

Praktikum Nr.4 Einsatz und Konfiguration einer Firewall

Versuchsaufbau

Sinn dieses Praktikums ist es, den Einsatz und die Konfiguration einer Firewall kennen zu lernen. Dabei werden Sie selbstständig vorgehen müssen, d.h. Informationen aus dem Internet und Try&Error gehören hier mit zur Aufgabe.

In diesem Praktikum arbeiten Sie mit 3 virtuellen Maschinen.

Prüfen Sie die Konfiguration der VM bevor Sie sie starten.

Es müssen folgende Einstellungen vorhanden sein:

Kali:

System: Prozessor 1, Ram 1024 KB

Netzwerk: Adapter 1: Internes Netzwerk/LAN; keine weiteren Adapter

OPNsense:

System: Prozessor 1, Ram 1024 KB

Netzwerk: Adapter 1: Internes Netzwerk/LAN; Adapter 2: Internes Netzwerk/inet; keine weiteren Adapter

Windows7:

System: Prozessor 1, Ram 2048 KB

Netzwerk: Adapter 1: Internes Netzwerk/inet; keine weiteren Adapter

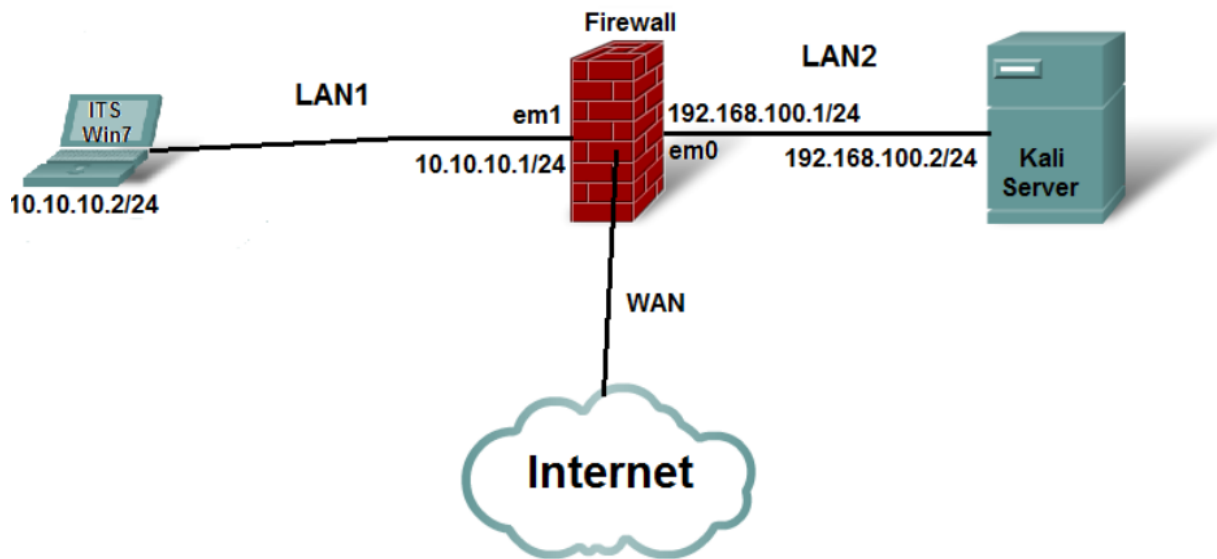
Wenn Sie diese Einstellungen haben und Sie haben nichts verändert können Sie die VMs starten.

Sollte Sie etwas verändern müssen, erzeugen Sie VOR dem Starten einen neuen Sicherungspunkt (Snapshot).

Eine Windows-7 VM (Client-Win7), eine Kali VM (Kali2018-ITS) und eine Linux VM (OPNsense), auf der die Firewall läuft.

Bei der Firewall handelt es sich um eine OPNsense Firewall. Diese FW ist eine Weiterentwicklung der pfSense FW. Daher gelten so gut wie alle Aussagen, die Sie für pfSense finden auch für OPNsense (hilft bei der Internetrecherche).

Der gesamte Aufbau sieht folgendermaßen aus:



Die VMs sind schon vorkonfiguriert, IP Adressen und Schnittstellen laufen schon. Einzig die Internetverbindung der Firewall ist noch nicht vorhanden und wird von Ihnen im Laufe des Praktikums konfiguriert.

Der Server steht in einem LAN, dass einen höheren Sicherheitsanspruch als das Laptop hat. Wenn das Internet dazu kommt, ist dies das Segment mit dem niedrigsten Sicherheitslevel.

Starten Sie nun nacheinander alle 3 VMs.

ITS Frage 4-1 Schauen Sie sich das VM-Fenster der FW an und ordnen Sie die IP Adressen einem Interface zu.

Interface em0 hat die IP Adresse

Interface em1 hat die IP Adresse

Richtig!

Loggen Sie sich direkt auf der FW mit root/opsense ein und pingen Sie die beiden angeschlossenen Systeme. Sollte eine Verbindung nicht funktionieren, rufen Sie einen Betreuer.

Hinweis: Der Mauszeiger wird von der FW VM gefangen. Wenn Sie ihn wieder verwenden wollen, drücken die die Taste Strg.

Frage ITS 4-2 Funktionieren die Pingverbindungen?

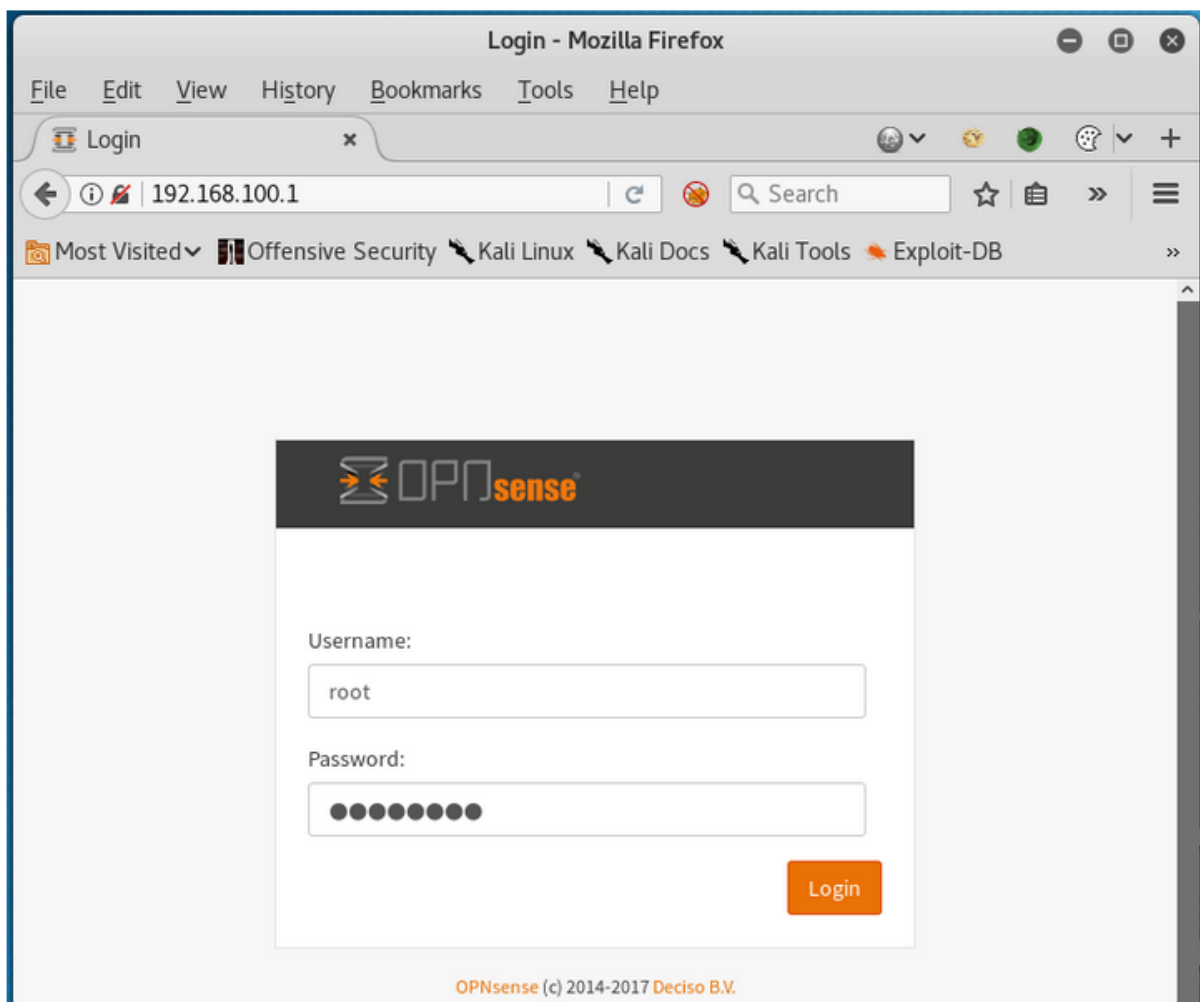
☒ Ja
☐ Nein

Richtig!
OK, machen Sie weiter.

Auswerten

Loggen Sie sich mit **ITS/P@ssw0rd** in die VM **Client-Win7** ein.

Loggen Sie sich mit **root/toor** in die Kali2018 VM ein, öffnen Sie Firefox und verbinden Sie sich mit der FW-IP. Loggen Sie sich auf der graphischen Oberfläche in die FW mit **root/opnsense** ein

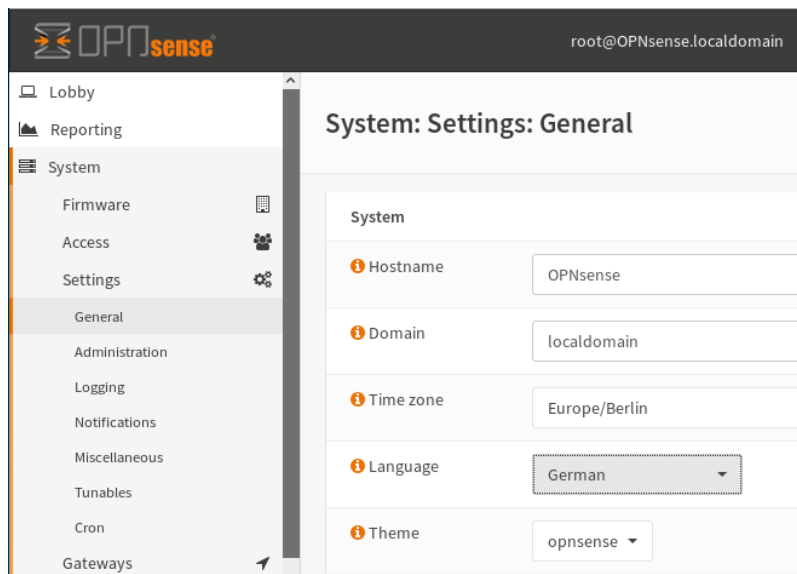


Machen Sie sich mit der graphischen Oberfläche der FW vertraut.

Ein gute Hilfe bietet <https://wiki.opnsense.org/>

Ändern Sie unter **System:Settings:General** die Zeitzone auf *Europe/Berlin* und die FW-

Anzeigesprache auf *Deutsch*.



Schauen Sie sich die Menüpunkte der FW an (gehen Sie einmal alle durch), und genauer die folgende Menüpunkte:

- Firewall:Regeln

Schauen Sie sich folgende Webseite an:


[doc.pfsense.org/index.php/Firewall Rule Processing Order](http://doc.pfsense.org/index.php/Firewall_Rule_Processing_Order)

Frage ITS 4-3 Welche Schnittstellen-Tabulatoren sind vorhanden (oben)?

☒ LAN
☐ EM1
☐ EM0
☒ WAN
☐ INET
☒ Floating

Richtig!
Stimmt, arbeiten Sie weiter.

Auswerten

Frage ITS 4-4 

Regeln einer Schnittstelle werden immer von oben nach unten verarbeitet

Benutzererstellte Regeln (Floating, Gruppe und Schnittstelle) werden in welcher Reihenfolge verarbeitet?

Floating Regeln

Regeln für eine Schnittstelle

Gruppenregeln

Richtig!

- Firewall:Diagnose:Status zurücksetzen

- Aliasse

Schauen Sie sich an, wie man Aliasse anlegt.

Was sind Aliasse?

Was kann man mit Aliassen machen?

- System:Konfiguration:Verlauf

Was können Sie hier sehen?

- Schnittstellen: [LAN] und [WAN]

Was kann hier eingetragen werden?

Wozu kann der Eintrag MAC-Adresse verwendet werden?

Wozu brauchen Sie den Eintrag IPv4 Upstream Gateway?

- Firewall:Protokolldateien

Schauen Sie all Unterpunkte an.

- Schnittstellen:Diagnose

Schauen Sie sich alle Unterpunkte an und probieren Sie die letzten 3 (Ping / Porttest /

Routenverfolgen selber praktisch aus.

- System:Routen und System:Gateway

Genau anschauen...

Sie sollten die Schnittstellen:Diagnose verwenden können.

Veranschlagen Sie ca. 20 Minuten für diese Aufgaben.

Aliasse

Legen sie Aliasse für folgende IP-Adressen an:

Windows7 - 10.10.10.2

Kali- 192.168.100.2

Google Public DNS - 8.8.8.8, 8.8.4.4

Firewall: Aliases: View

Add a new alias

| Name | Type | Description | Values |
|--|------|-------------|--------|
| Aliases act as placeholders for real hosts, networks or ports. They can be used to minimize the number of changes that have to be made if a host, network or port changes. You can enter the name of an alias instead of the host, network or port in all fields that have a red background. The alias will be resolved according to the list above. If an alias cannot be resolved (e.g. because you deleted it), the corresponding element (e.g. filter/NAT/shaper rule) will be considered invalid and skipped. | | | |

Firewall: Aliases: View

Alias Edit

Type: Host(s)

Name: Windows7

Description: WAN-Rechner

| Aliases | Host(s) | Description |
|---------|------------|-------------|
| - | 10.10.10.2 | |
| + | | |

Save Cancel

Firewall: Aliases: View

Add a new alias

The alias list has been changed.
You must apply the changes in order for them to take effect.

Apply changes



| Name | Type | Description | Values |
|----------|---------|-------------|------------|
| Windows7 | Host(s) | WAN-Rechner | 10.10.10.2 |

Aliases act as placeholders for real hosts, networks or ports. They can be used to minimize the number of changes that have to be made if a host, network or port changes. You can enter the name of an alias instead of the host, network or port in all fields that have a red background. The alias will be resolved according to the list above. If an alias cannot be resolved (e.g. because you deleted it), the corresponding element (e.g. filter/NAT/shaper rule) will be considered invalid and skipped.

Firewall: Aliases: View



The changes have been applied successfully.

| Name | Type | Description | Values |
|----------|---------|-------------|---|
| Windows7 | Host(s) | WAN-Rechner | 10.10.10.2   |

Aliases act as placeholders for real hosts, networks or ports. They can be used to minimize the number of changes that have to be made if a host, network or port changes. You can enter the name of an alias instead of the host, network or port in all fields that have a red background. The alias will be resolved according to the list above. If an alias cannot be resolved (e.g. because you deleted it), the corresponding element (e.g. filter/NAT/shaper rule) will be considered invalid and skipped.

Firewall: Aliases: View



Alias Edit

Type Host(s)

Name Kali

Description

Aliases

| Host(s) | Description |
|---|-------------|
|  192.168.100.2 | |
|  | |

Save **Cancel**

Firewall: Aliases: View




Alias Edit

Type Host(s)

Name OPNsense

Description

Aliases

| Host(s) | Description |
|---|-------------|
|  10.10.10.1 | |
|  192.168.100.1 | |
|  | |

Save **Cancel**

Firewall: Aliases: View

Alias Edit

Type: Host(s)

Name: Google_Public_DNS

Description:

Aliases:

| Host(s) | Description |
|---------|-------------|
| 8.8.8.8 | |
| 8.8.4.4 | |

Das Ergebnis sollte etwa so aussehen.

OPNsense root@OPNsense.localdomain

Firewall: Aliase: Ansicht

Die Änderungen wurden erfolgreich angewandt.

| Name | Typ | Beschreibung | Werte |
|-------------------|---------|-------------------------|---------------------------|
| Client_Win7 | Host(s) | Windows Client im WAN | 10.10.10.2 |
| Google_Public_DNS | Host(s) | Öffentlicher DNS Server | 8.8.8.8, 8.8.4.4 |
| Kali2018 | Host(s) | Kali Linux | 192.168.100.2 |
| OPNsense | Host(s) | Firewall | 10.10.10.1, 192.168.100.1 |

Frage ITS 4-5 Was gilt für Aliasse?




- ☒ Werden eingesetzt um die Anzahl der Änderungen zu minimieren
- ☐ Aliasse können in allen Feldern mit grünem Rand eingesetzt werden
- ☒ Agieren als Platzhalter für Hosts, Netzwerke oder Ports
- ☐ Falls ein Alias gelöscht wird, wird das entsprechende Element weiter als gültig betrachtet

Richtig!

Bearbeiten Ok

Verbindung Windows-FW

Versuchen Sie von der Windows VM über einen Browser auf die grafische Oberfläche der FW zuzugreifen.

Frage ITS 4-6 Funktioniert der Zugriff? 

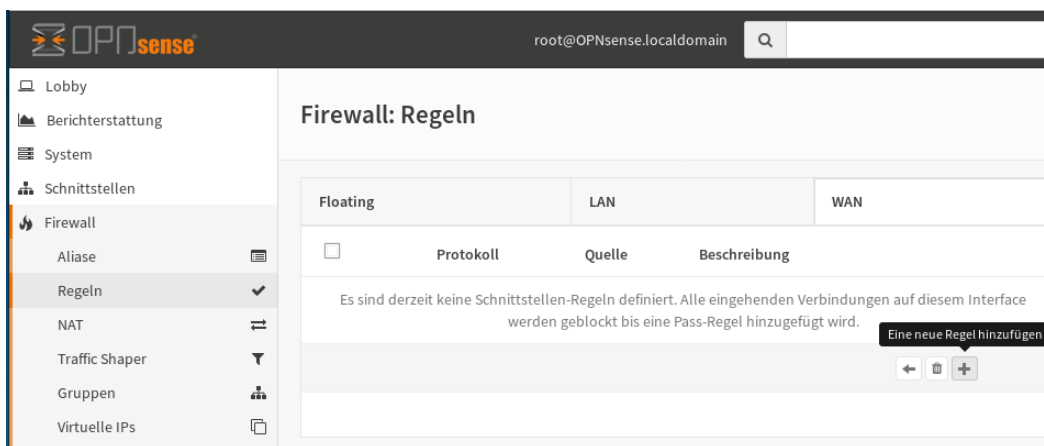
☐ Ja

☒ Nein

Richtig!

Damit die FW aber auch von der Windows VM konfiguriert und gemanaged werden kann, soll der Zugriff nun von Ihnen erlaubt werden.

Erstellen Sie eine Regel, die den Zugriff von der Windows VM auf die Weboberfläche erlaubt. Verwenden Sie eine Regel, die möglichst genau die Forderung abbildet und keine zusätzlichen Daten durchlässt.



Firewall: Regeln

Firewallregel bearbeiten

vollständige Hilfe

| | |
|------------------------------|---|
| Aktion | Erlauben |
| Deaktiviert | <input type="checkbox"/> Diese Regel deaktivieren |
| Schnittstelle | WAN |
| TCP/IP Version | IPv4 |
| Protokoll | TCP |
| Quelle / Umkehren | <input type="checkbox"/> |
| Quelle | jeglich |
| Quelle | Erweitert |
| Ziel / Umkehren | <input type="checkbox"/> |
| Ziel | OPNsense |
| Zielportbereich | von: HTTP an: HTTP |
| Protokoll | <input type="checkbox"/> Protokolliere Pakete die von dieser Regel behandelt werden |
| Kategorie | |
| Beschreibung | |
| Erweiterte Funktionen | |
| Quellbetriebssystem | Jedes |
| Keine XMLRPC Synchronisation | <input type="checkbox"/> |
| Zeitplan | keiner |
| Gateway | standard |
| Erweiterte Optionen | Zeigen/Verstecken |









Speichern

Abbrechen

Firewall: Regeln

Die Firewall Regel Konfiguration wurde geändert.
Sie müssen die Änderungen bestätigen damit sie wirksam werden.

Änderungen übernehmen

| Floating | | LAN | | WAN |
|--------------------------|--|--------|---|-----|
| <input type="checkbox"/> | Protokoll | Quelle | Beschreibung | |
| <input type="checkbox"/> |  IPv4 TCP | * |     | |
| | | |    | |
| | | | | |

Frage ITS 4-7 Öffnen Sie die Seite **Firewall:Regeln**.



Welchen Interface-Tabulator verwenden Sie?

Welche Einstellungen geben Sie den folgenden Daten?

Aktion:

Deaktiviert:

Schnittstelle:

IP Version:

Protokoll:

Quelle:

Quellportbereich:

Ziel:

Zielbereich: von an

Richtig!

Damit die Regel gültig wird, müssen Sie sie speichern und dann die **Änderungen übernehmen**.

Testen Sie nun, ob Sie von der Windows VM auf die FW über den Brower zugreifen können.

Frage ITS 4-8 Können Sie von der Windows VM die grafische Oberfläche der Firewall öffnen?

- ☒ Ja
☐ Nein

Richtig!

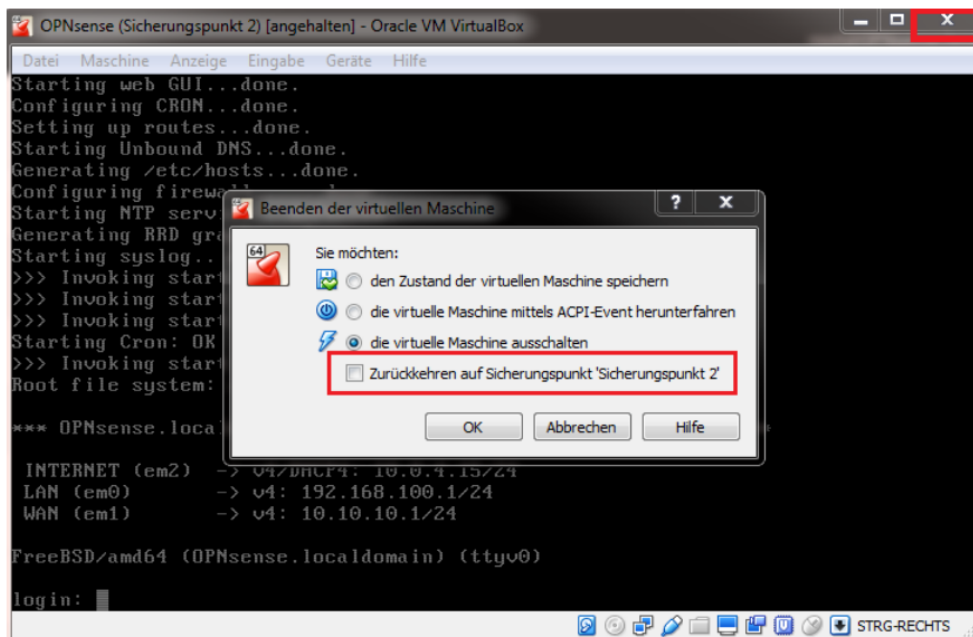
Prima, arbeiten Sie weiter.

Anlegen eines Netzwerkinterfaces

Legen Sie ein neues Interface für die Firewall an, das Internetzugang hat und die VM Client_Win7 mit dem Internet verbindet. Diese Schnittstelle soll dann auch Default Gateway der FW sein.

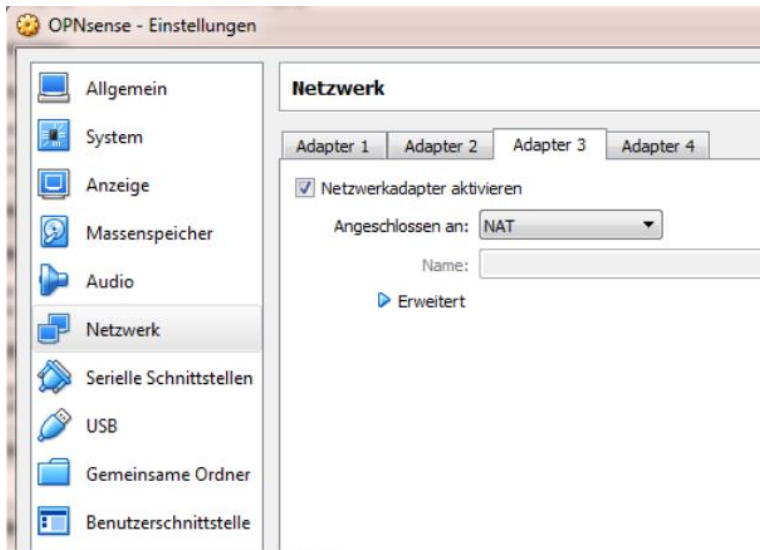
Dazu muss die Firewall heruntergefahren, und in Virtualbox ein neues Netzwerkinterface (NAT) angelegt werden.

Klicken Sie beim OPNsense VM Fenster rechts oben auf das x. Achten Sie darauf, dass der Hacken bei Zurückkehren auf Sicherungspunkt NICHT gesetzt ist (sonst verlieren Sie alle bisherigen Einstellungen (Alias, Zeitzone...))



Wählen Sie links die VM OPNsense aus und klicken Sie oben auf **Ändern**.

Es öffnet sich ein neues Fenster. Hier können Sie den neuen Adapter konfigurieren.

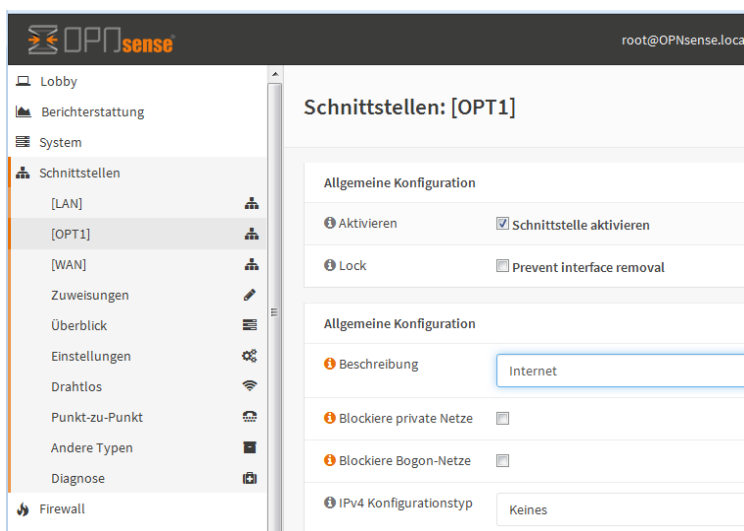
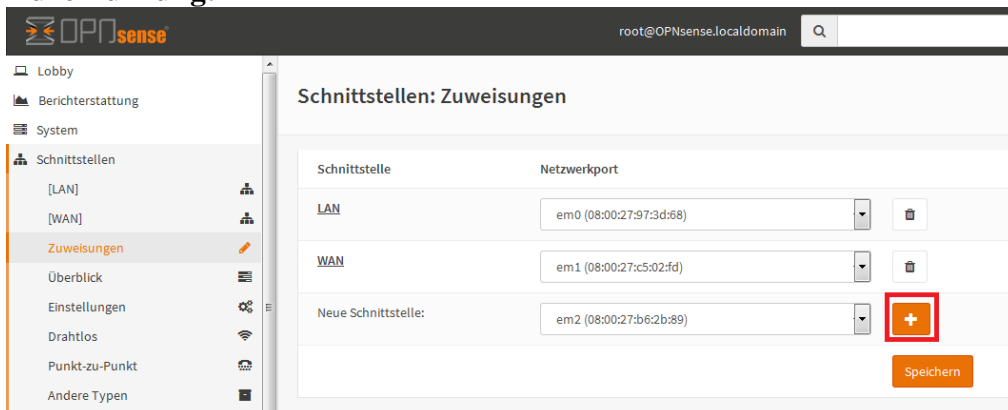


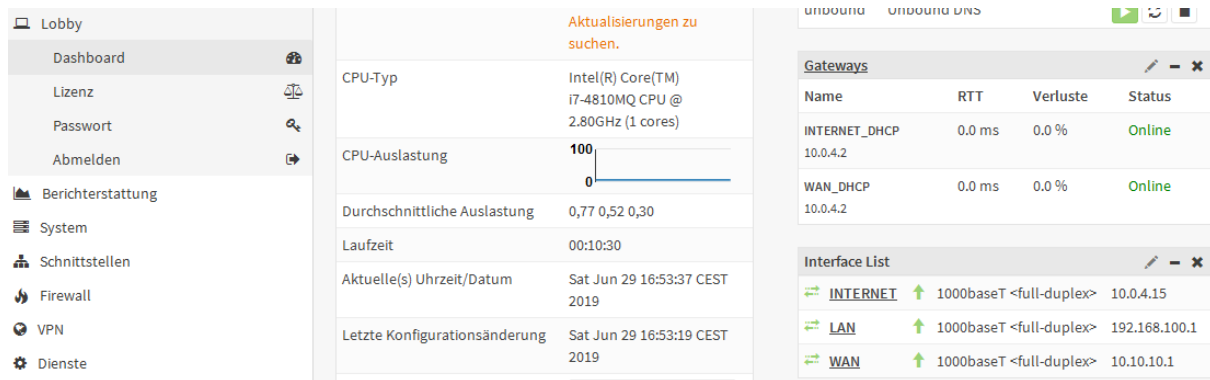
Starten Sie die VM dann wieder.

Dieses neue Interface muss danach auch in OPNsense angelegt werden (Name Internet).

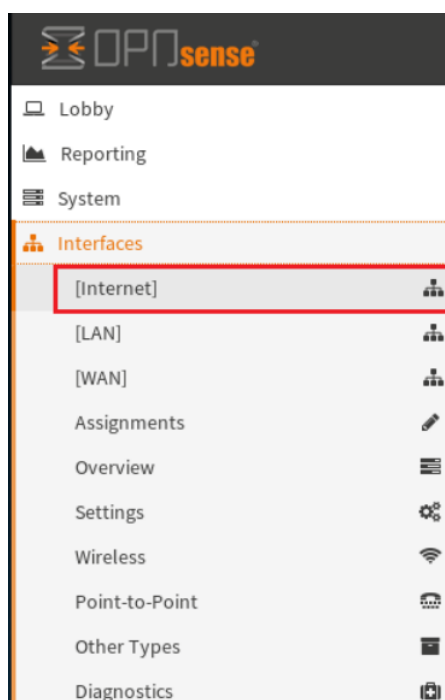
Hinweis: Als NAT-Interface erhält es seine IP Adresse über DHCP!

Durchführung:





So sieht es dann aus.



Im Dashboard können Sie sehen, dass das neue Interface aktiv ist (grüner Status) und welche IP Adresse es erhalten hat.

Lobby: Dashboard

System Information

| | |
|--------------------------------|--|
| Name | OPNsense.localdomain |
| Versionen | OPNsense 17.7.11-amd64 FreeBSD 11.0-RELEASE-p17 LibreSSL 2.5.5 |
| Aktualisierungen | Klicke um nach Aktualisierungen zu suchen. |
| CPU-Typ | Intel(R) Core(TM) i7-4810MQ CPU @ 2.80GHz (2 cores) |
| CPU-Auslastung | 100 |
| Durchschnittliche Auslastung | 0,35 0,26 0,18 |
| Laufzeit | 00:12:22 |
| Aktuelle(s) Uhrzeit/Datum | Fri Jan 19 5:03:13 CET 2018 |
| Letzte Konfigurationsänderung | Fri Jan 19 6:02:33 CET 2018 |
| Verbindungsstatustabellengröße | 0 % (220/98000) |
| MBUF Auslastung | 2 % (1526/61580) |
| Speicherauslastung | 16 % (163/988 MB) |

Dienste

| Dienst | Beschreibung | Status |
|---------|----------------------------|--------|
| configd | Systemkonfigurationsdienst | ▶ |
| ntpd | Netzwerk-Zeit-Daemon | ■▶ |
| pf | Paketfilter | ▶ |
| unbound | Unbound DNS | ▶ |

Gateways

| Name | RTT | Verluste | Status |
|---------------------------|--------|----------|--------|
| INTERNET_DHCP 10.0.4.2 | 0.0 ms | 0.0 % | Online |
| WAN_DHCP 10.0.4.2 | 0.0 ms | 0.0 % | Online |

Interface List

| Interface | Speed | Link | IP Address |
|-----------|-------------------------|------|---------------|
| INTERNET | 1000baseT <full-duplex> | ↑ | 10.0.4.15 |
| LAN | 1000baseT <full-duplex> | ↑ | 192.168.100.1 |
| WAN | 1000baseT <full-duplex> | ↑ | 10.10.10.1 |

Frage ITS 4-9 Ist Ihr Interface aktiv und hat es eine IP Adresse erhalten?

- ☒ Ja
☐ Nein

Richtig!

OK, dann arbeiten Sie weiter.

```

root@OPNsense:~ # ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=57 time=18.518 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=57 time=15.813 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=57 time=15.198 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=57 time=57.886 ms
  
```

... oder ...

Schnittstellen: Diagnose: Ping

Ping

Host: 8.8.8.8


IP Protokoll: IPv4

Quelladresse: INTERNET

Anzahl: 3

Ping

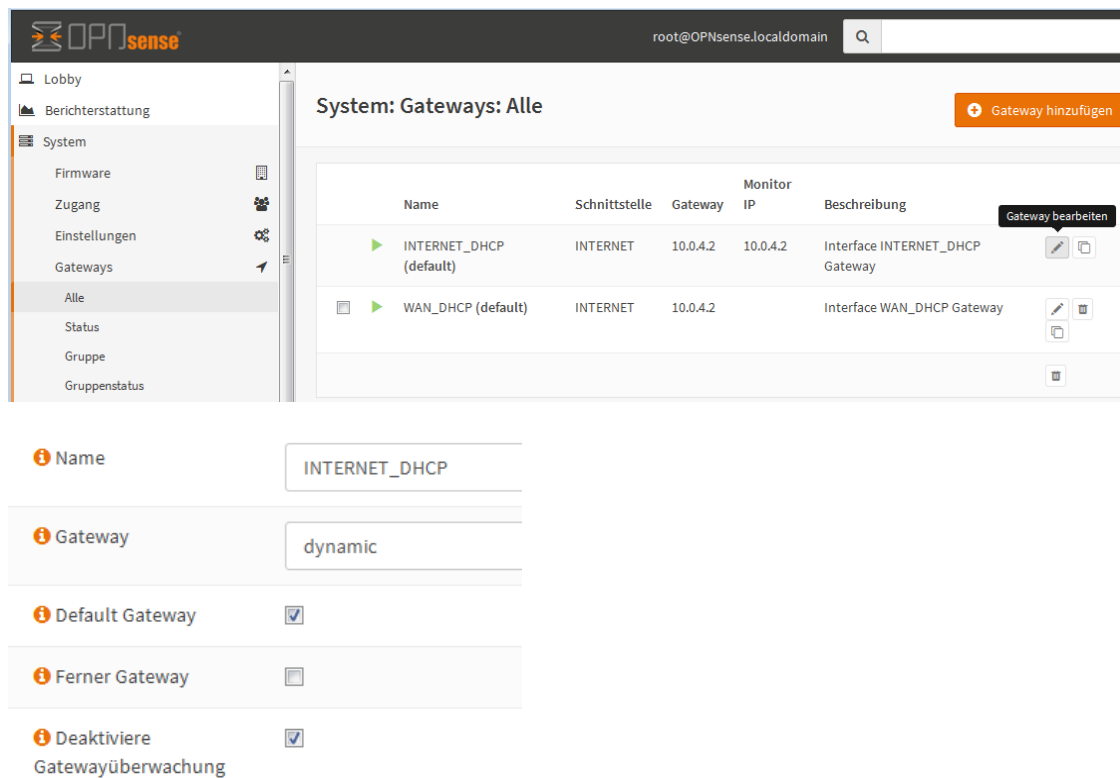
Testen Sie beide Arten aus!

Frage 4-10 Funktioniert der Ping von der FW zum Google DNS Server? 

☒ Ja
☐ Nein

Richtig!
Super, weiter so.

Im Anschluss muss dieses Interface noch als Default Gateway der FW gesetzt werden, damit auch Client_Win7 Internetzugang erhalten kann.



System: Gateways: Alle

Gateway hinzufügen

| Name | Schnittstelle | Gateway | Monitor IP | Beschreibung |
|-------------------------|---------------|----------|------------|---------------------------------|
| INTERNET_DHCP (default) | INTERNET | 10.0.4.2 | 10.0.4.2 | Interface INTERNET_DHCP Gateway |
| WAN_DHCP (default) | INTERNET | 10.0.4.2 | | Interface WAN_DHCP Gateway |

Gateway bearbeiten

Name: INTERNET_DHCP

Gateway: dynamic

Default Gateway: ☒

Ferner Gateway: ☐

Deaktiviere Gatewayüberwachung: ☒

Außerdem muss eine Firewall-Regeln angelegt werden, um der Windows VM den Internetzugang zu gewähren. (Die Regel soll erst einmal alle Protokolle und alle Ports erlauben, any/any).

Firewall: Regeln

Firewallregel bearbeiten

| | |
|----------------|---|
| Aktion | Erlauben |
| Deaktiviert | <input type="checkbox"/> Diese Regel deaktivieren |
| Schnell | <input checked="" type="checkbox"/> Wende die Aktion sofort bei einem Treffer an. |
| Schnittstelle | WAN |
| Richtung | any |
| TCP/IP Version | IPv4 |
| Protokoll | any |

```
C:\Windows\system32\cmd.exe

C:\Users\its>ping 8.8.8.8

Ping wird ausgeführt für 8.8.8.8 mit 32 Bytes Daten:
Antwort von 8.8.8.8: Bytes=32 Zeit=18ms TTL=56
Antwort von 8.8.8.8: Bytes=32 Zeit=15ms TTL=56
Antwort von 8.8.8.8: Bytes=32 Zeit=15ms TTL=56
Antwort von 8.8.8.8: Bytes=32 Zeit=16ms TTL=56

Ping-Statistik für 8.8.8.8:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
    (0% Verlust),
    Ca. Zeitangaben in Millisek.:
        Minimum = 15ms, Maximum = 18ms, Mittelwert = 16ms

C:\Users\its>
```

Frage 4-11 Funktioniert der Ping von der Windows VM zum Google DNS Server?

- ☐ Nein
☒ Ja

Richtig!
OK, weiter so!

☐ Bearbeiten

Wenn die Verbindung von der FW aus funktioniert, rufen Sie von der Windows VM im Browser die Webseite **www.fh-aachen.de** auf.

Installieren Sie nun auf der Windows VM die Programme NMAP ([nmap 6.47.exe](#)) und Netcat ([nmap.org/dist/ncat-portable-5.59BETA1.zip](#)). Auf Kali sind diese Programme schon installiert.

Ping zwischen Kali und Windows

Sie sollen nun ermöglichen, dass Kali und die Windows VM sich gegenseitig pingen können (beide Richtungen).

Erstellen und testen Sie zuerst die Regel Kali -> Windows.

Firewall: Regeln

Firewallregel bearbeiten

Aktion Erlauben

Deaktiviert ☐ Diese Regel deaktivieren

Schnittstelle LAN

TCP/IP Version IPv4

Protokoll ICMP

ICMP Typ jeglich

Quelle / Umkehren ☐

Quelle jeglich

Quelle Erweitert

Firewall: Regeln

The settings have been applied and the rules are now reloading in the background.

| Floating | INTERNET | LAN | WAN |
|------------------------------------|--------------------------|--------------------------|--------------------------|
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Protokoll | Quelle | Beschreibung | |
| <input type="checkbox"/> * | * | Anti-Aussperrregel | |
| <input type="checkbox"/> IPv4 ICMP | * | | |
| | | | |

Wenn das funktioniert erstellen Sie die Regel für die Gegenrichtung Windows->Kali. Testen Sie diese Regel ebenfalls.

Firewall: Regeln

Firewallregel bearbeiten

| | |
|--------------------------|---|
| Aktion | Erlauben |
| Deaktiviert | <input type="checkbox"/> Diese Regel deaktivieren |
| Schnittstelle | WAN |
| TCP/IP Version | IPv4 |
| Protokoll | ICMP |
| ICMP Typ | jeglich |
| Quelle / Umkehren | <input type="checkbox"/> |
| Quelle | jeglich |
| Quelle | Erweitert |

Führen Sie nun eine NMAP-Scans durch.

- Kali scannt OPNsense und Windows
- Windows scannt OPNsense und Kali

Frage ITS 4-12 Welche Ports von *OPNsense* findet die Windows VM offen (WAN Schnittstelle)?

- ☐ keine
☒ 53
☐ 21
☐ 7
☒ 80

Richtig!

Frage ITS 4-13 Welche Ports von *Kali2018* findet die Windows VM offen (WAN Schnittstelle)?

- ☐ 80
☐ 21
☐ 3389
☒ keine
☐ 53

Richtig!

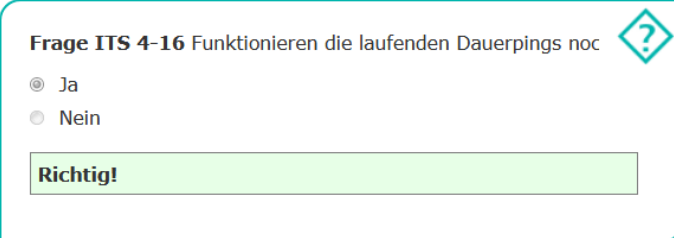
Sicherheit der Firewall erhöhen

Auch eine Firewall kann angegriffen werden. Damit die OPNsense nicht so offensichtlich erkannt und gefunden wird, soll ein Ping auf keinem Interface mehr beantwortet werden, die Firewall wird abgeschottet.

Führen Sie einen Dauerping von Windows und Kali auf die Firewall aus (das sollte funktionieren).

Legen Sie jetzt die notwendigen Regeln in der Firewall an, die (ausschließlich) die ICMP-Requests blocken.

Speichern und übernehmen Sie die FW-Regeln.



Frage ITS 4-16 Funktionieren die laufenden Dauerpings noch?

☒ Ja

☐ Nein

Richtig!

Die FW hat die laufenden Verbindungen gespeichert (Status) und beendet sie nicht wenn eine entsprechende Regel erzeugt wurde. Um die Funktion der Regeln durchzusetzen, muss der Status der FW gelöscht werden.

Das machen Sie im Menü **Firewall:Diagnose:Status** zurücksetzen

Setzen Sie den Status zurück und beobachten Sie die Dauerpings.

Netcat Verbindung


Nun soll mit einfachen Mitteln eine Dateiübertragung von Client_Win7 zu Kali2018 stattfinden. Verwenden Sie dazu Netcat.

Öffnen Sie ein Terminalfenster und geben Sie den Befehl netcat -lvp 6437 ein. Hiermit wird ein lauschender Port, an den ein Sender Daten übertragen kann, erzeugt.

Vom Windows System aus soll nun mit Ncat eine Verbindung zu Kali hergestellt werden. Ziel ist es eine Dateiübertragung zu Kali durchzuführen.

Kopieren Sie eine beliebige Datei.

Es kann auch eine Remote-Konsole von Kali2018 zu Client_Win7 eingerichtet werden (googlen Sie die entsprechenden Parameter von Netcat).

Frage IT 4-17 Hat die Dateiübertragung funktioniert? 

☒ Ja
☐ Nein

Richtig!

Feintuning der Firewall

Mit Blick auf die Sicherheit des Netzes und mit der Best-Practice Guideline: 'Grundsätzlich jeden Verkehr blocken und nur gezielt erlauben' sollen die Firewall-Regeln überarbeitet werden.

Falls Sie nicht wissen, wie Sie eine Aufgabe lösen sollen, recherchieren Sie im Internet und schauen Sie sich die Dokumentation der FW an.

Folgendes soll nachher möglich sein:

- Windows hat Zugriff auf Weboberfläche
- Windows kann Linux pingen
- Windows kann Linux Port 6437/TCP erreichen aber nur von Port 46825 (und maximal 3 Gleichzeitigen Verbindungen.)
- Windows hat Zugriff auf Webserver von Linux
- Windows hat Zugriff auf öffentlichen DNS (8.8.8.8)
- OPNsense kann ICMP Richtung Linux/Windows passieren lassen, aber nur nachts zwischen 1 und 3 Uhr
- OPNsense soll feststellen können, ob der Netcat TCP server auf Kali läuft (Portprobing)
- Kali kann 8.8.8.8 pingen
- Kali kann öffentliche DNS-Server verwenden (Port 53 TCP und UDP)

Folgendes sollte nicht mehr möglich sein (blocken):

- Aufrufen einer Öffentlichen Website aus Windows/Kali
 - Das Aufrufen der OPNsense Oberfläche von Kali aus (Floating Regeln mit Quick)
- Hinweis: Sie wissen nicht was das ist? Recherchieren Sie im Internet!

doc.pfsense.org/index.php/What_are_Floating_Rules

Beantworten Sie die folgenden Fragen, bevor Sie weiter arbeiten.

Frage ITS 4-18

Floating Regeln können Datenverkehr von der FW filtern:

Kann nur Daten, die in die FW hereinkommen (inbound) filtern:

Floating Regeln werden vor allen anderen Regeln geparsed:

Floating Regeln können mehreren Interfaces zugewiesen werden:

Wenn die 'Quick' Option gesetzt ist, wird die letzte und nicht die erste Regel angewendet:

Richtig!

-
- Pingen der Firewall von Windows/Kali

Abgabe

Zeigen Sie Ihr Endresultat einem(r) Betreuer/Betreuerin.

Schließen Sie anschließend die VMs (back to Snapshot) und fahren Sie den Hostrechner herunter.

Jetzt gibt's das Endtestat.

Abgabebestätigung Vom Betreuer auszufüllen!

Richtig!

Abgabe bestätigt