Unternehmensnetzwerkdesign
mit VLAN-Segmentierung, DMZ und GLBP

Philip Rojek

1) **Einleitung:**
   - Kurzbeschreibung des Projekts
   - Ziele des Netzwerks

2) **Netzwerkübersicht:**
   - Diagramm der Netzwerktopologie
   - Allgemeine Beschreibung der Netzwerktopologie

3) **Netzwerktopologie**
   - Detaillierte Beschreibung der Core-Switches, Access-Switches, Router, Firewall und DMZ
   - Erklärungen zu Trunk- und Access Ports
   - Erklärung der VLAN Struktur

4) **Netzwerkkonfigurationen**
   - Core-Switches (SVIs, GLBP, OSPF)
   - Access-Switches
   - Router (PAT, OSPF)
   - Firewall (Standard Paketinspektion)

5) **Sicherheitsmaßnahmen**
   - Beschreibung der SSH-Sicherheitsmaßnahmen für den Fileserver
   - Erklärung der Access Control Lists

1. Einleitung

Dieses Projekt beschreibt die Planung und Implementierung eines Testnetzwerks in GNS3 für ein kleines Unternehmen, das als Demonstration meiner Fähigkeiten und Kenntnisse im Bereich Netzwerktechnik dient. Das Netzwerk umfasst wesentliche Komponenten wie einen FTP-Server und einen Webserver, die für experimentelle Zwecke genutzt werden. Um das Design übersichtlich zu halten, repräsentieren die wenigen Client-Geräte in jedem VLAN eine größere Anzahl von Endbenutzern im echten Betrieb.

Das Hauptziel dieses Netzwerks ist es, grundlegende Netzwerkfunktionen und -technologien in einem realistischen, aber kontrollierten Umfeld zu demonstrieren. Dabei werden insbesondere die folgenden Aspekte hervorgehoben:

- **Segmentierung des Netzwerks durch VLANs:** Die Implementierung von VLANs (Virtual Local Area Networks) zur logischen Trennung der verschiedenen Abteilungen im Unternehmen (SALES, HR, IT und DMZ). Dies verbessert die Sicherheit und Verwaltung des Netzwerks erheblich.

- **Lastverteilung und Redundanz mit GLBP:** Die Nutzung des Gateway Load Balancing Protocol (GLBP) für die Lastverteilung und Redundanz. GLBP sorgt dafür, dass der Datenverkehr gleichmäßig auf die Core-Switches verteilt wird und bei einem Ausfall eines Switches die Verfügbarkeit erhalten bleibt.

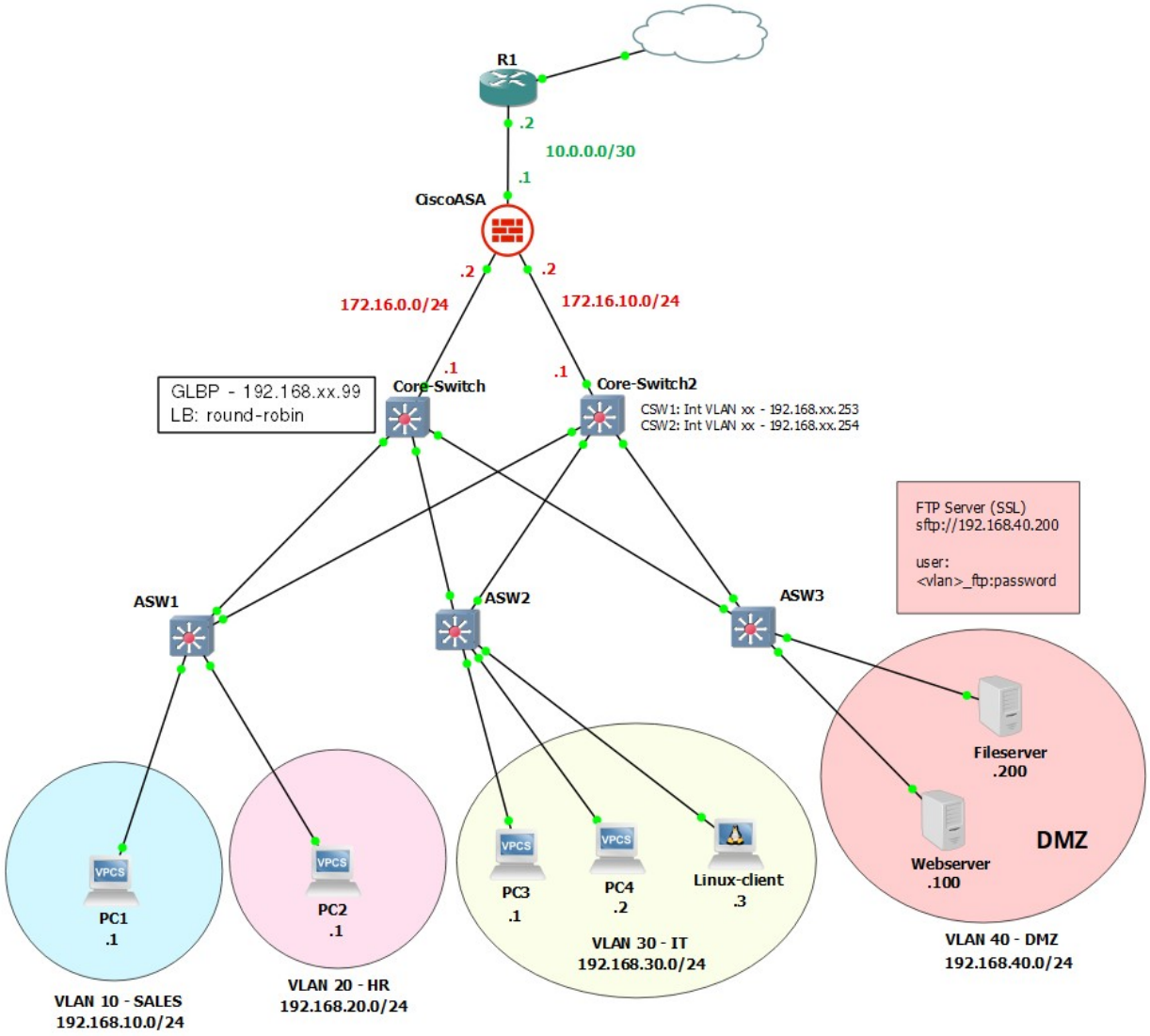
- **Sicherer Zugriff auf den FTP-Server:** Der FTP-Server ist mit vsftpd konfiguriert und durch SSL-Zertifikate gesichert, sodass nur verschlüsselte Verbindungen zugelassen werden. Dies stellt sicher, dass sensible Daten geschützt übertragen werden.

- **Firewall-Sicherheit und Paketinspektion:** Die Cisco ASA-Firewall übernimmt die Standard-Paketinspektion und bietet eine zusätzliche Sicherheitsebene. Sie kontrolliert den ein- und ausgehenden Datenverkehr und schützt das Netzwerk vor potenziellen Bedrohungen.

- **Access Control Lists (ACLs) in der DMZ:** Eine ACL auf den Core-Switches beschränkt den Zugriff auf die Server in der demilitarisierten Zone (DMZ) auf lokale Hosts, was die Sicherheit erhöht.

2. Netzwerkübersicht

Die folgende Netzwerktopologie zeigt strukturierte und ausfallsichere Design des Testnetzwerks, das zur Demonstration moderner Netzwerktechnologien für ein kleines Unternehmen erstellt wurde.



Allgemeine Beschreibung der Netzwerktopologie

Die dargestellte Netzwerktopologie besteht aus einem zentralen Router, einer Firewall, zwei Core-Switches und drei Access-Switches. Diese Komponenten sind miteinander verbunden, um Redundanz und Ausfallsicherheit zu gewährleisten.

Das Netzwerk ist in verschiedene VLANs unterteilt, die die verschiedenen Abteilungen des Unternehmens repräsentieren: SALES, HR, IT und DMZ. Die Core-Switches sind mit GLBP für Lastverteilung und Redundanz konfiguriert, während die Access-Switches die Endgeräte der jeweiligen VLANs verbinden. Der FTP-Server und der Webserver befinden sich in der DMZ und sind durch eine Access Control List (ACL) auf lokale Hosts beschränkt, was die Sicherheit erhöht. Die Firewall übernimmt die Standard-Paketinspektion und schützt das Netzwerk vor externen Bedrohungen.

3. Netzwerktopologie

Die dargestellte Netzwerktopologie wurde entwickelt, um die grundlegenden Netzwerkdienste eines kleinen Unternehmens zu unterstützen, wobei besonderes Augenmerk auf Redundanz, Lastverteilung und Sicherheit gelegt wurde. Die allgemeine Struktur des Netzwerks umfasst folgende Komponenten:

Core-Switches:

- **Core-Switch1 und Core-Switch2:** Diese beiden Switches bilden das Rückgrat des lokalen Netzwerks und sind über Trunk-Ports, die über die Access-Switches laufen, miteinander verbunden. Sie bieten redundante Pfade und erhöhen die Ausfallsicherheit des Netzwerks. Auf den Core-Switches sind Switch Virtual Interfaces (SVIs) für jedes VLAN konfiguriert, die als Standard-Gateways fungieren. GLBP (Gateway Load Balancing Protocol) ist auf diesen SVIs mit Round-Robin-Load-Balancing konfiguriert, wobei Core-Switch1 der Active Virtual Gateway (AVG) ist. Core-Switch1 hat eine höhere Priorität (120) auf allen VLANs, während Core-Switch2 eine niedrigere Priorität (90) hat.

Access-Switches:

- **ASW1, ASW2, ASW3:** Diese Access-Switches verbinden die Endgeräte (PCs, Server) mit dem Netzwerk. Jeder Access-Switch ist über Trunk-Ports sowohl mit Core-Switch1 als auch mit Core-Switch2 verbunden, was die Netzwerkstabilität durch redundante Verbindungen erhöht. Die Trunk-Ports erlauben nur die vorhandenen VLANs, und das Native VLAN wurde aus Sicherheitsgründen auf 99 geändert, um VLAN-Hopping-Angriffe zu vermeiden. Die Ports auf der Host-Seite der Access-Switches sind als Access-Ports konfiguriert, um die jeweiligen VLANs den Endgeräten zuzuweisen.

Routing und Redundanz:

- **OSPF (Open Shortest Path First):** Auf den Core-Switches, der Firewall und dem Router ist OSPF konfiguriert, um dynamisches Routing und schnelle Konvergenz im Netzwerk zu gewährleisten. Dies stellt sicher, dass im Falle eines Ausfalls eines Core-Switches oder eines anderen Routers die Netzwerkrouten schnell aktualisiert und angepasst werden.

Firewall

- Die Cisco ASA-Firewall bietet eine zusätzliche Sicherheitsebene und ist für die Standard-Paketinspektion konfiguriert. Sie ist mit dem Core-Switch und dem Router verbunden, um den ein- und ausgehenden Datenverkehr zu überwachen und zu kontrollieren.

Router und Port Address Translation (PAT)

- Der Router R1 verbindet das interne Netzwerk mit externen Netzwerken, wie dem Internet. Auf dem Router ist Port Address Translation (PAT) konfiguriert, wodurch Hosts aus den lokalen Netzwerken über die IP-Adresse der Schnittstelle f0/1 auf externe Netzwerke zugreifen können.

Demilitarisierte Zone (DMZ):

- Die DMZ enthält kritische Server wie den Webserver (192.168.40.100) und den Fileserver (192.168.40.200). Der Zugriff auf diese Server ist durch eine Access Control List, die auf den SVI´s von VLAN 40 (outbound), die auf beiden Core-Switches konfiguriert ist, auf lokale Hosts beschränkt, was die Sicherheit erhöht.
- Auf dem Webserver ist der Apache2-Webserver installiert, während der FTP-Server mit vsftpd konfiguriert ist. Der FTP-Zugang ist durch SSL-Zertifikate gesichert, sodass ungeschützte Verbindungen nicht zulässig sind

SSH-Zugriff auf Server

- Der SSH-Zugriff auf die beiden Server ist nur von dem Linux-Client im VLAN 30 (IT) möglich. Der Zugriff erfolgt über kryptografische Schlüssel. Die restlichen Hosts haben keinen Zugriff.

VLAN-Zuweisungen:

- Die VLANs sind logisch nach den existierenden Abteilungen im Unternehmen gegliedert:

  VLAN 10 (SALES): 192.168.10.0/24

  VLAN 20 (HR): 192.168.20.0/24

  VLAN 30 (IT): 192.168.30.0/24

  VLAN 40 (DMZ): 192.168.40.0/24

4. Netzwerkkonfigurationen

In diesem Abschnitt werden die spezifischen Konfigurationen der einzelnen Netzwerkkomponenten detailliert beschrieben. Dies umfasst die Einstellungen der Core-Switches, Access-Switches, des Routers und der Firewall.

Konfiguration der Core-Switches

- Switch Virtual Interfaces

  Jedes VLAN hat ein SVI, das als Gateway fungiert. Die IP-Adressen der SVIs von Core-Switch1 haben die Endung .253 und die von Core-Switch2 .die Endung .254.
  Zudem ist auf jedem SVI noch GLBP mit einer virtuellen IP im jeweiligen Subnetz mit der Endung .99 konfiguriert. Außerdem ist auf jedem SVI Round-Robin Lastenverteilung aktiviert.

```
interface Vlan10
 ip address 192.168.10.253 255.255.255.0
 glbp 10 ip 192.168.10.99
 glbp 10 priority 90
 glbp 10 preempt
!
interface Vlan20
 ip address 192.168.20.253 255.255.255.0
 glbp 20 ip 192.168.20.99
 glbp 20 priority 90
 glbp 20 preempt
!
interface Vlan30
 ip address 192.168.30.253 255.255.255.0
 glbp 30 ip 192.168.30.99
 glbp 30 priority 90
 glbp 30 preempt
!
interface Vlan40
 ip address 192.168.40.253 255.255.255.0
 glbp 40 ip 192.168.40.99
 glbp 40 priority 90
 glbp 40 preempt
!
```

- Open Shortest Path First (OSPF)

  OSPF wurde auf beiden Core-Switches als Routing-Protokoll konfiguriert um die Netzwerke aller SVIs und die, die an die Firewall angeschlossen sind, zu propagieren.

```
router ospf 1
 router-id 4.4.4.4
 log-adjacency-changes
 network 0.0.0.0 255.255.255.255 area 0
```

- Trunk Ports

  Die Interfaces, die an die Access-Switches angeschlossen sind, sind als Trunk-Ports konfiguriert, die nur existierende VLANS erlauben. Zudem wurde auf jedem Interface aus Sicherheitsgründen das Native-VLAN auf 99 geändert.

```
!
interface FastEthernet1/0
 switchport trunk native vlan 99
 switchport trunk allowed vlan 1,10,20,30,40,1002-1005
 switchport mode trunk
 duplex full
 speed 100
!
interface FastEthernet1/1
 switchport trunk native vlan 99
 switchport trunk allowed vlan 1,10,20,30,40,1002-1005
 switchport mode trunk
 duplex full
 speed 100
!
interface FastEthernet1/2
 switchport trunk native vlan 99
 switchport trunk allowed vlan 1,10,20,30,40,1002-1005
 switchport mode trunk
 duplex full
 speed 100
!
```

Konfiguration der Access-Switches

- Trunk und Access Ports

  Die Interfaces zu den Core-Switches sind als Trunk-Ports, die zu den Endhosts als Access-Ports mit VLAN-Zuweisung konfiguriert.

```
!
interface FastEthernet1/0
 switchport access vlan 10
 duplex full
 speed 100
!
interface FastEthernet1/1
 switchport access vlan 20
 duplex full
 speed 100
!
interface FastEthernet1/2
 switchport trunk native vlan 99
 switchport trunk allowed vlan 1,10,20,30,40,1002-1005
 switchport mode trunk
 duplex full
 speed 100
!
interface FastEthernet1/3
 switchport trunk native vlan 99
 switchport trunk allowed vlan 1,10,20,30,40,1002-1005
 switchport mode trunk
 duplex full
 speed 100
!
```

Konfiguration des Routers

- Port Address Translation

  Die IP-Adressen der VLAN-Subnetze verwenden die IP-Adresse des Outbound-Interfaces für Verbindungen zu externen Netzwerken. Die Subnetze der VLANs sind in der Standard-Access-List 1 definiert. Dabei ist das Interface F0/1 als nat outside und das Interface F0/0 als nat inside konfiguriert.

```
ip nat inside source list 1 interface FastEthernet0/1 overload
!
access-list 1 permit 192.168.0.0 0.0.255.255
```

- OSPF

  Das Netzwerk, welches ans Inbound Interface angeschlossen ist, wird außerdem in OSPF propagiert. Zudem wurde eine statische Default-Route, die über das Outbound Interface führt, festgelegt. Diese wird ebenfalls in OSPF propagiert.

```
router ospf 1
 log-adjacency-changes
 network 10.0.0.0 0.0.0.255 area 0
 default-information originate
!
```

Konfiguration der Firewall

- Festlegen der inneren und äußeren Interfaces

  Da G0/0 und G0/1 mit dem internen Netzwerk verbunden sind, sind sie als sehr vertrauenswürdig eingestuft und haben ein Security Level von 100. Das Interface G0/2 ist mit externen Netzwerken verbunden und daher als nicht vertrauenswürdig eingestuft, mit einem Security Level von 0. Dies bedeutet, dass Traffic von außen nach innen erst durch entsprechende ACLs erlaubt werden muss

```
!
interface GigabitEthernet0/0
 nameif inside1
 security-level 100
 ip address 172.16.0.2 255.255.255.0
!
interface GigabitEthernet0/1
 nameif inside2
 security-level 100
 ip address 172.16.10.2 255.255.255.0
!
interface GigabitEthernet0/2
 nameif outside
 security-level 0
 ip address 10.0.0.1 255.255.255.252
!
```

- OSPF

  Die Netzwerke, die an die Firewall angeschlossen sind, werden außerdem allesamt bei OSPF propagiert, damit die Hosts aus den VLANS eine Route zum Default Gateway (R1) haben.

```
router ospf 1
 router-id 9.9.9.9
 network 10.0.0.0 255.255.255.252 area 0
 network 172.16.0.0 255.255.255.0 area 0
 network 172.16.10.0 255.255.255.0 area 0
```

- Default Packet Inspection

  Es wurde die Default Packet Inspection global aktiviert. Dies bedeutet, dass die Firewall standardmäßig den Datenverkehr für verschiedene Protokolle inspiziert, um die Sicherheit und Integrität des Netzwerks zu gewährleisten. Hier ist die detaillierte Konfiguration:

  policy-map global_policy: Dies definiert eine globale Policy-Map namens global_policy.

  class inspection_default: Die Policy-Map verwendet die Klasse inspection_default, die eine Standardmenge an Inspektionsregeln enthält, die mit inspect beginnen.

```
policy-map global_policy
 class inspection_default
  inspect dns migrated_dns_map_1
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect ip-options
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
```

  Die letzte Zeile service-policy global_policy global wendet die global_policy auf den gesamten Datenverkehr an, der durch die Firewall fließt:

```
service-policy global_policy global
```

4. Sicherheitsmaßnahmen

In diesem Abschnitt wird erläutert, wie der Zugang zum Fileserver gesichert wurde und welche Access-Control-Lists (ACLs) im Netzwerk vorhandenvorhanden sind.

Beschreibung der SSH-Sicherheitsmaßnahmen für die Server

Um die Sicherheit des SSH-Zugangs auf dem Fileserver zu erhöhen, wurden folgende Maßnahmen in der Konfigurationsdatei /etc/ssh/sshd_config implementiert:

1. **Aktivierung der SSH-Schlüssel-Authentifizierung:** Die Authentifizierung mittels SSH-Schlüsseln wurde aktiviert, um eine sicherere Authentifizierungsmethode zu gewährleisten.

```
PubkeyAuthentication yes
```

2. **Optionale Deaktivierung des Root-Logins:** Der direkte Login als Root-Benutzer wurde deaktiviert, um die Systemsicherheit weiter zu erhöhen und den Zugriff auf privilegierte Konten zu beschränken.

```
PermitRootLogin no
```

Diese Maßnahmen helfen dabei, den SSH-Zugang zum Fileserver sicherer zu gestalten und unbefugten Zugriff zu verhindern.

Erklärung der Access-Control-Lists

Um den Zugang zu dem Web- und Fileserver auf lokale Hosts zu begrenzen wurden auf beiden Core-Switches die folgende Access-List mit dem SVI für VLAN 40 outbound verknüpft.

```
Standard IP access list 1
    10 permit 192.168.0.0, wildcard bits 0.0.255.255
```