


Übungsprotokoll

SYTS – Systemtechnik Systemintegration und Infrastruktur

	Übungsdatum: KW 37/2022 – KW 42/2022	Klasse: 5AHIT	Name: Felix Schneider
	Abgabedatum: 17.10.2023	Gruppe: SYTS_2	Note:
Leitung: DI (FH) Alexander MESTL	Mitübende: Clemens Schlipfinger, Jakob Pusch, Yanik Latzka		
Übungsbezeichnung: Unternehmensnetzwerk mit DMZ			

Inhaltsverzeichnis:

1	Aufgabenstellung.....	3
2	Abstract (English).....	3
3	Theoretische Grundlagen	4
3.1	DMZ	4
3.2	Firewall	5
4	Übungsdurchführung	6
4.1	Windows Server aufsetzen.....	6
4.2	FreeBSD für Firewall aufsetzen	6
4.3	Windows Client aufsetzen.....	9
4.4	Apache Webserver aufsetzen.....	10
4.4.1	Podman Webserver mittels Container-Virtualisierung	10
4.4.2	Webserver local testen.....	11
4.5	Firewall konfigurieren	12
4.5.1	Interfaces konfigurieren	12
4.5.2	Port Forwarding mittels NAT konfigurieren	15
4.5.3	Private Network blocked	16
5	Ergebnisse.....	17
6	Kommentar.....	18

1 Aufgabenstellung

Bauen Sie ein virtuelles Unternehmensnetzwerk mit einer Demilitarisierten Zone auf! Verwenden Sie hierfür PfSense als Firewall und Apache als Webserver. Der Einfachheit halber müssen Sie nur eine Firewall aufsetzen. Schlussendlich sollten Sie vier lauffähige, fertig konfigurierte, virtuelle Maschinen haben:

- Einen Windows Server mit DHCP, DNS und AD
- Einen Windows Client in der Domain htl.com
- Einen Webserver auf Debian in der DMZ
- Eine Firewall zwischen WAN, LAN und DMZ

Das Augenmerk der Übung liegt bei dem Zugriff auf den Webserver vom WAN.

2 Abstract (English)

Build a virtual corporate network with a Demilitarized Zone! For this, use PfSense as firewall and Apache as web server. For simplicity, you only need to set up one firewall. Finally, you should have four running, fully configured, virtual machines:

- A Windows server with DHCP, DNS and AD.
- A Windows client in the domain htl.com
- A web server on Debian in the DMZ
- A firewall between WAN, LAN and DMZ

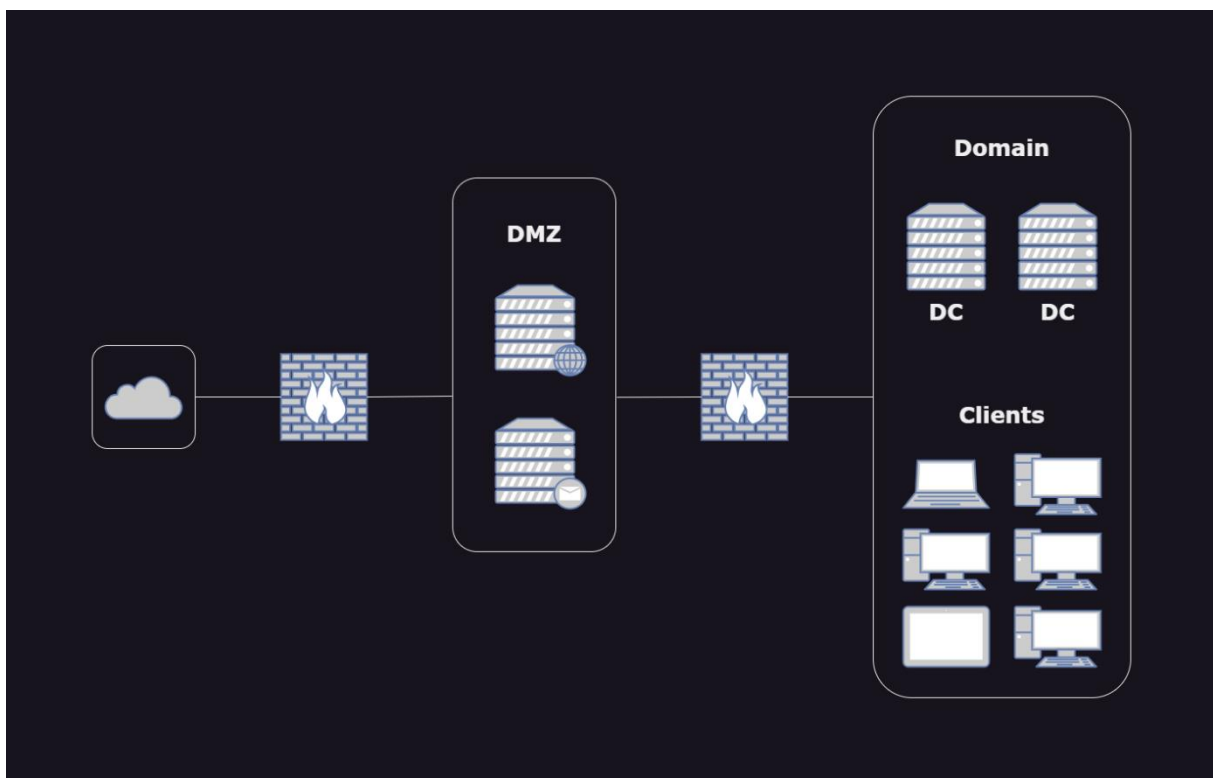
The focus of the exercise is on accessing the web server from the WAN.

3 Theoretische Grundlagen

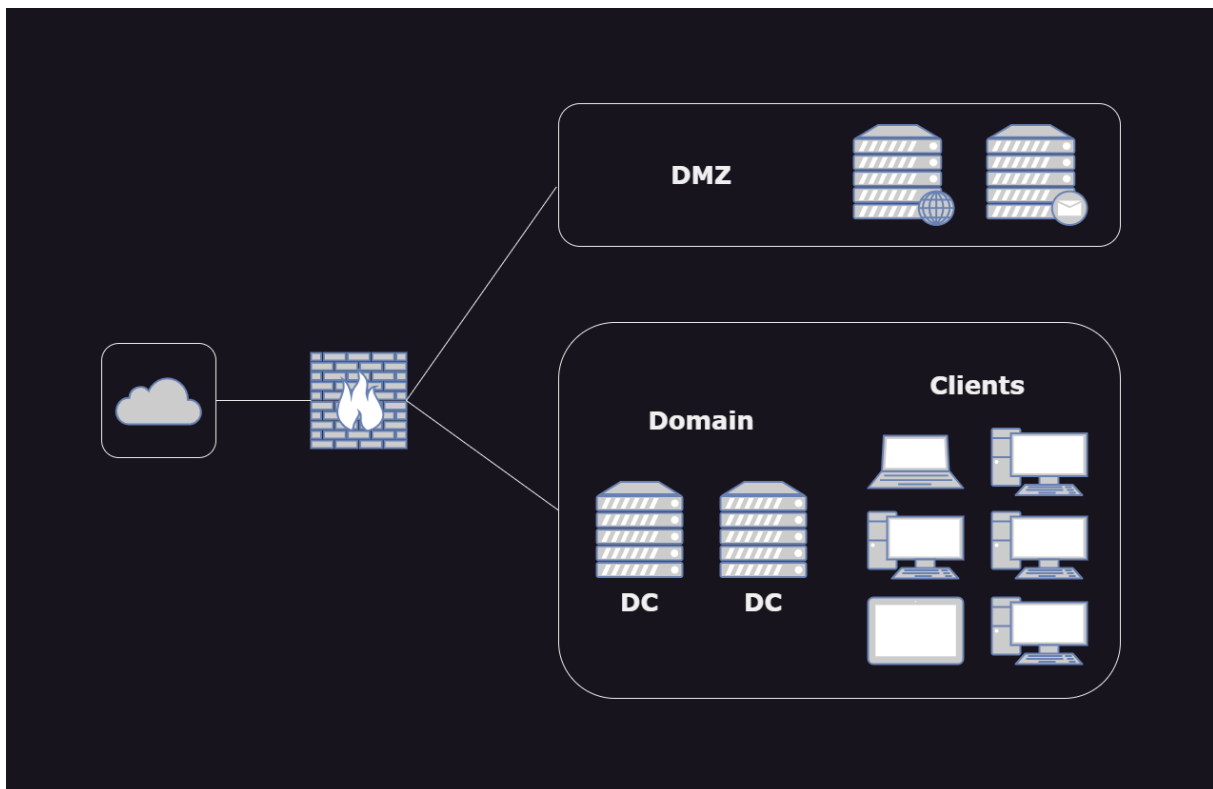
3.1 DMZ

Eine Demilitarisierte Zone ist ein Bereich in einem Computernetzwerk, der zwischen dem internen Netzwerk (LAN) und dem externen Netzwerk (normalerweise dem Internet) liegt. Die DMZ dient dazu, bestimmte Server oder Dienste zu isolieren, die für die öffentliche Erreichbarkeit bestimmt sind, ohne dabei die Sicherheit des internen Netzwerks zu gefährden. In der DMZ können beispielsweise Webserver, E-Mail-Server oder öffentliche Anwendungen platziert werden. Der Zweck besteht darin, potenziell gefährlichen Netzwerkverkehr von außen zu kontrollieren und zu überwachen, um das interne Netzwerk vor Bedrohungen zu schützen. Die DMZ agiert als Pufferzone, die es ermöglicht, öffentliche Dienste bereitzustellen, ohne direkten Zugriff auf das interne Netzwerk zu gewähren.

Eine reale DMZ hat diese Struktur:







Unser DMZ hat jedoch der Einfachheit halber nur eine Firewall. Eigentlich haben wir dann gar keine demilitarisierte Zone, weil keine Zone zwischen den Firewalls existiert, aber es ist einfacher nur eine Firewall aufzusetzen und vier VMs gleichzeitig laufen zu lassen als fünf...



3.2 Firewall

Eine Firewall ist eine Sicherheitsvorrichtung, die den Datenverkehr zwischen Netzwerken kontrolliert. Sie erlaubt oder blockiert den Datenverkehr basierend auf vordefinierten Regeln, um das Netzwerk vor Bedrohungen wie Cyberangriffen und Malware zu schützen. Aus diesem Grund ist diese Firewall-Regel unter ITlern ein Witz, weil sie keinen einzigen Traffic blockiert und deswegen den Sinn der Firewall aufhebt:

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	*	*	*	*	*	none		   

Diese Regeln können via Web Applikation vielfältig konfiguriert werden. In diesem Protokoll werden wir nur die einfachsten Möglichkeiten einer Firewall nutzen, doch das Potential für Nutzungs- und Einstellungsmöglichkeiten ist quasi unendlich groß.

4 Übungsdurchführung

4.1 Windows Server aufsetzen

Setzen Sie eine Virtuelle Maschine mithilfe von VMware / VirtualBox (Typ 2 Virtualisierung) auf und verwenden Sie die Windows Server 2022 ISO. Installieren Sie dann wieder die Standardfeatures: DNS, AD, DHCP...

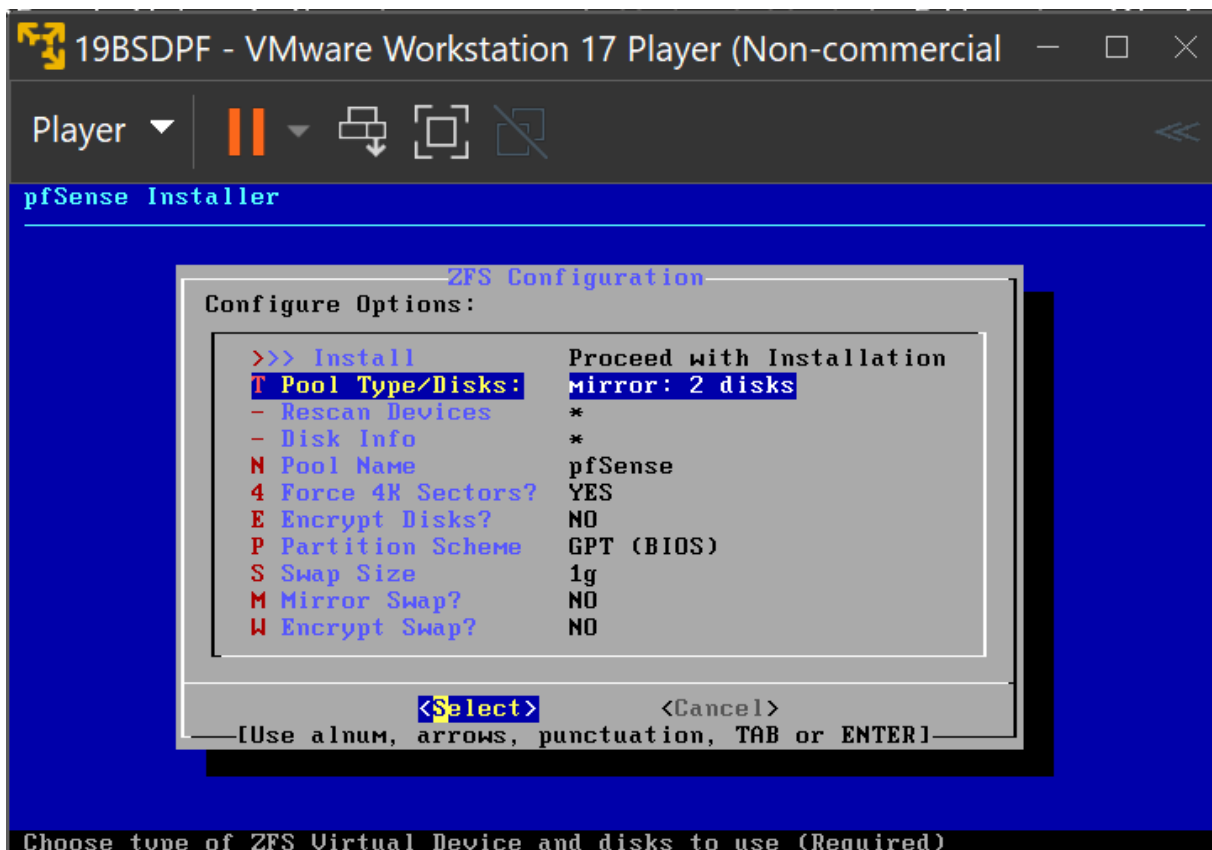
Falls Sie Schwierigkeiten mit der Firewall haben, probieren Sie temporär vielleicht auch die Windows Firewall zu deaktivieren.

Konfigurationen:

- Name: dc-master
- IP-Address: 192.168.19.2
- Gateway: 192.168.19.1 (Firewall)

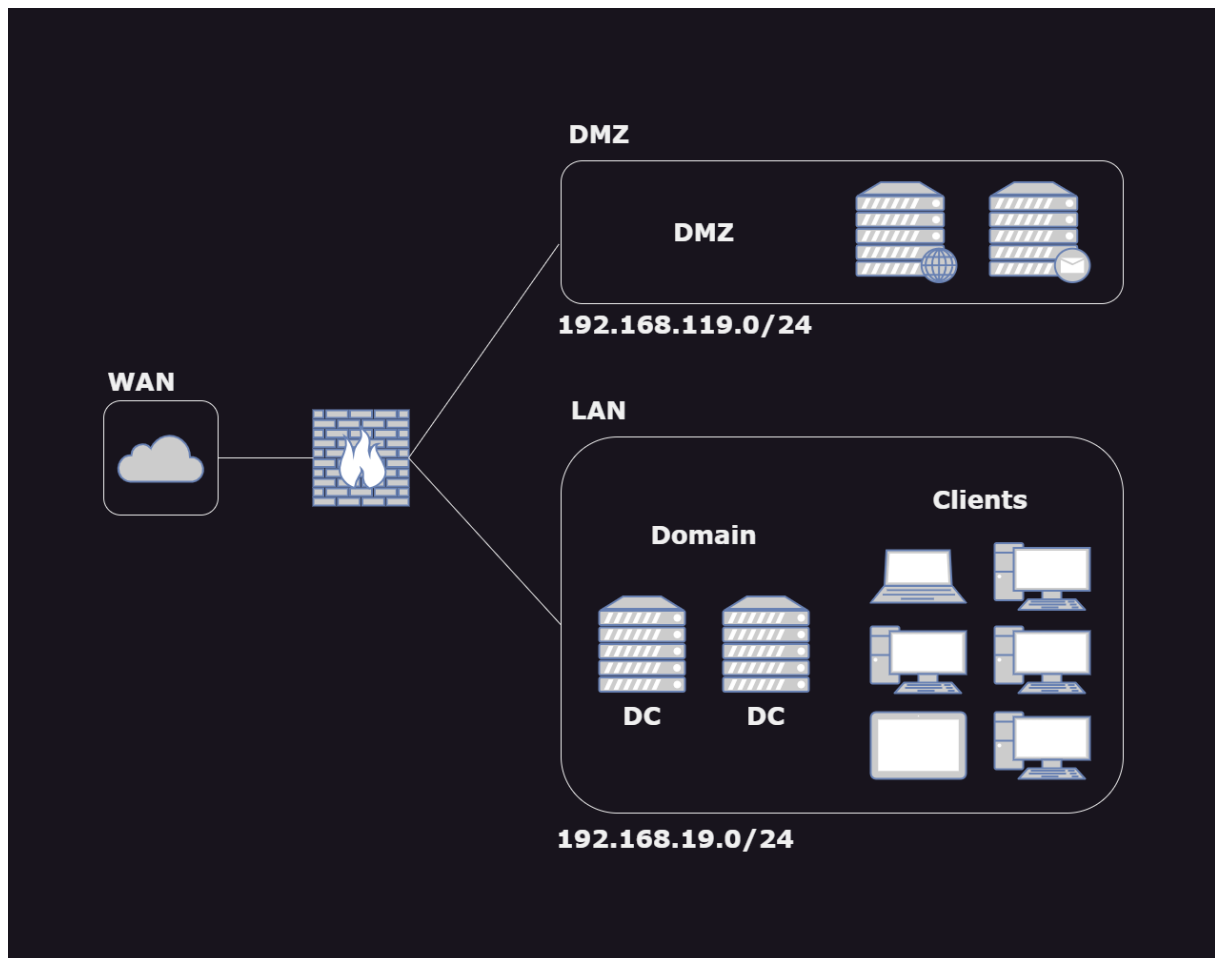
4.2 FreeBSD für Firewall aufsetzen

Verwenden Sie eine pfSense ISO, um eine VM mit FreeBSD aufzusetzen. Diese dient später als Firewall. Da die pfSense Installation auch RAID unterstützt, kann man gleich mehrere Disks erstellen und spiegeln:



Starten Sie die Maschine nach der Installation neu, fahren Sie sie herunter und werfen Sie das CD-Laufwerk mit der ISO Datei raus, damit beim Starten keine Installation mehr durchgeführt werden kann.

Außerdem müssen Sie nun insgesamt drei Netzwerkkarten konfigurieren, damit die Firewall (also unser FreeBSD Maschine) mit allen voneinander getrennten Netzwerken verbunden ist, wie hier im Screenshot gezeigt:



Das bedeutet, dass wir ein **NAT**, ein **LAN-Segment mit DMZ** und ein **LAN-Segment mit dem internen LAN** konfigurieren. Dabei befindet sich im internen LAN-Netzwerk der Domain Controller und im DMZ-Netzwerk ein Webserver, welcher zum Beispiel mit Apache2 realisiert ist.

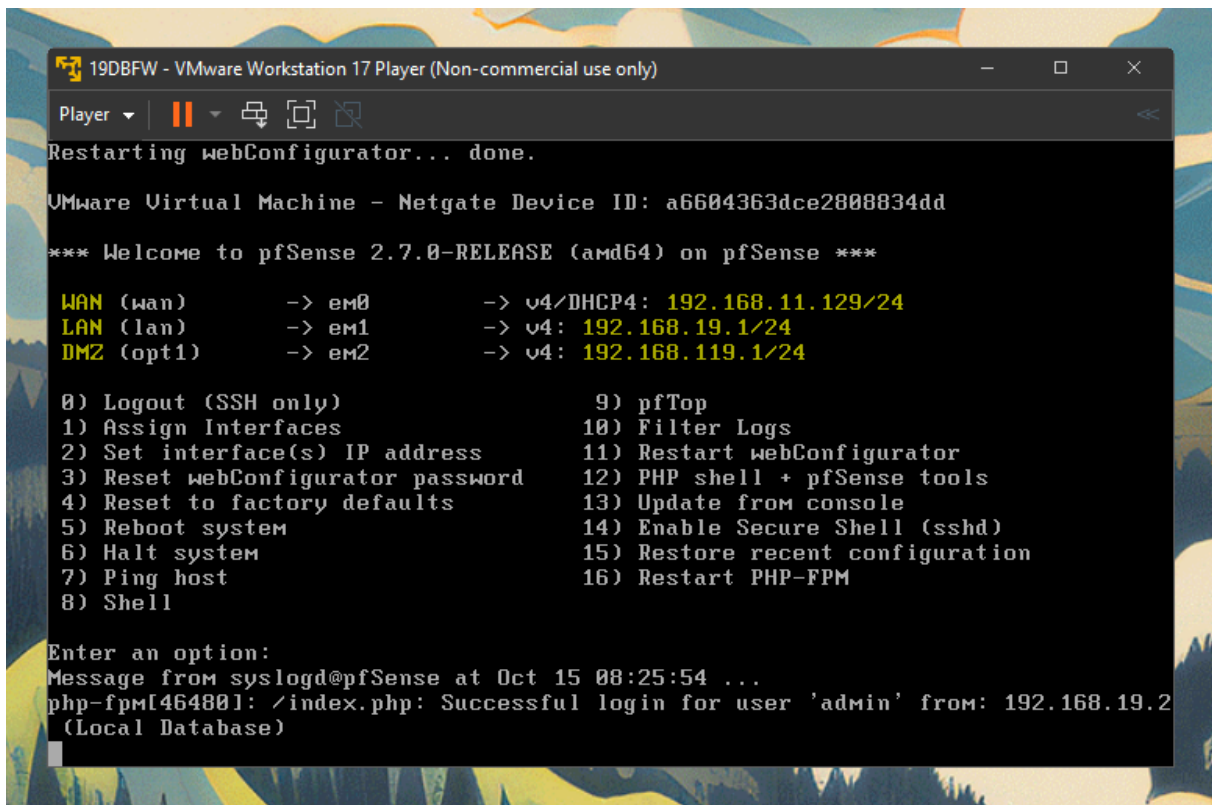
Nun starten Sie die Maschine wieder und konfigurieren die IPv4-Adresse für das LAN-Segment, welches im internen LAN hängt. Wählen Sie dazu die Option „Set interface IP address (2)“ aus:

```

19DBFW - VMware Workstation 17 Player (Non-commercial use only)
Player | [Icons]
Enter an option: 2
Available interfaces:
1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)
Enter the number of the interface you wish to configure: 2
Configure IPv4 address LAN interface via DHCP? (y/n) n
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.19.5
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0  = 16
     255.0.0.0    = 8
Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24
For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

```

Anschließend sehen Sie, dass das LAN nun im gleichen Subnetz wie der Windows Server ist:



```
19DBFW - VMware Workstation 17 Player (Non-commercial use only)
Player | [Icons]
Restarting webConfigurator... done.
VMware Virtual Machine - Netgate Device ID: a6604363dce2808834dd
*** Welcome to pfSense 2.7.0-RELEASE (amd64) on pfSense ***

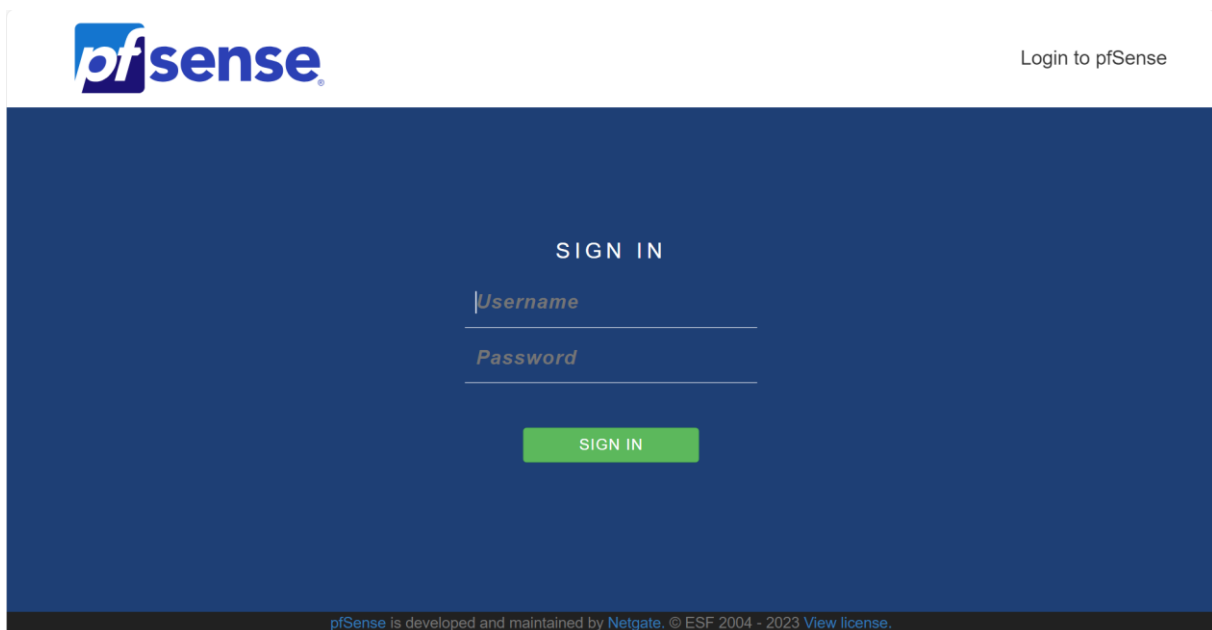
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.11.129/24
LAN (lan)      -> em1      -> v4: 192.168.19.1/24
DMZ (opt1)     -> em2      -> v4: 192.168.119.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults    13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option:
Message from syslogd@pfSense at Oct 15 08:25:54 ...
php-fpm[464801]: /index.php: Successful login for user 'admin' from: 192.168.19.2
(Local Database)
```

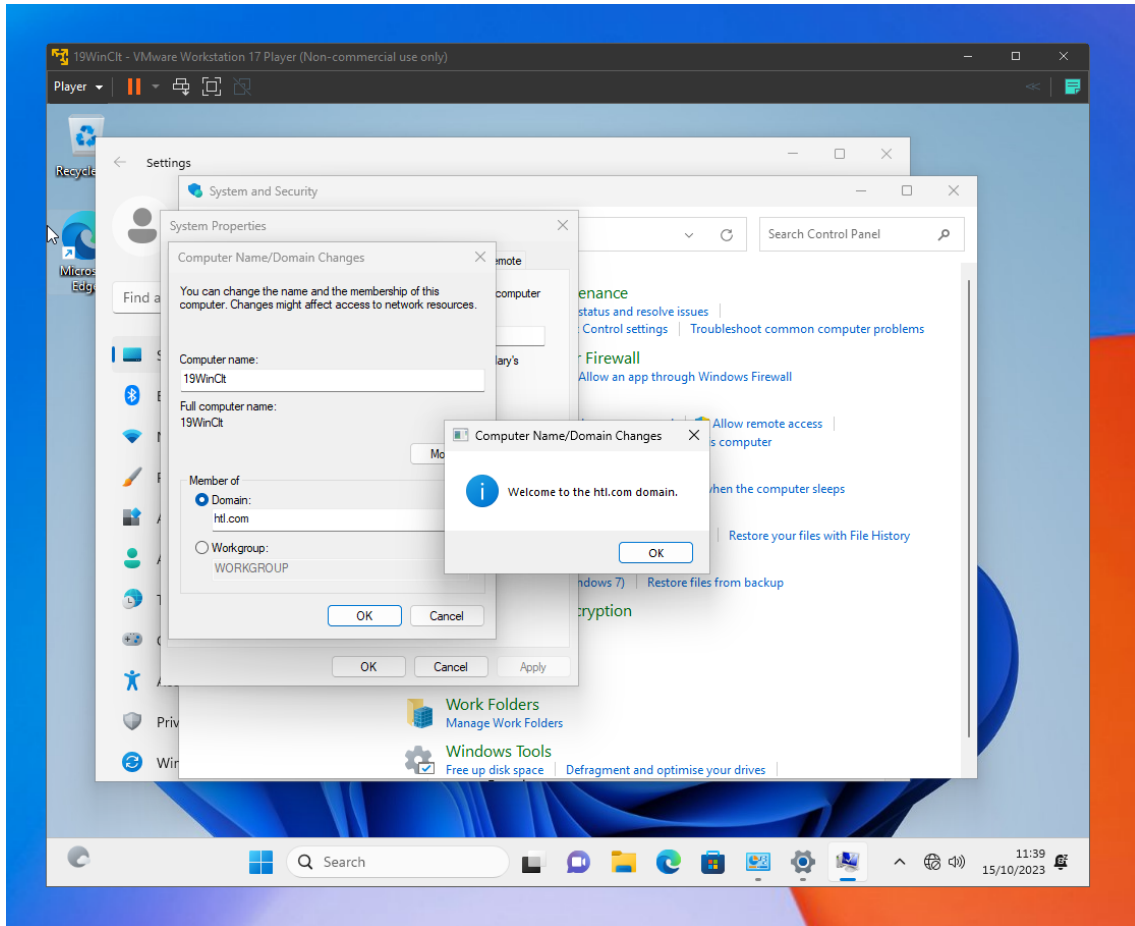
Keine Sorge, das DMZ Interface werden Sie später noch konfigurieren...

Nun können Sie am Windows Server über irgendeinen Browser die IPv4-Adresse der Firewall (192.168.19.1) aufrufen und können sich mit Username „**admin**“ und Passwort „**pfsense**“ anmelden, wie Sie es hier sehen können:

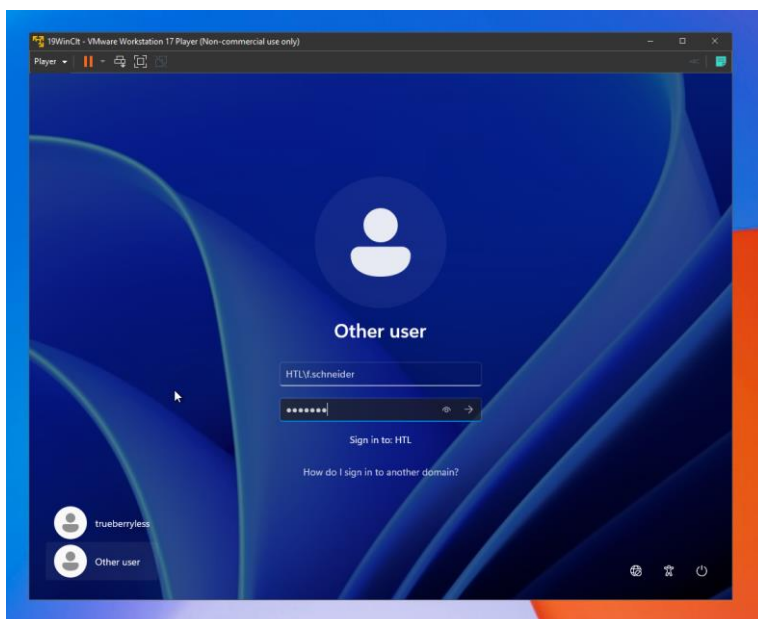


4.3 Windows Client aufsetzen

Setzen Sie einen Standard Windows Client mit Windows 11 auf. Falls die Windows 11 Installation Sie wegen einer Netzwerkverbindung nervt, öffnen Sie die Kommandozeile mittels FN + 10 und geben Sie den Befehl „OOBE\BYPASSNRO“ ein, damit Sie ohne Netzwerk fortfahren können.

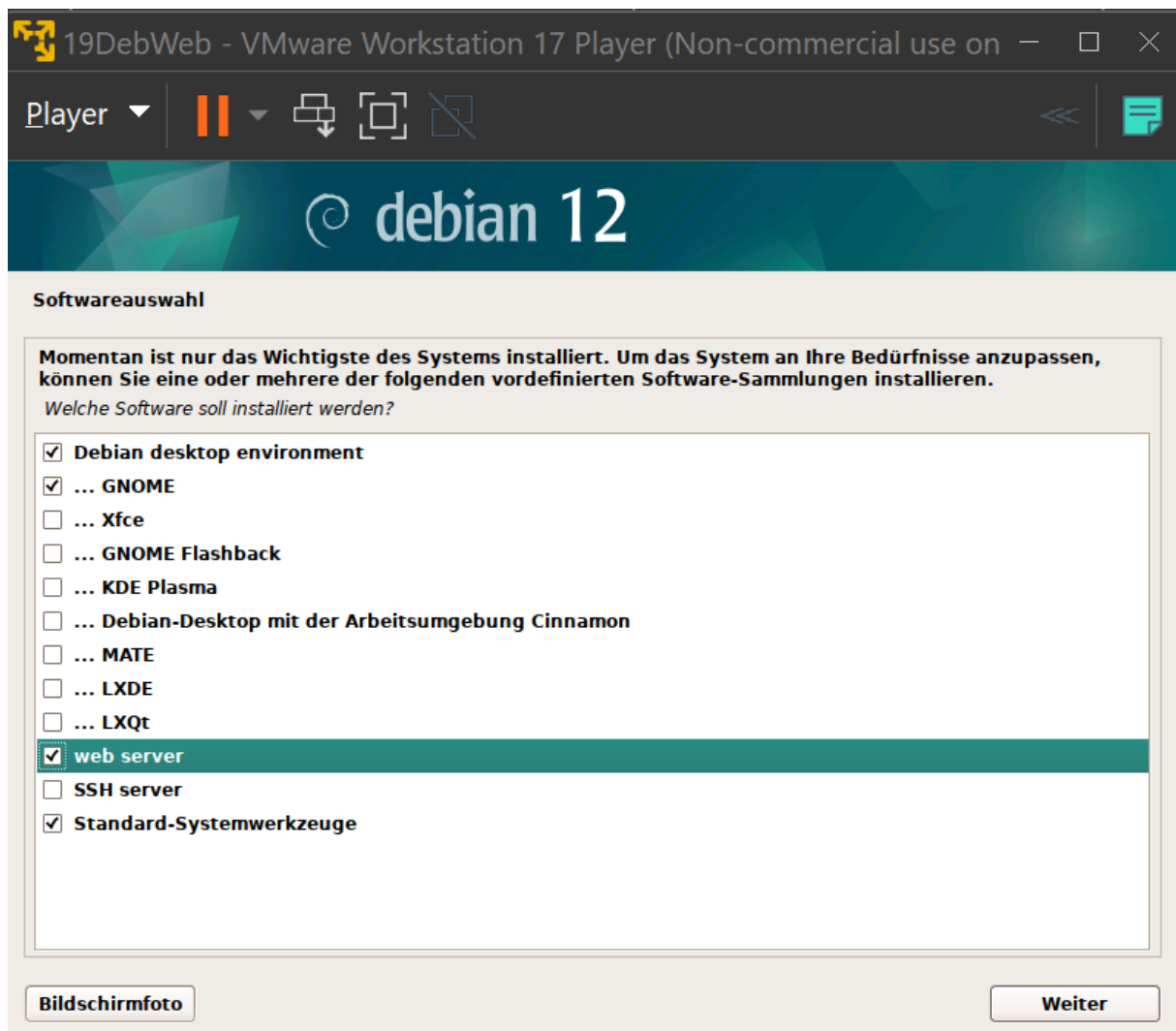


Sobald Sie der Domain beigetreten sind, können Sie sich mit einem Benutzer in der Domain anmelden:



4.4 Apache Webserver aufsetzen

Setzen Sie mithilfe einer Debian Amd64 ISO einen Apache Webserver auf. Dabei können Sie bereits bei der Installation der Software die Option „web server“ auswählen, wie man hier sieht:



4.4.1 Podman Webserver mittels Container-Virtualisierung

Es gäbe auch die coolere Möglichkeit einen Webserver über HTTPS zur Verfügung zu stellen. Dafür müssen Sie Podman oder Docker auf Debian installieren und anschließend diesen Command runnen:

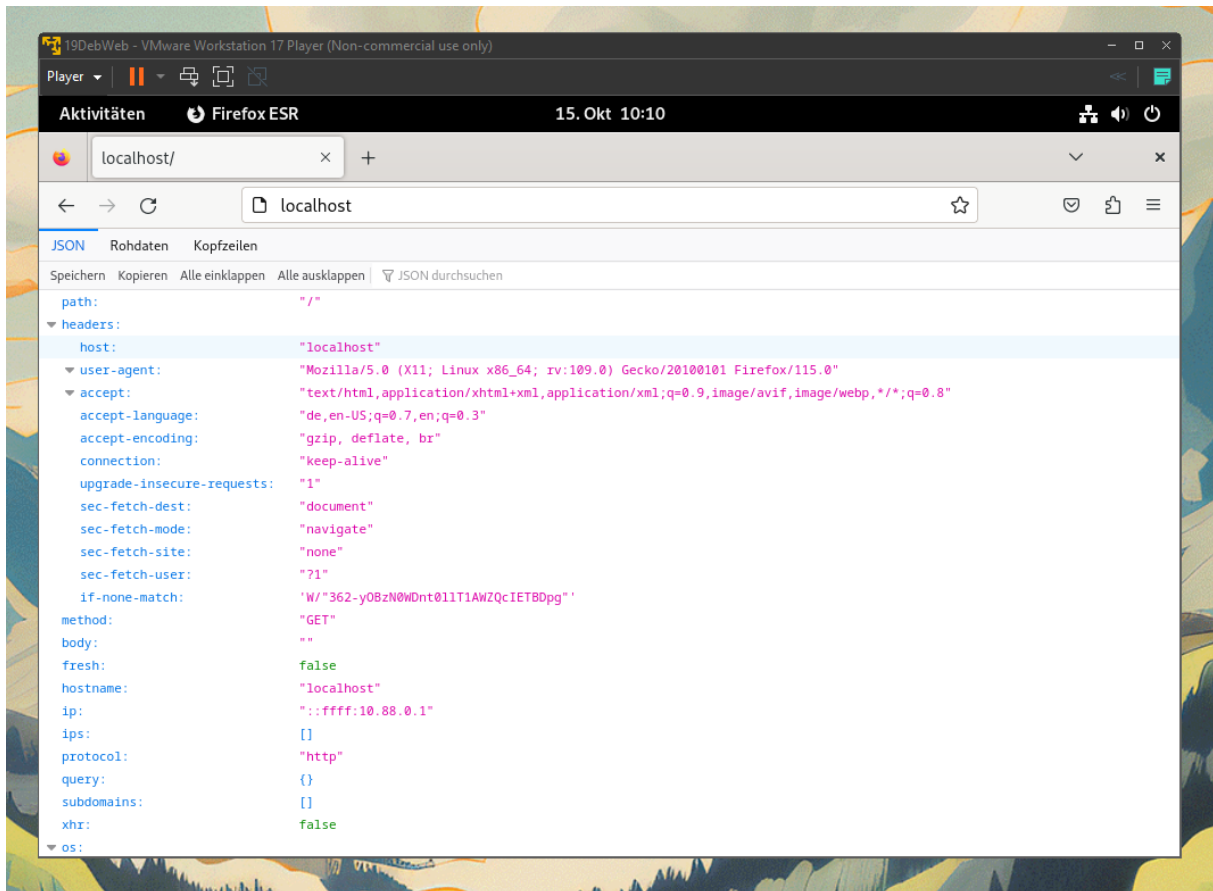
```
podman run -d -p 80:8080/tcp -p 443:8443 --name httpd
docker.io/mendhak/http-https-echo:30
```

Wenn Sie dann noch cooler sein wollen, konfigurieren Sie systemd, sodass der Container automatisch startet:

```
podman generate systemd httpd >
/etc/systemd/system/httpd.service
```

4.4.2 Webserver local testen

Öffnen Sie einen Browser und suchen Sie in der URL-Leiste nach „localhost“:



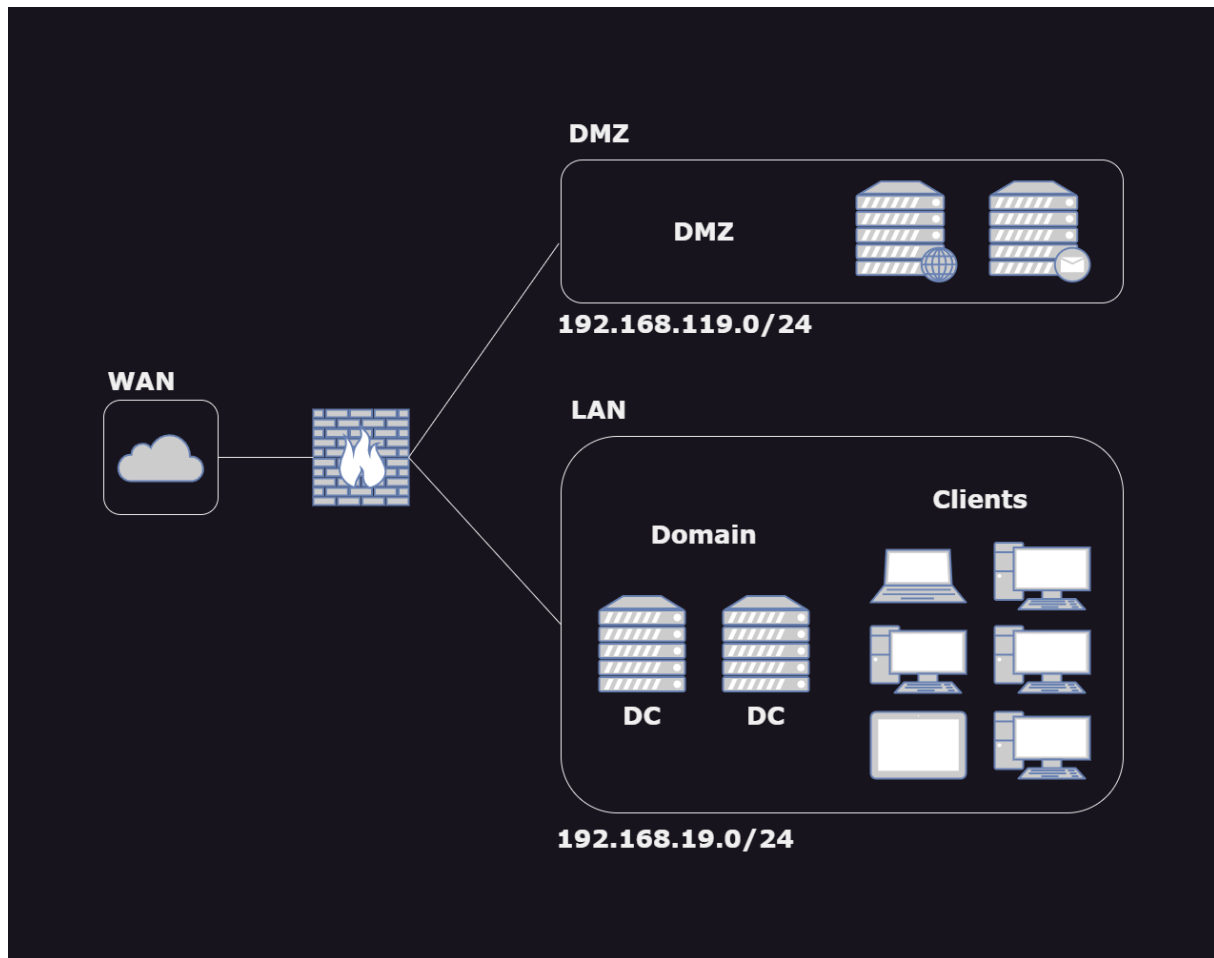
4.5 Firewall konfigurieren

4.5.1 Interfaces konfigurieren

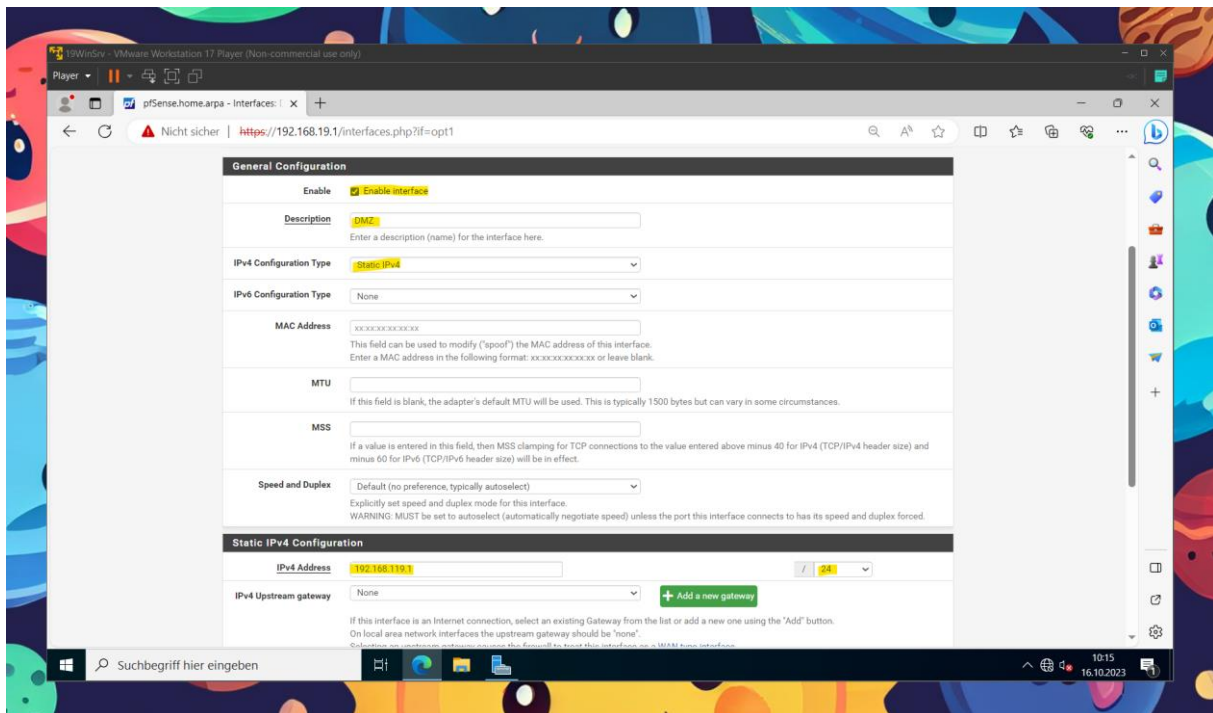
PfSense hat bereits drei Netzwerkkarten:

- WAN: geht ins Internet (NAT)
- LAN: geht zum DC und den Clients (192.168.19.0/24)
- DMZ: geht zum Apache Webserver (192.168.119.0/24)

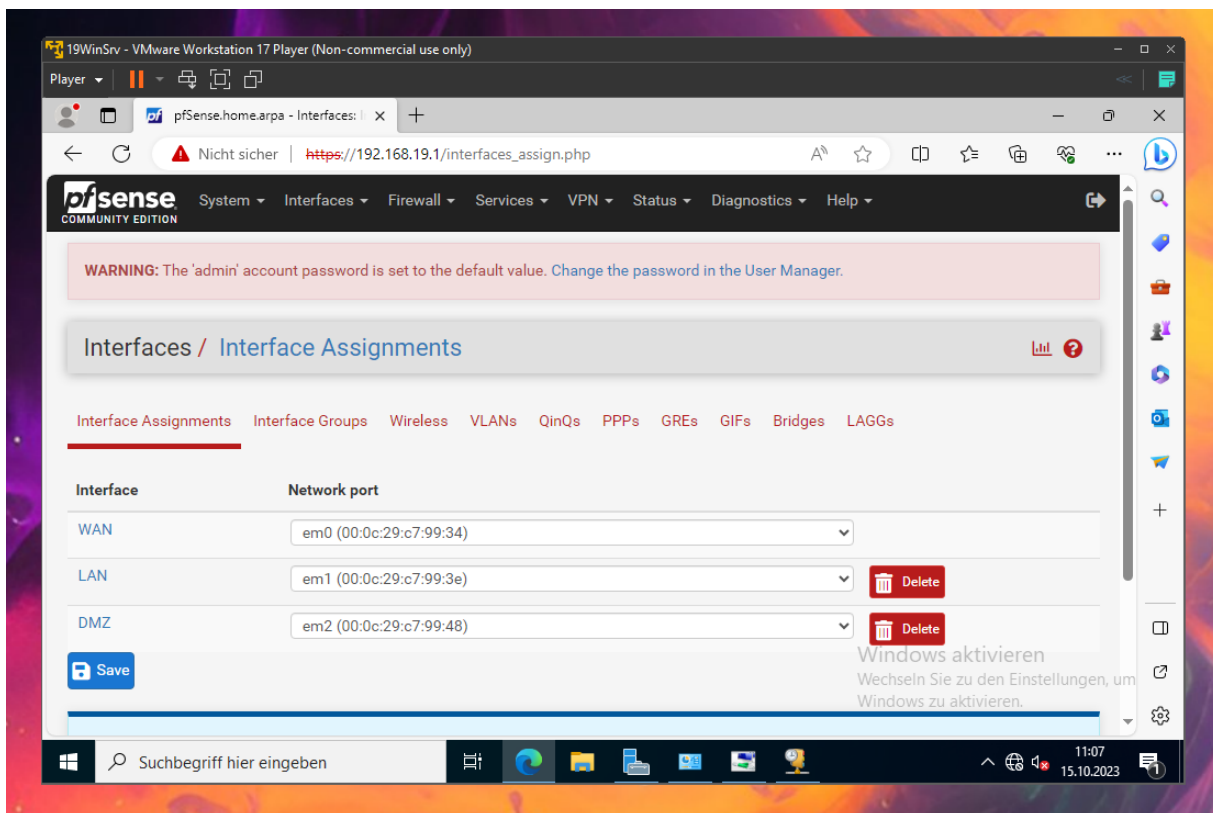
Folgende Zeichnung demonstriert diese Struktur:



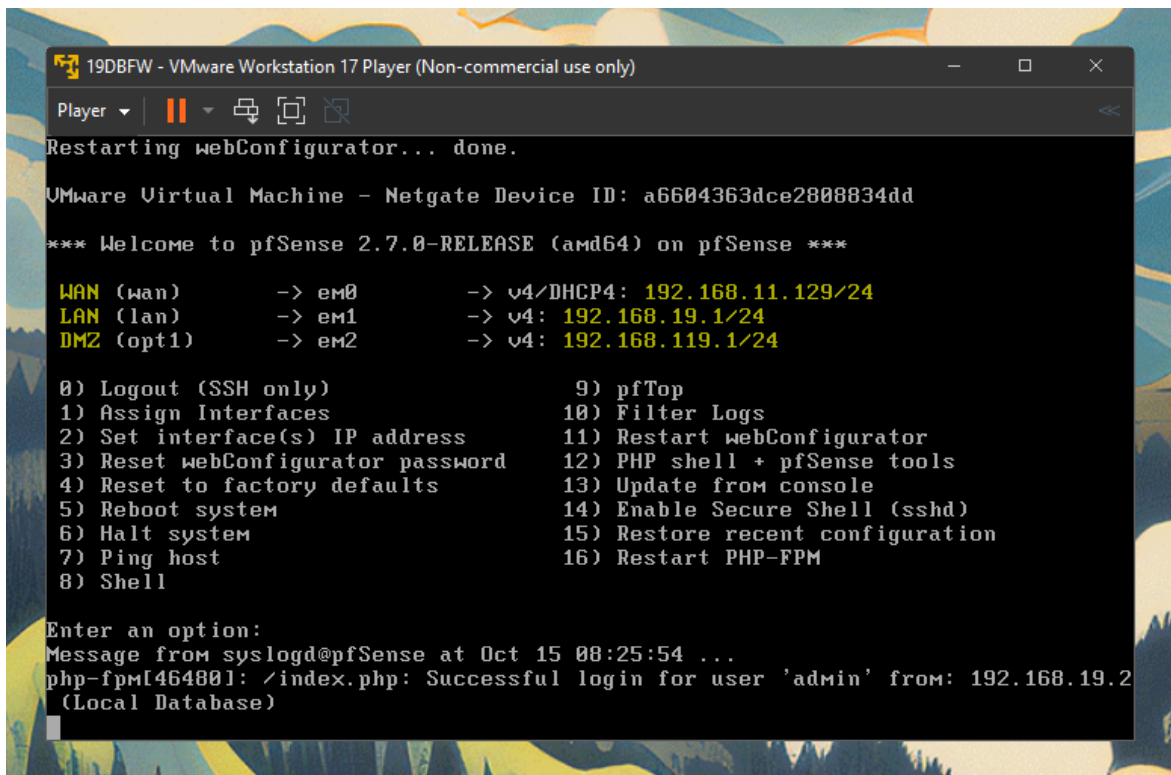
Damit wir diese Struktur aufbauen können, müssen Sie zuerst das dritte Interface (192.168.119.1) konfigurieren, damit dieses die richtige IP-Adresse bekommt.



Nach der Konfiguration, sollten alle Interfaces aktiviert sein und ca. so aussehen:



Nachdem Sie die Interfaces richtig in der UI konfiguriert haben, können Sie diese im Terminal der Firewall überprüfen. Wählen Sie einfach die Option: „Restart webConfigurator (11)“ aus, um die neuen Interfaces zu laden:



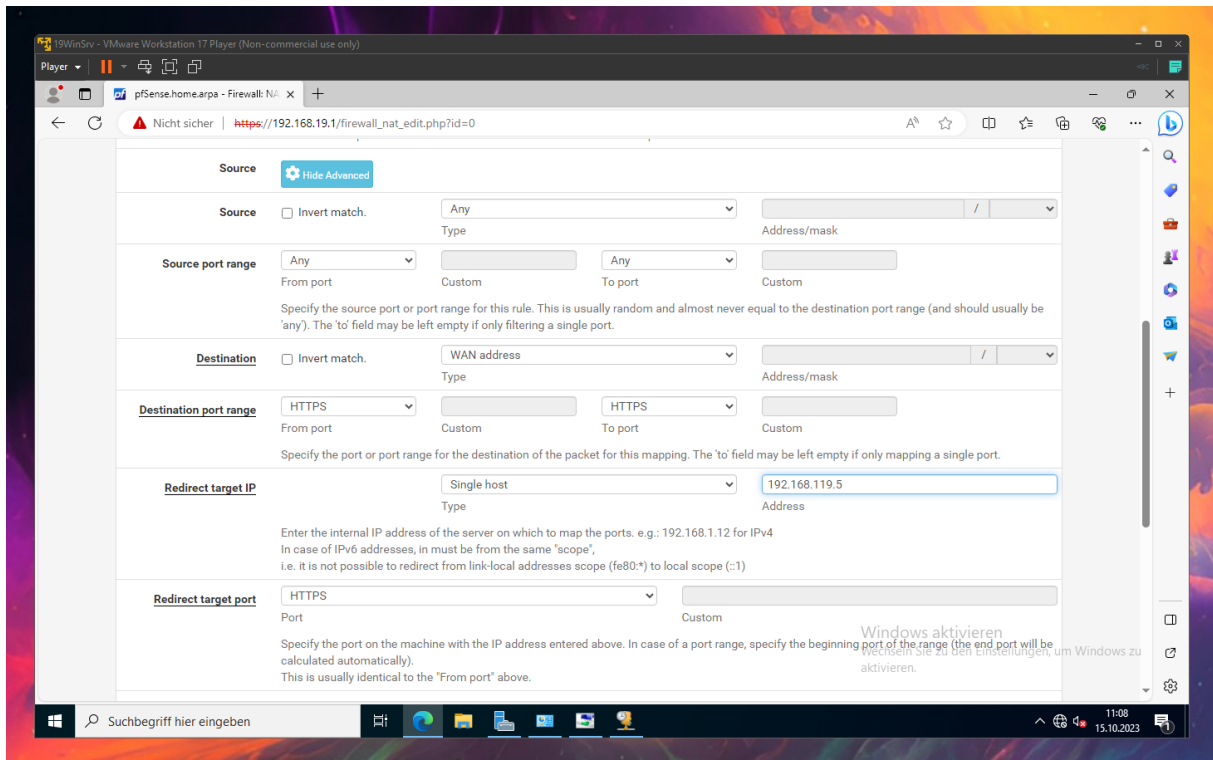
```
19DBFW - VMware Workstation 17 Player (Non-commercial use only)
Player
Restarting webConfigurator... done.
VMware Virtual Machine - Netgate Device ID: a6604363dce2808834dd
*** Welcome to pfSense 2.7.0-RELEASE (amd64) on pfSense ***
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.11.129/24
LAN (lan)      -> em1      -> v4: 192.168.19.1/24
DMZ (opt1)     -> em2      -> v4: 192.168.119.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

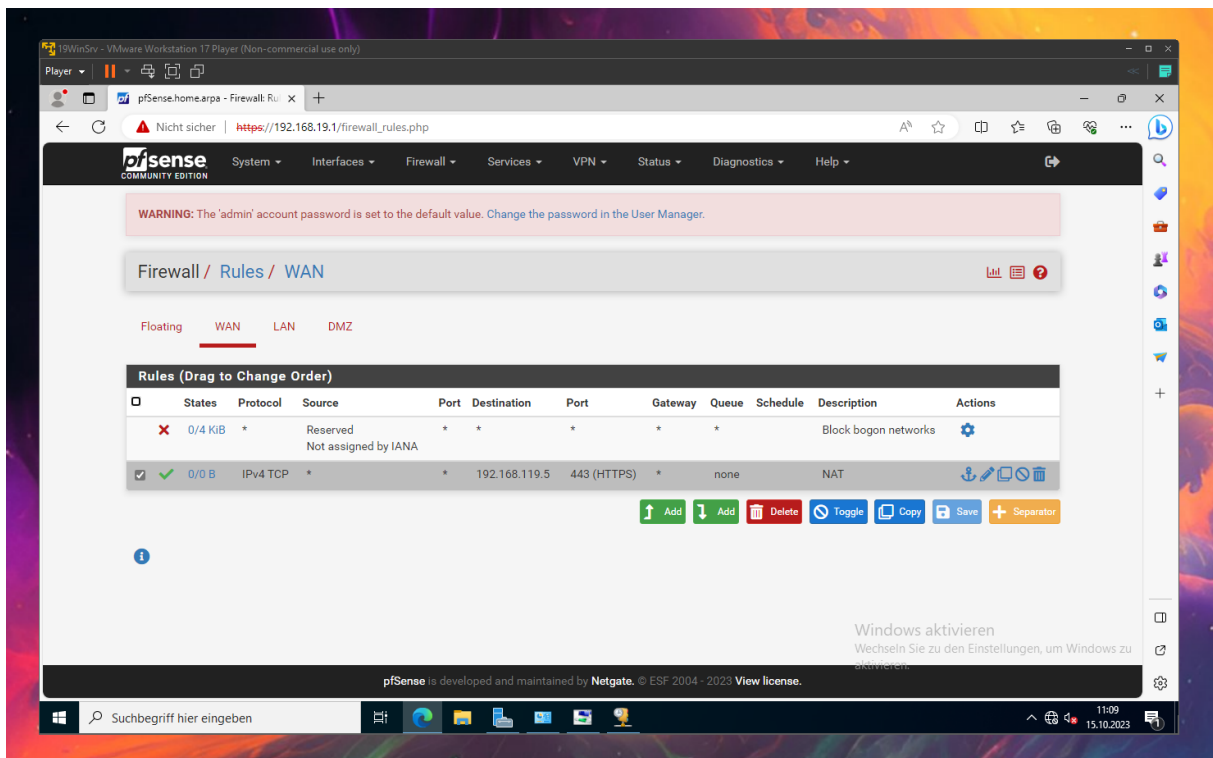
Enter an option:
Message from syslogd@pfSense at Oct 15 08:25:54 ...
php-fpm[464801]: /index.php: Successful login for user 'admin' from: 192.168.19.2
(Local Database)
```

4.5.2 Port Forwarding mittels NAT konfigurieren

Alle Anfragen auf die Firewall werden direkt auf den Webserver (192.168.119.5) weitergeleitet:

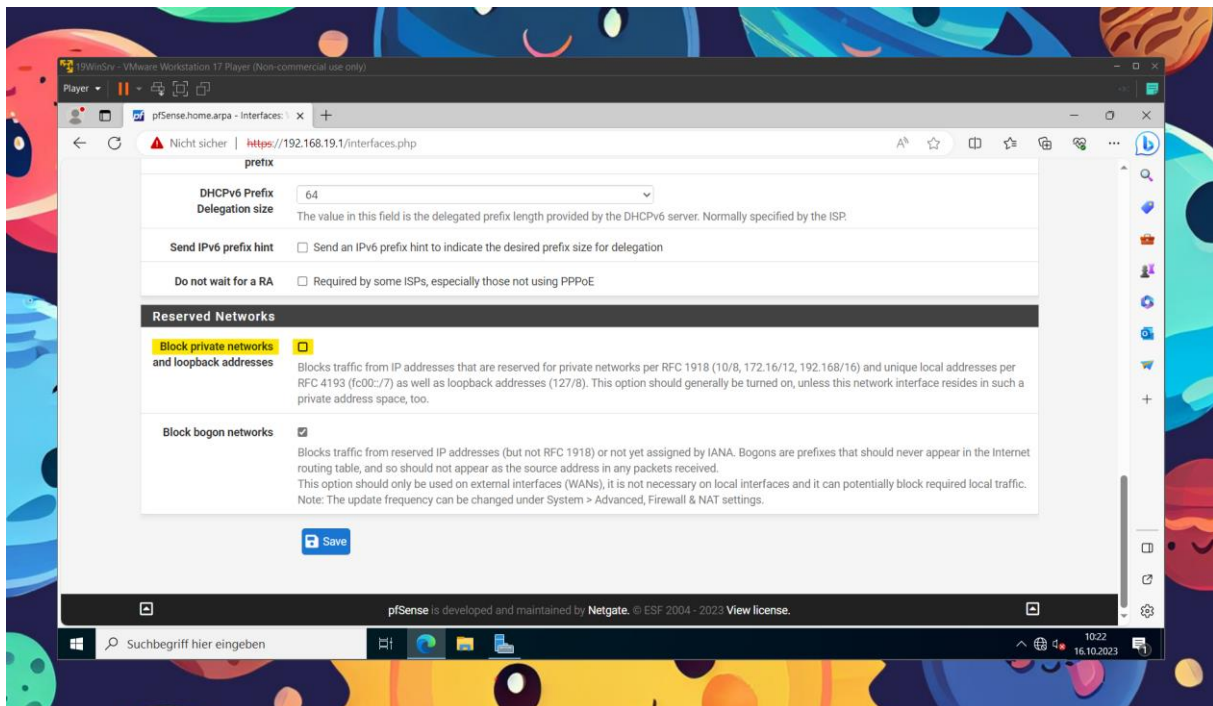
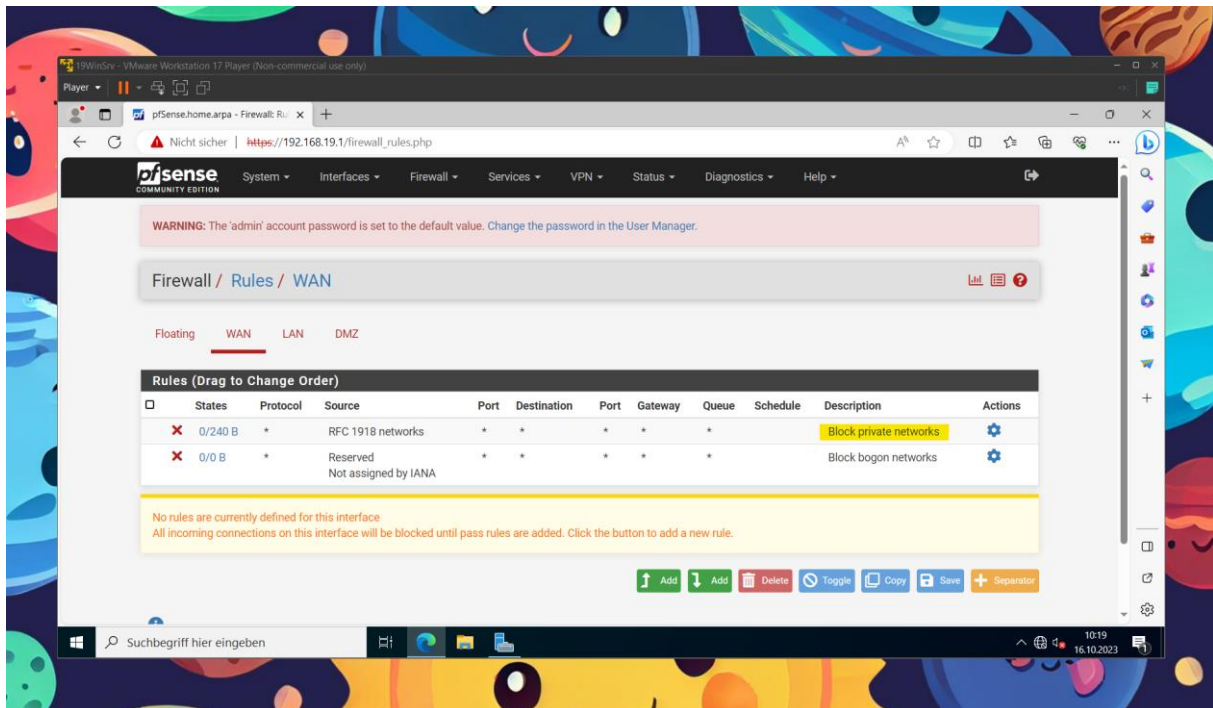


Sobald Sie NAT Port-Forwarding einrichten, wird automatisch eine Rule beim WAN definiert, damit die Anfragen aus dem Internet auch zum Webserver dürfen:



4.5.3 Private Network blocked

Außerdem müssen Sie aufpassen, dass Anfragen aus einem privaten Netzwerk nicht blockiert werden (da das Schulnetzwerk als privates Netzwerk zählt (ist ja genattet), ist dies besonders wichtig!):

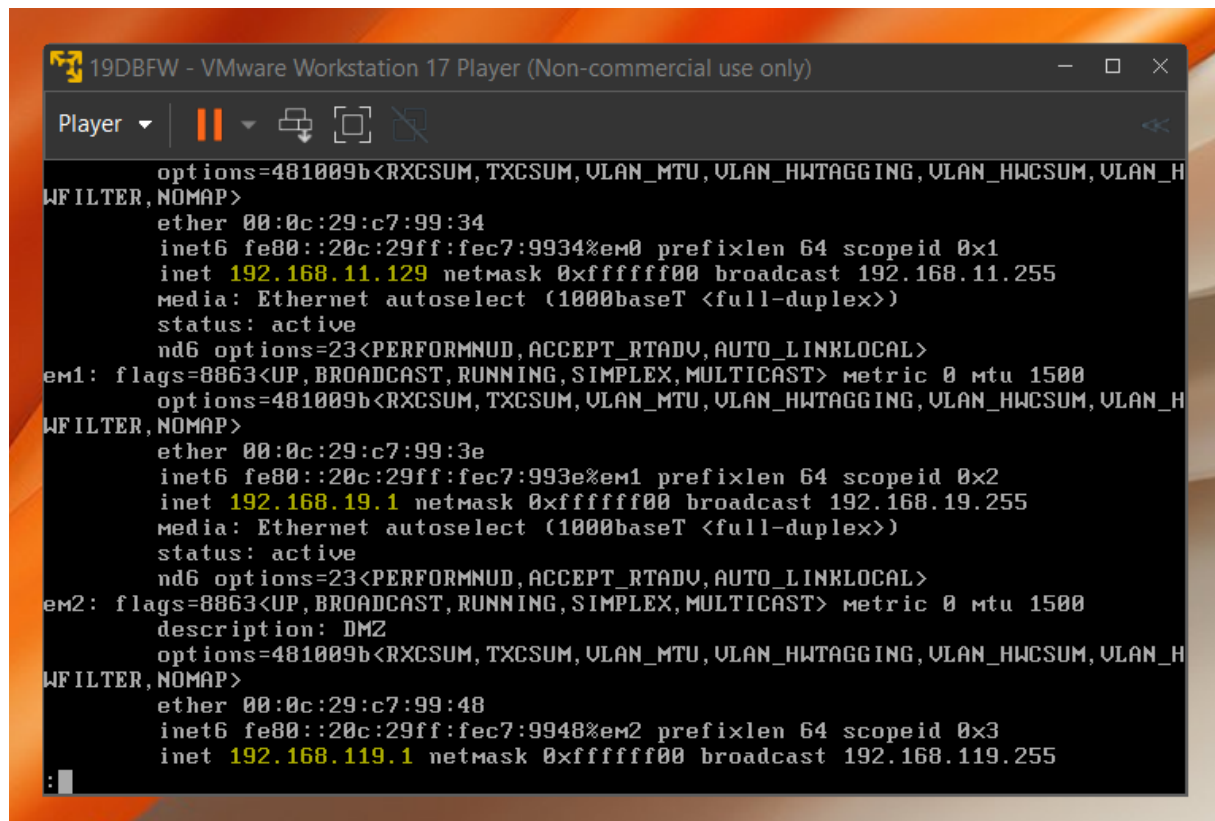


5 Ergebnisse

Fassen wir noch einmal zusammen, fass Sie nun eigentlich alles konfiguriert haben:

- Einen Windows Server, welcher die Features DHCP, DNS und Active Directory installiert hat
- PfSense, eine Firewall, welche Anfragen auf den Webserver von außen und innen zulässt
- Eine Linux VM, welche einen Webserver hostet
- Einen Windows Client, welcher in der htl.com Domain ist

Rein theoretisch müsste nun der Zugriff vom WAN Interface auf den Webserver mittels Firewall IP möglich sein. Bei mir geht's trotzdem nicht. Ich hab jetzt 3x die FW, 2x einen Windows Clt und jeweils 1x Webserver und Winserver aufgesetzt und mindestens 5x alle Einstellungen auf Korrektheit überprüft. Der Wille ist da.



```
19DBFW - VMware Workstation 17 Player (Non-commercial use only)
Player
options=481009b<RXCSUM, TXCSUM, VLAN_MTU, VLAN_HWTAGGING, VLAN_HWCSUM, VLAN_H
WFILTER, NOMAP>
ether 00:0c:29:c7:99:34
inet6 fe80::20c:29ff:fec7:9934%em0 prefixlen 64 scopeid 0x1
inet 192.168.11.129 netmask 0xffffffff00 broadcast 192.168.11.255
media: Ethernet autoselect (1000baseT <full-duplex>)
status: active
nd6 options=23<PERFORMNUD, ACCEPT_RTADV, AUTO_LINKLOCAL>
em1: flags=8863<UP, BROADCAST, RUNNING, SIMPLEX, MULTICAST> metric 0 mtu 1500
options=481009b<RXCSUM, TXCSUM, VLAN_MTU, VLAN_HWTAGGING, VLAN_HWCSUM, VLAN_H
WFILTER, NOMAP>
ether 00:0c:29:c7:99:3e
inet6 fe80::20c:29ff:fec7:993e%em1 prefixlen 64 scopeid 0x2
inet 192.168.19.1 netmask 0xffffffff00 broadcast 192.168.19.255
media: Ethernet autoselect (1000baseT <full-duplex>)
status: active
nd6 options=23<PERFORMNUD, ACCEPT_RTADV, AUTO_LINKLOCAL>
em2: flags=8863<UP, BROADCAST, RUNNING, SIMPLEX, MULTICAST> metric 0 mtu 1500
description: DMZ
options=481009b<RXCSUM, TXCSUM, VLAN_MTU, VLAN_HWTAGGING, VLAN_HWCSUM, VLAN_H
WFILTER, NOMAP>
ether 00:0c:29:c7:99:48
inet6 fe80::20c:29ff:fec7:9948%em2 prefixlen 64 scopeid 0x3
inet 192.168.119.1 netmask 0xffffffff00 broadcast 192.168.119.255
:
```

6 Kommentar

Ich habe insgesamt bereits mindestens drei Stunden in den PfSense Logs und Diagnostics verschiedenste Debugmöglichkeiten ausprobiert und bin schließlich daraufgekommen, dass ich von der Firewall (192.168.11.129) nicht auf den Host-Rechner (192.168.11.1) pingen kann. Dafür kann ich von allen Maschinen auf die Adresse 192.168.11.2 pingen, wobei ich nicht weiß, welche Maschine das sein soll. Der einzig andere Ort, wo ich die Adresse 192.168.11.2 gefunden haben, ist bei der PfSense GUI unter Status -> Dashboard unter DNS-Server nach 127.0.0.1 (localhost).

Schlussendlich habe ich deswegen von NAT auf Bridge (automated) umgestellt und nun stecke ich gerade bei dem nächsten Fehler: „ping: sendto: No route to host“, wenn ich versuche, die Adresse 192.168.150.1 oder 192.168.0.128 (mein Host) zu pingen. Ich glaube nämlich, dass bei NAT der Host die Adresse 192.168.11.1 und bei Bridge die Adresse 192.168.150.1 bekommt. Also es ändert sich logischerweise das Subnetz.