

Berufliches Schulzentrum für Elektrotechnik Dresden

Fachbereich Informationstechnik

Projektdokumentation

Lernfeld 9 - Projekt 3

Auftraggeber: Doubtful-Joy SE

Auftragnehmer: High-Secure GmbH - Projektteam IT20/2 Gruppe 7

Auftragsdatum: 2021.11.15

Historie:

Inhaltsverzeichnis

Abkürzungsverzeichnis

1	Pflichtenheft	1
1.1	Auftraggeber und Auftragnehmer	1
1.2	Ausgangslage	1
1.3	Projektziel	1
1.4	Funktionsspezifikation	2
1.5	Datenspezifikation	2
1.6	Schnittstellenspezifikation	4
1.7	Rahmenbedingungen	4
1.8	Qualitätsbetrachtung	5
1.9	Projektplanung	5
1.10	Kosten-Nutzen-Analyse	6
2	Auswertung und Reflexion	7
2.1	Ablaufdokumentation	7
2.2	Einrichtung IPFire	7
2.3	Einrichtung Admin-PC	8
2.4	Einrichtung DHCP-DNS-DB-Server	9
2.5	Einrichtung Webserver	9
	Abbildungsverzeichnis	10
	Tabellenverzeichnis	11
	Listings	12
	Anhang	13

Abkürzungsverzeichnis

DB	Datenbank	7
DHCP	Dynamic Host Configuration Protocol	1
DNS	Domain Name System	1
DMZ	Demilitarisierte Zone	3
VM	virtuelle Machine	7

1 Pflichtenheft

1.1 Auftraggeber und Auftragnehmer

Beim Auftraggeber handelt es sich um die Gaming-Plattform **Doubtful-Joy SE**. Ansprechpartner sind

Tabelle 1.1: Ansprechpartner Auftraggeber

Funktion	Name	Vorname	Email
Auftraggeber	Hempel	Steffen	⟨hempel@bszetdd.lernsax.de⟩

Beim Auftragnehmer handelt es sich um das **High-Secure GmbH - Projektteam IT20/2 Gruppe 7**. Ansprechpartner sind

Tabelle 1.2: Ansprechpartner Auftragnehmer

Funktion	Name	Vorname	Email
Projektmanager	Egermann	Péter	⟨i20egermannpe@bszetdd.lernsax.de⟩
Teamleiter	Leyrer	Johannes	⟨i20leyrerjo@bszetdd.lernsax.de⟩
Netzwerkingenieur	Brethfeld	Vinzenz	⟨i20brethfeldvi@bszetdd.lernsax.de⟩

1.2 Ausgangslage

Die existierende Support-Infrastruktur der Gaming-Plattform Doubtful-Joy SE lässt sich über Mail und Telefon kontaktieren. Dabei wird jeder Anruf und jede Mail individuell von einem Mitarbeiter als Ticket gespeichert und in einem zentralen Laufwerk abgelegt. Effizienz, Ordnung und Übersichtlichkeit sind nicht ausreichend vorhanden.

1.3 Projektziel

Die Gaming-Plattform Doubtful-Joy SE möchte ihre existierende Support-Infrastruktur durch ein Ticketsystem ersetzen. Dieses soll für Kunden und Mitarbeiter über ein Web-Interface erreichbar sein. Tickets sollen über dieses direkt erstellt und mit beliebig vielen Attachments versehen werden können.

Außerdem soll eine Segmentierung der Netzinfrastruktur mit einer sichereren Trennung von öffentlich erreichbaren Diensten und dem Intranet eingerichtet werden. Ebenso sollen die internen Dienste Domain Name System (DNS) und Dynamic Host Configuration Protocol (DHCP) auf einem separatem System bereitgestellt werden, um eine Abhängigkeit von der Firewall auszu-schließen.

Doubtful-Joy SE setzt auf RedHat und binärkompatible Systeme, weshalb diese System-Strategie weiterhin umgesetzt werden soll.

1.4 Funktionsspezifikation

Von der Realisierung sind betroffen:

Manware

- Projektteam IT20/2 Gruppe 7
- Support-Mitarbeiter des Auftraggeber
- IT-Mitarbeiter des Auftraggebers

Orgware

- Sicherheitsanforderungen
- Benutzerhandbuch
- Benutzerschulung

Hardware

- Server
- Mitarbeiter-PCs

Software

- VM-Ware
- Datenbank-Server
- Web-Server
- Firewall-System
- DNS
- DHCP

1.5 Datenspezifikation

Da von etwa 1000 Telefonanrufen und Emails pro Tag ausgegangen wird, kann dies etwa 1:1 in 1000 Tickets übertragen werden. Der Speicherbedarf pro Ticket wird hier im Schnitt auf etwa 5 MB geschätzt, da wahrscheinlich häufiger Anhänge in Bildform zur besseren Problembeschreibung genutzt werden. Zusätzlich wird davon ausgegangen, dass die Daten zur Sicherheit und Nachvollziehbarkeit für ein Jahr gespeichert werden, wodurch die Datenbank 1830 GB Speicher in einem Jahr benötigt.

$$\frac{5 \text{ MB}}{\text{Ticket}} \cdot \frac{1000 \text{ Ticket}}{\text{Tag}} = \frac{5000 \text{ MB}}{\text{Tag}}$$

$$\frac{5000 \text{ MB}}{\text{Tag}} \cdot 365 \text{ Tage} = \frac{1\,825\,000 \text{ MB}}{\text{Jahr}} \stackrel{\wedge}{=} \frac{1830 \text{ GB}}{\text{Jahr}}$$

Da es keine Good-Practice ist, die Bilder in der Datenbank zu speichern, wird nur der Dateipfad zu den Bildern in der Datenbank hinterlegt, die Bilder selbst liegen auf der Festplatte des Webservers. Damit verringert sich der geschätzte Speicherbedarf der Datenbank auf etwa 183 GB pro Jahr.

$$\frac{0,5 \text{ MB}}{\text{Ticket}} \cdot \frac{\text{Ticket}}{\text{Tag}} = \frac{500 \text{ MB}}{\text{Tag}} \stackrel{\wedge}{=} \frac{183 \text{ GB}}{\text{Jahr}}$$

Die Bilder selbst benötigen zum aktuellen Stand auf der Festplatte 1643 GB Speicher pro Jahr.

$$\frac{4,5 \text{ MB}}{\text{Bild}} \cdot 1000 \frac{\text{Bild}}{\text{Tag}} = \frac{4500 \text{ MB}}{\text{Tag}} \stackrel{\wedge}{=} \frac{1643 \text{ GB}}{\text{Jahr}}$$

Die Art von Daten sind personenbezogene Daten in Text- und Bildform.

Der Datenfluss geht vom Clienten zur Demilitarisierte Zone (DMZ) und zur Bearbeitung dann zum PC des Support-Mitarbeiters, grafisch dargestellt in Abb. 1.1 auf der nächsten Seite.

1.6 Schnittstellenspezifikation

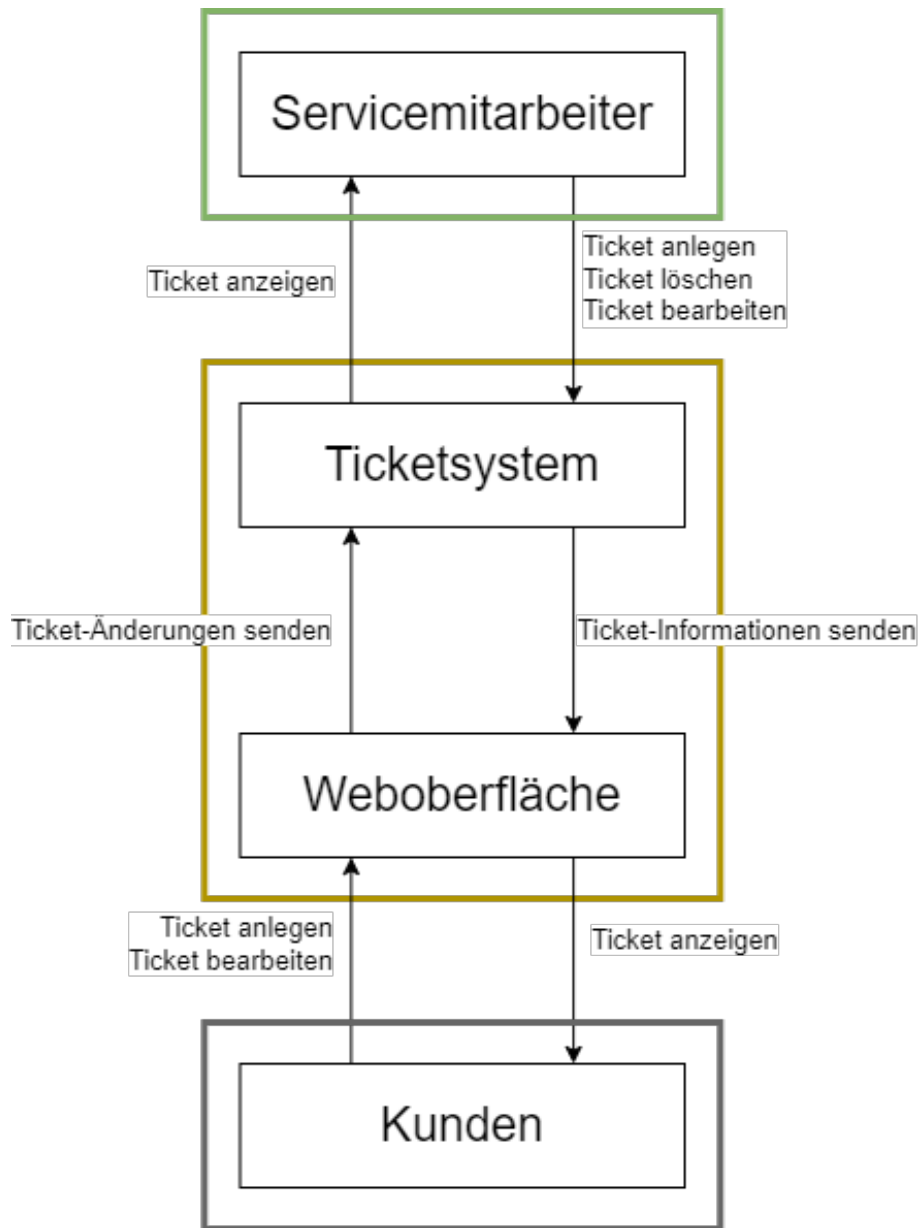


Abbildung 1.1: Schnittstellenspezifikation

1.7 Rahmenbedingungen

Der Auftraggeber hat folgende Ressourcen bereitzustellen und Mitwirkungspflichten:

- Server
- Mitarbeiter-PCs
- Zugriff auf alle zu bearbeitenden Systeme und Zutritt zu den notwendigen Räumlichkeiten
- Kooperation und eventuell notwendigen lokalen Support

1.8 Qualitätsbetrachtung

Die Arbeitspakete werden stets während der Bearbeitung sowie nach der Fertigstellung auf Funktion und Qualität überprüft.

Wöchentlich werden Meetings abgehalten um den Stand des Projekts zu erörtern und auf eventuell auftretende Probleme zeitnah reagieren zu können.

Die Zeitplanung und damit der Aufwand ist in Abb. A.1 auf Seite 14 in kleinem Format und groß in Abb. A.1 auf Seite 14 zu sehen. Für einen langfristigen Support für nach der der Fertigstellung wird ein zusätzliches Angebot vorgelegt.

1.9 Projektplanung

Die Projektplanung ist im Projektstrukturplan, zu sehen in Abb. 1.2, und im Gantt-Diagramm, zu sehen in Abb. 1.3 auf der nächsten Seite, bzw. Abb. A.1 auf Seite 14, abgebildet. Ebenso wird der im Anhang Seite 15 zu betrachtende Netzwerkplan Abb. B.1 auf Seite 15 umgesetzt.

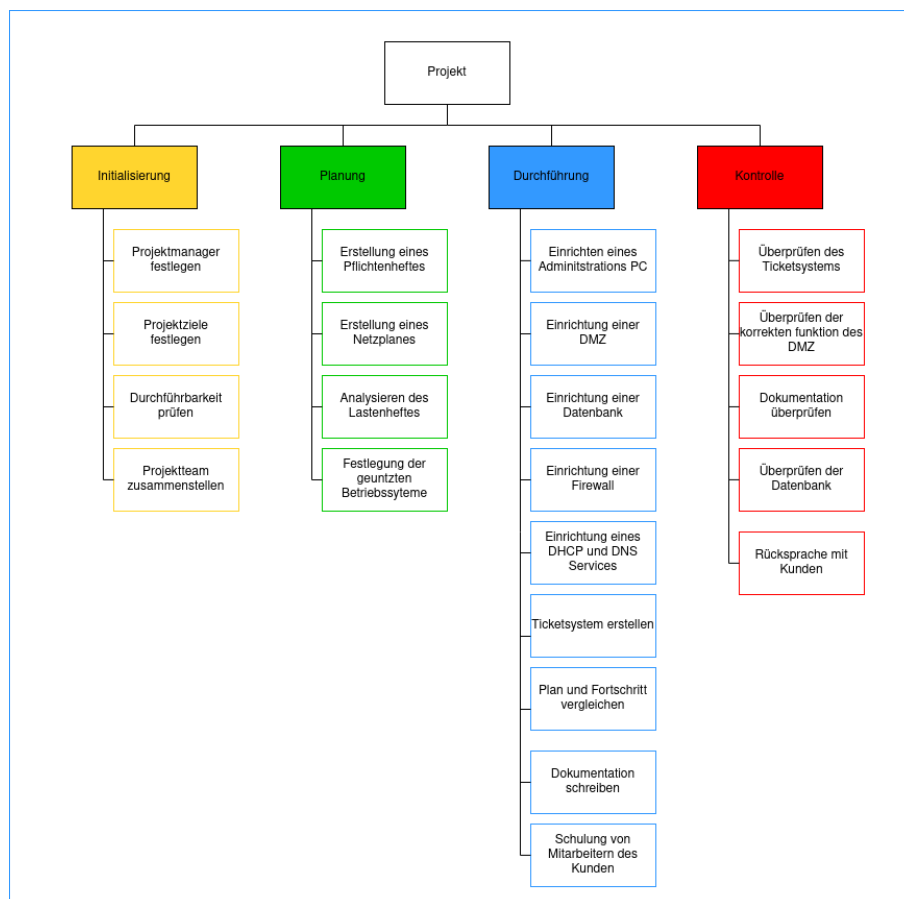


Abbildung 1.2: Projektstrukturplan

GANTT Diagramm Gruppe 7

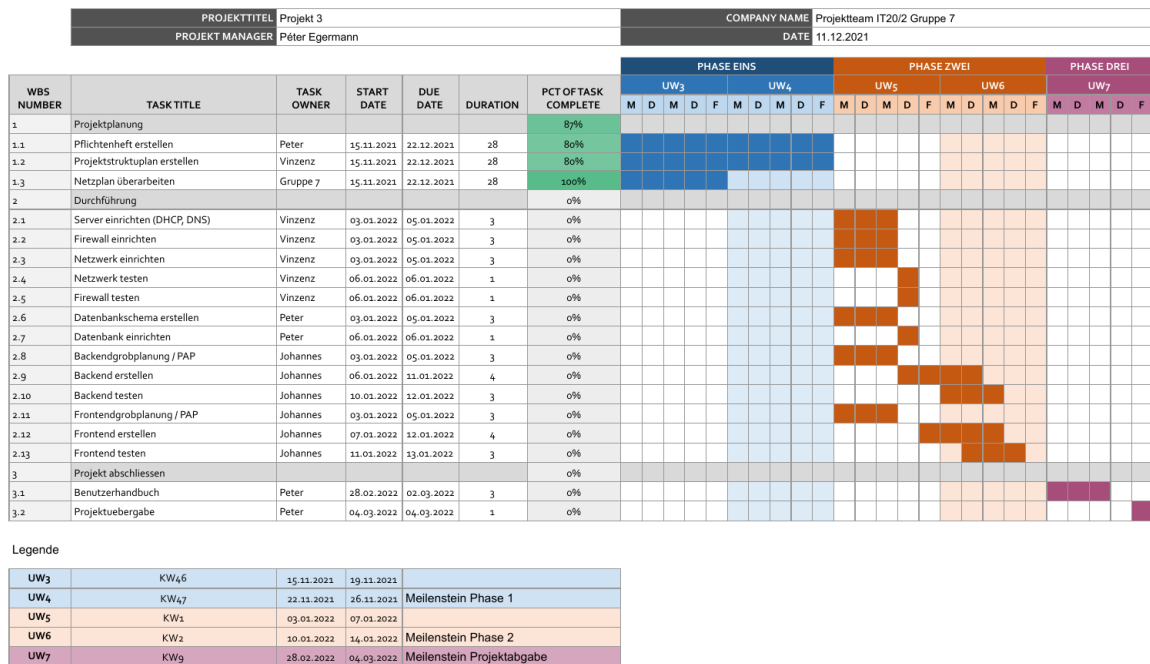


Abbildung 1.3: Gantt-Diagramm

1.10 Kosten-Nutzen-Analyse

Eine Kosten-Nutzen-Analyse ist zum jetzigen Zeitpunkt nicht notwendig, da der Support erst mal entlastet werden muss. Dies ist durch das neue System auf jeden Fall der Fall, da quasi der Kunde das Ticket erstellt und nicht der Support-Mitarbeiter. Somit kann sich voll auf das Beheben des Problems konzentriert werden.

2 Auswertung und Reflexion

2.1 Ablaufdokumentation

In diesem Projekt wurden drei Netze eingerichtet, um ein echtes Netzwerk wiederzugeben. Dabei handelt es sich um das rote Netz, das das Internet wiedergeben soll, das orange Netz, was eine sogenannte DMZ darstellt und das grüne Netz, das das interne Netz darstellt. Um die Kommunikation und den Zugriff zwischen den Netzen zu regeln wird in diesem Projekt die Firewall verwendet. Somit kann aus dem roten Netz nur mit dem orangen Netz kommunizieren werden, aus dem grünen Netz ist kein Zugriff auf das Internet möglich und zwischen dem orangen und grünen Netz sind nur bestimmte Ports zur Kommunikation und Datenübertragung zugelassen. Um Maschinen in den verschiedenen Netzen darzustellen wurden vier verschiedene virtuelle Maschinen (VMs) aufgesetzt, die bis auf der IPFire auf CentOS 8 Stream basieren:

- IPFire (als Knotenpunkt für alle drei Netze)
- Admin-PC (grünes Netz)
- DHCP-DNS-Datenbank (DB)-Server (grünes Netz)
- Webserver (DMZ, oranges Netz)

2.2 Einrichtung IPFire

Vor dem Einrichten der IPFire müssen noch zwei Netzwerke zu dem schon bestehenden Netzwerk hinzugefügt werden, da die Firewall mit drei verschiedenen Netzen interagieren soll. Noch dazu werden den einzelnen Netzen verschiedene MAC-Adressen zugeteilt, damit sie in der späteren Nutzung zuordenbar sind.

In unserem Projekt wurden die Netzwerke wie in Tabelle 2.1 zu sehen verteilt.

Tabelle 2.1: Netzwerkauslegung

Netzwerk-Farbe	MAC-Adresse	Netzwerk
Rot	00:50:56:32:BA:0F	NAT
Grün	00:50:56:3D:EC:D6	VMnet1
Orange	00:50:56:3E:56:B7	VMnet2

Als Hostname der Firewall wurde `ipfireund` als Domaine wurde `"doubtful-joy07.com"` festgelegt. Nach dem Auswählen der Sprache wurde aufgrund der Kundenspezifikation das Filesystem `ext4` Filesystem ausgewählt. Nach dem Zuweisen der einzelnen Netze mit den IP- und MAC-Adressen wurde der DHCP deaktiviert, damit es später mit dem DHCP-Server im grünen Netz nicht zu Komplikationen führt.

Nachdem die Firewall eingerichtet wurde können aus dem grünen Netz mittels des IPFire-WebInterfaces verschiedene Einstellungen der Firewall bearbeitet werden. Für die Verbindungen zwischen Admin-PC, DHCP-DNS-DB-Server und Webserver sowie für die Erreichbarkeit des Webserver aus dem roten Netz wurden vier verschiedene Regeln erstellt, die in n Abb. 2.1 zu sehen sind.

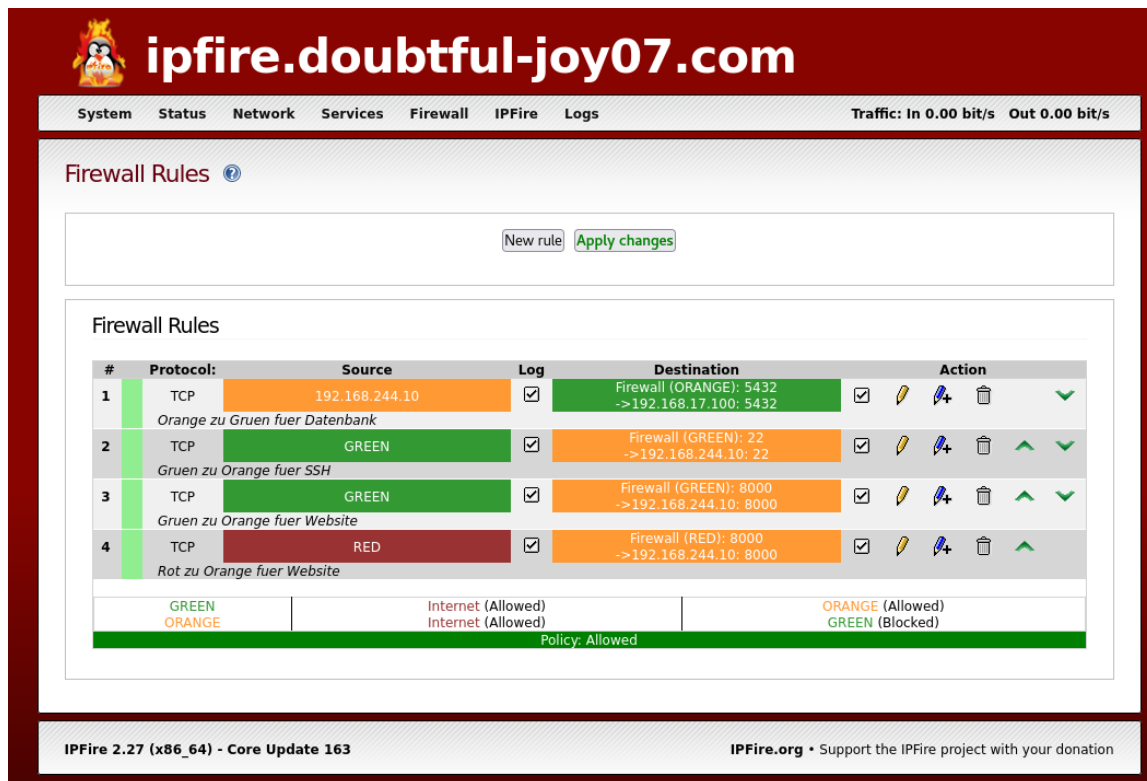


Abbildung 2.1: Firewall-Regeln

Die erste Regel dient der Kommunikation zwischen Webserver (DMZ) und Datenbank (grünes Netz), sodass Tickets abgerufen und gespeichert werden können. Damit aus dem grünen Netz der Webserver gestartet und gestoppt werden kann, wurde Regel 2 implementiert. Die Erreichbarkeit des WebInterface der Ticket-Seite durch die Mitarbeiter aus dem grünen Netz wurde mit Regel 3 erreicht. Die letzte Regel erlaubt den Zugriff aus dem Internet auf die Ticket-Website.

2.3 Einrichtung Admin-PC

Nach der Standard-Installation von CentOS 8 Stream wurden das Netzwerk der VM angepasst. Hier wurde der DNS auf die IP-Adresse des DHCP-DNS-DB-Servers gesetzt.

Da in CentOS 8 Stream SSH-Client und -Server bereits installiert und aktiviert sind, konnte der Webserver direkt angesprochen werden. Dies erfolgte ueber das Gateway des grünen Netzes, wie in Abb. 2.2 auf der nächsten Seite zu sehen. Um zu sehen, ob der Webserver aktiv ist, können mittels `ps -ef | grep python` alle laufenden Python-Anwendungen aufgelistet werden, was ebenfalls in Abb. 2.2 auf der nächsten Seite zu sehen ist.

Ist der Webserver aktiv und soll gestoppt werden, kann mittels `ps -ef | grep python` die ID

```
[admin@localhost ~]$ ssh admin@192.168.17.3
admin@192.168.17.3's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Sun Mar 13 10:01:19 2022 from 192.168.17.58
[admin@localhost ~]$ ps -ef | grep python
root      1076      1  0 09:22 ?        00:00:00 /usr/libexec/platform-python -s /usr/sbin/firewalld --nofork --nopid
root      1144      1  0 09:22 ?        00:00:04 /usr/libexec/platform-python -Es /usr/sbin/tuned -l -P
admin     5027      1  0 10:02 ?        00:00:00 python3.10 main.py
admin     5139    5096  0 10:03 pts/1    00:00:00 grep --color=auto python
[admin@localhost ~]$
```

Abbildung 2.2: SSH-Login sowie Auflisten aller laufenden Python-Anwendungen

des Scripts ermittelt und mittels `kill -9 ID` gestoppt werden. Dies ist in Abb. 2.3 zu sehen.

```
[admin@localhost ~]$ kill -9 5027
[admin@localhost ~]$ ps -ef | grep python
root      1076      1  0 09:22 ?        00:00:00 /usr/libexec/platform-python -s /usr/sbin/firewalld --nofork --nopid
root      1144      1  0 09:22 ?        00:00:04 /usr/libexec/platform-python -Es /usr/sbin/tuned -l -P
admin     5172    5096  0 10:04 pts/1    00:00:00 grep --color=auto python
[admin@localhost ~]$
```

Abbildung 2.3: Stoppen einer bestimmten Python-Anwendungen

Soll der Webserver gestartet werden, kann dies mittels Navigation in den Ordner, in dem die auszuführende Datei liegt und `python3.10 name-der-datei &` gestartet werden, zu sehen in der Abb. 2.4. Das `&` erlaubt das Laufen der Anwendung im Hintergrund und wird so nicht gestoppt, wenn die SSH-Verbindung geschlossen wird.

```
[admin@localhost ~]$ cd /home/admin/Documents/LF9_Project3-main/backend/
[admin@localhost backend]$ python3.10 main.py &
[1] 5027
[admin@localhost backend]$ INFO:      Started server process [5027]
INFO:      Waiting for application startup.
INFO:      Application startup complete.
INFO:      Uvicorn running on http://0.0.0.0:8000 (Press CTRL+C to quit)
exit
logout
Connection to 192.168.17.3 closed.
[admin@localhost ~]$
```

Abbildung 2.4: Starten einer bestimmten Python-Anwendungen

2.4 Einrichtung DHCP-DNS-DB-Server

2.5 Einrichtung Webserver

Abbildungsverzeichnis

1.1	Schnittstellenspezifikation	4
1.2	Projektstrukturplan	5
1.3	Gantt-Diagramm	6
2.1	Firewall-Regeln	8
2.2	SSH-Login sowie Auflisten aller laufenden Python-Anwendungen	9
2.3	Stoppen einer bestimmten Python-Anwendungen	9
2.4	Starten einer bestimmten Python-Anwendungen	9

Tabellenverzeichnis

1.1	Ansprechpartner Auftraggeber	1
1.2	Ansprechpartner Auftragnehmer	1
2.1	Netzwerkauslegung	7

Listings

Anhang

A Gantt-Diagramm

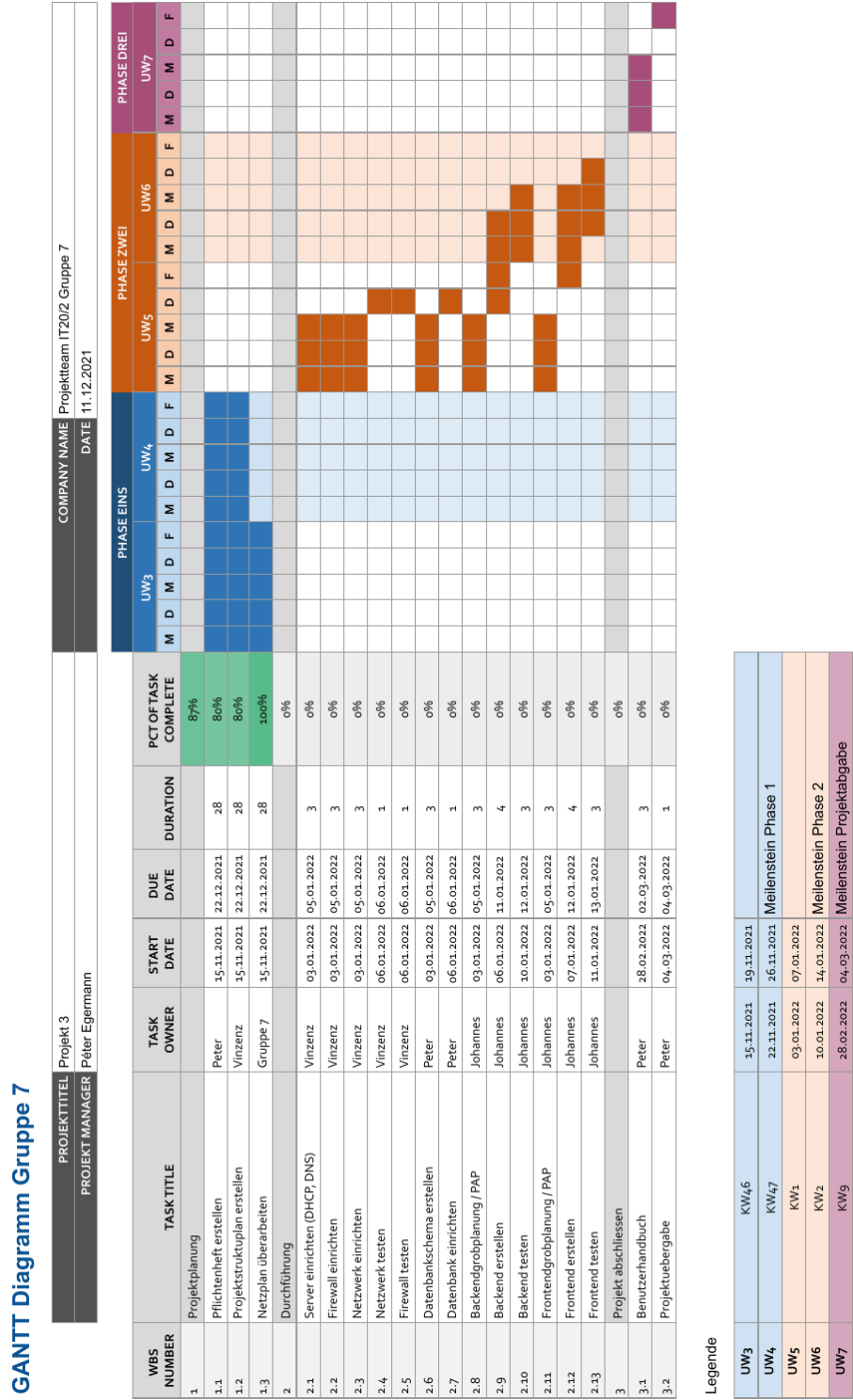


Abbildung A.1: Gantt-Diagramm

B Netzwerkplan

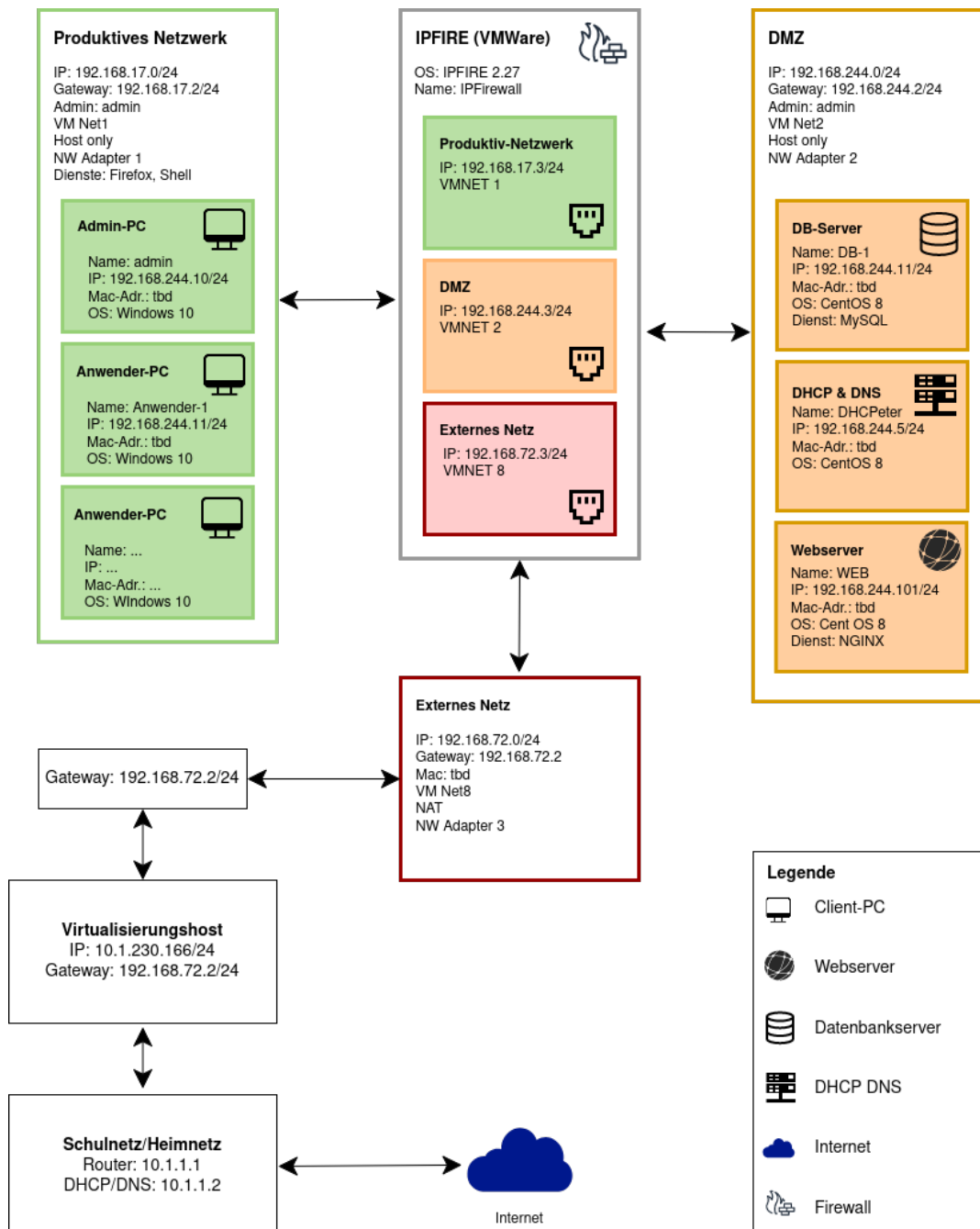


Abbildung B.1: Netzwerkplan