

TH Brandenburg
Online Studiengang IT Sicherheit
Fachbereich Informatik und Medien
Netzwerksicherheit
Prof. Dr. Michael Pilgermann

Zusatz-Einsendeaufgabe 1

Wintersemester 2023

10. Dezember 2023

Gruppe 11
Mathias Baumbach (Matr-Nr. 20213703)
Mara Schulke (Matr-Nr. 20215853)

Zusammenfassung

Inhaltsverzeichnis

1	Introduction	2
2	Preparation	3
2.1	Connect to lab (VNL) and initialize systems	3
2.2	Check communication between components	3
2.3	Access your group firewall	4
3	Execution	4
3.1	Part 1: Effective firewall rules	4
3.1.1	Implement white listing for outgoing traffic	5
3.1.2	Allow for http/https traffic	5
3.1.3	Which additional traffic is required?	6
3.1.4	Secure admin access	8
3.2	Part 2: Analyze firewall audit trail	9
4	References / Documentation	10

Abbildungsverzeichnis

1	Netztopologie	2
2	Dokumentierte Netztopologie mit IP-Adressen	4
3	Lan VLAN Default Rule	5
4	Server_LAN VLAN Default Rule	5
5	Fehlgeschlagener Aufruf des Webservers via IP-Adresse	6
6	Erfolgreicher Aufruf des Webservers via IP-Adresse	6
7	Fehlgeschlagener Aufruf eines Webservers via URL	7
8	Erfolgreicher Aufruf eines Webservers via URL	7
9	SSH Verbindung vom Admin-Client zum Server	8
10	SSH Verbindung vom User-Client zum Server	8
11	SSH Verbindung vom Admin-Client zum Server mit SSH Regel	9
12	SSH Verbindung vom User-Client zum Server mit SSH Regel	9
13	Erfolgreiche SSH Verbindung vom Admin-Client	10
14	Erfolglose SSH Verbindung vom User-Client	10

1 Introduction

Firewalls are one of the basic, yet very effective security controls in network security. Packet filters is the entry level firewall technology.

The experiment shall secure a topology with three network segments, which are each connected to a unique port at a firewall:

- Client-LAN: Client network (1 admin client, 1 user client; both Ubuntu Linux)
- Server-LAN: Server network (1 server acting as web server; Ubuntu Server)
- WAN: External network

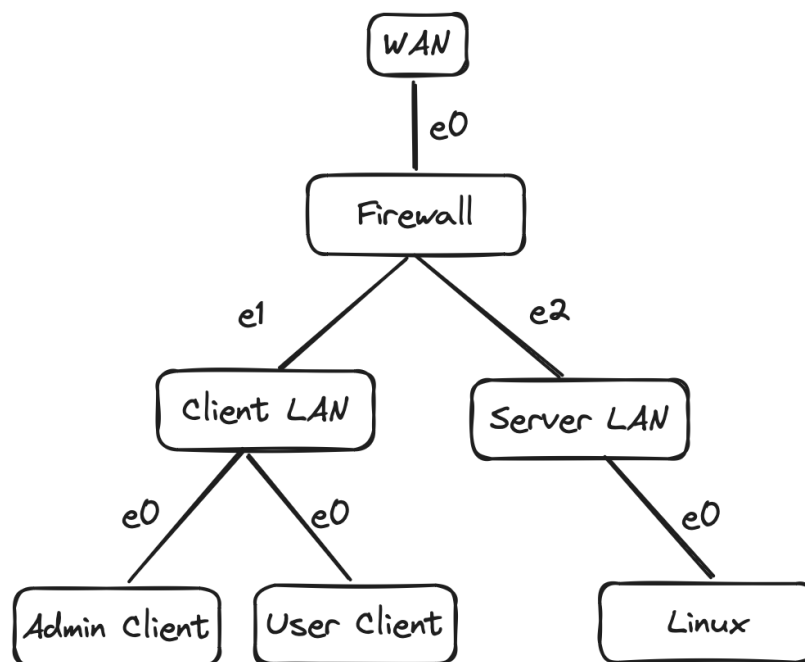


Abbildung 1: Netztopologie

The topology with the firewall (pfSense), three Ubuntu boxes (2 clients and one server) and the external connection has been prepared in the virtual lab environment already. However, the ruleset of the firewall is empty; the exercise is about developing a ruleset based on the “white listing” paradigm, implementing it on the firewall and checking connectivity.

The following communication shall be allowed (including corresponding reply traffic):

- All endpoints (server as well as clients) shall connect to the external net for HTTP / HTTPS traffic on the corresponding ports.
- The admin client shall connect to the server via SSH.

2 Preparation

2.1 Connect to lab (VNL) and initialize systems

Connect to the Virtual Network Security Lab (VNL) of THB using your web browser as documented (incl. group credentials).

Navigate to shared space in VNL and create a copy of the lab `Shared/Netzwerksicherheit/2023_exercise_firewalls.unl`

and place the copy in your user folder. Boot up the systems in your lab – make sure, to always start with the pfSense-Firewall, as this one acts as DHCP-Server for the clients and the server. When booting the systems for the first time, some initial configuration has to be applied – check **appendix 1 – startup configurations** at the end of this document for details.

2.2 Check communication between components

Open up the user interface for each component (command line for servers, remote desktop for clients) inside your web browser; login using the eve-ng default credentials.

Check connectivity internally (web server via IP) and to the outside world (e.g. web browser on GUI environments or wget on command line). Document your network topology in a corresponding plan including the IP addresses.

Antwort

Zur Dokumentation der Netztopologie haben wir unsere grafische Darstellung der Netzwerktopologie um die IP Adressen erweitert:

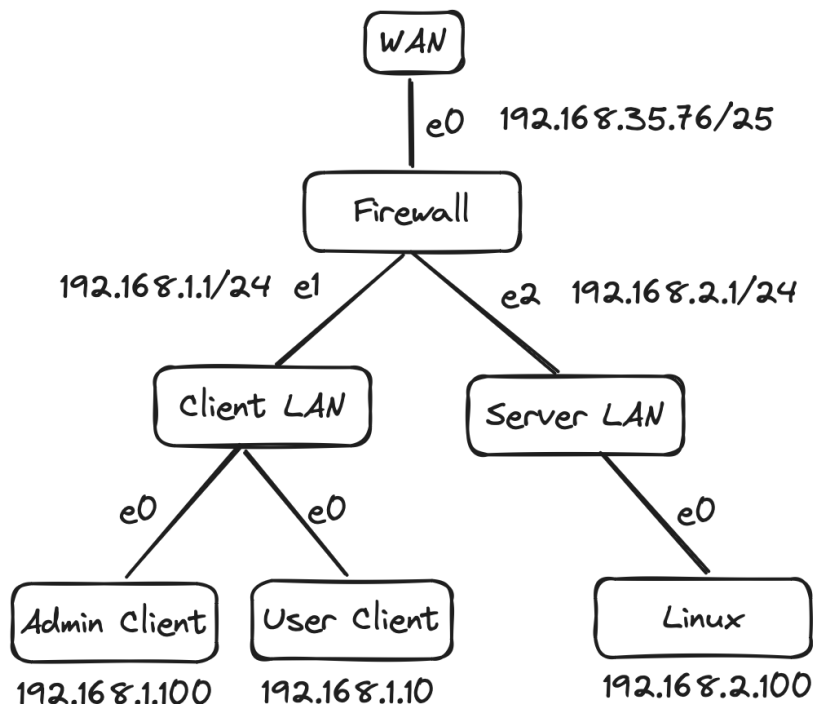


Abbildung 2: Dokumentierte Netztopologie mit IP-Adressen

2.3 Access your group firewall

Using the remote desktop of the admin client, open firewall web gui in the web browser. Get a very first impression of the ruleset and familiarize yourself with the handling.

3 Execution

Having tested, that the lab environment works fine including all communication, next action is to step-by-step restrict the firewall ruleset.

3.1 Part 1: Effective firewall rules

Prepare a table for documentation of your firewall policy. Include at least: Type (14), source IP, source port, destination IP, destination port, action. This policy / documentation shall always be updated before applying changes to the firewall ruleset.

Antwort

Unsere Tabelle der pfSense Firewall Policies ist bereits mit einigen Standard-Regeln, die pfSense initial anlegt, gefüllt:

VLAN	Type (I4)	Source IP	Source Port	Destination IP	Destination Port	Action	Beschreibung
LAN	Any	Any	Any	LAN Address	443 & 80	allow	Anti-Lockout Rule
LAN	Any	EasyRuleBlock HostVLAN	Any	Any	Any	block	Durch initiale Configuration angelegt
LAN	IPv4/IPv6	LAN	Any	Any	Any	allow	Default allow LAN to any rule
SERVER_LAN	IPv4/IPv6	SERVER_LAN	Any	Any	Any	allow	Default allow SERVER_LAN to any rule

3.1.1 Implement white listing for outgoing traffic

The default behavior of the firewall for outgoing traffic (“black listing”) shall be inversed. This is achieved by changing the default rule. The default rule of a ruleset will always apply, if no other rule matched the traffic before. The configuration needs to be applied to the 2 LAN interfaces.

Antwort

Die default deny Regeln im pfSense Menü:



Abbildung 3: Lan VLAN Default Rule

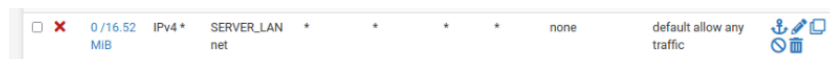


Abbildung 4: Server_LAN VLAN Default Rule

Unsere Tabelle der pfSense Firewall Policies mit den veränderten default Regeln:

VLAN	Type (I4)	Source IP	Source Port	Destination IP	Destination Port	Action	Beschreibung
LAN	Any	Any	Any	LAN Address	443 & 80	allow	Anti-Lockout Rule
LAN	Any	EasyRuleBlock HostVLAN	Any	Any	Any	block	Durch initiale Konfiguration angelegt
LAN	IPv4/IPv6	LAN	Any	Any	Any	deny	Default deny LAN to any rule
SERVER_LAN	IPv4/IPv6	SERVER_LAN	Any	Any	Any	deny	Default deny SERVER_LAN to any rule

3.1.2 Allow for http/https traffic

Add additional rules for allowing http/https traffic from all clients / servers. Which ports are required? TCP or UDP? Adopt your firewall policy before applying changes to the firewall.

Test your firewall configuration by web browsing from within your ubuntu client.

Antwort

Bevor man den Datenverkehr auf Port 80 & 443 erlaubt für http/https, erhält man die folgende Meldung beim Aufruf unseres Webserver:

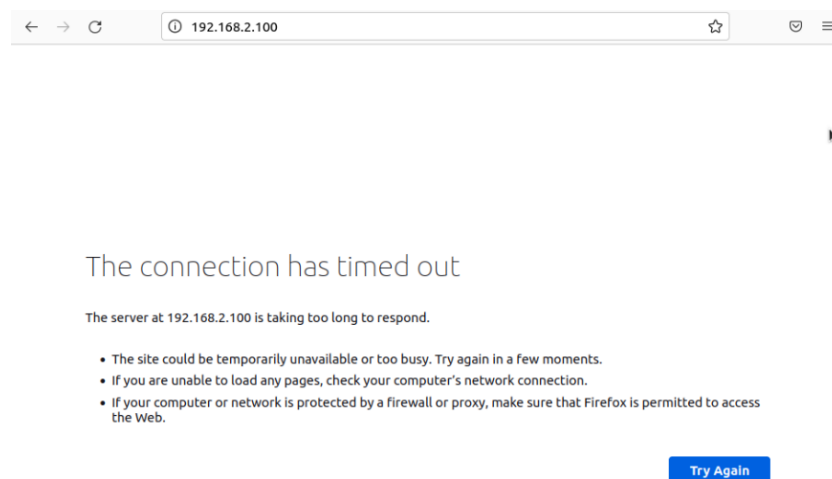


Abbildung 5: Fehlgeschlagener Aufruf des Webservers via IP-Adresse

Um diese Fehlermeldung zu umgehen sind folgende zusätzliche Firewall Regeln nötig:

VLAN	Type (I4)	Source IP	Source Port	Destination IP	Destination Port	Action
LAN	TCP	LAN net VLAN	Any	Any	80 (http)	allow
LAN	TCP	LAN net VLAN	Any	Any	443 (https)	allow
SERVER_LAN	TCP	SERVER_LAN net VLAN	Any	Any	80 (http)	allow
SERVER_LAN	TCP	SERVER_LAN net VLAN	Any	Any	443 (https)	allow

Nun kann bei erneutem Aufruf der IP unseres Webservers erfolgreich die Webseite abgerufen werden:

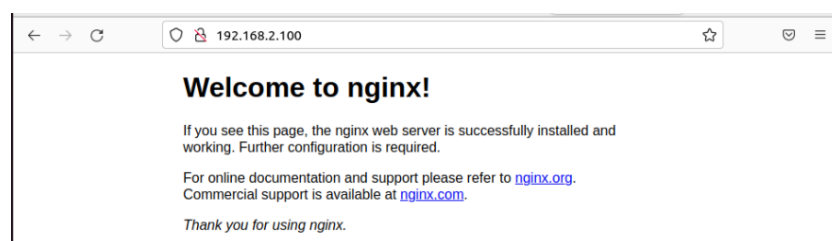


Abbildung 6: Erfolgreicher Aufruf des Webservers via IP-Adresse

3.1.3 Which additional traffic is required?

You should experience issues when browsing the web.

Discuss: Which additional traffic is required? Which changes need to be applied to your firewall policy? Adopt and test again.

Antwort

Unser Webserver war in der vorherigen Aufgabe erreichbar, weil der Aufruf per IP- Adresse erfolgte. Für Zugriff auf Webseiten im Internet ist die Anfrage an einen DNS Server nötig, der die URL in eine IP Adresse für den Browser übersetzt.

Da wir bisher keine Regel für DNS Traffic angelegt haben, schlägt ein Aufruf einer URL fehl:

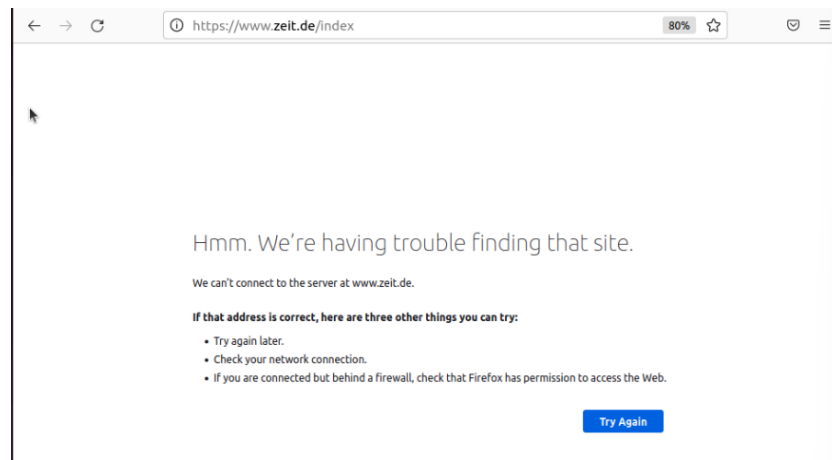


Abbildung 7: Fehlgeschlagener Aufruf eines Webservers via URL

Es sind folgende zusätzliche Firewall Regeln nötig:

VLAN	Type (I4)	Source IP	Source Port	Destination IP	Destination Port	Action
LAN	TCP/UDP	LAN net VLAN	Any	Any	53 (dns)	allow
SERVER_LAN	TCP/UDP	LAN net VLAN	Any	Any	53 (dns)	allow

Dadurch können nun Webseiten-Aufrufe im Internet erfolgreich übersetzt werden:



Abbildung 8: Erfolgreicher Aufruf eines Webservers via URL

Darüber hinaus gäbe es noch weitere Ports, deren Freigabe nützlich wäre. Beispiel wären WebRTC (Port-Range 48k bis 65k?) oder IMAP (143).

3.1.4 Secure admin access

SSH access to the server should be restricted to the admin client; all other traffic between those two networks shall be prohibited.

- Add a rule for allowing access to the webserver (HTTP / HTTPS) from any endpoint in the client LAN.
- Add a rule for allowing admin access to the webserver (SSH) from the admin client.

Test the communication.

Antwort

Die default deny Regel verhindert den SSH Zugang vom Admin- und vom User-Client zum Server:

```
user@ubuntu22-desktop:~$ ssh 192.168.2.100
ssh: connect to host 192.168.2.100 port 22: Connection timed out
```

Abbildung 9: SSH Verbindung vom Admin-Client zum Server

```
user@ubuntu22-desktop:~$ ssh 192.168.2.100
ssh: connect to host 192.168.2.100 port 22: Connection timed out
```

Abbildung 10: SSH Verbindung vom User-Client zum Server

Es ist folgende zusätzliche Firewall Regeln nötig:

VLAN	Type (I4)	Source IP	Source Port	Destination IP	Destination Port	Action
LAN	TCP	192.168.1.100	Any	SERVER_LAN net VLAN	22 (SSH)	allow

Nach Aktivierung dieser Regel ist der SSH Zugriff weiterhin für den User-Client geblockt, für den Admin-Client aber möglich:

```

user@ubuntu22-desktop:~$ ssh 192.168.2.100
user@192.168.2.100's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-27-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Sun Nov 26 01:48:04 PM UTC 2023

System load:  0.0               Processes:           103
Usage of /:   38.8% of 18.53GB   Users logged in:    1
Memory usage: 9%               IPv4 address for ens3: 192.168.2.100
Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

13 updates can be applied immediately.
11 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

*** System restart required ***
Last login: Sun Nov 26 13:42:06 2023 from 192.168.2.100
user@ubuntu22-server:~$

```

Abbildung 11: SSH Verbindung vom Admin-Client zum Server mit SSH Regel

```

user@ubuntu22-desktop:~$ ssh 192.168.2.100
ssh: connect to host 192.168.2.100 port 22: Connection timed out

```

Abbildung 12: SSH Verbindung vom User-Client zum Server mit SSH Regel

3.2 Part 2: Analyze firewall audit trail

Apply changes to your firewall ruleset, so that events are being logged whenever anybody accesses the server on port 22 (no matter whether it is successful or not).

Trigger those firewall rules by starting SSH connection to the server from

- 1) the admin client and
- 2) the “normal” client.

Observe the events in the audit trail on the firewall.

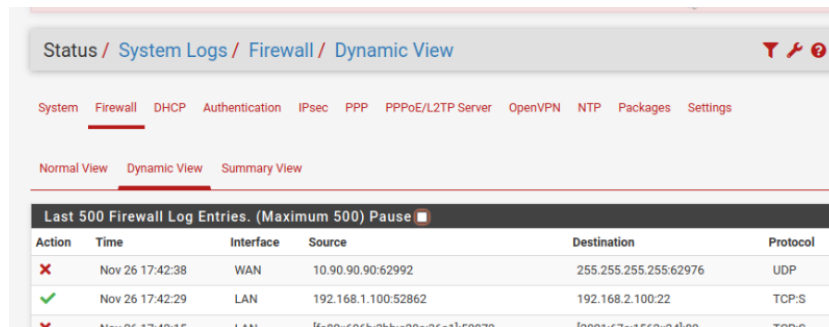
Antwort

Für diese Aufgabe müssen zwei Regeln aus den vorherigen Aufgaben erweitert werden:

VLAN	Type (I4)	Source IP	Source Port	Destination IP	Destination Port	Action
LAN	TCP	192.168.1.100	Any	SERVER_LAN net VLAN	22 (SSH)	allow
LAN	IPv4/IPv6	LAN net VLAN	Any	Any	Any	deny

An beiden Regeln muss die Extra Option "Log packets that are handled by this rule" angehakt werden.

Danach kann in den System Logs der pfSense (Status / System Logs / Firewall / Dynamic View) der erfolgreiche und erfolglose ssh Verbindungsversuch verfolgt werden:

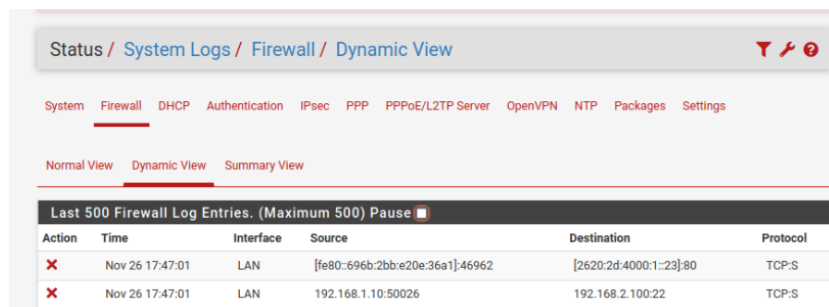


The screenshot shows the pfSense Firewall Log Dynamic View. The breadcrumb trail is Status / System Logs / Firewall / Dynamic View. The 'Dynamic View' tab is selected. The table title is 'Last 500 Firewall Log Entries. (Maximum 500) Pause'. The table has columns: Action, Time, Interface, Source, Destination, and Protocol. The second row shows a successful connection (green checkmark) on Nov 26 17:42:29 from LAN interface, source 192.168.1.100:52862, to destination 192.168.2.100:22 using TCP:S protocol.

Action	Time	Interface	Source	Destination	Protocol
✗	Nov 26 17:42:38	WAN	10.90.90.90:62992	255.255.255.255:62976	UDP
✓	Nov 26 17:42:29	LAN	192.168.1.100:52862	192.168.2.100:22	TCP:S
✗	Nov 26 17:42:15	LAN	192.168.1.100:50026	192.168.2.100:22	TCP:S

Abbildung 13: Erfolgreiche SSH Verbindung vom Admin-Client

In der 2. Zeile (grüner Haken) kann man den erfolgreichen Zugriff von 192.168.1.100 Port 52862 auf 192.168.2.100 Port 22 beobachten.



The screenshot shows the pfSense Firewall Log Dynamic View. The breadcrumb trail is Status / System Logs / Firewall / Dynamic View. The 'Dynamic View' tab is selected. The table title is 'Last 500 Firewall Log Entries. (Maximum 500) Pause'. The table has columns: Action, Time, Interface, Source, Destination, and Protocol. The second row shows a failed connection (red X) on Nov 26 17:47:01 from LAN interface, source 192.168.1.10:50026, to destination 192.168.2.100:22 using TCP:S protocol.

Action	Time	Interface	Source	Destination	Protocol
✗	Nov 26 17:47:01	LAN	[fe80::696b:2bbe:20e:36a1]:46962	[2620:2d:4000:1::23]:80	TCP:S
✗	Nov 26 17:47:01	LAN	192.168.1.10:50026	192.168.2.100:22	TCP:S

Abbildung 14: Erfolgreiche SSH Verbindung vom User-Client

Ebenfalls in der 2. Zeile ist der fehlgeschlagene Zugriff von 192.168.1.10 Port 50026 auf 192.168.2.100 Port 22 dokumentiert.

4 References / Documentation

- 1) Eve-ng cookbook: <https://www.eve-ng.net/index.php/documentation/professional-cookbook/>
- 2) pfSense Firewall configuration documentation: <https://docs.netgate.com/pfSense/en/latest/firewall/index.html>