain-Services" -IncludeManagementTools  
3 Install-WindowsFeature -Name "DNS" -IncludeManagementTools  
4  
5 # Domäne erstellen  
6 Install-ADDSDomain -DomainType "child" -NewDomainName "wakanda" -  
ParentDomainName "AvengerHQ.at" -Credential (Get-Credential  
"AvengerHQ.at\Administrator") -SafeModeAdministratorPassword (ConvertTo-  
SecureString "Supergeheim123!" -AsPlainText -Force) -InstallDNS -Confirm:  
$true  
7  
8 # DNS zurück ändern  
9 Set-DnsClientServerAddress -InterfaceAlias "Wakanda" -ServerAddresses  
("10.10.0.1", "192.168.50.1")
```

5.1.6. DC4

Grundkonfiguration

```
1 Rename-Computer -NewName "DC4"
2
3 # Netzwerkkonfiguration
4 Get-NetAdapter Ethernet0 | Rename-NetAdapter -NewName "Wakanda"
5 New-NetIPAddress -InterfaceAlias "Wakanda" -IPAddress "10.10.0.2" -
6 PrefixLength 24 -DefaultGateway "10.10.0.254"
7 Set-DnsClientServerAddress -InterfaceAlias "Wakanda" -ServerAddresses
8 ("10.10.0.1")
9 # Zeitzone setzen
10 Set-TimeZone -Id "W. Europe Standard Time"
11 Restart-Computer
```

Wakanda.AvengerHQ.at beitreten

```
1 # Features installieren
2 Install-WindowsFeature -Name "AD-Domain-Services" -IncludeManagementTools
3 Install-WindowsFeature -Name "DNS" -IncludeManagementTools
4
5 # Domäne beitreten
6 Install-ADDSDomainController -DomainName "wakanda.AvengerHQ.at" -Sitetename
7 Default-First-Site-Name -Credential (Get-Credential
8 "wakanda.AvengerHQ.at\Administrator") -SafeModeAdministratorPassword
9 (ConvertTo-SecureString "Supergeheim123!" -AsPlainText -Force) -InstallDNS
-Confirm:$false
10
11 # DNS zurück ändern
12 Set-DnsClientServerAddress -InterfaceAlias "Wakanda" -ServerAddresses
13 ("10.10.0.2", "192.168.50.1")
```

5.1.7. RODC

Grundkonfiguration

```
1 Rename-Computer -NewName "RODC"
2
3 # Netzwerkkonfiguration
4 Get-NetAdapter Ethernet0 | Rename-NetAdapter -NewName "SS"
5 New-NetIPAddress -InterfaceAlias "SS" -IPAddress "192.168.125.1" -
PrefixLength 24 -DefaultGateway "192.168.125.254"
```

```
6 Set-DnsClientServerAddress -InterfaceAlias "SS" -ServerAddresses
7   ("192.168.50.1", "192.168.50.2")
8 # Zeitzone setzen
9 Set-TimeZone -Id "W. Europe Standard Time"
10
11 Restart-Computer
```

RODC hochstufen und AvengerHQ.at beitreten

```
1 # Features installieren
2 Install-WindowsFeature -Name "AD-Domain-Services" -IncludeManagementTools
3 Install-WindowsFeature -Name "DNS" -IncludeManagementTools
4
5 # Domäne beitreten
6 Install-ADDSDomainController -DomainName "AvengerHQ.at" -ReadOnlyReplica:$true -Sitename Default-First-Site-Name -Credential (Get-Credential
7   "AvengerHQ.at\Administrator") -SafeModeAdministratorPassword (ConvertTo-
8   SecureString "Supergeheim123!" -AsPlainText -Force) -InstallDNS -Confirm:$false
9
10 # DNS zurück ändern
11 Set-DnsClientServerAddress -InterfaceAlias "SS" -ServerAddresses
12   ("192.168.125.1", "192.168.50.1")
```

5.2. Active Directory Sites und Services

5.2.1. Standorte

Site-1-AvangerHQ

```
1 New-ADReplicationSite -Name "Site-1-AvangerHQ"
2 New-ADReplicationSubnet -Name "192.168.50.0/24" -Site "Site-1-AvangerHQ"
```

Site-2-Wakanda

```
1 New-ADReplicationSite -Name "Site-2-Wakanda"
2 New-ADReplicationSubnet -Name "10.10.0.0/24" -Site "Site-2-Wakanda"
```

Site-3-SS

```
1 New-ADReplicationSite -Name "Site-3-SS"  
2 New-ADReplicationSubnet -Name "192.168.125.0/24" -Site "Site-3-SS"
```

5.2.2. Site-Links

Site-1-AvangerHQ und Site-2-Wakanda

```
1 New-ADReplicationSiteLink -Name S1-S2 -SitesIncluded Site-1-AvangerHQ,Site-2-Wakanda -Cost 50 -ReplicationFrequencyInMinutes 15
```

Site-2-Wien und Site-3-SS

```
1 New-ADReplicationSiteLink -Name S2-S3 -SitesIncluded Site-2-Wien,Site-3-SS -Cost 100 -ReplicationFrequencyInMinutes 15
```

Site-3-SS und Site-1-HQ

```
1 New-ADReplicationSiteLink -Name S3-S1 -SitesIncluded Site-3-SS,Site-1-HQ -Cost 50 -ReplicationFrequencyInMinutes 15
```

5.2.3. Server in Standorte verschieben

```
1 Move-ADDirectoryServer -Identity "DC1" -Site "Site-1-AvangerHQ"  
2 Move-ADDirectoryServer -Identity "DC2" -Site "Site-1-AvangerHQ"  
3 Move-ADDirectoryServer -Identity "DC3" -Site "Site-2-Wakanda"  
4 Move-ADDirectoryServer -Identity "DC4" -Site "Site-2-Wakanda"  
5 Move-ADDirectoryServer -Identity "RODC" -Site "Site-3-SS"
```

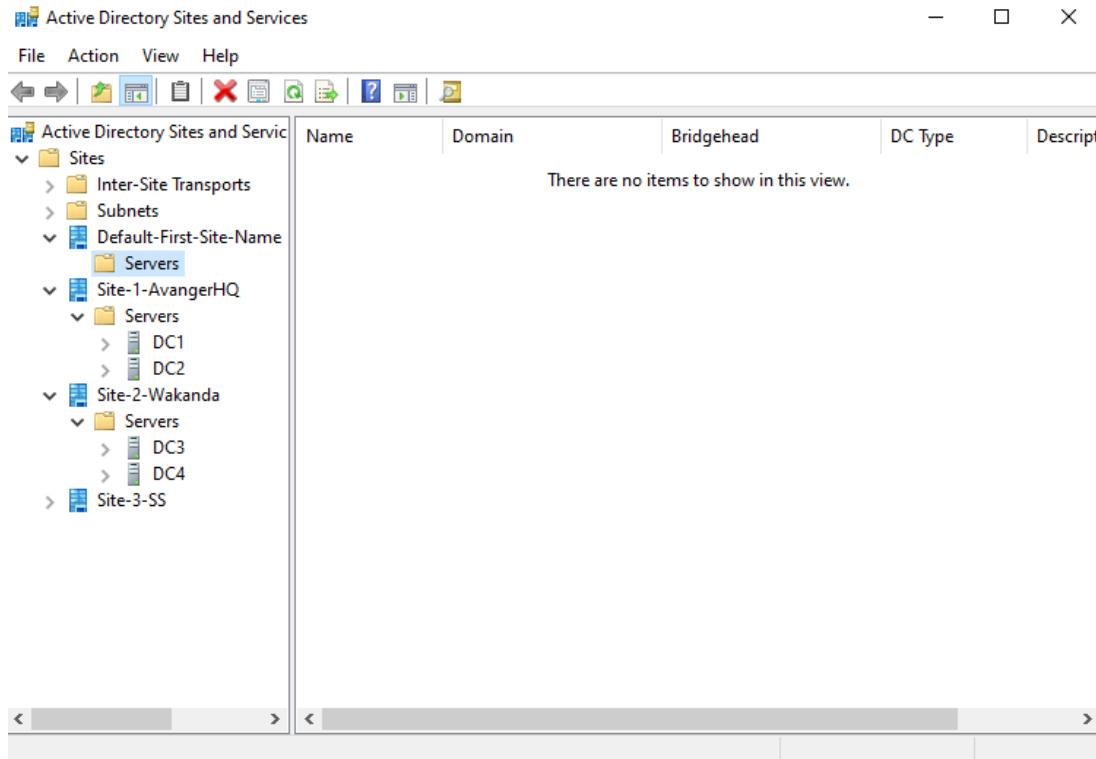


Abbildung 26: Active Directory Sites und Site-Links

5.3. Active Directory Users und Computers

5.3.1. OU Struktur

Die Organizational Unit (OU) Struktur wurde nach dem Business-Unit Modell aufgebaut. Die Struktur ist in vier Abteilungen unterteilt:

- Marketing
- IT
- Sales
- Geschäftsführung

```

1 $domainDN = "DC=AvengerHQ,DC=at"
2
3 # Top-Level OUs
4 $topLevelOUs = @("Marketing", "IT", "Sales", "Geschäftsführung")
5 foreach ($ou in $topLevelOUs) {
6     $ouPath = "OU=$ou,$domainDN"
7     if (-not (Get-ADOrganizationalUnit -Filter { DistinguishedName -eq
$ouPath } -ErrorAction SilentlyContinue)) {

```

```

8 New-ADOrganizationalUnit -Name $ou -Path $domainDN -
9 ProtectedFromAccidentalDeletion $true
10 Write-Output "Created OU: $ou"
11 } else {
12     Write-Output "OU already exists: $ou"
13 }
14
15 # Child OUs for each Top-Level OU
16 $childOUs = @("Users", "Computers", "Resources", "Special")
17 foreach ($parentOU in $topLevelOUs) {
18     foreach ($childOU in $childOUs) {
19         $childPath = "OU=$childOU,OU=$parentOU,$domainDN"
20         if (-not (Get-ADOrganizationalUnit -Filter { DistinguishedName -
21 eq $childPath } -ErrorAction SilentlyContinue)) {
22             New-ADOrganizationalUnit -Name $childOU -Path "OU=$parentOU,
23 $domainDN" -ProtectedFromAccidentalDeletion $true
24             Write-Output "Created OU: $childOU under $parentOU"
25         } else {
26             Write-Output "OU already exists: $childOU under $parentOU"
27         }
28     }
29 }

```

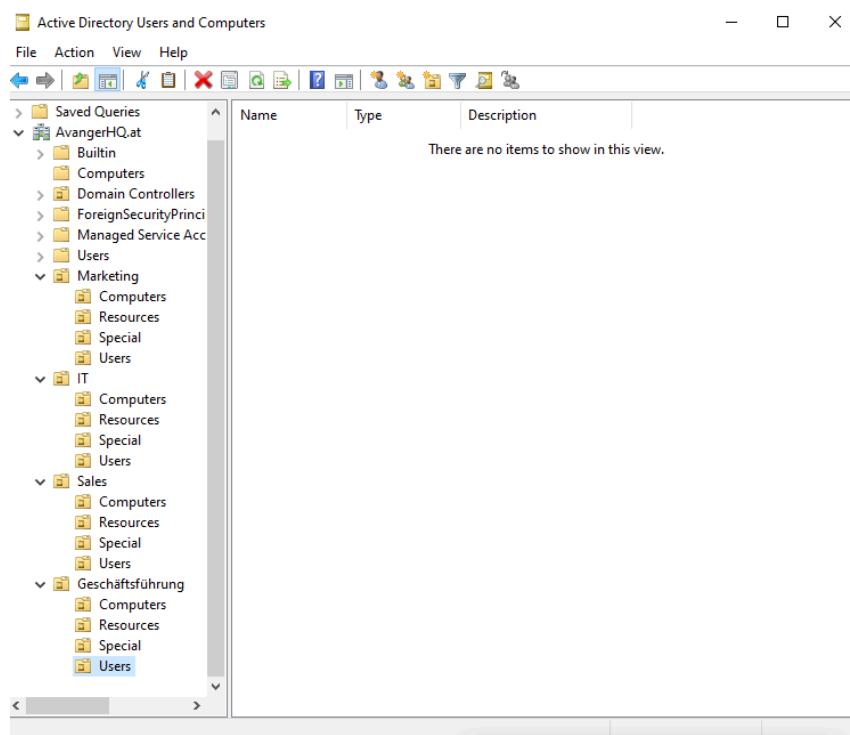


Abbildung 27: Active Directory OU Struktur

5.3.2. User und Gruppen

Für jede Abteilung wurde eine globale Gruppe erstellt:

- G_Marketing
- G_IT
- G_Sales
- G_Geschäftsführung

Darüber hinaus wurde für jede Abteilung realistische Benutzer erstellt:

Name: Laura Becker

- Benutzername: l.becker
- Passwort: „M@rketing2024!“
- Abteilung: Marketing

Name: Anna Bauer

- Benutzername: a.bauer
- Passwort: „A.B2024!“
- Abteilung: Marketing

Name: Lena Schmidt

- Benutzername: l.schmidt
- Passwort: „L.S2024!“
- Abteilung: Marketing

Name: Thomas Meier

- Benutzername: t.meier
- Passwort: „IT@M2024!“
- Abteilung: IT

Name: Sarah Meier

- Benutzername: s.meier
- Passwort: „IT@M2024!“
- Abteilung: IT

Name: David Weber

- Benutzername: d.weber
- Passwort: „IT@W2024!“

- Abteilung: IT

Name: Julia Fischer

- Benutzername: j.fischer
- Passwort: „S@les2024!“
- Abteilung: Sales

Name: Peter Hoffmann

- Benutzername: p.hoffmann
- Passwort: „P.H2024!“
- Abteilung: Sales

Name: Markus Becker

- Benutzername: m.becker
- Passwort: „M.B2024!“
- Abteilung: Sales

Name: Klaus Wagner

- Benutzername: k.wagner
- Passwort: „G@Führung2024!“
- Abteilung: Geschäftsführung

5.4. Distributed File System

Grundkonfiguration

```
1 Rename-Computer -NewName "DFS"
2
3 # Netzwerkkonfiguration
4 Get-NetAdapter Ethernet0 | Rename-NetAdapter -NewName "LAN"
5   New-NetIPAddress -InterfaceAlias "LAN" -IPAddress "192.168.50.4" -
6     PrefixLength 24 -DefaultGateway "192.168.50.254"
7     Set-DnsClientServerAddress -InterfaceAlias "LAN" -ServerAddresses
8       ("192.168.50.1", "192.168.50.2")
9
10 # Zeitzone setzen
11 Set-TimeZone -Id "W. Europe Standard Time"
12
13 Restart-Computer
```

AvengerHQ.at beitreten

```
1 Add-Computer -DomainName "AvengerHQ.at" -Credential (Get-Credential) -
  Restart
```

5.4.1. Konfiguration

Windows -> Search -> Disk Management

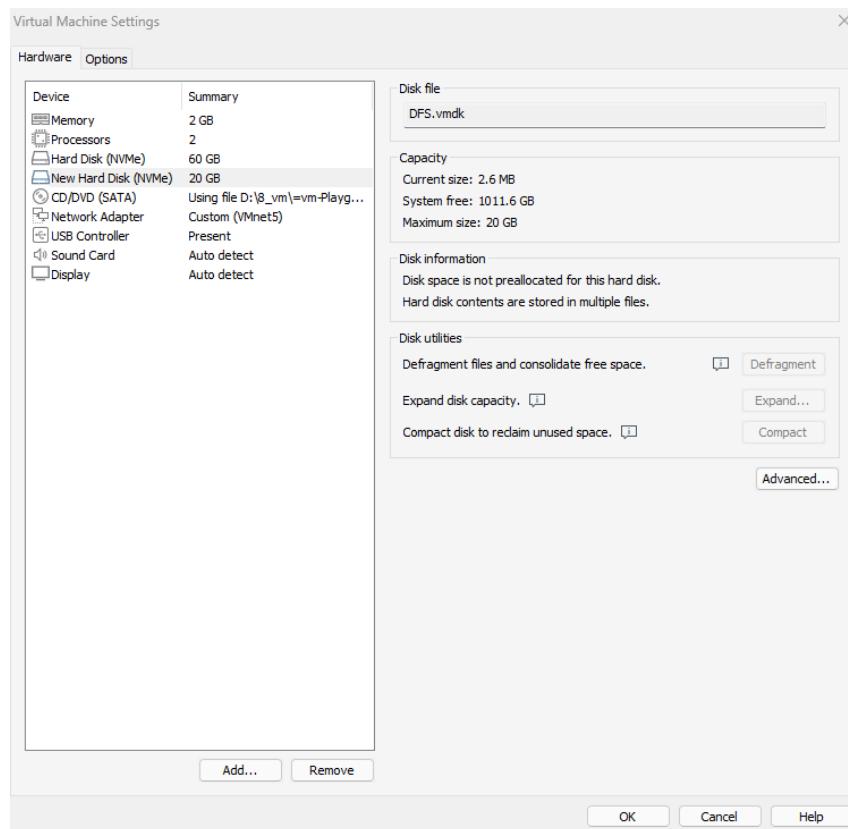


Abbildung 28: Hard Disk erstellen

Windows -> Search -> Disk Management -> Right Click on Disk 1 -> New Simple Volume ->
 Select Letter S: -> Name: Share -> Finish

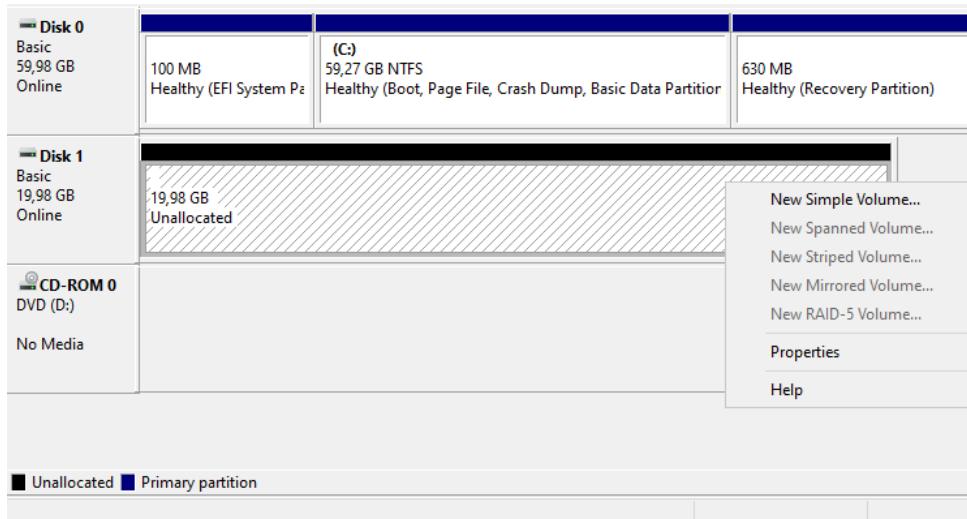


Abbildung 29: Neues Volume erstellen

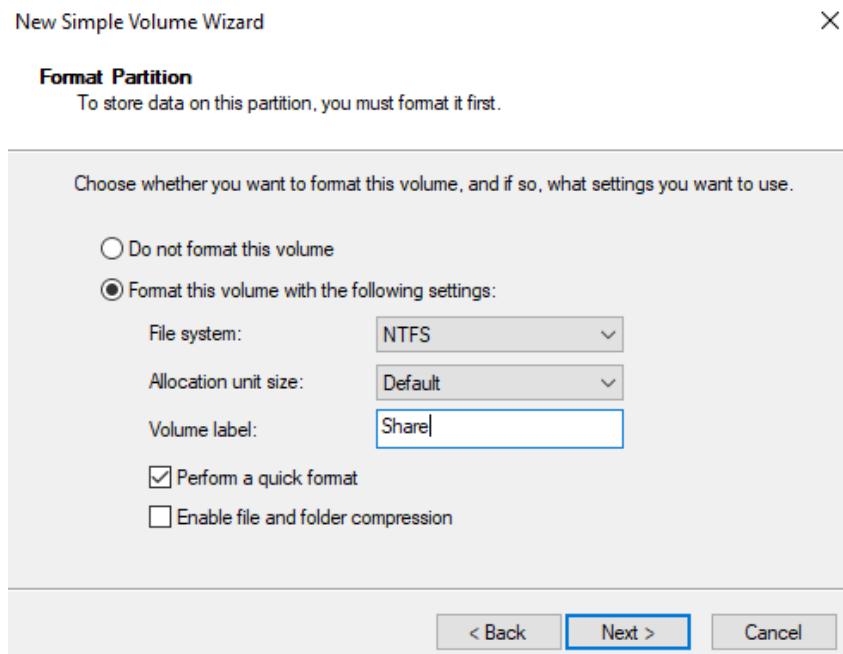


Abbildung 30: Volumen konfigurieren

5.4.2. Ordnerstruktur erstellen

Für jede Abteilung wurde ein Ordner erstellt, zusätzlich auch ein Allgemein Ordner.

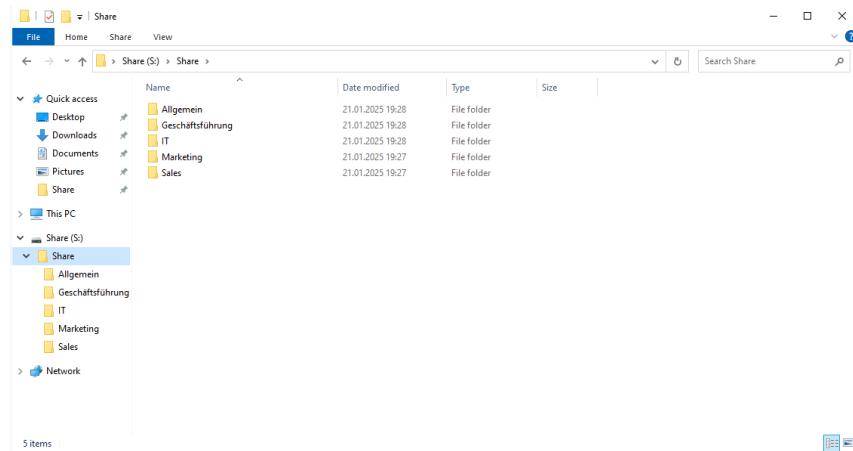


Abbildung 31: Ordnerstruktur erstellen

5.4.3. AGDLP

Das AGDLP (Account, Global, Domain Local, Permission) Konzept schaut wie folgt aus:

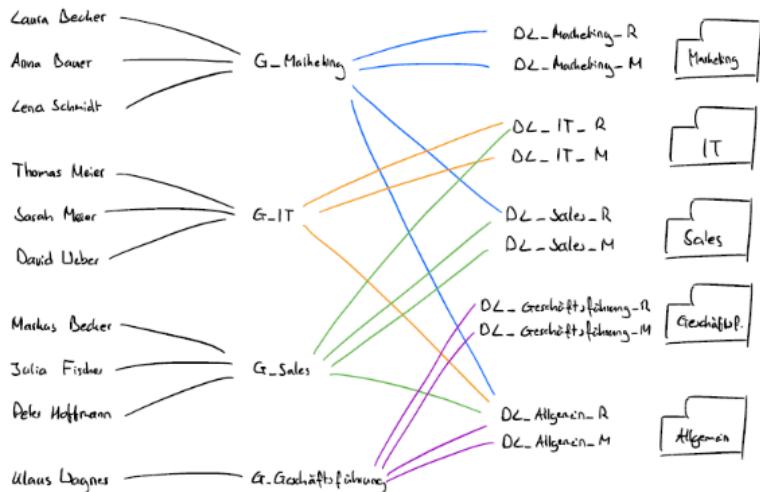


Abbildung 32: AGDLP Konzept

5.4.4. DFS verwalten

Server Manager -> Tools -> DFS Management -> Namespaces -> New Namespace -> Select DFS Server -> Name: DFS -> Next -> Create

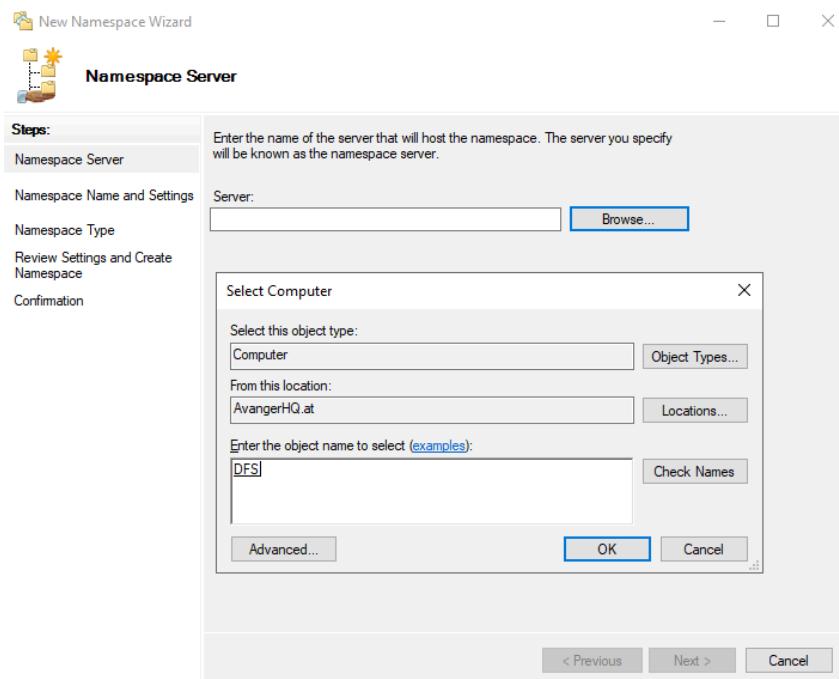


Abbildung 33: DFS Namespace erstellen

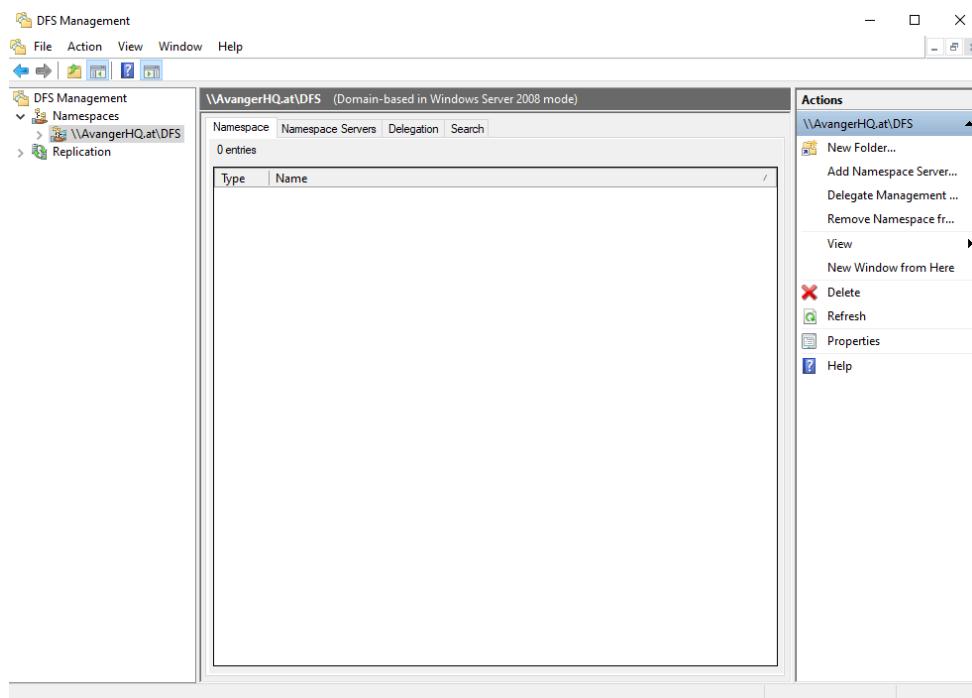


Abbildung 34: DFS Management

New Folder -> zB. Marketing -> Add -> Browse -> Share\Marketing
 Für alle anderen Ordner wiederholen

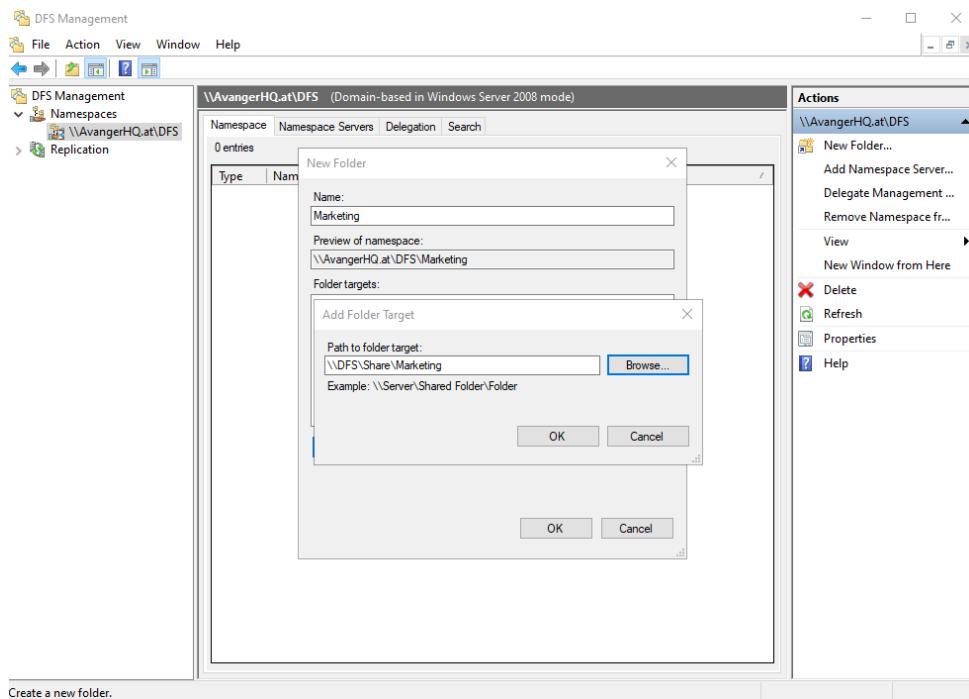


Abbildung 35: DFS Ordner erstellen

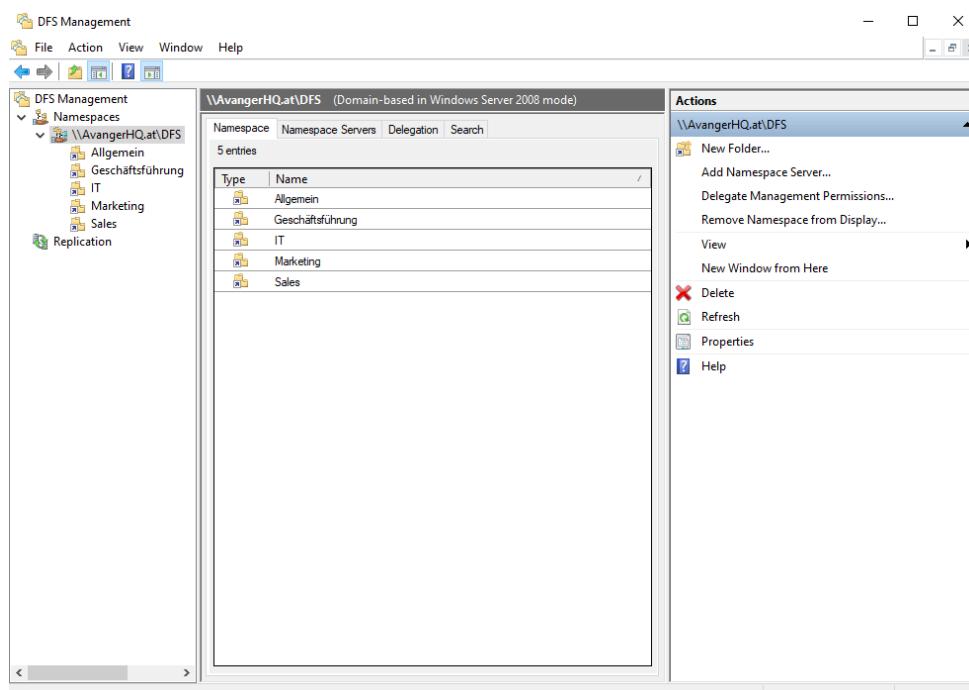


Abbildung 36: DFS Ordnerstruktur

5.4.5. GPO DriveMapPolicy

Group Policy Management -> New -> DriveMapPolicy -> Link to all Users OUs -> Edit und zu folgendem Pfad navigieren: User Configuration\Preferences\Drive Maps\New MappedDrive

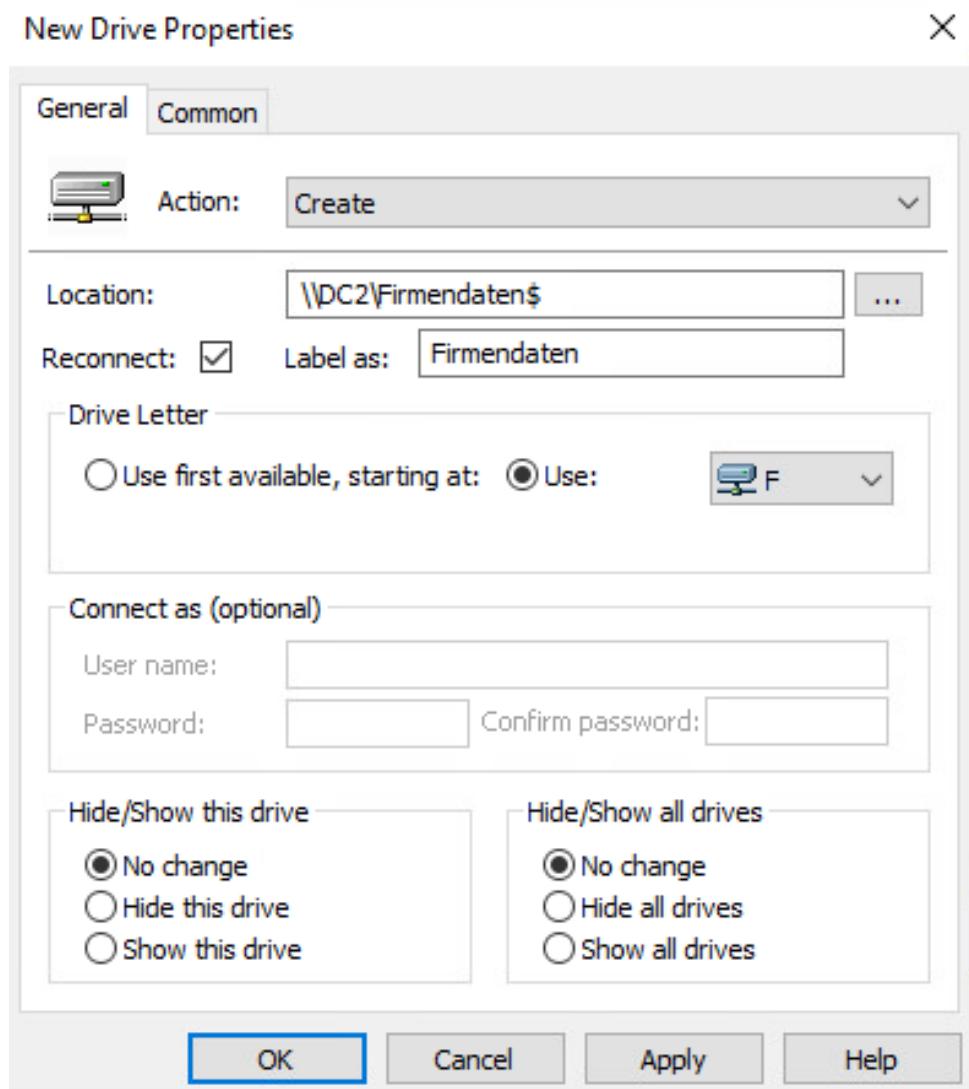


Abbildung 37: GPO DriveMapPolicy

5.4.6. Überprüfung

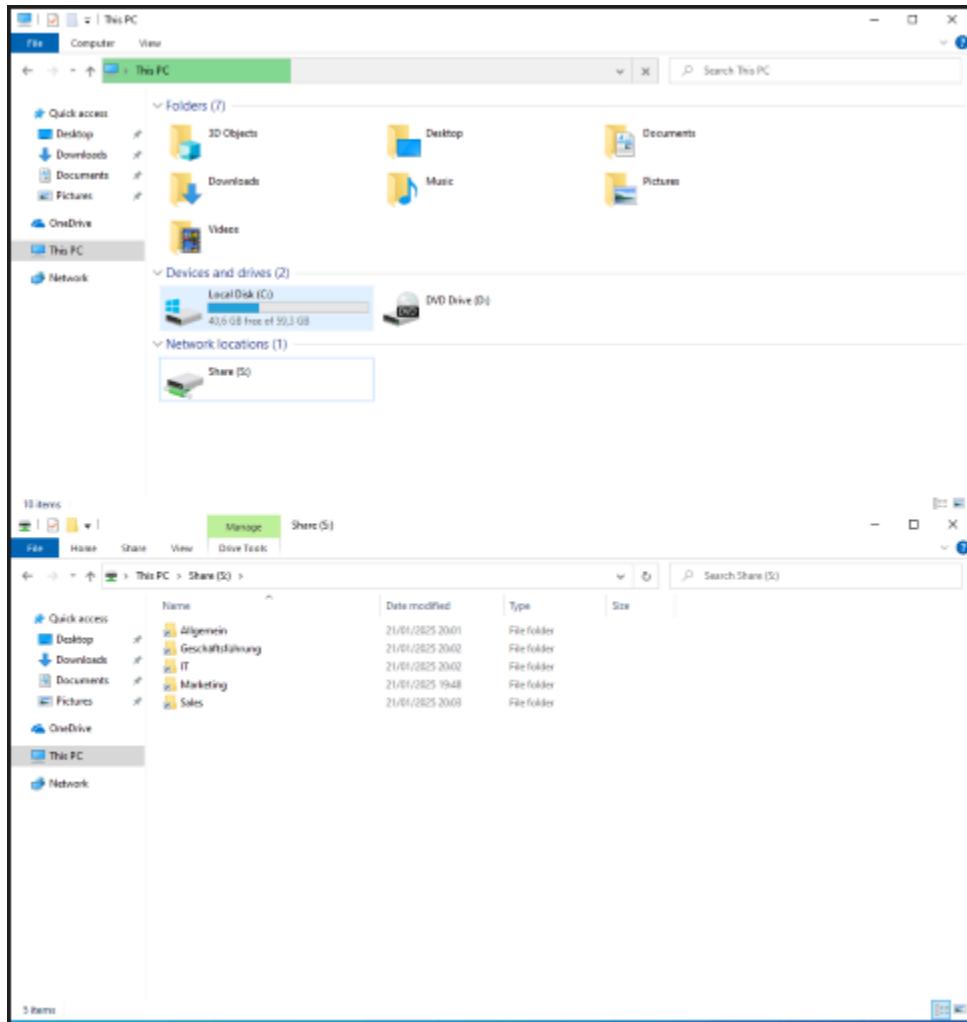


Abbildung 38: GPO Überprüfung

5.5. IIS

Grundkonfiguration

```

1 Rename-Computer -NewName "IIS"
2
3 # Netzwerkkonfiguration
4 Get-NetAdapter Ethernet0 | Rename-NetAdapter -NewName "AvengerHQ"
5 New-NetIPAddress -InterfaceAlias "AvengerHQ" -IPAddress "192.168.50.3" -
6 PrefixLength 24 -DefaultGateway "192.168.50.254"
7 Set-DnsClientServerAddress -InterfaceAlias "AvengerHQ" -ServerAddresses
   ("192.168.50.1", "192.168.50.2")

```

```
8 # Zeitzone setzen
9 Set-TimeZone -Id "W. Europe Standard Time"
10
11 Restart-Computer
```

AvengerHQ.at beitreten

```
1 Add-Computer -DomainName "AvengerHQ.at" -Credential (Get-Credential) -
Restart
```

5.5.1. Web Server IIS Role installieren

login with AvangerHQ\Administrator

```
1 Install-WindowsFeature -Name Web-Server -IncludeManagementTools
```

5.5.2. CertEnroll Folder erstellen und Share

```
1 New-Item -Path C:/CertEnroll -ItemType Directory -Force
2 New-SmbShare -Name CertEnroll -Path C:/CertEnroll -FullAccess
AvengerHQ\Cert Publishers -ChangeAccess "Authenticated Users"
```

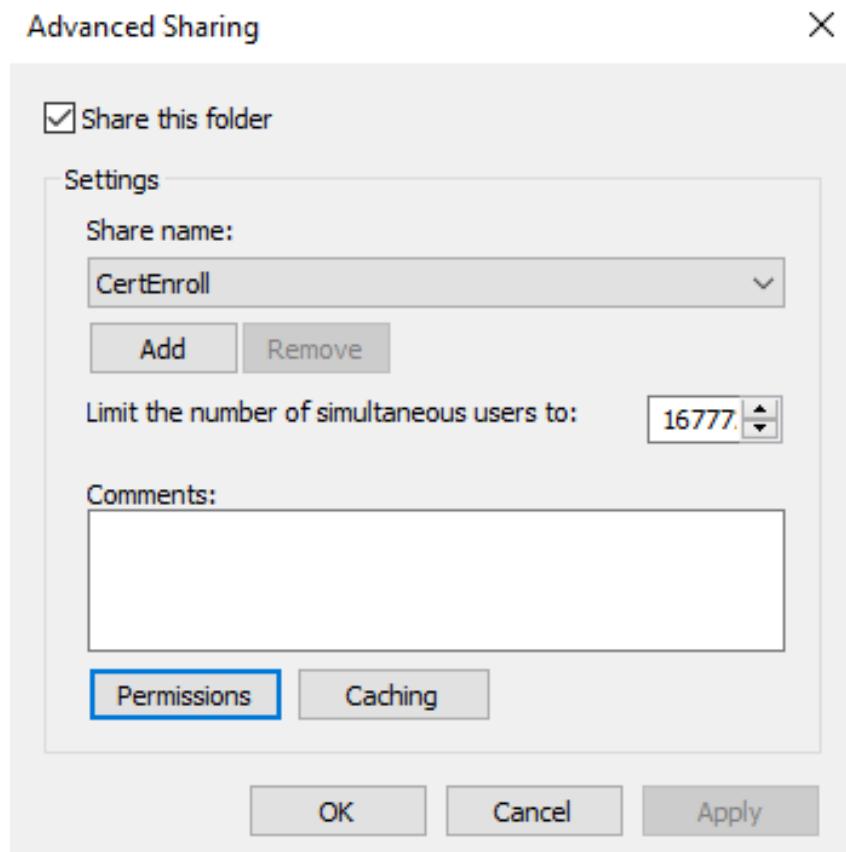


Abbildung 39: CertEnroll Share erstellen

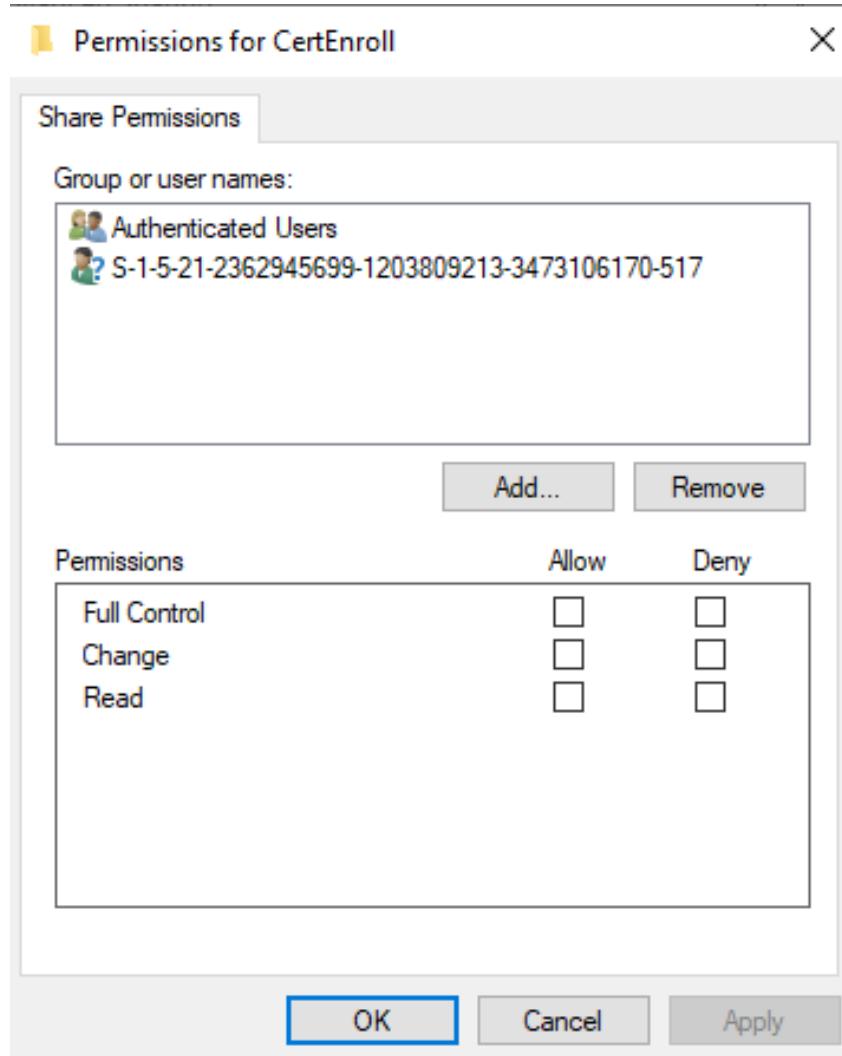


Abbildung 40: CertEnroll Share Berechtigungen

5.5.3. NTFS Berechtigungen festlegen

```
1 icacls "C:\CertEnroll" /inheritance:d
 icacls "C:\CertEnroll" /grant "SYSTEM:F" "CREATER OWNER:F"
2  "Administrators:F" "AvangerHQ\Cert Publishers:M" "Authenticated Users:RX"
```

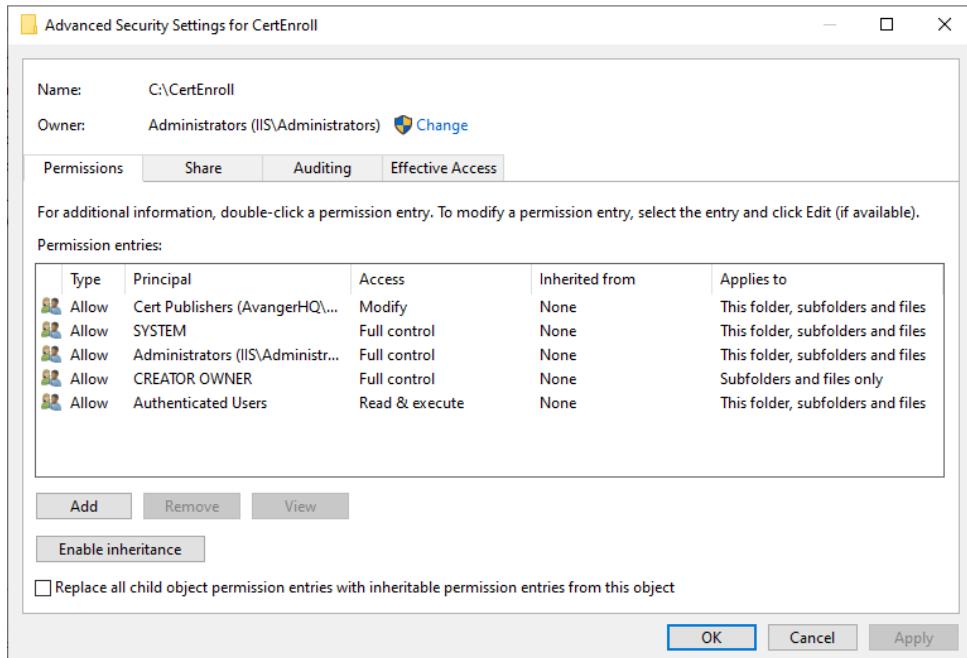


Abbildung 41: CertEnroll NTFS Berechtigungen

5.5.4. CertEnroll Virtual Directory erstellen auf IIS

Server Manager -> Tools -> Internet Information Services (IIS) Manager
 IIS -> Sites -> Default Web Site -> right click -> Add Virtual Directory

```
1 New-WebVirtualDirectory -Site "Default Web Site" -Name "CertEnroll" -  

PhysicalPath "C:\CertEnroll"
```

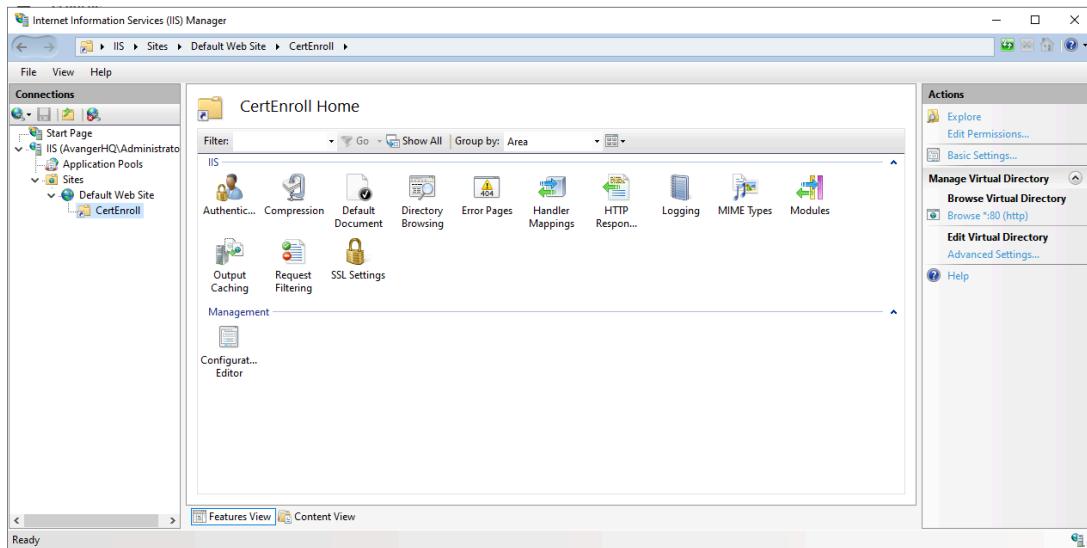


Abbildung 42: CertEnroll IIS Folder

5.5.5. Double Escaping auf IIS Server aktivieren

```

1 cd C:\windows\system32\inetsrv\
2 appcmd set config "Default Web Site" /section:system.webServer/Security/
   requestFiltering -allowDoubleEscaping:True
3 iisreset

```

5.5.6. CNAME erstellen

```

1 Add-DnsServerResourceRecordCName -Name "PKI" -ZoneName "AvengerHQ.at" -
   HostNameAlias "IIS.AvengerHQ.at" -ComputerName "DC1.AvengerHQ"

```

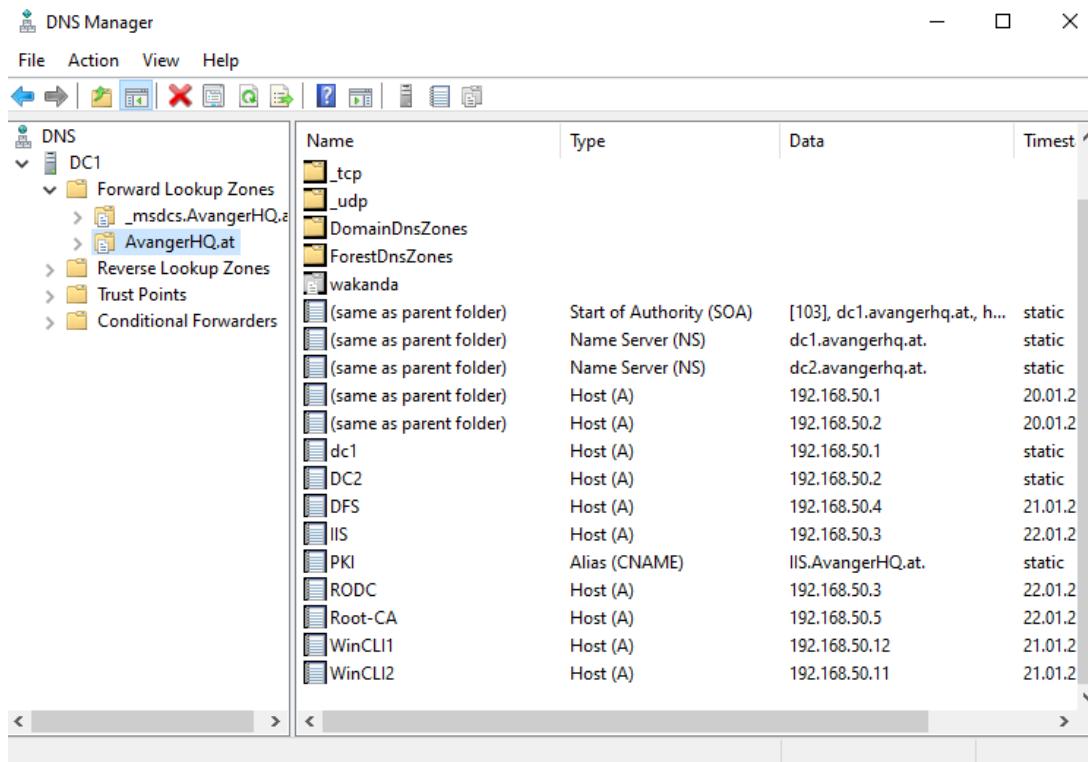


Abbildung 43: CNAME erstellen

5.6. Certificate Authority

Grundkonfiguration

```

1 Rename-Computer -NewName "Root-CA"
2
3 # Netzwerkkonfiguration
4 Get-NetAdapter Ethernet0 | Rename-NetAdapter -NewName "AvengerHQ"
5 New-NetIPAddress -InterfaceAlias "AvengerHQ" -IPAddress "192.168.50.5" -
6 PrefixLength 24 -DefaultGateway "192.168.50.254"
7 Set-DnsClientServerAddress -InterfaceAlias "AvengerHQ" -ServerAddresses
8 ("192.168.50.1", "192.168.50.2")
9
10 # Zeitzone setzen
11 Set-TimeZone -Id "W. Europe Standard Time"
12
13 Restart-Computer

```

AvengerHQ.at beitreten

```
1 Add-Computer -DomainName "AvengerHQ.at" -Credential (Get-Credential) -  
1 Restart
```

5.6.1. CAPolicy.inf erstellen

Start -> Run -> notepad C:\Windows\CAPolicy.inf (Create New File)

```
1 [Version]  
2 Signature="$Windows NT$"  
3  
4 [PolicyStatementExtension]  
5 Policies=InternalPolicy  
6  
7 [InternalPolicy]  
8 OID= 1.2.3.4.1455.67.89.5  
9 Notice="Legal Policy Statement"  
10 URL=http://Root-CA.AvengerHQ.at/cps.txt  
11  
12 [CertSrv_Server]  
13 RenewalKeyLength=2048  
14 RenewalValidityPeriod=Years  
15 RenewalValidityPeriodUnits=10  
16 LoadDefaultTemplates=0  
17 AlternateSignatureAlgorithm=1
```

5.6.2. Post Installation Timer Konfiguration

```
1 # Best Practice "Timer" Configuration  
2 Certutil -setreg CA\CRLPeriodUnits 2  
3 Certutil -setreg CA\CRLPeriod "Weeks"  
4 Certutil -setreg CA\CRLDeltaPeriodUnits 1  
5 Certutil -setreg CA\CRLDeltaPeriod "Days"  
6  
7 Certutil -setreg CA\CRLOverlapPeriodUnits 12  
8 Certutil -setreg CA\CRLOverlapPeriod "Hours"  
9  
10 Certutil -setreg CA\ValidityPeriodUnits 10  
11 Certutil -setreg CA\ValidityPeriod "Years"  
12  
13 Certutil -setreg CA\AuditFilter 127
```

5.6.3. AIA konfigurieren

AIA (Authority Information Access)

Gibt an, wo Informationen über die ausstellende CA oder den Zertifikatsstatus (z. B. über OCSP) gefunden werden können.

```
1 certutil -setreg CA\CACertPublicationURLs "1:C:  
  \Windows\system32\CertSrv\CertEnroll\%1_%3%4.crt\n2:ldap:///  
  CN=%7,CN=AIA,CN=Public Key Services,CN=Services,%6%11\n2:http://pki.  
  AvengerHQ.at/CertEnroll/%1_%3%4.crt"  
2 certutil -getreg CA\CACertPublicationURLs
```

5.6.4. CDP konfigurieren

CDP (CRL Distribution Point) Zeigt, wo die Zertifikatsperrliste (CRL) abgerufen werden kann, um widerrufene Zertifikate zu prüfen.

```
1 certutil -setreg CA\CRLOperationURLs "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.AvengerHQ.at/CertEnroll/%3%8%9.crl\n65:file:///\br/>  \IIS.AvengerHQ.at\CertEnroll\%3%8%9.crl"  
2 certutil -getreg CA\CRLOperationURLs
```

5.6.5. CA Certificate AIA veröffentlichen

```
1 cd c:\windows\system32\certsrv\certenroll  
2 copy "Root-CA.AvengerHQ.at_AvengerHQ-Root-CA.crt" \\IIS.AvengerHQ.at\C$  
  \CertEnroll  
3 net stop certsvc && net start certsvc
```

5.6.6. CA Certificate CDP veröffentlichen

Server Manager -> Tools -> Certificate Authority -> AvengerHQ-Root-Ca -> Revoked Certificates -> All Tasks -> Publish

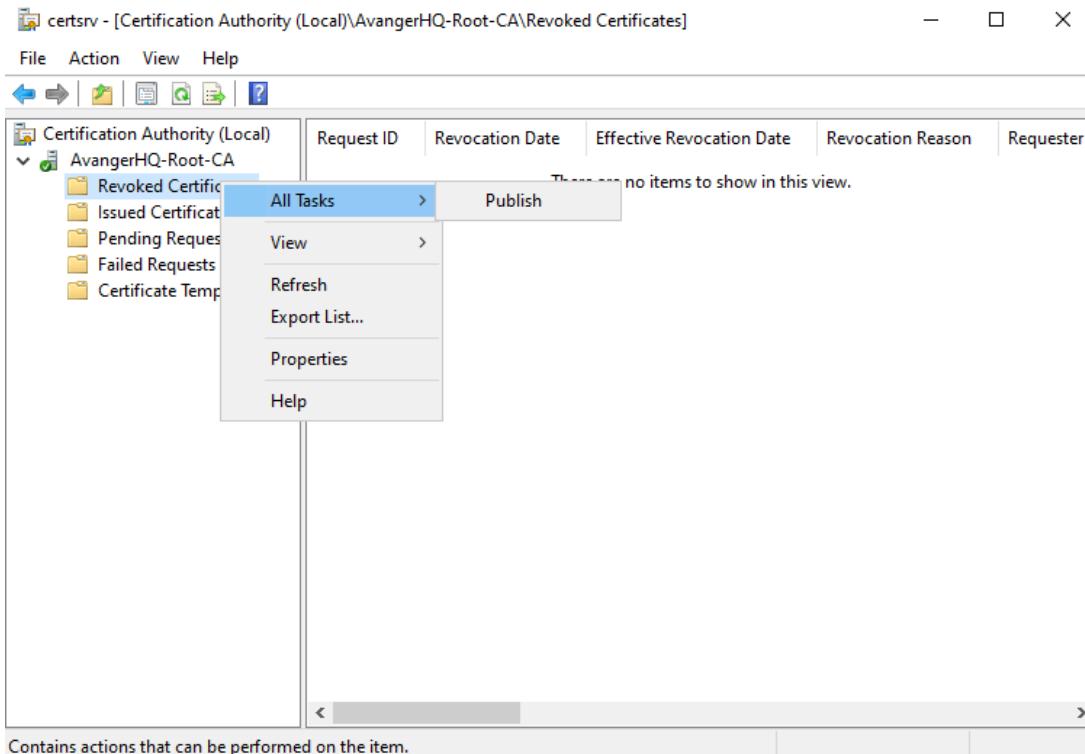


Abbildung 44: Root Zertifikat veröffentlichen

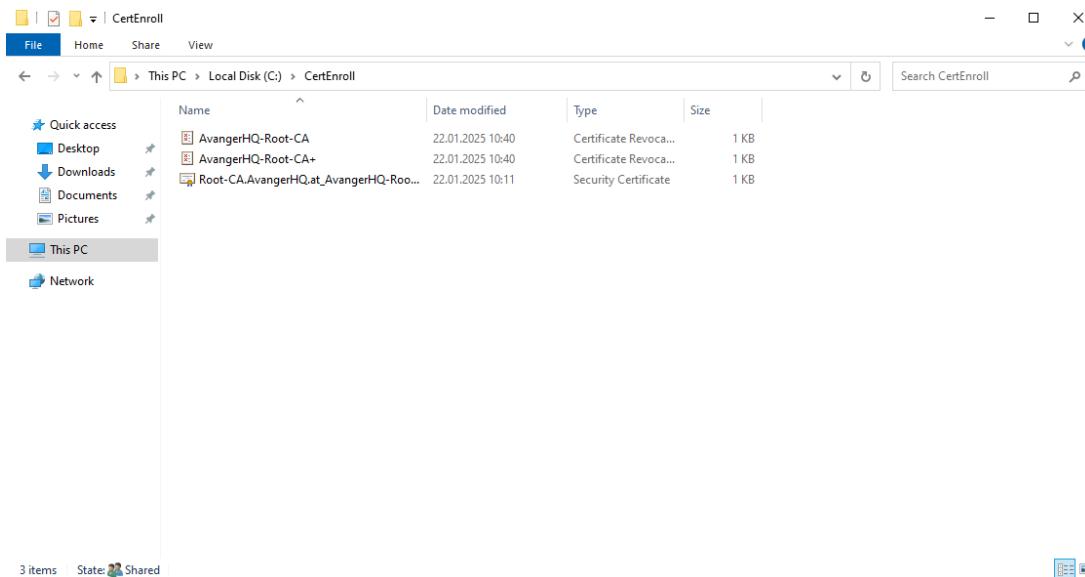


Abbildung 45: Root Zertifikat überprüfen

5.6.7. Web Server Security Group

Server Manager -> Tools -> Active Directory -Users and -Computers -> Users -> New -> Group

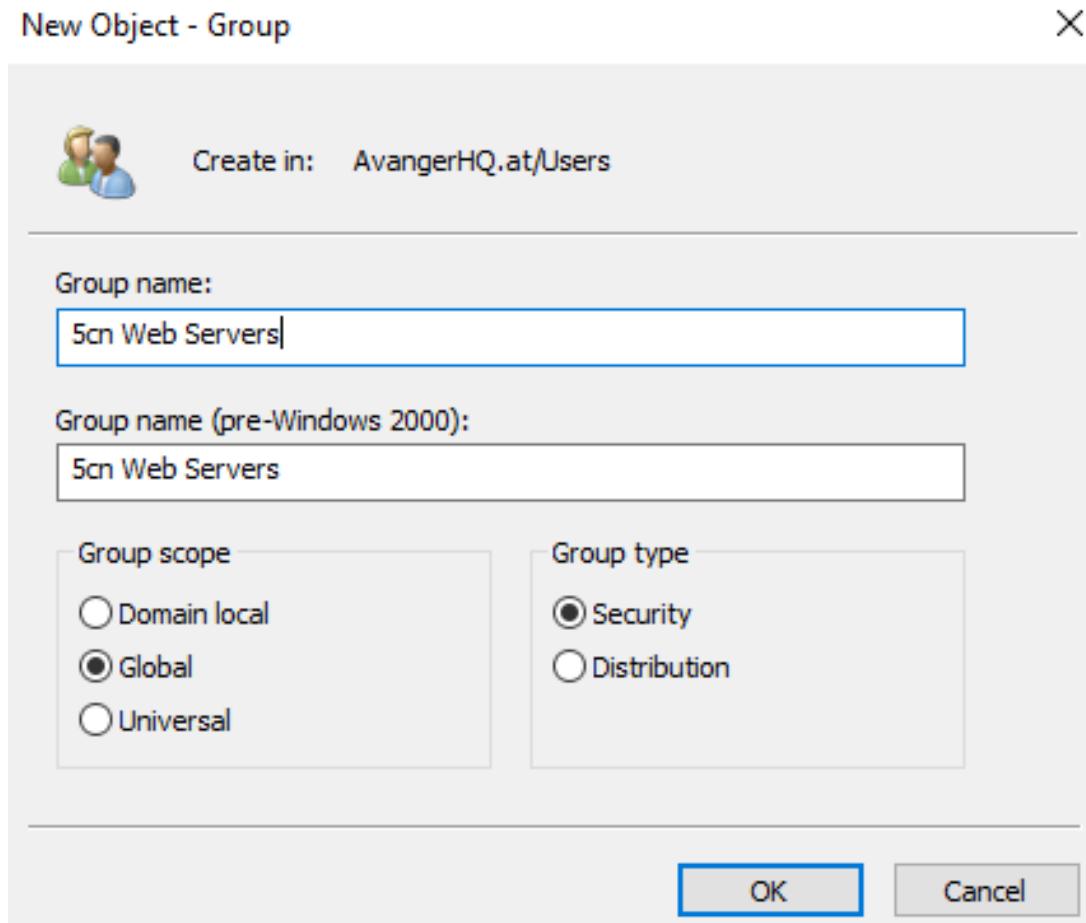


Abbildung 46: Security Group Web Server erstellen

IIS Webserver der Gruppe hinzufügen

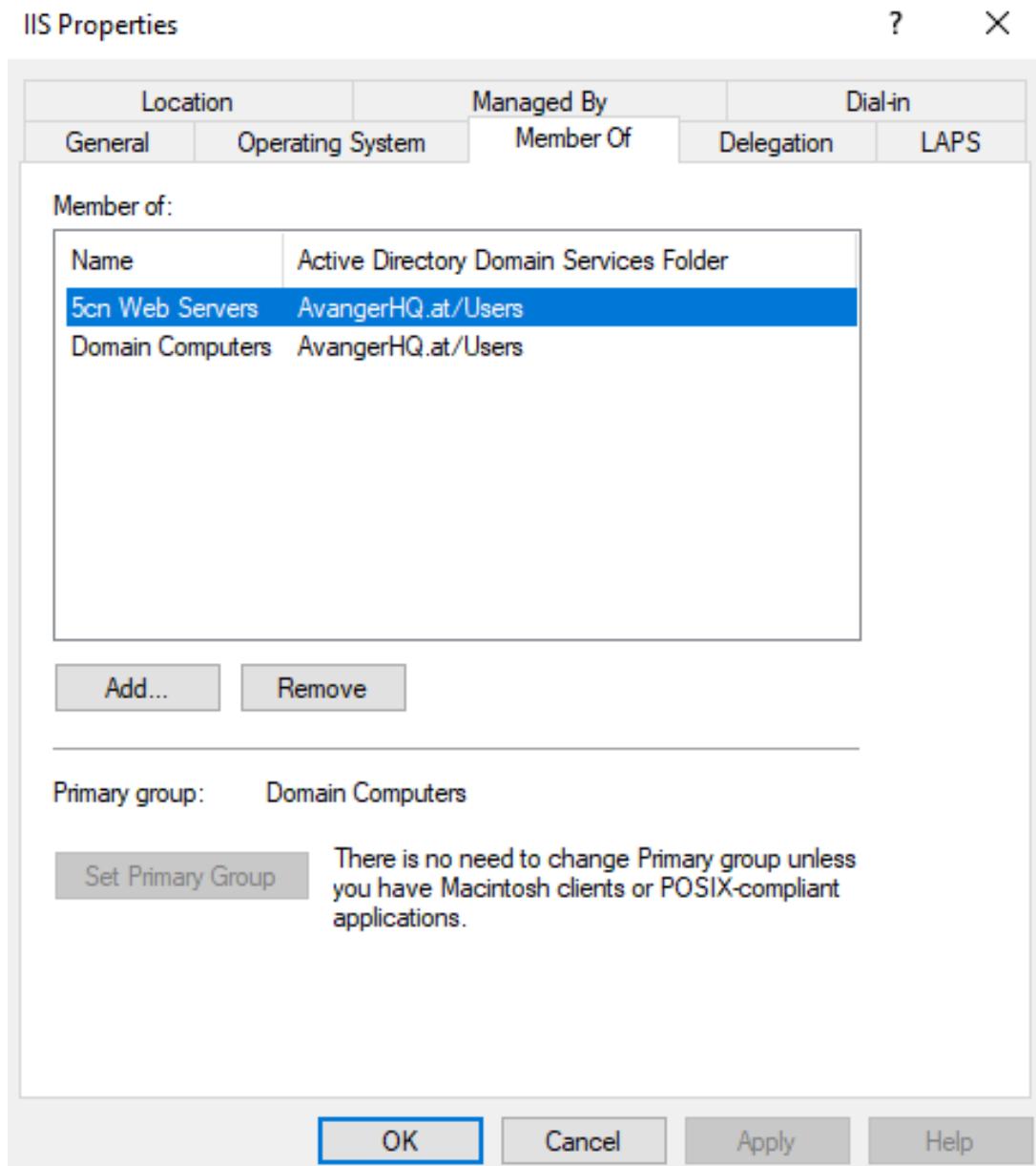


Abbildung 47: IIS Webserver der Gruppe hinzufügen

5.6.8. Webserver Certificate Template erstellen

Server Manager -> Tools -> Certificate Authority -> 5cn Root CA -> Certificate Templates -> Manage -> Web Server -> Duplicate Template

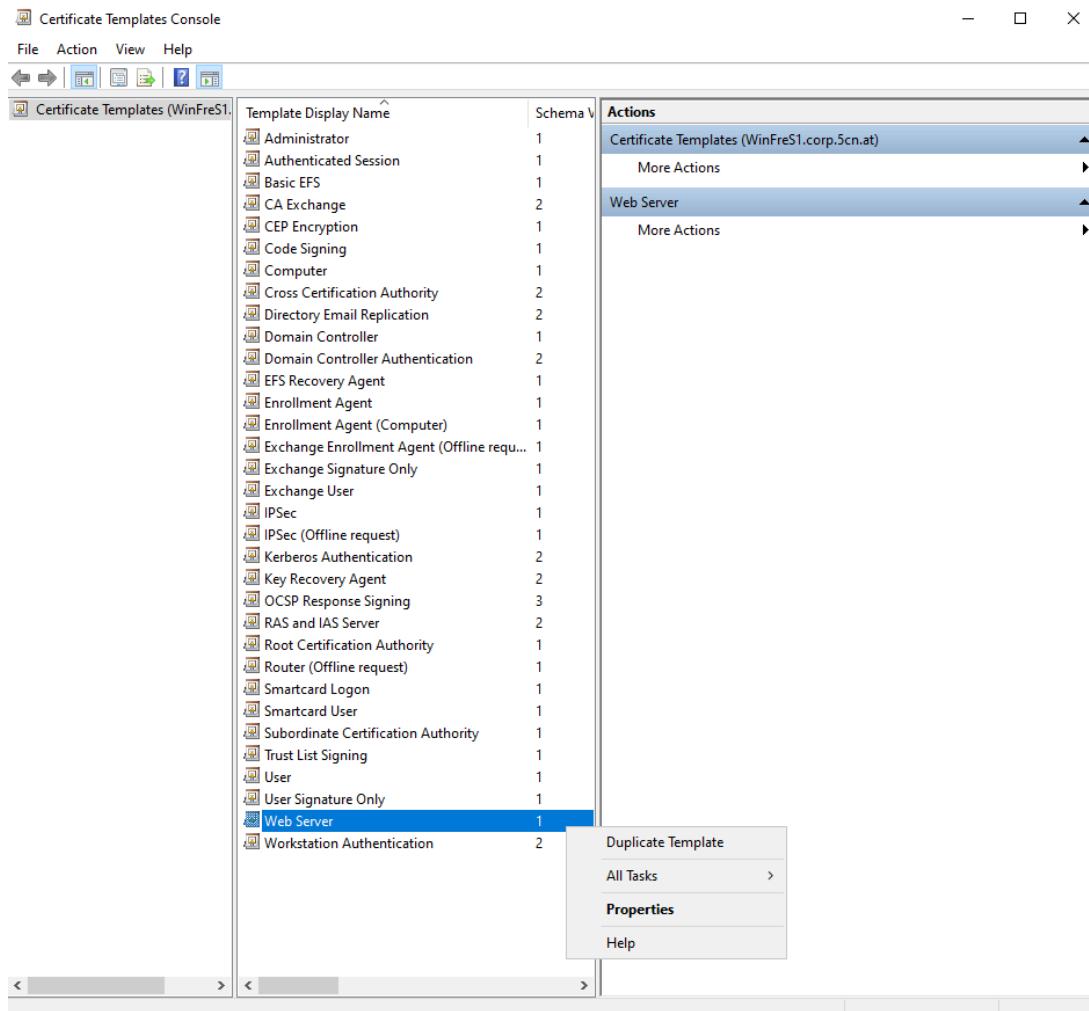


Abbildung 48: Webserver Certificate Template erstellen

Folgende Properties anpassen:

- Template Display Name: 5cn Web Server
- Subject Name: DNS name
- Security: Web Server Group hinzufügen
 - Permissions: Read & Enroll

5.6.9. CA für Zertifikatsausstellung konfigurieren

Certificate Templates -> New -> Certificate Template to Issue -> 5cn Web Server

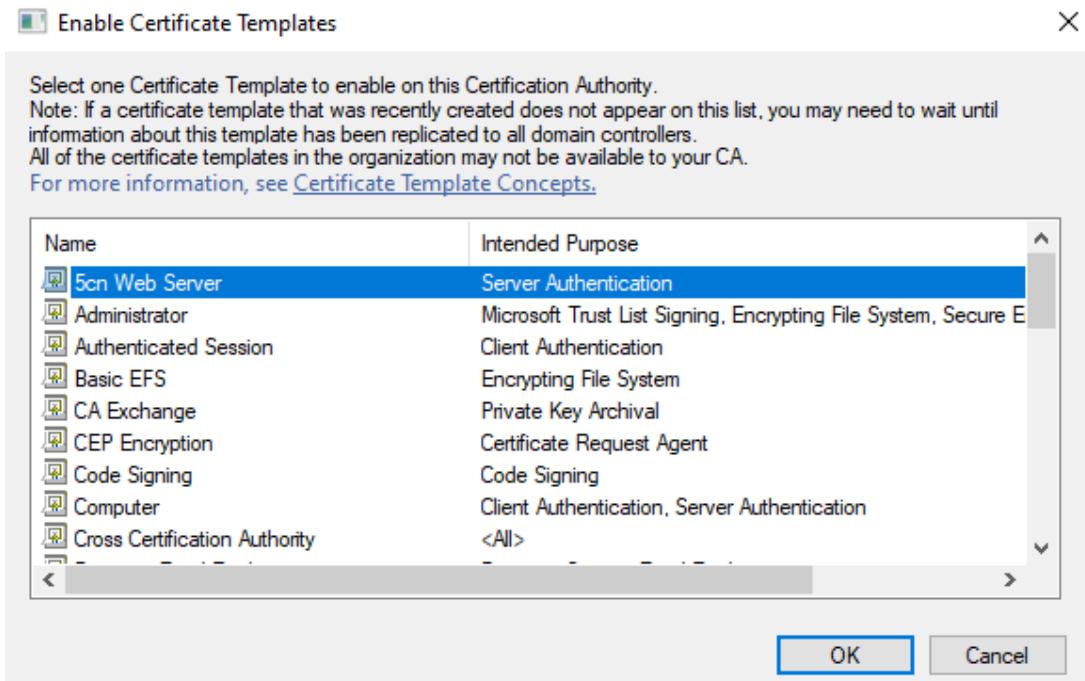


Abbildung 49: Certificate Template ausstellen

5.6.10. Request SSL Certificate

Open MMC -> File -> Add/Remove Snap-in -> Certificates -> Computer account -> Finish -> Ok

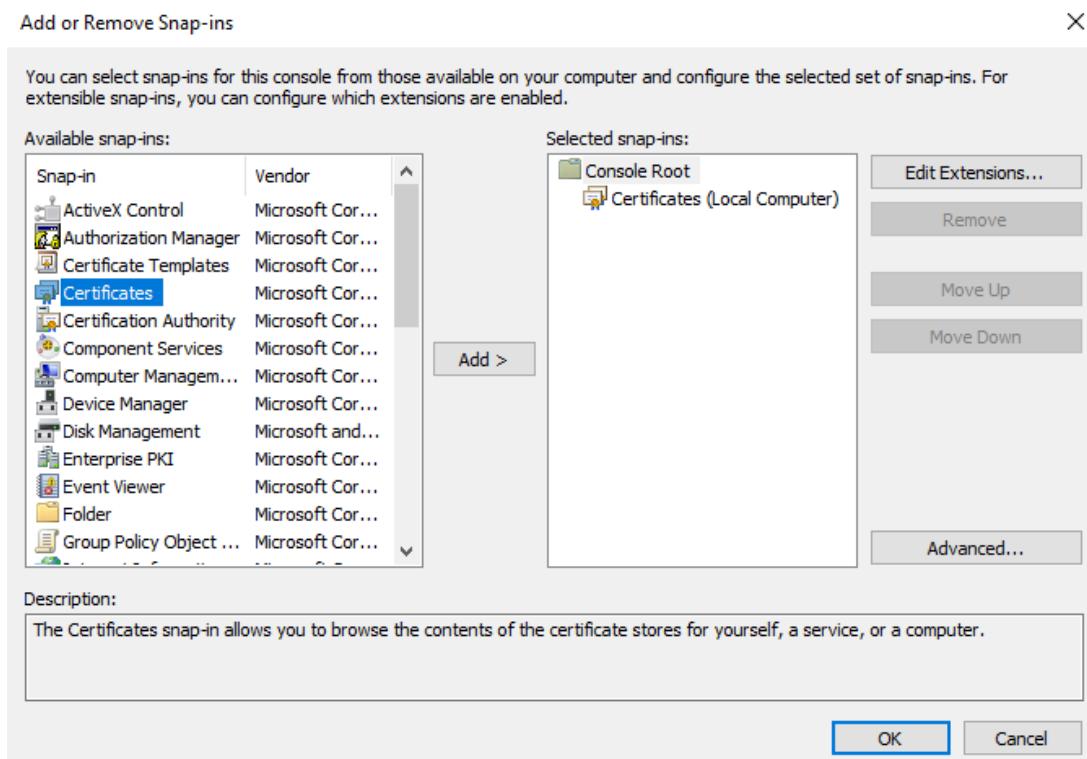


Abbildung 50: MMC Certificate Snap-in

Certificates (Local Computer) > Personal -> All Tasks -> Request New Certificate -> Next -> Next -> Select 5cn Web Server Template -> Enroll -> Finish

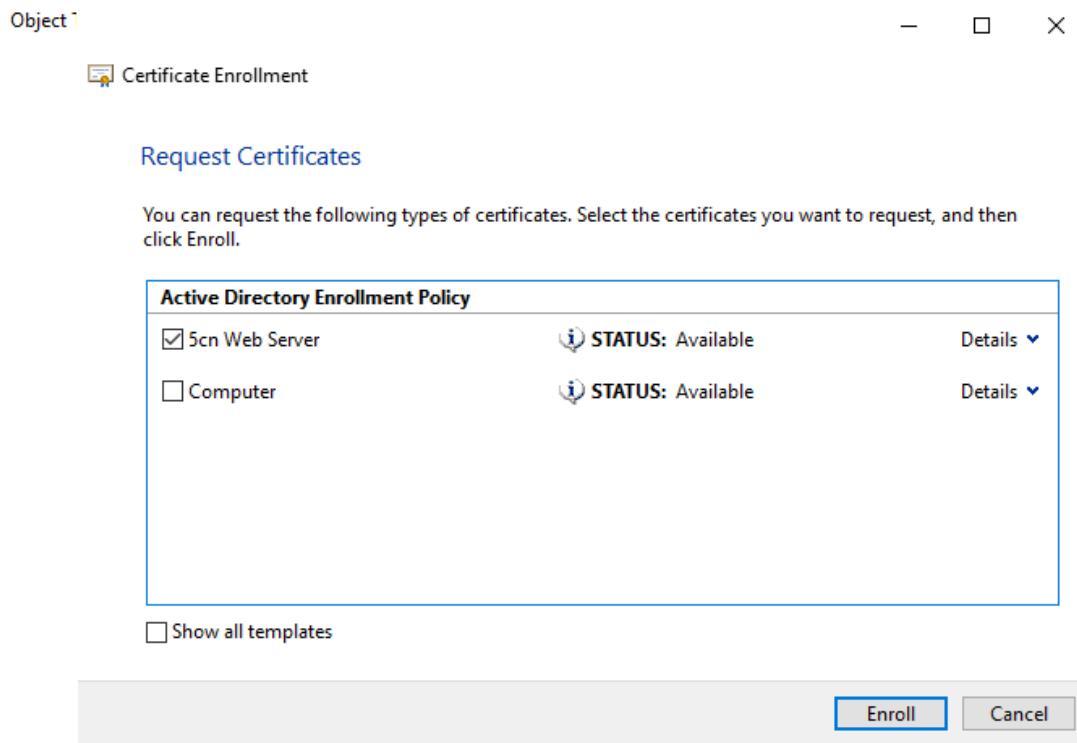


Abbildung 51: Web Server Certificate auswählen

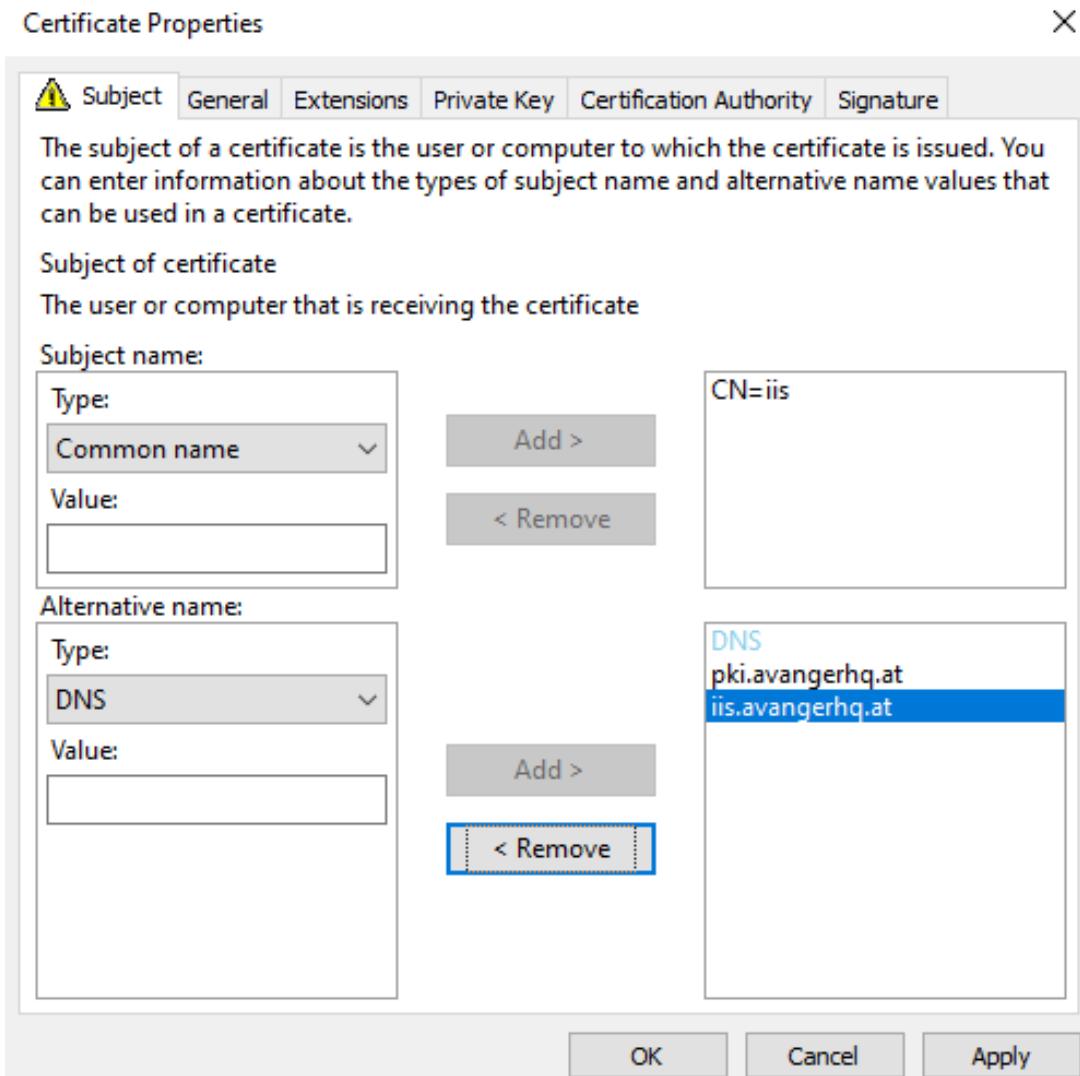


Abbildung 52: Web Server Certificate Properties festlegen

5.6.11. Enable SSL

Server Manager -> Tools -> Internet Information Service (IIS) Manager -> WinFres4 -> Sites -> Default Web Site -> Edit Bindings -> Add-Computer

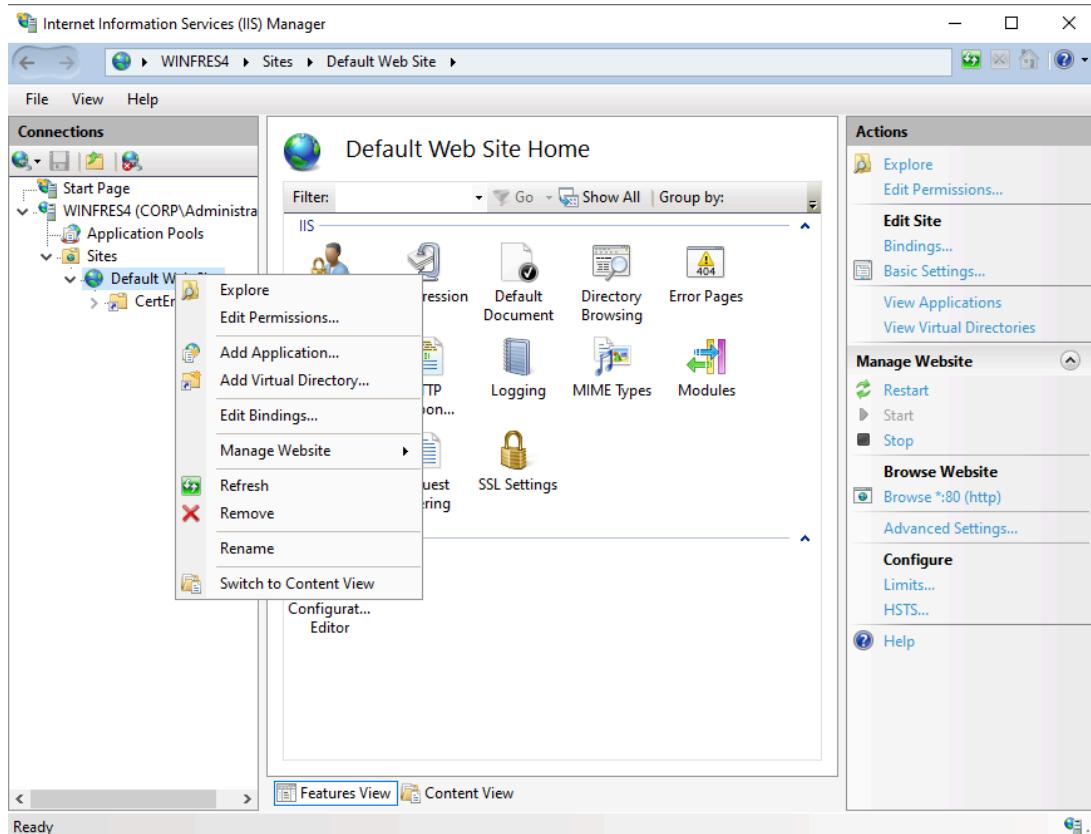


Abbildung 53: IIS Manager SSL aktivieren

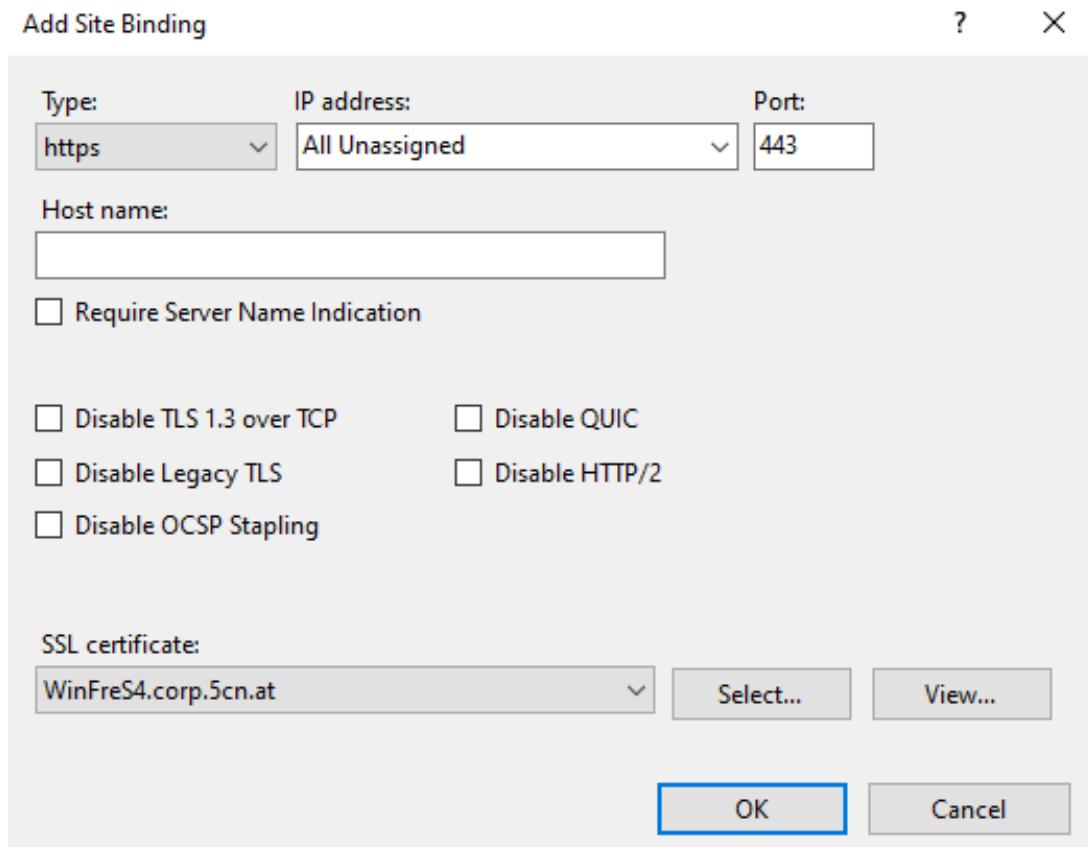


Abbildung 54: IIS Manager SSL aktivieren

5.6.12. Web Server Certificate Test

Internet Explorer -> <https://iis.avengerHQ.at> oder <https://pki.avengerHQ.at>

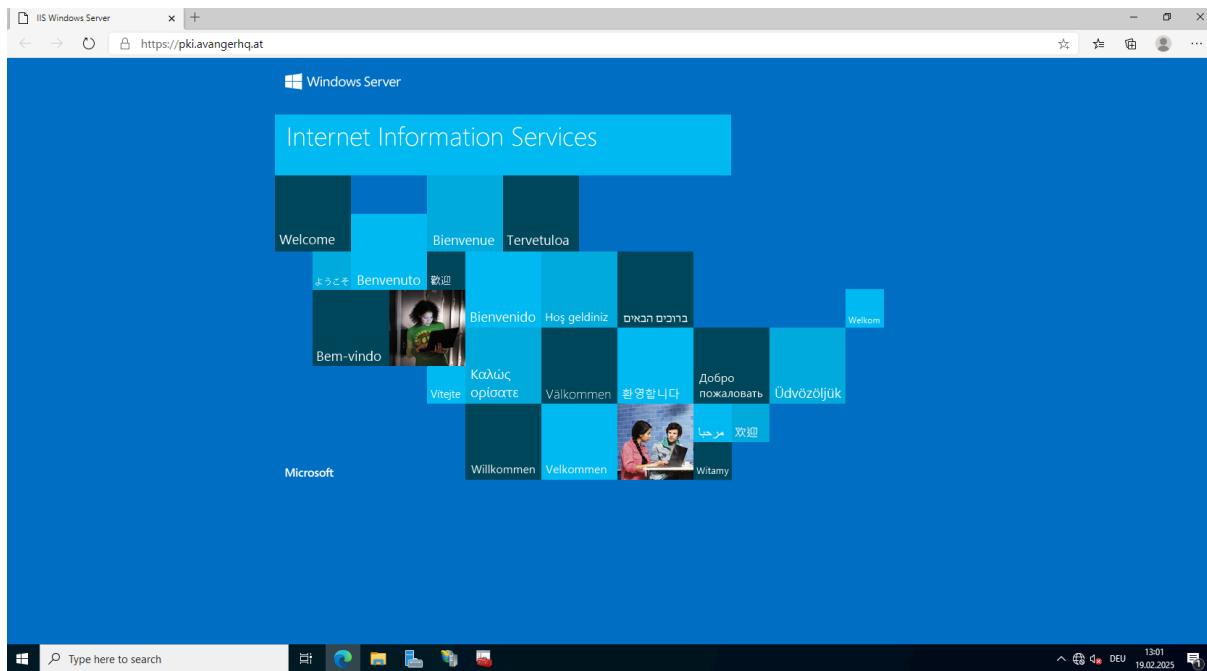


Abbildung 55: Web Server Certificate Test

5.7. Hardening

5.7.1. GPOs

5.7.1.1. GPO Desktop Hintergrund

Fileserver Ablageort

Durch den Fileserver ist es möglich ein Hintergrundbild für alle Clients zu speichern. Dazu wurde unter dem Ordner Share und Allgemein ein Hintergrundbild gespeichert.

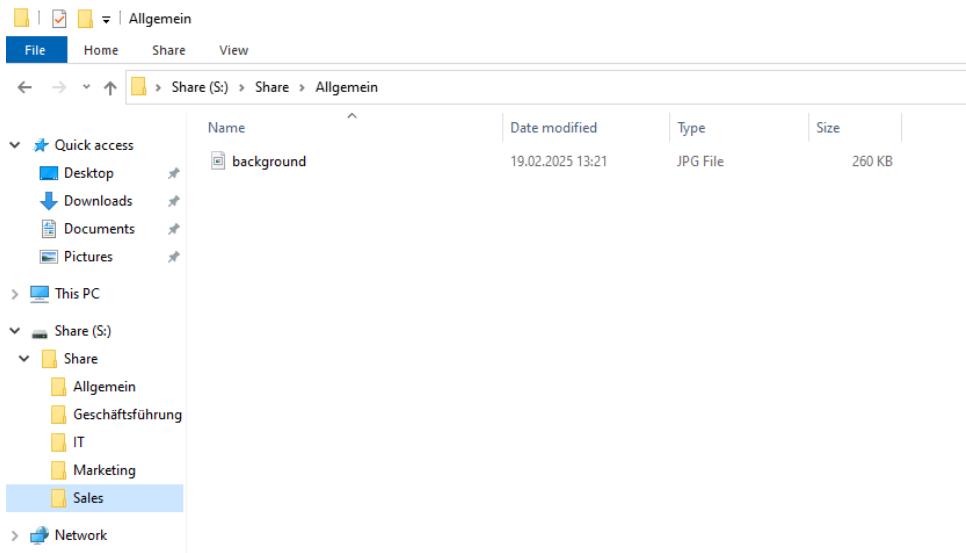


Abbildung 56: Fileserver Desktop Wallpaper

GPO erstellen

Auf dem Domänen Controller wird im Server Manager unter Tools die Gruppenrichtlinienverwaltung geöffnet. Dort wird eine neue Gruppenrichtlinie erstellt und konfiguriert.

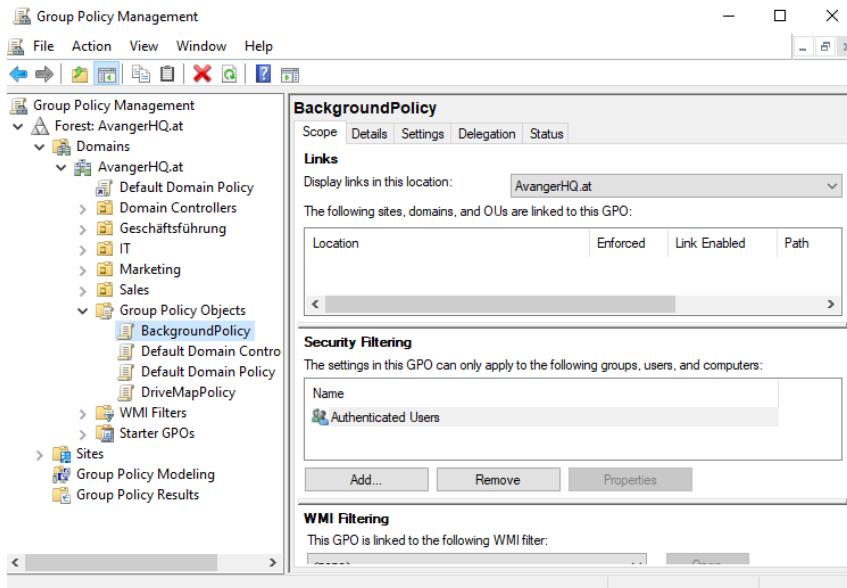


Abbildung 57: Desktop Wallpaper GPO erstellen

GPO bearbeiten

In der Gruppenrichtlinienverwaltung kann dann unter folgendem Pfad die Gruppenrichtlinie

konfiguriert werden:

User Configuration -> Policies -> Administrative Templates -> Desktop -> Desktop Wallpaper

Dort kann dann die Option enabled und der Pfad zum Hintergrundbild angegeben werden.

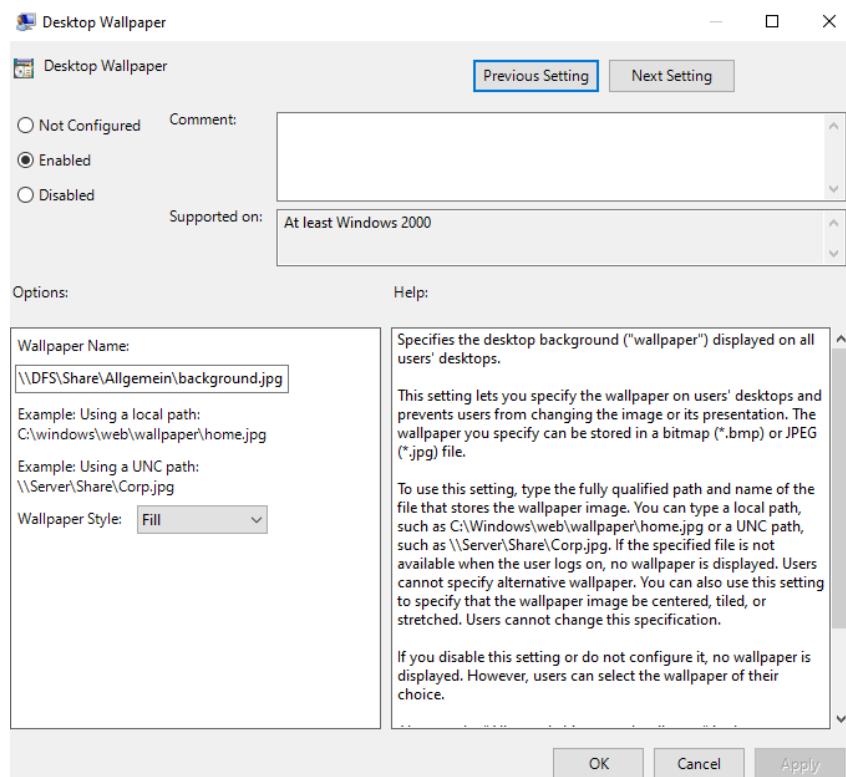


Abbildung 58: Desktop Wallpaper GPO konfigurieren

Überprüfung

Wenn sich jetzt ein Benutzer ab- und anmeldet erscheint der neue Hintergrund wie in folgendem Bild zu sehen:



Abbildung 59: Desktop Wallpaper GPO test

5.7.1.2. GPO Lock/Logon Screen

GPO erstellen

Auf dem Domänen Controller wird im Server Manager unter Tools die Gruppenrichtlinienverwaltung geöffnet. Dort wird eine neue Gruppenrichtlinie erstellt und konfiguriert.

GPO bearbeiten

In der Gruppenrichtlinienverwaltung kann dann unter folgendem Pfad die Gruppenrichtlinie konfiguriert werden:

Computer Configuration -> Policies -> Administrative Templates -> Control Panel -> Personalization -> Force a specific default lock screen and logon image

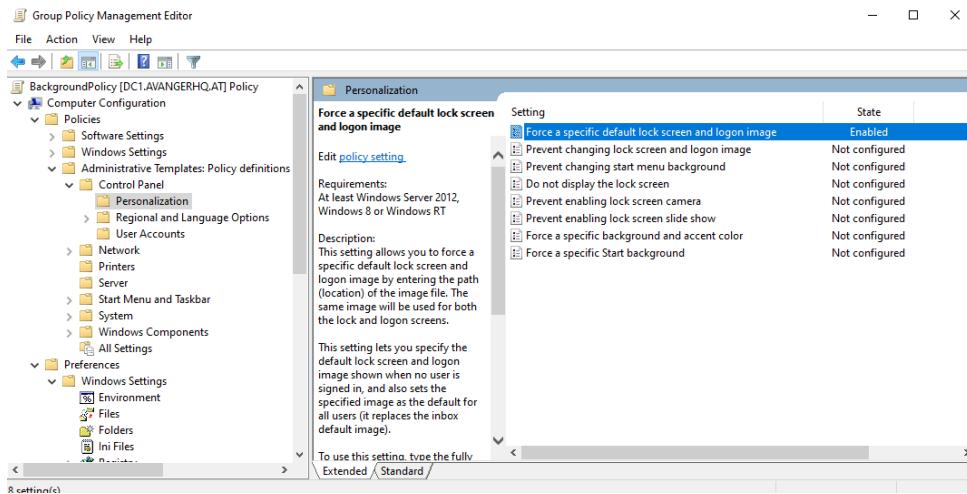


Abbildung 60: Lock/Logon Screen GPO Pfad

Dort kann dann die Option enabled und der Pfad zum Hintergrundbild angegeben werden. In diesem Beispiel wird ein bereits vorhandenes Bild verwendet.

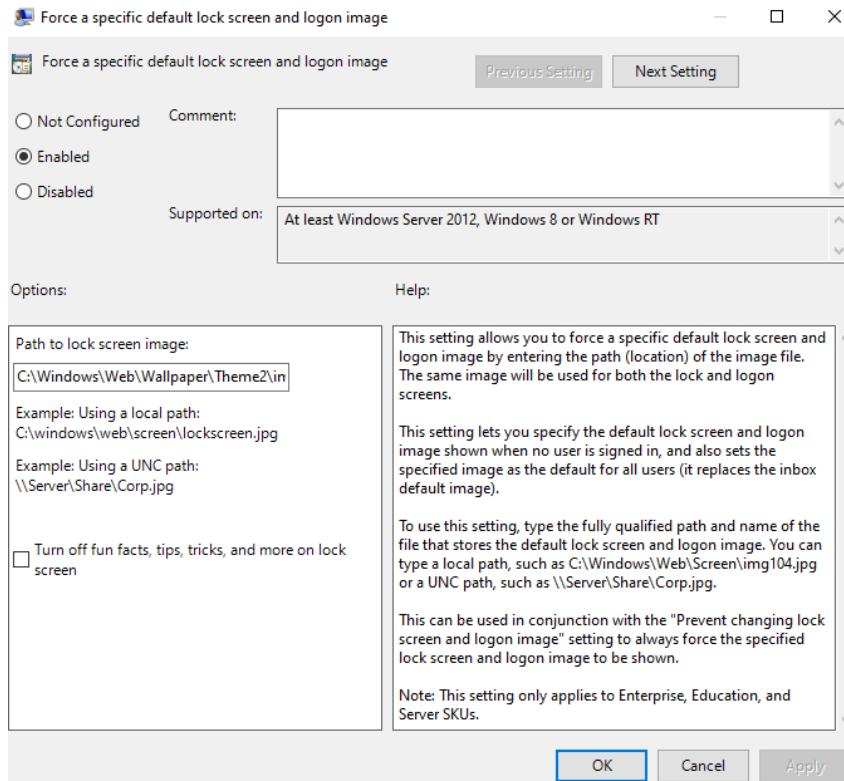


Abbildung 61: Lock/Logon Screen GPO konfigurieren

Überprüfung

Wenn sich jetzt ein Benutzer abmeldet erscheint in der Anmeldeansicht das neue Lock/Logon Bild.

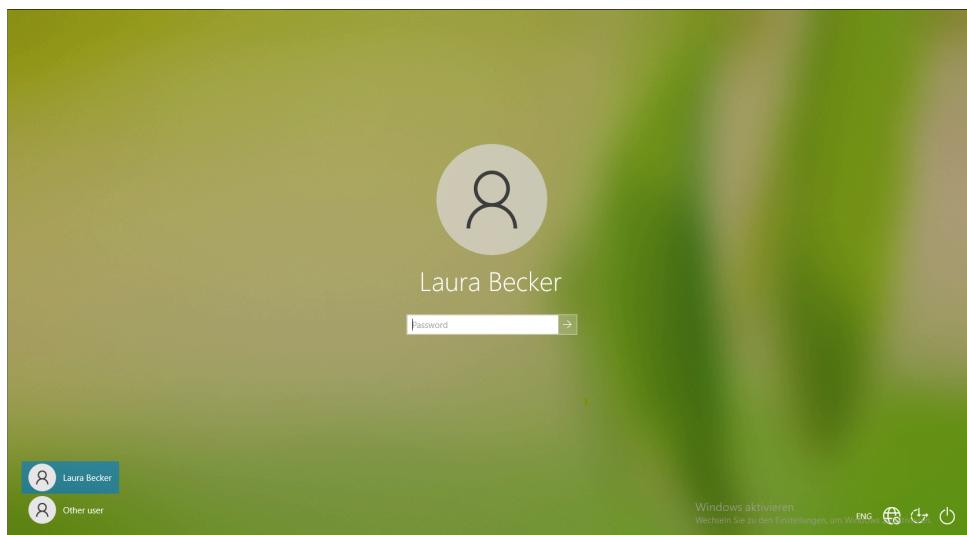


Abbildung 62: Lock/Logon Screen GPO test

5.7.1.3. GPO Last signed in user not shown

GPO erstellen

Auf dem Domänen Controller wird im Server Manager unter Tools die Gruppenrichtlinienverwaltung geöffnet. Dort wird eine neue Gruppenrichtlinie erstellt und konfiguriert.

GPO bearbeiten

In der Gruppenrichtlinienverwaltung kann dann unter folgendem Pfad die Gruppenrichtlinie konfiguriert werden:

Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Local Policies -> Security Options -> Interactive logon: Do not display last signed-in

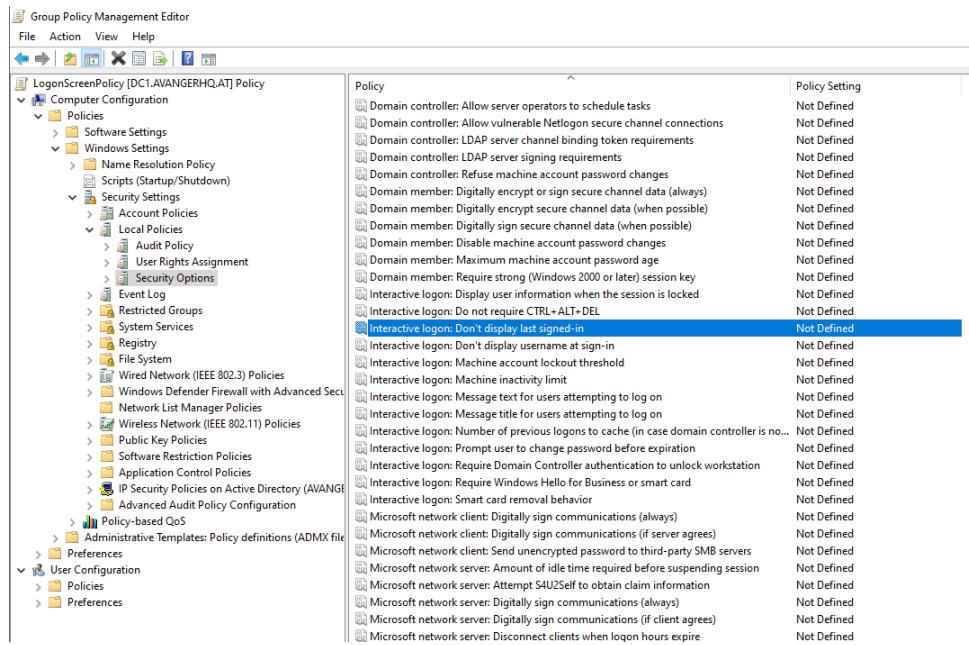


Abbildung 63: Last signed in GPO erstellen

Dort kann dann die Option enabled und der Pfad zum Hintergrundbild angegeben werden. In diesem Beispiel wird ein bereits vorhandenes Bild verwendet.

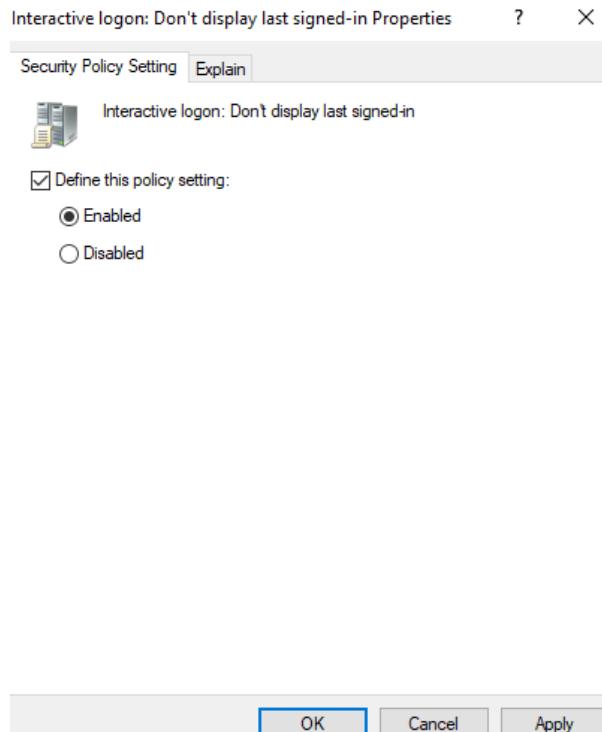


Abbildung 64: Last signed in GPO konfigurieren

Überprüfung

Wenn sich jetzt ein Benutzer abmeldet erscheint in der Anmeldeansicht kein Benutzername mehr.

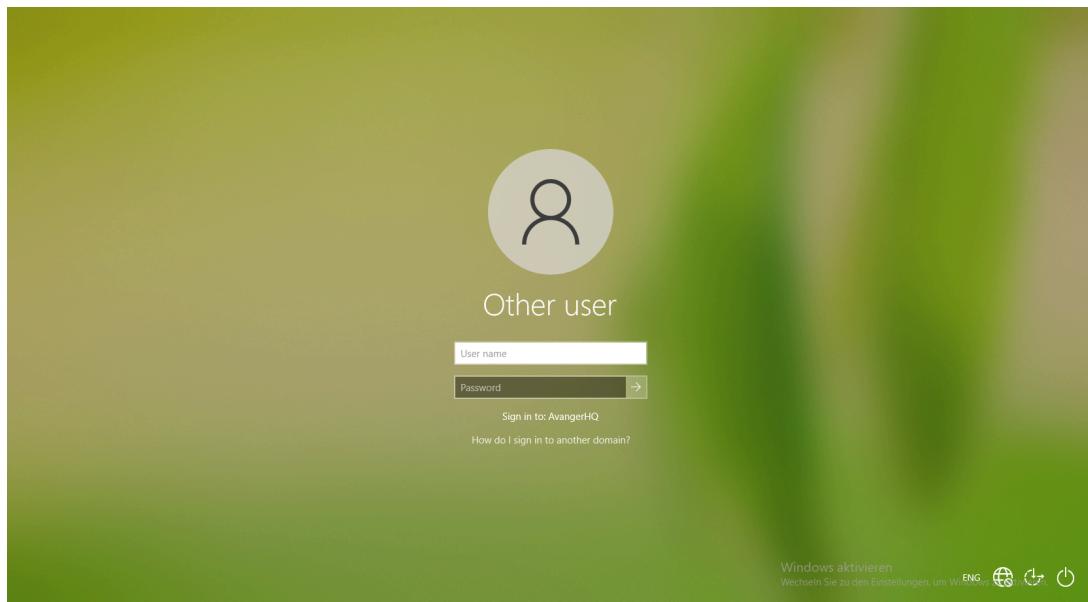


Abbildung 65: Last signed in GPO test

5.7.1.4. GPO Password Security Settings

GPO erstellen

Auf dem Domänen Controller wird im Server Manager unter Tools die Gruppenrichtlinienverwaltung geöffnet. Dort wird eine neue Gruppenrichtlinie erstellt und konfiguriert.

GPO bearbeiten

In der Gruppenrichtlinienverwaltung kann dann unter folgendem Pfad die Gruppenrichtlinie konfiguriert werden:

Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Account Policies -> Password Policy

Dort können jetzt die verschiedenen Einstellungen für das Passwort festgelegt werden.

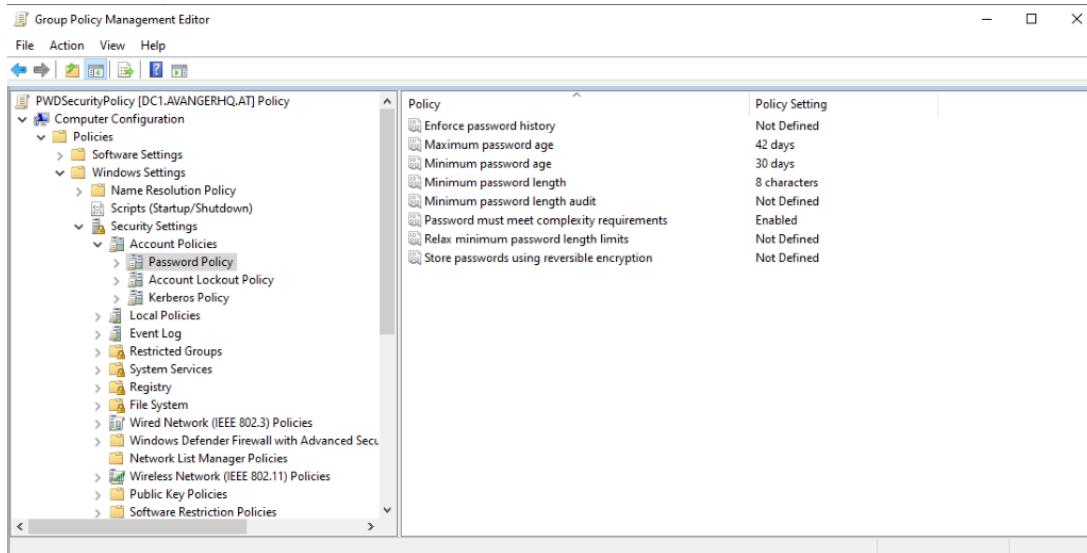


Abbildung 66: Password Security GPO konfigurieren

5.7.1.5. GPO Lokale Firewall Einstellungen (per PS-Skript)

PS-Skript erstellen

Zuerst wird ein PowerShell Skript erstellt, welches die Firewall Einstellungen setzt. Dieses Skript wird dann auf dem Domänen Controller gespeichert. Es handelt sich in diesem Skript vor allem um IPv6 Regeln, da diese in unserem Fall deaktiviert werden sollen.

```

1 # Liste wichtiger IPv6-Firewallregeln
2 $importantRules = @(
3     "Core Networking - ICMPv6-In",
4     "Core Networking - Teredo-In",
5     "Core Networking - LLMNR (UDP-In)",
6     "Remote Desktop - User Mode (TCP-In)",
7     "Remote Desktop - User Mode (UDP-In)"
8 )
9
10 # Deaktiviere die angegebenen Regeln
11 foreach ($rule in $importantRules) {
12     if (Get-NetFirewallRule -DisplayName $rule -ErrorAction
13     SilentlyContinue) {
14         Set-NetFirewallRule -DisplayName $rule -Enabled False
15         Write-Output "Regel '$rule' wurde deaktiviert."
16     } else {
17         Write-Output "Regel '$rule' nicht gefunden."
18 }

```

GPO erstellen

Auf dem Domänen Controller wird im Server Manager unter Tools die Gruppenrichtlinienverwaltung geöffnet. Dort wird eine neue Gruppenrichtlinie erstellt und konfiguriert.

GPO bearbeiten

In der Gruppenrichtlinienverwaltung kann dann unter folgendem Pfad die Gruppenrichtlinie konfiguriert werden:

Computer Configuration -> Policies -> Windows Settings -> Scripts -> Startup

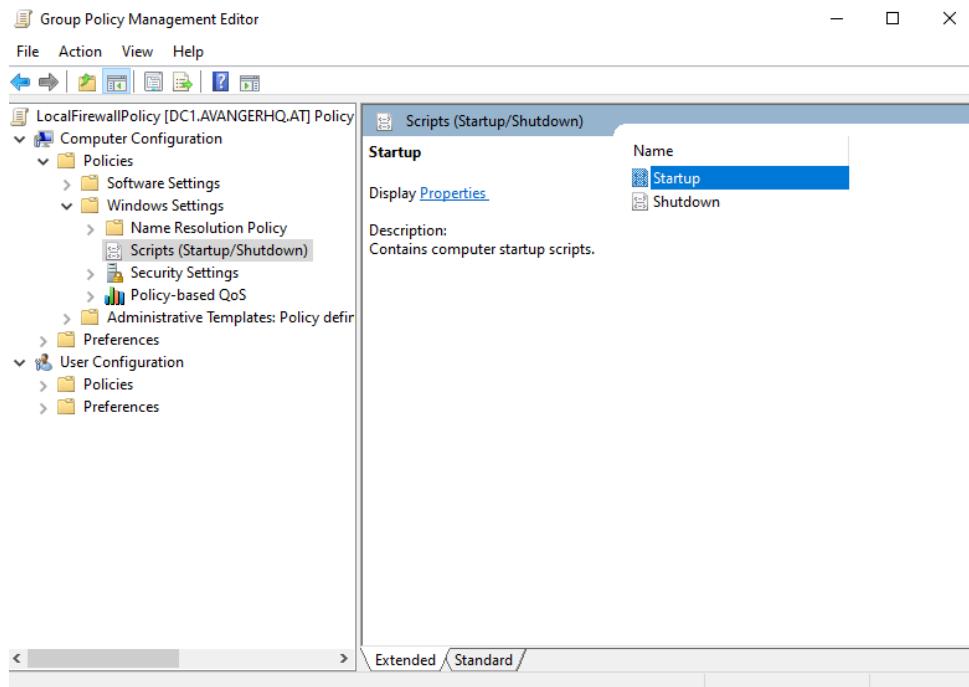


Abbildung 67: Local Firewall GPO Pfad

Dort kann jetzt das Skript hinzugefügt werden, welches beim Starten des Computers ausgeführt wird.

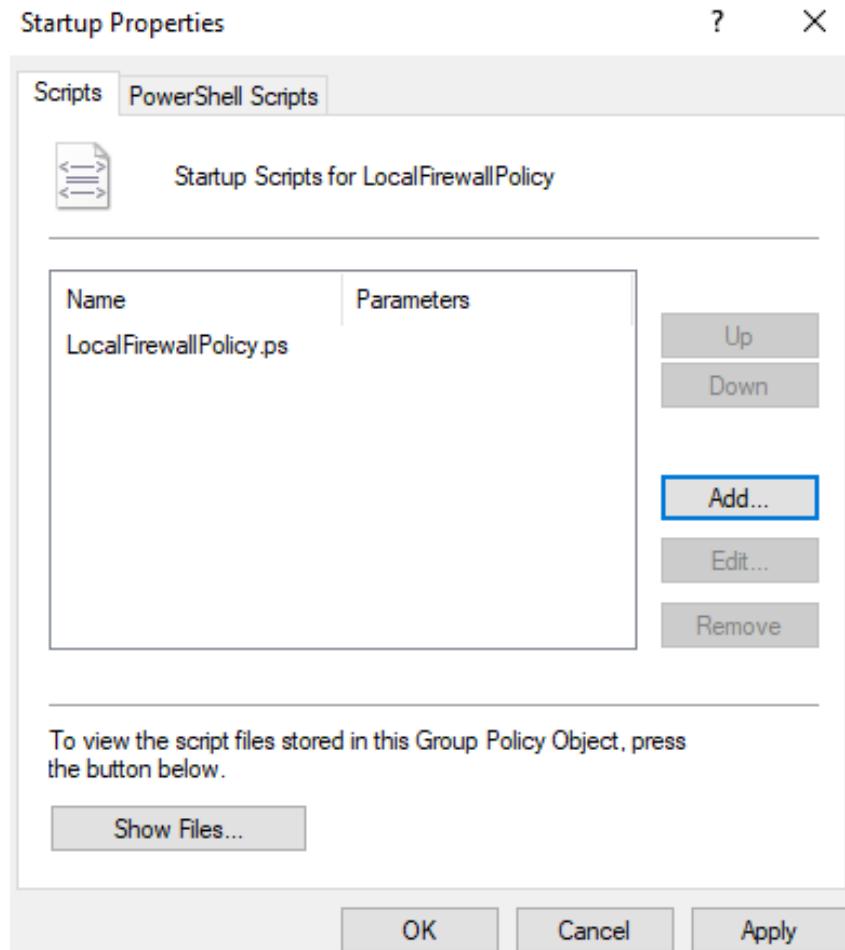


Abbildung 68: Local Firewall GPO konfigurieren

5.7.1.6. GPO Account Sperrung

GPO erstellen

Auf dem Domänen Controller wird im Server Manager unter Tools die Gruppenrichtlinienverwaltung geöffnet. Dort wird eine neue Gruppenrichtlinie erstellt und konfiguriert.

GPO bearbeiten

In der Gruppenrichtlinienverwaltung kann dann unter folgendem Pfad die Gruppenrichtlinie konfiguriert werden:

Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Account Policies -> Account Lockout Policy

Dort können dann die einzelnen Konfigurationen vorgenommen werden, wie in folgendem Bild zu sehen:

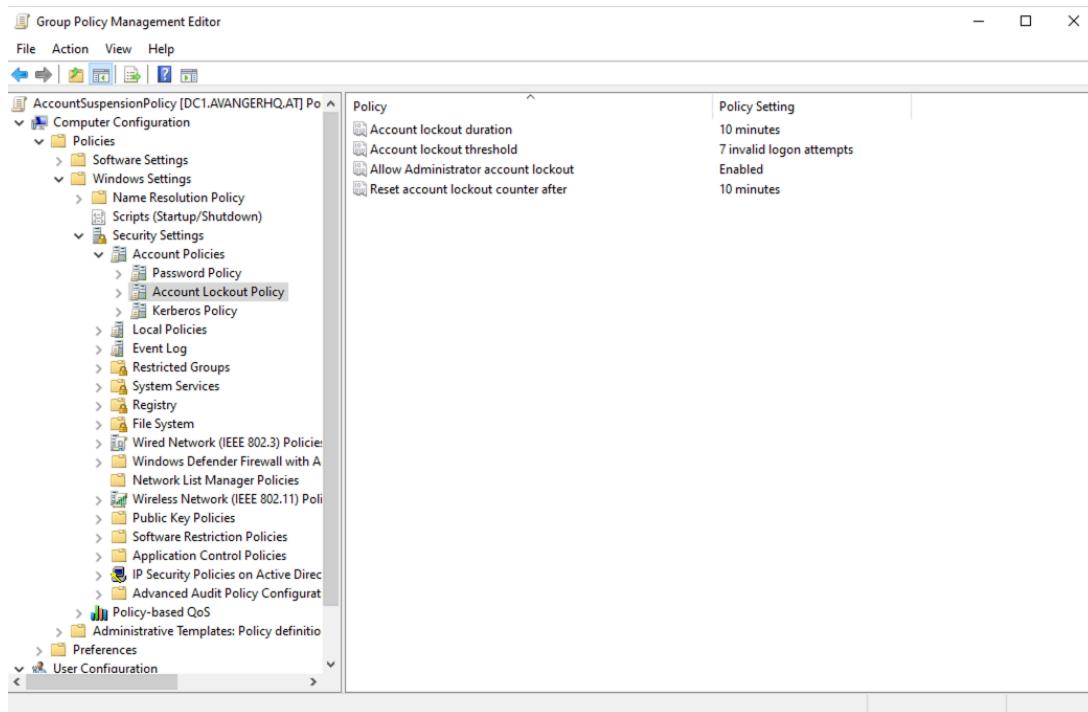


Abbildung 69: Account Sperrung GPO konfigurieren

Überprüfung

Sollte ein Angreifer versuchen das Password mit einer Brute-Force Attacke kacken, wird der Account nach 7 Fehlversuchen gesperrt.

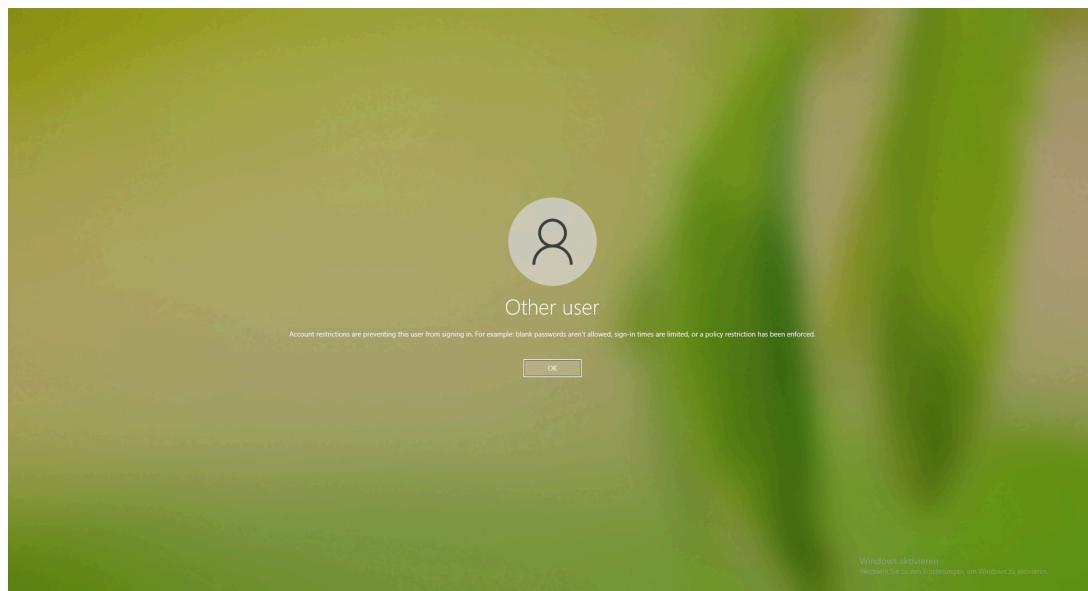


Abbildung 70: Last signed in GPO test

5.7.1.7. GPO Software Installation

.msi Datei bereitstellen

Als Software wird der Google Chrome Browser installiert, die zugehörige .msi Datei kann im Internet heruntergeladen werden. Diese muss dann auf einen erreichbaren Share gespeichert werden, in unserm Fall auf dem Fileserver.

GPO erstellen

Auf dem Domänen Controller wird im Server Manager unter Tools die Gruppenrichtlinienverwaltung geöffnet. Dort wird eine neue Gruppenrichtlinie erstellt und konfiguriert.

GPO bearbeiten

In der Gruppenrichtlinienverwaltung kann dann unter folgendem Pfad die Gruppenrichtlinie konfiguriert werden:

User Configuration -> Policies -> Software Settings -> Software Installation

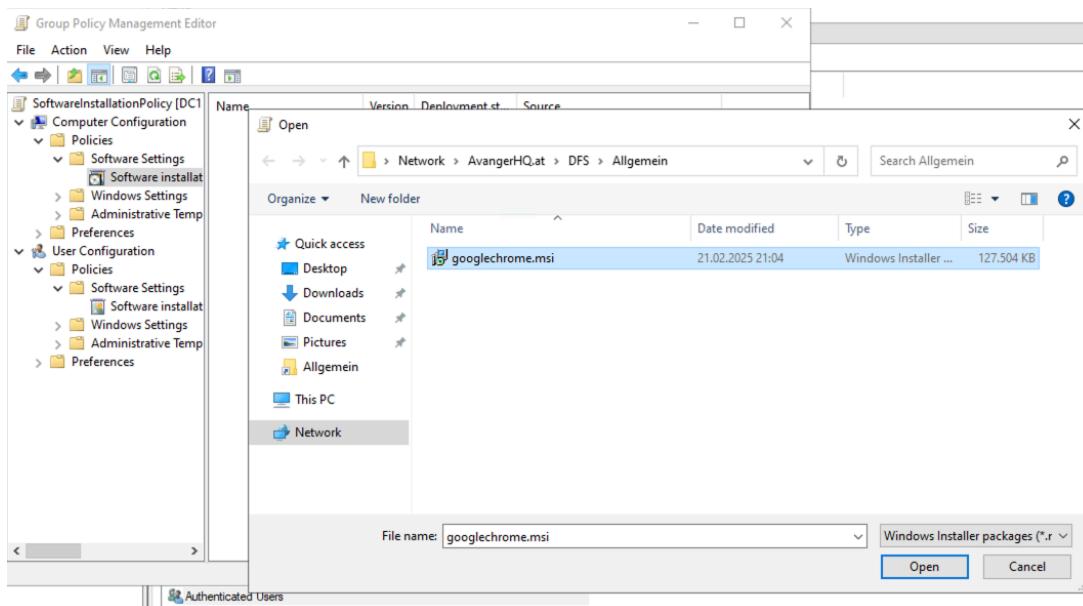


Abbildung 71: Software Installation GPO konfigurieren

5.7.2. Credential Guard

Der Credential Guard verhindert Identitätsdiebstahl, durch das absichern und schützen von den

- NTLM Passwort Hashes,
- dem Kerberos Ticket Granting Tickets (TGTs) und
- den gespeicherten Credentials von Applikationen als Domain Credentials.

5.7.2.1. Nutzen/Vorteil

- hardware security
- virtualization-based security
- protection against advanced persistant threats

5.7.2.2. Requirements

Folgende Einstellungen sind essenziell:

- Virtualization-based security (VBS)
- Secure Boot

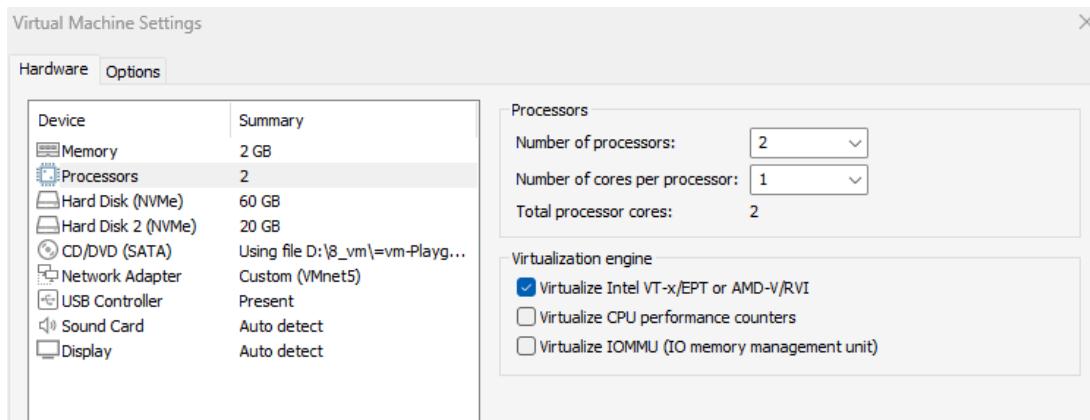


Abbildung 72: Enable VBS

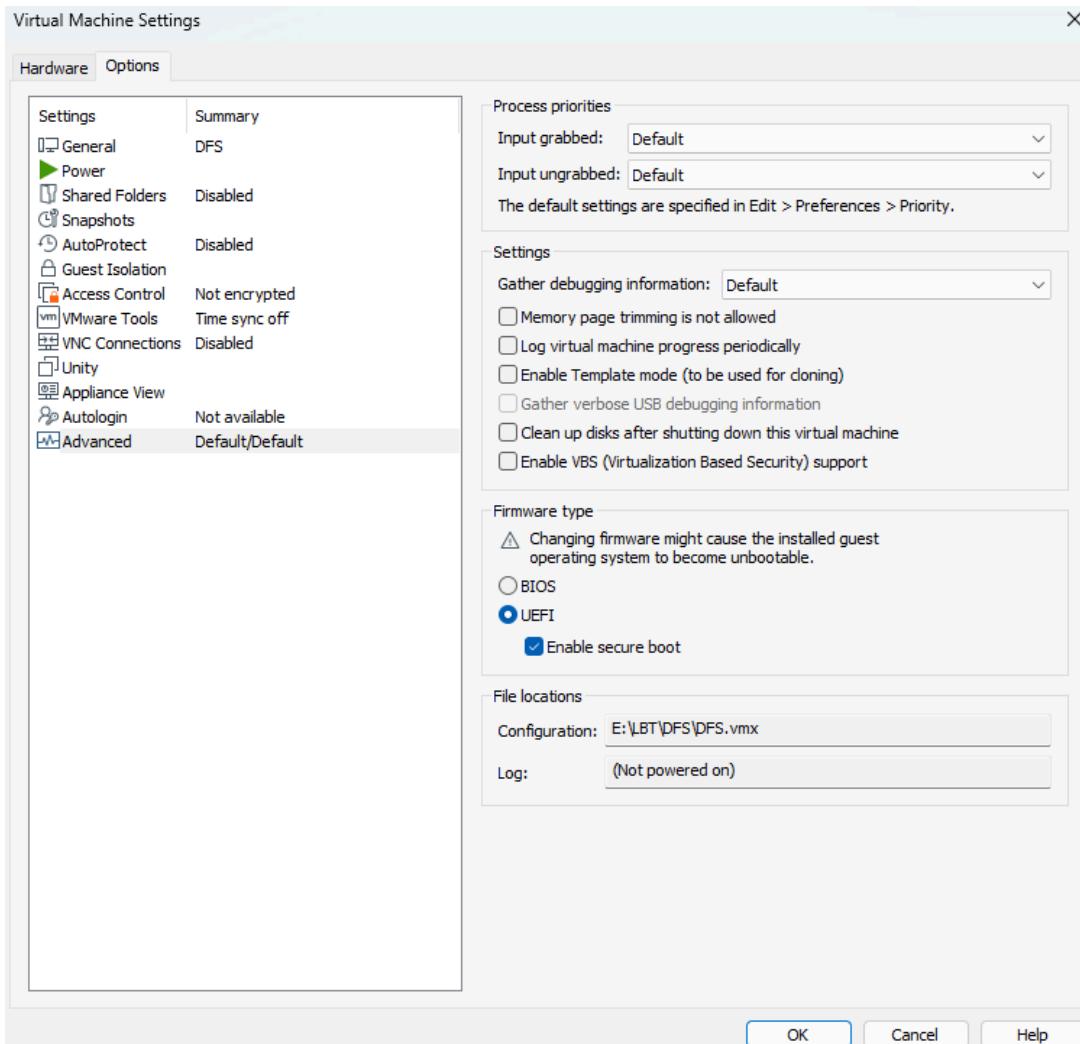


Abbildung 73: Enable Secure Boot

Folgende Einstellungen sind empfehlenswert:

- Trusted Platform Module (TPM)
- UEFI lock

5.7.2.3. Wichtig!

Credential Guard hat bei Domänen Controllern (DCs) ist nicht empfohlen zu aktivieren, da er keine erweiterte Security hinzufügt. Das aktivieren kann zu Problemen mit Applikationskompatibilität führen.

5.7.2.4. Default Enablement

Windows 11 (22H2) und Windows Server 2025 oder später sollten die Credential Guard bei folgenden Bedingungen standardmäßig aktiviert sein.

Windows 11 (22H2)

- entspricht den license requirements
- entspricht den hardware and software requirements
- Credential Guard ist nicht explizit deaktiviert

Windows Server 2025

- entspricht den license requirements
- entspricht den hardware and software requirements
- Credential Guard ist nicht explizit deaktiviert
- Mitglied einer Domäne
- Kein Domänen Controller

5.7.2.5. GPO Konfiguration

- Local Group Policy Editor öffnen (oder für mehrere Geräte eine GPO erstellen)
- Pfad folgen Computer Configuration\Administrative Templates\System\Device Guard\Turn on Virtualization Based Security
- Enable und unter Credential Guard Configuration zwischen den Optionen
 - Enabled with UEFI lock
 - Enabled without lock
- In CMD gpupdate /force eingeben

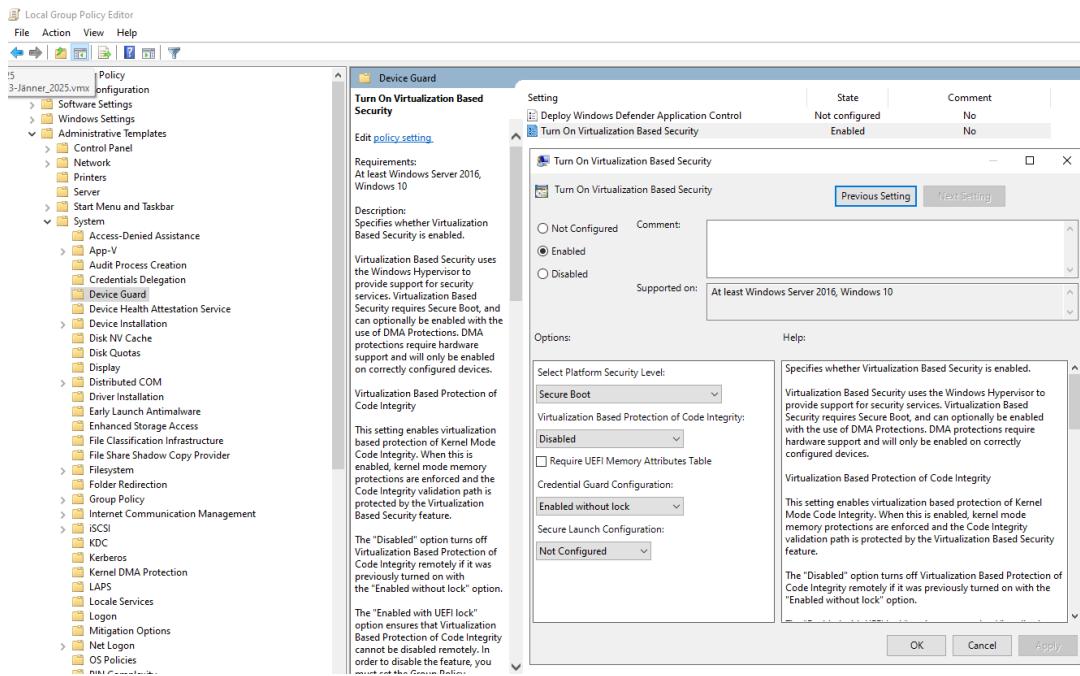


Abbildung 74: Credential Guard GPO

5.7.2.6. Überprüfung

System Information

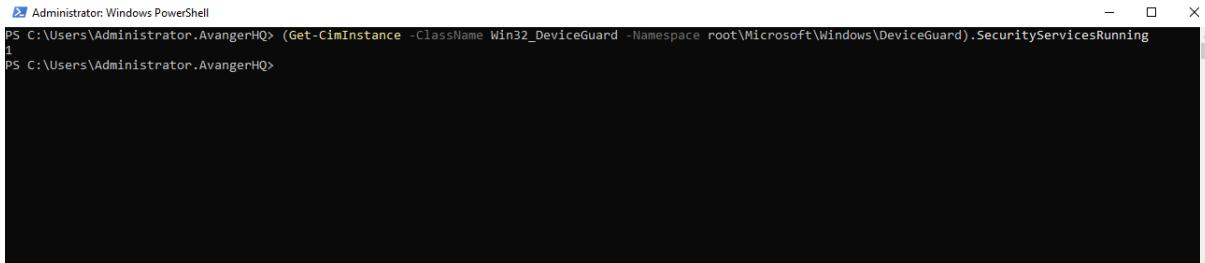
- Start
- msinfo32.exe eingeben
- System Information auswählen
- System Summary auswählen
- überprüfen ob der Credential Guard neben der Virtualization-based Security Services Running angezeigt wird

PowerShell

Folgenden Command in der PowerShell eingeben:

```
(Get-CimInstance -ClassName "Win32_DeviceGuard" -Namespace
"root\Microsoft\Windows\DeviceGuard").SecurityServicesRunning
```

- 0: Credential Guard disabled
- 1: Credential Gurad enabled/running



```
Administrator: Windows PowerShell
PS C:\Users\Administrator.AvangerHQ> (Get-CimInstance -ClassName Win32_DeviceGuard -Namespace root\Microsoft\Windows\DeviceGuard).SecurityServicesRunning
1
PS C:\Users\Administrator.AvangerHQ>
```

Abbildung 75: Credential Guard Überprüfung

5.7.3. Protected Users Security Group

Die Global Group Protect Users wurde zum Schutz vor Diebstahl von Anmeldeinformationen entwickelt. Die Gruppe löst nicht konfigurierbaren Schutz auf Geräten und Hostcomputern aus, um zu verhindern, dass Anmeldeinformationen bei der Anmeldung von Gruppenmitgliedern zwischengespeichert werden.

5.7.3.1. Wichtig!

Niemals Konten für Dienst (zB. NT AUTHORITY\SYSTEM, NT AUTHORITY\NETWORK SERVICE) und Computer (Jeder Computer der Domäne beitritt zB. Kontoname PC-01\$) hinzufügen, da für diese Konten die Mitgliedschaft keinen lokalen Schutz bietet. Kennwort und Zertifikat sind immer auf dem Host verfügbar.

Mitglieder von Gruppen mit hoher Berechtigung (Enterprise Admins & Domain Admins) nicht hinzufügen, bis man sicher ist das das Hinzufügen keine negativen Konsequenzen hat.

5.7.3.2. Requirements

Hosts Betriebssystem:

- Windows 8.1 or later
- Windows Server 2012 R2 or later

Domain functional Level:

- Windows Server 2012 R2 or later

Mitglieder der Protected User Group müssen AES Authentifikation unterstützen

5.7.3.3. Device Protection für Protected Users

- Keine Speicherung von Klartext-Anmeldedaten bei Credential Delegation (CredSSP), Windows Digest, NTLM und Kerberos.
- Kerberos erzeugt keine DES- oder RC4-Schlüssel.

- Kein Offline-Login, da das System keinen zwischengespeicherten Verifier erstellt.
- Schutzmechanismen greifen erst nach der nächsten Anmeldung des Nutzers.

5.7.3.4. Domain Controller Protection für Protected Users

- Keine NTLM-Authentifizierung möglich.
- Kerberos erlaubt nur moderne Verschlüsselungen, keine DES oder RC4.
- Keine unbeschränkte oder beschränkte Delegation möglich.
- Kerberos-Tickets (TGTs) können nicht über vier Stunden hinaus verlängert werden.
- Ticket-Lebensdauer ist fest auf 600 Minuten gesetzt und kann nur durch Verlassen der Gruppe geändert werden.

5.7.3.5. Konfiguration

Active Directory Users and Computers

- Zu folgendem Pfad wechseln:
Server Manager -> Tools -> Active Directory Users and Computers -> Folder Users
- den User auswählen und zu der Gruppe Protected Users hinzufügen

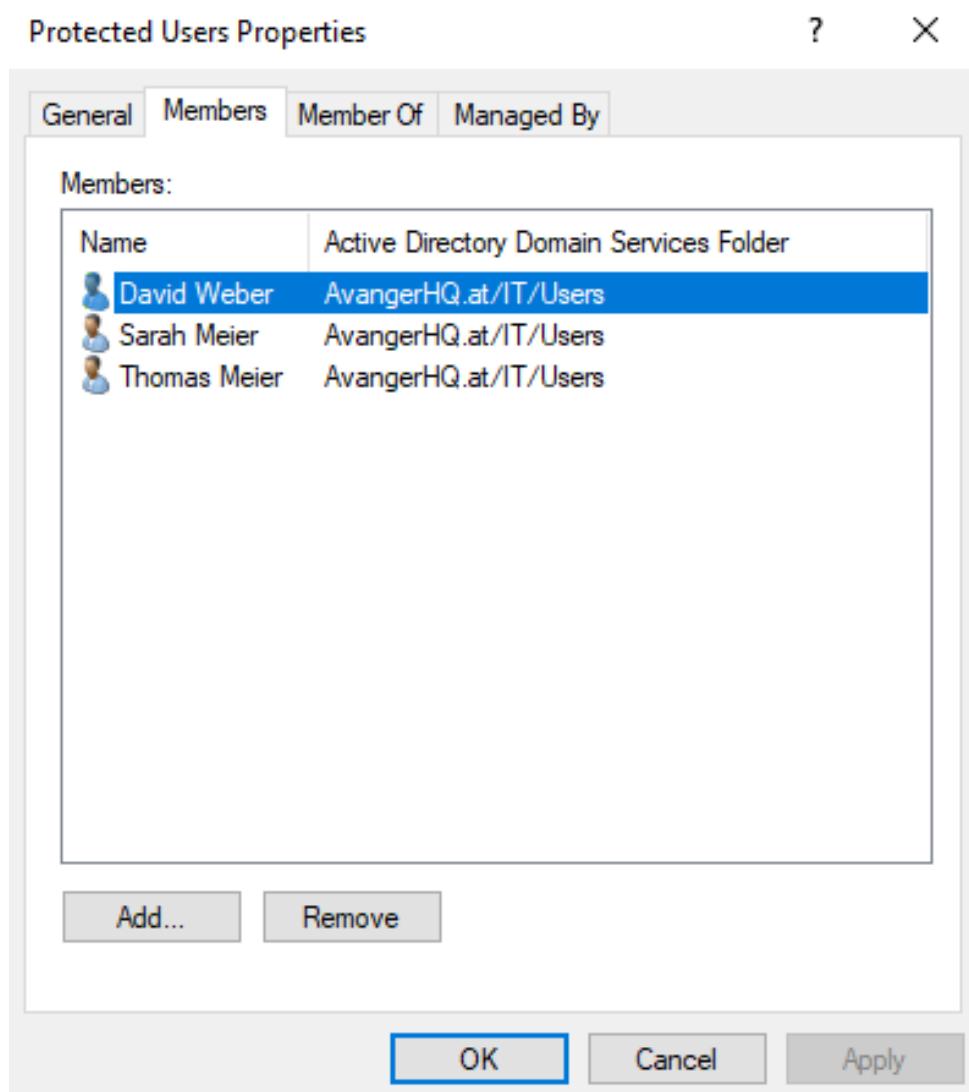


Abbildung 76: Protected Users Überprüfung

PowerShell folgenden Befehl in der PowerShell ausführen:

```
1 Add-ADGroupMember -Identity "Protected Users" -Members "USERNAME"
```

5.7.4. Windows Security Baseline

5.7.4.1. Was ist eine Security Baseline?

Eine Security Baseline ist eine Gruppe von von Microsoft empfohlenen Konfigurationseinstellungen, die deren Auswirkungen auf die Sicherheit erläutern. Diese Einstellungen basieren

auf Feedback von Microsoft Security-Entwicklungsteams, -Produktgruppen, -Partnern und -Kunden.

5.7.4.2. Warum werden Security Baselines benötigt?

- Standardisierte Sicherheitskonfigurationen für alle Systeme
- Reduzierung von Sicherheitsrisiken
- Einhaltung von Compliance-Vorgaben und Sicherheitsstandards
- Minimierung von Fehlkonfigurationen
- Erleichterte Verwaltung und Automatisierung der Sicherheitsrichtlinien
- Bessere Nachvollziehbarkeit von Änderungen und Sicherheitsmaßnahmen
- Effiziente Reaktion auf Bedrohungen durch vordefinierte Sicherheitsmaßnahmen

5.7.4.3. Policy Analyzer

Der PolicyAnalyzer ist ein Microsoft-Tool, das Administratoren hilft, Gruppenrichtlinien objektiv zu analysieren und zu vergleichen. Es wird oft in Verbindung mit den Windows Security Baselines genutzt, um Sicherheitsrichtlinien zu überprüfen und sicherzustellen, dass sie den empfohlenen Best Practices entsprechen. PolicyAnalyzer kann verschiedene GPOs (Group Policy Objects) auswerten, Abweichungen zwischen ihnen aufzeigen und mit den vordefinierten Compliance-Vorgaben der Security Baselines abgleichen. Dies erleichtert es Unternehmen, ihre Systeme auf Sicherheitslücken zu prüfen, Richtlinien zentral zu verwalten und sicherzustellen, dass alle Geräte den vorgeschriebenen Sicherheitsstandards entsprechen.

5.7.4.4. Konfiguration

Download

Auf folgender Website können die verschiedenen Baselines heruntergeladen werden: <https://www.microsoft.com/en-us/download/details.aspx?id=55319&msokid=06c952b1aa3966680c3847e3ab9067f8>

In meinem Fall habe ich die Windows Server 2022 Security Baseline und den Policy Analyzer installiert.

Choose the download you want

<input type="checkbox"/> Windows 11 v23H2 Security Baseline.zip	1.2 MB
<input type="checkbox"/> Windows 10 version 22H2 Security Baseline.zip	1.2 MB
<input type="checkbox"/> Windows 11 version 22H2 Security Baseline.zip	1.4 MB
<input type="checkbox"/> Windows 10 version 21H2 Security Baseline.zip	1.2 MB
<input type="checkbox"/> Windows 11 Security Baseline.zip	1.2 MB
<input checked="" type="checkbox"/> Windows Server 2022 Security Baseline.zip	1.3 MB
<input type="checkbox"/> Windows 10 Update Baseline.zip	452.4 KB
<input type="checkbox"/> SetObjectSecurity.zip	313.9 KB
<input checked="" type="checkbox"/> PolicyAnalyzer.zip	1.5 MB
<input type="checkbox"/> LGPO.zip	519.2 KB
<input type="checkbox"/> Windows 10 Version 1607 and Windows Server 2016 Security Baseline.zip	1.5 MB
<input type="checkbox"/> Windows 10 Version 1507 Security Baseline.zip	903.4 KB

Windows aktiv
Wechseln Sie zu di

Abbildung 77: Windows Security Baseline Download

Policy Analyzer

Der Policy Analyzer kann durch die .exe ausgeführt werden und unter dem Punkt Add kann die Windows Security Baseline importiert werden.

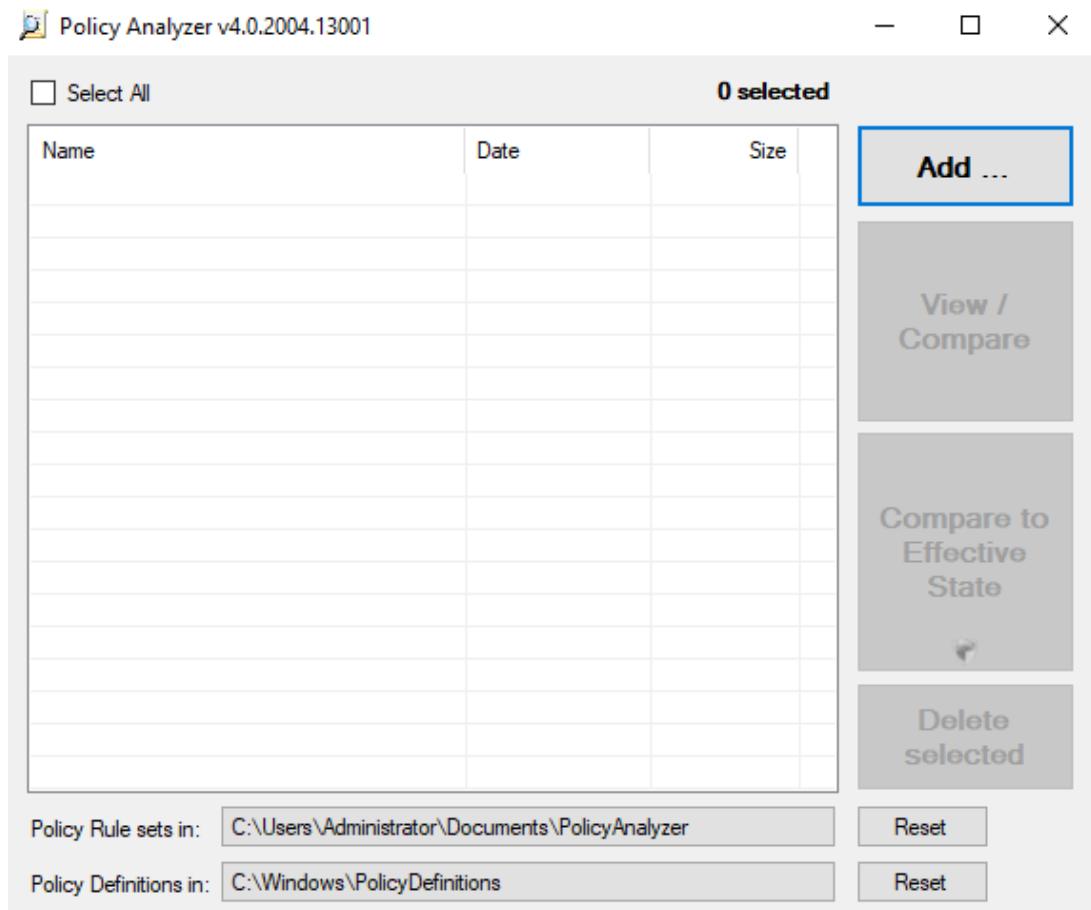


Abbildung 78: Policy Analyzer starten

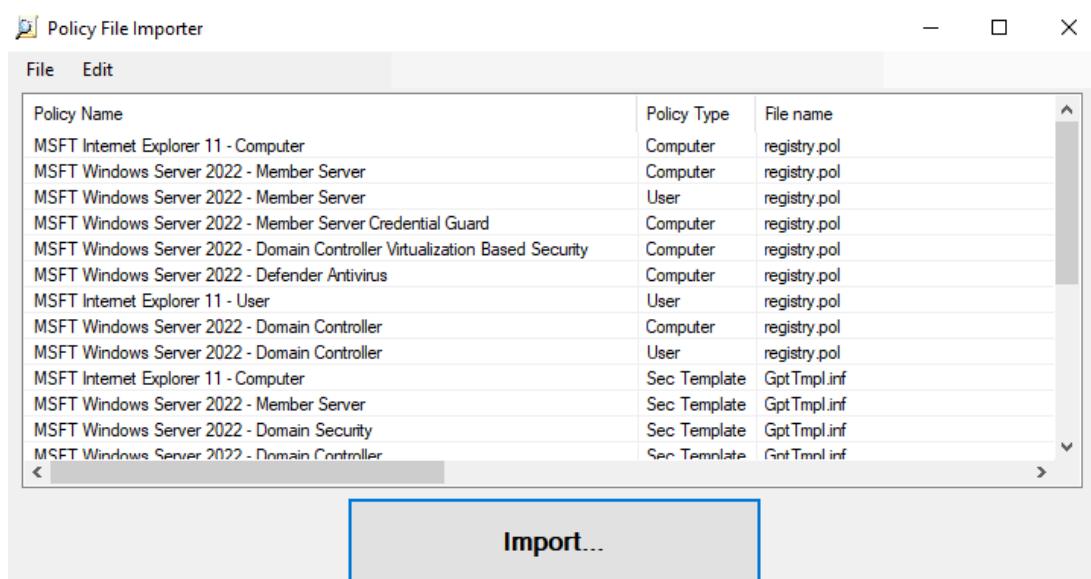


Abbildung 79: Policy Analyzer Baseline importieren

Unter dem Punkt Compare to Effective State können die GPOs der Baseline mit den aktuellen Sicherheitskonfigurationen verglichen werden.

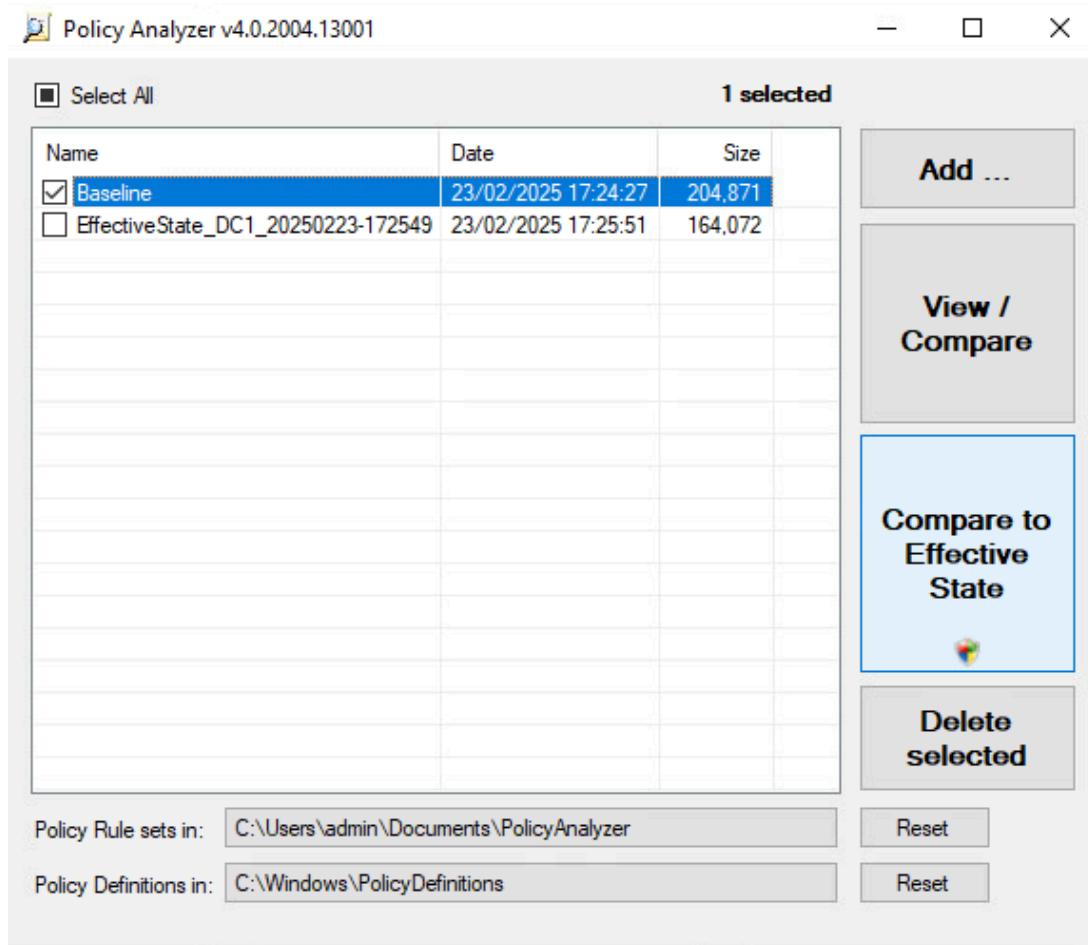


Abbildung 80: Baseline mit Effective State vergleichen

Die gelb makierten Felder zeigen schlussendlich die Unterschiede an.

The screenshot shows the Windows Policy Viewer window titled "Policy Viewer - 338 items". The interface includes a toolbar with "Clipboard", "View", "Export", and "Options" buttons. Below the toolbar is a table with columns: "Policy Type", "Policy Group or Registry Key", "Policy Setting", "Baseline(s)", and "Effective state". The table lists numerous security policies such as "Audit Policy Account Logon", "Audit Policy Account Management", "Audit Policy Detailed Tracking", "Audit Policy DS Access", "Audit Policy Logon/Logoff", etc. Many rows show a conflict between the baseline and effective states, indicated by yellow background color.

Policy Type	Policy Group or Registry Key	Policy Setting	Baseline(s)	Effective state
Audit Policy	Account Logon	Credential Validation	***CONFLICT***	Success
Audit Policy	Account Logon	Kerberos Authentication Service	Success and Fail...	Success
Audit Policy	Account Logon	Kerberos Service Ticket Operations	Failure	Success
Audit Policy	Account Management	Computer Account Management	Success	Success
Audit Policy	Account Management	Other Account Management Events	Success	No Auditing
Audit Policy	Account Management	Security Group Management	Success	Success
Audit Policy	Account Management	User Account Management	Success and Fail...	Success
Audit Policy	Detailed Tracking	PNP Activity	Success	No Auditing
Audit Policy	Detailed Tracking	Process Creation	Success	No Auditing
Audit Policy	DS Access	Directory Service Access	Failure	Success
Audit Policy	DS Access	Directory Service Changes	Success	No Auditing
Audit Policy	Logon/Logoff	Account Lockout	Failure	Success
Audit Policy	Logon/Logoff	Group Membership	Success	No Auditing
Audit Policy	Logon/Logoff	Logon	Success and Fail...	Success and Fail...
Audit Policy	Logon/Logoff	Other Logon/Logoff Events	Success and Fail...	No Auditing
Audit Policy	Logon/Logoff	Special Logon	Success	Success
Audit Policy	Object Access	Detailed File Share	Failure	No Auditing
Audit Policy	Object Access	File Share	Success and Fail...	No Auditing
Audit Policy	Object Access	Other Object Access Events	Success and Fail...	No Auditing
Audit Policy	Object Access	Removable Storage	Success and Fail...	No Auditing
Audit Policy	Policy Change	Audit Policy Change	Success	Success
Audit Policy	Policy Change	Authentication Policy Change	Success	Success

Policy Path:
Computer Configuration
System\Device Guard
Turn On Virtualization Based Security -> Credential Guard Configuration:
Specifies whether Virtualization Based Security is enabled.
Virtualization Based Security uses the Windows Hypervisor to provide support for security services. Virtualization Based Security requires Secure Boot, and can optionally be enabled with the use of DMA Protections. DMA protections require hardware support and will only be enabled on correctly configured devices.
Virtualization Based Protection of Code Integrity:
This setting enables virtualization based protection of Kernel Mode Code Integrity. When this is enabled, kernel mode memory protections are enforced and the Code Integrity validation path is protected by the Virtualization Based Security feature.
The "Disabled" option turns off Virtualization Based Protection of Code Integrity remotely if it was previously turned on with the "Enabled without lock" option.
The "Enabled with UEFI lock" option ensures that Virtualization Based Protection of Code Integrity cannot be disabled remotely. In order to disable the feature, you must set the Group Policy to "Disabled" as well as remove the security functionality from each computer, with a physically present user, in order to clear configuration persisted in UEFI.

Abbildung 81: Baseline mit Effective State vergleichen

Security Baseline für DCs per GPO bereitstellen

Zuerst müssen die Templates, die im Ordner der Windows Security Baseline gefunden werden können, in die PolicyDefinitions der Domäne kopiert werden.

The screenshot shows a Windows File Explorer window with the title bar "PolicyDefinitions". The address bar shows the path: "This PC > Local Disk (C:) > Windows > SYSVOL > sysvol > AvangerHQ.at > Policies > PolicyDefinitions >". The left sidebar shows "This PC" and "Network". The main pane displays a list of files under "PolicyDefinitions": "en-US", "AdminPwd.admx", "MSS-legacy.admx", and "SecGuide.admx". The "en-US" folder has a timestamp of "19.02.2025 17:00". The ADMX files have timestamps from "01.11.2019 00:58" to "09.07.2021 19:25". The "Type" column indicates they are "ADMX File" and the "Size" column shows values like "4 KB" and "32 KB".

Abbildung 82: Windows Security Baseline Templates kopieren

Im Server Manager unter Tools kann dann die Group Policy Management Console geöffnet werden und eine neue GPO unter dem Ordner Group Policy Objects erstellt werden. Der Name sollte sinnvoll gewählt werden.

In diese GPO kann dann die Windows Security Baseline für DCs implementiert werden. Rechts Klick -> Import Settings - Pfad auswählen -> Windows Server 2022 - Domain Controller

5.7.5. Advanced Security Audit Policies

Die Advanced Security Audit Policies ermöglichen eine detaillierte Kontrolle über sicherheitsrelevante Ereignisse im Netzwerk. Sie erweitern die klassischen Audit Policies und bieten granulare Einstellungsmöglichkeiten zur Überwachung sicherheitskritischer Prozesse.

5.7.5.1. Nutzen/Vorteil

- Verbesserte Transparenz und Nachvollziehbarkeit von sicherheitsrelevanten Ereignissen
- Frühe Erkennung von Sicherheitsvorfällen
- Einhaltung von Compliance-Vorgaben
- Präzisere Kontrolle durch detaillierte Audit-Kategorien

5.7.5.2. GPO Konfiguration

- Group Policy Management öffnen
- Eine neue GPO unter OU erstellen
- Zu folgendem Pfad navigieren
Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System Audit Policies
- Folgende Kategorien aktivieren:
 - Account Management -> Audit User Account Management
 - Logon/Logoff -> Audit Kerberos Authentication Service
 - Account Management -> Audit Security Group Management
 - DS Access -> Audit Directory Service Changes
- Apply und OK drücken

5.7.5.3. Überprüfung

Event Viewer

- Windows Logs -> Security
- Filtern nach Event-IDs:

- 4720 (Benutzerkonto erstellt)
- 4740 (Konto gesperrt)
- 4765 (Sicherheitsgruppen-Änderung)
- 4766 (Fehlgeschlagene Kerberos-Anmeldung)
- 5136 (Directory Service Änderungen)
- Dokumentiere relevante Einträge

PowerShell

Aktive Audit Policies anzeigen:

```
1 auditpol /get /category:*
```

Überprüfen, ob ein spezifisches Audit-Event aktiviert ist:

```
1 auditpol /get /subcategory:"User Account Management"
```

Ereignisse aus dem Event Log abrufen:

```
1 Get-WinEvent -LogName "Security" | Where-Object { $_.Id -eq 4720 }
```

6. Linux

6.1. Bind9 Forwarder

Ein Forwarder in der DNS-Welt ist ein DNS-Server, der Anfragen an einen anderen DNS-Server weiterleitet, anstatt sie selbst zu beantworten. BIND9, als einer der beliebtesten DNS-Server, ermöglicht es, Anfragen an sogenannte Forwarder-Server weiterzuleiten, wenn der BIND9-Server selbst die Anfrage nicht lösen kann.

6.1.1. Checkliste

- Installieren des Diensts
- Forwarder Konfigurieren
- Konfiguration überprüfen
- BIND9-Dienst neu starten

- Installieren des Diensts

```
1 sudo apt install bind9 bind9utils bind9-doc dnsutils
```

6.1.2. Forwarder Konfigurieren

```
1 options {
2     directory "/var/cache/bind";
3     forwarders {
4         8.8.8.8;
5         8.8.4.4;
6     };
7     forward only;
8     allow-query { local-lan; };
9     dnssec-validation auto;
10    auth-nxdomain no;      // conform to RFC1035
11    listen-on-v6 { any; }D;
12    recursion yes;
13    querylog yes; // Disable if you want, nice for debugging.
14    version "not available"; // Disable for security
15 }
```

6.1.2.1. Konfiguration überprüfen

```
1 sudo named-checkconf
```

BIND9-Dienst neu starten

```
1 sudo systemctl restart bind9
```

6.2. Metasploit Scan

Als zweiten Schritt soll mithilfe von Metasploit ein Scan durchgeführt werden. Zuerst erfolgt aber die Installation von Metasploit. Da Metasploit in der Regel auf Kali Linux vorinstalliert ist, verwenden wir dieses. In dem Root terminal werden folgende Befehle ausgeführt, damit Metasploit gestartet wird. Zuerst wird ein Database Server installiert damit alle Ergebnisse gespeichert werden können.

```
1 sudo systemctl start postgresql
2 sudo msfdb init
```

Anschließend wird Metasploit gestartet mit `msfconsole`.

Sobald Metasploit geladen ist, werden Sie die folgende Eingabeaufforderung in Ihrem Terminal sehen - die Startbildschirme sind zufällig, machen Sie sich also keine Sorgen, wenn Ihrer anders aussieht:



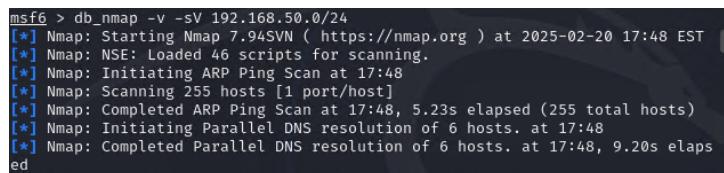
The screenshot shows the Metasploit msfconsole interface. It starts with a stylized logo composed of various symbols like arrows and brackets. Below the logo, the text reads: "Metasploit tip: Network adapter names can be used for IP options set LHOST eth0". Then it displays the command history: "root@kali:[~] # msfconsole". Following this, there is a summary of available modules: "[metasploit v6.4.9-dev]", "[2420 exploits - 1248 auxiliary - 423 post]", "[1465 payloads - 47 encoders - 11 nops]", and "[9 evasion]". At the bottom, it says "Metasploit Documentation: <https://docs.metasploit.com/>".

Abbildung 83: „Metasploit Ausgabe“

Mit dem Befehl `search portscan` wird eine Liste aller verfügbaren Portscannern zurückgeliefert.

6.2.1. Nmap Scan

Mit dem Befehl `db_nmap -v -sV 192.168.50.0/24` wird ein Nmap Scan durchgeführt. Dieser Scan zeigt alle offenen Ports und die Versionen der Dienste, die auf diesen Ports laufen.



The screenshot shows the Metasploit msf6 console. The user has run the command `db_nmap -v -sV 192.168.50.0/24`. The output shows the progress of the scan: "Starting Nmap 7.94SVN (https://nmap.org) at 2025-02-20 17:48 EST", "NSE: Loaded 46 scripts for scanning.", "Initiating ARP Ping Scan at 17:48", "Scanning 255 hosts [1 port/host]", "Completed ARP Ping Scan at 17:48, 5.23s elapsed (255 total hosts)", "Initiating Parallel DNS resolution of 6 hosts. at 17:48", and "Completed Parallel DNS resolution of 6 hosts. at 17:48, 9.20s elapsed".

Abbildung 84: „Metasploit nmap Scan“

Der Befehl `hosts` zeigt eine Liste an aller Geräte die im Netz gefunden worden sind.

Hosts									
address	mac	name	os_name	os_flavor	os_sp	purpose	info	comments	
192.168.50.1	00:0c:29:d2:4e:10		Unknown			device			
192.168.50.2	00:0c:29:7f:99:ca		Unknown			device			
192.168.50.3	00:0c:29:ff:a7:cb		Unknown			device			
192.168.50.4	00:0c:29:db:37:88		Unknown			device			
192.168.50.5	00:0c:29:66:38:99		Unknown			device			
192.168.50.12	00:0c:29:5b:67:f9		Unknown			device			
192.168.50.133			Unknown			device			

Abbildung 85: „Hosts im Netz“

Mit dem Befehl `services` können alle gefunden und offen Ports angezeigt werden.

address	port	proto	service	state	version	product
192.168.50.2	3268	tcp	ldap	open	VangerHQ	Microsoft Windows Active Directory LDAP Domain: AvangerHQ.at0., Site: Site-1-A vangerHQ
192.168.50.2	3269	tcp	ssl/ldap	open	VangerHQ	Microsoft Windows Active Directory LDAP Domain: AvangerHQ.at0., Site: Site-1-A vangerHQ
192.168.50.3	80	tcp	http	open	Microsoft IIS	httpd 10.0
192.168.50.3	135	tcp	msrpc	open	Microsoft Windows	RPC
192.168.50.3	443	tcp	ssl/http	open	Microsoft IIS	httpd 10.0
192.168.50.3	445	tcp	microsoft-ds	open		
192.168.50.3	135	tcp	msrpc	open	Microsoft Windows	RPC
192.168.50.4	139	tcp	netbios-ssn	open	Microsoft Windows	netbios-ssn
192.168.50.4	445	tcp	microsoft-ds	open		
192.168.50.4	135	tcp	msrpc	open	Microsoft Windows	RPC
192.168.50.5	139	tcp	netbios-ssn	open	Microsoft Windows	netbios-ssn
192.168.50.5	445	tcp	microsoft-ds	open		
192.168.50.5	3389	tcp	ms-wbt-server	open	Microsoft Terminal Service	
192.168.50.5	135	tcp	msrpc	open	Microsoft Windows	RPC
192.168.50.12	22	tcp	ssh	open	OpenSSH	9.7p1 Debian 7 protocol 2.0
192.168.50.133						

Abbildung 86: „Hosts im Netz“

6.3. Prometheus/Grafana

6.3.1. Theorie

6.3.1.1. Was ist Prometheus?

Prometheus ist ein Open-Source-Überwachungstool, das auf Metriken basiert und speziell für die Überwachung von Anwendungen und Infrastruktur entwickelt wurde. Es ermöglicht

die Erfassung und Analyse von Leistungsdaten wie CPU-Auslastung, Speichernutzung und Netzwerkauslastung, was dabei hilft, die Effizienz und Stabilität von IT-Systemen zu gewährleisten. Durch seine flexible Architektur und die Möglichkeit der Integration in verschiedene Systeme ist Prometheus ein wertvolles Werkzeug für Entwickler und IT-Administratoren, um die Gesundheit ihrer Systeme zu überwachen und Probleme frühzeitig zu erkennen.

6.3.1.2. Was ist Grafana?

Grafana ist ein Open-Source-Tool, das speziell dafür entwickelt wurde, Daten aus Prometheus grafisch darzustellen. Es ermöglicht die Erstellung detaillierter Dashboards, die in Echtzeit Einblicke in die Leistung von Systemen wie CPU-Auslastung und Speichernutzung bieten. Mit Grafana können Benutzer Alarne einrichten, um schnell auf ungewöhnliche Aktivitäten reagieren zu können. Es ist das perfekte grafische Tool zur Ergänzung von Prometheus und ein unverzichtbares Werkzeug für IT-Administratoren und Entwickler, die ihre Systemüberwachung optimieren möchten.

6.3.2. Installation

6.3.2.1. Grundkonfiguration Prometheus Server

Die folgenden Konfigurationen wurden auf dem Ubuntu Server bzw. auf dem Prometheus eingefügt.

```
1 hostnamectl hostname Prometheus
2
3 sudo nano /etc/netplan/00-installer-config.yaml
4 network:
5   version: 2
6   renderer: networkd
7   ethernets:
8     LAN1:
9       addresses:
10      - 192.168.10.100/24
11       routes:
12         - to: default
13           via: 192.168.10.1
14       match:
15         macaddress: 00:0c:29:46:22:de
16       set-name: LAN1
17
18 sudo netplan apply
```

Mit dieser Konfiguration werden die Netzwerk Einstellungen festlegt.

6.3.2.2. Installation Prometheus

Anschließend wird auf dem Prometheusserver die verschiedenen Dienste für Prometheus installiert.

```
1 wget https://github.com/prometheus/prometheus/releases/download/v2.51.1/
2   prometheus-2.51.1.linux-amd64.tar.gz # Installieren von Prometheus
3 tar xzf prometheus-2.51.1.linux-amd64.tar.gz # entpacken der Datei
4 mv prometheus-2.51.1.linux-amd64 /etc/prometheus # verschieben der Datei
5 in den Ordner /etc/prometheus
6
7 nano /etc/systemd/system/prometheus.service
8 [Unit]
9 Description=Prometheus
10 Wants=network-online.target
11 After=network-online.target
12 [Service]
13 ExecStart=/etc/prometheus/prometheus --config.file=/etc/prometheus/
14   prometheus.yml
15 Restart=always
16 [Install]
17 WantedBy=multi-user.target
```

Hier wird der Prometheus Server installiert und die Konfiguration wird in der Datei /etc/prometheus/prometheus.yml festgelegt. Anschließend wird ein Service erstellt, der den Prometheus Server startet.

Mit den Befehlen:

```
1 systemctl daemon-reload
2 systemctl restart prometheus
3 systemctl enable prometheus
4 systemctl status prometheus
```

werden die **Services** neugestartet.

```
1 /etc/prometheus/prometheus --config.file=/etc/prometheus/prometheus.yml #
2 Starte den Prometheus Server mit einer bestimmten Konfigurationsdatei
```

Anschließend kann in der Konfigurationsdatei Jobs angelegt werden auf denen der Node Explorer installiert worden ist.

```

1 nano /etc/prometheus/prometheus.yml # A scrape configuration containing
2 exactly one endpoint to scrape from node_exporter running on a host:
3   scrape_configs: # The job name is added as a label `job=<job_name>` to any
4     timeseries scraped from this config.
5     - job_name: 'node'
6       # metrics_path defaults to '/metrics'
7       # scheme defaults to 'http'.
8       static_configs:
9         - targets: ['localhost:9100']
10      systemctl restart prometheus
11      systemctl status prometheus

```

6.3.2.3. Überprüfen des Web-Zugriffs

Danach sollte unter der :9090 der Prometheus Server erreichbar sein.

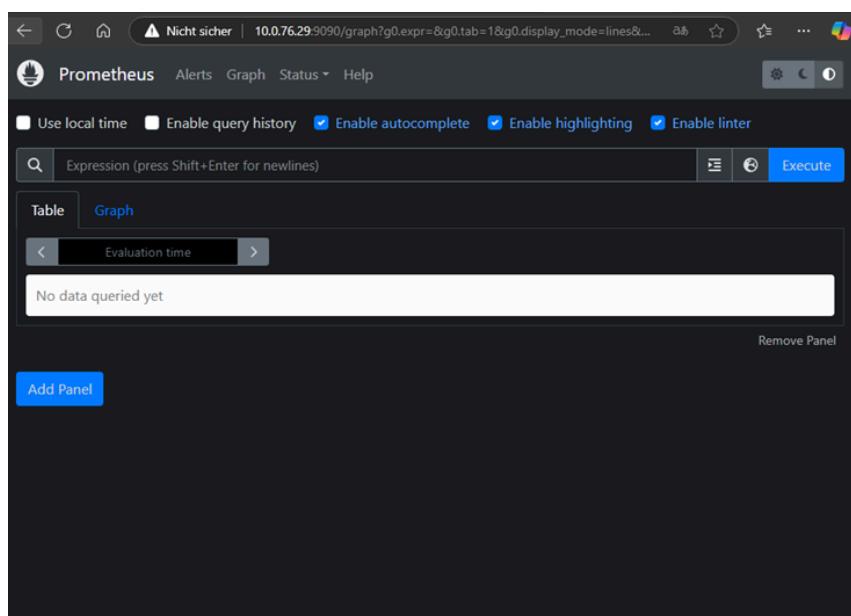


Abbildung 87: Prometheus Web Access

6.3.2.4. Installation Grafana

```

1 sudo apt-get install -y adduser libfontconfig1 musl # Installation von
2 Installation der Abhängigkeiten für Grafana
3 wget https://dl.grafana.com/enterprise/release/grafana-enterprise_10.4.1_
4 amd64.deb # installation von Grafana
5
6 sudo apt install musl # Installation von musl
7
8 sudo dpkg -i grafana-enterprise_10.4.1_amd64.deb # Entpacken der Datei

```

Durch folgende Befehle wird der Grafana Server gestartet und aktiviert.

```
1 sudo systemctl restart grafana-server
2 sudo systemctl enable grafana-server
3 sudo systemctl status grafana-server
```

6.3.2.5. Node Explorer Ubuntu

Damit wir Server auf dem Dashboard anzeigen lassen können, müssen wir auf den Geräten den Node_exporter einrichten. Folgenden Befehle werden dafür ver-wendet.

```
1 wget https://github.com/prometheus/node_exporter/releases/download/v1.7.0/node_exporter-1.7.0.linux-amd64.tar.gz # Download von Node_exporter
2 tar xzf node_exporter-1.7.0.linux-amd64.tar.gz # Entpackung der Datei
3 mv node_exporter-1.7.0.linux-amd64 /etc/node_exporter # # Verschieben der
4 Datei in den Ordner /etc/node_exporter
5 nano /etc/systemd/system/node_exporter.service # Erstellen der Service
6 Datei
7 [Unit]
8 Description=Node Exporter
9 Wants=network-online.target
10 After=network-online.target
11 [Service]
12 ExecStart=/etc/node_exporter/node_exporter
13 Restart=always
14 [Install]
15 WantedBy=multi-user.target
```

Durch folgende Befehle wird der Node Exporter gestartet und aktiviert.

```
1 systemctl daemon-reload
2 systemctl restart node_exporter
3 systemctl enable node_exporter
4 systemctl status node_exporter
```

6.3.3. Dashboard einrichten

Damit die Metriken von den Maschinen in numerische Werte umgewandelt werden, muss ein neues Dashboard angelegt werden. Dazu wird unter **Dashboard > New > Import** kann ein benutzerdefiniertes Dashboard oder ein vorgefertigtes Dashboard importierte werden. Mit der Dashboard ID: 1860 sieht das Dashboard wie folgt aus:

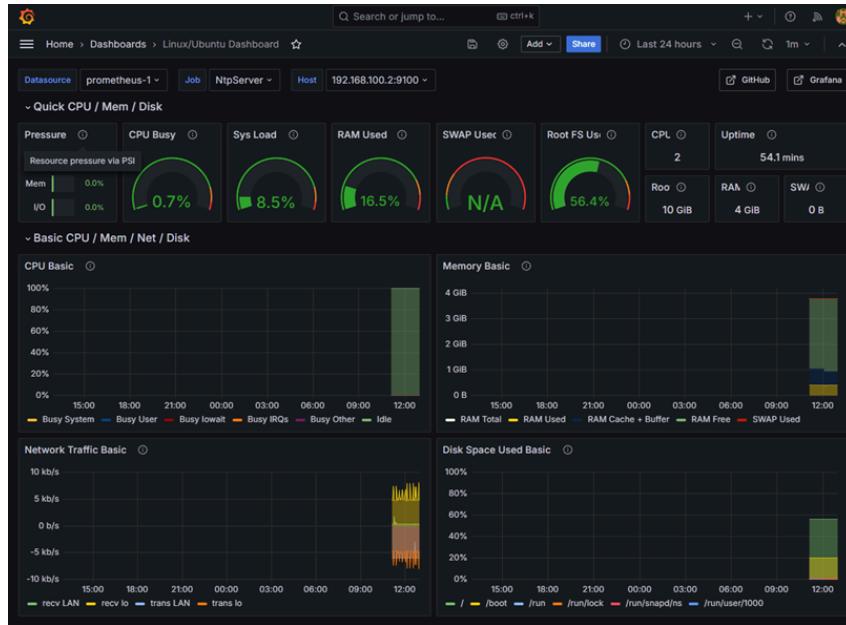


Abbildung 88: Linux/Ubuntu Dashboard

Unter dem Reiter Jobs können die verschiedenen Geräte ausgewählt werden, die davor in der prometheus.yml Datei angelegt wurden. Nach der Konfiguartion des Dashboards kann man Alerts festlegen, die in unserem Fall die CPU-Auslastung überwacht.

6.3.4. Alerts

In Grafana gibt es verschiedene Zustände für Alarmregeln und deren Instanzen, die den aktuellen Status eines Alarms widerspiegeln:

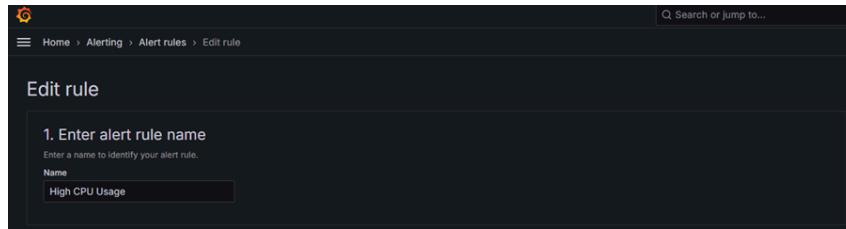


Abbildung 89: Regel Namen festlegen

The screenshot shows the 'Define query and alert condition' step in Grafana. It includes a query editor for Prometheus, a metric selector for 'process_cpu_seconds_total', a label filter for 'job' set to 'NtpServer', and a threshold-based alert condition where the value is checked against 0.3.

Abbildung 90: Regel definieren

In dieser Abbildung ist zu erkennen, dass die CPU Auslastung ausgewertet wird. Falls die Auslastung über 0.3 liegt, wird ein Alert erstellt.

The screenshot shows the 'Set evaluation behavior' step in Grafana. It allows setting the folder ('Alerts') and evaluation group ('CPU Usage Group') for the rule, as well as defining a pending period of 0s and pausing the evaluation.

Abbildung 91: Ordner festlegen

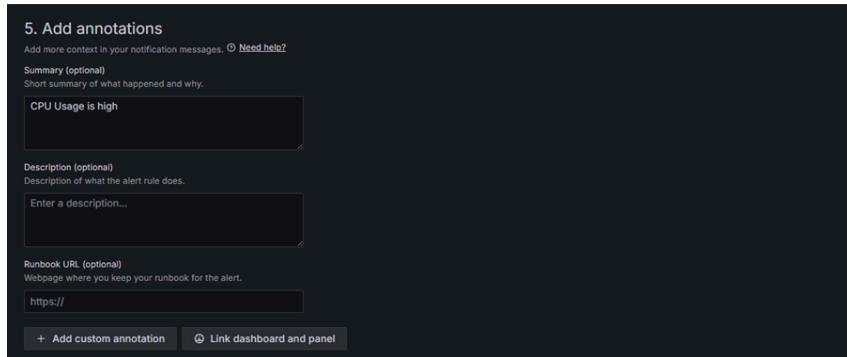


Abbildung 92: Dashboard und Link festlegen

Nachdem die Regel konfiguriert wurde kann anschließend noch ein Alert Manager eingebunden werden. Der Alert Manager ist ein System, das es ermöglicht, Benachrichtigungen über Alerts zu senden.

6.3.5. Alert Manager

Der Alert Manager wurde lokal auf der Prometheus Maschine installiert. Die Konfiguration des Alert Managers wird in der Datei `prometheus.yml` beschrieben.

```

1 wget https://github.com/prometheus/alertmanager/releases/download/v0.23.0/
2 alertmanager-0.23.0.linux-amd64.tar.gz # Download von Alert Manager
3 tar -xvf alertmanager-0.23.0.linux-amd64.tar.gz # Entpacken
4 sudo mkdir -p /alertmanager-data /etc/alertmanager
5 sudo mv alertmanager-0.23.0.linux-amd64/alertmanager /usr/local/bin/ #
6 Verschieben der Datei
7 sudo mv alertmanager-0.23.0.linux-amd64/alertmanager.yml /etc/
     alertmanager/ # Verschieben der Datei

```

Durch folgende Befehle wird der Alert Manager gestartet und aktiviert.

```

1 sudo systemctl enable alertmanager.service
2 sudo systemctl start alertmanager.service
3 sudo systemctl status alertmanager.service

```

AlertManager in Prometheus integrieren

```

1 sudo nano /etc/prometheus/prometheus.yml

```

```

2 # my global config
3 global:
4     scrape_interval: 15s # Set the scrape interval to every 15 seconds.
5     Default is every 1 minute.
6     evaluation_interval: 15s # Evaluate rules every 15 seconds. The default
7     is every 1 minute.
8     # scrape_timeout is set to the global default (10s).
9
10 # Alertmanager configuration
11 alerting:
12     alertmanagers:
13         - static_configs:
14             - targets:
15                 - alertmanager:9093

```

Abschließend muss das Prometheus Service neu gestartet werden.

```
1 sudo systemctl restart prometheus.service
```

6.3.6. Testen

Wenn man jetzt den NTP-Server neustartet geht die CPU Auslastung hoch und wir bekommen zweimal einen Alert. In Grafana steht Firing, dass beschreibt das sich eine Alarminstanz in Alerting befindet. In Grafana ist diese Nachricht bei den Alerts zu sehen.

The screenshot shows the Grafana Alert rules interface. At the top, there's a search bar and filters for 'Dashboard', 'State' (Firing), 'Rule type' (Alert), and 'Health'. Below this, a table lists alerts. There is one entry:

State	Name	Health	Summary	Next evaluation	Actions
Firing	for 43m	ok	CPU Usage is high	in 2 minutes	More

At the bottom left, it says 'Mimir / Cortex / Loki' and 'No rules found.'.

Abbildung 93: Alert ist im Zustand Firing

Unter der <IP-Adresse>:9093 können wir sehen, dass es einen neuen Alert gibt unter der Instanz 192.168.100.2. Der nachfolgende Screenshot zeigt diesen Alert.

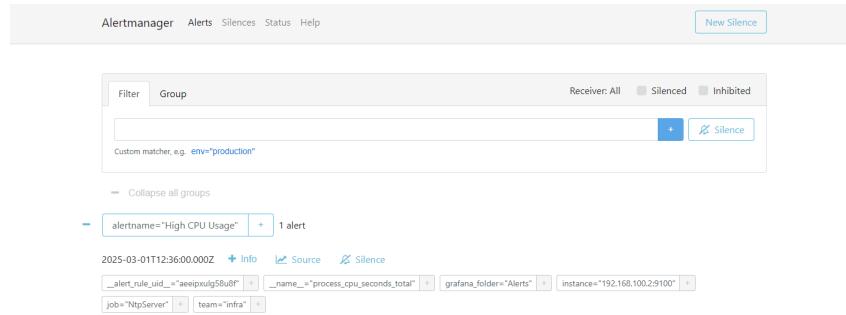


Abbildung 94: Alertmanager Alert

6.4. Wireguard VPN

Wireguard ist eigenen Angaben zufolge schneller, simpler, schlanker und nützlicher als IPsec. Verglichen zu OpenVPN hat es eine höhere Performance. Richte einen abgesicherten Wireguard Server und Client mit Skripten unter Ubuntu ein (IPv4 und IPv6) und messe den Datendurchsatz (mit iperf) und die Prozessorauslastung. Zum Schluss besitzt du Skripte für die rasche und sichere Konfiguration von Server und Clients.

6.4.1. WG-Client

```
1 sudo hostnamectl hostname WG-Client
```

6.4.2. WG-Server

```
1 sudo hostnamectl hostname WG-Server
```

6.4.2.1. Netzwerkkonfiguration

```
1 sudo nano /etc/netplan/.yaml
2 network:
3   ethernets:
4     ens33:
5       dhcp4: no
6       addresses:
7         - 192.168.159.251/24
8       routes:
9         - to: default
10        via: 192.168.159.2
11      nameserver:
12        addresses: [8.8.8.8, 8.8.4.4]
```

```
13      version: 2
14  sudo netplan apply
```

Mit den obigen Befehlen wird die Netzwerkkonfiguration für den Server und den Client konfiguriert. Der Server erhält die IP-Adresse **192.168.159.251** und der Client wird über DHCP konfiguriert.

6.4.3. Wireguard Installation

6.4.3.1. Server

Kommen wir anschließend zu der Konfiguration des Wireguard Servers. Zuerst installieren wir Wireguard auf dem Server.

```
1  sudo apt update
2  sudo apt install wireguard
```

Daraufhin erstellen wir einen privaten und öffentlichen Schlüssel für den Server und versichern uns, dass niemand außer der Owner auf den Schlüssel zugreifen kann.

```
1  unmask 077
2  wg genkey > privatekey # Private-key erstellen und in Datei speichern
3  wg pubkey < privatekey > publickey # public-key erstellen und in Datei
   speichern
```

Anschließend erstellen wir die Konfigurationsdatei für den Server.

```
1  [Interface]
2  # Interfaces wg0 configuration
3  PrivateKey = GL0pF34wB8duF5ogv5Ze/IbStlDi+j1GwkGKem+ExlY=
4  ListenPort = 51820
5  Address = 172.16.99.254/24, fd00::254/64 # Server-IP-Adresse
6
7  [Peer]
8  # WG-Client
9  PublicKey = WuGzEf7E+seUcJ3aih+uykqGcHeptIiJqab+1xaSfgQ= # Public-key des
   Clients
10 AllowedIps = 172.16.99.1/32, fd00::1/128 # Erlaubte IP-Adressen
```

Die Konfigurationsdatei für den Server wird in der Datei **wg0.conf** gespeichert.

6.4.4. Wireguard starten

Zum Starten von Wireguard auf dem Server und dem Client wird der folgende Befehl verwendet.

```
1 sudo wg-quick up wg0 # Zum Starten von Wireguard
2 sudo wg-quick down wg0 # Zum Stoppen von Wireguard
3 sudo systemctl enable wg-quick@wg0 # Autostart von Wireguard
```

6.4.5. Überprüfung

Mithilfe des Befehls `wg show` kann überprüft werden, ob die Verbindung zwischen Server und Client erfolgreich hergestellt wurde. Folgender Screenshot zeigt die Ausgabe des Befehls.

```
morris@WGServer:~$ sudo wg show
interface: wg0
    public key: LVp4G0xoVnY2ZlsVnsdjkxE/8+G97JldZhPrRggXNrTs=
    private key: (hidden)
    listening port: 51820

    peer: WuGzEf7E+seUcJ3aih+uykqGcHeptIiJqab+1xaSfgQ=
        endpoint: 192.168.159.249:60671
        allowed ips: 172.16.99.1/32, fd00::1/128
        latest handshake: 37 minutes, 2 seconds ago
        transfer: 692 B received, 604 B sent
```

Abbildung 95: Wireguard Verbindung

Auf der Abbildung kann man erkennen, dass die Verbindung zwischen Server und Client erfolgreich hergestellt wurde. Der letzte Handshake war in diesem Fall vor 37 Minuten und 2 Sekunden.

Da wir auch eine IPv6 Verbindung konfiguriert haben, können wir auch die IPv6 Verbindung testen. Dafür verwenden wir den Befehl `ping fd00::1`

```
morris@WGServer:~$ ping fd00::1
PING fd00::1(fd00::1) 56 data bytes
64 bytes from fd00::1: icmp_seq=1 ttl=64 time=2.46 ms
64 bytes from fd00::1: icmp_seq=2 ttl=64 time=1.43 ms
64 bytes from fd00::1: icmp_seq=3 ttl=64 time=1.30 ms
64 bytes from fd00::1: icmp_seq=4 ttl=64 time=1.76 ms
64 bytes from fd00::1: icmp_seq=5 ttl=64 time=1.14 ms
```

Abbildung 96: IPv6 Verbindung

6.5. Syslog Server Linux

6.5.1. Setup

Da Cisco-Router und Switches nicht kompatibel mit systemd sind verwendet wird als Syslog-Server. Dieser wird auf einem Linux-Server installiert.

6.5.2. Konfiguration

Zuerst wird mit dem Befehl `apt-get install syslog-ng` syslog-ng installiert. Anschließend wird die Konfigurationsdatei `/etc/syslog-ng/syslog-ng.conf` angepasst. Hier ein Beispiel:

```
#log { source(s_src); destination(d_net); };
source s_net { tcp(); udp(); };
destination d_file { file("/var/log/network.log"); };
log { source(s_net); destination(d_file); };
```

Abbildung 97: Änderungen in der syslog-ng.conf

Daraufhin wird der syslog-ng Service mit `systemctl restart syslog-ng` neu gestartet. Der Router auf dem in der Zwischenzeit die Interfaces konfiguriert wurden, wird nun so konfiguriert, dass er die Syslog-Meldungen an den Syslog-Server sendet.

```
R1(config)#logging 192.168.0.2
R1(config)#
*Feb 18 18:48:00.556: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.0.2 port 514 started - CLI initiated
```

Abbildung 98: Logging Cisco Router

Abschließend werden die Syslog Messages an den Syslog-Server geschickt. Diese können mit dem `cat` Befehl angezeigt werden.

```
morris@LSRV01:~$ cat /var/log/network.log
Feb 18 18:48:00 192.168.0.1 %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.0.2 port 514 start
ed - CLI initiated
morris@LSRV01:~$
```

Abbildung 99: Logging Linux Server

6.6. Linux Firewall mit iptables

iptables ist ein Paketfilter-Firewall-Framework für den Linux-Kernel. Es ermöglicht die Kontrolle des Netzwerkverkehrs basierend auf vordefinierten Regeln. iptables arbeitet auf der Netzwerkebene und nutzt verschiedene Tabellen und Chains zur Verarbeitung von Paketen.

6.6.1. Konfiguration

Die Firewall dient für die Verbindung zwischen den Standorten via Wireguard sowie NAT.

```
1  #!/bin/bash
2  # iptables binary
3  IPT="/sbin/iptables"
4
5  # delete old config
6  $IPT -F
7  $IPT -X
8
9  # set default policy
10 $IPT -P INPUT DROP
11 $IPT -P OUTPUT DROP
12 $IPT -P FORWARD DROP
13
14 # interfaces (intern, extern, DMZ)
15 INT=ens33
16 EXT=ens37
17 wg=wg0
18
19 # allow ongoing connections
20 $IPT -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
21 $IPT -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
22 $IPT -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
23
24 # allow loopback
25 $IPT -A INPUT -i lo -j ACCEPT
26 $IPT -A OUTPUT -o lo -j ACCEPT
27
28 # create own chains
29 $IPT -N int_to_ext
30 $IPT -N wg_to_int
31 $IPT -N int_to_wg
32
33 # divide traffic
34 $IPT -A FORWARD -i $INT -o $EXT -j int_to_ext
35 $IPT -A FORWARD -i $wg -o $INT -j wg_to_int
36 $IPT -A FORWARD -i $INT -o $wg -j int_to_wg
37
38 ### traffic from intern to extern
39 $IPT -A int_to_ext -m state --state NEW -p tcp -m multiport --dport
40 http,https -j ACCEPT
41 $IPT -A int_to_ext -m state --state NEW -p tcp --dport domain -j ACCEPT
42 $IPT -A int_to_ext -m state --state NEW -p udp --dport domain -j ACCEPT
```

```

42 $IPT -A int_to_ext -m state --state NEW -p udp --dport ntp -j ACCEPT
43 $IPT -A int_to_ext -m state --state NEW -p icmp -j ACCEPT
44 $IPT -A int_to_ext -j REJECT
45
46 ### traffic from wireguard into intern
47 $IPT -A wg_to_int -m state --state NEW -p tcp -m multiport --dport
48 http,https,3000,9090 -j ACCEPT
49 $IPT -A wg_to_int -m state --state NEW -p tcp --dport domain -j ACCEPT
50 $IPT -A wg_to_int -m state --state NEW -p udp --dport domain -j ACCEPT
51 $IPT -A wg_to_int -m state --state NEW -p udp --dport ntp -j ACCEPT
52 $IPT -A wg_to_int -m state --state NEW -p icmp -j ACCEPT
53 $IPT -A wg_to_int -m state --state NEW -p tcp --dport 22 -j ACCEPT
54 $IPT -A wg_to_int -m state --state NEW -p udp --dport 22 -j ACCEPT
55 $IPT -A wg_to_int -j REJECT
56
57 ### traffic from intern to wireguard
58 $IPT -A int_to_wg -m state --state NEW -p tcp -m multiport --dport
59 http,https,3000,9090 -j ACCEPT
60 $IPT -A int_to_wg -m state --state NEW -p tcp --dport domain -j ACCEPT
61 $IPT -A int_to_wg -m state --state NEW -p udp --dport domain -j ACCEPT
62 $IPT -A int_to_wg -m state --state NEW -p udp --dport ntp -j ACCEPT
63 $IPT -A int_to_wg -m state --state NEW -p icmp -j ACCEPT
64 $IPT -A int_to_wg -m state --state NEW -p tcp --dport 22 -j ACCEPT
65 $IPT -A int_to_wg -m state --state NEW -p udp --dport 22 -j ACCEPT
66 $IPT -A int_to_wg -j REJECT
67
68 ### rules for the fw
69 # incoming
70 $IPT -A INPUT -m state --state NEW -p icmp -j ACCEPT
71 $IPT -A INPUT -m state --state NEW -p tcp --dport 22 -j ACCEPT
72 $IPT -A INPUT -m state --state NEW -p udp --dport 22 -j ACCEPT
73 $IPT -A INPUT -m state --state NEW -p udp --dport 51820 -j ACCEPT
74
75 # outgoing
76 $IPT -A OUTPUT -o $EXT -j ACCEPT
77 $IPT -A OUTPUT -o $EXT -m state --state NEW -p tcp -m multiport --dport
78 http,https -j ACCEPT
79 $IPT -A OUTPUT -o $EXT -m state --state NEW -p tcp --dport domain -j
80 ACCEPT
81 $IPT -A OUTPUT -o $EXT -m state --state NEW -p udp --dport domain -j
82 ACCEPT
83 $IPT -A OUTPUT -o $EXT -m state --state NEW -p udp --dport ntp -j ACCEPT
84 $IPT -A OUTPUT -o $EXT -m state --state NEW -p icmp -j ACCEPT
85
86 # nat
87 $IPT -t nat -A POSTROUTING -o outside -j MASQUERADE

```

6.7. Apparmor

Das Ziel dieses Labs ist es, einen TFTP-Server aufzusetzen, der zur Sicherung von Konfigurationsdateien genutzt wird. Zusätzlich wird der Server mit AppArmor abgesichert, indem ein

eigenes AppArmor-Profil erstellt wird. AppArmor ist eine Sicherheitslösung in Linux, die den Zugriff auf Dateien und Systemressourcen für Anwendungen einschränkt.

6.7.1. Konfiguration des TFTP-Servers

Installation des Dienstes:

```
1 sudo apt install tftpd-hpa
```

Bearbeiten der Konfigurationsdatei:

```
1 sudo nano /etc/default/tftpd-hpa
2 TFTP_USERNAME="tftp"
3 TFTP_DIRECTORY="/srv/tftp"
4 TFTP_ADDRESS="0.0.0.0:69"
5 TFTP_OPTIONS="--secure --create"
```

Rechte Setzen:

```
1 sudo chmod -R 777 /srv/tftp
2 sudo chown -R tftp:tftp /srv/tftp
```

6.7.2. Überprüfung

TFTP-Client

```
1 tftp 192.168.0.1
2 put testfile.txt
3 quit
```

TFTP-Server

Damit ein neues Profil für den TFTP-Server erstellt werden kann, muss das Profil des TFTP-Servers generiert werden. Dazu wird der Server gestartet und der Zugriff auf die Dateien überprüft.

```
1 sudo aa-genprof in.tftpd
```

```
Profile: /usr/sbin/in.tftpd
Path: /srv/tftp/testfile.txt
New Mode: rk
Severity: 4

1 - /srv/tftp/testfile.txt rk,
[2 - /srv/tftp/* rk,]
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / Abo(r)t / (F)inish
```

Abbildung 100: Gehärtetes TFTP-System