

Berufliches Schulzentrum für Elektrotechnik Dresden

Fachbereich Informationstechnik

Projektdokumentation

Lernfeld 9 - Projekt 3 und 4

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 Projekt 3	7
2.1	Ablaufdokumentation	7
2.2	Einrichtung IPFire	7
2.3	Einrichtung Admin-PC	8
2.4	Einrichtung DHCP-DNS-DB-Server	9
2.4.1	Einrichtung der CentOS-Installation	9
2.4.2	Einrichtung des DHCP und DNS	10
2.4.3	Einrichtung des Datenbank-Servers	11
2.5	Einrichtung Webserver	13
2.5.1	Einrichtung der CentOS-Installation	13
2.5.2	Einrichtung des Backends	13
2.5.3	Einrichtung des Frontends	13
2.6	Soll-Ist-Vergleich	13
2.7	Abweichung zum Zeitplanung	13
2.8	Optimierungsvorschläge zur Projektrealisierung	14
3	Auswertung und Reflexion Projekt 4	15
3.1	Schutzbedarfsanalyse und TOM-Identifikation	15
3.2	Cybersecurity implementieren	17
3.2.1	Datensicherung des Datenbankservers	17
3.2.2	E2E-Verschlüsselung der DMZ-Kommunikation	18
3.2.3	SSH ohne Passwort	18
	Abbildungsverzeichnis	20

Tabellenverzeichnis	21
Listings	22
Literaturverzeichnis	23
Anhang	24

Abkürzungsverzeichnis

API	Application Programming Interface	13
CRUD	create, read, update und delete	13
DB	Datenbank	8
DHCP	Dynamic Host Configuration Protocol	1
DNS	Domain Name System	1
DMZ	Demilitarisierte Zone	3
SSH	Secure Shell	8
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.

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

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

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.

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

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

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

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

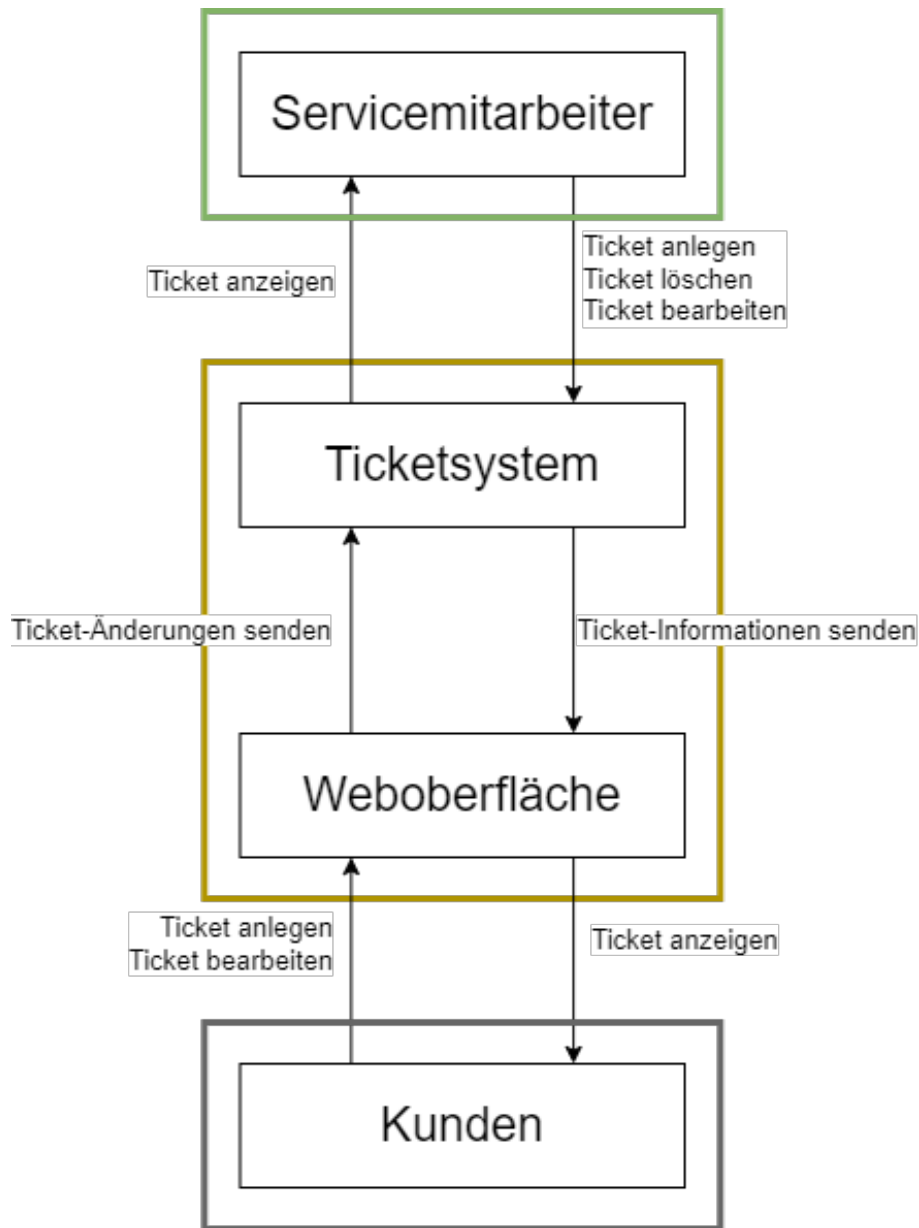


Abbildung 1.1: Schnittstellenspezifikation

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. 1.3 auf der nächsten Seite in kleinem Format und groß in Abb. A.1 auf Seite 25 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 25, abgebildet. Ebenso wird der im Anhang Seite 27 zu betrachtende Netzwerkplan Abb. B.1 auf Seite 27 umgesetzt.

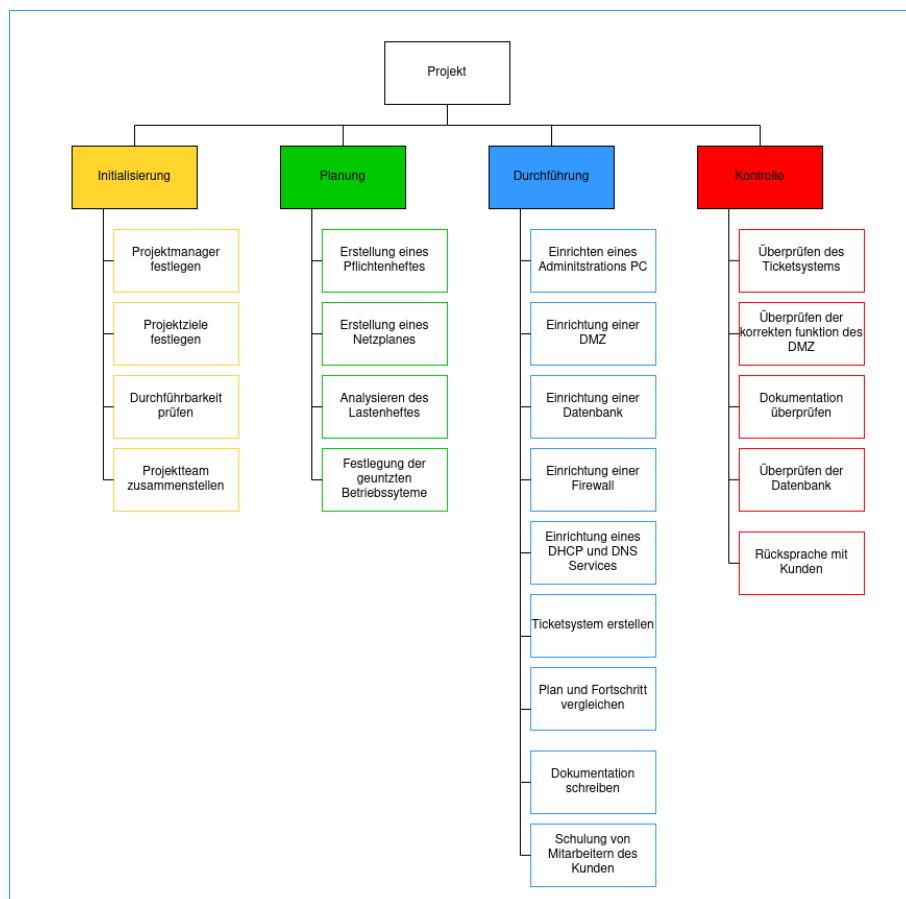


Abbildung 1.2: Projektstrukturplan

GANTT Diagramm Gruppe 7

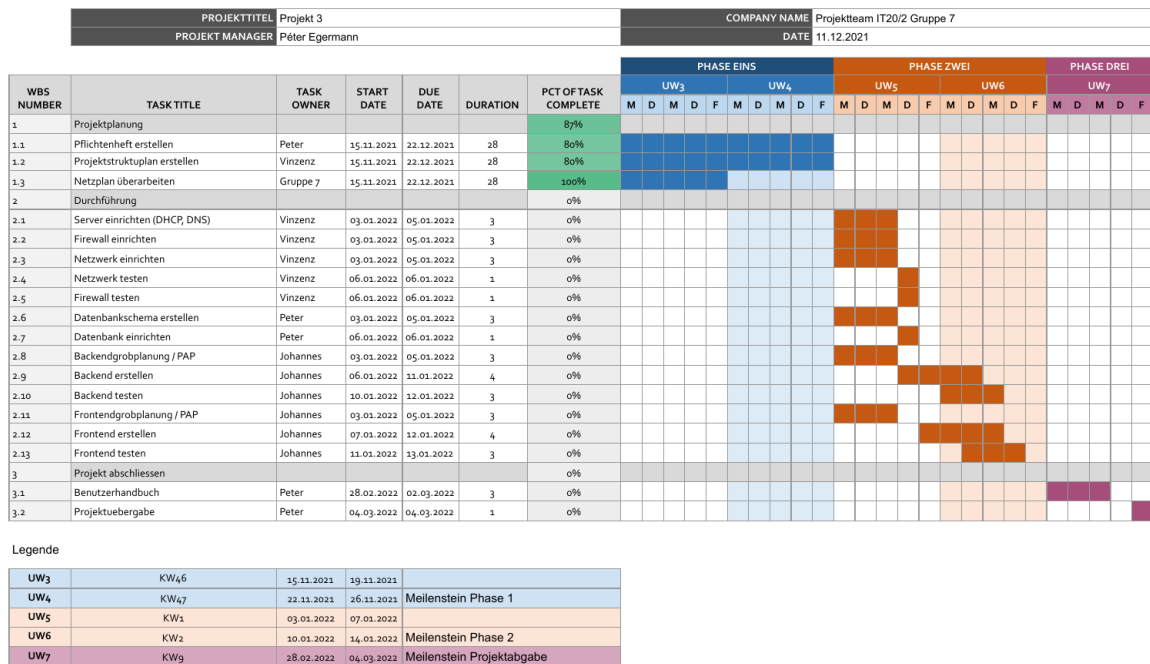


Abbildung 1.3: Gantt-Diagramm

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 Projekt 3

2.1 Ablaufdokumentation

In diesem Projekt werden drei virtuelle Netze eingerichtet, um den Aufbau eines echten Netzwerks zu simulieren. 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, welches 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 kommuniziert 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 die IPFire auf CentOS 8 Stream basieren:

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

2.2 Einrichtung IPFire

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

Die Netzwerke werden 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 wird „ipfire“ und als Domaine „doubtful-joy07.com“ festgelegt. Nach dem Auswählen der Sprache wird aufgrund der Kundenspezifikation das Filesystem „ext4 Filesystem“ ausgewählt. Nach dem Zuweisen der einzelnen Netze mit den IP- und MAC-Adressen

wird der DHCP deaktiviert, damit es später mit dem DHCP-Server im grünen Netz nicht zu Komplikationen führt.

Nach dem Einrichten der Firewall werden aus dem grünen Netz mittels des IPFire-Webinterfaces verschiedene Einstellungen der Firewall bearbeitet. Für die Verbindungen zwischen Admin-PC, DHCP-DNS-Datenbank (DB)-Server und Webserver sowie für die Erreichbarkeit des Webserver aus dem roten Netz werden vier verschiedene Regeln erstellt, die in Abb. 2.1 zu sehen sind.

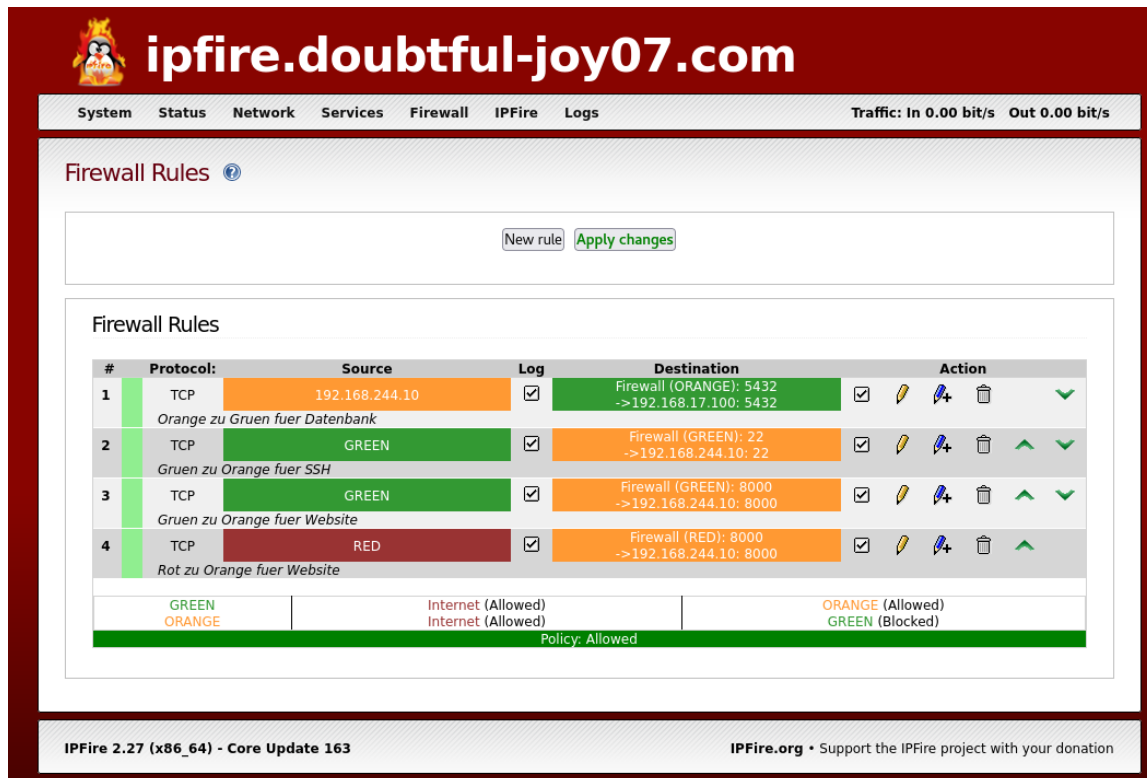


Abbildung 2.1: Firewall-Regeln

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, wird Regel 2 implementiert, welche einen Secure Shell (SSH)-Zugang aus dem grünen Netz erlaubt. Die Erreichbarkeit des Webinterface der Ticket-Seite durch die Mitarbeiter aus dem grünen Netz wird 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 wird das Netzwerk der VM angepasst. Hier wird 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, kann der Webserver direkt angesprochen werden. Dies erfolgt über 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 zu sehen ist.

```
[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

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

2.4.1 Einrichtung der CentOS-Installation

Wie auch der Admin-PC wird der DHCP-DNS-DB-Server mit CentOS 8 Stream eingerichtet. In den Netzwerkeinstellungen wird die IP-Adresse fest auf 192.168.17.100, die Netzwerkmaske auf 255.255.255.0 und das Gateway auf 192.169.17.3 gesetzt. Außerdem werden die Dienste DNS und DHCP in der Firewall freigegeben, zu sehen in Listing 2.1.

Listing 2.1: Dienste-Freigabe einer CentOS-Firewall

```
# firewall-cmd --add-service=dns --permanent
```

```
# firewall-cmd --add-service=dhcp --permanent
# firewall-cmd --reload
```

2.4.2 Einrichtung des DHCP und DNS

Die Installation und Einrichtung des DHCPs und DNS erfolgt mittels der Anleitung für dnsmasq von Michelle Ferron. [2]

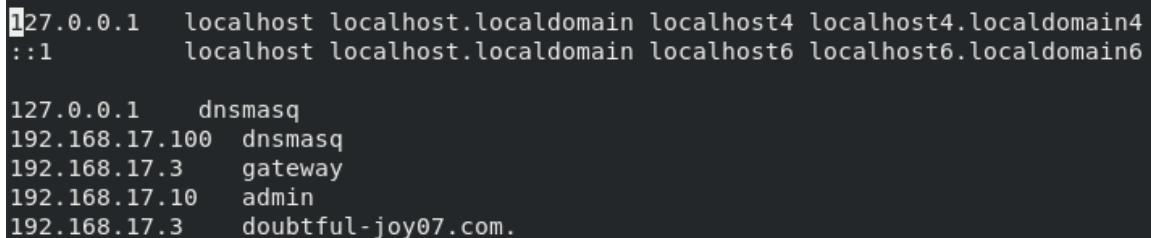
Die Einstellungen des DHCP wird mittels der in Listing 2.2 zu sehenden Befehle und Einstellungen angepasst.

Listing 2.2: DHCP-Einstellungen

```
# nano /etc/dnsmasq.conf
listen-address=::1,127.0.0.1,192.168.17.100
interface=ens160
domain=doubtful-joy07.com
```

Nach der Einrichtung wird das Netzwerk des Admin-PCs ausgeschaltet, die DHCP-Einstellungsoption ausgewählt und das Netzwerk wieder angeschaltet. Der Admin-PC bekommt durch den DHCP automatisch eine neue IP-Adresse.

Die Einstellungen des DNS wird mittels der `/etc/hosts`-Datei angepasst. Die hier einzustellenden Werte sind in Abb. 2.5 zu sehen.

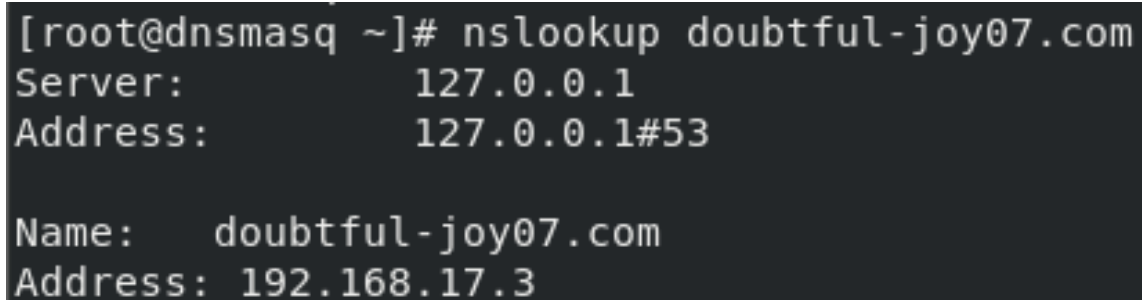


```
127.0.0.1    localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6

127.0.0.1    dnsmasq
192.168.17.100 dnsmasq
192.168.17.3  gateway
192.168.17.10 admin
192.168.17.3  doubtful-joy07.com.
```

Abbildung 2.5: DNS-Einstellungen

Die Funktion des DNS kann mittels `nslookup`, zu sehen in Abb. 2.6, oder über das Aufrufen des Frontends des Webservers, zu sehen in Abb. 2.7 auf der nächsten Seite, überprüft werden.



```
[root@dnsmasq ~]# nslookup doubtful-joy07.com
Server:           127.0.0.1
Address:          127.0.0.1#53

Name:   doubtful-joy07.com
Address: 192.168.17.3
```

Abbildung 2.6: Überprüfen des DNS mittels Namens

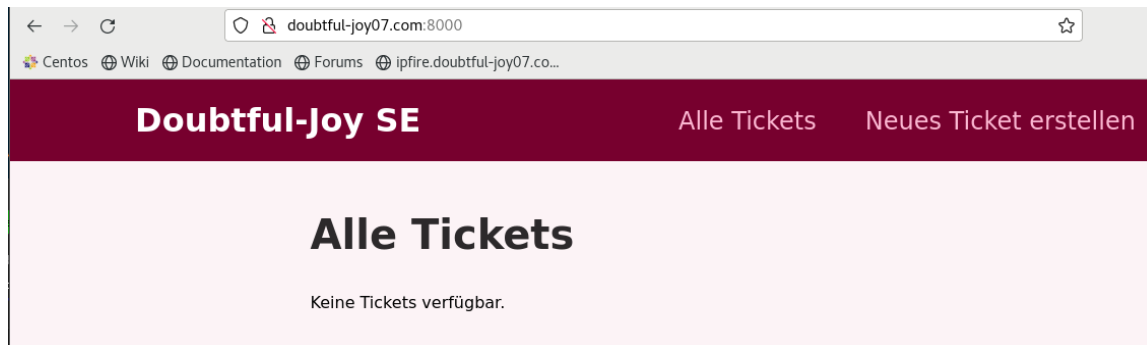


Abbildung 2.7: Aufrufen des Frontends mittels Name

2.4.3 Einrichtung des Datenbank-Servers

Die Einrichtung eines Datenbank-Servers erfolgt mittels der Anleitung von Aaron Kili. [3] Mit dieser wird PostgreSQL, ein „leistungsstarkes, weit verbreitetes, quelloffenes, plattformübergreifendes und fortschrittliches objektrelationales Datenbanksystem“ [3] und pgAdmin, ein „fortschrittliches, quelloffenes, voll funktionsfähiges und webbasiertes Verwaltungs- und Managementwerkzeug“ [3], installiert.

Mittels des Webinterfaces, das pgAdmin bereitstellt, lässt sich eine Datenbank erstellen, zu sehen in Abb. 2.8 auf der nächsten Seite. Der Name der Datenbank wird auf „tickets“, der Benutzername auf „ticketadmin“ und das Passwort auf „adminadmin“ festgelegt.

Um die Kommunikation zwischen der Datenbank und dem Backend des Webservers zu erlauben, muss der Port 5432 freigegeben werden, zu sehen in Listing 2.3.

Listing 2.3: Port-Freigabe einer CentOS-Firewall

```
# firewall-cmd --zone=public --add-port=5432/tcp --permanent
# firewall-cmd --reload
```

Ebenso muss die `postgresql.conf` angepasst werden, so dass ein Zugriff von außerhalb überhaupt möglich ist. [1] Dies ist in folgendem Listing 2.4 zu sehen.

Listing 2.4: Einrichtung Zugriff PostgreSQL

```
# nano /var/lib/pgsql/data/postgresql.conf
listen_addresses = '*'
```

Da im Front- und Backend Timestamps als Zahlen verwendet werden, muss die Tabelle noch geändert werden, damit kein `integer-out-of-range`-Fehler geworfen wird. Dies wird mittels der Befehls `ALTER TABLE` wie in Listing 2.5 umgesetzt.

Listing 2.5: Ändern der tickets-Tabelle

```
ALTER TABLE order_detail ALTER COLUMN amount TYPE BIGINT;
```

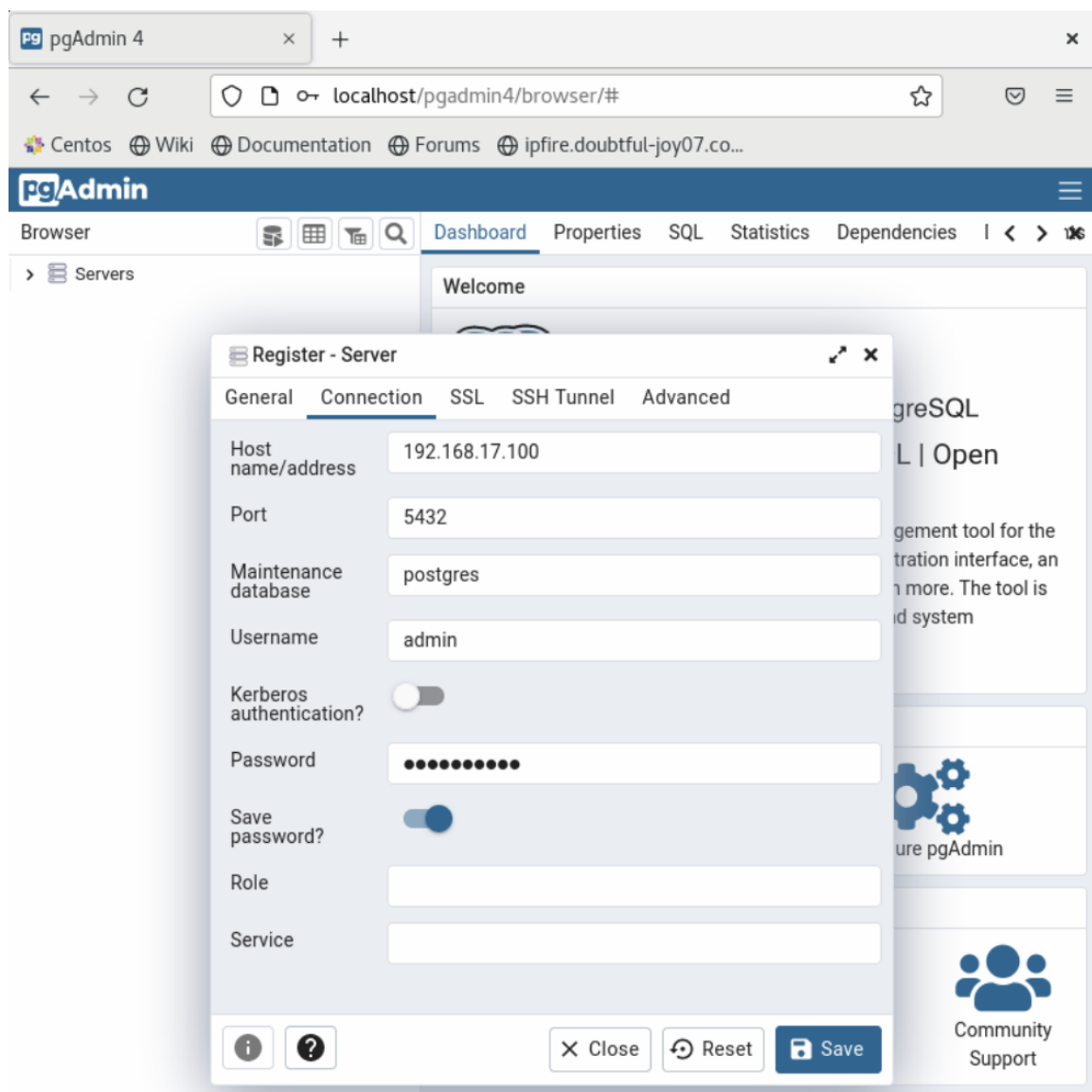


Abbildung 2.8: Einrichtung der Tickets-Datenbank

2.5 Einrichtung Webserver

2.5.1 Einrichtung der CentOS-Installation

Nach der Standard-Installation von CentOS 8 Stream wird das Netzwerk der VM angepasst. Hier wird die IP-Adresse fest auf 192.168.244.10, die Netzwerkmaske auf 255.255.255.0 und das Gateway auf 192.169.244.3 gesetzt. Außerdem wird der Port 8000 und Port 22 freigegeben. Port 8000 dient dem Zugriff auf die Website von den beiden anderen Netzen aus und Port 22 erlaubt den SSH-Zugriff des Admin-Pcs. Als Beispiel ist die Port-Freigabe für Port 8000 im Listing 2.6 zu sehen.

Listing 2.6: Port-Freigabe einer CentOS-Firewall

```
# firewall-cmd --zone=public --add-port=8000/tcp --permanent
# firewall-cmd --reload
```

Abschließend wird Python3.10 installiert, um das Backend betreiben zu können.

2.5.2 Einrichtung des Backends

Das Backend wird mit Python3.10 umgesetzt. Hierfür wird mit Hilfe von FastAPI eine Application Programming Interface (API) geschrieben, die verschiedene Routen bereitstellt, mit denen create, read, update und delete (CRUD)-Anweisungen ausgeführt werden können. Außerdem dient das Backend auch gleich als Server für das Frontend, da es eben dieses bereitstellt.

Die benötigten Pakete können mittels `pip3.10 requirements.txt` installiert werden.

2.5.3 Einrichtung des Frontends

Für das Frontend wird die JavaScript-Softwarebibliothek React verwendet. Hier werden alle vom Kunden geforderten Anzeige und Bedienelemente implementiert. Da das Frontend bereits nach der Umsetzung gebaut und durch das Backend bereitgestellt wird, müssen keine Pakete installiert werden.

2.6 Soll-Ist-Vergleich

Der Zustand der abgelieferten Arbeit entspricht dem Soll-Zustand und somit den Kundenwünschen. Es werden alle Kriterien umgesetzt. Das Firewall-System, DHCP und DNS, Webserver und Datenbanksystem funktionieren einwandfrei.

2.7 Abweichung zum Zeitplanung

Der ursprüngliche Zeitplan, zu sehen in Abb. 1.3 auf Seite 6, bzw. Abb. A.1 auf Seite 25, konnten nicht eingehalten werden. Es gab zwei Probleme:

- Die Linux-Clients im IPFire Netz konnten keine Software installieren.
Hier wurde vermutet, dass es an der Einrichtung der Firewall-Regeln lag, weswegen eine komplette Neuinstallation vorgenommen wurde. Dies hat unnötig Zeit gefressen. Die Lösung war dann, die System zu Hause einzurichten.

- Durch den Zeitverzug, den das erste Problem mit sich trug, konnte die Dokumentation nicht rechtzeitig fertiggestellt werden.

Das aktualisierte Gantt-Diagramm ist in klein in Abb. 2.9 und groß im Anhang in Abb. A.2 auf Seite 26 zu sehen.

GANTT Diagramm Gruppe 7

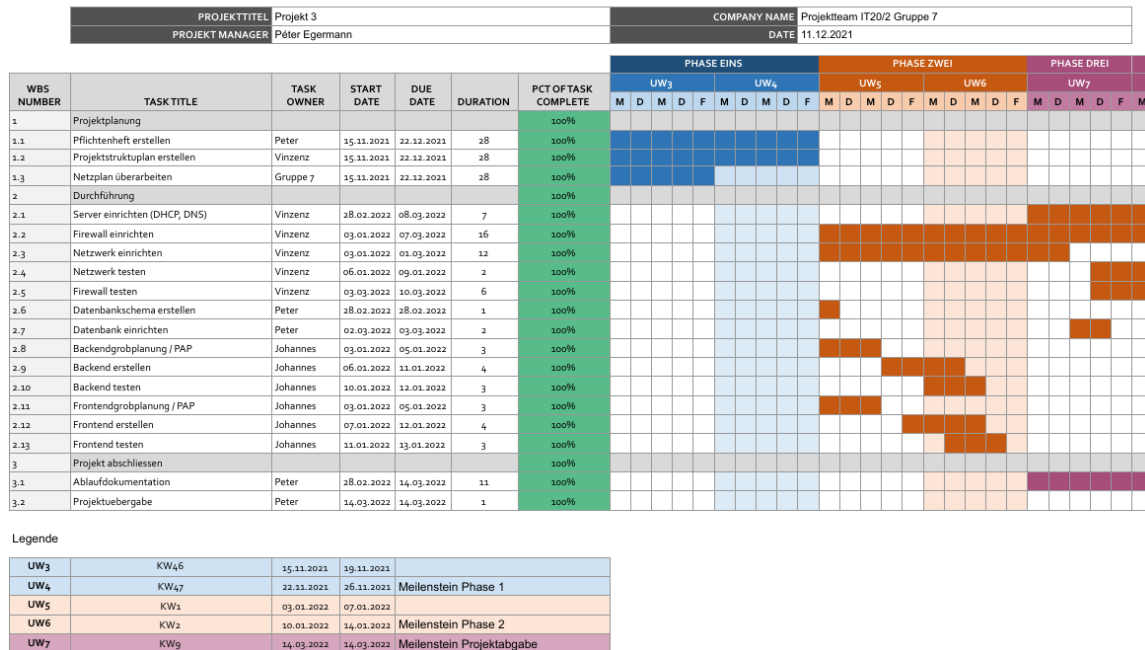


Abbildung 2.9: Gantt-Diagramm

2.8 Optimierungsvorschläge zur Projektrealisierung

Das Projektteam IT20/2 Gruppe 7 besteht aus drei Anwendungsentwicklern, was die Sache deutlich erschwert hat. Hier wäre eine Überarbeitung der Gruppeneinteilung von Vorteil gewesen, so dass ein Team durch einen Systemintegrator und einen Anwendungsentwickler gebildet wird, wodurch sich gewisse Synergieeffekte ergeben könnten.

3 Auswertung und Reflexion Projekt 4

3.1 Schutzbedarfsanalyse und TOM-Identifikation

Tabelle 3.1: Gefährdungsübersicht für Datenbank-Server und Web-Server

Risiko	Auswirkung	Schweregrad
G 0.8 Ausfall oder Störung der Stromversorgung	Durch einen Ausfall oder eine Störung der Stromversorgung können die Server ebenfalls in ihrer Funktionsweise eingeschränkt sein oder komplett ausfallen. Dies ist besonders schwerwiegend, da die Behebung eines Stromausfalls in den meisten Fällen einen längeren Ausfall zur Folge hat. Das abrupte Abstürzen der Systeme verhindert ein sofortiges manuelles Backup.	5/5
G 0.9 Ausfall oder Störung von Kommunikationsnetzen	Durch den Ausfall des Kommunikationsnetzes kann keine Verbindung mehr zu den Servern hergestellt werden. Zum einen sind diese für den Kunden nicht mehr erreichbar und zum anderen kann ein Systemadmin diese Systeme (falls sie nicht On-Site stehen) auch nicht erreichen. Dies ist als Totalausfall des Systems zu werten und verhindert eine normale Benutzung.	5/5
G 0.23 Unbefugtes Eindringen in IT-Systeme	Durch ein unbefugtes Eindringen in IT-Systeme können die komplette Server-Infrastruktur und die Funktionalität des Systems beeinträchtigt werden. Vorhandene Daten könnten manipuliert, gelöscht oder gestohlen werden. Das komplette System kann kompromittiert werden, es könnten andere Informationen angezeigt werden, als vom Betreiber angedacht. Ein unbefugter Zutritt ist aufgrund der aufgeführten Punkte als höchst kritisch zu werten.	5/5

G 0.25 Ausfall von Geräten oder Systemen	Ein Ausfall von Geräten oder Systemen ist als höchst kritisch zu werten. Da in der aktuellen Umsetzung keine Art von Replikation, Loadbalancing oder High-Availability Lösung vorhanden ist, würde der Ausfall eines einzelnen Gerätes einen Komplettausfall des Systems zur Folge haben. Der Ausfall von Hardware ist ein durchaus realistisches und auf längere Zeit gesehen ein sehr wahrscheinliches Szenario.	5/5
G 0.27 Ressourcenmangel	Ein Mangel an Ressourcen ist durchaus realistisch und mit steigender Nutzerzahl auch ein wahrscheinlich auftretendes Problem. Wenn viele Personen gleichzeitig versuchen ein Ticket zu öffnen, könnte dies etwa einem DDoS-Angriff entsprechen. Die Antwortzeit des Systems verlangsamt sich, manche Anfragen werden vielleicht nicht bearbeitet, Daten werden nicht korrekt in die Datenbank geschrieben, was ebenfalls einen Informationsverlust zur Folge haben kann. Deshalb ist es wichtig, stets genügend Ressourcen zur Verfügung zu stellen, das betrifft unter anderem Arbeitsspeicher, persistenter Speicher, Rechenleistung und den Netzwerkdurchsatz.	5/5

Tabelle 3.2: Technisch- Organisatorische Maßnahmen zur Verminderung der Risiken

Maßnahmen	Beschreibung	Bezug
Verwendung einer unterbrechungsfreien Stromversorgung	Durch die Verwendung einer unterbrechungsfreien Stromversorgung kann man zeitweise vom Stromnetz unabhängig agieren. Dies ermöglicht entweder die Überbrückung des Ausfalls oder das korrekte herunterfahren der einzelnen Server. Aufwand ist für unser angestrebtes Konzept noch relativ gering, der Nutzen aber auch groß.	G .0.8

Verwendung von Zugriffsbeschränkungen	Der Zugriff auf die Server sollten nur für autorisierte Nutzer ermöglicht sein, damit kein unberechtigter Nutzer das System manipulieren kann. Dies kann in Form von Nutzerkonten mit starken Passwörtern, oder durch das Hinterlegen von SSH-Keys auf dem Server erreicht werden. Aufwand ist dabei relativ gering und der Nutzen sehr groß.	G 0.23 Unbefugtes Eindringen in IT-Systeme
Nutzung von high-availability-clustern	Diese Lösung erfordert das doppelte Vorhandensein von allen wichtigen Servern. Falls ein Teilsystem ausfällt wird einfach das andere Backup-System verwendet, wodurch die Funktionalität des Gesamtsystems erhalten bleibt. Der Aufwand dafür ist groß, da jedes System in doppelter Ausführung vorhanden sein muss, was doppelten Preis und doppelte Konfiguration bedeutet. Außerdem ist die Einrichtung eines High availability clusters mit zusätzlichem Aufwand verbunden. Der Nutzen der daraus gezogen wird ist sehr groß, besonders bei kritischen Systemen ist man dadurch vor einem Ausfall des Gesamtsystems sicher.	G 0.25 Ausfall von Geräten oder Systemen

3.2 Cybersecurity implementieren

3.2.1 Datensicherung des Datenbankservers

Zur Datensicherung des Datenbankservers im laufenden Betriebs werden folgende Schritte abgearbeitet:

- Einloggen als User *ticketadmin*, mit dem Passwort „adminadmin“.
- Neues Verzeichnis mit dem Namen „backups“ erstellen, zu sehen in Abb. 3.1 auf der nächsten Seite.
- Erstellen eines Cron-Tasks, ebenfalls zu sehen in Abb. 3.1 auf der nächsten Seite.
- Eintragen der in Listing 3.1 zu sehenden Einstellungen.

Mit diesen Einstellungen wird jeden Sonntag um Mitternacht ein Backup der Datenbank erstellt und in dem Verzeichnis „backups“ gespeichert.

Listing 3.1: Einrichtung eines Cron-Tasks

```
0 0 * * 0 pg_dump -U postgres dbname > ~/postgres/backups/tickets.bak
```

```
[admin@dnsmasq ~]$ su
Password:
[root@dnsmasq admin]# mkdir -p ~/backups
[root@dnsmasq admin]# crontab -e
no crontab for root - using an empty one
crontab: installing new crontab
[root@dnsmasq admin]#
```

Abbildung 3.1: Erstellen eines Verzeichnisses und eines Cron-Tasks

3.2.2 E2E-Verschlüsselung der DMZ-Kommunikation

Voraussetzung für das Erstellen eines SSL-Zertifikats auf dem Dienst-Server die Installation von *openssl*, was bei CentOS standardmäßig vorhanden ist.

Mittels des in Listing 3.2 zu sehenden Befehls wird ein self-signed-certificate erstellt.

Listing 3.2: Erstellen eines self-signed-certificates

```
# openssl req -x509 -newkey rsa:4096 -keyout privatekey.pem \
-out certificate.pem -sha256 -days 365
```

Die beiden erstellten Dateien und das damit verbundene Zertifikat ist ein Jahr gültig und muss in das Python-Backend eingebunden werden. Dafür wird die „main“-Funktion um „ssl_keyfile“ und „ssl_certfile“ erweitert, zu sehen in Listing 3.3.

Listing 3.3: Einbinden des self-signed-certificate

```
if __name__ == "__main__":
    uvicorn.run(
        app,
        host="0.0.0.0",
        port=8000,
        ssl_keyfile="./privatekey.pem",
        ssl_certfile="./certificate.pem",
        log_level="debug",
    )
```

Die Verbindungen zum Frontend/Backend sind jetzt mittels HTTPS verschlüsselt.

3.2.3 SSH ohne Passwort

Voraussetzung für einen Zugriff auf den Dienst-Server ohne Passwort ist die Installation des *openssh-server*. Bei CentOS ist dieser standardmäßig installiert.

Mittels *ssh-keygen* kann ein SSH-Schlüssel erstellt werden. Dieser kann mittels des in Listing 3.4 auf der nächsten Seite zu sehenden Befehls in das „.ssh“-Verzeichnis des Dienst-Servers kopiert werden. Die nächste Anmeldung auf dem Dienst-Server kann nun ohne Passworteingabe erfolgen.

Listing 3.4: Kopieren des SSH-Keys auf den Dienste-Server

```
ssh-copy-id -i ~/.ssh/id_rsa.pub ticketadmin@192.168.244.10
```

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
2.5	DNS-Einstellungen	10
2.6	Überprüfen des DNS mittels Namens	10
2.7	Aufrufen des Frontends mittels Name	11
2.8	Einrichtung der Tickets-Datenbank	12
2.9	Gantt-Diagramm	14
3.1	Erstellen eines Verzeichnisses und eines Cron-Tasks	18

Tabellenverzeichnis

1.1	Ansprechpartner Auftraggeber	1
1.2	Ansprechpartner Auftragnehmer	1
2.1	Netzwerkauslegung	7
3.1	Gefährdungsübersicht für Datenbank-Server und Web-Server	15
3.2	Technisch- Organisatorische Maßnahmen zur Verminderung der Risiken	16

Listings

2.1	Dienste-Freigabe einer CentOS-Firewall	9
2.2	DHCP-Einstellungen	10
2.3	Port-Freigabe einer CentOS-Firewall	11
2.4	Einrichtung Zugriff PostgreSQL	11
2.5	Ändern der tickets-Tabelle	11
2.6	Port-Freigabe einer CentOS-Firewall	13
3.1	Einrichtung eines Cron-Tasks	17
3.2	Erstellen eines self-signed-certificates	18
3.3	Einbinden des self-signed-certificate	18
3.4	Kopieren des SSH-Keys auf den Dienste-Server	19

Literaturverzeichnis

- [1] Karim Buzdar. *How to install PostgreSQL Database Server CentOS 8*. Vitux. Verfügbar unter: <https://vitux.com/postgresql-centos/>. abgerufen am 14.03.2022.
- [2] Michele Ferron. *Installing DNS Server on CentOS/RHEL using dnsmasq*. Zextras Suite & Zimbra OSE. 2021. Verfügbar unter: <https://community.zextras.com/dns-server-installation-guide-on-centos-7-rhel-7-and-centos-8-rhel-8-using-dnsmasq/>. abgerufen am 14.03.2022.
- [3] Aaron Kili. *How to Install PostgreSQL and pgAdmin in CentOS 8*. TecMint. 2021. Verfügbar unter: <https://www.tecmint.com/install-postgressql-and-pgadmin-in-centos-8/>. abgerufen am 14.03.2022.

Anhang

A Gantt-Diagramme

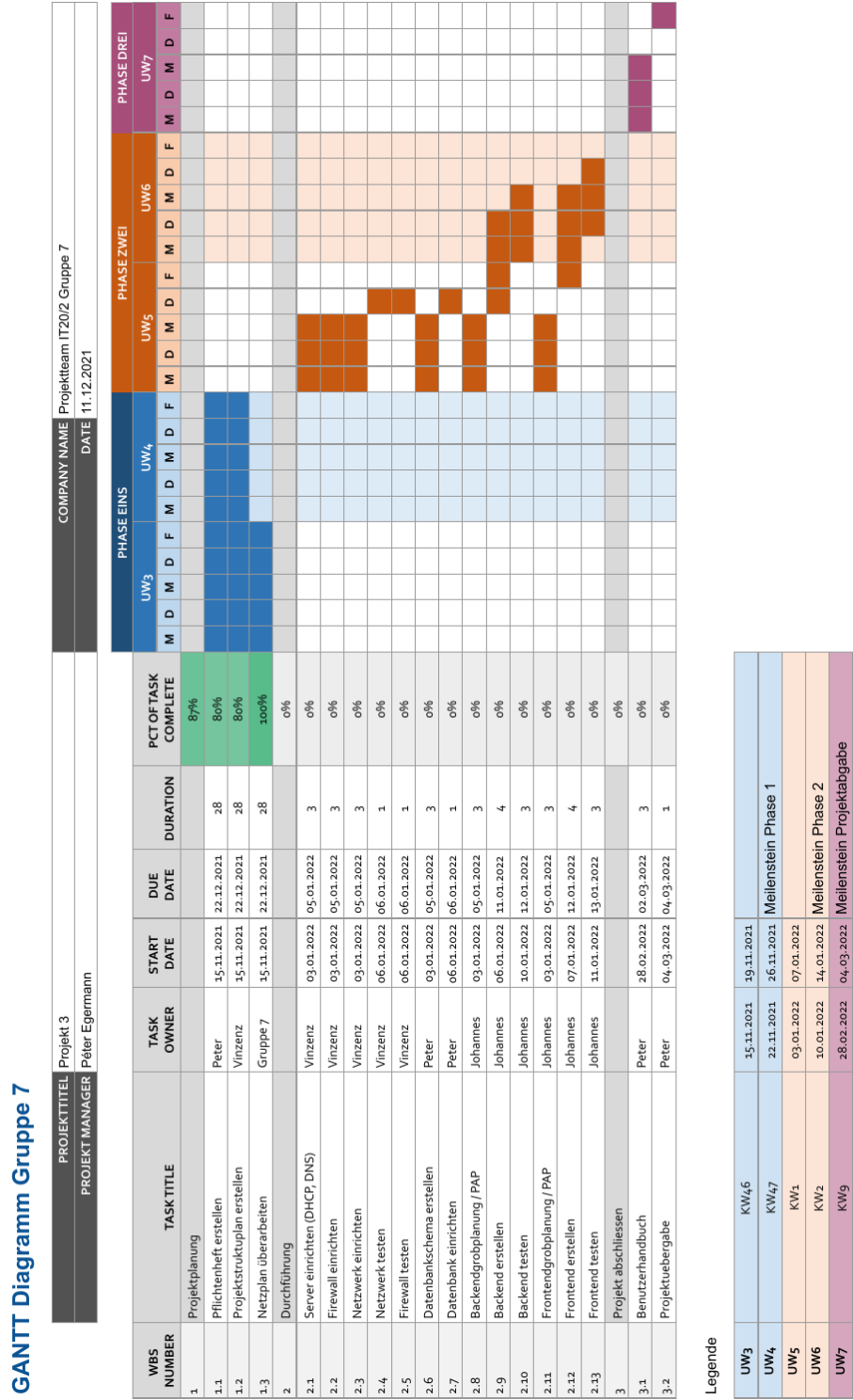


Abbildung A.1: Gantt-Diagramm

GANTT Diagramm Gruppe 7

PROJEKTITITEL			Projekt 3		COMPANY NAME		Projektteam IT20/2 Gruppe 7																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																					
PROJEKT MANAGER			P�ter Egernmann		DATE		11.12.2021																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																					
WBS NUMBER	TASK TITLE	TASK OWNER	START DATE	DUE DATE	DURATION	PCT OF TASK COMPLETE	PHASE INS									PHASE ZWEI									PHASE DREI																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																			
							UW3			UW4			UW5			UW6			UW7			UW8			UW9			UW10			UW11			UW12			UW13			UW14			UW15			UW16			UW17			UW18			UW19			UW20			UW21			UW22			UW23			UW24			UW25			UW26			UW27			UW28			UW29			UW30			UW31			UW32			UW33			UW34			UW35			UW36			UW37			UW38			UW39			UW40			UW41			UW42			UW43			UW44			UW45			UW46			UW47			UW48			UW49			UW50			UW51			UW52			UW53			UW54			UW55			UW56			UW57			UW58			UW59			UW60			UW61			UW62			UW63			UW64			UW65			UW66			UW67			UW68			UW69			UW70			UW71			UW72			UW73			UW74			UW75			UW76			UW77			UW78			UW79			UW80			UW81			UW82			UW83			UW84			UW85			UW86			UW87			UW88			UW89			UW90			UW91			UW92			UW93			UW94			UW95			UW96			UW97			UW98			UW99			UW100			UW101			UW102			UW103			UW104			UW105			UW106			UW107			UW108			UW109			UW110			UW111			UW112			UW113			UW114			UW115			UW116			UW117			UW118			UW119			UW120			UW121			UW122			UW123			UW124			UW125			UW126			UW127			UW128			UW129			UW130			UW131			UW132			UW133			UW134			UW135			UW136			UW137			UW138			UW139			UW140			UW141			UW142			UW143			UW144			UW145			UW146			UW147			UW148			UW149			UW150			UW151			UW152			UW153			UW154			UW155			UW156			UW157			UW158			UW159			UW160			UW161			UW162			UW163			UW164			UW165			UW166			UW167			UW168			UW169			UW170			UW171			UW172			UW173			UW174			UW175			UW176			UW177			UW178			UW179			UW180			UW181			UW182			UW183			UW184			UW185			UW186			UW187			UW188			UW189			UW190			UW191			UW192			UW193			UW194			UW195			UW196			UW197			UW198			UW199			UW200			UW201			UW202			UW203			UW204			UW205			UW206			UW207			UW208			UW209			UW210			UW211			UW212			UW213			UW214			UW215			UW216			UW217			UW218			UW219			UW220			UW221			UW222			UW223			UW224			UW225			UW226			UW227			UW228			UW229			UW230			UW231			UW232			UW233			UW234			UW235			UW236			UW237			UW238			UW239			UW240			UW241			UW242			UW243			UW244			UW245			UW246			UW247			UW248			UW249			UW250			UW251			UW252			UW253			UW254			UW255			UW256			UW257			UW258			UW259			UW260			UW261			UW262			UW263			UW264			UW265			UW266			UW267			UW268			UW269			UW270			UW271			UW272			UW273			UW274			UW275			UW276			UW277			UW278			UW279			UW280			UW281			UW282			UW283			UW284			UW285			UW286			UW287			UW288			UW289			UW290			UW291			UW292			UW293			UW294			UW295			UW296			UW297			UW298			UW299			UW300			UW301			UW302			UW303			UW304			UW305			UW306			UW307			UW308			UW309			UW310			UW311			UW312			UW313			UW314			UW315			UW316			UW317			UW318			UW319			UW320			UW321			UW322			UW323			UW324			UW325			UW326			UW327			UW328			UW329			UW330			UW331			UW332			UW333			UW334			UW335			UW336			UW337			UW338			UW339			UW340			UW341			UW342			UW343			UW344			UW345			UW346			UW347			UW348			UW349			UW350			UW351			UW352			UW353			UW354			UW355			UW356			UW357			UW358			UW359			UW360			UW361			UW362			UW363			UW364			UW365			UW366			UW367			UW368			UW369			UW370			UW371			UW372			UW373			UW374			UW375			UW376			UW377			UW378			UW379			UW380			UW381			UW382			UW383			UW384			UW385			UW386			UW387			UW388			UW389			UW390			UW391			UW392			UW393			UW394			UW395			UW396			UW397			UW398			UW399			UW400			UW401			UW402			UW403			UW404			UW405			UW406			UW407			UW408			UW409			UW410			UW411			UW412			UW413			UW414			UW415			UW416			UW417			UW418			UW419			UW420			UW421			UW422			UW423			UW424			UW425			UW426			UW427			UW428			UW429			UW430			UW431			UW432			UW433			UW434			UW435			UW436			UW437			UW438			UW439			UW440			UW441			UW442			UW443			UW444			UW445			UW446			UW447			UW448			UW449			UW450			UW451			UW452			UW453			UW454			UW455			UW456			UW457			UW458			UW459			UW460			UW461			UW462			UW463			UW464			UW465			UW466			UW467			UW468			UW469			UW470			UW471			UW472			UW473			UW474			UW475			UW476			UW477			UW478			UW479			UW480			UW481			UW482			UW483			UW484			UW485			UW486			UW487			UW488			UW489			UW490			UW491			UW492			UW493			UW494			UW495			UW496			UW497			UW498			UW499			UW500			UW501			UW502			UW503			UW504			UW505			UW506			UW507			UW508			UW509			UW510			UW511			UW512			UW513			UW514			UW515			UW516			UW517			UW518			UW519			UW520			UW521			UW522			UW523			UW524			UW525			UW526			UW527			UW528			UW529			UW530			UW531			UW532			UW533			UW534			UW535			UW536			UW537			UW538			UW539			UW540			UW541			UW542			UW543			UW544			UW545			UW546			UW547			UW548			UW549			UW550			UW551			UW552			UW553			UW554			UW555			UW556			UW557			UW558			UW559			UW560			UW561			UW562			UW563			UW564			UW565			UW566			UW567			UW568			UW569			UW570			UW571			UW572			UW573			UW574			UW575			UW576			UW577			UW578			UW579			UW580			UW581			UW582			UW583			UW584			UW585			UW586			UW587			UW588			UW589			UW590			UW591			UW592			UW593			UW594			UW595			UW596			UW597			UW598			UW599			UW600			UW601			UW602			UW603			UW604			UW605			UW606			UW607			UW608			UW609			UW610			UW611			UW612			UW613			UW614			UW615			UW616			UW617			UW618			UW619			UW620			UW621			UW622			UW623			UW624			UW625			UW626			UW627			UW628			UW629			UW630			UW631			UW632			UW633			UW634			UW635			UW636			UW637			UW638			UW639			UW640			UW641			UW642			UW643			UW644			UW645			UW646			UW647			UW648			UW649			UW650			UW651			UW652			UW653			UW654			UW655			UW656			UW657			UW658			UW659			UW660			UW661			UW662			UW663			UW664			UW665			UW666			UW667			UW668			UW669			UW670			UW671			UW672			UW673			UW674			UW675			UW676			UW677			UW678			UW679			UW680			UW681			UW682			UW683			UW684			UW685			UW686			UW687			UW688			UW689			UW690			UW691			UW692			UW693			UW694			UW695			UW696			UW697			UW698			UW699			UW700			UW701			UW702			UW703			UW704			UW705			UW706			UW707			UW708			UW709			UW710			UW711			UW712			UW713			UW714			UW715			UW716			UW717			UW718			UW719			UW720			UW721			UW722			UW723			UW724			UW725			UW726			UW727			UW728			UW729			UW730			UW731			UW732			UW733			UW734			UW735			UW736			UW737			UW738			UW739			UW740			UW741			UW742			UW743			UW744			UW745			UW746			UW747			UW748			UW749			UW750			UW751			UW752			UW753			UW754			UW755			UW756			UW757			UW758			UW759			UW760			UW761			UW762			UW763			UW764			UW765			UW766			UW767			UW768			UW769			UW770			UW771			UW772			UW773			UW774			UW775			UW776			UW777			UW778			UW779			UW780			UW781			UW782			UW783			UW784			UW785			UW786			UW787			UW788			UW789			UW790			UW791			UW792			UW793			UW794			UW795			UW796			UW797			UW798			UW799			UW800			UW801			UW802			UW803			UW804			UW805			UW806			UW807			UW808			UW809			UW810			UW811			UW812			UW813			UW814			UW815			UW816			UW817			UW818			UW819			UW820			UW821			UW822			UW823			UW824			UW825			UW826			UW827			UW828			UW829			UW830			UW831			UW832			UW833			UW834			UW835			UW836			UW837			UW838			UW839			UW840			UW841			UW842			UW843			UW844			UW845			UW846			UW847			UW848			UW849			UW850			UW851			UW852			UW853			UW854			UW855			UW856			UW857			UW858			UW859			UW860			UW861			UW862			UW863			UW864			UW865			UW866			UW867			UW868			UW869			UW870			UW871			UW872			UW873			UW874			UW875			UW876			UW877			UW878			UW879			UW880			UW881			UW882			UW883			UW884			UW885			UW886			UW887			UW888			UW889			UW890			UW891			UW892			UW893			UW894			UW895			UW896			UW897			UW898			UW899			UW900			UW901			UW902			UW903			UW904			UW905			UW906			UW907			UW908			UW909			UW910			UW911			UW912			UW913			UW914			UW915			UW916			UW917			UW918			UW919			UW920			UW921			UW922			UW923			UW924			UW925			UW926			UW927			UW928			UW929			UW930			UW931			UW932			UW933			UW934			UW935			UW936			UW937			UW938			UW939			UW940			UW941			UW942			UW943	

B Netzwerkplan

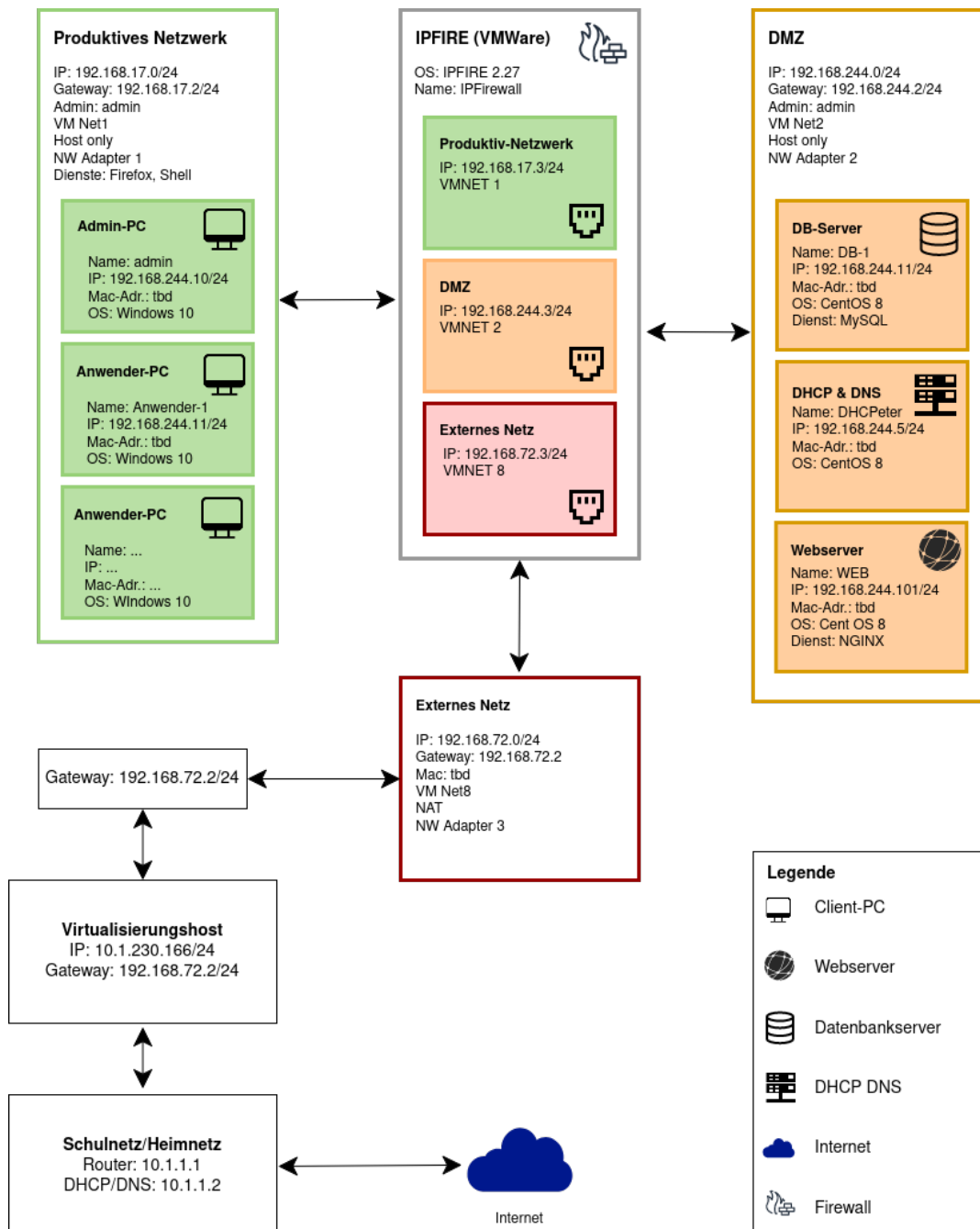


Abbildung B.1: Netzwerkplan