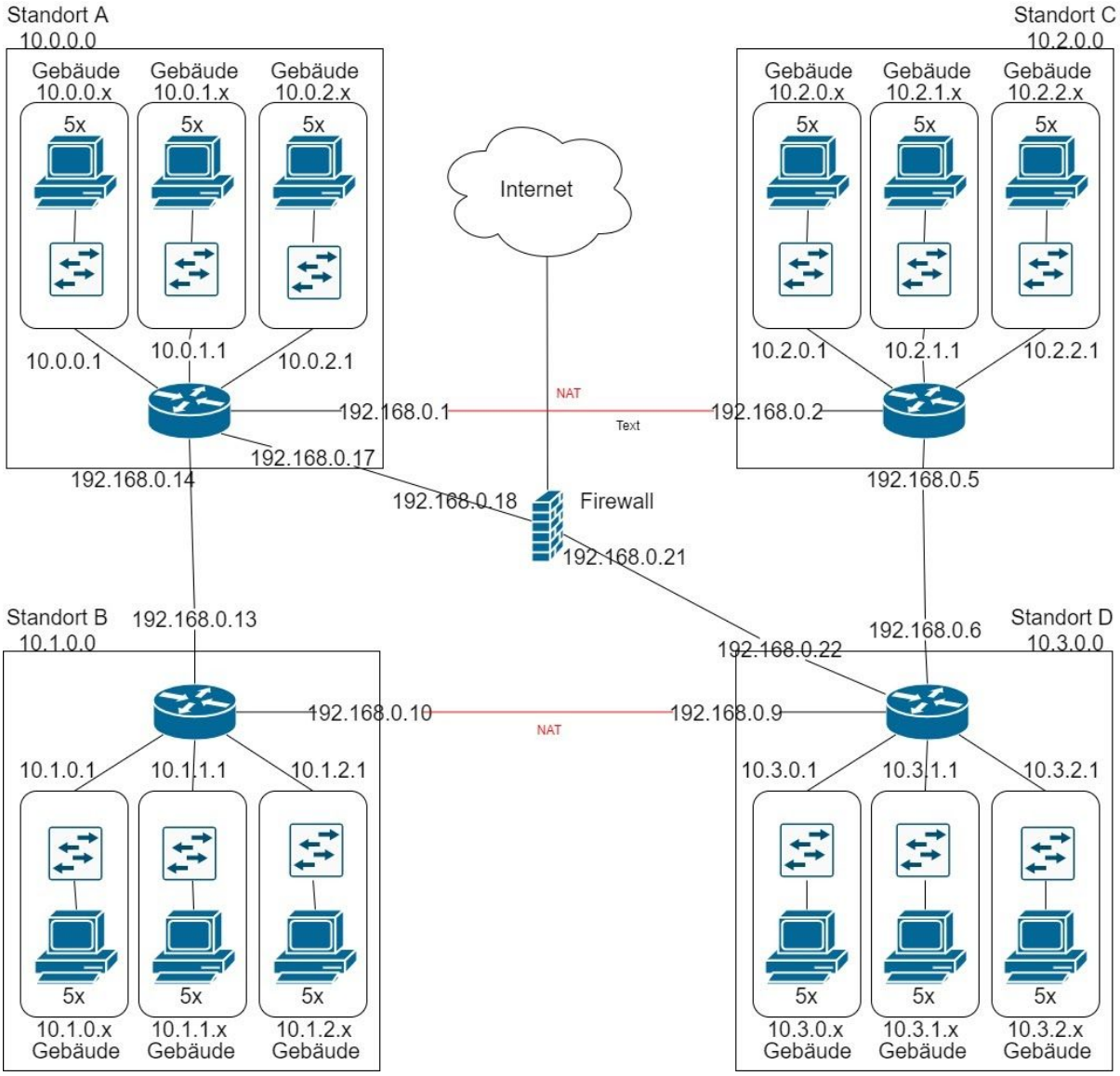
Netztechnik - Praktische Prüfungsleistung

Joshua Notheisen - 4610068
Kai Boncourt - 6380532
Simon Walz - 7765019
Silas Pohl - 7598669



Die Standorte sollen mit hoher Verfügbarkeit (Redundanz!) angebunden werden.
Innerhalb jedes Standorts existiert ein Router, welcher mit jeweils zwei anderen Standorten in Verbindung steht, damit eine hohe Verfügbarkeit gewährleistet werden kann. So ist bei einem Ausfall des Standorts die Verbindung zwischen den drei verbleibenden Standorten verfügbar. Die Wahrscheinlichkeit, dass zwei Standorte gleichzeitig ausfallen, geht gegen null.

Sichere Schnittstelle zur Konfiguration der Netzwerk-Komponenten
Zur Realisierung der sicheren Schnittstellen wird auf jedem Router R1, R2, R3, R4 SSH konfiguriert.

<u>Zentrale Aufgabe 1:</u> Namensauflösung für jedes Gerät im Netzwerk. (Silas Pohl)
Innerhalb des Unternehmensnetzwerk, wird der Router 1 (Standort A) als DNS dienen. Wir haben uns jedoch dazu entschieden auch Router 4 (Standort D) als DNS zu konfigurieren, damit eine Redundanz im Falle eines Ausfalls gewährleistet ist. Zur Überprüfung der Funktionalität des DNS vergeben wir mehrere static IP-Adressen, welchen wir jeweils Namen zuweisen.

<u>Zentrale Aufgabe 2:</u> IP-Adressen sollen Rückschluss auf den Standort und das Gebäude geben können. Adressen sollen automatisch vergeben werden. (Joshua Notheisen)
Die IP-Adressen des Netzwerks werden durch den Adressbereich 10.0.0.0 /8 realisiert. Es wurde sich für das Konzept der sprechenden IP-Adressen entschieden. Folglich sieht die Aufteilung der IP-Adressen wie folgt aus:

Name	**IP-Adressen-Range**	**CIDR-Suffix**	**Netzwerkmaske**
Standort A	10.0.0.0-10.7.0.0	/24	255.255.255.0
Standort B		/24	255.255.255.0
Standort C		/24	255.255.255.0
Standort D		/24	255.255.255.0
Gebäude 1	10.X.0.1 - 10.X.0.255	/24	255.255.255.0
Gebäude 2	10.X.1.1 - 10.X.1.255	/24	255.255.255.0
Gebäude 3	10.X.2.1 - 10.X.2.255	/24	255.255.255.0

Die Clients werden innerhalb der Gebäude mit der entsprechenden IP-Adresse versorgt, welche sich in der IP-Adressen Range des jeweiligen Gebäudes befindet. Diese Clients bekommen das CIDR-Suffix /24 und besitzen eine Netzmaske von 255.255.255.0.
Die automatische Vergabe der IP-Adressen soll über einen DHCP-Server laufen. Dieser Server weist den Clients die entsprechenden IP-Adressen innerhalb einer Range zu. Standort A-D wird jeweils 10.0.0.0 - 10.3.0.0 zuteil. Je nach Standort fällt die IP-Adresse also anders aus.
Die Verbindung zwischen den Routern und der Firewall werden jeweils in einem 192.168.0.X /30 Netz realisiert. Jede Schnittstelle bekommt hierbei eine andere IP-Adresse eines der /30 Subnetze zugewiesen.

<u>Zentrale Aufgabe 3:</u> Die Kommunikation zwischen den Standorten (A,B) und (C,D) soll maskiert erfolgen. (Kai Boncourt)

Die maskierte Verbindung erfolgt durch ein One-to-One-NAT. Also gibt es jeweils für die Standorte A & B und C & D eine IP-Adresse, welche gebündelt nach außen kommuniziert, um die privaten IP-Adressen der jeweiligen Subnetze zu schützen, bzw. zu maskieren.

<u>Zentrale Aufgabe 4:</u> Die Kommunikation zum Internet soll durch eine Firewall gesichert werden. Die einzige erlaubte Kommunikation zwischen dem Unternehmen und dem Internet soll das Surfen sein. (Simon Walz)

Beim Zugriff auf das Internet, wird jede Verbindung durch eine Firewall gespeist. Es wurde sich für die Verwendung einer Black-List entschieden, damit die Nutzer daran gehindert werden bestimmte Seiten aufzurufen. Außerdem sollen nur bestimmte Protokolle und deren Ports verwendet werden.
Dies führt dazu, dass nur HTTPS-Verbindungen über Port 443 erlaubt werden. HTTP-Verbindungen über Port 80 werden bewusst blockiert.