Nina, Anna, Naemi

DMZ

Netzwerk mit Firewall einrichten

Inhaltsverzeichnis

**Inhalt**

[1 Einleitung 1](#_Toc168053018)

[2 Namensschema 2](#_Toc168053019)

[3 Netzwerkplan 2](#_Toc168053020)

[4 IP-Konzept 2](#_Toc168053021)

[5 Gerätebeschreibung 2](#_Toc168053022)

[6 Installation / Konfiguration 3](#_Toc168053023)

[7 Firewall Regeln 6](#_Toc168053024)

[8 Testing 8](#_Toc168053025)

[8.1 Testkonzept 8](#_Toc168053026)

[8.2 Testprotokoll 10](#_Toc168053027)

[Abbildung 1: Netzerkplan 2](#_Toc168053870)

[Abbildung 2 Workstation: Server Verbindung 3](#_Toc168053871)

[Abbildung 3 Hyper V VMs 3](#_Toc168053872)

[Abbildung 4: Switche von DMZ 4](#_Toc168053873)

[Abbildung 5: Switch WAN 4](#_Toc168053874)

[Abbildung 6: Switch LAN 4](#_Toc168053875)

[Abbildung 7 PFSense Router 5](#_Toc168053876)

[Abbildung 8 Statische IP Webserver 5](#_Toc168053877)

[Abbildung 5 Firewall Einstellungen WAN 6](#_Toc168053878)

[Abbildung 6 Firewall Einstellungen LAN 6](#_Toc168053879)

[Abbildung 11: Einstellungen Firewall WNC-01 7](#_Toc168053880)

[Abbildung 12: Default Apache page von Workstation 7](#_Toc168053881)

[Tabelle 1: Namens Konzept 2](#_Toc168053459)

[Tabelle 2: IP-Konzept 2](#_Toc168053460)

[Tabelle 3: Gerätebeschreiung 3](#_Toc168053461)

[Tabelle 4:Test 1 8](#_Toc168053462)

[Tabelle 5:Test 2 8](#_Toc168053463)

[Tabelle 6:Test 3 9](#_Toc168053464)

[Tabelle 7: Test 4 9](#_Toc168053465)

[Tabelle 8: Testprotokoll 10](#_Toc168053466)

# Einleitung

Die Aufgabe bestand darin, ein virtuelles Netzwerk zu erstellen und mit PFsense als Firewall/Router zu konfigurieren. Dieses Netzwerk wurde in drei Hauptbereiche unterteilt: LAN, DMZ und WAN.

Im WAN, dem Wide Area Network, sollte eine dynamische IP-Adresse verwendet werden. Zwei virtuelle Maschinen, ein Windows Server und ein Linux Webserver, sollten über den physikalischen WAN Port erreichbar sein.

Das LAN, das Local Area Network, wurde in zwei Subnetze aufgeteilt: das Büronetzwerk mit der IPv4-Netzwerkadresse 192.168.1.0/24 und das Produktionsnetzwerk mit der IPv4-Netzwerkadresse 192.168.2.0/24.

Die DMZ, die demilitarisierte Zone, war für das Besuchernetzwerk reserviert und hatte die IPv4-Netzwerkadresse 192.168.3.0/24.

# Namensschema

|  |  |  |
| --- | --- | --- |
| Webserver | websrv-Y | Y = zufällige Zahl |
| Windows Client | WNC-Y | Y = zufällige Zahl |
| Workstation | Workstation |  |
| PFSense | PFSense |  |

Tabelle 1: Namensschema

# Netzwerkplan

Ein Bild, das Text, Screenshot, Diagramm, Plan enthält.

Automatisch generierte Beschreibung

Abbildung 1: Netzwerkplan

# IP-Konzept

|  |  |  |
| --- | --- | --- |
| Gerätetyp | Art | IP-Adressen |
| Webserver | Statisch | 10.30.30.5/24 |
| Windows 10 Client | Statisch | 10.20.20.10/24 |
| Workstation | Statisch | 192.168.0.133/24 |
| PFSense | Statisch | 192.168.0.123/24 |

Tabelle 2: IP-Konzept

# Gerätebeschreibung

|  |  |
| --- | --- |
| Gerätetyp | Service |
| Webserver | Apache2 |
| PFSense | PFSense Router, Firewall |
| Windows 10 Client | Windows 10 |
| Webserver | Windows 11 |

Tabelle 3: Gerätebeschreibung

# Installation / Konfiguration

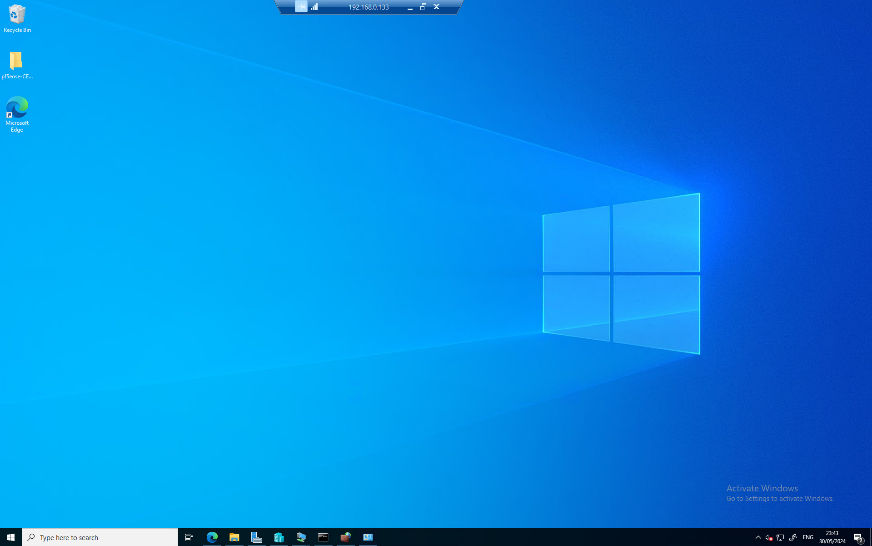


Abbildung 2 Workstation: Server Verbindung

Mit Server verbinden. (Windows Taste und Remote eintragen und verbinden)

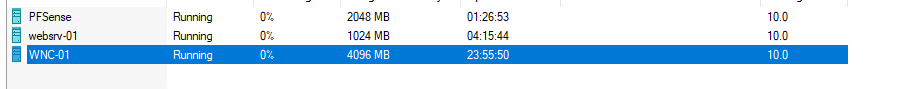


Abbildung 3 Hyper V VMs

Zuerst PF-Sense einrichten danach Windows Client installieren. (im Browser IP des PF-Sense eintragen und konfigurieren)

Ein Bild, das Text, Screenshot, Software, Webseite enthält.

Automatisch generierte Beschreibung

Abbildung 4: Switche von DMZ

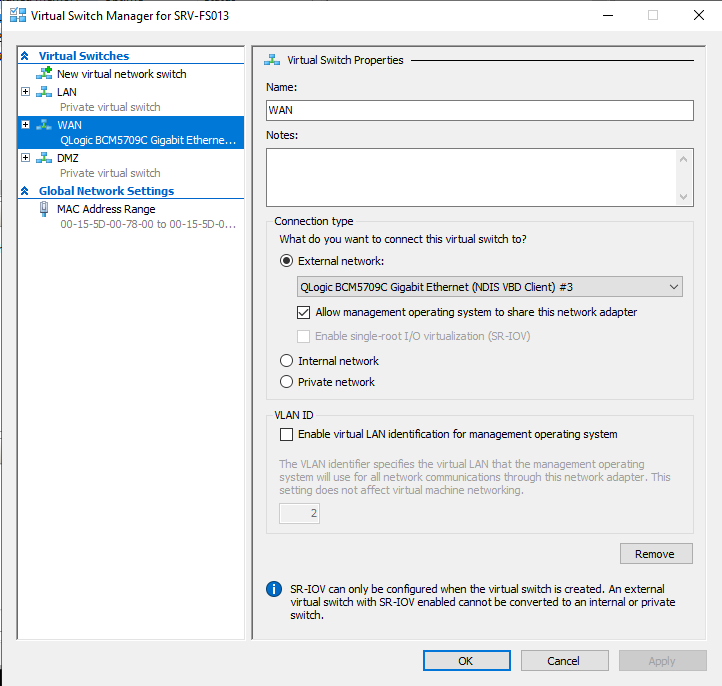


Abbildung 5: Switch WAN

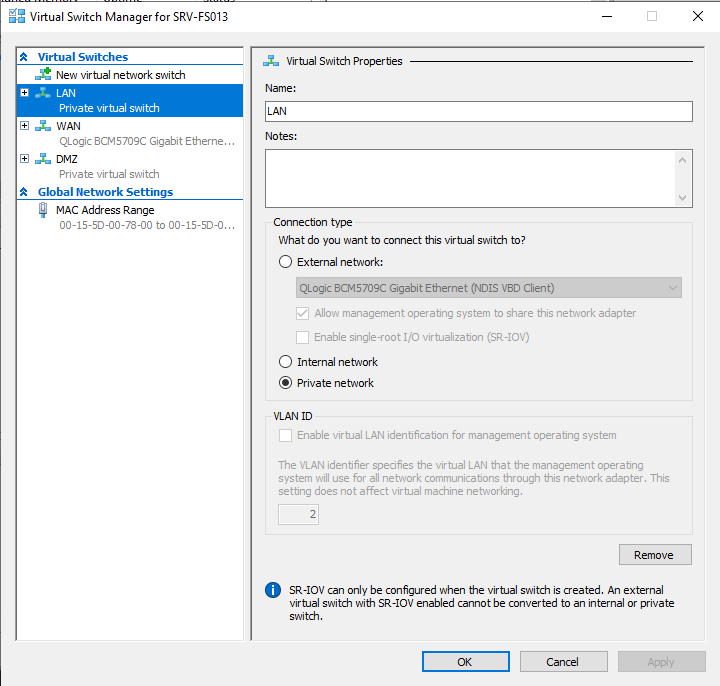


Abbildung 6: Switch LAN

LAN, DMZ und WAN Adapter erstellen. (LAN und DMZ Privat setzten)

Ein Bild, das Text, Elektronik, Screenshot, Software enthält.

Automatisch generierte Beschreibung

Abbildung 7 PFSense Router

Linux Server aufsetzen. (PF-Sense installieren)  
WAN, LAN und OPT1(DMZ) muss IP-Adressen zugewiesen haben. (wenn keine da sind, dann noch erledigen)



Abbildung 8 Statische IP Webserver

Webserver aufgesetzt und statische IP setzten. (Apache2 installieren)

# Firewall Regeln

Ein Bild, das Text, Schrift, Screenshot, Reihe enthält.

Automatisch generierte Beschreibung

Abbildung 5 Firewall Einstellungen WAN

Ein Bild, das Text, Zahl, Schrift, Software enthält.

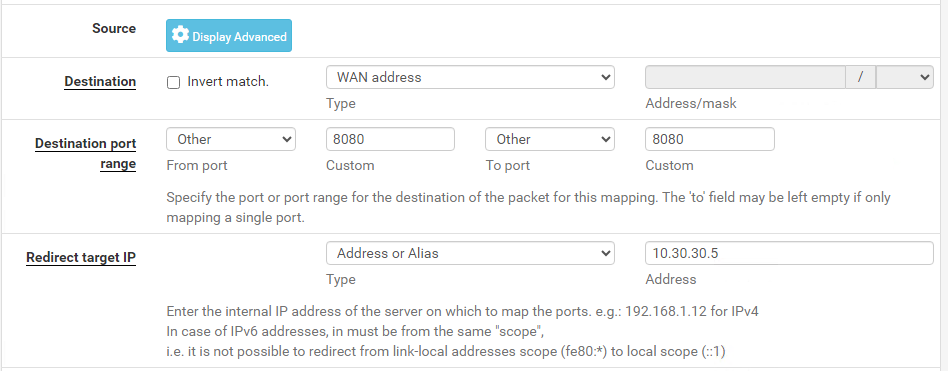
Automatisch generierte Beschreibung

Abbildung 6 Firewall Einstellungen LAN

Ein Bild, das Text, Schrift, Zahl, Software enthält.

Automatisch generierte Beschreibung

Im Browser vom Windows Client IP-Adresse vom LAN eintragen und Firewall einrichten.



Im NAT Port Forward, Port angeben.

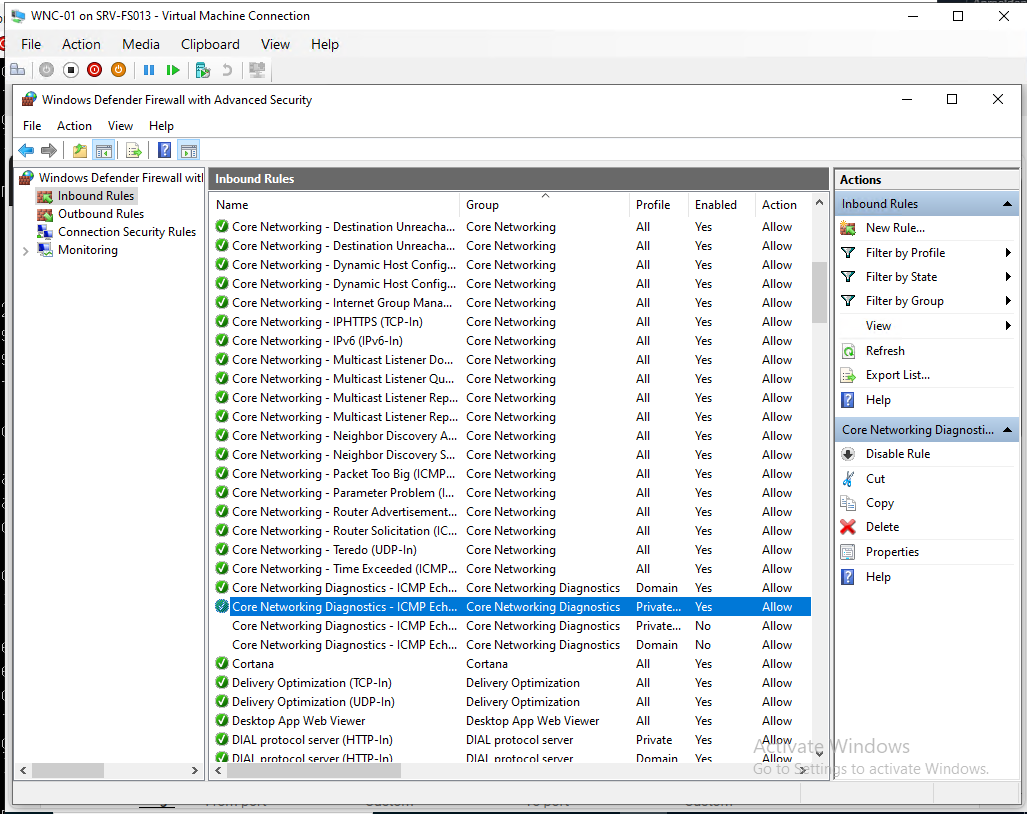


Abbildung 11: Einstellungen Firewall WNC-01

Im Windows Client anpingen ermöglichen.



Abbildung 12: Default Apache page von Workstation

Jetzt kannst du vom WAN ins DMZ, indem du die IP des Routers einträgst.

# Testing

## Testkonzept

|  |  |
| --- | --- |
| **ID** | **T01** |
| **Testfall** | Zugriff auf die Webseite über das LAN überprüfen |
| **Host** | Workstation |
| **Beschreibung** | Vom Webserver zum LAN gelangen. Die IP-Adresse pingen. |
| **Testmethoden/ Testschritte** | Die Firewall wurde so angepasst, dass auch LAN mit dem Webserver kommunizieren kann. So musste bei LAN der Zugriff auf den Webserver erlaubt werden. Danach kann man die IP des Webservers, also 10.20.20.10 bei WNC-01 in den Browser eingeben, dann sollte eine Default Webseite von Apachen sein. |
| **Erwartetes Ergebnis** | Der WNC-01 sollte unter der IP des Webservers erreichbar sein und eine Default Webseite anzeigen. |

Tabelle 4:Test 1

|  |  |
| --- | --- |
| **ID** | **T02** |
| **Testfall** | Zugriff auf die Webseite über das WAN überprüfen |
| **Host** | Workstation |
| **Beschreibung** | Workstation sollte in der Lage sein, den Webserver im Browser aufzurufen. |
| **Testmethoden/ Testschritte** | Angefangen damit, dass man im NAT Port Forward den Port angeben muss, damit der Server die Webseite aufrufen kann. D.h. wir können die Webseite mit der IP 10.30.30.5 im Browser aufrufen. |
| **Erwartetes Ergebnis** | Auf der Workstation sollte die Default Webseite von Apache sein. |

Tabelle 5:Test 2

|  |  |
| --- | --- |
| **ID** | **T03** |
| **Testfall** | Zugang vom Webserver auf LAN überprüfen |
| **Host** | Workstation |
| **Beschreibung** | Der Websever sollte den das LAN bzw. den WNC-01 pingen können |
| **Testmethoden/ Testschritte** | Damit der Webserver nach aussen kommunizieren kann, muss dem OPT1 die Erlaubnis erteilt werden. In der Firewall dem OPT1 die Erlaubnis geben. Das heisst, wir sollten auch der WNC-01 mit der IP 10.20.20.10 pingen können. Wenn der Server auch Pakete zurückerhält, sollte er erreichbar sein. |
| **Erwartetes Ergebnis** | Der Webserver konnte den WNC-01 pingen und hat die Pakete erfolgreich empfangen. |

Tabelle 6:Test 3

|  |  |
| --- | --- |
| **ID** | **T04** |
| **Testfall** | Zugang vom LAN auf WAN überprüfen |
| **Host** | Workstation |
| **Beschreibung** | Der WNC-01 sollte den im CMD mit ping erreichen können. |
| **Testmethoden/ Testschritte** | Beim WNC-01 muss die Firewall geändert werden. Das heisst, man muss ICMP Echo IPv4 hinzufügen, damit der WNC-01 auch den Server pingen kann. Jetzt können wir im CMD den Router mit der IP-Adresse 192.168.0.123 pingen. |
| **Erwartetes Ergebnis** | Der WNC-01 sollte Pakete vom Router empfangen. |

Tabelle 7: Test 4

## Testprotokoll

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Nr.** | **Person** | **Datum** | **Test Name** | **Ergebnis** |
| **T01** | NR | 30.05.2024 | Zugriff auf die Webseite über das LAN überprüfen | Erfolgreich |
| **T02** | NR | 31.05.2024 | Zugriff auf die Webseite über das WAN überprüfen | Erfolgreich |
| **T03** | NR | 30.05.2024 | Zugang vom Webserver auf LAN überprüfen | Erfolgreich |
| **T04** | NR | 31.05.2024 | Zugang vom LAN auf WAN überprüfen | Erfolgreich |

Tabelle 8: Testprotokoll