

Sohpos – Netzwerke Verbinden

In diesem Teil der Doku widme ich mich der Sophos, einem Softwarerouter mit Firewall. Die Ausgangssituation ist, dass ich das Netz in eine Unterdomäne unterteilen möchte. Diese Domäne wird im Netzwerkbereich 192.168.3.0/24 erreichbar sein. Sie soll aber über 192.168.2.0/24 ins Internet gehen.

Der Anfang

Um das zu erreichen, erstelle ich zwei VMs für den Router mit jeweils zwei Netzwerkkarten, wobei ich die zweite Karte nachträglich hinzufügen muss. Dazu noch jeweils eine Client VM für jeden Netzwerkbereich. Da ich jede Sophos identisch konfigurieren muss, beschreibe ich nur die Konfiguration der Sophos 1.

Das Netzwerk

Zu erst beginne ich mit dem Netzwerk, das wie folgt aufgebaut ist:

Verbindung	Netz	Sophos 1 IP	Sophos 2 IP
Site-Link	192.168.0.0/30	192.168.0.1	192.168.0.2

LANs an den Standorten:

Standort	LAN-Netz	Gateway (Sophos LAN-IP)
1	192.168.2.0/24	z.B. 192.168.2.100
2	192.168.3.0/24	z.B. 192.168.3.100

Da das LAN-Netz bereits bei der Konfiguration der Sophos erzeugt wurde, füge ich nun manuell das Externe Netz hinzu. Das Externe Netz ist die Autobahn, die beide Netze verbindet. Die /30 bedeutet das ich in dem Netz 4 IP-Adressen habe, von denen ich zwei nutzen kann.

The screenshot shows the Sophos UTM 9 web interface. The 'Interfaces' tab is selected. On the left, a sidebar lists various configuration options under 'Interfaces & Routing'. The main area displays the 'Add Interface' dialog box. The 'Name' field is set to 'extern'. The 'Type' is 'Ethernet' and the 'Hardware' is 'eth1 Virtio network device'. The 'IPv4 address' is '192.168.0.1' and the 'IPv4 Netmask' is '/30 (255.255.255.252)'. The 'IPv4 Default GW' is empty. The 'Comment' field is also empty. At the bottom of the dialog are 'Save' and 'Cancel' buttons. To the right of the dialog, a table lists existing interfaces: 'Intern [Up] on eth0' with IP '192.168.2.100/24', MTU 1500, and default gateway 192.168.2.1. It is noted as 'Auto-created on installation'.

Danach aktiviere ich das Interface

The screenshot shows the Sophos UTM 9 web interface after the 'extern' interface has been added. The 'Interfaces' tab is still selected. The main area now displays a table with two interfaces: 'Intern [Up] on eth0' and 'extern [Up] on eth1'. The 'extern' interface has IP '192.168.0.1/30' and MTU 1500. Both interfaces have 'Edit', 'Delete', and 'Clone' action buttons. The status of both interfaces is shown as 'Up' with a green icon. The table is sorted by 'Name asc' and shows 1-2 of 2 items.

Die Route

Im nächsten Schritt erstelle ich statische Routen. Um einen Fuß in das jeweilige Netz zu haben muss ich für jedes Netz eine Route erstellen. Dazu verwende ich hier Gateway-Routen.

Auf Sophos 1

Feld	Wert
Typ	Gateway
Zielnetz	192.168.3.0/24
Gateway	192.168.1.2
Interface	WAN-Interface wählen (wo 192.168.1.1 liegt)

Feld	Wert
Typ	Gateway
Zielnetz	192.168.2.0/24
Gateway	192.168.1.2
Interface	WAN-Interface wählen (wo 192.168.1.1 liegt)

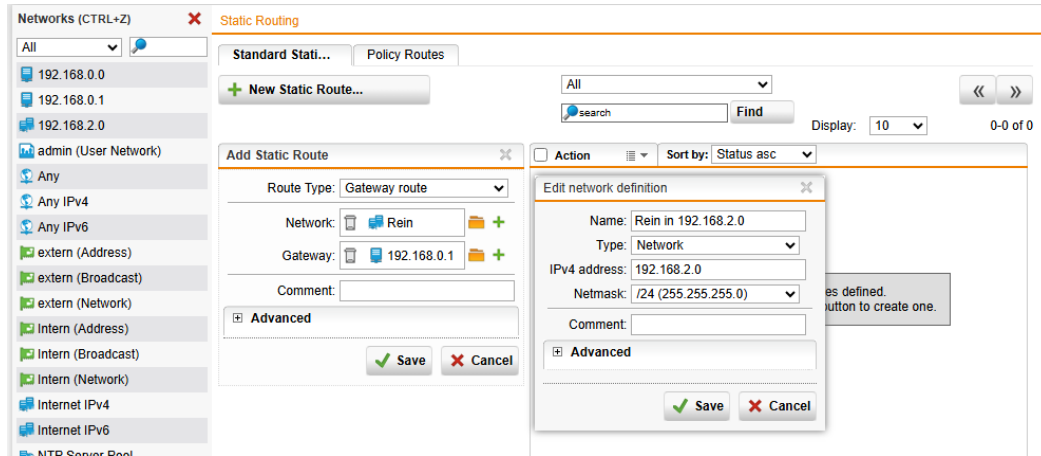
Auf Sophos 2:

Feld	Wert
Typ	Gateway
Zielnetz	192.168.2.0/24
Gateway	192.168.1.1
Interface	WAN-Interface wählen (wo 192.168.1.2 liegt)

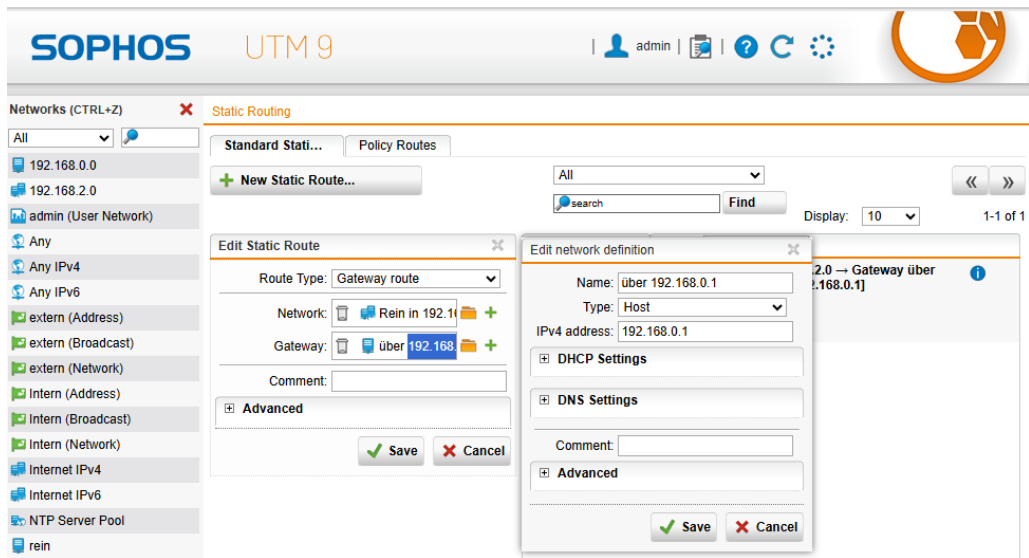
Feld	Wert
Typ	Gateway
Zielnetz	192.168.2.0/24
Gateway	192.168.1.1
Interface	WAN-Interface wählen (wo 192.168.1.2 liegt)

Dazu erstelle ich mir über Interfaces & Routing eine neue Statische Route.
 Wenn ich bei dem Autobahnbeispiel bleibe, ich komme über 192.168.0.1 in das Netz 192.168.3.0 und wenn ich von 192.168.3.0 nach 192.168.2.0 möchte, muss ich über 192.168.0.1 raus auf die Autobahn

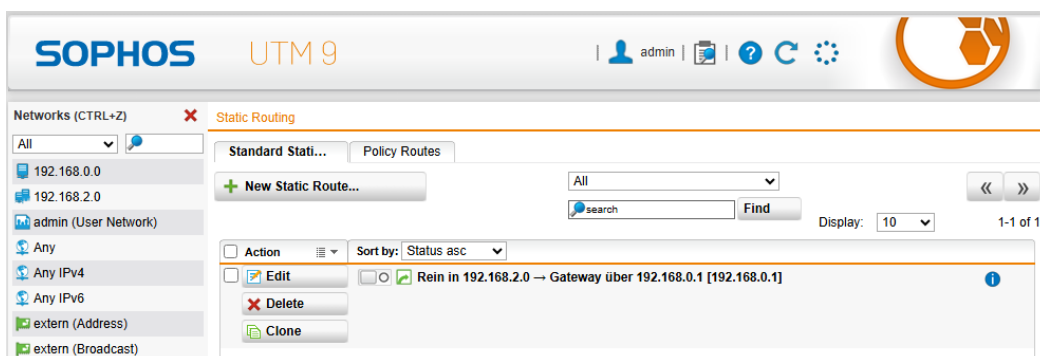
Nach Sophos 1



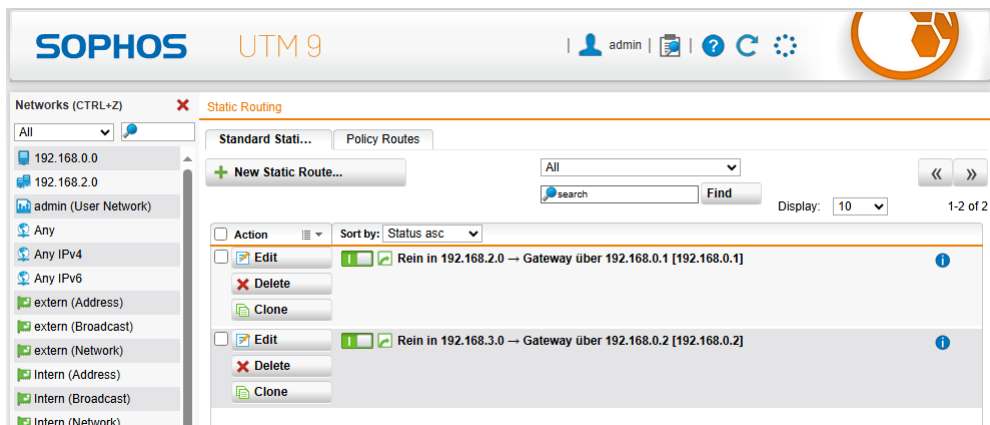
Über



Ergibt folgenden Weg

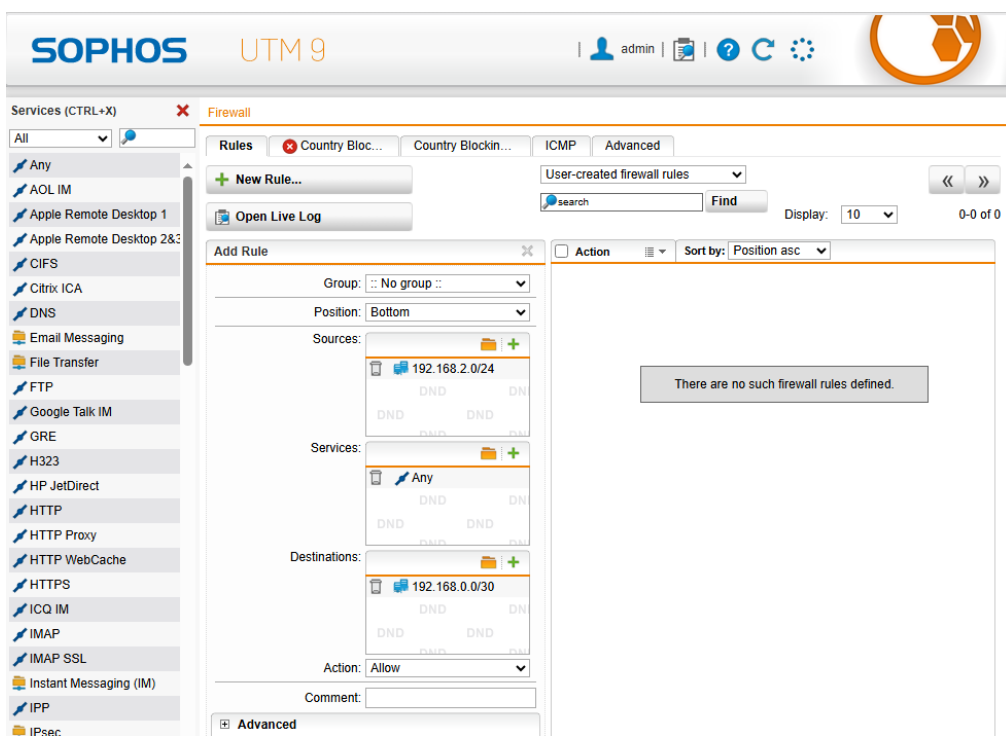


Das selbe nun mit dem Netzwerk 192.168.3.0



Die Verkehrsregeln

Eine Autobahn braucht auch Regeln und Schilder, beispielsweise in welche Richtung der Verkehr fließt, und welche Ausfahrt wohin führt. Dazu erstelle ich entsprechende Firewall-Regeln. Um diese Regeln zu erstellen, gehe ich in den Bereich Networkprotection



Sophos 1

192.168.2.0/24 --> Any --> 192.168.0.0/30

192.168.0.0/30 --> Any --> 192.168.2.0/24

SOPHOS UTM 9

admin

Services (CTRL+X)

Firewall

Rules Country Block... Country Blockin... ICMP Advanced

+ New Rule...

User-created firewall rules

Open Live Log

search Find

Display: 10 1-2 of 2

Action	Sort by: Position asc	1	2
<input type="checkbox"/> Edit <input type="checkbox"/> Delete <input type="checkbox"/> Clone		192.168.2.0/24	192.168.0.0/30
<input type="checkbox"/> Edit <input type="checkbox"/> Delete <input type="checkbox"/> Clone		192.168.0.0/30	192.168.2.0/24

Link

192.168.0.0/30 --> Any --> 192.168.0.0/30

192.168.0.0/30 --> Any --> 192.168.0.0/30

SOPHOS UTM 9

admin

Networks (CTRL+Z)

Firewall

Rules Country Block... Country Blockin... ICMP Advanced

+ New Rule...

User-created firewall rules

Open Live Log

search Find

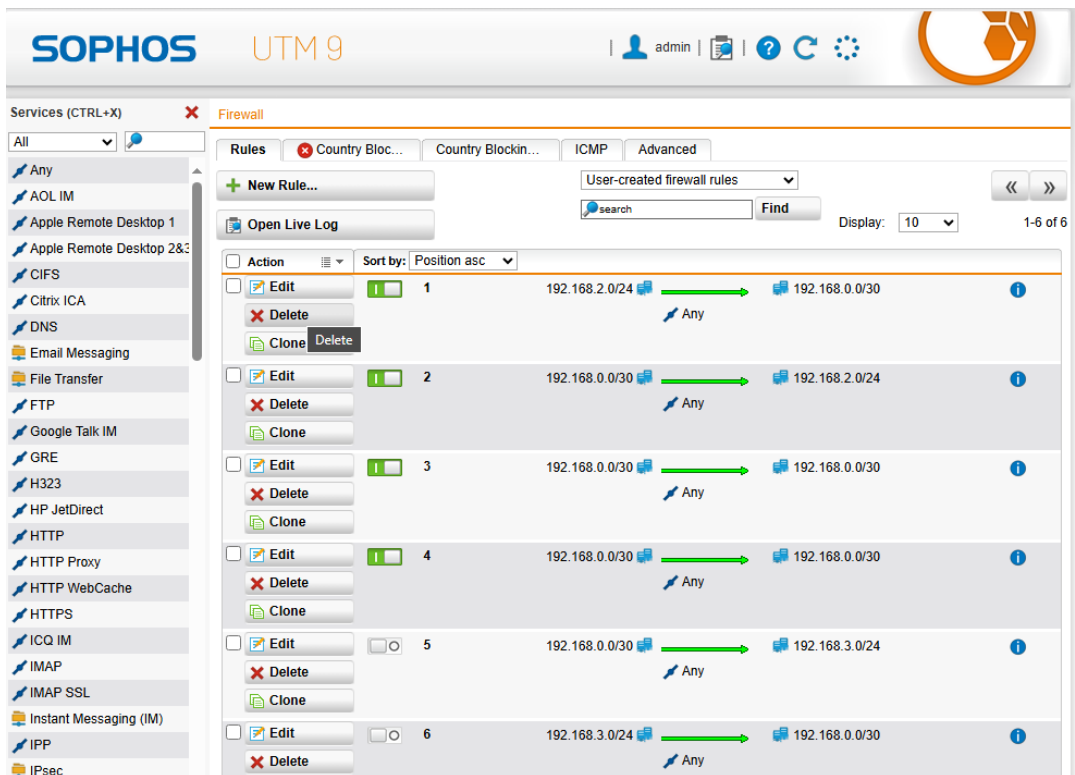
Display: 10 1-4 of 4

Action	Sort by: Position asc	1	2	3	4
<input type="checkbox"/> Edit <input type="checkbox"/> Delete <input type="checkbox"/> Clone		192.168.2.0/24	192.168.0.0/30		
<input type="checkbox"/> Edit <input type="checkbox"/> Delete <input type="checkbox"/> Clone		192.168.0.0/30	192.168.2.0/24		
<input type="checkbox"/> Edit <input type="checkbox"/> Delete <input type="checkbox"/> Clone		192.168.0.0/30	192.168.0.0/30		
<input type="checkbox"/> Edit <input type="checkbox"/> Delete <input type="checkbox"/> Clone		192.168.0.0/30	192.168.0.0/30		

Sophos 2

192.168.0.0/30 --> Any --> 192.168.3.0/24

192.168.3.0/24 --> Any --> 192.168.0.0/30



Damit wäre eine Seite fertig, nun das selbe nochmal auf Sophos 2. Nach dem ich die andere Sophos konfiguriert habe, kommt die Stunde der Wahrheit, stimmt alles?

Der Test

Um zu sehen ob alles funktioniert schaue ich erst mal, ob ich alles anpingen kann. Dazu nutze ich ping und pinge den Weg.

Kann ich die Sophos anpingen?

```
PS C:\Users\Admin> ping 192.168.3.100

Ping wird ausgeführt für 192.168.3.100 mit 32 Bytes Daten:
Antwort von 192.168.3.100: Bytes=32 Zeit<1ms TTL=64
Antwort von 192.168.3.100: Bytes=32 Zeit<1ms TTL=64
Antwort von 192.168.3.100: Bytes=32 Zeit<1ms TTL=64
Antwort von 192.168.3.100: Bytes=32 Zeit<1ms TTL=64

Ping-Statistik für 192.168.3.100:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
    (0% Verlust),
    Ca. Zeitangaben in Millisek.:
        Minimum = 0ms, Maximum = 0ms, Mittelwert = 0ms
PS C:\Users\Admin>
```

Kann ich das Gateway anpingen?

```
PS C:\Users\Admin> ping 192.168.0.2

Ping wird ausgeführt für 192.168.0.2 mit 32 Bytes Daten:
Antwort von 192.168.0.2: Bytes=32 Zeit<1ms TTL=64
Antwort von 192.168.0.2: Bytes=32 Zeit<1ms TTL=64
Antwort von 192.168.0.2: Bytes=32 Zeit<1ms TTL=64
Antwort von 192.168.0.2: Bytes=32 Zeit<1ms TTL=64

Ping-Statistik für 192.168.0.2:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
    (0% Verlust),
    Ca. Zeitangaben in Millisek.:
        Minimum = 0ms, Maximum = 0ms, Mittelwert = 0ms
PS C:\Users\Admin>
```

Komme ich über die Autobahn zur anderen Sophos?

```
PS C:\Users\Admin> ping 192.168.0.1

Ping wird ausgeführt für 192.168.0.1 mit 32 Bytes Daten:
Antwort von 192.168.0.1: Bytes=32 Zeit<1ms TTL=63
Antwort von 192.168.0.1: Bytes=32 Zeit<1ms TTL=63
Antwort von 192.168.0.1: Bytes=32 Zeit<1ms TTL=63
Antwort von 192.168.0.1: Bytes=32 Zeit<1ms TTL=63

Ping-Statistik für 192.168.0.1:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
    (0% Verlust),
    Ca. Zeitangaben in Millisek.:
        Minimum = 0ms, Maximum = 0ms, Mittelwert = 0ms
PS C:\Users\Admin>
```

Kann ich dort abfahren?

```
PS C:\Users\Admin> ping 192.168.2.100

Ping wird ausgeführt für 192.168.2.100 mit 32 Bytes Daten:
Zeitüberschreitung der Anforderung.
Zeitüberschreitung der Anforderung.
Zeitüberschreitung der Anforderung.
Zeitüberschreitung der Anforderung.

Ping-Statistik für 192.168.2.100:
    Pakete: Gesendet = 4, Empfangen = 0, Verloren = 4
    (100% Verlust),
PS C:\Users\Admin>
```


Scheinbar ist die Abfahrt gesperrt. Mal sehen woran das liegt. Dazu verfolge ich mal die Route zu einem Rechner im anderen Netz.

```
PS C:\Users\Admin> tracert 192.168.2.11

Routenverfolgung zu 192.168.2.11 über maximal 30 Hops

 1  <1 ms    <1 ms    <1 ms    192.168.3.100
 2  *        *        *        Zeitüberschreitung der Anforderung.
 3  *        *        *        Zeitüberschreitung der Anforderung.
 4  *        *        *        Zeitüberschreitung der Anforderung.
 5
PS C:\Users\Admin>
```

Und mache das selbe vom anderen Netz aus

Kann ich dort die Sophos anpingen?

```
PS C:\Users\ykurahashi> ping 192.168.2.100

Ping wird ausgeführt für 192.168.2.100 mit 32 Bytes Daten:
Antwort von 192.168.2.100: Bytes=32 Zeit=2ms TTL=64
Antwort von 192.168.2.100: Bytes=32 Zeit=2ms TTL=64
Antwort von 192.168.2.100: Bytes=32 Zeit<1ms TTL=64
Antwort von 192.168.2.100: Bytes=32 Zeit=4ms TTL=64

Ping-Statistik für 192.168.2.100:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
    (0% Verlust),
Ca. Zeitangaben in Millisek.:
    Minimum = 0ms, Maximum = 4ms, Mittelwert = 2ms
PS C:\Users\ykurahashi>
```

Und das Gateway?

```
PS C:\Users\ykurahashi> ping 192.168.0.1

Ping wird ausgeführt für 192.168.0.1 mit 32 Bytes Daten:
Antwort von 192.168.0.1: Bytes=32 Zeit=8ms TTL=63
Antwort von 192.168.0.1: Bytes=32 Zeit=11ms TTL=63
Antwort von 192.168.0.1: Bytes=32 Zeit=8ms TTL=63
Antwort von 192.168.0.1: Bytes=32 Zeit=8ms TTL=63

Ping-Statistik für 192.168.0.1:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
    (0% Verlust),
Ca. Zeitangaben in Millisek.:
    Minimum = 8ms, Maximum = 11ms, Mittelwert = 8ms
PS C:\Users\ykurahashi>
```

Die Ausfahrt bei der anderen Sophos?

```
PS C:\Users\ykurahashi> ping 192.168.0.2

Ping wird ausgeführt für 192.168.0.2 mit 32 Bytes Daten:
Zeitüberschreitung der Anforderung.
Zeitüberschreitung der Anforderung.
Zeitüberschreitung der Anforderung.
Zeitüberschreitung der Anforderung.

Ping-Statistik für 192.168.0.2:
    Pakete: Gesendet = 4, Empfangen = 0, Verloren = 4
    (100% Verlust),
PS C:\Users\ykurahashi> _
```

Da ist was Kaputt. Mal sehen was. Was sagt tracert über die Route

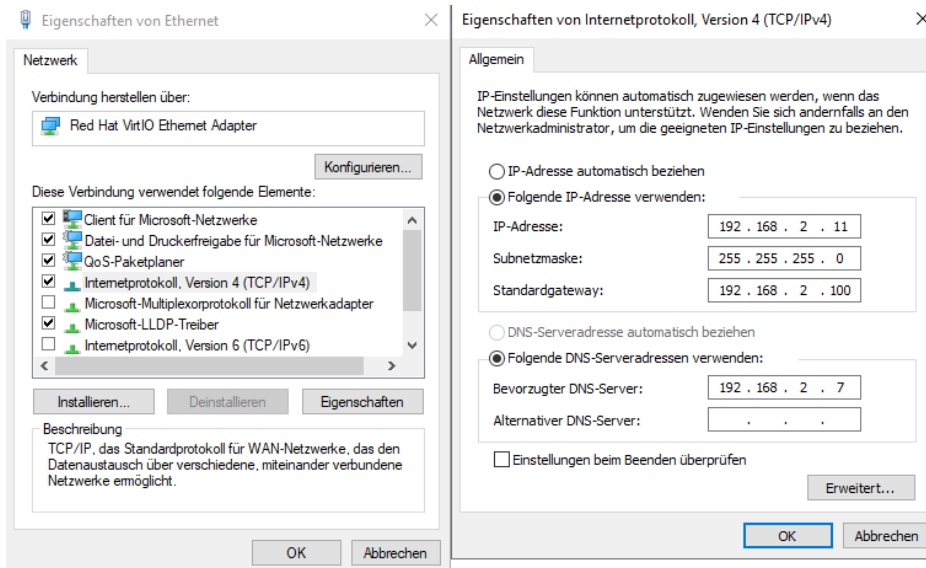
```
PS C:\Users\ykurahashi> tracert 192.168.0.2

Routenverfolgung zu Kako.Sotoba.de [192.168.0.2]
über maximal 30 Hops:

 1          2 ms      <1 ms      1 ms    192.168.2.1
 2          *          *          *        Zeitüberschreitung der Anforderung.
 3          *          *          *        Zeitüberschreitung der Anforderung.
 4

PS C:\Users\ykurahashi>
```

Ah, die Pakete nehmen die falsche Autobahn und wollen über das Standardgateway raus.
Dann muss ich wohl die IP der Sophos als Gateway hinzufügen.



Nach dem ich den Gateway über die Sophos laufen lasse, funktioniert auch der andere Weg.

```
Windows PowerShell

PS Z:\> ping 192.168.3.100

Ping wird ausgeführt für 192.168.3.100 mit 32 Bytes Daten:
Antwort von 192.168.3.100: Bytes=32 Zeit<1ms TTL=63
Antwort von 192.168.3.100: Bytes=32 Zeit<1ms TTL=63
Antwort von 192.168.3.100: Bytes=32 Zeit<1ms TTL=63
Antwort von 192.168.3.100: Bytes=32 Zeit<1ms TTL=63

Ping-Statistik für 192.168.3.100:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
            (0% Verlust),
    Ca. Zeitangaben in Millisek.:
        Minimum = 0ms, Maximum = 0ms, Mittelwert = 0ms
PS Z:\> tracert 192.168.3.100

Routenverfolgung zu Fuso.Sotoba.de [192.168.3.100]
über maximal 30 Hops:

 1      <1 ms    <1 ms    <1 ms    192.168.2.100
 2      <1 ms    <1 ms    <1 ms    Fuso.Sotoba.de [192.168.3.100]

Ablaufverfolgung beendet.
PS Z:\>
```

Der Verkehr zwischen den beiden Sophos funktioniert also. Als nächstes schaue ich, ob ich einen Rechner im anderen Netz tracen kann

```
Windows PowerShell
PS C:\Users\Admin> ping 192.168.2.125

Ping wird ausgeführt für 192.168.2.125 mit 32 Bytes Daten:
Zeitüberschreitung der Anforderung.
Zeitüberschreitung der Anforderung.
Zeitüberschreitung der Anforderung.
Zeitüberschreitung der Anforderung.

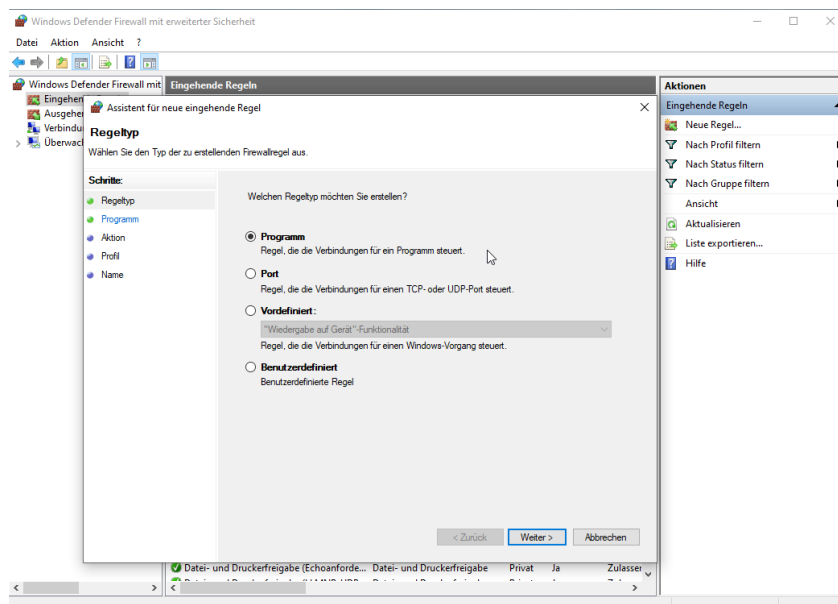
Ping-Statistik für 192.168.2.125:
    Pakete: Gesendet = 4, Empfangen = 0, Verloren = 4
    (100% Verlust),
PS C:\Users\Admin> tracert 192.168.2.125

Routenverfolgung zu 192.168.2.125 über maximal 30 Hops

 1  <1 ms    <1 ms    <1 ms    192.168.3.100
 2  <1 ms    <1 ms    <1 ms    192.168.0.1
 3  *                *                Zeitüberschreitung der Anforderung.
 4

PS C:\Users\Admin>
```

Das sieht aus als hätte die Windows-Firewall die Grenzen dicht gemacht. Um das zu ändern, baue ich mir eine eigene Regel. Dazu gehe in die erweiterten Firewalloptionen



und erstelle mir eine benutzerdefinierte Regel für alle Programme

Assistent für neue eingehende Regel

Programm

Geben Sie den vollständigen Programmpfad und den Namen der ausführbaren Datei des Programms an, dem diese Regel entspricht.

Schritte:

- Regeltyp
- Programm
- Protokolle und Ports
- Bereich
- Aktion
- Profil
- Name

Betrifft diese Regel alle oder nur ein bestimmtes Programm?

☒ **Alle Programme**
Die Regel wird auf alle Computerverbindungen angewendet, die mit anderen Regeleigenschaften übereinstimmen.

☐ **Dieser Programmpfad:**

Beispiel: c:\Pfad\Programm.exe
%ProgramFiles%\Browser\Browser.exe

Dienste
Legen Sie die Dienste fest, die diese Regel betrifft.

< Zurück Weiter > Abbrechen

zum anpingen eine Regel für ICMP

Assistent für neue eingehende Regel

Protokolle und Ports

Geben Sie die Protokolle und Ports an, für die diese Regel gilt.

Schritte:

- Regeltyp
- Programm
- Protokolle und Ports
- Bereich
- Aktion
- Profil
- Name

Für welche Ports und Protokolle gilt diese Regel?

Protokolltyp: ICMPv4

Protokollnummer: 1

Lokaler Port: Alle Ports

Beispiel: 80, 443, 5000-5010

Remoteport: Alle Ports

Beispiel: 80, 443, 5000-5010

ICMP-Einstellungen:

< Zurück Weiter > Abbrechen

Danach gebe ich an für wem diese Regel gilt

Assistent für neue eingehende Regel

Bereich

Geben Sie die lokalen IP-Adressen und die Remote-IP-Adressen an, auf die diese Regel angewendet wird.

Schritte:

- Regeltyp
- Programm
- Protokolle und Ports
- Bereich**
- Aktion
- Profil
- Name

Für welche lokalen IP-Adressen gilt diese Regel?

☒ Beliebige IP-Adresse

☐ Diese IP-Adressen:

Hinzufügen...
Bearbeiten...
Entfernen

Passen Sie Schnittstellentypen an, für die die Regel angewendet wird:

Für welche Remote-IP-Adressen gilt diese Regel?

☒ Beliebige IP-Adresse

☐ Diese IP-Adressen:

Hinzufügen...
Bearbeiten...
Entfernen

< Zurück **Weiter >** Abbrechen

und lasse diese Verbindung dann zu

Assistent für neue eingehende Regel

Aktion

Legen Sie die Aktion fest, die ausgeführt werden soll, wenn eine Verbindung die in der Regel angegebenen Bedingungen erfüllt.

Schritte:

- Regeltyp
- Programm
- Protokolle und Ports
- Bereich
- Aktion**
- Profil
- Name

Welche Aktion soll durchgeführt werden, wenn eine Verbindung die angegebenen Bedingungen erfüllt?

☒ **Verbindung zulassen**

Dies umfasst sowohl mit IPsec geschützte als auch nicht mit IPsec geschützte Verbindungen.

☐ **Verbindung zulassen, wenn sie sicher ist**

Dies umfasst nur mithilfe von IPsec authentifizierte Verbindungen. Die Verbindungen werden mit den Einstellungen in den IPsec-Eigenschaften und -regeln im Knoten "Verbindungssicherheitsregel" gesichert.

☐ **Verbindung blockieren**

< Zurück **Weiter >** Abbrechen

Und bestimme wo die Regel angewendet werden soll.

Assistent für neue eingehende Regel

Profil

Geben Sie die Profile an, für die diese Regel zutrifft.

Schritte:

- Regeltyp
- Programm
- Protokolle und Ports
- Bereich
- Aktion
- Profil**
- Name

Wann wird diese Regel angewendet?

☒ **Domäne**
Wird angewendet, wenn ein Computer mit der Firmendomäne verbunden ist.

☒ **Privat**
Wird angewendet, wenn ein Computer mit einem privaten Netzwerk (z.B. zu Hause oder am Arbeitsplatz) verbunden ist.

☒ **Öffentlich**
Wird angewendet, wenn ein Computer mit einem öffentlichen Netzwerk verbunden ist.

< Zurück Weiter > Abbrechen

Zum Schluss bekommt die Regel einen Namen

Assistent für neue eingehende Regel

Name

Geben Sie den Namen und die Beschreibung dieser Regel an.

Schritte:


- Regeltyp
- Programm
- Protokolle und Ports
- Bereich
- Aktion
- Profil
- Name**

Name:
Ping Zulassen

Beschreibung (optional):

< Zurück Fertig stellen Abbrechen

Nach dem Fertigstellen, teste ich mit Ping und Tracert, ob der Rechner nun erreichbar ist
Das ganze muss ich nun bei dem anderen Rechner auch machen

 Windows PowerShell

```
PS C:\Users\Admin> ping 192.168.2.125

Ping wird ausgeführt für 192.168.2.125 mit 32 Bytes Daten:
Antwort von 192.168.2.125: Bytes=32 Zeit=1ms TTL=126
Antwort von 192.168.2.125: Bytes=32 Zeit=1ms TTL=126
Antwort von 192.168.2.125: Bytes=32 Zeit=1ms TTL=126
Antwort von 192.168.2.125: Bytes=32 Zeit=1ms TTL=126

Ping-Statistik für 192.168.2.125:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
    (0% Verlust),
    Ca. Zeitangaben in Millisek.:
        Minimum = 1ms, Maximum = 1ms, Mittelwert = 1ms
PS C:\Users\Admin> tracert 192.168.2.125

Routenverfolgung zu 192.168.2.125 über maximal 30 Hops

 1    <1 ms    <1 ms    <1 ms    192.168.3.100
 2    <1 ms    <1 ms    <1 ms    192.168.0.1
 3     1 ms    <1 ms    <1 ms    192.168.2.125

Ablaufverfolgung beendet.
PS C:\Users\Admin> 
```

Da ich nun in beiden Netzen den Rechner anpingen kann endet diese Story hier erstmal für heute. Morgen geht es weiter