

## ALL7007 VPN-Tunnel

# Musterkonfiguration zwischen zwei ALL7007 über dynamische IP-Adressen mit PPPoE

**Wichtig: Beide Geräte müssen auf der LAN-Seite unterschiedliche IP-Kreise verwenden! Jeder der Schritte muss auf BEIDEN Geräten durchgeführt werden!**

### Konfiguration der Test-Router:

#### **LAN1:**

Router IP: 192.168.1.1

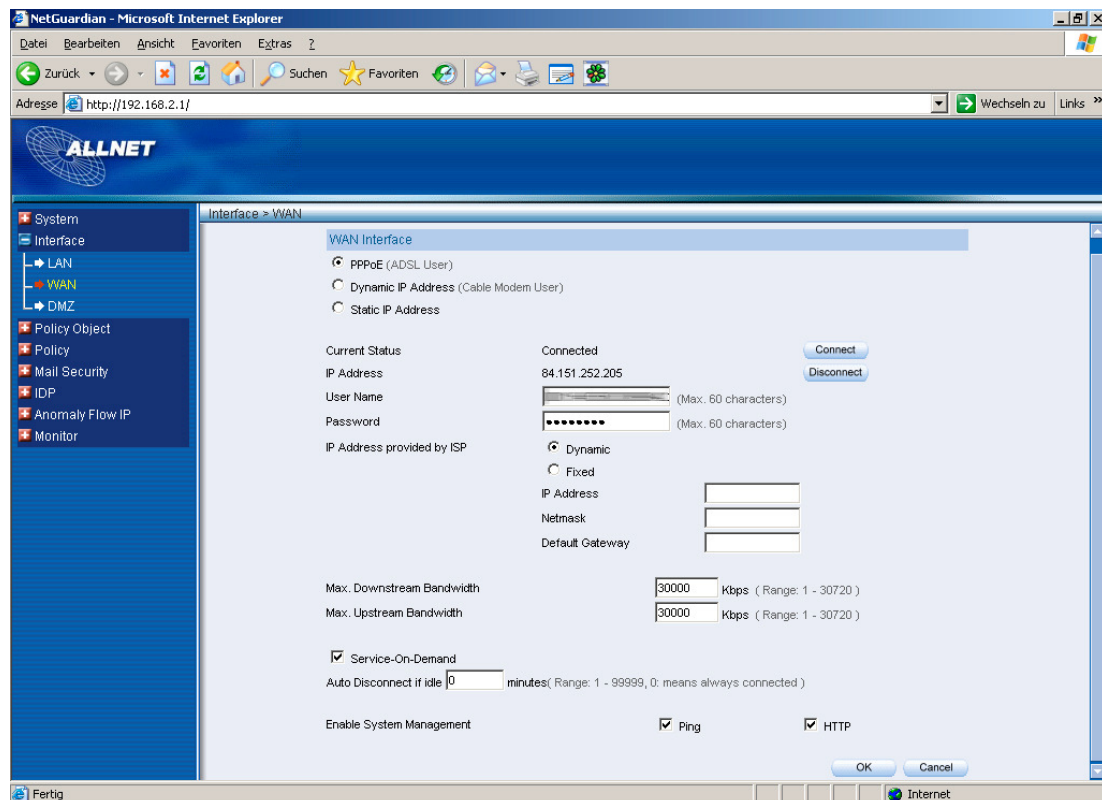
#### **LAN2:**

Router IP: 192.168.2.1

Alle für ALLNET sicherheitsrelevanten Daten wurden in dieser Anleitung unkenntlich gemacht!

### Schritt 1: Einrichtung WAN-Port

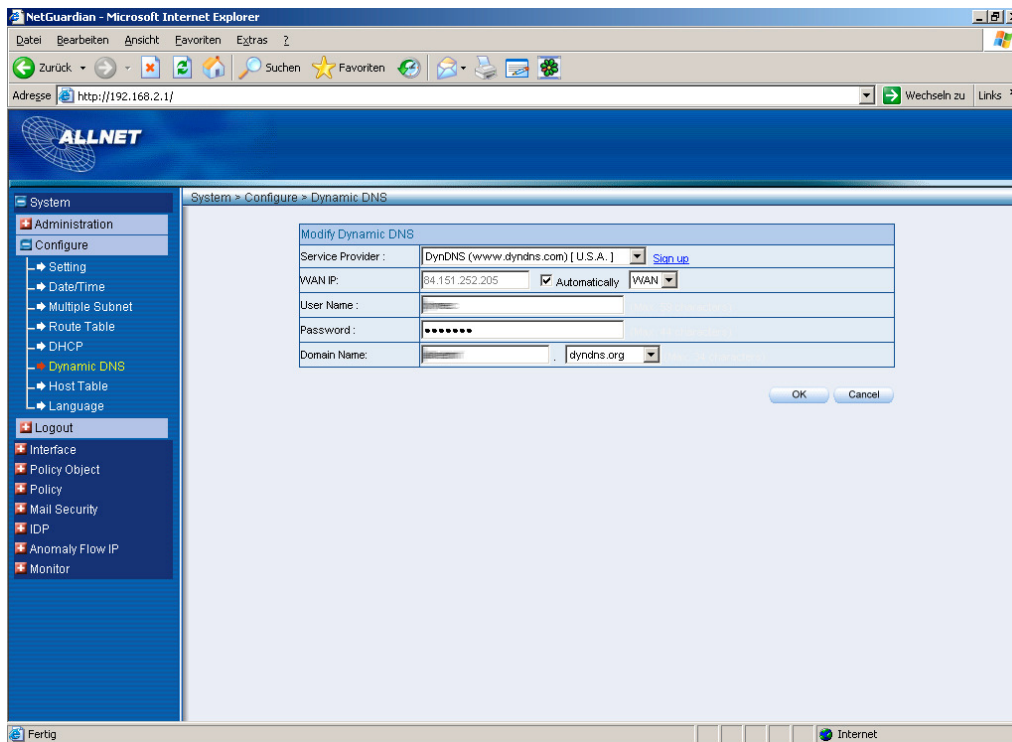
Öffnen sie das Menü „Interface → WAN“ und tragen sie dort ihre Internetzugangsdaten ein und speichern diese über einen Klick auf „OK“ ab.



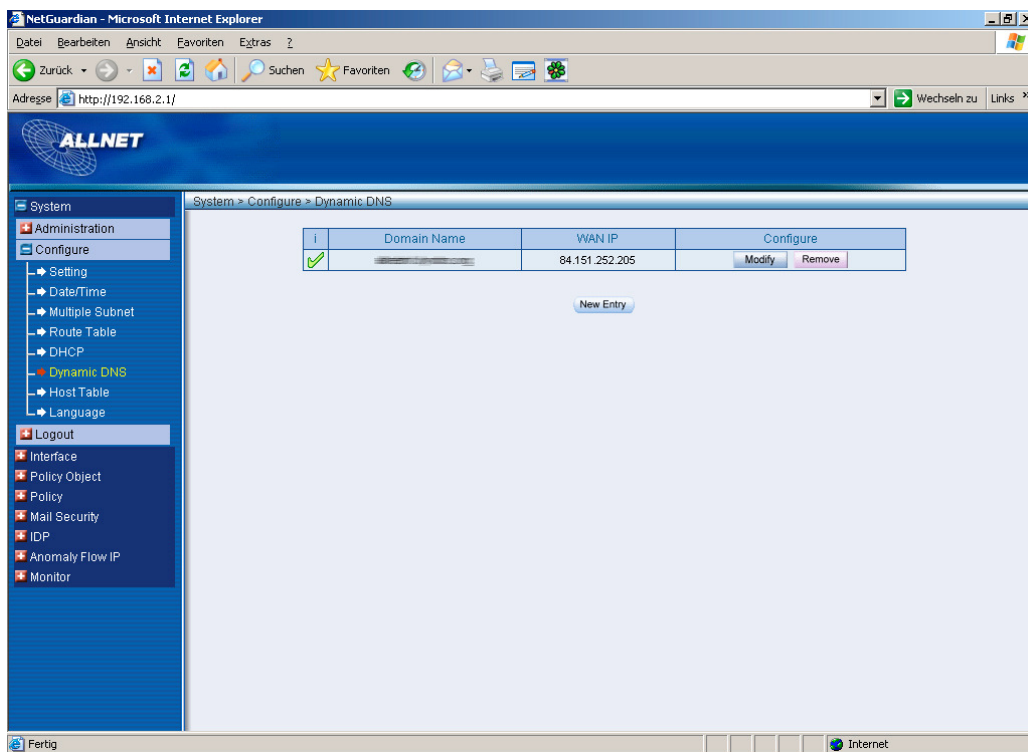
### Schritt 2: Einrichtung DynDNS

Sie benötigen hierfür einen dynamischen Domainnamen. Diesen erhalten sie beispielsweise auf [www.dyndns.org](http://www.dyndns.org). Wenn sie bereits einen Account haben können sie diesen in der ALL7007 eintragen.

Gehen sie hierfür in das Menü „System → Configuration → Dynamic DNS“. Hier können sie ihren DynDNS-Server auswählen und ihre Zugangsdaten eintragen.



Wenn ihre Daten korrekt abgeglichen werden konnten, sehen sie folgenden Bildschirm:



### **Schritt 3: Einrichtung IPSec-Policy**

Für die Konfiguration der IP-Sec-Policy begeben sie sich bitte in das Menü „Policy Object → VPN → IPSec Autokey“. Tragen sie hier ihre Daten gemäß der Musterkonfiguration ein. Wichtig sind hierbei folgende Punkte:

- Im Feld „To Destination → Remote Gateway“ können sie den DynDNS-Domainnamen der gegenüberliegenden Seite eintragen.

- Der Preshared-Key muss aus mindestens acht Zeichen bestehen und muss auf beiden Geräten identisch konfiguriert werden.
- Alle Verschlüsselungsoptionen müssen identisch eingestellt werden.
- Die Werte in den Feldern „My ID“ und „Peer ID“ müssen auf den Geräten jeweils gespiegelt konfiguriert werden. Das @-Zeichen ist hierbei wichtig!
- In den Feldern „GRE Local IP“ und „GRE Remote IP“ werden die LAN-Adressen der Geräte eingetragen. „GRE Local IP“ beschreibt die lokale, „GRE Remote IP“ beschreibt die entfernte LAN-Adresse.

NetGuardian - Microsoft Internet Explorer

Adresse: <http://192.168.2.1/>

**ALLNET**

Policy Object > VPN > IPSec Autokey

**Necessary item**

Name	ALLTEST
To Destination	<input checked="" type="radio"/> Remote Gateway -- Fixed IP or Domain Name <input type="radio"/> Remote Gateway or Client -- Dynamic IP
Authentication Method	Preshare
Preshared Key	12345678
Encapsulation	
ISAKMP Algorithm	
ENC Algorithm	DES
AUTH Algorithm	MD5
Group	GROUP 1
IPsec Algorithm	
<input checked="" type="radio"/> Data Encryption + Authentication <input type="radio"/> Authentication Only	
ENC Algorithm	DES
AUTH Algorithm	MD5

**Optional item**

Perfect Forward Secrecy	NO-PFS
ISAKMP Lifetime	3600 Seconds
IPsec Lifetime	28800 Seconds

Fertig

NetGuardian - Microsoft Internet Explorer

Adresse: <http://192.168.2.1/>

**ALLNET**

Policy Object > VPN > IPSec Autokey

**Optional item**

Perfect Forward Secrecy	NO-PFS
ISAKMP Lifetime	3600 Seconds
IPsec Lifetime	28800 Seconds

**Mode**

☒ Main mode  
☐ Aggressive mode

My ID: @all7007-2

Peer ID: @all7007-1

GRE Local IP: 192.168.2.1

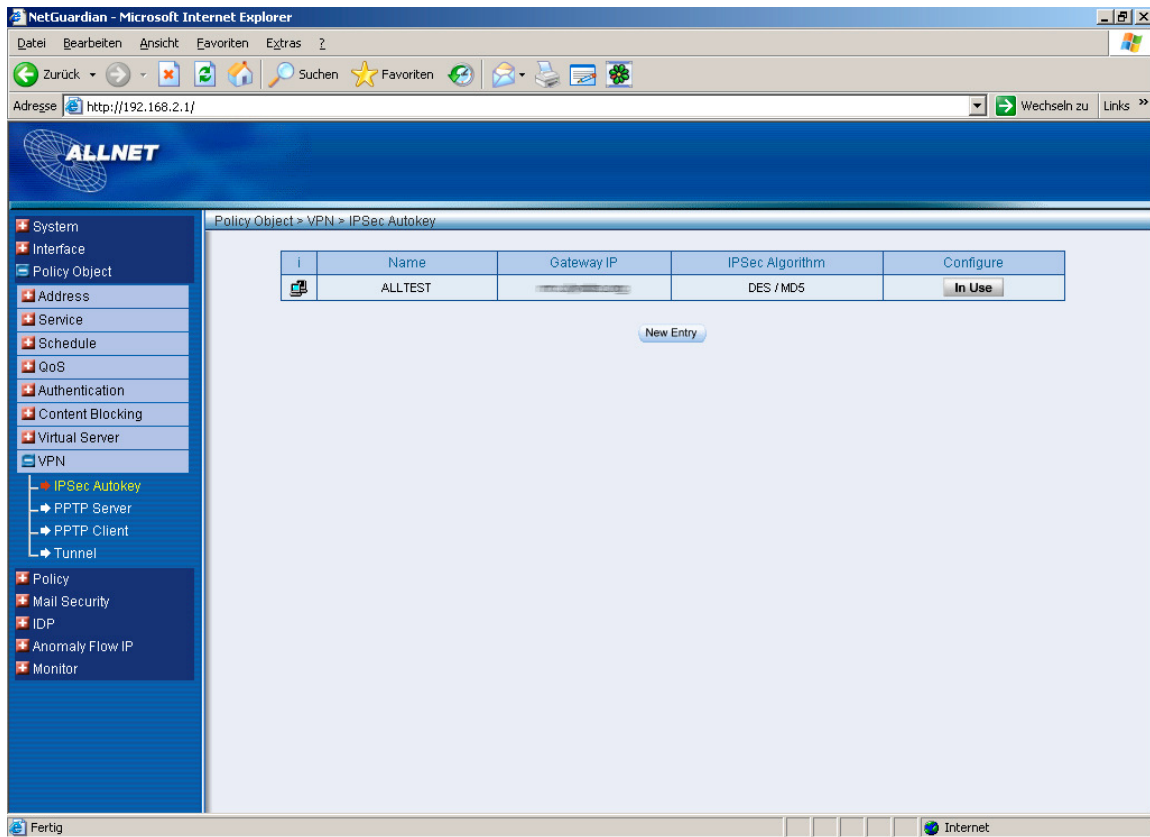
GRE Remote IP: 192.168.1.1

☐ Manual Connect

Dead Peer Detection: Retry 5 times, Timeout 5 Second

Cancel

Fertig



#### **Schritt 4: Konfiguration des Tunnels**

Nach der Konfiguration der IP-Sec-Policy müssen sie dem Gerät mitteilen, dass sie einen VPN-Tunnel nutzen möchten. Hierfür gehen sie im Menü auf den Punkt „Policy Object → VPN → Tunnel“. Hier haben sie die Möglichkeit den Tunnel wie folgt zu öffnen:

- Geben sie im Bereich „From Source Subnet / Mask“ ihr lokales Subnetz und die lokale Subnetzmaske an.
- Im Bereich „To Destination“ wählen sie „To Destination Subnet / Mask“ und geben hier das entfernte lokale Subnetz und die entsprechende Subnetzmaske ein.
- Im Feld „IPsec/PPTP-Setting“ wählen sie die vorher konfigurierte IPsec Policy aus.
- Im Feld „Keep alive IP“ tragen sie eine lokale IP-Adresse aus dem gegenüberliegenden Netz ein.

NetGuardian - Microsoft Internet Explorer

Adresse: http://192.168.2.1/

**ALLNET**

System  
Interface  
Policy Object  
Address  
Service  
Schedule  
QoS  
Authentication  
Content Blocking  
Virtual Server  
VPN  
IPSec Autokey  
PPTP Server  
PPTP Client  
Tunnel  
Policy  
Mail Security  
IDP  
Anomaly Flow IP  
Monitor

Policy Object > VPN > Tunnel

Modify ALLTEST2 Tunnel

Name	ALLTEST2	
From Source	<input checked="" type="radio"/> LAN <input type="radio"/> DMZ	
From Source Subnet / Mask	192.168.2.0	/ 255.255.255.0
To Destination	<input checked="" type="radio"/> To Destination Subnet / Mask	
	192.168.1.0	/ 255.255.255.0
<input type="radio"/> Remote Client		
IPSec / PPTP Setting	ALLTEST	
Keep alive IP:	192.168.1.1	
<input checked="" type="checkbox"/> Show remote Network Neighborhood		

Cancel

Fertig

Internet

NetGuardian - Microsoft Internet Explorer

Adresse: http://192.168.2.1/

**ALLNET**

System  
Interface  
Policy Object  
Address  
Service  
Schedule  
QoS  
Authentication  
Content Blocking  
Virtual Server  
VPN  
IPSec Autokey  
PPTP Server  
PPTP Client  
Tunnel  
Policy  
Mail Security  
IDP  
Anomaly Flow IP  
Monitor

Policy Object > VPN > Tunnel

	Name	Source Subnet	Destination Subnet	IPSec / PPTP	Configure
	ALLTEST2	192.168.2.0	192.168.1.0	ALLTEST	In Use

New Entry

Fertig

Internet

## Schritt 5: Konfiguration der Outgoing/Incoming Policy's

Damit ihr VPN funktioniert müssen sie sowohl eine Outgoing wie auch eine Incoming Policy für das VPN definieren. Zusätzlich muss jeweils eine Outgoing und eine Incoming Policy für den Internettraffic vergeben werden. Diese müssen wie folgt konfiguriert werden (Traffic Log und Statistic können, müssen aber nicht aktiviert werden):

**Wichtig: Im Feld „Tunnel“ wählen sie den von ihnen vorher konfigurierten VPN-Tunnel aus.**

### Outgoing-Policy VPN:

The screenshot shows the NetGuardian web interface in Microsoft Internet Explorer. The browser address bar shows <http://192.168.2.1/>. The left sidebar contains a navigation menu with the following items: System, Interface, Policy Object, Policy, Outgoing (selected), Incoming, WAN To DMZ, LAN To DMZ, DMZ To WAN, DMZ To LAN, Mail Security, IDP, Anomaly Flow IP, and Monitor. The main content area is titled "Policy > Outgoing" and displays the "Modify Policy" form. The form fields are as follows:

Field	Value
Comment	ALLTEST_OUT (Max. 32 characters)
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	None
Tunnel	ALLTEST2
Action	PERMIT
Traffic Log	<input checked="" type="checkbox"/> Enable
Statistics	<input checked="" type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> Enable
MAX. Concurrent Sessions	0
QoS	None

At the bottom right of the form are "OK" and "Cancel" buttons. The status bar at the bottom of the browser window shows "Fertig" and "Internet".

### Outgoing-Policy:

The screenshot shows the NetGuardian web interface in Microsoft Internet Explorer. The browser address bar shows <http://192.168.2.1/>. The left sidebar contains a navigation menu with the following items: System, Interface, Policy Object, Policy, Outgoing (selected), Incoming, WAN To DMZ, LAN To DMZ, DMZ To WAN, DMZ To LAN, Mail Security, IDP, Anomaly Flow IP, and Monitor. The main content area is titled "Policy > Outgoing" and displays the "Modify Policy" form. The form fields are as follows:

Field	Value
Comment	(Max. 32 characters)
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	None
Tunnel	None
Action	PERMIT
Traffic Log	<input checked="" type="checkbox"/> Enable
Statistics	<input checked="" type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> Enable
MAX. Concurrent Sessions	0
QoS	None

At the bottom right of the form are "OK" and "Cancel" buttons. The status bar at the bottom of the browser window shows "Fertig" and "Internet".



Wenn sie beide Policies konfiguriert haben erhalten sie folgende Übersichtsseite. **Wichtig ist, dass die VPN-Policy als erster Eintrag in der Liste steht!**

NetGuardian - Microsoft Internet Explorer

Adresse: <http://192.168.2.1/>

**ALLNET**

System  
Interface  
Policy Object  
Policy

- Outgoing
  - Incoming
  - WAN To DMZ
  - LAN To DMZ
  - DMZ To WAN
  - DMZ To LAN
- Mail Security
- IDP
- Anomaly Flow IP
- Monitor

Policy > Outgoing

Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	ANY	VPN		Modify Remove Pause	To 1
Inside_Any	Outside_Any	ANY	✓		Modify Remove Pause	To 2

New Entry

Fertig

Internet

## Incoming Policy VPN:

NetGuardian - Microsoft Internet Explorer

Adresse: http://192.168.2.1/

**ALLNET**

System  
Interface  
Policy Object  
Policy  
  ↳ Outgoing  
  ↳ Incoming  
  ↳ WAN To DMZ  
  ↳ LAN To DMZ  
  ↳ DMZ To WAN  
  ↳ DMZ To LAN  
Mail Security  
IDP  
Anomaly Flow IP  
Monitor

Policy > Incoming

Comment: ALLTEST\_JN (Max. 32 characters)

Modify Policy

Source Address	Outside_Any
Destination Address	Inside_Any
Service	ANY
Schedule	None
Tunnel	ALLTEST2
Action	PERMIT
Traffic Log	<input checked="" type="checkbox"/> Enable
Statistics	<input checked="" type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
MAX. Concurrent Sessions	0
QoS	None
NAT	<input type="checkbox"/> Enable

OK Cancel

Fertig Internet

## Incoming Policy:

NetGuardian - Microsoft Internet Explorer

Adresse: http://192.168.2.1/

**ALLNET**

System  
Interface  
Policy Object  
Policy  
  ↳ Outgoing  
  ↳ Incoming  
  ↳ WAN To DMZ  
  ↳ LAN To DMZ  
  ↳ DMZ To WAN  
  ↳ DMZ To LAN  
Mail Security  
IDP  
Anomaly Flow IP  
Monitor

Policy > Incoming

Comment: (Max. 32 characters)

Modify Policy

Source Address	Outside_Any
Destination Address	Inside_Any
Service	ANY
Schedule	None
Tunnel	None
Action	PERMIT
Traffic Log	<input checked="" type="checkbox"/> Enable
Statistics	<input checked="" type="checkbox"/> Enable
IDP	<input type="checkbox"/> Enable
MAX. Concurrent Sessions	0
QoS	None
NAT	<input checked="" type="checkbox"/> Enable

OK Cancel

Fertig Internet



Wenn sie beide Policies konfiguriert haben erhalten sie folgende Übersichtsseite. **Wichtig ist, dass die VPN-Policy als erster Eintrag in der Liste steht!**

NetGuardian - Microsoft Internet Explorer

Adresse <http://192.168.2.1/>

**ALLNET**

System  
Interface  
Policy Object  
Policy  
  ↳ Outgoing  
  ↳ **Incoming**  
  ↳ WAN To DMZ  
  ↳ LAN To DMZ  
  ↳ DMZ To WAN  
  ↳ DMZ To LAN  
Mail Security  
IDP  
Anomaly Flow IP  
Monitor

Policy > Incoming

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Inside_Any(Routing)	ANY	VPN		Modify Remove Pause	To 1
Outside_Any	Inside_Any(Routing)	ANY			Modify Remove Pause	To 2

New Entry

Fertig Internet

## Schritt 6: Prüfen ob Tunnel aufgebaut wurde

Um zu sehen ob ihr Tunnel aufgebaut wurde können sie im Menü „Monitor → Statistics → Policy“ folgenden Screen aufrufen:

The screenshot shows the ALLNET NetGuardian web interface in a Microsoft Internet Explorer browser window. The address bar shows the URL <http://192.168.2.1/>. The left sidebar contains a navigation menu with the following items: System, Interface, Policy Object, Policy, Mail Security, IDP, Anomaly Flow IP, Monitor, Log, Accounting Report, Statistics, WAN, Policy (highlighted), and Status. The main content area displays the 'Monitor > Statistics > Policy' view, which contains a table with the following data:

Source	Destination	Service	Action	Time					
Inside_Any	Outside_Any	ANY	VPN	Minute	Hour	Day	Week	Month	Year
Outside_Any	Inside_Any(Routing)	ANY	VPN	Minute	Hour	Day	Week	Month	Year

Sofern hier bei Action ein grünes VPN-Icon zu sehen ist wurde der Tunnel erfolgreich aufgebaut.