VPN-Server & VM-Server

Detailstudie

Inhalt

[Dokumentbeschreibung 2](#_bookmark0)

[Ziel 2](#_bookmark1)

[Soll-Wert 2](#_bookmark2)

[Materialliste 3](#_bookmark3)

[Gant-Diagramm: 1 4](#_bookmark4)

[OpnSense-Router 5](#_bookmark5)

[Download 5](#_bookmark6)

[Installation 5](#_bookmark7)

[WebGUI 7](#_bookmark8)

[VPN-Server 8](#_bookmark9)

[Netzwerktopologie 8](#_bookmark10)

[Konfiguration 9](#_bookmark11)

[Authorities 9](#_bookmark12)

[Certificate 10](#_bookmark13)

[Users 10](#_bookmark14)

[VPN-Server 11](#_bookmark15)

[Firewall 13](#_bookmark16)

[VMware ESXi 14](#_bookmark17)

[Installation 14](#_bookmark18)

[Zusätzliche Interfaces 17](#_bookmark19)

[DHCP-Server hinzufügen 18](#_bookmark20)

[Firewall-Regeln für mehrere Interfaces 18](#_bookmark21)

[Pass-Regel 19](#_bookmark22)

[Block-Regel 19](#_bookmark23)

[Gantt-Diagramm: 2 20](#_bookmark24)

[Ist-Wert 20](#_bookmark25)

[Analyse 20](#_bookmark26)

# Dokumentbeschreibung

Wegen der angehenden Pandemie seit letztem Jahr waren sehr viele Unternehmen angewiesen auf das Home-Office. Dies brachte viele Vorteile mit sich, aber sowohl auch ein grosses Problem bei der IT-Sicherheit. Grund dafür ist, das Fehlen an Sicherheits-Tools, welche eigentlich nur in Firmennetzwerken eingesetzt werden und nicht in Heimnetzwerken. Nicht nur der Mangel an Sicherheits-Tools ist ein Problem, aber auch das Vernachlässigen von Sicherheitsmassnahmen, welche normalerweise am Arbeitsplatz strengstens befolgt werden. Diese erwähnten Massnahmen und Sicherheitsinstrumente, welche sich zuhause befinden und befolgt werden, reichen wahrscheinlich nicht aus, um sensible Unternehmensdaten zu schützen.

In diesem Dokument geht es über das Aufsetzen und konfigurieren eines VPN-Servers mit OpnSense und das eingebaute OpenVPN, damit ein gesicherter Zugang zum Firmennetzwerk jeder Zeit für ausgewählte Benutzer gewährleistet ist und die Sicherheitslücken füllen. Wir gehen über die verschiedenen Schritte des OpnSense-Router, OpenVPN und VMWare ESXi, welches wir für unseren VM-Server nutzen, ins genauste Detail.

Für was die verschiedenen Konfigurationen in diesen Schritten zuständig sind, wird in diesem Dokument auch beschrieben. Man wird in diesem Projekt nur mit virtuellen Maschinen arbeiten und nicht mit zusätzlicher Hardware.

# Ziel

Mein Ziel für dieses Projekt, ist es, eine sichere Verbindung zum Firmennetzwerk durch einen VPN-Tunnel mit OpnSense zu verschaffen, um auf den VM-Server des jeweiligen Netzwerkes zugreifen zu können, egal wo und zu jeder Zeit. Für den VPN-Server werde ich eine zweifache Authentifizierung verlangen, um so mehr Sicherheit für die Umgebung zu gewährleisten.

# Soll-Wert

Das Projekt soll am Ende der Frist diese wichtigen Punkte erfüllt sein:

* Der OpnSense-Router funktioniert einwandfrei, mit mehreren tauglichen Interfaces.
* Die verschiedenen Interfaces können keine Verbindung mit anderen Interfaces aufbauen, ohne eine VPN-Verbindung
* Jedes Netzwerk hat einen funktionierenden VPN-Server, mit dem man von überall aus und wann man möchte, darauf zugreifen kann.
* Die VPN-Server verschaffen Zugriff auf ihre Netzwerke für bestimmte Benutzer mit Zertifikat und Login-Informationen (Two-Factor Authentification).
* Die VM-Server sind erreichbar und man kann durch eine VPN-Verbindung auch auf VMs zugreifen.

# Materialliste

Da hier hauptsächlich und auch nur mit virtuellen Maschinen gearbeitet wird, gibt es keine zusätzliche Hardware. Bei Hardware-Umsetzung solle man am besten für den VM-Server, Server-Hardware nutzen und für den Router natürlich auch einen physikalischen Router selbstverständlich.

Was man braucht um das Projekt umzusetzen:

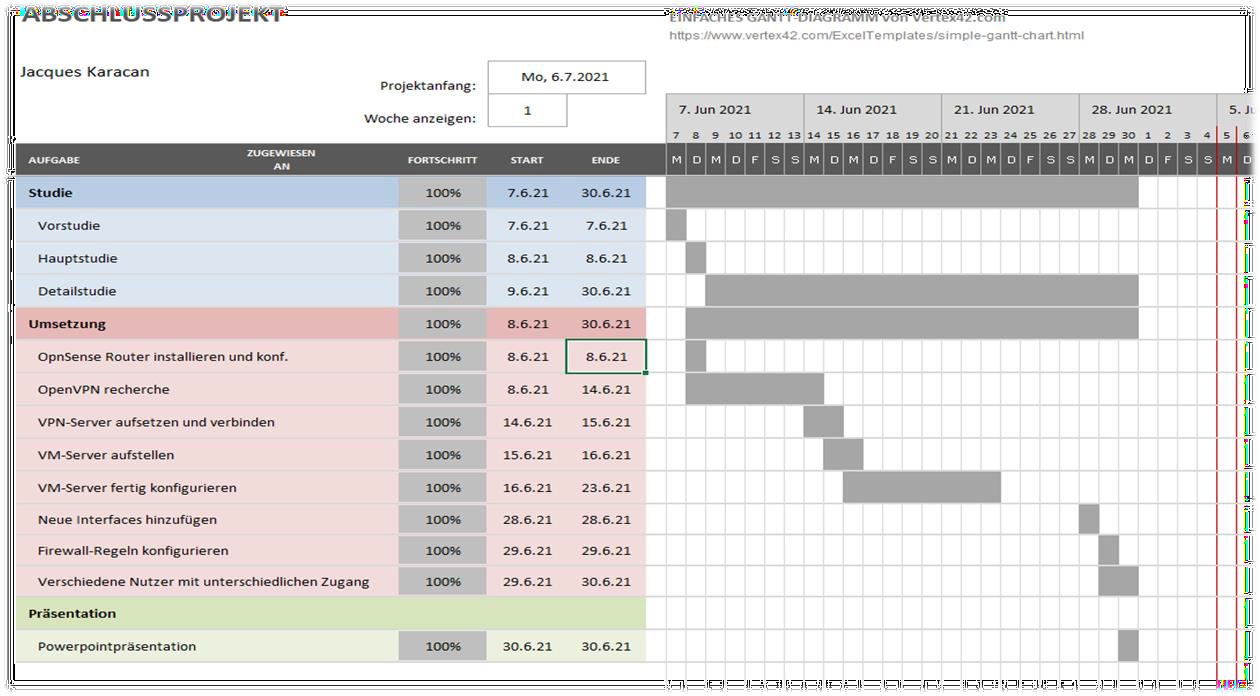
* OpnSense-ISO-File (Für das Aufsetzen des OpnSense-Routers)
* Windows-ISO oder Ubuntu-ISO (Für den Zugriff auf das Web-GUI, um Konfigurationen zu machen)
* VMWare ESXi-ISO (ISO für den VM-Server)
* OpenVPN Connect (Client für OpenVPN)

Für das Projekt braucht man nur diese Dateien und den OpenVPN-Client, welche man alle Online herunterladen kann.

Bei der VMWare ESXi hat man eine Testzeit von bis zu 60 Tagen.



# Gant-Diagramm: 1

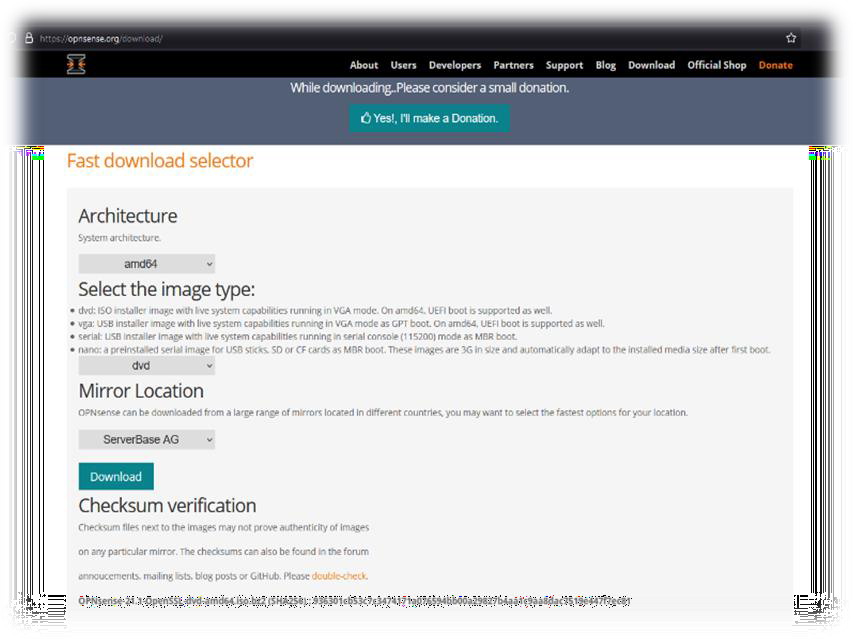
Mein erwarteter Zeitaufwand für das Projekt für die nächsten Wochen.

# OpnSense-Router

OpnSense ist eine Open-Source Firewall-Distribution und Routing-Plattform. OpnSense ermöglicht das Nutzen eines DHCP, DNS und das wichtigste für unser Projekt; einen VPN- Server. Kurzgesagt, sie ist der Router für unser Netzwerk

## Download

Das ISO-File für den OpnSense-Router ist auf der offiziellen Website von OpnSense zu finden.

«Architecture» wählt man je nach Systemarchitektur aus. In meinem Fall ist meine Auswahl auf «amd64», da mein System natürlich auf 64bit läuft.

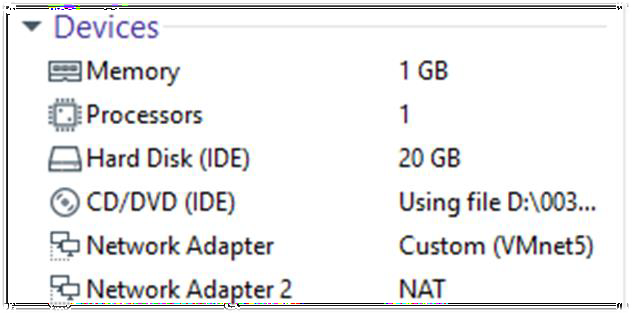
«Select the image type» wählt man aus, wie man das Betriebssystem auf den Rechner installieren möchte. Ich habe mich für «dvd» entschieden.

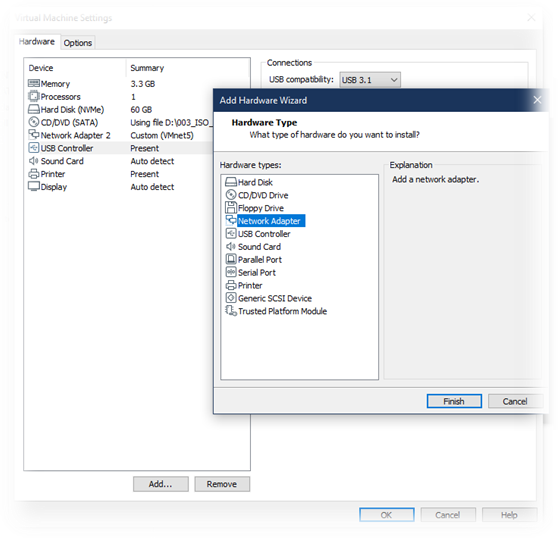
«Mirror Location» ist von welchem Server man das File herunterladen möchte.

## Installation

Den OpnSense-Router tut man wie gewohnt auf VMWare Workstation aufstellen. Bei den Netzwerkkonfigurationen auf der VM ist jedoch etwas zu beachten;

Da der OpnSense-VM der Router ist, müssen zwei Netzwerkadapter vorhanden sein. Der Network Adapter 2 dient als WAN Interface, während der Network Adapter als LAN dient.



Der WAN gewährleistet den Zugang auf das Internet, währen das LAN das Lokale Netzwerk ist. Wichtig ist, dass bewusst ist, welcher Port als WAN und LAN auf OpnSense dient.

Falls man den WAN-Port auf OpnSense bei VMWare als LAN konfiguriert hat und vice versa, funktioniert dieser natürlich nicht. Wenn man nicht sicher ist, welches was ist, kann man die MAC- Adresse dieser Ports beide auf OpnSense und VMWare nachschauen.

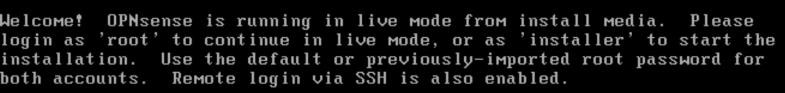
Falls die VM und OpnSense problemlos lauft, wird man im Terminalfenster mit dieser Tabelle begrüsst. Für den Set-up Boot muss man [Enter] bzw. 1 eingeben.

Nachdem OpnSense sich fürs erste fertig konfiguriert hat, wird man mit der IP-Adresse vom LAN und WAN und Login- Fenster begrüsst. Die LAN- Adresse 192.168.1.1/24 ist standartmässig aus von OpnSense vorkonfiguriert.

Bei OpnSense ist das default login «root» und das default Passwort «opnsense», aber da

OpnSense im Live Modus ist, muss man sich als erstes erst mit dem login «installer» und Passwort

«opnsense» einloggen. Grund dafür ist, dass die Konfiguratoinen nicht gespeichert sind, weil OpnSense eigentlich nicht ganz installiert ist und bei einem Shutdown oder Reboot alles verloren geht.



Nachdem man sich als Installer eingeloggt hat, kommt ein neues blaues Fenster auf.

Danach gibt man in den folgenden Eingaben [Enter] ein;

«Guided installation» → Disk für die Insallation eingeben → «GPT/UEFI mode» → Neues Root- Passwort einstellen → Reboot

Wenn man das gemacht hat und zurück zum vorherigen Fenster kommt, kann man auf eine Option auswählen. Auf Wunsch kann man die aus Standart zugewiesene LAN-Adresse ändern mit der Option

##### Assign interface IP-Address.

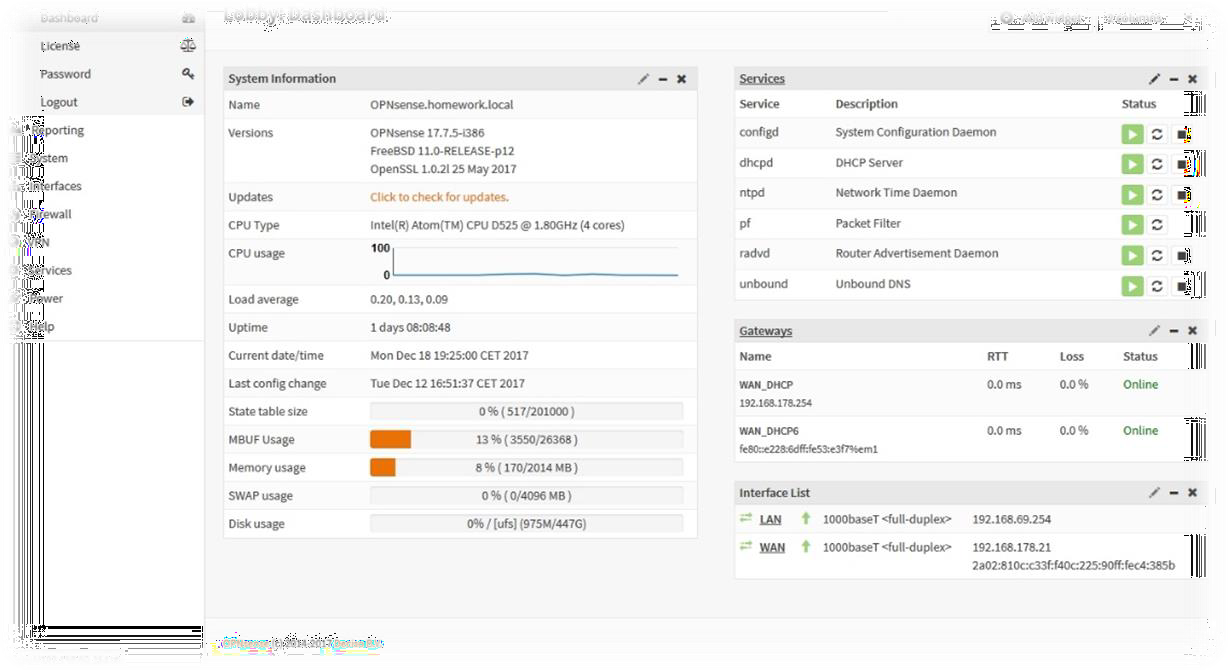
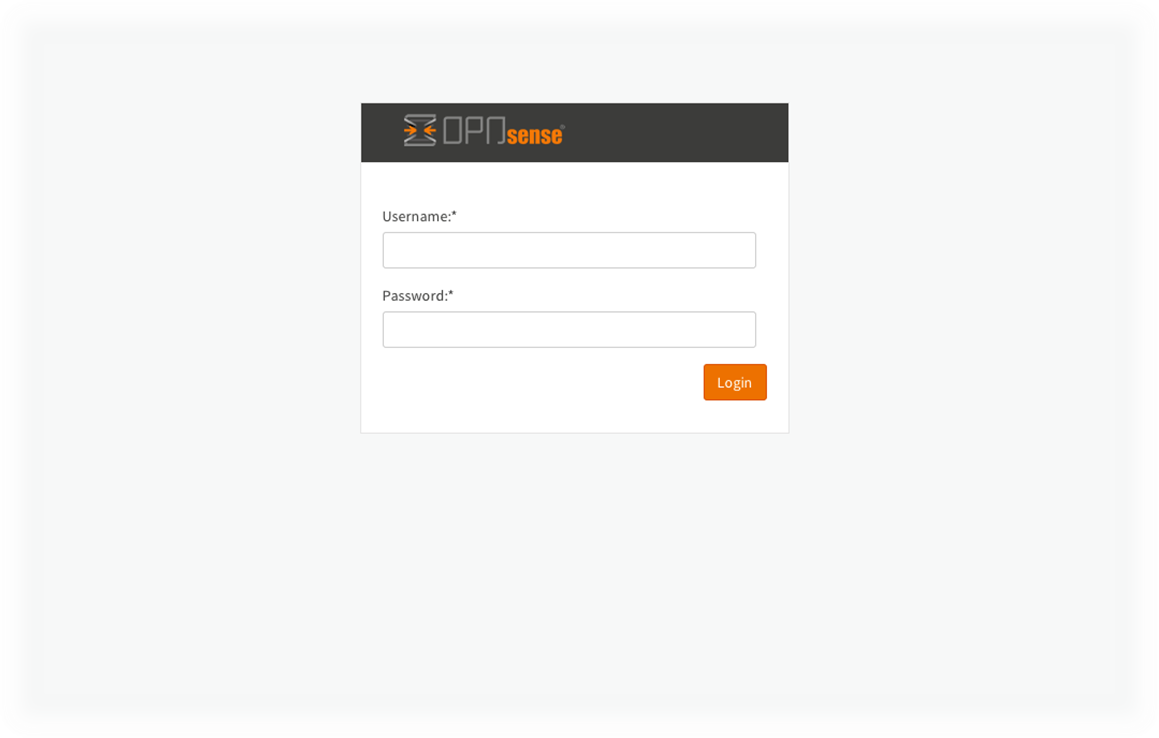
Ab diesem Punkt muss man nichts wichtiges machen, um mit der Konfiguration des OpenVPN- Servers anzufangen.

## WebGUI

Im Browser einer anderen VM, welches mit dem Router verbunden ist bzw. sich im Netzwerk befinden, die IP-Adresse des

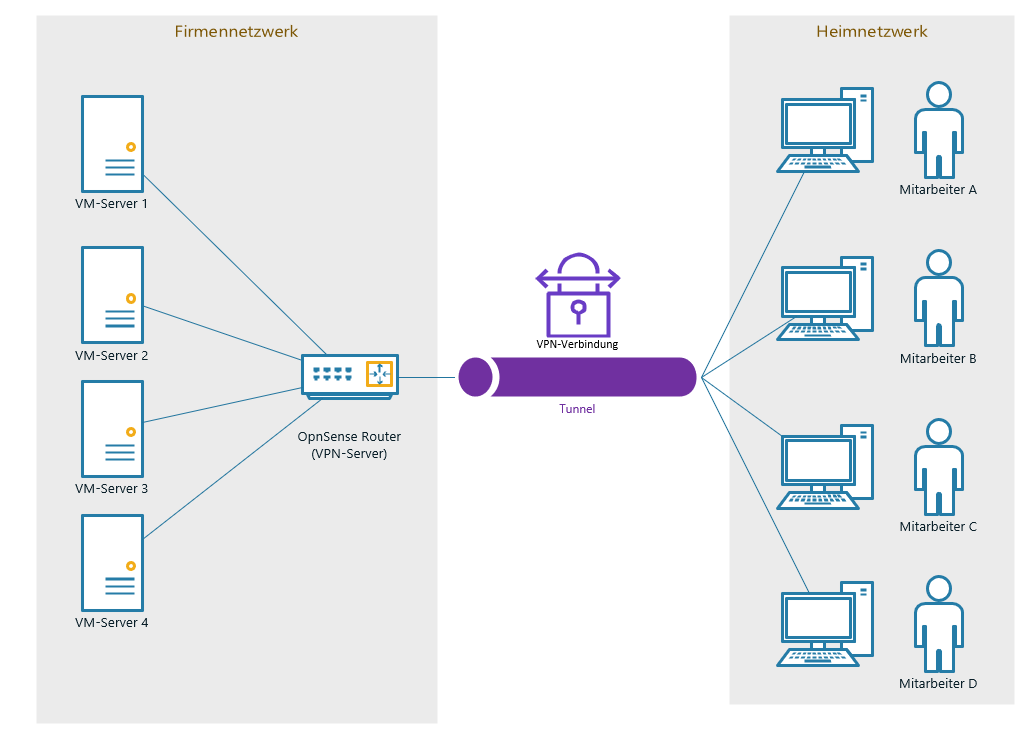
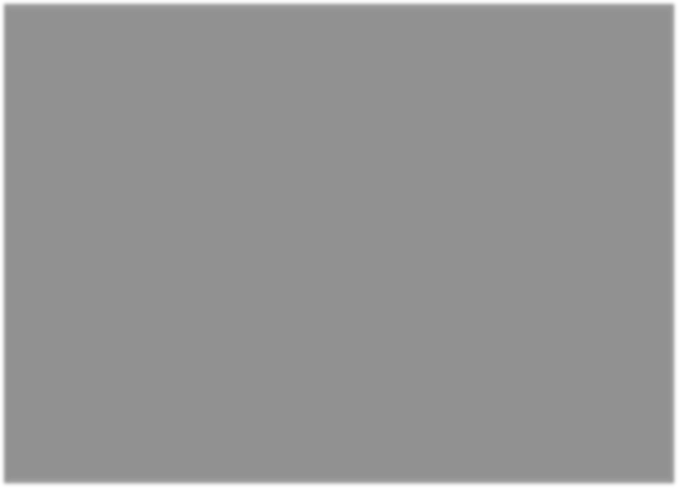
Routers in die Searchbar eingeben und sich mit den

default Login-informationen einloggen.



# VPN-Server

## Netzwerktopologie



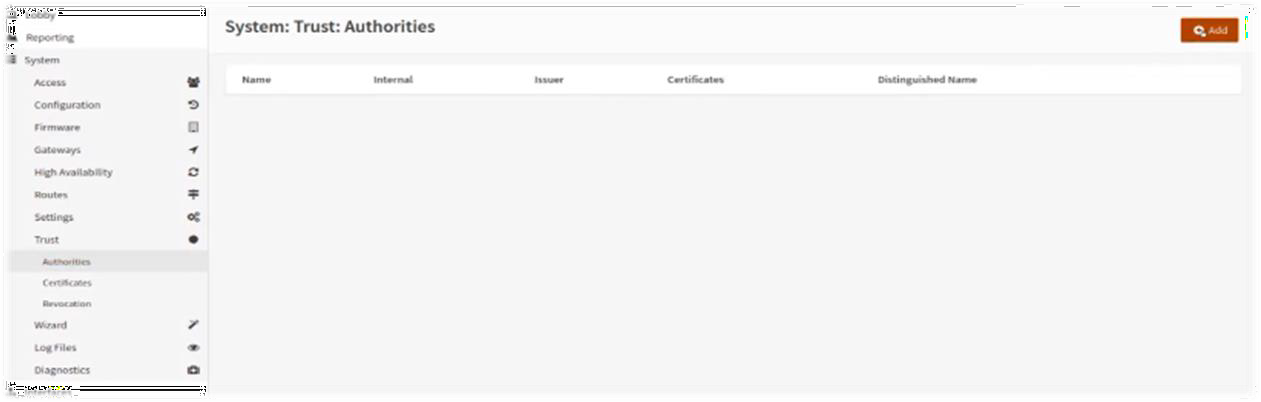
In der Netzwerktopologie ist deutlich zu erkennen, dass der VPN-Server, welches sich im OpnSense Router selbst befindet, einen abgesicherten Zugang von Zuhause aus gewährleistet. Jeder Mitarbeiter hat einen bestimmten Zugang auf bestimmte Subnetze von wo auch immer man möchte, welche durch eine zweifache-Authentifizierung abgesichert ist;

* + VM-Server-1 → 192.168.10.0 – Netzwerk 1
  + VM-Server-2 → 192.168.11.0 – Netzwerk 2
  + VM-Server-3 → 192.168.12.0 – Netzwerk 3
  + VM-Server-4 → 192.168.13.0 – Netzwerk 4

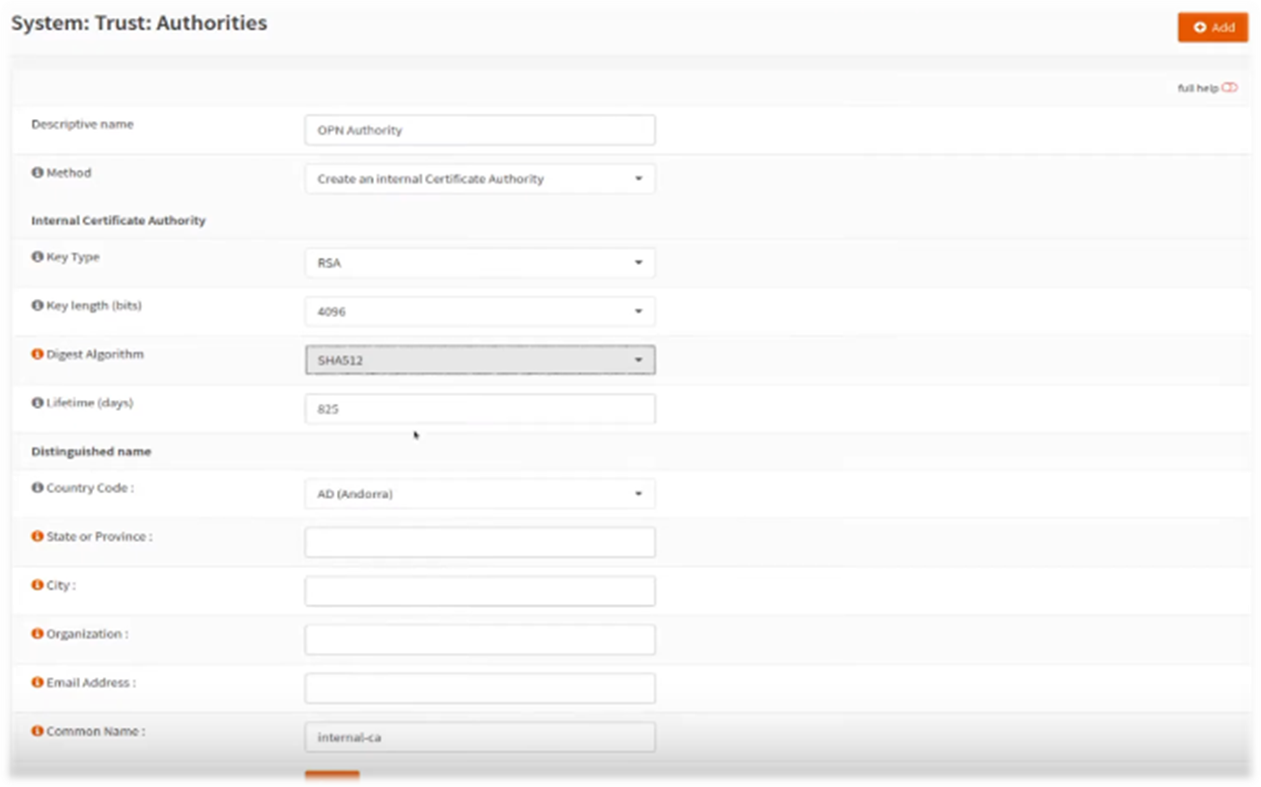
Dies wurde bei meinem Projekt so eingeplant, dass ich vier unterschiedliche Interfaces konfiguriert habe und sich im jedem dieser Subnetze ein VPN und VM-Server befindet. Wie man zusätzliche Interfaces hinzufügen kann, ist weiter im Dokument zu finden.

## Konfiguration

### Authorities



Unter [System] → [Trust] → [Authorities] und dann auf [Add] erstellt man Authoritäten.



Als «Descriptive Name» kann man einen gewünschten Namen geben, mit dem man das Authority- Zertifikat erkennen kann.

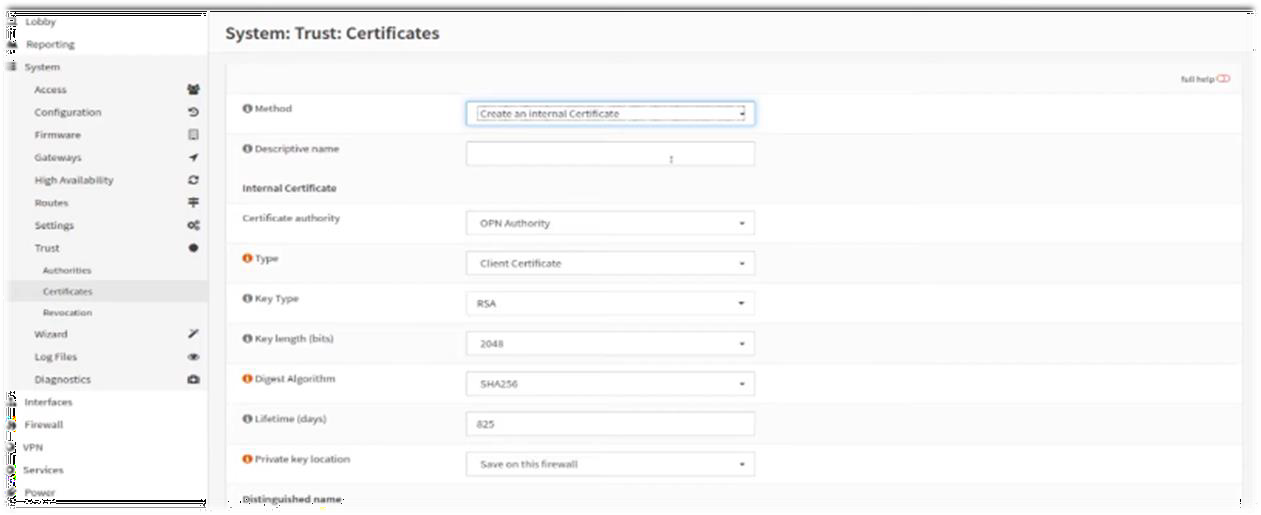
«Key Type» → «RSA».

«Key length» → empfiehlt sich 4096 für mehr Sicherheit.

«Digest Algorithm» → empfiehlt sich SHA512 für eine stärkere Verschlüsselung und Sicherheit. Der letzte Abschnitt ist abhängig vom jeweiligen Wohnort.

### Certificate

Unter dem Abschnitt [Authorities], ist [Certificates] zu finden.



Bei «Method» → «Create an internal Certificate», da wir ein neues Zertifikat generieren möchten.

«Descriptive Name» → Einen Namen, mit dem wir das Certificate identifizieren können.

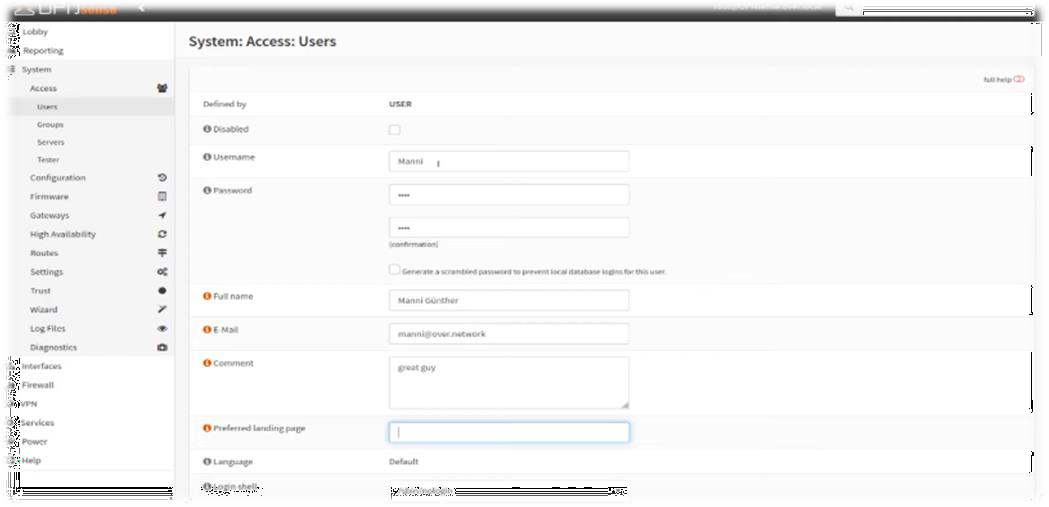
«Type» → «Server Certificate», welche Art von Zertifikat.

«Key Type», «Digest Algorith», «Key length» ist gleich wie beim «Authorities».

«Private key location» → «Save on this Firewall» .

### Users

Unter [System] → [Access] → [Users] und [Add] kann man neue Benutzer hinzufügen.



«Username» → Den Benutzername für den Login festlegen.

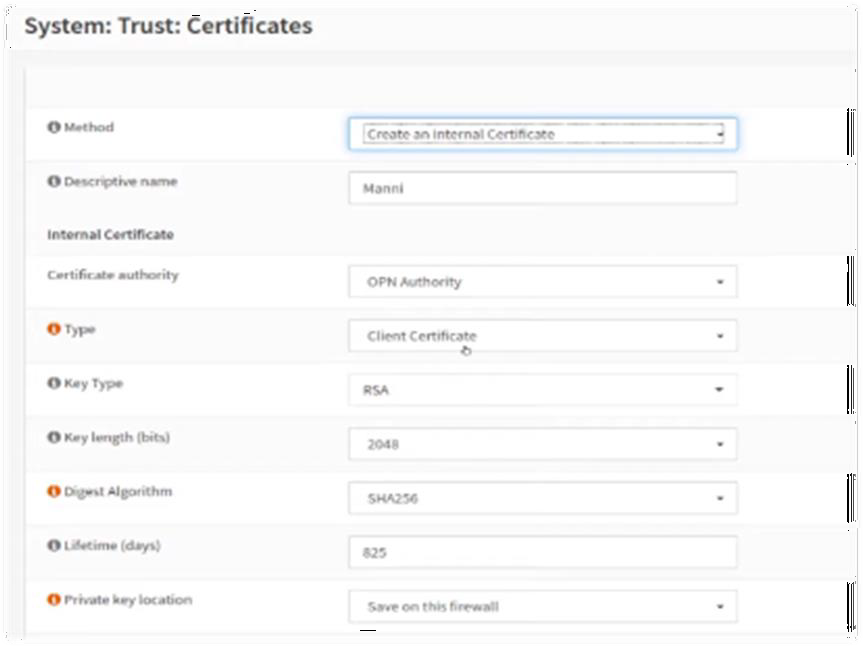
«Password» → Das Passwort für den Benutzer festlegen.

«Full name» → Der volle Name dieser Person.

«E-Mail» → Gibt man eine E-Mail-Adresse ein.

«Certificate» → Die Box mit der beschriftung «Click to create a user certificate» muss angekreuzt sein, um ein User Certifiacte zu erstellen.

Nachdem man auf Save clickt, wird man zum Certificat-Fenster weiter geführt.

«Methods» → «Create an internal Certificate»

«Certificate Authority» → Das Ausgewählte Certificate Authority vom jeweiligen VPN-Server

«Type» → «Client Certificate»

«Key Type», «Key length»,

«Digest Algorithm» → Identisch zu den vorherigen Einstellungen

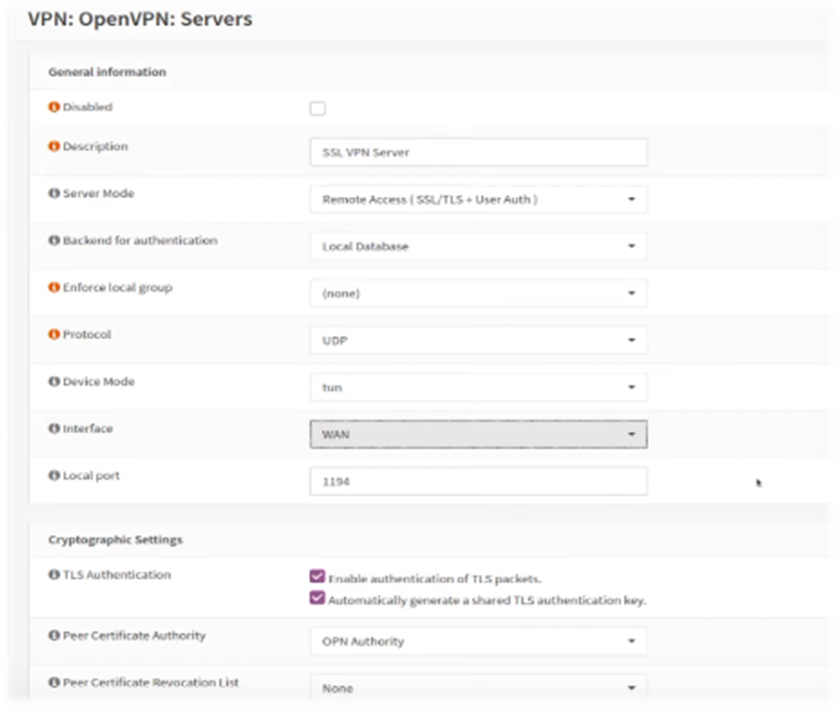
«Private Key Location» →

«Save on this Firewall»

Nachdem man auf [Save] drückt, kommt man zurück auf das vorherige Fenster. Um diesen Abschnitt abzuschliessen, drückt man auf [Save and go back].

### VPN-Server

Unter [VPN] → [OpenVPN] → [Servers] kann man den VPN-Server aufstellen.

«Server Mode» → «TLS + User Auth» für eine zweifach- Authentifizierung.

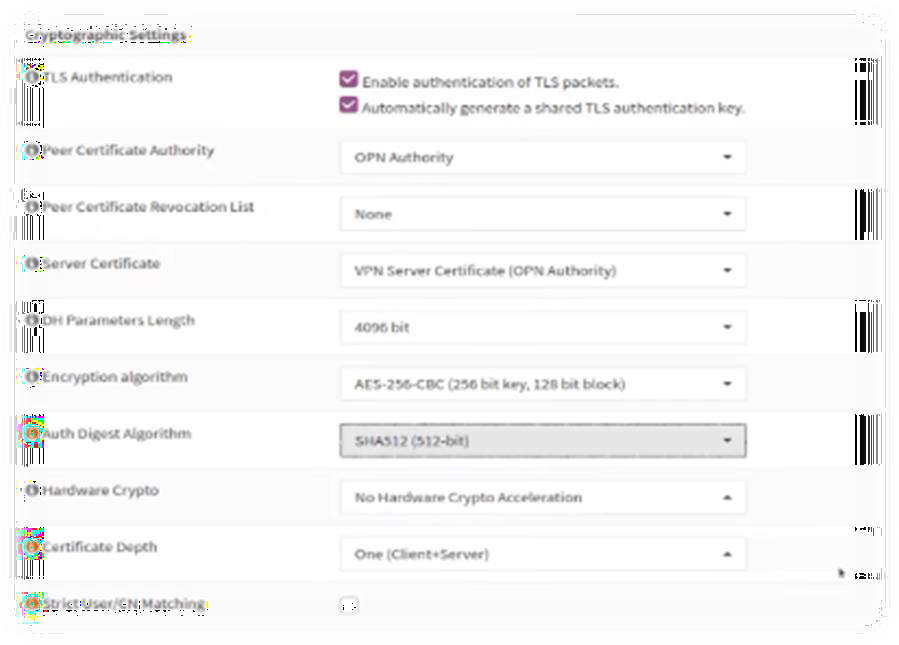
«Protocol» → «UDP»

«Interface» → WAN, damit man von überall auf den VPN- Server zugreifen kann.

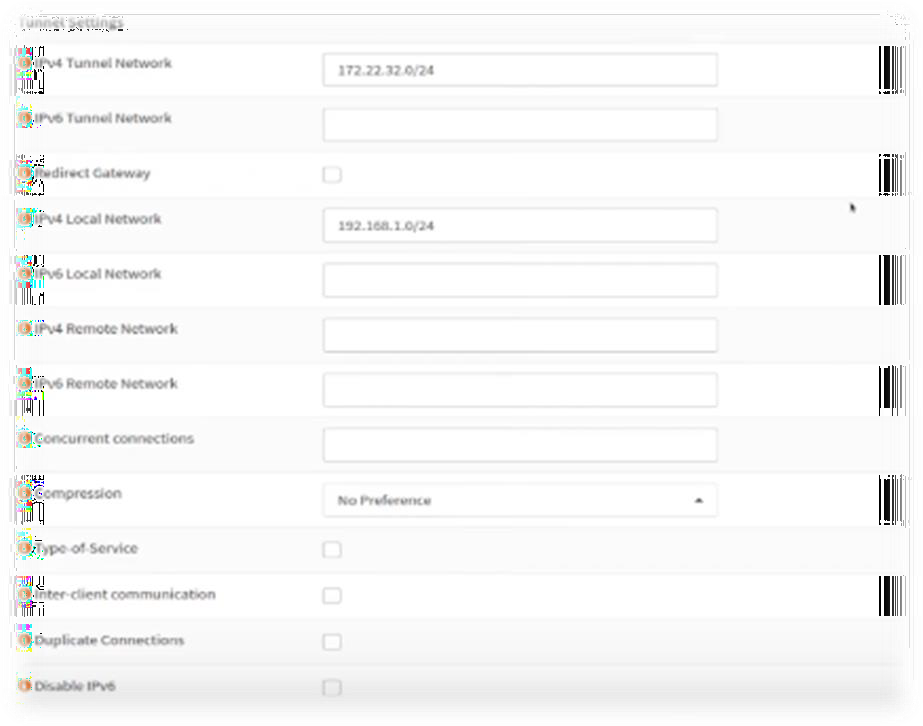
«Local port» → Auf welches Port der VPN-Server zugreift

«TLS Authentication» → Die Boxen sind vorgewählt.

«Peer Certificate Authority» → Das erstellte Authority- Certificate.

«Server Certificate» → Das erstellte Server-Zertifikat für den jeweiligen VPN-Server.

Die jeweiligen Verschlüsselungsoptionen sind in diesem Screenshot enthalten.

«IPv4 Local Network» → Auf welches Netzwerk dieser VPN-Server Zugriff verschaffen soll. (Bsp.

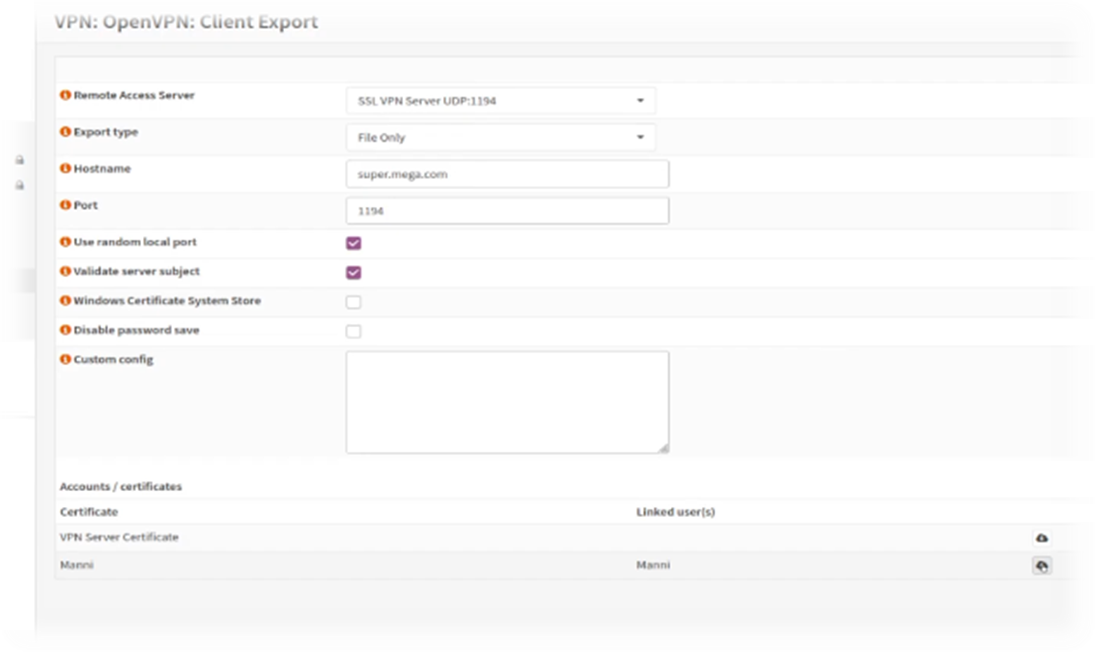
192.168.1.0/24)

«IPv4 Tunnel Network» → Was für eine IP-Adresse der Tunnel haben soll.

Da wir kein IPv6 benutzen, kreuzen wir «Disable IPv6» an.»

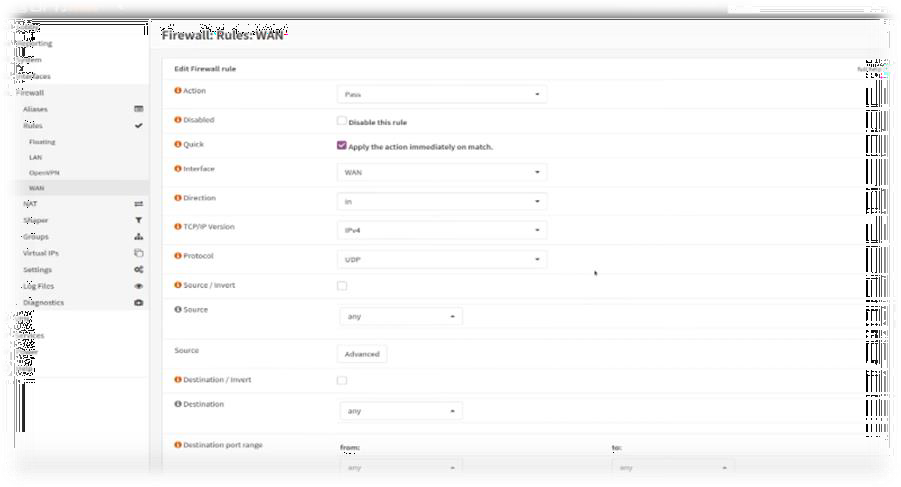
Mit den Konfigurationen abgeschlossen, läuft der VPN- Server ohne jegliche Einschränkungen.

# Firewall



Unter [Firewall] → [Rules] → [Interface] kann man die Firewall-Regeln der jeweiligen Interfaces konfigurieren

Für das [WAN] Interface muss diese Regel konfiguriert werden, damit der OpenVPN-Server Zugang bekommt von aussen.

Das Interface → «WAN»

«Direction» → «in»

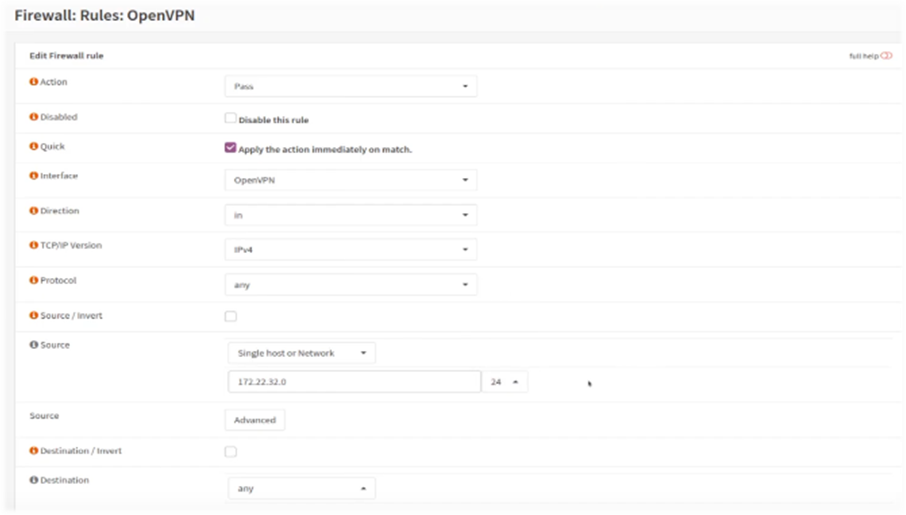
«Protocol» → «UDP»

«Destination port range»

→ «From: OpenVPN, to: OpenVPN»

Nachdem man [Save] drückt kommt man zurück und muss auf [Apply Changes] drücken.

#### Das [WAN] muss man nur einmal machen!

Unter den Firewall Rules von **OpenVPN** muss man diese Konfigurationen machen, damit VPN- Nutzer Zugang auf das Lokale Netzwerk bekommen.

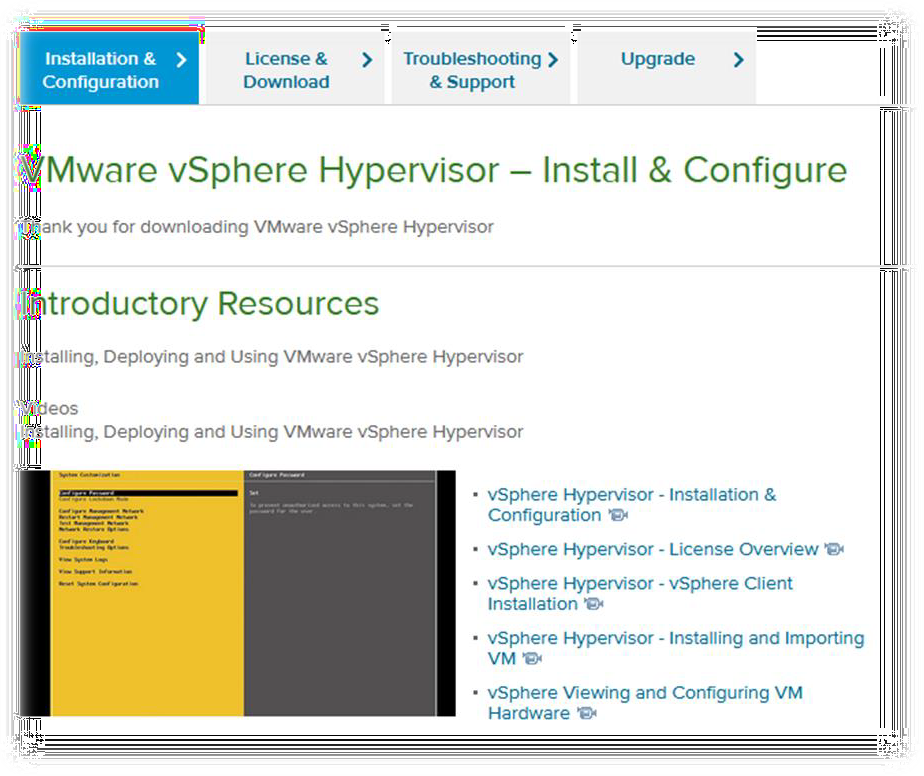
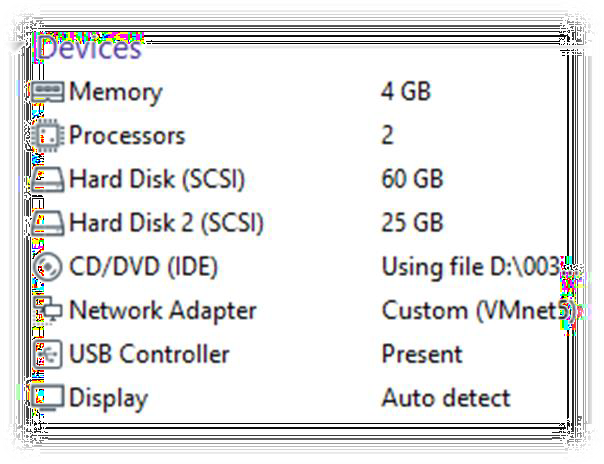
«Source: Single host or Network» ist welches spezifische VPN-Adresse man nutzt. Danach [Save] und [Apply Changes]

Nach diesen Konfigurationen kann man nun endlich die Zertifikate für die Benutzer herunterladen, und sich mit dem OpenVPN-Client namens: «OpenVPN Connect» verbinden. Wichtig ist dass «Export Type» «File Only» ist. Mit dem roten Kreis tut man es herunterladen

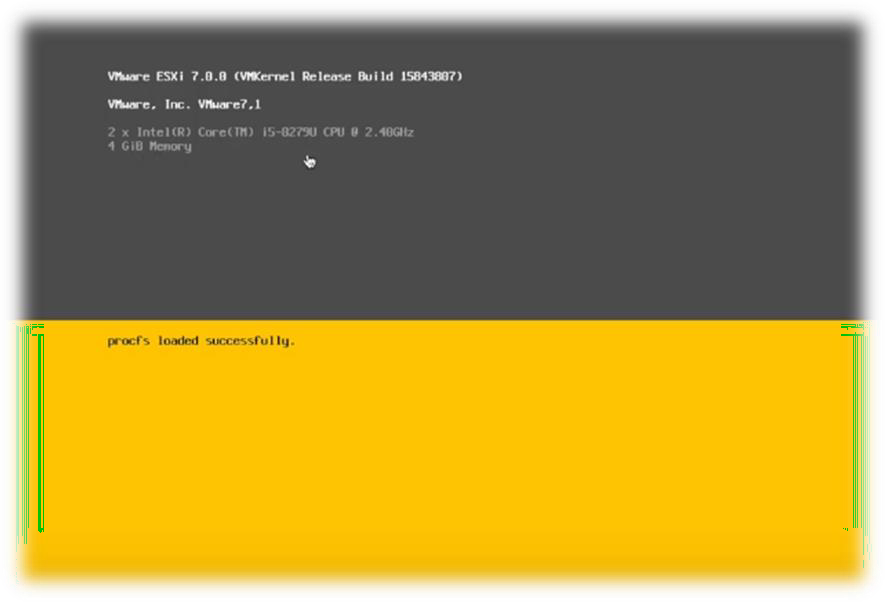
# VMware ESXi

VMWare ESXI wird im Bereich der Server-Virtualisierung benutzt. Mithilfe der Hypervisoren lassen sich virtuelle Maschinen auf Basis eines oder mehrerer physischer Hostsysteme erstellen.

## Installation

Den VM-Server tut man wie OpnSense auf VMWare als VM aufsetzen. Das ISO-File bezieht man unter «License und Download», nachdem man sich registriert hat.

Für den VM-Server sollte man mindestens 4GB RAM nutzen und eine Speichermenge an mindestens 40GB. Beachte den Netzwerk Adapter in jedem VM-Server.



Nachdem die VM läuft und

alles vorbereitet, kommt ein Konfigurationsfenster auf.

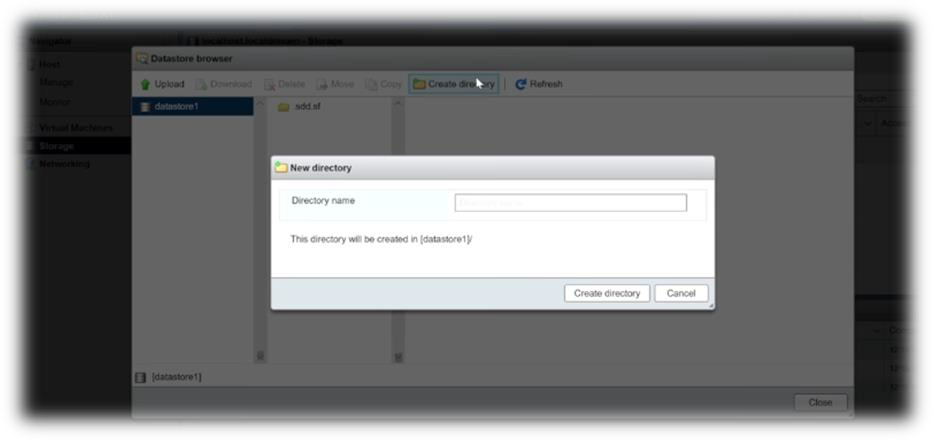
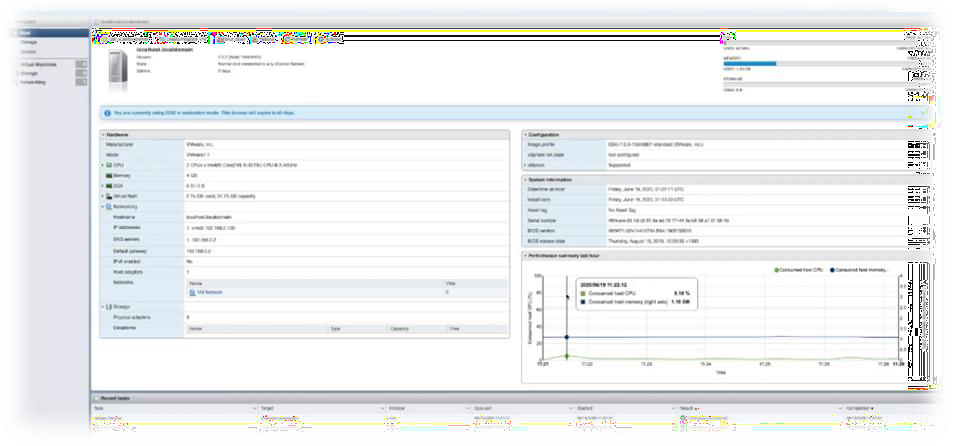
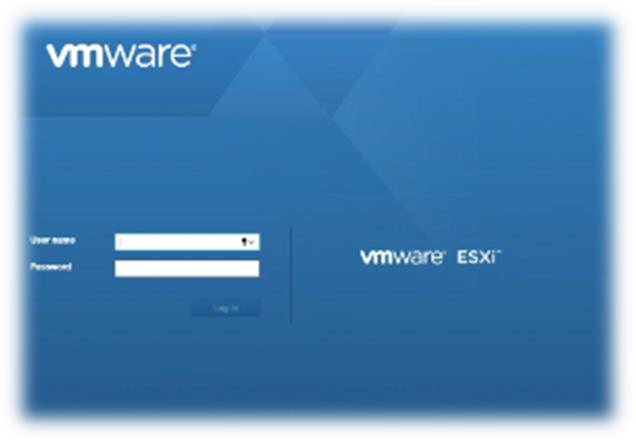
14

Nachdem man die Lizenzvereinbarung akzeptiert hat, kann man weiter mit der Konfiguration machen.

Man wählt hier das Installationsmedium aus, damit VMware ESXi installiert werden kann.

Nachher muss man ein Root Passwort festlegen, für den Zugang auf VMware ESXi’s WebGUI. Es wird nachhinein gefragt, ob man die Installation durchnehmen möchte. Dies muss man akzeptieren.

Wenn die Installation beendet ist, wird die IP-Adresse des VM-Servers unten deutlich angezeigt.



Um den VM-Server konfigurieren zu können, muss man wie

gewohnt mit einer separaten Windows oder Linux VM, welches im gleichen Netzwerk ist, die IP-Adresse im Webbrowser einzugeben.

Man wird dann vom WebGUI Login-Fenster begrüsst. In den zwei Feldern kommt der User name und Root-Passwort ein. Der «User name» ist vom Standard her «Root» und das Passwort hat man vorher selbst eingestellt.

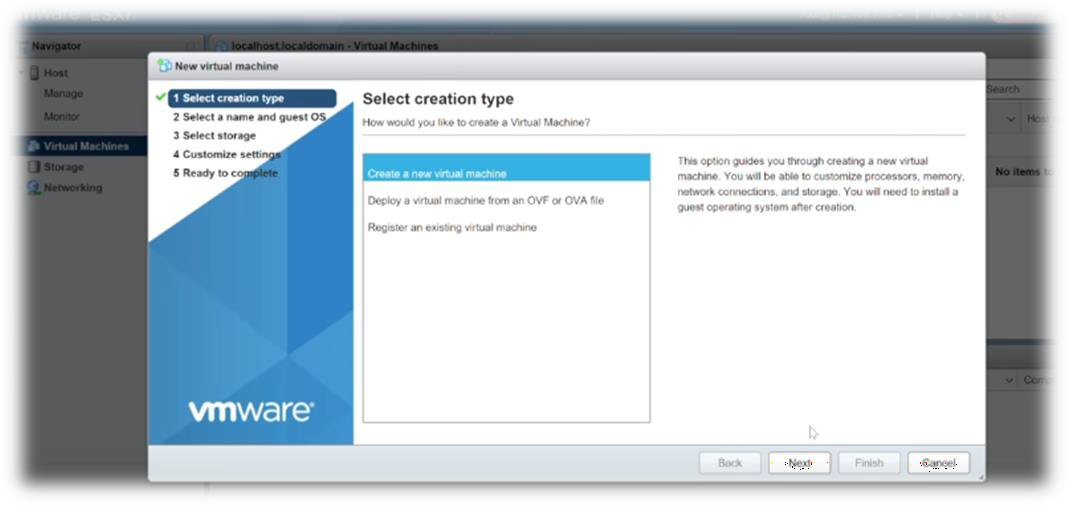
Das GUI-Dashboard von

VMware ESXi seht so aus.

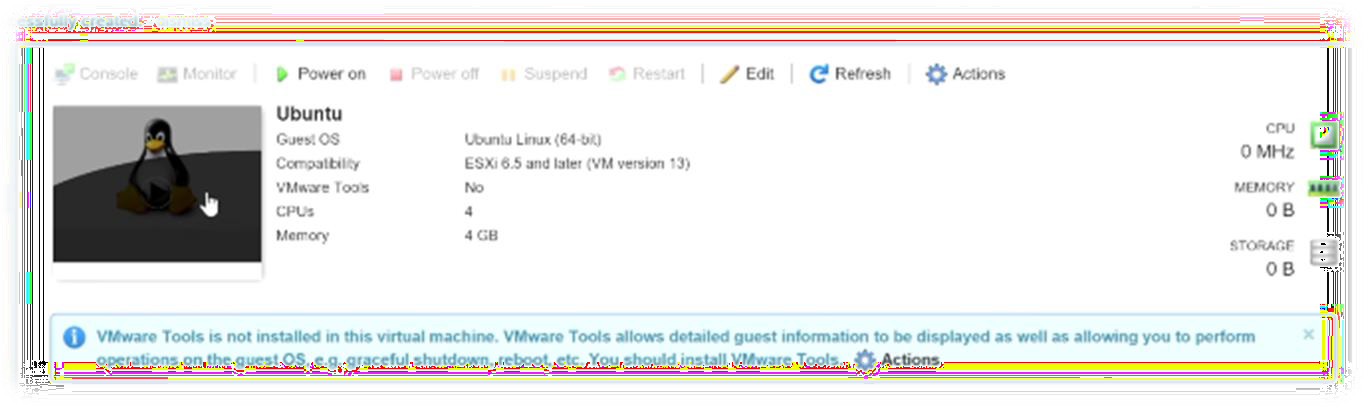
Nun kann man mit dem Aufstellen der VMs anfangen.

Unter [Storage] → [Data store] kann man neue Verzeichnisse erstellen, um das ISO-Files zu uploaden. Aus diesem ISO-File beziehen die VMs ihr Betriebssystem.

Unter [Virtual Machine] → [Create/Register VM] erstellt man eine VM. Die Schritte sind so ähnlich wie im VMWare Workstation. Die

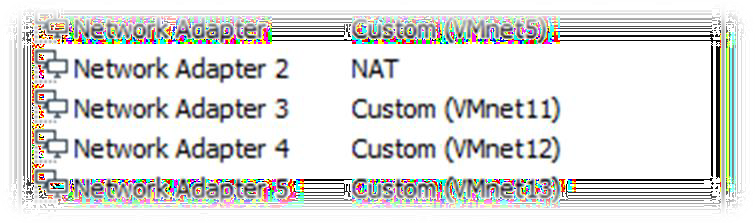


VM-Hardware konfiguriert man ab [Customize Settings] und den Speicherplatz in [Select Storage].

Falls alles erfolgreich abgeschlossen ist, kann man die VM in einem kleinen Fenster mit [Power On] zum Laufen bringen. Diese VM kann man wie gerade jetzt darauf zugreifen oder mit RDP zugreifen.

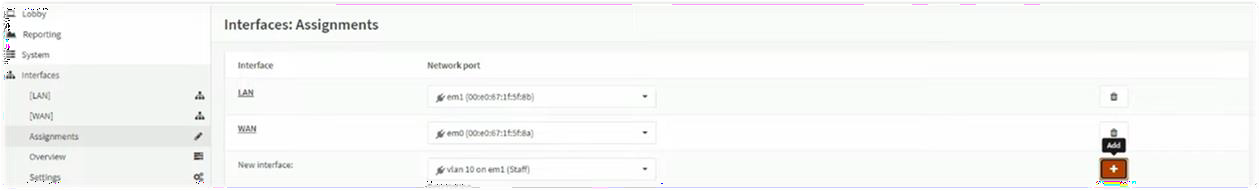
# Zusätzliche Interfaces

Um zusätzliche Interfaces zum Router hinzuzufügen, muss man dies natürlich auf VMware

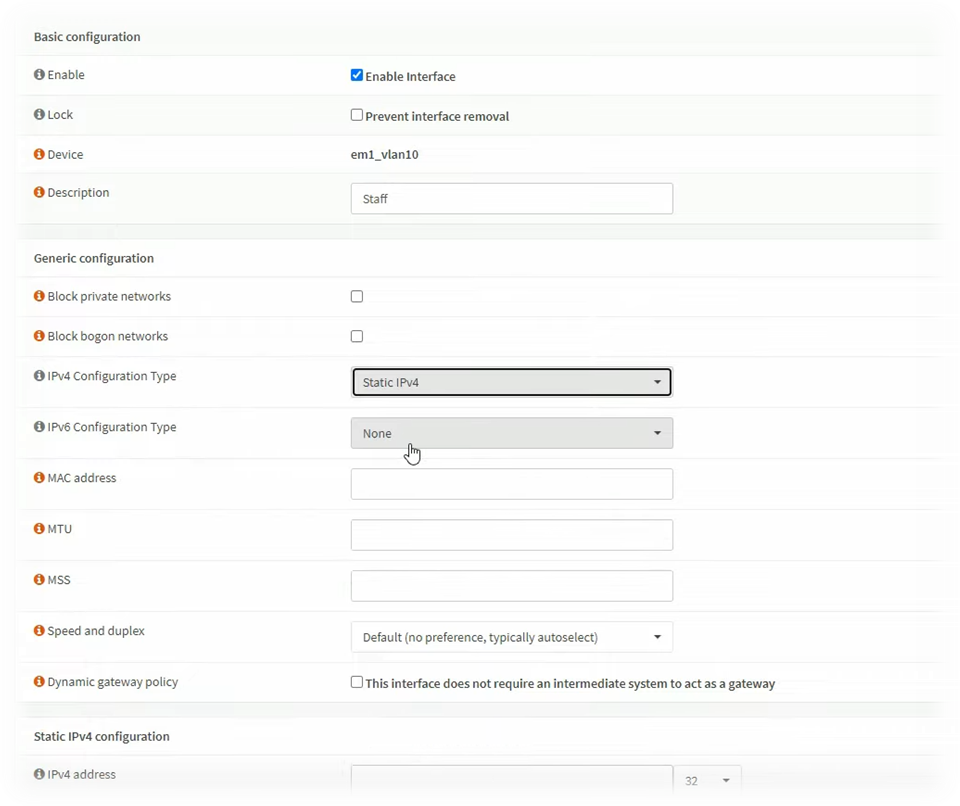
vornehmen und mehr Netzwerk Adapters hinzufügen.

Wichtig ist, dass beim Verbinden der Clients die Windows-Firewall ausgeschaltet sein muss, sonst blockiert die Windows-Firewall die Verteilung der IP-Adresse für den Client.

Unter [Interfaces] → [Assignments] kann man das neu erstellte Interface hinzufügen.



Indem man das neue Interface auf «New Interface» auswählt und auf [Add] drückt, wird das neue Interface hinzugefügt, jedoch muss diese manuell eingestellt werden, indem man auf der Bezeichnung des neuen Interfaces drückt (Rot umkreist).

«Enable Interface» → Ankreuzen, um das Interface zu aktivieren.

«IPv4 Configuration Type» → «Static IPv4» um eine statische IP-Adresse zu setzen. IPv6 bleibt aus «None».

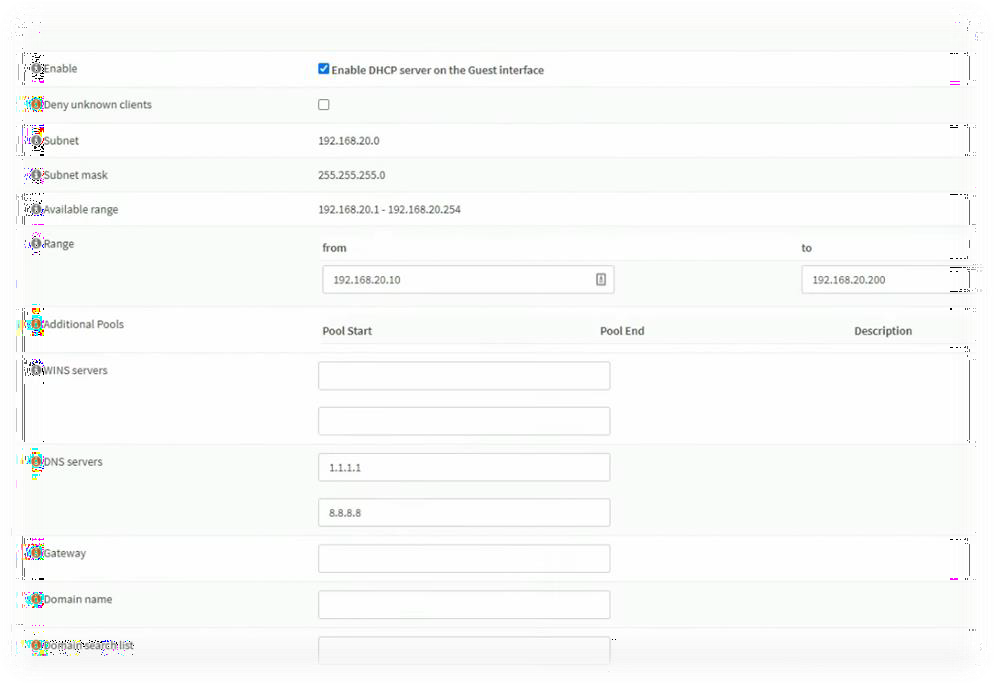
«IPv4 address» → Gewünschte IP- Adresse setzen (Bsp. 192.168.2.1) +

Subnetz.

Um es abzuschliessen, auf [Save] und [Apply Changes] clicken.

# DHCP-Server hinzufügen

Unter [Services] → [DHCPv4] → [Gewünschtes Interface] kann man den DHCP-Server für spezifische Subnetze erstellen.

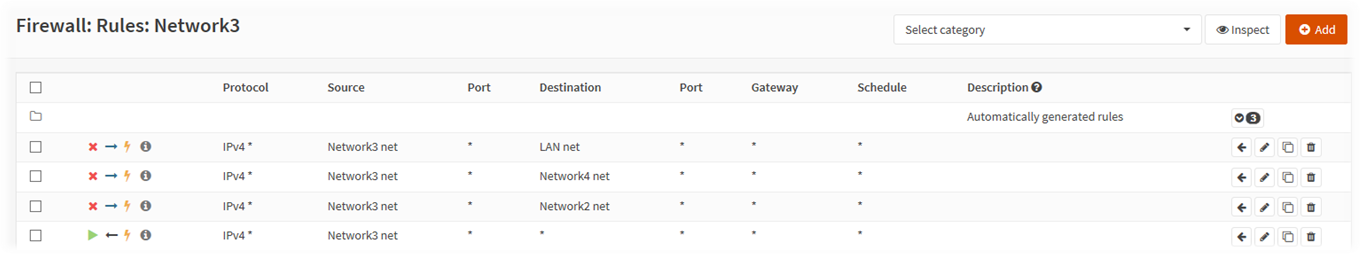


# Firewall-Regeln für mehrere Interfaces

«Range» → Range der verfügbaren IP-Adressen für den DHCP-Server.

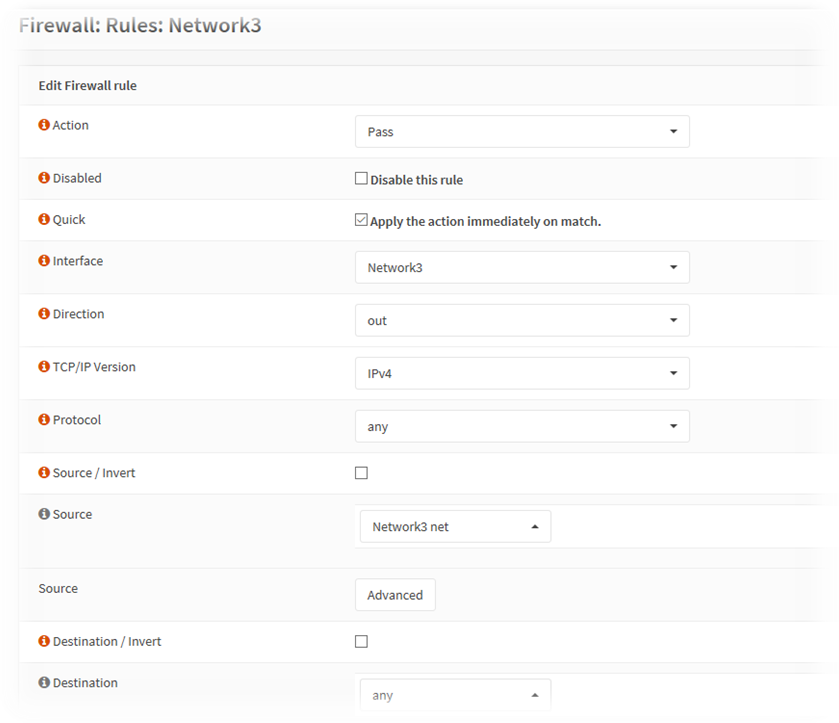
«DNS-Server» → DNS-Server der Wahl eingeben.

Danach auf [Save] drücken, um die Änderungen einzustellen.

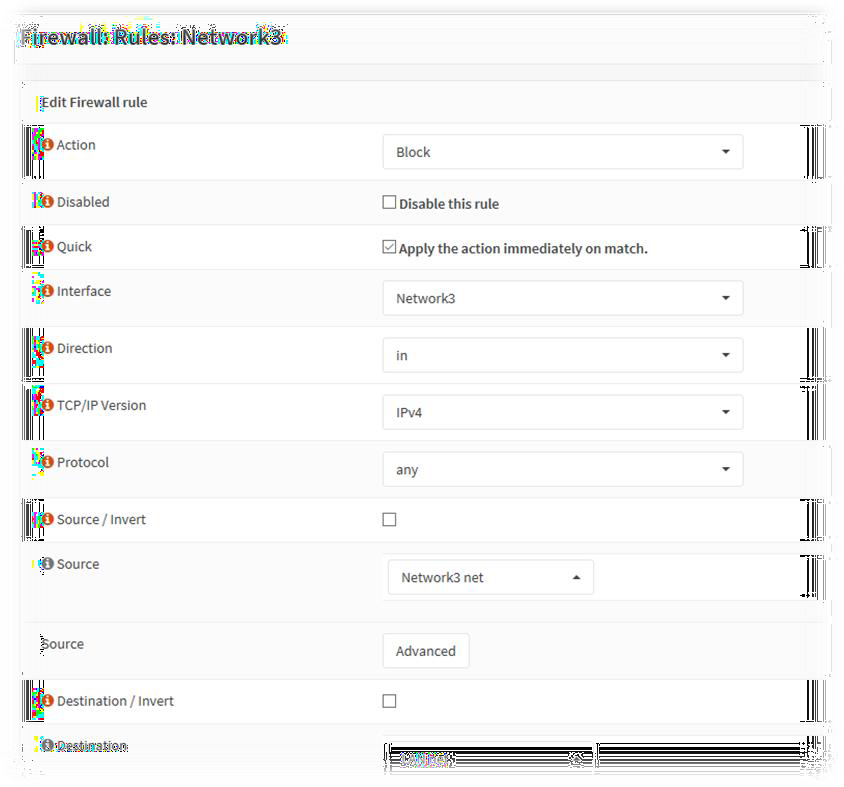


Um den Zugang ins Internet bzw. WAN zu ermöglichen, muss man eine bestimmte «Pass»-Regel erstellen. Diese bestimmte Regel verschafft aber auch Zugang auf die andere Netzwerke, jedoch werden wir jede offene Stelle zu den anderen Netzwerken, mit einzelnen «Block»-Regeln verschliessen. Hierarchisch müssen die «Block»-Regeln über die «Pass»-Regel sein.

## Pass-Regel



## Block-Regel



«Source» -> [Interface Name] Net.

«Destination» → [Any]

«Direction» → [out]

Nach dieser Konfiguration hat man Zugriff auf das WAN Interface und kann raus ins Internet.

«Action» → [Block]

«Source» → [Interface Name] Net.

«Destination» → [Name des spezifische Interface]

«Direction» → [in]

Mit dieser Firewall-Konfiguration blockiert man in diesem Interface den Zugriff auf ein anderes Subnetz (Deshalb mehrere Regeln, um alle zu blockieren). Jedoch kann das andere Netzwerk vis-à- vis immer noch darauf zugreifen. Diese Regel muss man deshalb auch auf den Firewall-Regeln des anderen Netzwerkes machen, damit der Zugriff von beiden Seiten aus blockiert ist.

# Gantt-Diagramm: 2

Im Gantt-Diagramm ist zu sehen, wieviel Zeit ich für das ganze Projekt investiert habe. Im Grossen und Ganzen ist dies mehr oder weniger, wie ich es mir bei der Planung meines Projektes vorgestellt habe. Das Projekt verlief recht gut, jedoch gab es einige Stolpersteine, die mir eine Menge Zeit gekostet haben, wie zum Beispiel die Windows-Firewall als diese meinen Verbindungsaufbau beim Erstellen der Interfaces blockiert hat, oder eine falsche Konfiguration in der OpnSense-Firewall.

# Ist-Wert

Meine Arbeit hat/kann am Ende dieses Projektes:

* + Einen funktionierenden OpnSense-Router mit mehreren Interfaces, welche sich ohne eine VPN-Verbindung nicht gegenseitig anpingen können.
  + Einen VPN-Server für jedes Netzwerk, auf den man überall und wann man möchte zugreifen kann.
  + Durch VPN einen Zugriff auf ihre Netzwerke verschaffen für bestimmte Benutzer mit Zertifikat und Login-Informationen (Two-Factor Authentification).
  + VM-Server erreichen und mit einem VPN-Tunnel auf VMs zugreifen.

# Analyse

### Am Ende meines Projektes habe ich jedes Ziel, welches ich mir vorgenommen habe, erreicht. Ich habe sehr eigenständig gearbeitet und mit eigener Recherche meine Hürden überwunden. Über die Wochen habe ich mich mit dem Thema VPN und OpnSense sehr vertraut gemacht, was mein Knowhow weit voranbrachte. Jedoch blieb mir für meine optionale Arbeit keine Zeit, wegen den zeitkonsumierenden Problemen.