Ük 184

1. Repetition Netzwerk Grundlagen:

1. **Was macht ein Router?**
   Ein **Router** ist ein Netzwerkgerät, das Datenpakete zwischen Computernetzwerken **weitergeleitet.**

2. **Was macht eine Bridge?**
   Eine Bridge ist ein Netzwerkgerät, das zwei oder mehr Netzwerke miteinander **verbindet**.

3. **Was macht eine Firewall?**
   Eine Firewall ist ein Netzwerkgerät, das den Datenverkehr zwischen Computernetzwerken überwacht und reguliert. Eine Firewall kann den Datenverkehr basierend auf verschiedenen Kriterien wie IP-Adresse, Portnummer und Protokolltyp blockieren oder zulassen.

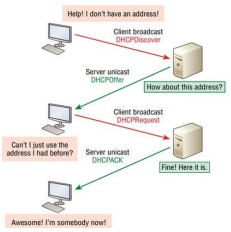
4. **Was versteht man unter dem Begriff Broadcast Domain?**
   Eine Broadcast Domain ist eine Gruppe von Geräten in einem Computernetzwerk, die alle Broadcast-Nachrichten empfangen, die von einem Gerät in der Gruppe gesendet werden. Ein Broadcast ist eine Nachricht, die an alle Geräte in einem Netzwerk gesendet wird.

5. **Wozu verwendet man VLANs?**
   VLANs (Virtual Local Area Networks) sind logische Gruppen von Geräten in einem Computernetzwerk, die unabhängig von ihrer physischen Position in verschiedenen Netzwerksegmenten organisiert werden können. VLANs ermöglichen es, den Datenverkehr in einem Netzwerk zu **segmentieren** und zu

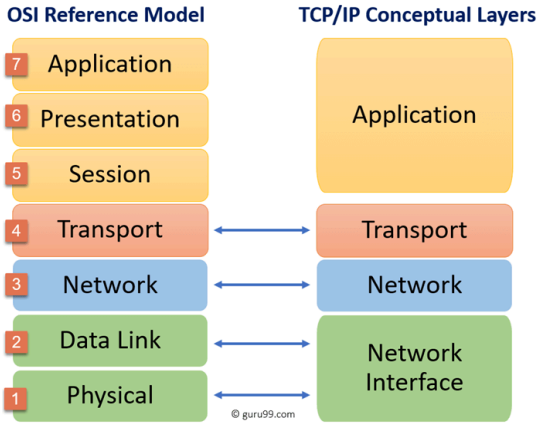
isolieren.

6. **Was ist ein ARP Broadcast?**
   Ein ARP Broadcast ist eine Art von Broadcast-Nachricht, die von einem Gerät in einem Netzwerk gesendet wird, um die MAC-Adresse eines anderen Geräts im Netzwerk zu ermitteln.

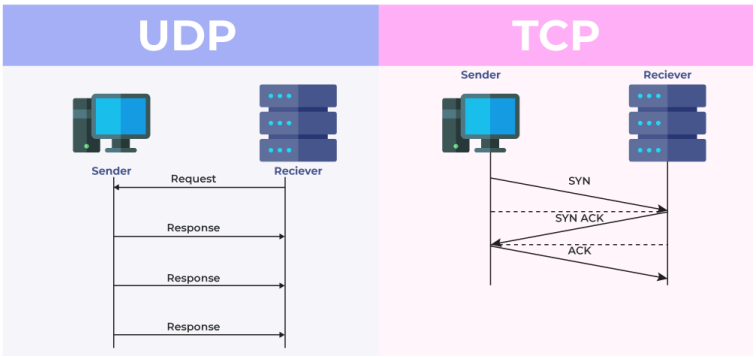
7. **Wie funktioniert der DHCP Discovery?**
   Der DHCP Discovery ist ein Prozess, bei dem ein Gerät in einem Netzwerk einen DHCP-Server sucht, um eine IP-Adresse und andere Netzwerkkonfigurationsinformationen zu erhalten.



8. **Was versteht man unter TCP/IP Stack?**
   Der TCP/IP-Stack ist eine Sammlung von Protokollen, die zur Übertragung von Daten über Computernetzwerke verwendet werden. Der TCP/IP-Stack besteht aus vier Schichten: **Anwendungsschicht**, **Transportschicht**, **Internetschicht** und **Netzwerkschnittstellenschicht**.



9. **Wie unterscheiden sich TCP und UDP?**
   TCP (Transmission Control Protocol) und UDP (User Datagram Protocol) sind zwei verschiedene Protokolle, die zur Übertragung von Daten über Computernetzwerke verwendet werden. **TCP ist ein verbindungsorientiertes** Protokoll, während **UDP ein verbindungsloses** Protokoll ist.



10. **Wie funktioniert der TCP Verbindungsaufbau?**
    Der TCP-Verbindungsaufbau ist ein Prozess, bei dem ein Client und ein Server eine Verbindung über das TCP-Protokoll herstellen. Der TCP-Verbindungsaufbau besteht aus drei Schritten: **SYN**, **SYN-ACK** und **ACK**.

11. **Was versteht man unter Well-Known Port?**
    Ein Well-Known Port ist ein Port, der einem bestimmten Netzwerkprotokoll oder einer bestimmten Anwendung zugeordnet ist. Well-Known-Ports haben Portnummern im Bereich von **0 bis 1023**.

12. **Was ist ein Portscan?**
    Ein Portscan ist ein Prozess, bei dem ein Computer die Ports eines anderen Computers gescannt, um offene Ports zu finden. Ein Portscan kann verwendet werden, um Schwachstellen in der Netzwerksicherheit zu identifizieren.

13. **Wozu dient das Protokoll DNS?**
    Das DNS-Protokoll (Domain Name System) wird verwendet, um Domainnamen in IP-Adressen umzuwandeln. DNS ist ein wichtiger Bestandteil des Internets und ermöglicht es Benutzern, Websites und andere Netzwerkressourcen über ihren Domainnamen zu finden.

14. **Wofür verwendet man NAT und Masquerading?**
    NAT (Network Address Translation) und Masquerading sind Technologien, die verwendet werden, um **private IP-Adressen in öffentliche IP-Adressen** umzuwandeln. NAT und Masquerading werden häufig verwendet, um mehrere Geräte in einem privaten Netzwerk mit dem Internet zu verbinden.

15. **Wie unterscheiden sich Source und Destination NAT?**
    Source NAT ändert die Quell-IP-Adresse, Destination NAT ändert die Ziel-IP-Adresse.

16. **Wann benötigt man Portforwarding?**
    Weiterleitung von Netzwerkverkehr von einem bestimmten Port auf einem Router

zu einem internen Gerät.Interner Webserver

17. **Wozu wird ICMP verwendet?**
    Ein Protokoll, das für Fehlerberichterstattung und Diagnose in IP-Netzwerken verwendet wird, z.B. Ping.

18. **Was ist der Unterschied zwischen HTTP und HTTPS?**
    HTTP überträgt Daten unverschlüsselt, während HTTPS eine verschlüsselte Verbindung verwendet, um Sicherheit zu gewährleisten.

19. **Wie unterscheiden sich Endpoint- und Perimeter-Security?**
    Endpoint-Security schützt individuelle Geräte, während Perimeter-Security das gesamte Netzwerk schützt, oft an den Netzwerkrändern.

2. Kontrollfragen:

1. **Wie unterscheidet sich ein Keylogger von einem Tool wie Hydra?**

   Ein Keylogger zeichnet Tastatureingaben auf, während Hydra ein Tool für Brute-Force-Angriffe ist, das darauf abzielt, Zugangsdaten zu knacken, indem es verschiedene Kombinationen von Benutzernamen und Passwörtern ausprobiert. In dem man das Opfer zuerst mit einem Keylogger ausspioniert und dann die Keylogger-Datei mit Hydra verbindet, kann man das Passwort vom Opfer knacken.

2. **Was ist eine Fragmentation Attack?**

   Eine Fragmentation Attack manipuliert die Art und Weise, wie Daten in kleine Teile aufgeteilt und wieder zusammengesetzt werden. Sie können genutzt werden, um Sicherheitslücken auszunutzen oder Systeme zu überlasten, indem sie die Fragmentierungsfunktionen von Netzwerken ausnutzen. Diese Angriffe können dazu führen, dass Systeme Daten fehlerhaft oder langsamer rekonstruieren, was

zu Schwachstellen oder Überlastungen führt.

3. **Wie unterscheidet sich eine SYN-Flood Attacke von einem DDoS Angriff?**

   Eine SYN-Flood Attacke ist eine spezifische Art von DoS-Angriff, der auf die Überlastung eines Zielsystems durch das Senden einer grossen Anzahl von SYN-Anfragen abzielt, während ein DDoS-Angriff ein breiterer Angriff ist, der von vielen verschiedenen Quellen gleichzeitig ausgeführt wird, um ein System oder Netzwerk zu überlasten oder zu stören. Artikel wie man SYN Flood atack macht.

4. **Nennen Sie DDoS Angriffsformen?**

   Syn Flood, UDP Flood, HTTP Flood, ICMP Flood etc. und Protokoll basiert Anwendung basiert.

5. **Wie schützen Sie ihr Unternehmen vor Angriffen auf den TCP/IP Stack des Betriebssystems?**

   Firewalls, regelmässige Updates, Sicherheitsrichtlinien

6. **Welche Voraussetzung benötigt ein Angreifer, um sich per ARP Poisioning in eine MITM Position zu bringen?**

   Er muss im Netzwerk sein, die IP- und Mac Adresse seines Opfers kennen und die nötigen Tools haben.

7. **Aus welchem Grund macht ein Angreifer zuerst ARP Poisioning, um anschliessend DNS Spoofing zu betreiben?**

   Durch die Kombination von ARP-Spoofing und DNS-Spoofing kann der Angreifer eine effektive Position als "Man-in-the-Middle" einnehmen, den Datenverkehr abfangen oder manipulieren und die Opfer dazu verleiten, auf gefälschte Seiten oder Server zuzugreifen, was erhebliche Sicherheitsrisiken birgt. Diese Techniken werden oft in Angriffen wie Phishing, Datendiebstahl oder der Verbreitung von Malware eingesetzt.

8. **Kennen Sie andere Möglichkeiten, um einem Client falsche DNS Antworten zuzuspielen?**

   DNS Cache Poisoning, Man-in-the-Browser-Angriffe (MITB), Router-Kompromittierung, BGP Hijacking

9. **Warum ist eine grosse Broadcast Domain unsicher?**

   Alle Geräte habe auf alle Netzwerkressourcen Zugriff, falls ein Client komprimiert wird, kann der Angreifer von dort aus auch auf Server zugreifen.

10. **Weshalb sollte man heute die Protokolle FTP und Telnet nicht mehr verwenden?**

    Weil diese alten Protokolle unverschlüsselt sind, sollte man lieber SFTP oder SSH verwenden.

11. Wozu dient der SSH Hostkey?

Der SSH-Hostkey trägt dazu bei, sicherzustellen, dass die Verbindung zwischen dem Client und dem Server vertrauenswürdig und nicht von einem Angreifer manipuliert wurde.

12. Wie führen Sie eine Host Discovery mit arp-scan und mit nmap durch?

1. sudo arp-scan --interface=**eth0 192.168.1.0/24** .Subnetz und Schnittstelle definieren
2. sudo nmap -sn 192.168.1.0/24 . -sn ist für ping scan

Kali Aufgabe 1:

1. **Klären Sie, mit welchem Befehl Sie in Kali mit einem ARP Scan aktive Hosts entdecken können**
   sudo arp-scan <net ip>/<CIDR>

2. **Klären Sie, mit welchem Befehl Sie in Kali mit nmap einen DHCP Discovery durchführen**
   sudo nmap -sn <net ip>/<CIDR>

3. **Klären Sie, mit welchem nmap Befehl Sie verfügbare Services von Hosts und das Hostbetriebssystem erfahren können**
   sudo nmap --script broadcast-dhcp-discovery

4. **Klären Sie, wie Sie mit Hydra, einer User Liste und einer Passwortliste Passwörter für Dienste hacken können**
   Auf der Kali VM, User ist kali
   Ins Verzeichnis UeK-184 wechseln (/home/kali/UeK-184)
   Dort finden sich zwei Files: m184_passwords.txt und m184_users.txt
   Mit diesen Files lassen sich die Credentials der beiden ssh Server hacken.

Praktischer Auftrag

1. Stellen Sie sicher, dass Sie in Ihrer Vmware Umgebung ein ein Host Only Netzwerk konfiguriert haben

2. Fügen Sie die Windows VM, Ubuntu VM und Kali VM

3. Sie arbeiten nun ausschliesslich auf der Kali VM (username: *kali*, pwd: *kali)*

4. Führen Sie einen ARP Scan aus

5. Welcher der Hosts ist der Netzwerk Gateway?
   192.168.174.1
6. Welcher der Hosts ist der DHCP Server
   192.168.174.254
7. Welcher der Hosts ist die Windows VM und welcher ist die Ubuntu VM
   Ubuntu: 192.168.174.129
   Windows: 192.170.104

8. Sie finden im Home Verzeichnis des Users Kali ein User und ein Passwort File

9. Knacken Sie Username und Passwort der offenen Dienste auf dem Ubuntu und dem Windows Host. Starten Sie mit dem Ubuntu Host

10. Prüfen Sie, ob Sie sich mit den gefunden Credentials auf den Hosts anmelden können
11. Was sind Ihre Sofortmassnahmen Empfehlungen um die Sicherheit der Hosts zu erhöhen?

sudo nmap --script=dhcp-discover 192.168.27.0/24

Wie funktioniert ARP Spoofing und welche Voraussetzungen benötigt ein Angreifer?

Funktionsweise: ARP Spoofing beinhaltet das Senden gefälschter ARP-Pakete an ein lokales Netzwerk, um die Zuordnung zwischen IP-Adressen und MAC-Adressen zu manipulieren. Der Angreifer täuscht andere Geräte im Netzwerk, indem er falsche ARP-Nachrichten sendet, die behaupten, dass die MAC-Adresse des Angreifers mit einer bestimmten IP-Adresse verbunden ist. Dadurch können Datenpakete an den Angreifer umgeleitet werden, als wäre er ein anderer vertrauenswürdiger Host im Netzwerk.

Wie funktioniert DNS Spoofing und welche Voraussetzungen benötigt ein Angreifer?

Voraussetzungen: Der Angreifer benötigt Zugriff auf dasselbe lokale Netzwerk wie das Opfer, um ARP Spoofing durchzuführen. Einige Tools wie arpspoof oder ettercap werden verwendet, um gefälschte ARP-Pakete zu senden.

```
sudo apt install telnetd -y
```

```
sudo systemctl status inetd
```

Block 2

How to install opnsense:

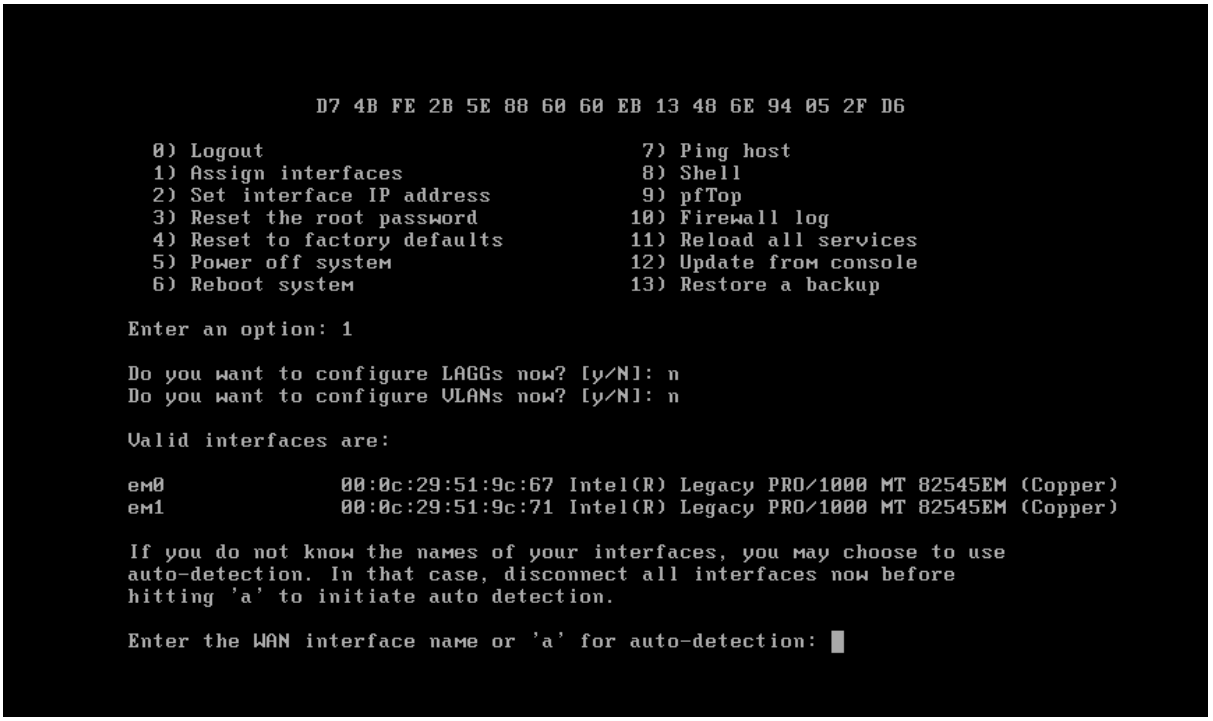
1.

installer →opnsense

Login → root PWD: opnsense

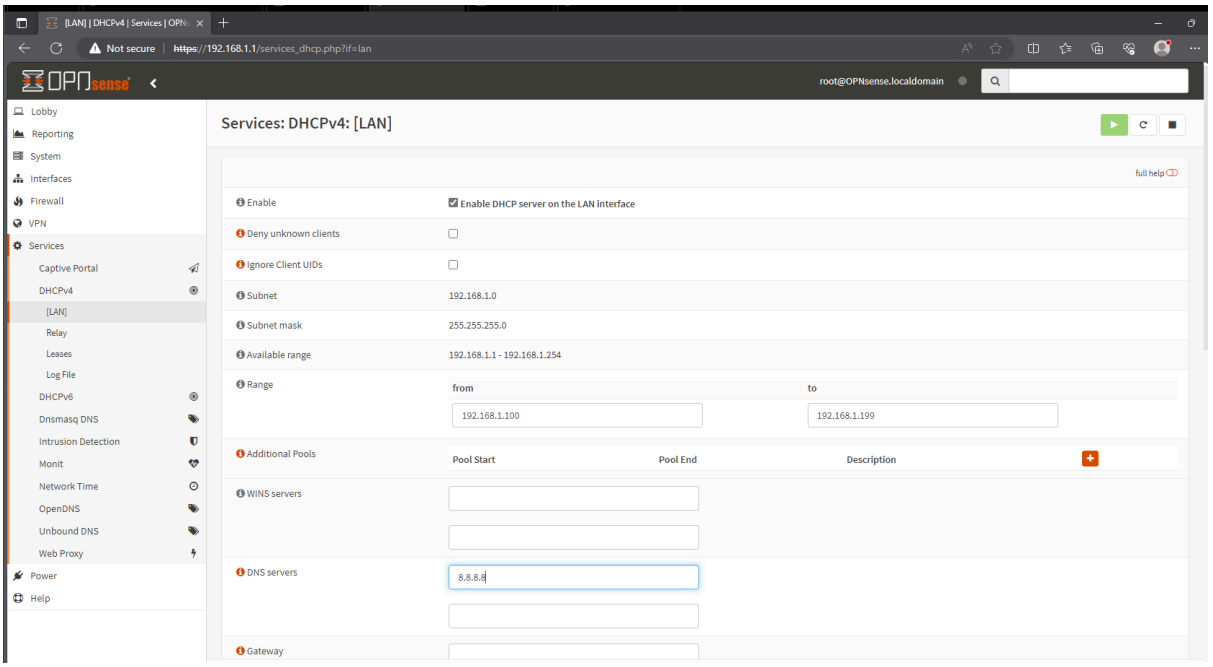

OPNsense Installer
Keymap Selection
The system console driver for OPNsense defaults to standard
"US"
keyboard map. Other keymaps can be chosen below.
( ) Spanish (accent keys)
( ) Spanish Dvorak
( ) Swedish
( ) Swiss-French
( ) Swiss-French (accent keys)
( ) Swiss-German
( ) Swiss-German (MacBook/MacBook Pro) (accent keys)
( ) Swiss-German (accent keys)
( ) Turkish (F)
( ) Turkish (Q)
( ) Ukrainian
81%
<Select>
<Cancel>
[Press arrows, TAB or ENTER]
ch.kbd: Swiss-German


OPNsense Installer
OPNsense 23.7
Choose one of the following tasks to perform.
Install (UFS) UFS GPT/UEFI Hybrid
Install (ZFS) ZFS GPT/UEFI Hybrid
Other Modes >> Extended Installation
Import Config Load Configuration
Password Reset Recover Installation
Force Reboot Reboot System
< OK >
< Exit >

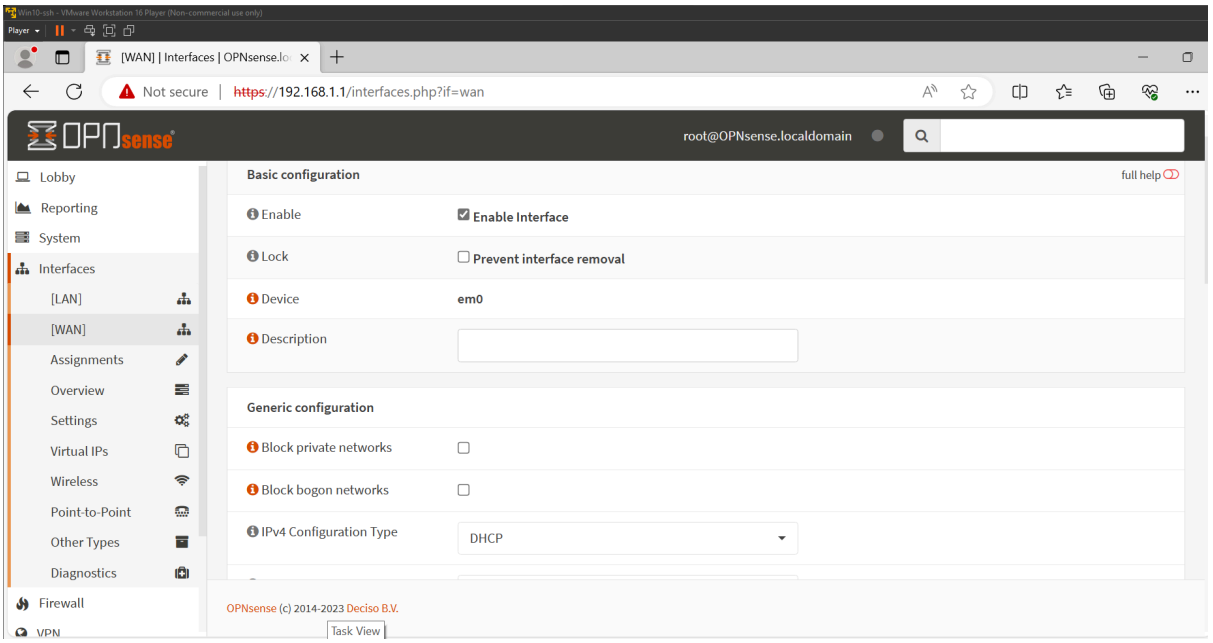


Wähle Option 1 → Nein zu LAGGs → Nein zu Vlan → enstprechend Eintragen, hier em0

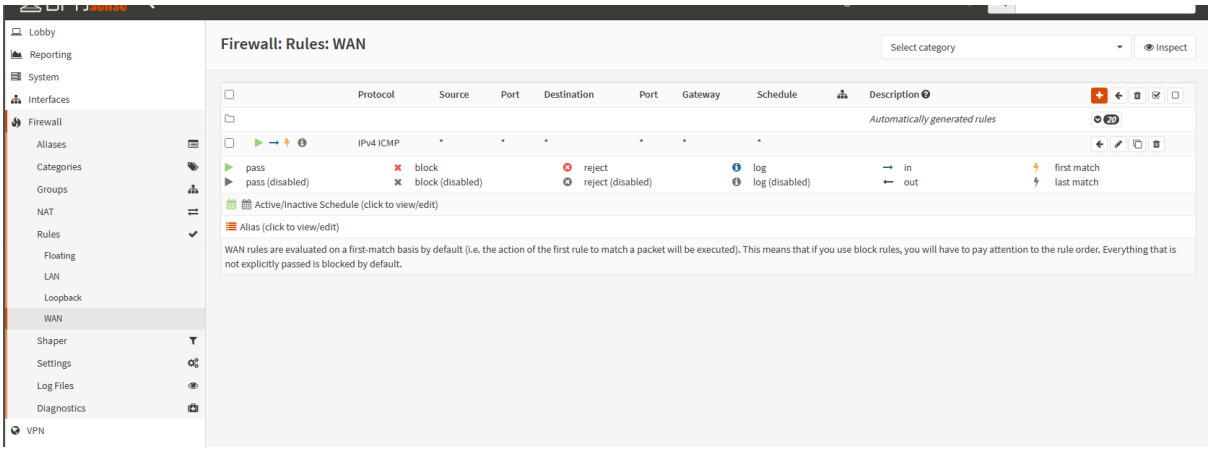
Alles entsprechend eintragen

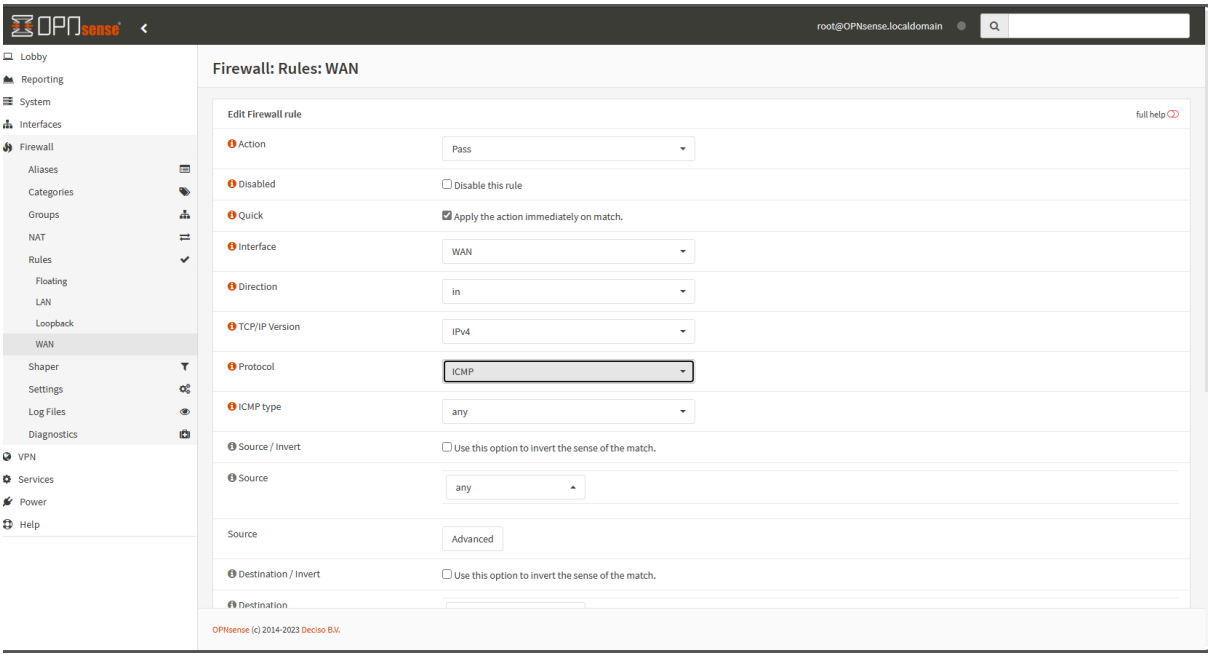


Hier kann man den DNS server konfigurieren

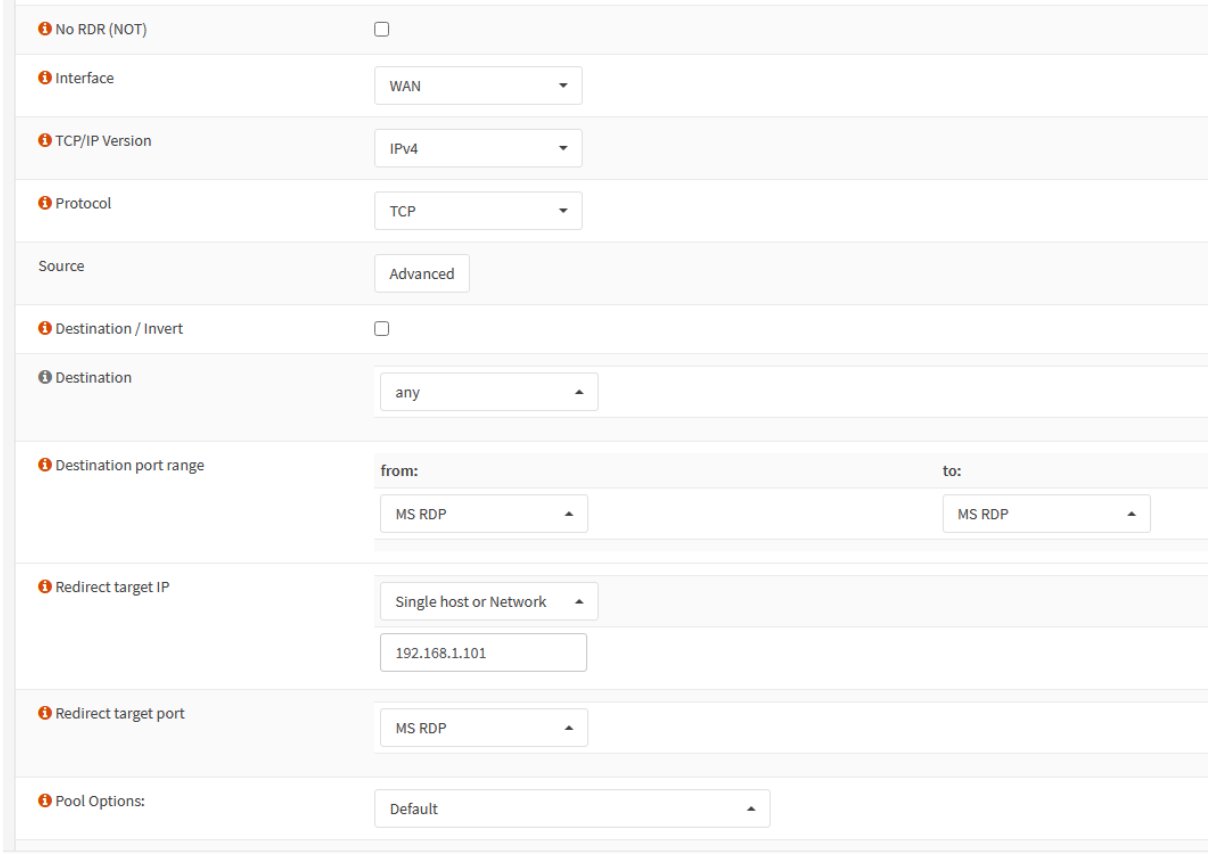


Lokal zu Firewall ping





Wichtig für Remote Verbindung



1. **Verbindung eines Ports der physischen Firewall mit dem physischen Netzwerk in VMWare Workstation:**
    - In VMWare Workstation können Sie die Netzwerkkonfiguration in den Einstellungen der virtuellen Maschine ändern. Normalerweise können Sie zwischen Bridged, NAT, Host-Only und anderen Modi wählen, um die Verbindung zur physischen Firewall und zum physischen Netzwerk herzustellen.
2. **Verbindung von zwei virtuellen Maschinen im gleichen virtuellen Netzwerk ohne Internetzugang:**
    - Sie können ein Host-Only-Netzwerk in VMWare Workstation einrichten und beide virtuellen Maschinen diesem Netzwerk zuweisen.
3. **OPNsense als Bridge oder als Router:**
    - Das hängt von Ihrer Konfiguration ab. OPNsense kann sowohl als Router als auch als Bridge konfiguriert werden, je nach den Anforderungen Ihres Netzwerks.
4. **Problematische Einstellung "Block private Networks":**
    - Das Blockieren privater Netzwerke könnte problematisch sein, wenn Sie Interkommunikation zwischen internen Netzwerken zulassen müssen. Diese Einstellung könnte den Datenverkehr blockieren, der von privaten IP-Adressen stammt.
5. **Default Policy von OPNSense:**
    - Standardmäßig blockiert OPNsense den eingehenden Datenverkehr und erlaubt den ausgehenden. Die genauen Standardeinstellungen können jedoch je nach Installation variieren.
6. **Zusätzliche Firewall-Regeln für die Aufgabe:**
    - Zusätzliche Firewall-Regeln können benötigt werden, um den Datenverkehr zu steuern, z. B. um bestimmte Ports für spezifische Anwendungen zu öffnen.
7. **Ping von der Firewall ausführen:**
    - In der OPNsense-Webbenutzeroberfläche können Sie in den Diagnosewerkzeugen einen Ping durchführen.
8. **IP-Adressen der Netzwerkschnittstellen der Firewall:**
    - Die IP-Adressen der Netzwerkschnittstellen finden Sie in der OPNsense-Webbenutzeroberfläche unter "Interfaces".
9. **Standort des Firewall-Logs:**
    - Das Firewall-Log finden Sie in der OPNsense-Webbenutzeroberfläche unter "Logs" > "Firewall".
10. **Notwendigkeit von NAT:**
    - NAT wird benötigt, um private IP-Adressen im internen Netzwerk auf eine einzige externe IP-Adresse zu übersetzen, wenn der Datenverkehr das WAN verlässt.
11. **Notwendigkeit von Port Forwarding:**
    - Port Forwarding ist erforderlich, um den Datenverkehr von bestimmten externen Ports auf interne Ressourcen weiterzuleiten.
12. **NAT und Firewall-Regel für RDP-Zugriff:**
    - NAT wird verwendet, um den RDP-Verkehr von externen Quellen auf die interne IP-Adresse umzuleiten. Firewall-Regeln werden benötigt, um sicherzustellen, dass nur autorisierter RDP-Verkehr erlaubt ist.

13. **Unterschied zwischen Portscan aus dem ZLI Netzwerk und internen virtuellen Netzwerk:**
    - Der Unterschied könnte in den Zugriffsberechtigungen liegen. Ein Portscan aus dem ZLI (Zero Trust Internal) Netzwerk könnte Zugriff auf mehr Ressourcen haben als ein Portscan aus dem internen virtuellen Netzwerk, je nach Firewall-Regeln und Sicherheitsrichtlinien.

Wie setze ich eine statische IP bei Ubuntu Server?

https://www.linuxtechi.com/static-ip-address-on-ubuntu-server/

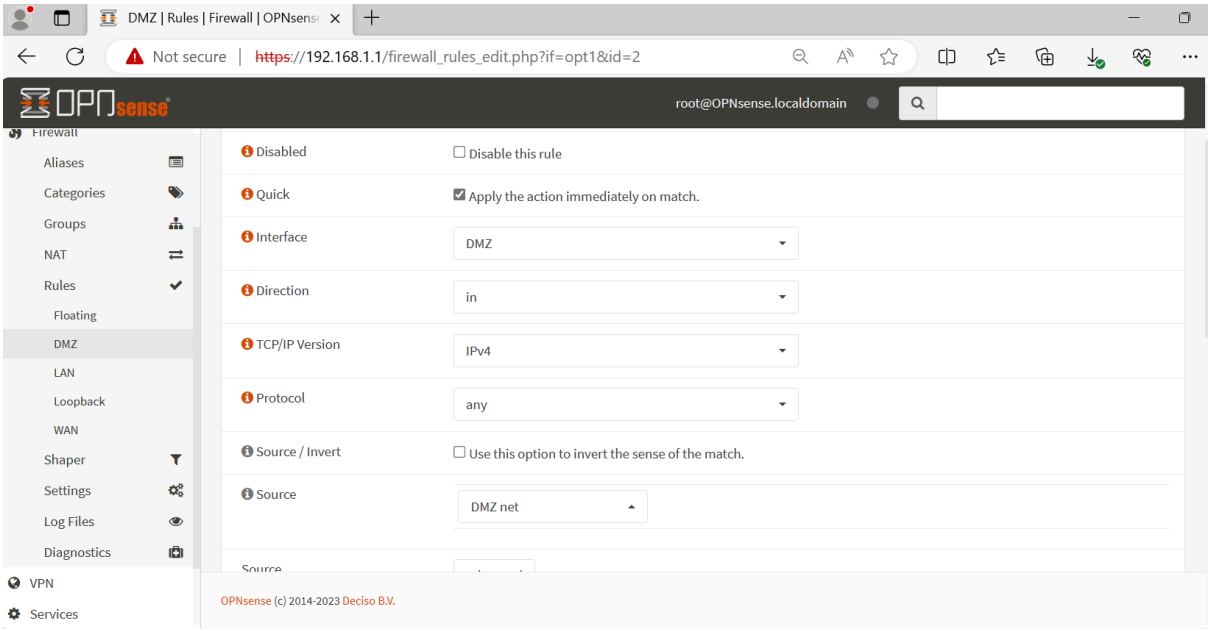
im /etc/netplan/00_.yaml

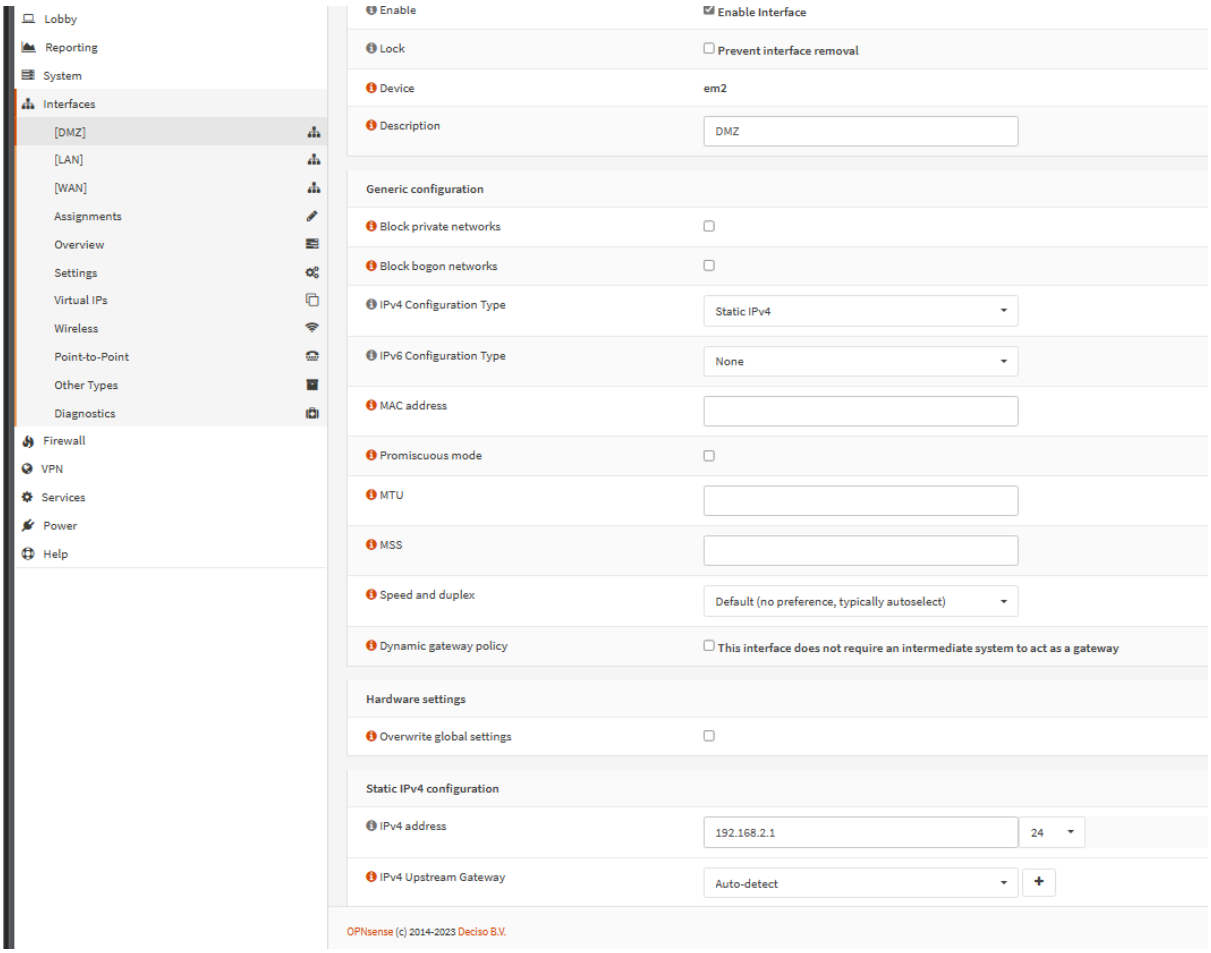
```
network:
  renderer: networkd
  ethernets:
        ens33:
        addresses:
        - 192.168.xxx.xxx/24
        nameservers:
        addresses: [x.x.x.x, 8.8.8.8]
        routes:
        - to: default
        via: 192.168.x.x
```

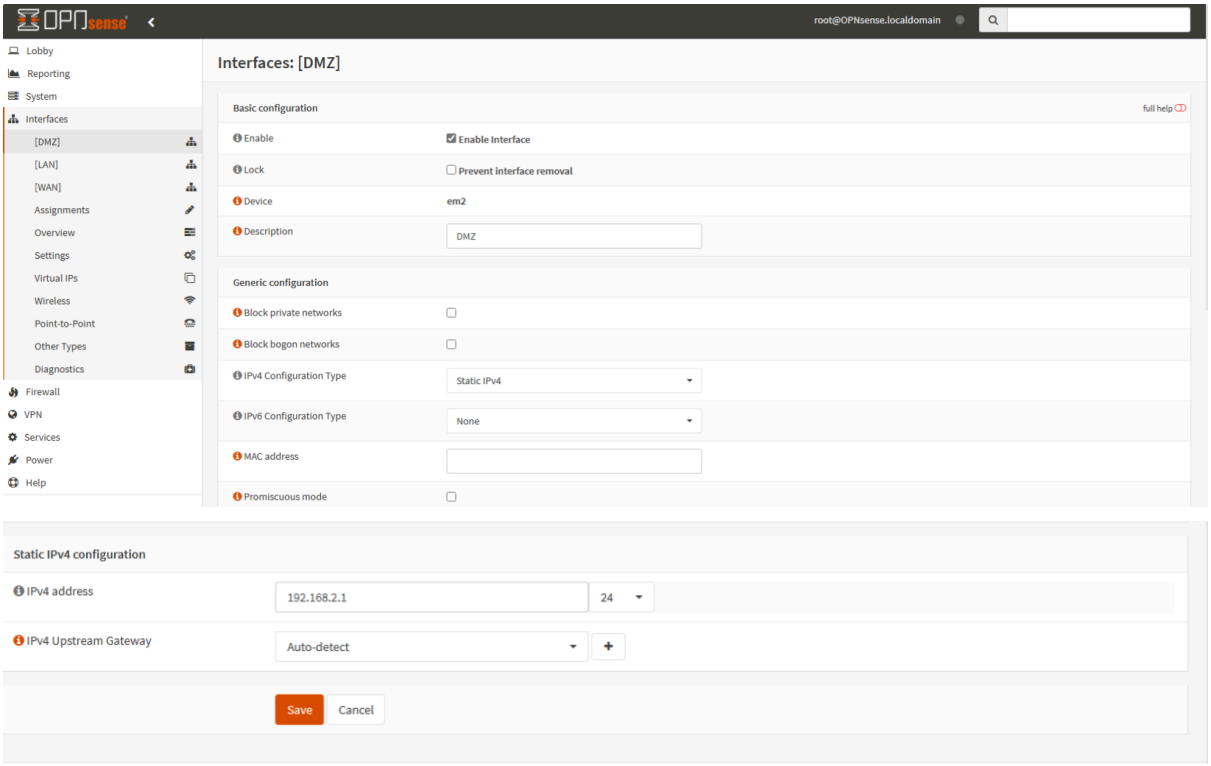
```
  GNU nano 6.2                          00-installer-config.yaml
# This is the network config written by 'subiquity'
network:
  renderer: networkd
  ethernets:
    ens33:
      addresses:
        - 192.168.2.20/24
      nameservers:
        addresses: [1.1.1.1, 8.8.8.8]
      routes:
        - to: default
          via: 192.168.2.1
  version: 2
```

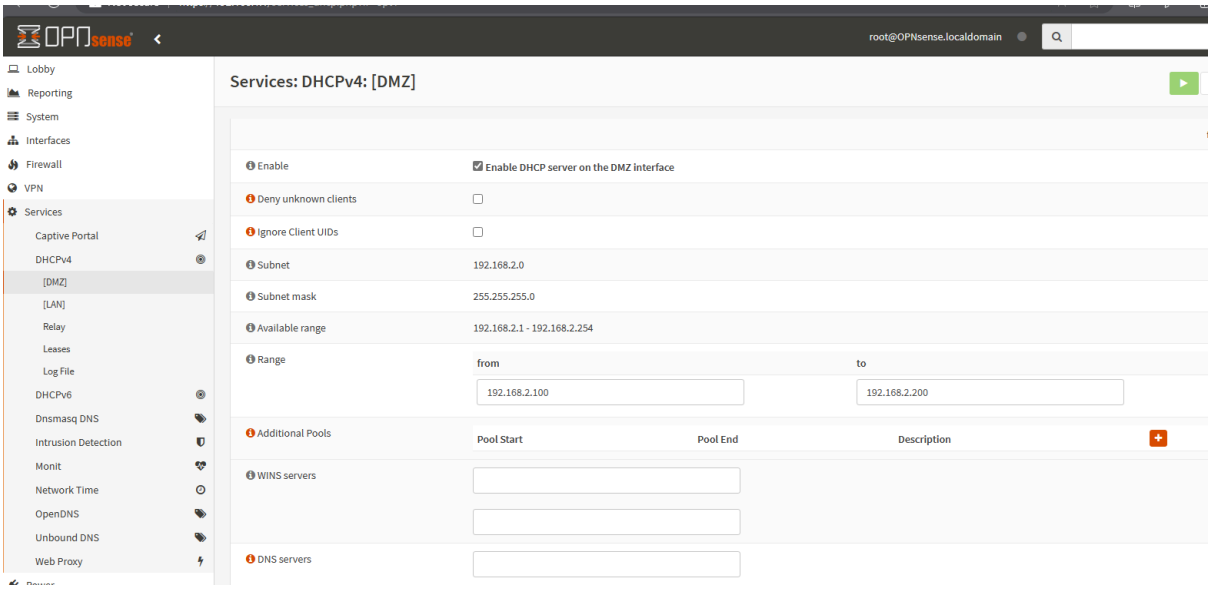
version: 2

sudo netplan apply



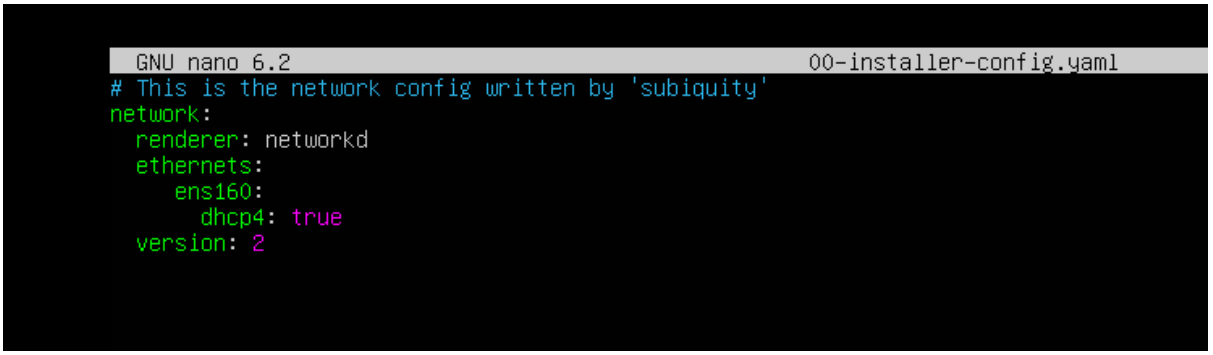

Lobby
Reporting
System
Interfaces
[DMZ]
[LAN]
[WAN]
Assignments
Overview
Settings
Virtual IPs
Wireless
Point-to-Point
Other Types
Diagnostics
Firewall
VPN
Services
Power
Help
Enable
Enable Interface
Lock
Prevent interface removal
Device
em2
Description
DMZ
Generic configuration
Block private networks
Block bogon networks
IPv4 Configuration Type
Static IPv4
IPv6 Configuration Type
None
MAC address
Promiscuous mode
MTU
MSS
Speed and duplex
Default (no preference, typically autoselect)
Dynamic gateway policy
This interface does not require an intermediate system to act as a gateway
Hardware settings
Overwrite global settings
Static IPv4 configuration
IPv4 address
192.168.2.1
24
IPv4 Upstream Gateway
Auto-detect
OPNsense (c) 2014-2023 Deciso B.V.

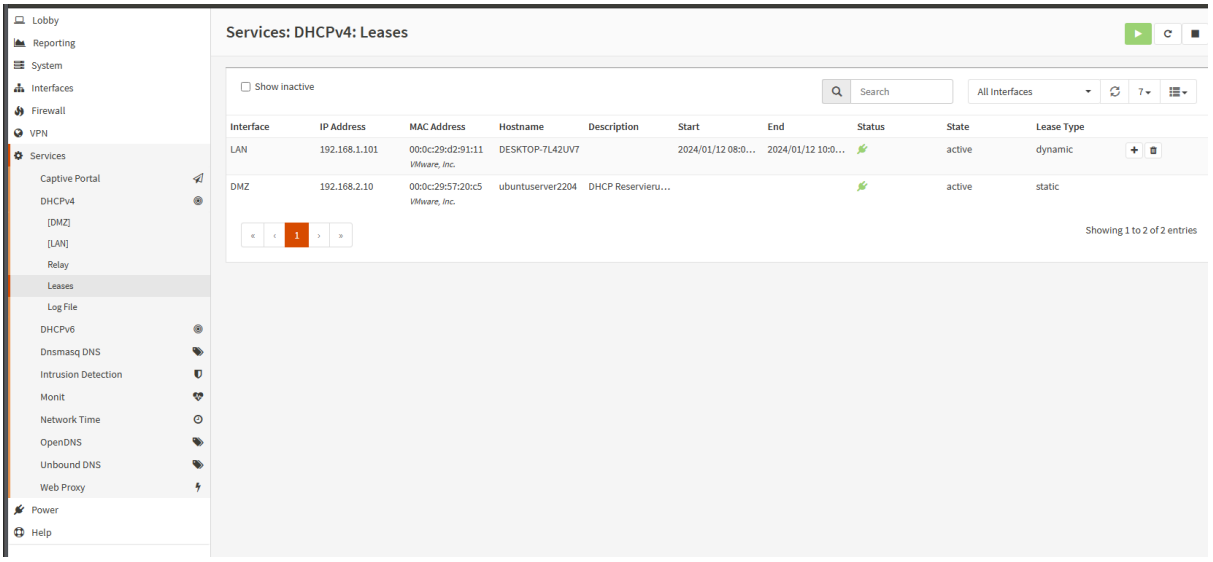

root@OPNsense.localdomain
Interfaces: [DMZ]
Basic configuration
full help
Enable
Enable Interface
Lock
Prevent interface removal
Device
em2
Description
DMZ
Generic configuration
Block private networks
Block bogon networks
IPv4 Configuration Type
Static IPv4
IPv6 Configuration Type
None
MAC address
Promiscuous mode
Static IPv4 configuration
IPv4 address
192.168.2.1
24
IPv4 Upstream Gateway
Auto-detect
Save
Cancel

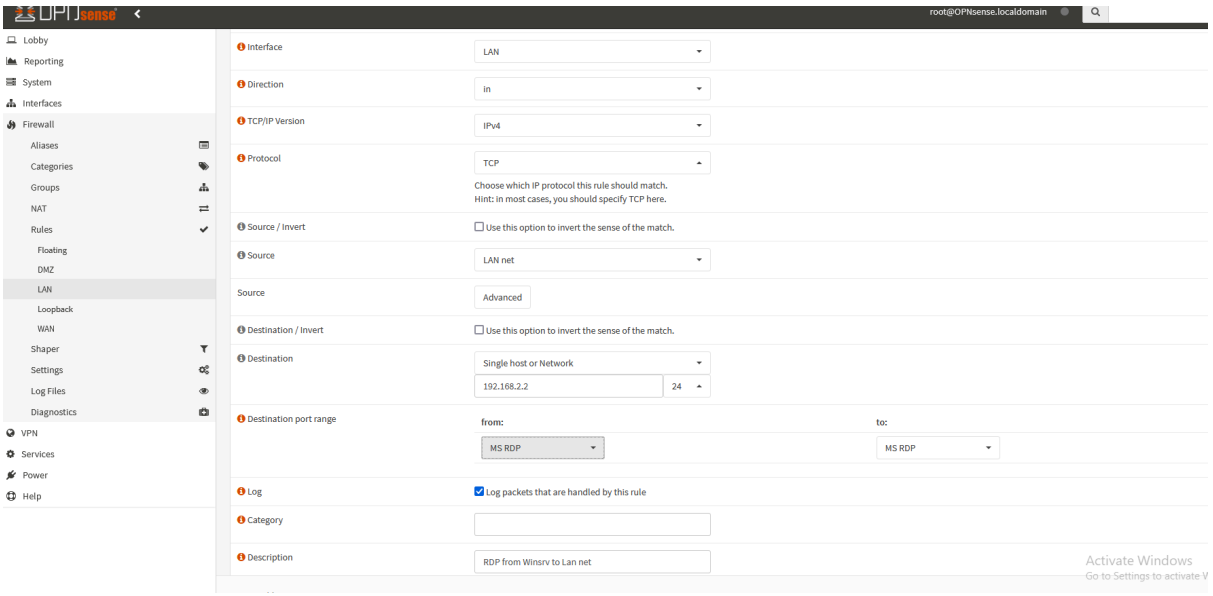


Http treiber starten: sc qt http → net start http

Ubuntu dhcp über netplan config:





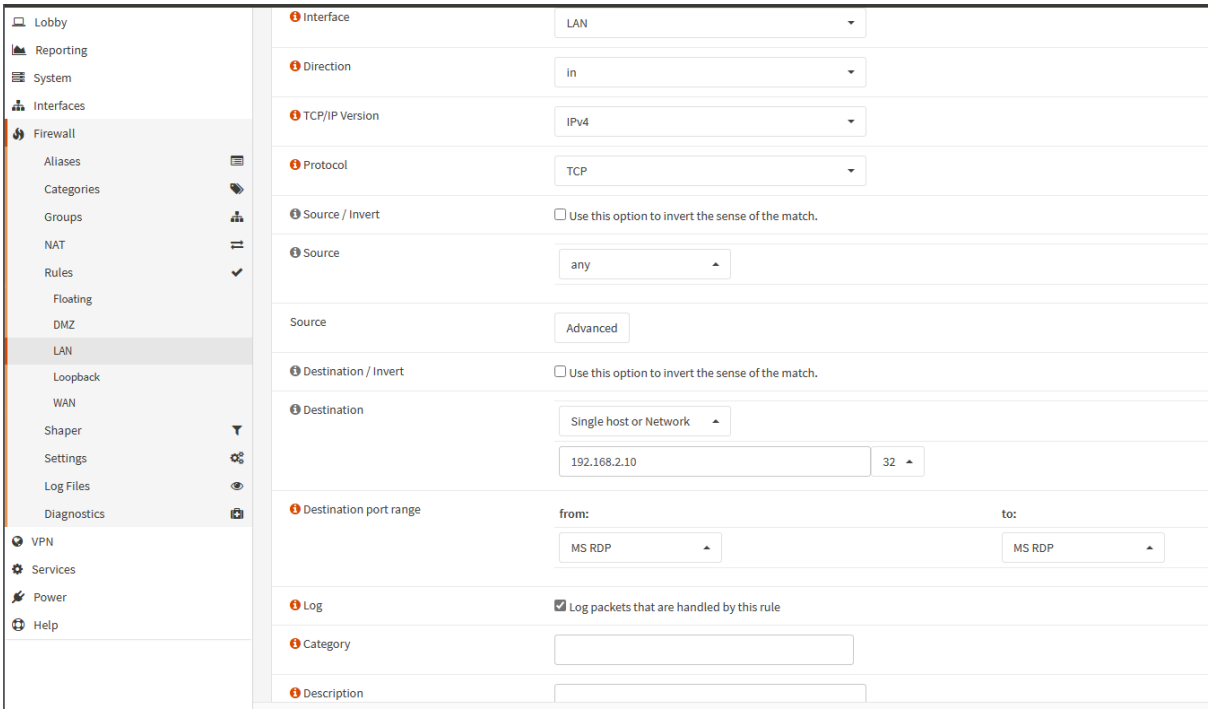

root@OPNsense.localdomain
Lobby
Reporting
System
Interfaces
Firewall
Aliases
Categories
Groups
NAT
Rules
Floating
DMZ
LAN
Loopback
WAN
Shaper
Settings
Log Files
Diagnostics
VPN
Services
Power
Help
Interface
LAN
Direction
in
TCP/IP Version
IPv4
Protocol
TCP
Choose which IP protocol this rule should match.
Hint: in most cases, you should specify TCP here.
Source / Invert
Use this option to invert the sense of the match.
Source
LAN net
Source
Advanced
Destination / Invert
Use this option to invert the sense of the match.
Destination
Single host or Network
192.168.2.2
24
Destination port range
from:
to:
MS RDP
MS RDP
Log
Log packets that are handled by this rule
Category
Description
RDP from Winsrv to Lan net
Activate Windows

Port-Matrix erstellen

Erstellen Sie für ihre Firewall eine Port-Matrix für ihre Firewall Konfiguration.

⇩SRC DST ⇨	Firewall	Linux Server	Windows Server	LAN	DMZ	ANY
Firewall						
Linux Server						
Windows Server						
LAN						ANY
DMZ						!LAN
ANY		TCP/22, TCP/80	TCP/3389, TCP/80, UDP/161			

- **SRC ist der Absender, DST der Empfänger.**
- **Die Firewall arbeitet mit der Default Policy „Deny All".**
- **Tragen Sie die Protokolle ein, die Sie auf der Firewall öffnen müssen (Positive Rules).**
- **Zeichnen Sie alle benötigten Ports ein.**



1. **Was ist SSL/TLS?**

SSL (Secure Sockets Layer) und TLS (Transport Layer Security) sind Protokolle, die entwickelt wurden, um die Sicherheit der Kommunikation über ein Computernetzwerk zu gewährleisten, insbesondere im Kontext von Datenübertragungen über das Internet

2. **Wozu dienen X.509 Zertifikate?**

X.509-Zertifikate dienen der Authentifizierung und Verschlüsselung in sicherheitskritischen Anwendungen wie HTTPS. Sie ermöglichen es, die Identität von Kommunikationspartnern zu verifizieren, indem sie digitale Signaturen und Public-Key-Infrastrukturen verwenden.

3. **Wie unterscheiden sich symmetrische und asymmetrische**

Asymmetrische Verschlüsselung für den sicheren Austausch von symmetrischen Schlüsseln verwendet wird, um dann die tatsächlichen Daten mit symmetrischer Verschlüsselung zu schützen.

4. **Verschlüsselungsalgorithmen?**

Verschlüsselungsalgorithmen sind mathematische Verfahren, die Daten in eine unleserliche Form umwandeln, um ihre Vertraulichkeit zu gewährleisten. Ein Schlüssel wird verwendet, um die Daten zu verschlüsseln und später wieder zu entschlüsseln. Gängige Verschlüsselungsalgorithmen umfassen symmetrische (gleicher Schlüssel für Verschlüsselung und Entschlüsselung) und asymmetrische (unterschiedliche Schlüssel für Verschlüsselung und Entschlüsselung) Methoden.

5. **Nennen Sie sichere symmetrische und asymmetrische Verschlüsselungsalgorithmen.**

Symmetrische: AES, DES

Asymetrisch: RSA, ECC

6. **Wozu benötigt man kryptographische Hashing Algorithmen?**

Kryptographische Hashing-Algorithmen werden verwendet, um Daten wie Passwörter oder Nachrichten in eine feste Länge von Zeichen umzuwandeln, die als Hash-Wert bezeichnet wird. Diese Hash-Werte dienen zur Überprüfung der Integrität von Daten, zum Speichern von Passwörtern sicher in Datenbanken und zur Erstellung digitaler Signaturen.

7. **Nennen Sie einen sicheren kryptographischen Hashing Algorithmus.**

   SHA-256

8. **Mit welchem Verfahren werden Schlüssel über ein unsicheres Netzwerk getauscht?**

Das Diffie-Hellman-Schlüsselaustauschverfahren verwendet. Bei diesem Protokoll können zwei Parteien, auch wenn sie sich in einem unsicheren Netzwerk befinden, einen gemeinsamen geheimen Schlüssel erstellen, ohne ihn direkt miteinander zu teilen.

9. **Welche 4 Arten von Algorithmen gehören zu einer Cipher-Suite?**

Schlüsselaustauschalgorithmus (Key Exchange Algorithm),

Authentifizierungsalgorithmus (Authentication Algorithm**),**

Verschlüsselungsalgorithmus (Encryption Algorithm),

Integritätsprüfalgorithmus (Integrity Check Algorithm).

10. **AES256 ist ein Verschlüsselungsalgorithmus. Was bedeutet die Zahl 256 in diesem Beispiel?**

Das die Schlüssellänge 256 Bits ist.

1. **Was versteht man unter Public Key Infrastructure PKI?**
   Infrastruktur für die Verwaltung von Schlüsselpaaren, Zertifikaten und anderen kryptografischen Schlüsseln.

2. **Wozu benötigt ein Server ein Zertifikat?**

   Ein Server benötigt ein Zertifikat, um seine Identität zu verifizieren und eine sichere Kommunikation mit anderen zu ermöglichen.

3. **Was macht eine Certificate Authority CA?**

   CA ist eine vertrauenswürdige Stelle, die Zertifikate ausstellt und digitale Signaturen überprüft.

4. **Was versteht man unter Root-Certificate?**
   Ein Root-Certificate ist das oberste Zertifikat in einer PKI-Hierarchie und dient als Vertrauensanker für alle anderen Zertifikate.

5. **Was ist ein self-signed Certificate?**

   Ein self-signed Certificate wird von derselben Entität erstellt und signiert, was bedeutet, dass es nicht von einer externen CA verifiziert wird.

6. **Was ist ein Certificate Signing Request?**
   Ein Certificate Signing Request (CSR) ist eine Anfrage, die von einer Entität an eine CA gesendet wird, um ein Zertifikat zu erhalten

7. **Wozu wird eine Certificate Revocation List CRL geführt?**
   Eine Certificate Revocation List (CRL) enthält ungültige Zertifikate, die von der CA zurückgezogen wurden.

8. **Nennen Sie einen sicheren symmetrischen Verschlüsselungsalgorithmus mit Schlüssellänge.**
   AES-256

9. **Nennen Sie einen sicheren asymmetrischen Verschlüsselungsalgorithmus mit Schlüssellänge.**
   RSA-4096.

10. **Nennen Sie einen sicheren, kryptographischen Hashing-Algorithmus.**
    SHA-256.

11. **Was macht "Let's encrypt"?**
    Let's Encrypt ist eine CA, die kostenlose SSL/TLS-Zertifikate automatisch ausstellt.

12. **Erklären Sie, wie man vorgehen muss, um für einen Server im Internet ein gültiges, signiertes Zertifikat zu bekommen.**
    Um ein gültiges, signiertes Zertifikat für einen Server zu erhalten, muss man ein CSR erstellen, es an eine CA senden und deren Überprüfungsprozess durchlaufen.

1. Unterschied zwischen Endpoint- und Perimeter-Security:

Endpoint-Security: Schützt einzelne Geräte (Endpunkte) wie Computer oder Mobilgeräte vor Bedrohungen.
Perimeter-Security: Schützt das gesamte Netzwerk und die Ressourcen, die sich innerhalb einer definierten Grenze (Perimeter) befinden.

2. Bedeutung von Zone Based Firewall:
Eine Zone-Based Firewall ist eine Sicherheitskonfiguration, bei der Netzwerkverbindungen basierend auf logischen Zonen verwaltet werden. Jede Zone enthält eine Gruppe von Netzwerkgeräten mit ähnlichen Sicherheitsanforderungen.

3. Zweck der Firewall Zonen LAN, DMZ und WAN:
LAN (Local Area Network): Interne Zone, in der sich vertrauenswürdige Ressourcen wie Computer und Server befinden.
DMZ (Demilitarized Zone): Eine Zwischenzone zwischen dem internen Netzwerk und dem öffentlichen Internet, in der öffentliche Dienste gehostet werden können.
WAN (Wide Area Network): Externe Zone, repräsentiert das Internet und andere externe Netzwerke.

4. Unterschiede zwischen OPNSense Firewall und Windows Firewall:
OPNSense: Eine auf FreeBSD basierende Firewall-Distribution mit umfassenden Funktionen für Netzwerksicherheit.
Windows Firewall: Die integrierte Firewall in Microsoft Windows-Betriebssystemen.

5. Funktion eines Paketfilters:
Ein Paketfilter überwacht den Datenverkehr zwischen Netzwerken und entscheidet basierend auf vordefinierten Regeln, ob ein Datenpaket zugelassen oder blockiert wird.

6. Unterschied zwischen Stateful und Stateless Inspection:
Stateful Inspection: Berücksichtigt den Zustand der Netzwerkverbindung und erlaubt den Durchgang von Datenpaketen basierend auf dem Verbindungszustand.

Stateless Inspection: Entscheidet über den Datenpaketdurchgang basierend auf einzelnen Paketattributen, ohne den Verbindungszustand zu berücksichtigen.

7. Aufgaben eines Application Layer Gateway (ALG):
Ein ALG erleichtert die Kommunikation von Anwendungen, die verschiedene Netzwerkprotokolle verwenden, indem es spezifische Anwendungsprotokolle erkennt und dafür geeignete Übersetzungen vornimmt.

8. Erhöhung der Sicherheit durch NAT (Network Address Translation):
NAT verbirgt interne Netzwerkstrukturen, indem es private IP-Adressen in öffentliche IP-Adressen umwandelt. Dadurch erschwert es Angriffen von außen, da die internen Adressen nicht direkt sichtbar sind.

9. Unterschied zwischen positiven und negativen Firewall Regeln:
Positive Regel: Erlaubt bestimmten Datenverkehr.
Negative Regel: Blockiert bestimmten Datenverkehr.

10. Aufgabe der Default Policy einer Firewall:
Die Default Policy legt fest, was mit Datenverkehr geschieht, der keiner expliziten Regel entspricht. Sie kann "Allow" (erlauben) oder "Deny/Drop" (ablehnen/blockieren) sein.

11. Bedeutung von Default Policy "Deny/Drop All":
Alle Datenverkehrsarten werden standardmäßig blockiert, es sei denn, es gibt eine explizite Regel, die diesen Datenverkehr erlaubt.

12. Aktionen einer Firewall-Regel:
Allow: Erlaubt den Datenverkehr.
Deny/Drop: Blockiert den Datenverkehr.
Reject: Blockiert den Datenverkehr und sendet eine Benachrichtigung an den Absender.

13. Unterschied zwischen Aktionen Drop/Deny und Reject:
Drop/Deny: Der Datenverkehr wird blockiert, ohne eine spezifische Ablehnungsnachricht zurückzusenden.
Reject: Der Datenverkehr wird blockiert, und die Firewall sendet eine Ablehnungsnachricht an den Absender./32 = immer wen einzelner rechner steht

https://docs.opnsense.org/manual/how-tos/self-signed-chain.html

1. **Wozu verwendet man VPNs?**

   VPNs werden verwendet, um eine sichere Verbindung über unsichere Netzwerke herzustellen, und um Daten verschlüsselt zu übertragen.

2. **Was ist der Unterschied zwischen einem Remote Access VPN und einem Site-to-Site VPN?**

   Remote Access VPN ermöglicht Einzelpersonen den sicheren Zugriff auf das Netzwerk, während Site-to-Site VPN die Verbindung zwischen Netzwerken herstellt.

3. **Was ist OpenVPN?**

   OpenVPN ist eine Open-Source-Software für VPN-Verbindungen, die verschiedene Verschlüsselungsprotokolle unterstützt.

4. **Was bringt 2-Factor Authentifizierung 2FA?**

   2-Factor Authentifizierung (2FA) erhöht die Sicherheit, indem sie neben dem Passwort eine zweite Authentifizierungsmethode erfordert.

5. **Was ist TOTP und wie funktioniert der Google Authenticator?**

   TOTP (Time-based One-Time Password) ist ein Algorithmus, der Zeit-basierte Einmalpasswörter generiert. Der Google Authenticator verwendet TOTP.

6. **Wieso benötigt ein WireGuard RoadWarrior Setup keine Benutzerverwaltung?**

   WireGuard RoadWarrior Setup benötigt keine Benutzerverwaltung, da es auf öffentlichen Schlüsseln basiert, wodurch die Verwaltung vereinfacht wird.

7. **Wozu dient das Protokoll IPSec?**

   IPSec ist ein Protokoll, das Sicherheit für Internet Protocol (IP) bietet, einschließlich Verschlüsselung und Authentifizierung.

8. **Was machen die Protokolle PPTP, SSTP, L2TP?**

   PPTP, SSTP und L2TP sind VPN-Protokolle. PPTP ist unsicher, SSTP ist für Windows optimiert, und L2TP bietet Tunneling.

9. **Was versteht man unter PSK?**

   PSK (Pre-Shared Key) ist ein vorab geteilter Schlüssel, der bei VPN-Verbindungen für die Authentifizierung verwendet wird.

10. Wozu verwenden VPN Verbindungen X.509 Zertifikate?

VPN-Verbindungen verwenden X.509 Zertifikate zur Authentifizierung und Verschlüsselung der Datenübertragung.

11. Welche Aufgabe erfüllt das Protokoll RADIUS?

RADIUS (Remote Authentication Dial-In User Service) ist ein Protokoll für die Authentifizierung, Autorisierung und Buchhaltung von Netzwerkdiensten.