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

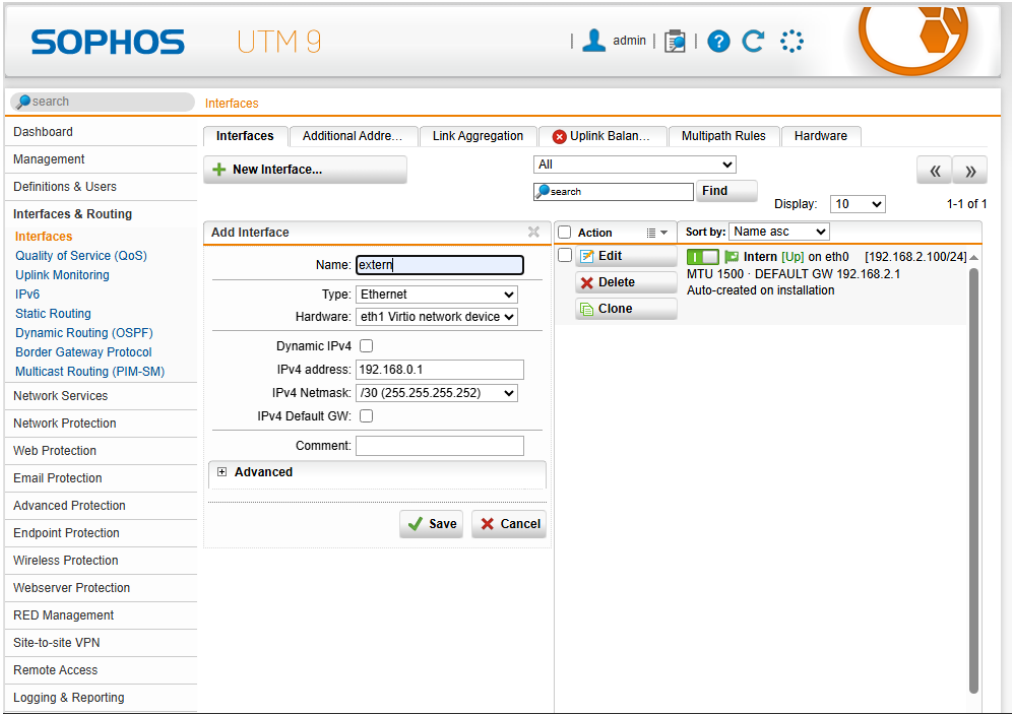
Zu erst beginne ich mit dem Netzwerk, das wie folgt aufgebaut ist

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

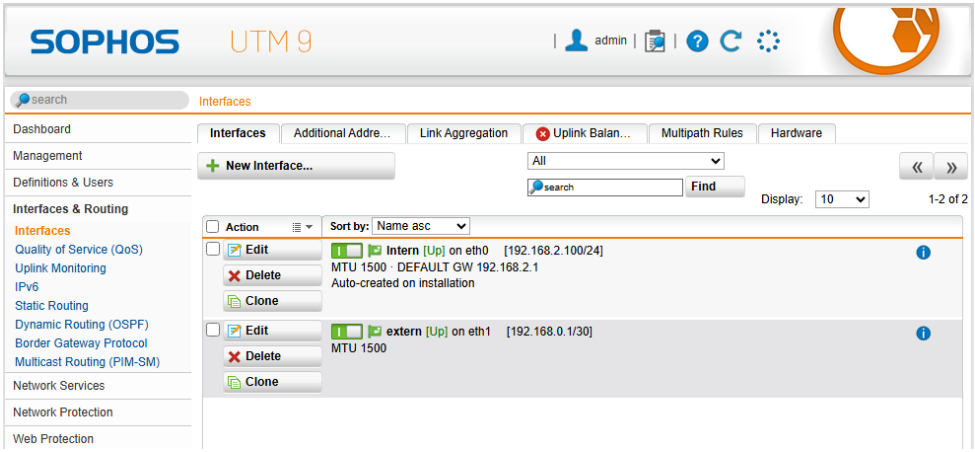
LANs an den Standorten:

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 ich zwei nutzen kann.



Danach aktiviere ich das Interface



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)

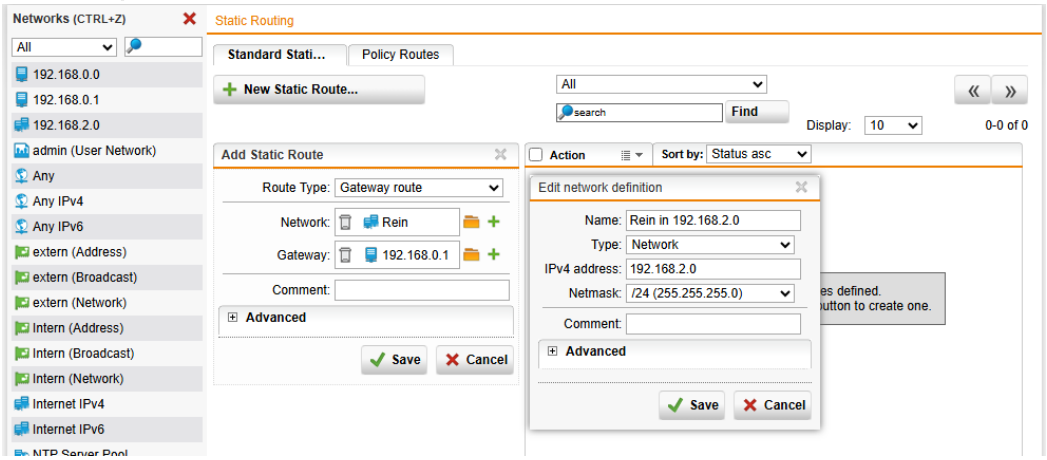
Auf Sophos 2:

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)

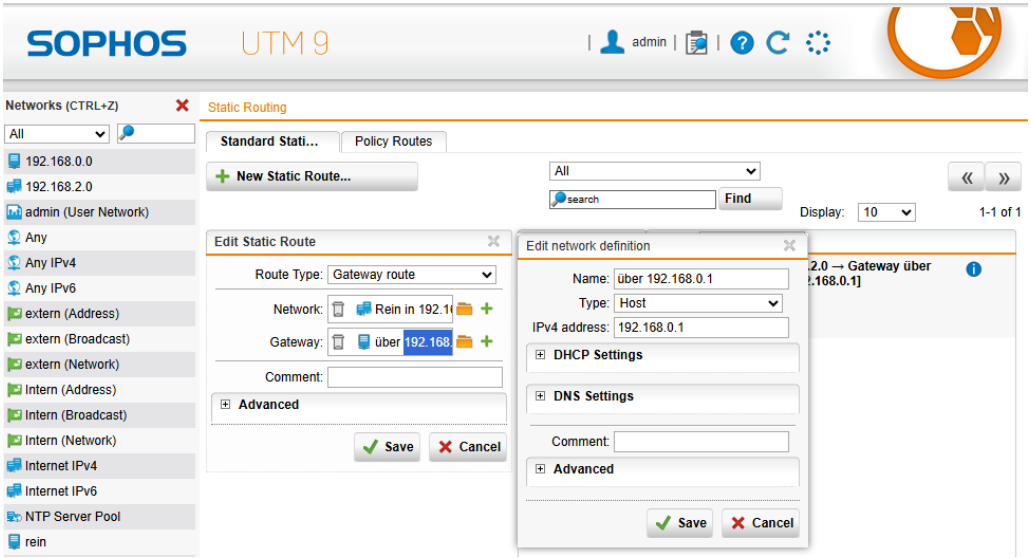
Feld	Wert
Typ	**Gateway**
Zielnetz	192.168.2.0/24
Gateway	192.168.1.1
Interface	WAN-Interface wählen (wo 192.168.1.2 liegt)

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

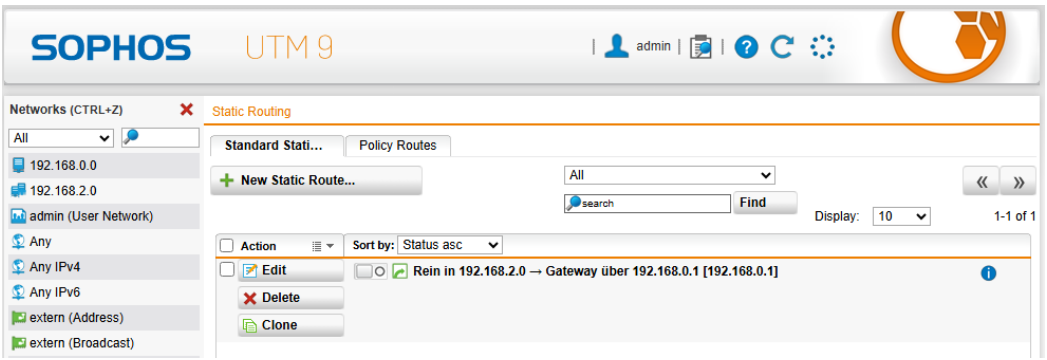
Nach Sophos 1



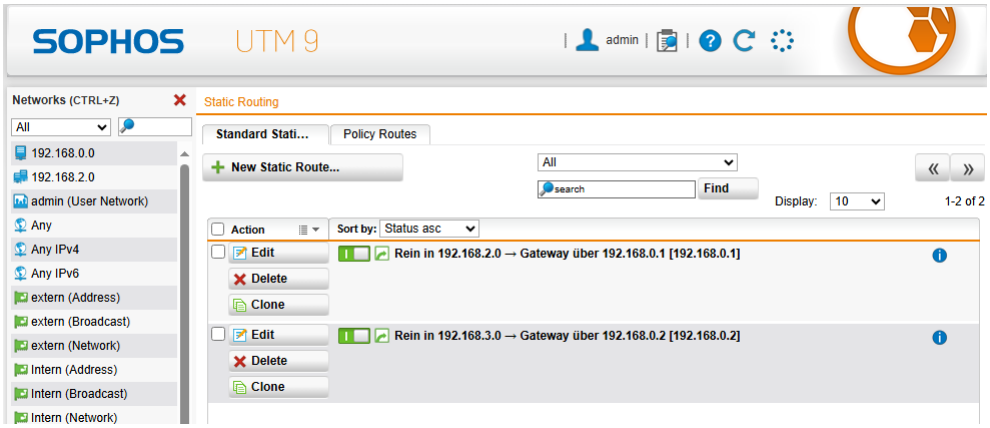
Über



Ergibt folgenden Weg

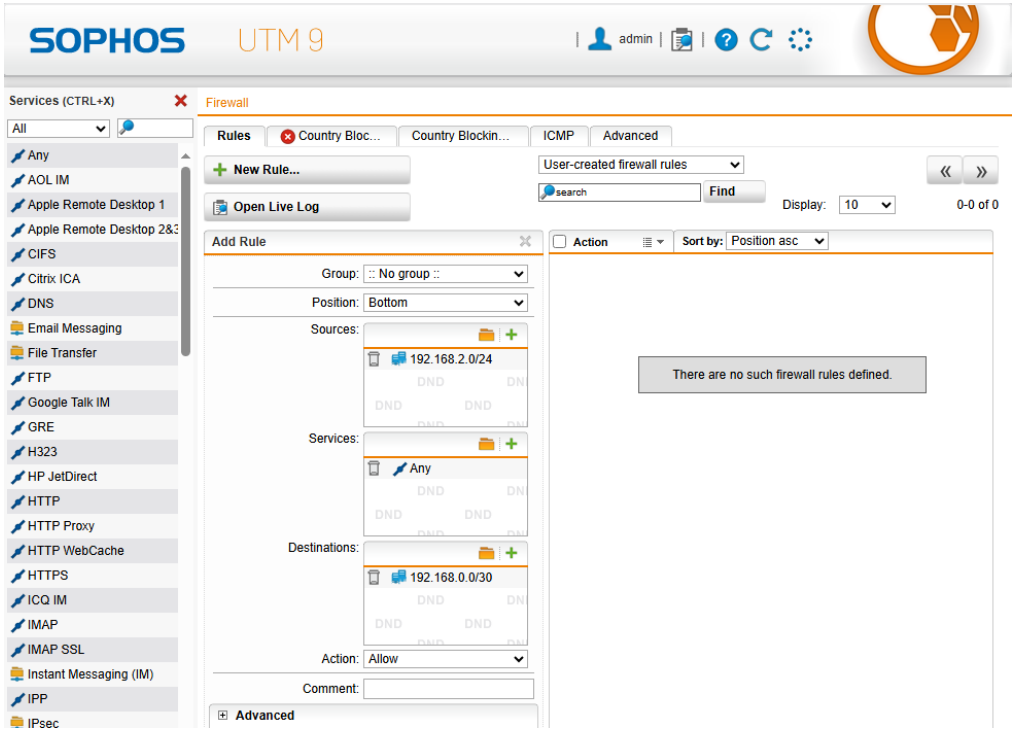


Das selbe nun mit dem Netzwerk 192.168.3.0



Die Verkehrsregeln

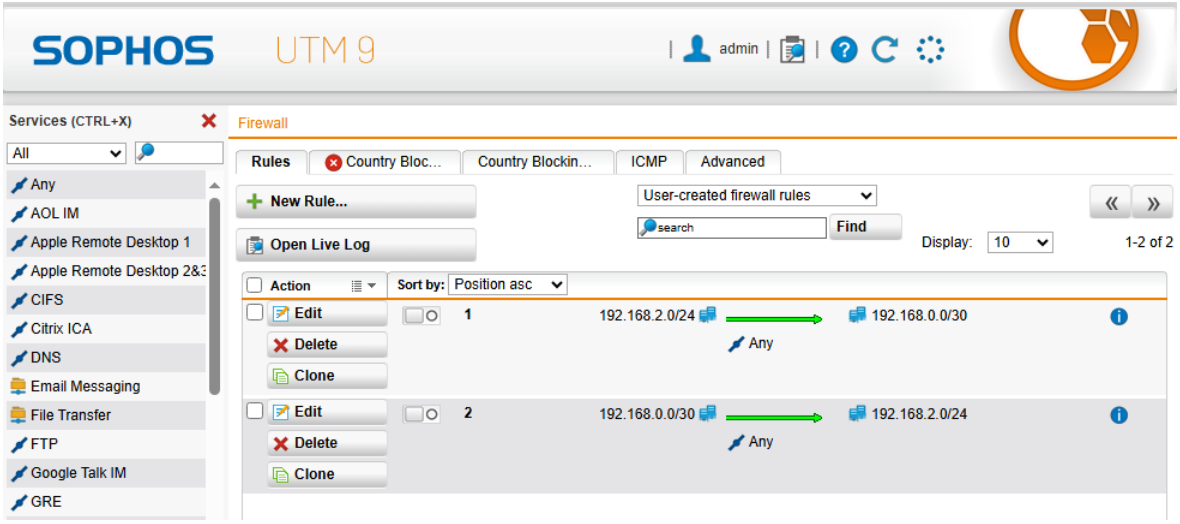
Eine Autobahn braucht auch Regeln und Schilder, beispielsweise in welche Richtung der Verkehr fliest, und welche Ausfahrt wohin führt. Dazu erstelle ich entsprechende Firewall-Regeln. Um diese Regeln zu erstellen, gehe ich in den Bereich Networkprotection



Sophos 1

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

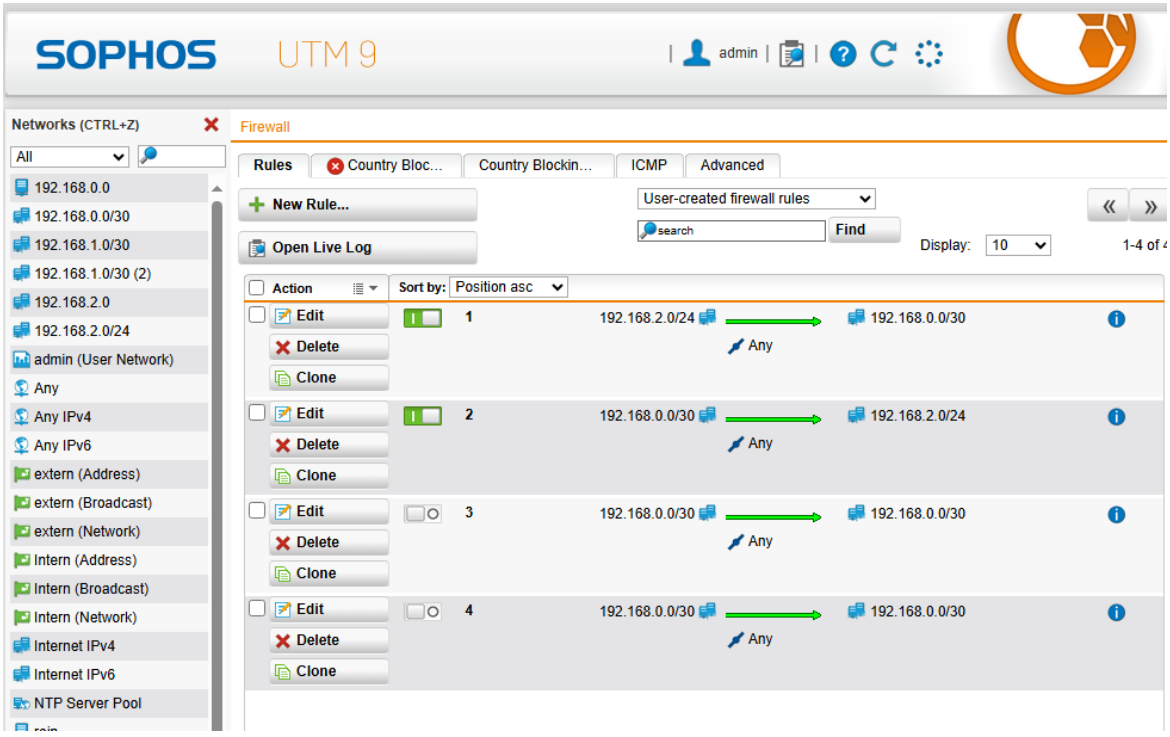
192.168.0.0/30 --> Any --> 192.168.2.0/24



Link

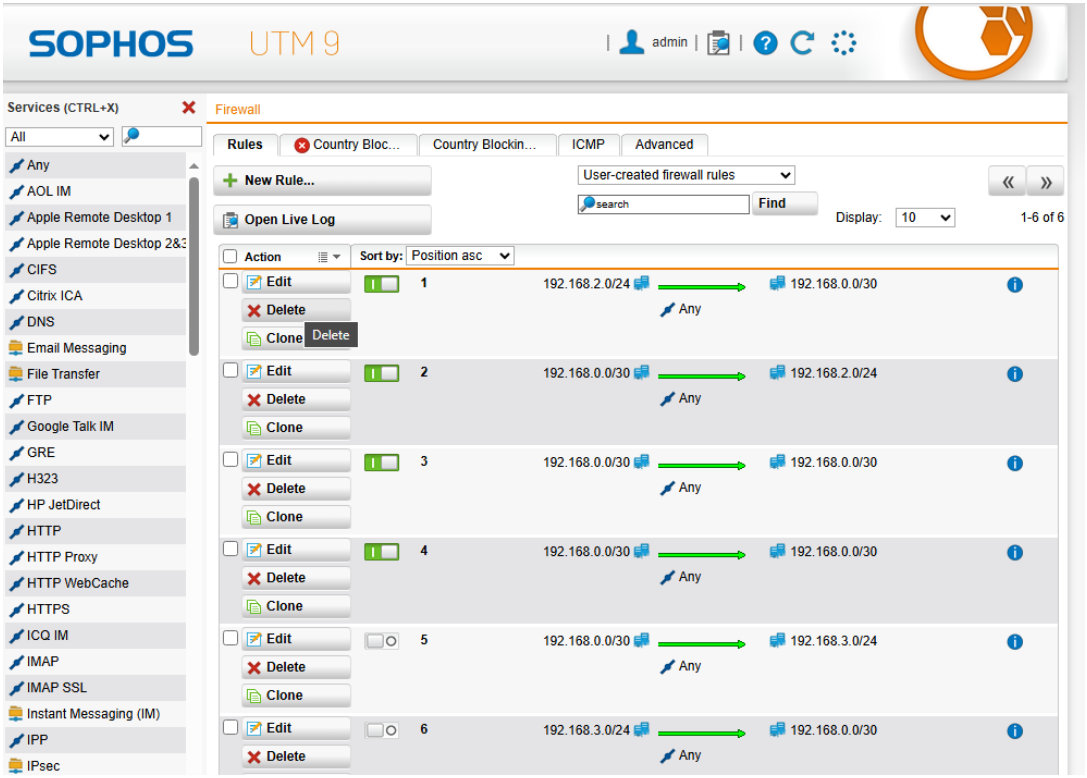
192.168.0.0/30 --> Any --> 192.168.0.0/30

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

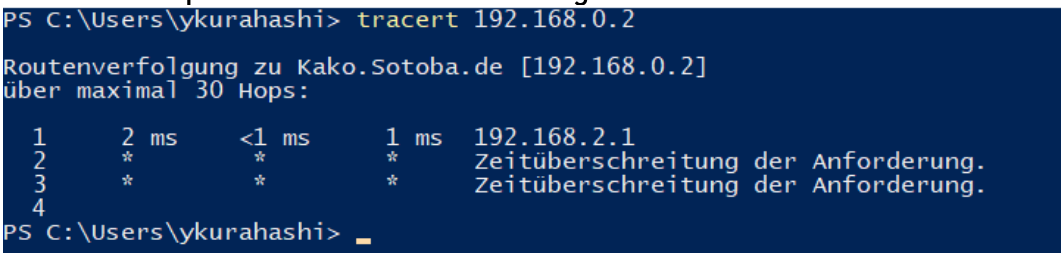
Die Ausfahrt bei der anderen Sophos?

```
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



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

Danach ist ein Neustart empfehlenswert. Nach dem Neustart mache ich den Test nochmal mache ich den Test nochmal