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:

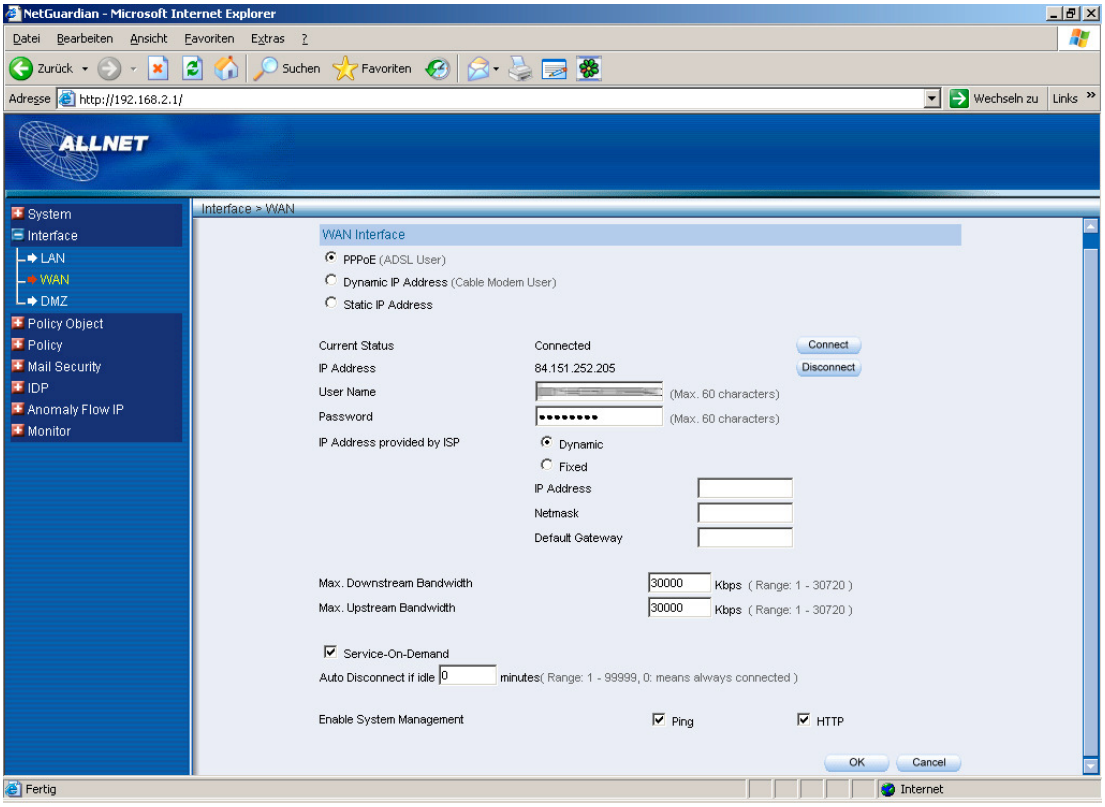
LAN1:
Router IP: 192.168.1.1

LAN2:
Router IP: 192.168.2.1

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

Schritt 1: Einrichtung WAN-Port

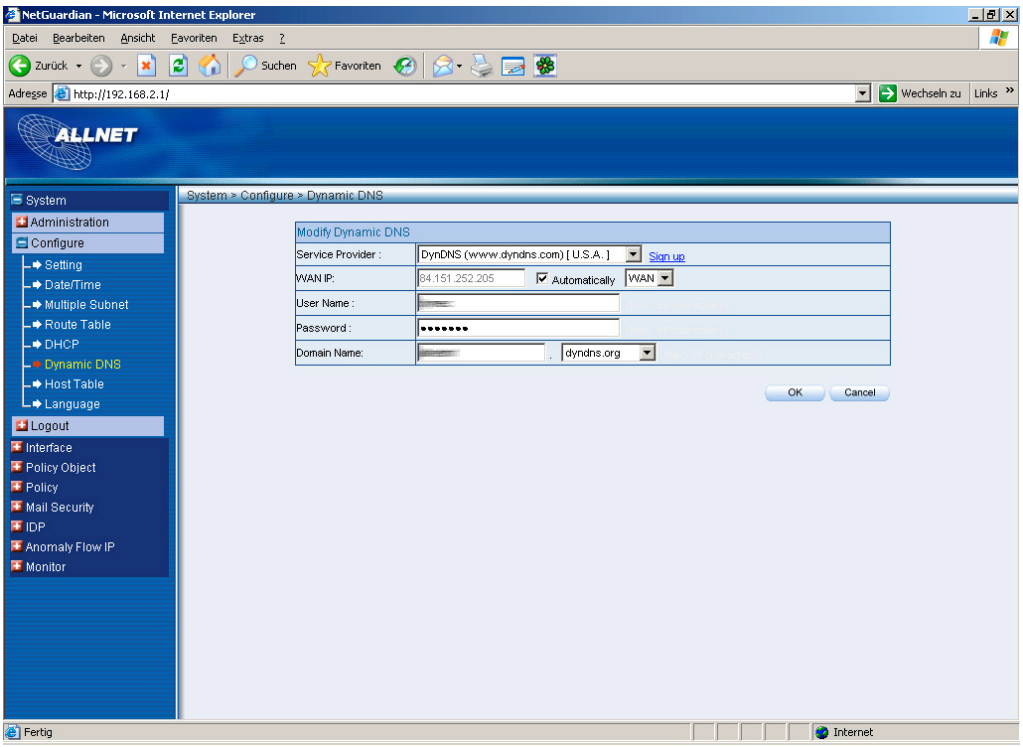
Öffnen sie das Menü „Interface → WAN“ und tragen sie dort ihre Internetzugangsdaten ein und speichern diese über einen Klick auf „OK“ ab.



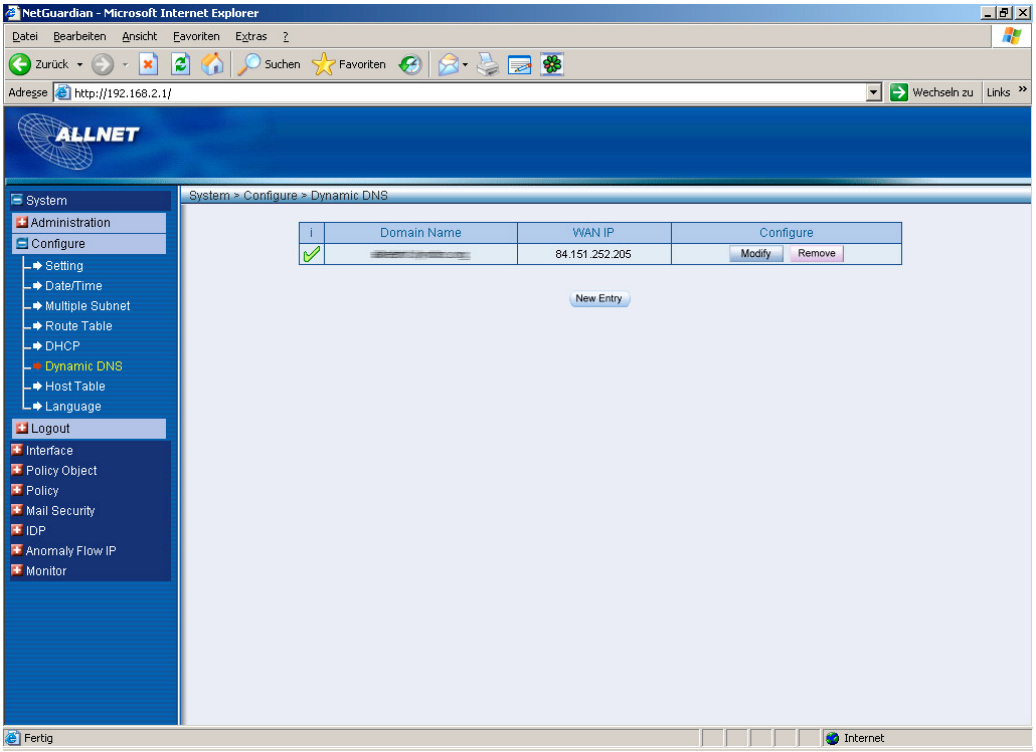
Schritt 2: Einrichtung DynDNS

Sie benötigen hierfür einen dynamischen Domainnamen. Diesen erhalten sie beispielsweise auf www.dyndns.org. 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:

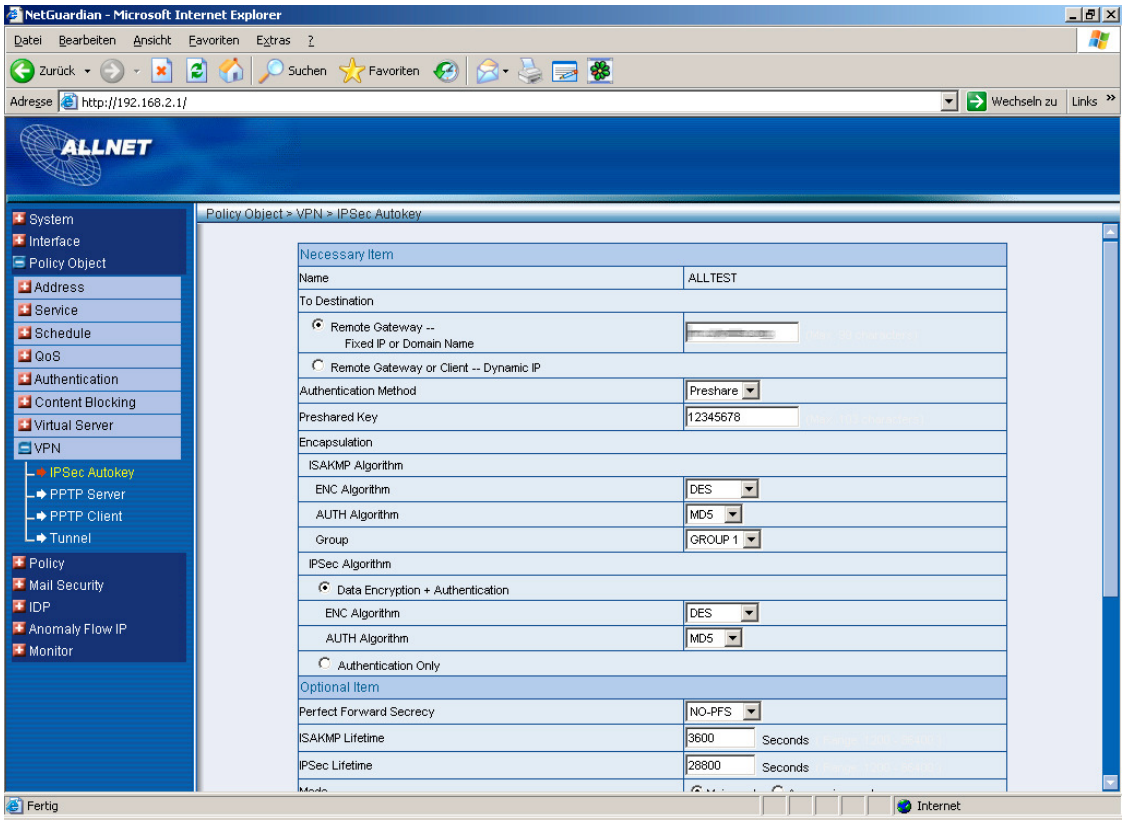


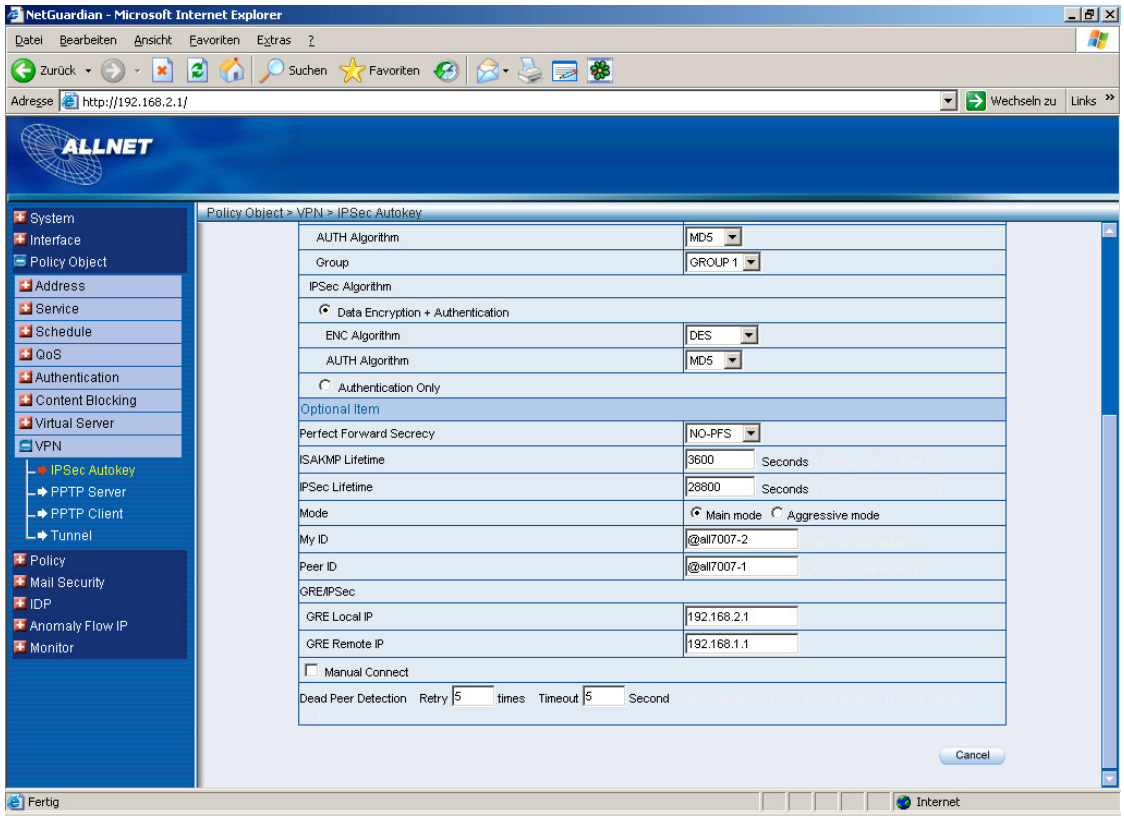
Schritt 3: Einrichtung IPSec-Policy

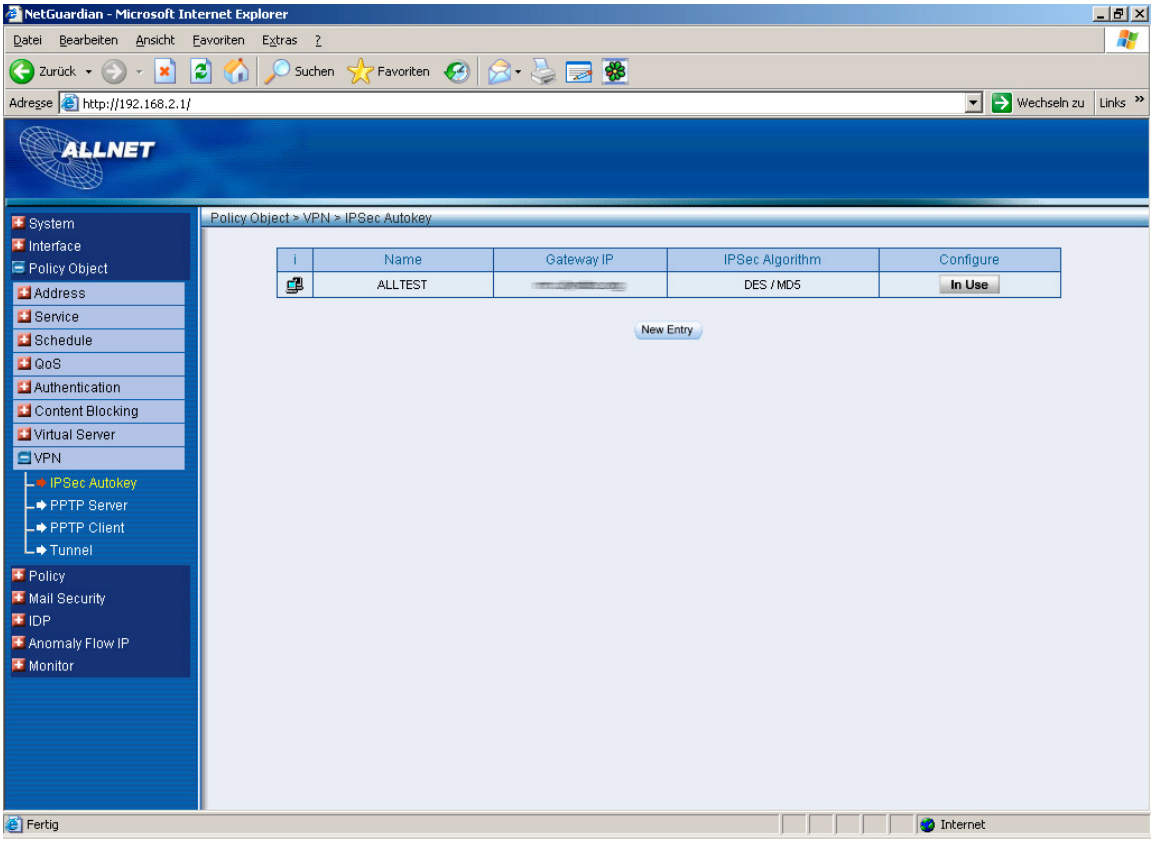
Für die Konfiguration der IP-Sec-Policy begeben sie sich bitte in das Menü „Policy Object → VPN → IPSec Autokey“. Tragen sie hier ihre Daten gemäß der Musterkonfiguration ein. Wichtig sind hierbei folgende Punkte:

- 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.



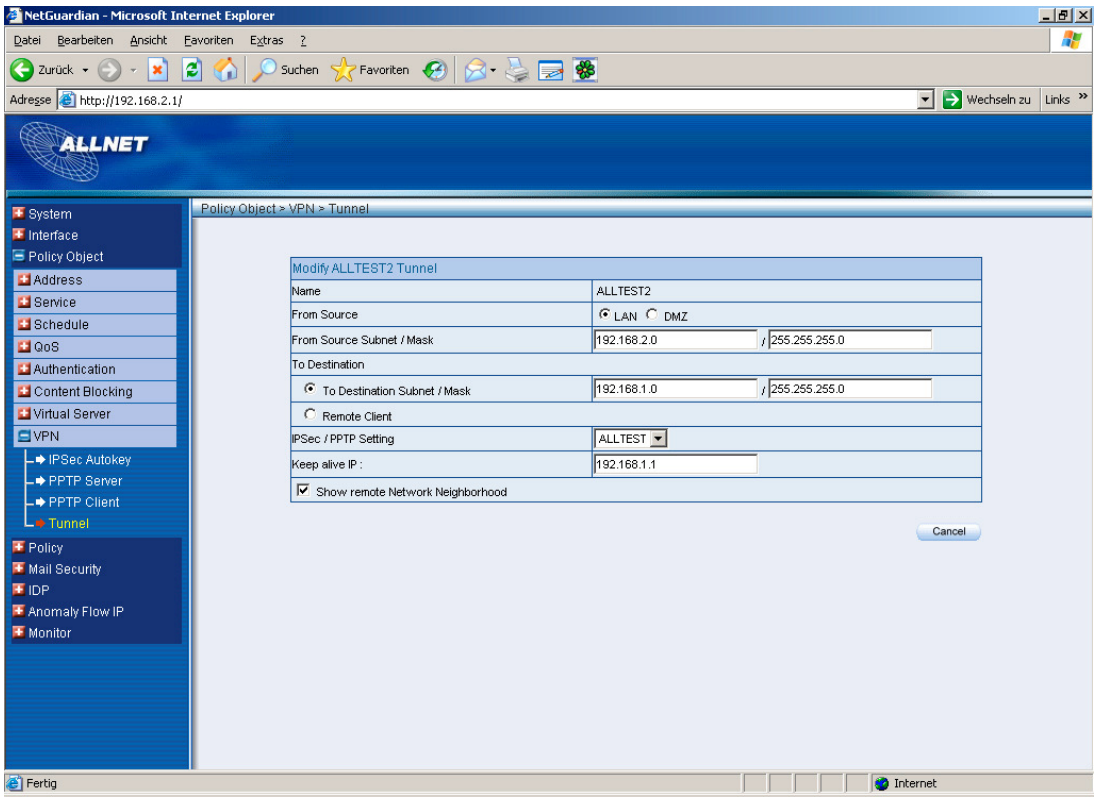


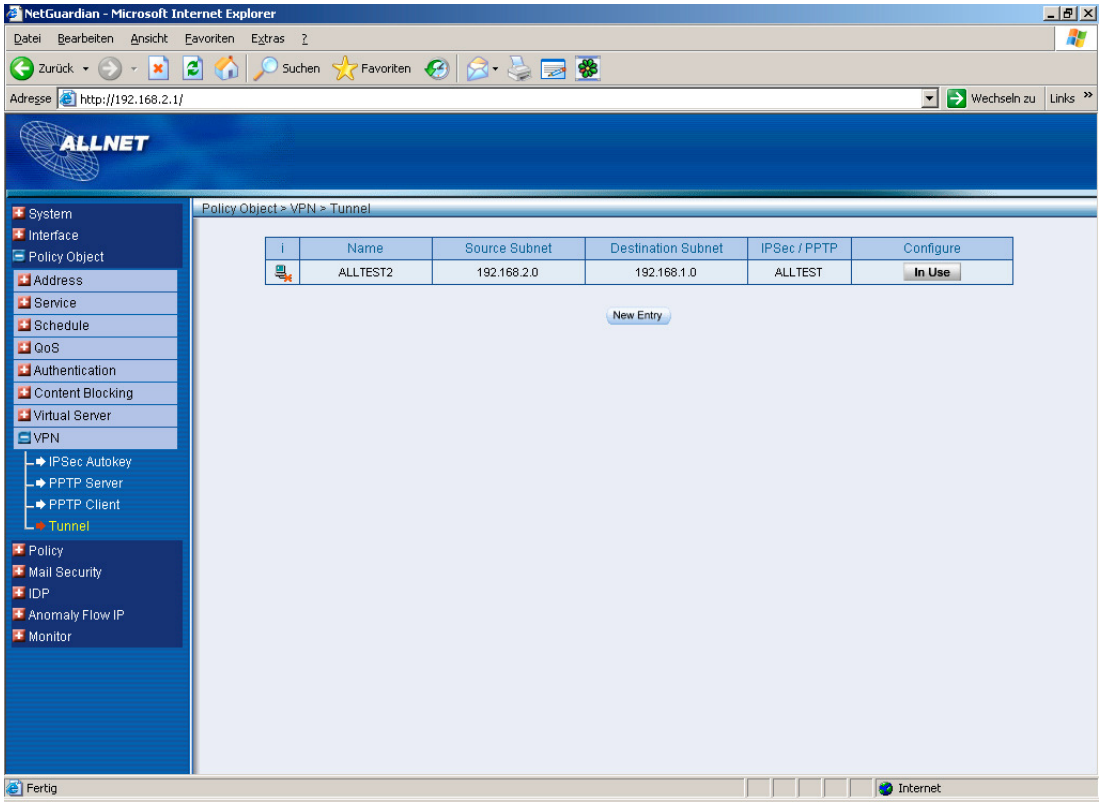


Schritt 4: Konfiguration des Tunnels

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
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück Suchen Favoriten
Adresse http://192.168.2.1/
Wechseln zu Links
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
LAN DMZ
From Source Subnet / Mask
192.168.2.0 / 255.255.255.0
To Destination
To Destination Subnet / Mask
192.168.1.0 / 255.255.255.0
Remote Client
IPSec / PPTP Setting
ALLTEST
Keep alive IP :
192.168.1.1
Show remote Network Neighborhood
Cancel
Fertig
Internet

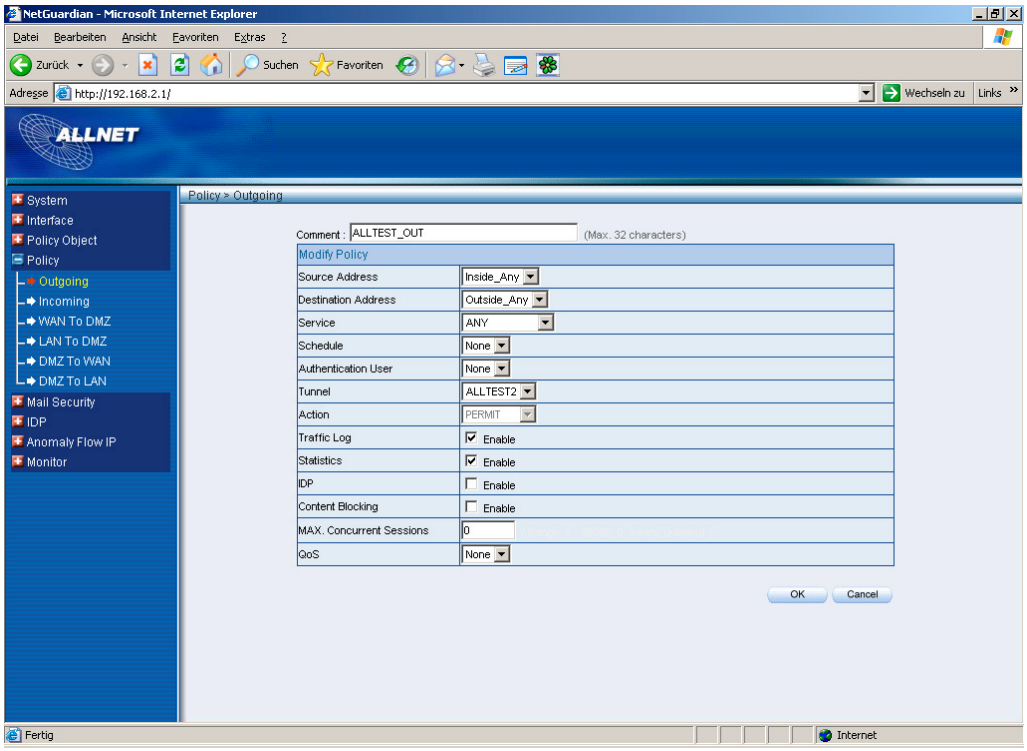

NetGuardian - Microsoft Internet Explorer
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück Suchen Favoriten
Adresse http://192.168.2.1/
Wechseln zu Links
ALLNET
System
Interface
Policy Object
Address
Service
Schedule
QoS
Authentication
Content Blocking
Virtual Server
VPN
IPSec Autokey
PPTP Server
PPTP Client
Tunnel
Policy
Mail Security
IDP
Anomaly Flow IP
Monitor
Policy Object > VPN > Tunnel
i
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 Policys

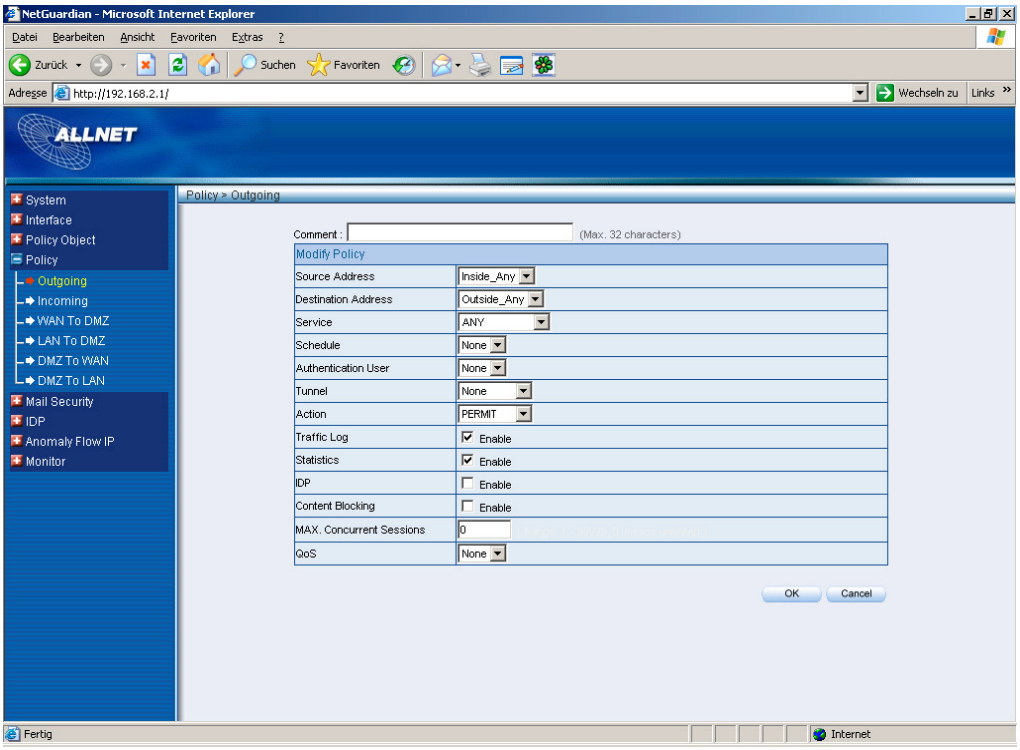
Damit ihr VPN funktioniert müssen sie sowohl eine Outgoing wie auch eine Incoming Policy für das VPN definieren. Zusätzlich muss jeweils eine Outgoing und eine Incoming Policy für den Internettraffic vergeben werden. Diese müssen wie folgt konfiguriert werden (Traffic Log und Statistic können, müssen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

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

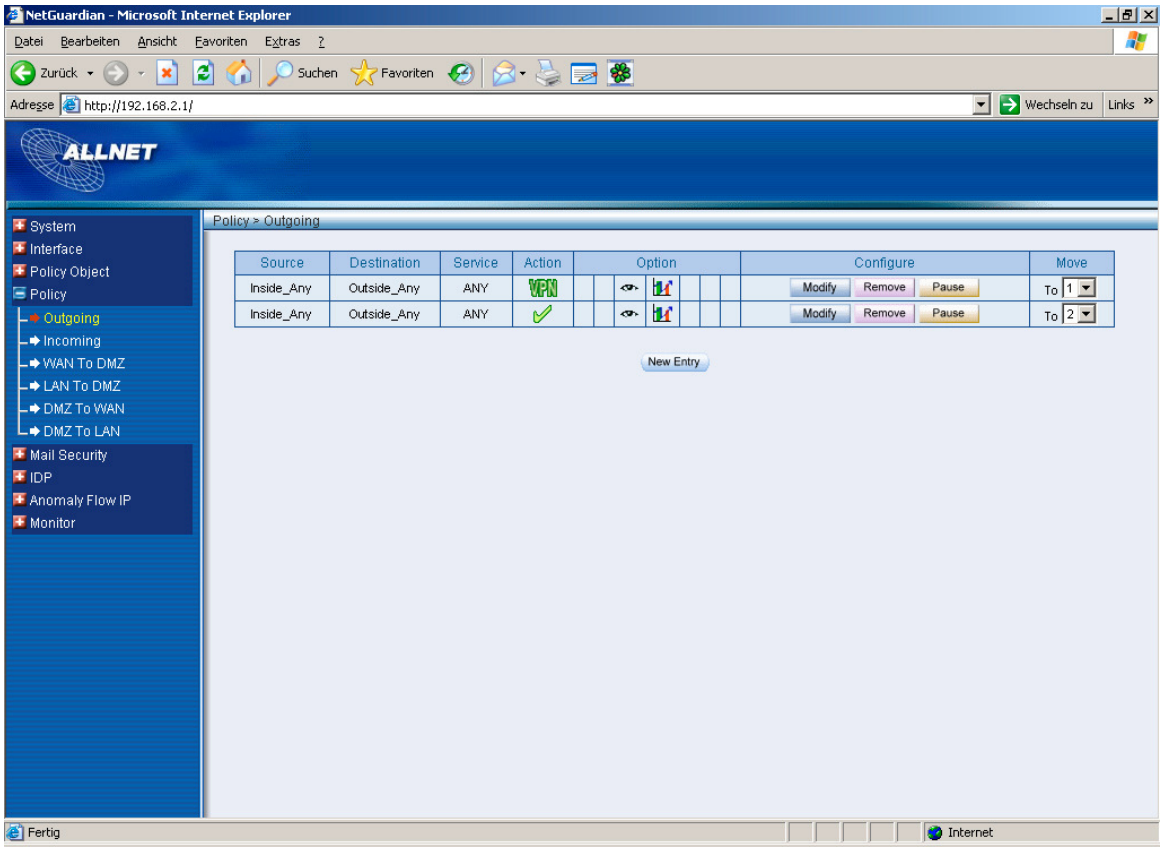
Outgoing-Policy VPN:



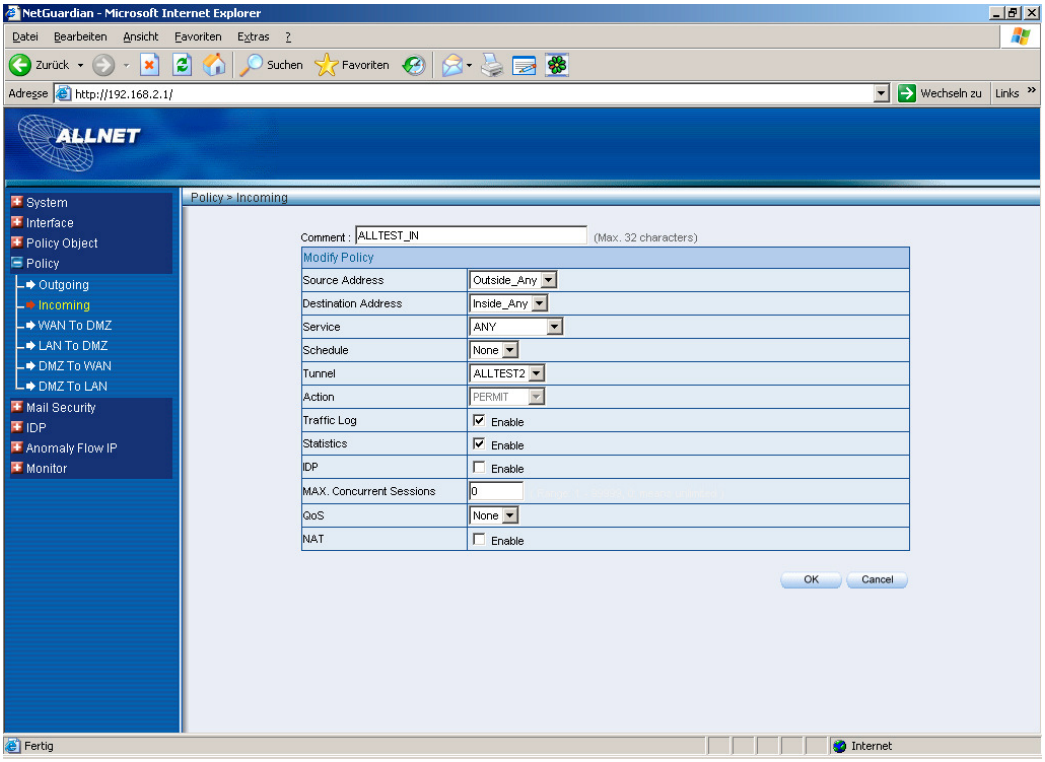
Outgoing-Policy:



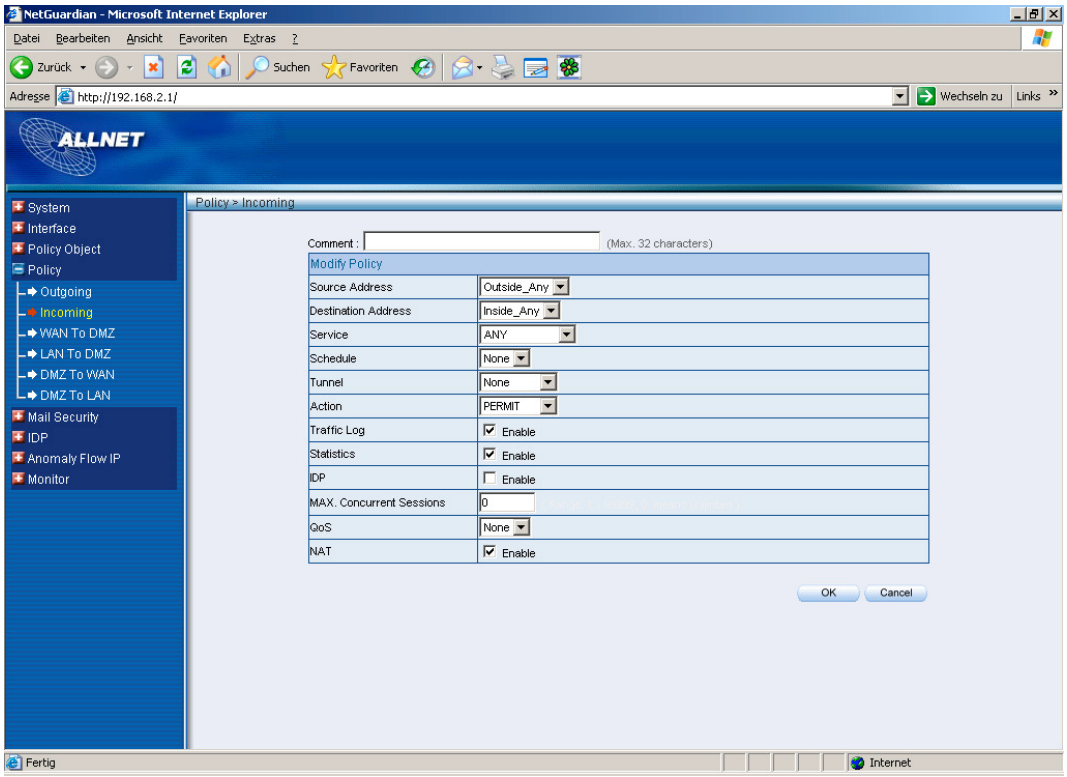
Wenn sie beide Policies konfiguriert haben erhalten sie folgende Übersichtsseite. **Wichtig ist, dass die VPN-Policy als erster Eintrag in der Liste steht!**



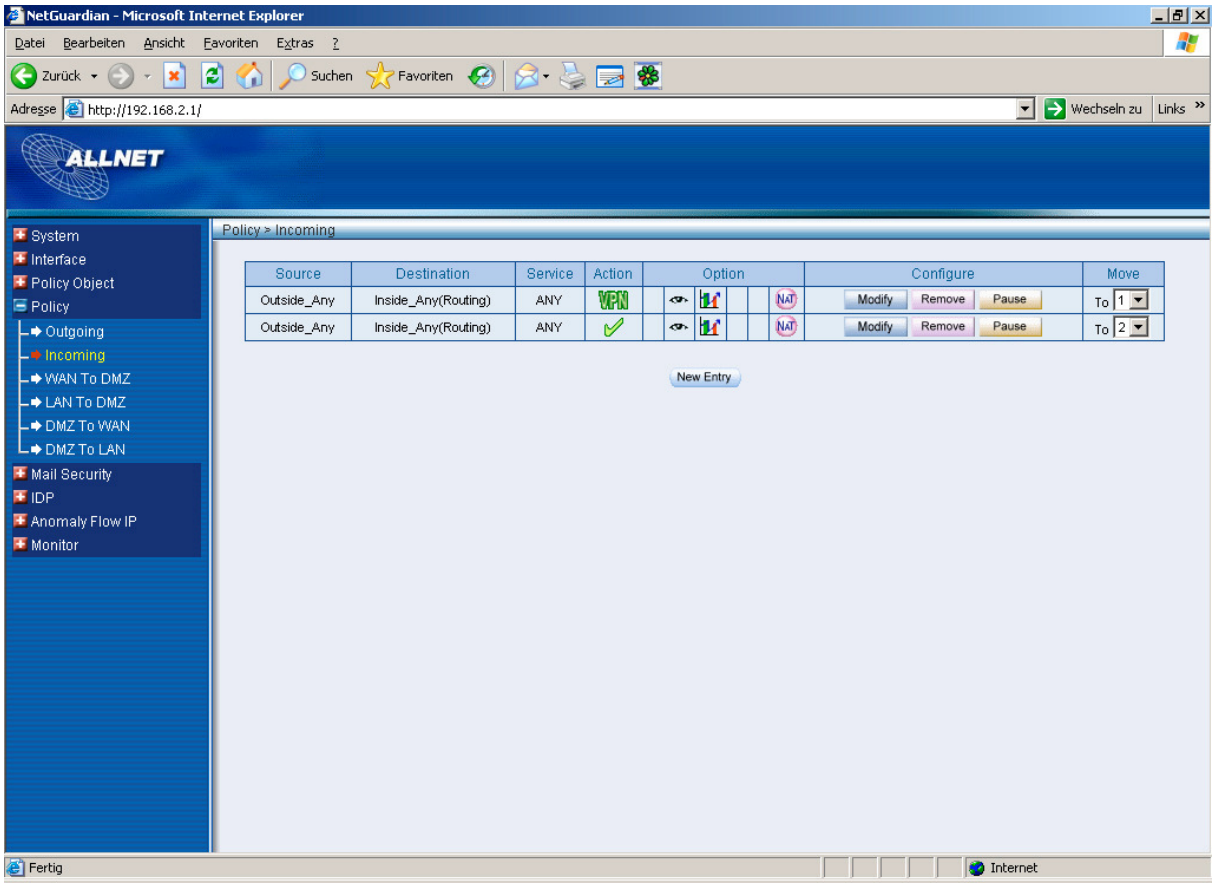
Incoming Policy VPN:



Incoming Policy:

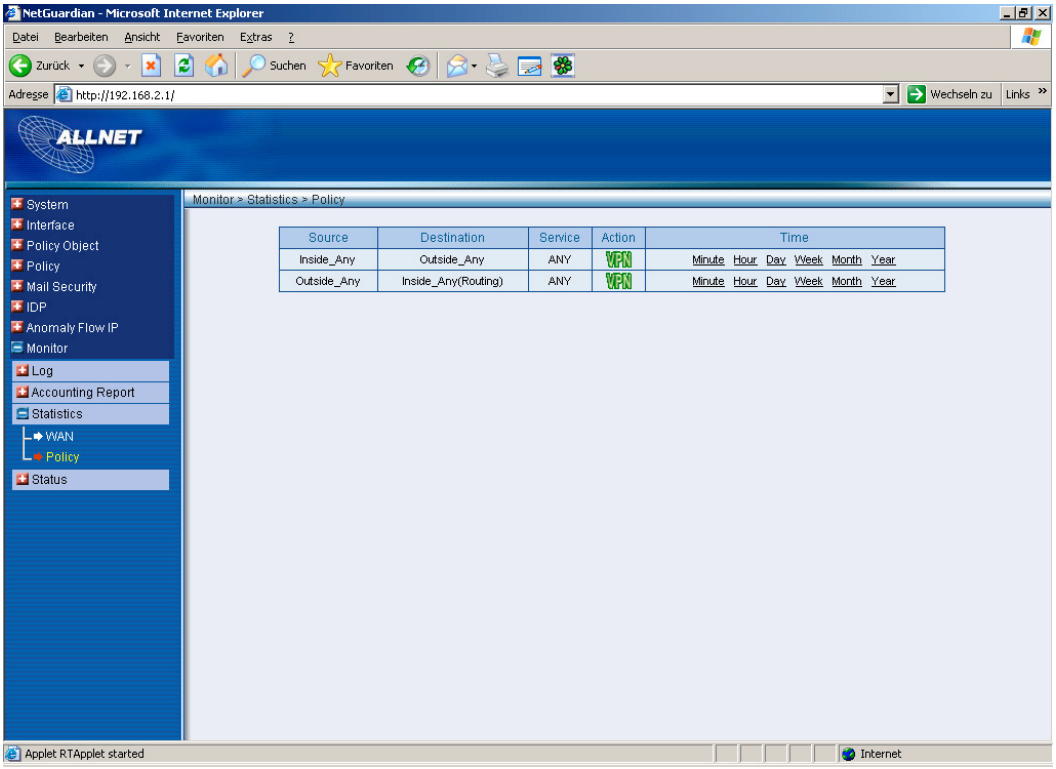


Wenn sie beide Policies konfiguriert haben erhalten sie folgende Übersichtsseite. **Wichtig ist, dass die VPN-Policy als erster Eintrag in der Liste steht!**



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:



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