# 3.2 Analyse

1.

Grundsätzlich sollten nur Systeme von außerhalb erreichbar sein, die auch von Kunden genutzt werden sollen.

Das Firewall-System darf nicht öffentlich erreichbar sein, um die Sicherheit des Netzwerkes zu garantieren, damit keine Partei die Einstellung von außerhalb des Netzwerkes verändern kann. Es stellt den zentralen Sicherheitsknoten zur Trennung der Netzwerke dar, und würde das gesamte Netzwerk gefährden, wenn es kompromittiert wäre.

Der DNS-Server muss nicht von außen erreichbar sein, da er nur für interne Geräte eingerichtet werden soll. Deswegen ist die Ermöglichung eines öffentlichen Zugriffes nicht nötig.

Der DHCP-Server vergibt IP-Adressen an interne Systeme und muss daher ebenfalls nicht öffentlich erreichbar sein.

Der Web-Server muss von außerhalb erreichbar sein, da spezifiziert wurde, dass Kunden über die Website Tickets erstellen können sollen (Siehe 2.1 Ausgangslage). Daher wird der Web-Server in der DMZ platziert.

Der Datenbank-Server darf nicht von außen erreichbar sein, um die Sicherheit der Daten zu gewährleisten. Hierfür wird der Datenbank-Server im Grünen Netz platziert und Kommunikation mit dem öffentlichen Netz findet ausschließlich über den Webserver statt. Dieser darf von der DMZ in das Grüne Netz hinein auf den Datenbankserver zugreifen.

2.

a) Der Kunde befindet sich im Roten Netz, wenn der Kunde ein Ticket erstellt, geht eine Anfrage an den Webserver (Doubtful-Joy09.de) über die Firewall. Hierzu muss die Firewall eine Verbindung von außerhalb in die DMZ erlauben (optimal nur für https Port 443), um dem Kunden die Website darstellen zu können. Wenn dieser dann ein Ticket erstellt, schickt er Daten zurück den Webserver. Der Webserver benötigt nun die Möglichkeit Daten auf dem Datenbankserver zu speichern. Hierfür muss eine Verbindung von der DMZ von IP 192.168.109.4 in das Grüne Netz zu IP 192.168.9.5 von der Firewall erlaubt sein (optimal nur für einen bestimmten Port, bspw. 3306).

b) Der Administrator befindet sich im Grünen Netz am Admin-PC, von hier hat er internen Zugriff auf alle drei Systeme. Die Firewall bietet ein Webinterface unter 192.168.9.3:444, welches im Grünen Netz erreichbar ist. Der DNS / DHCP Server befindet sich ebenfalls im Grünen Netz und muss so eingerichtet werden, dass er nur von dort aus erreichbar ist.

c) Für die Webserver-Administration muss der Administrator, welcher sich im Grünen Netz befindet, auf den Webserver in der DMZ zugreifen. Die Firewall muss dafür die Kommunikation vom Grünen Netz in die DMZ zwischen 192.168.9.7 und 192.168.109.4 erlauben.

d) Der Akteur ist hierbei ein Mitarbeiter der Doubtful-Joy und befindet sich im Grünen Netz. Hierfür muss nur die Firewall des Datenbankservers Verbindungen aus dem Grünen Netz gewähren. Die Daten verlassen hierbei das Grüne Netz nicht.