



DMZ

Netzwerk mit Firewall einrichten

Nina, Anna, Naemi

Inhaltsverzeichnis

Inhalt

1	Einleitung	2
2	Namensschema	2
3	Netzwerkplan.....	3
4	IP-Konzept	3
5	Gerätebeschreibung	3
6	Installation / Konfiguration	4
7	Firewall Regeln	7
8	Testing	9
8.1	Testkonzept	9
8.2	Testprotokoll	11

Abbildung 1: Netzerkplan	3
Abbildung 2 Workstation: Server Verbindung	4
Abbildung 3 Hyper V VMs	4
Abbildung 4: Switche von DMZ.....	4
Abbildung 5: Switch WAN.....	5
Abbildung 6: Switch LAN	5
Abbildung 7 PFSense Router	6
Abbildung 8 Statische IP Webserver	6
Abbildung 5 Firewall Einstellungen WAN.....	7
Abbildung 6 Firewall Einstellungen LAN	7
Abbildung 11: Einstellungen Firewall WNC-01	8
Abbildung 12: Default Apache page von Workstation	8

Tabelle 1: Namens Konzept	2
Tabelle 2: IP-Konzept.....	3
Tabelle 3: Gerätebeschreibung	3
Tabelle 4:Test 1.....	9
Tabelle 5:Test 2.....	9
Tabelle 6:Test 3.....	10
Tabelle 7: Test 4.....	10
Tabelle 8: Testprotokoll	11

1 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.

2 Namensschema

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

Tabelle 1: Namensschema

3 Netzwerkplan

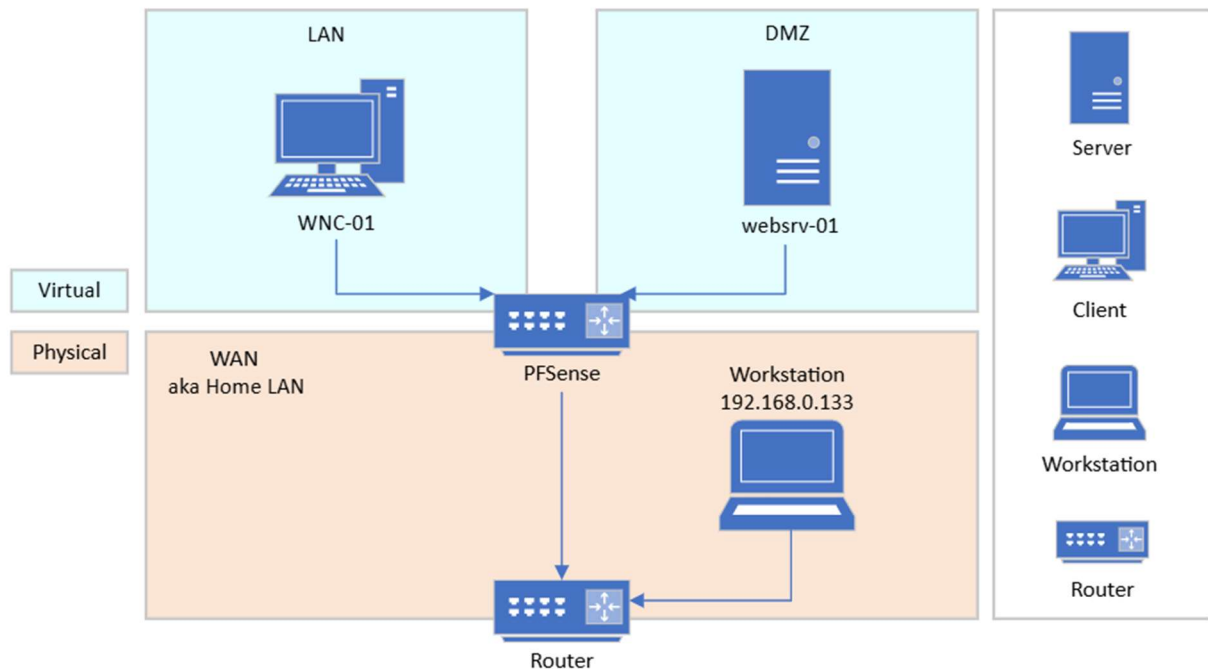


Abbildung 1: Netzwerkplan

4 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

5 Gerätebeschreibung

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

Tabelle 3: Gerätebeschreibung

6 Installation / Konfiguration

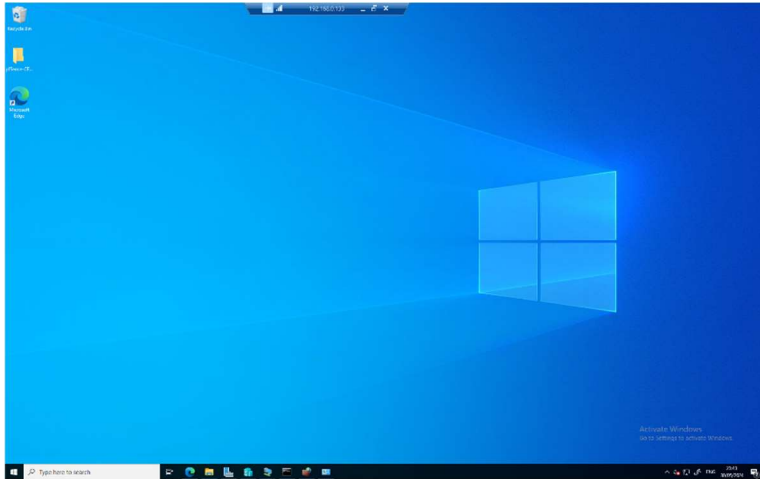


Abbildung 2 Workstation: Server Verbindung

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

PFSense	Running	0%	2048 MB	01:26:53	10.0
webserv-01	Running	0%	1024 MB	04:15:44	10.0
WNC-01	Running	0%	4096 MB	23:55:50	10.0

Abbildung 3 Hyper V VMs

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

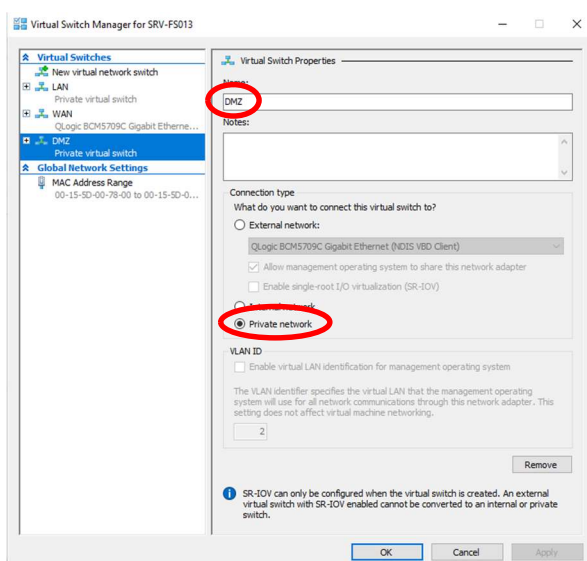


Abbildung 4: Switche von DMZ

Netzwerk mit Firewall einrichten

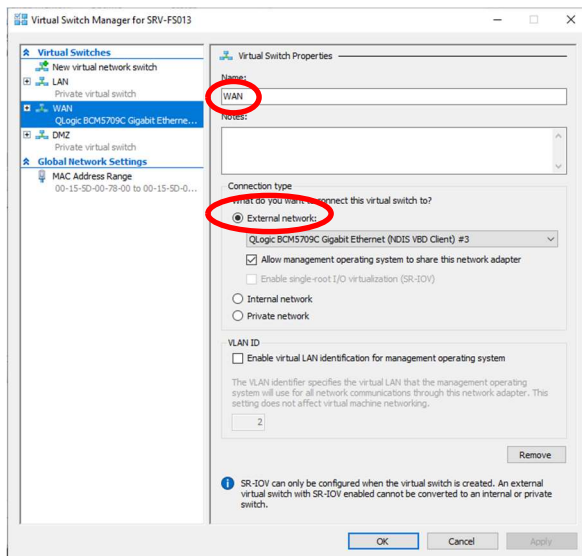


Abbildung 5: Switch WAN

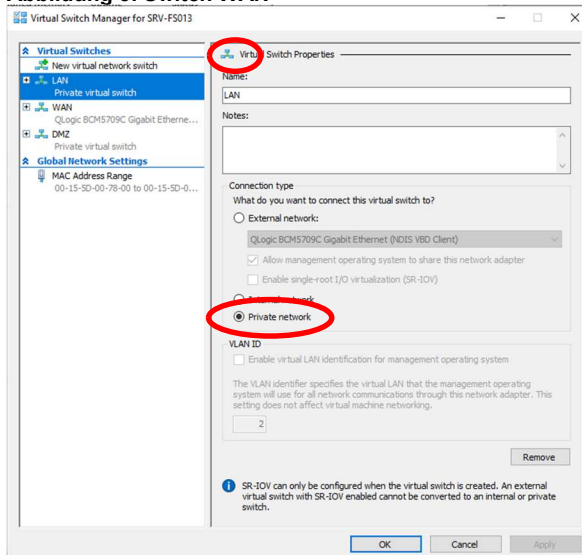
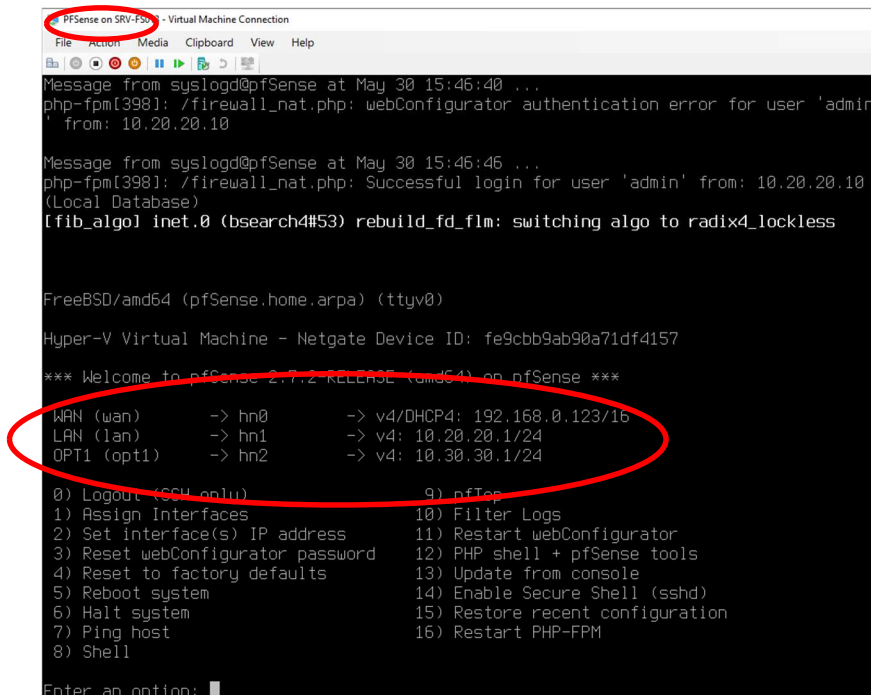


Abbildung 6: Switch LAN

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

Netzwerk mit Firewall einrichten



```

PFSense on SRV-F50 - Virtual Machine Connection
File Action Media Clipboard View Help

Message from syslogd@pfSense at May 30 15:46:40 ...
php-fpm[398]: /firewall_nat.php: webConfigurator authentication error for user 'admin'
' from: 10.20.20.10

Message from syslogd@pfSense at May 30 15:46:46 ...
php-fpm[398]: /firewall_nat.php: Successful login for user 'admin' from: 10.20.20.10
(Local Database)
[[fib_algo] inet.0 (bsearch4#53) rebuild_fd_flm: switching algo to radix4_lockless

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

Hyper-V Virtual Machine - Netgate Device ID: fe9cbb9ab90a71df4157

*** Welcome to pfSense 2.7.2 RELEASE (amd64) on pfSense ***

WAN (wan)      -> hn0      -> v4/DHCP4: 192.168.0.123/16
LAN (lan)      -> hn1      -> v4: 10.20.20.1/24
OPT1 (opt1)    -> hn2      -> v4: 10.30.30.1/24

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

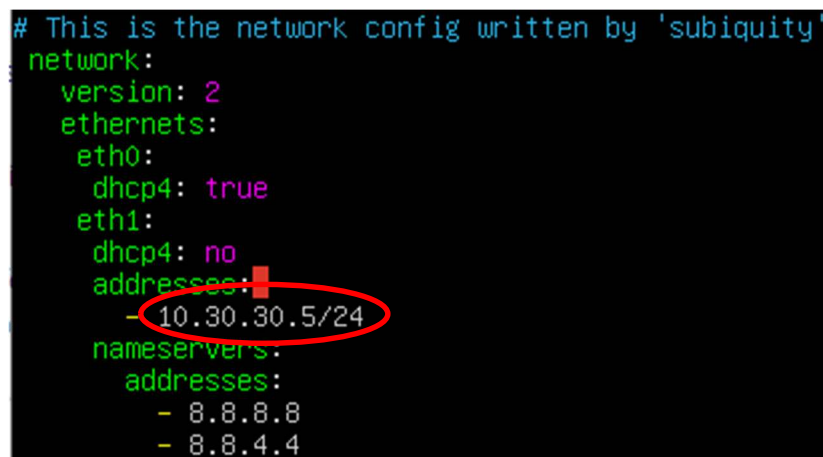
Enter an option:

```

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)



```

# This is the network config written by 'subiquity'
network:
  version: 2
  ethernets:
    eth0:
      dhcp4: true
    eth1:
      dhcp4: no
      addresses:
        - 10.30.30.5/24
  nameservers:
    addresses:
      - 8.8.8.8
      - 8.8.4.4

```

Abbildung 8 Statische IP Webserver

Webserver aufgesetzt und statische IP setzen. (Apache2 installieren)

7 Firewall Regeln





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 *	OPT1 address	*	WAN address	*	*	none			 
<input type="checkbox"/>	✗ 0/0 B	IPv4 *	OPT1 address	*	LAN address	*	*	none			 

Abbildung 9 Firewall Einstellungen WAN
















Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓ 2/1.92 MiB	*	*	*	LAN Address	443	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	✓ 0/0 B	IPv4 *	LAN address	*	OPT1 address	*	*	none			 
<input type="checkbox"/>	✓ 0/0 B	IPv4 *	LAN address	*	WAN address	*	*	none			 
<input type="checkbox"/>	✓ 29/4.68 MiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	 
<input type="checkbox"/>	✓ 0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	 

Abbildung 10 Firewall Einstellungen LAN

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✗ 0/1.74 MiB	*	RFC 1918 networks	*	*	*	*	*		Block private networks	
<input type="checkbox"/>	✗ 0/9 KiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	
<input type="checkbox"/>	✓ 0/0 B	IPv4 *	WAN address	*	OPT1 address	*	*	none			 
<input type="checkbox"/>	✗ 0/0 B	IPv4 *	WAN address	*	LAN address	*	*	none			 

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

Source

Display Advanced

Destination

☐ Invert match.

WAN address

Type

Address/mask

Destination port range

Other

8080

Other

8080

From port

Custom

To port

Custom

Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

Redirect target IP

Address or Alias

10.30.30.5

Type

Address

Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4
In case of IPv6 addresses, it must be from the same "scope", i.e. it is not possible to redirect from link-local addresses scope (fe80:*) to local scope (::1)

Im NAT Port Forward, Port angeben.

Netzwerk mit Firewall einrichten

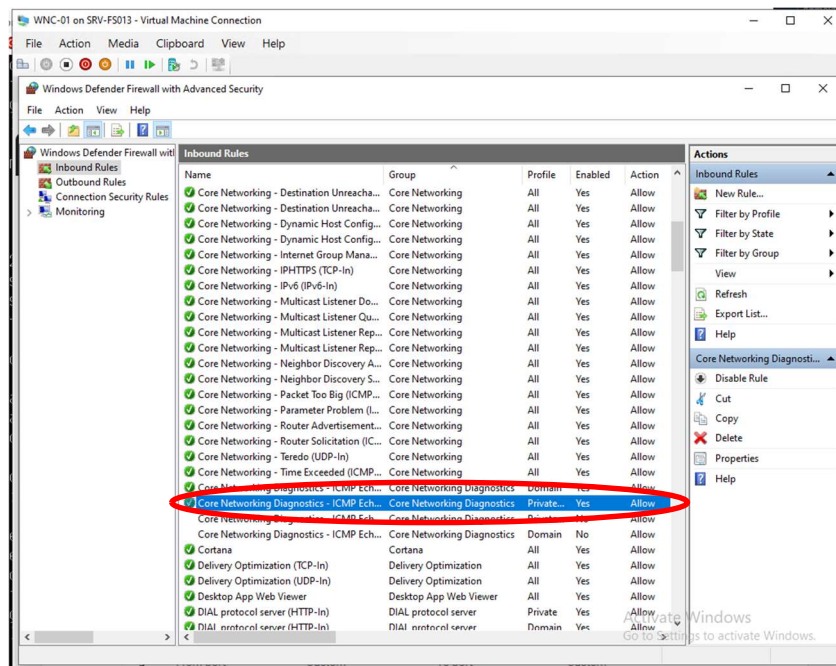


Abbildung 11: Einstellungen Firewall WNC-01
Im Windows Client anpingen ermöglichen.

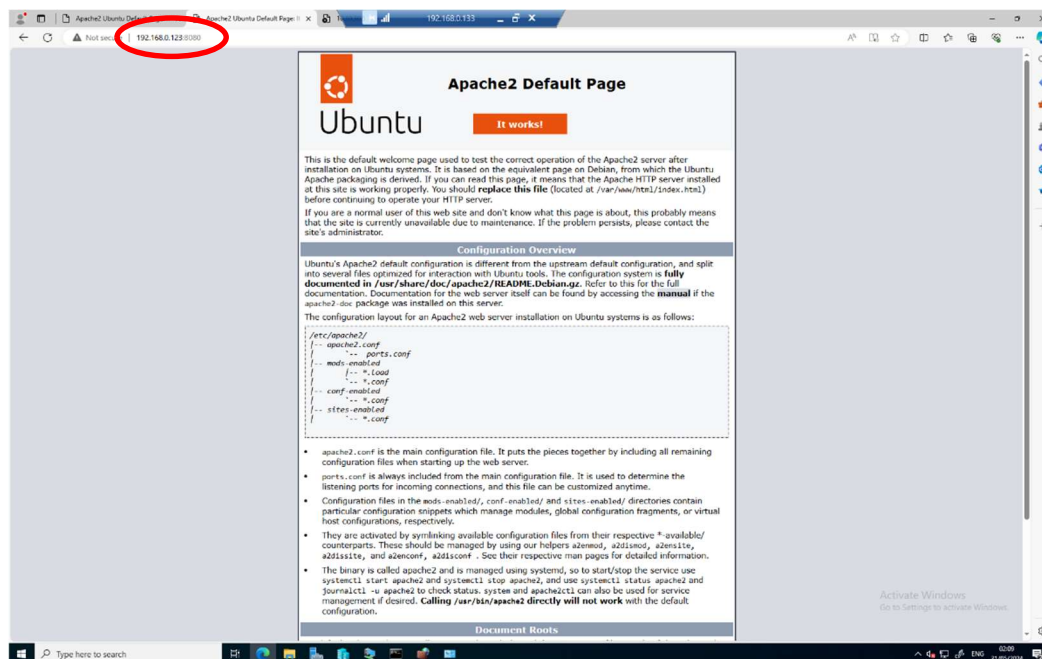


Abbildung 12: Default Apache page von Workstation

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

8 Testing

8.1 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 Webserver, 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 Webserver 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	Anfangen 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

Netzwerk mit Firewall einrichten

ID	T03
Testfall	Zugang vom Webserver auf LAN überprüfen
Host	Workstation
Beschreibung	Der Webserver 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 zurück erhält, 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

8.2 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