

ISA Server 2004 – Erstellen eines neuen Netzwerkes - Von Marc Grote

Die Informationen in diesem Artikel beziehen sich auf:
Microsoft ISA Server 2004

Einleitung

Microsoft ISA Server 2004 bietet als erste Microsoft Firewall die Möglichkeit, mehrere Netzwerkobjekte zu definieren und diese Netzwerkobjekte mit beliebigen anderen Netzwerkobjekten in Beziehung zu setzen.

Netzwerke

Edgefirewall

Das Diagramm zeigt die Konfiguration einer Edgefirewall. Ein lokaler Host (links) ist über eine Firewall (orange) mit dem Externen Netzwerk (Internet) verbunden. Das Externe Netzwerk ist weiter mit dem VPN-Clientnetzwerk verbunden.

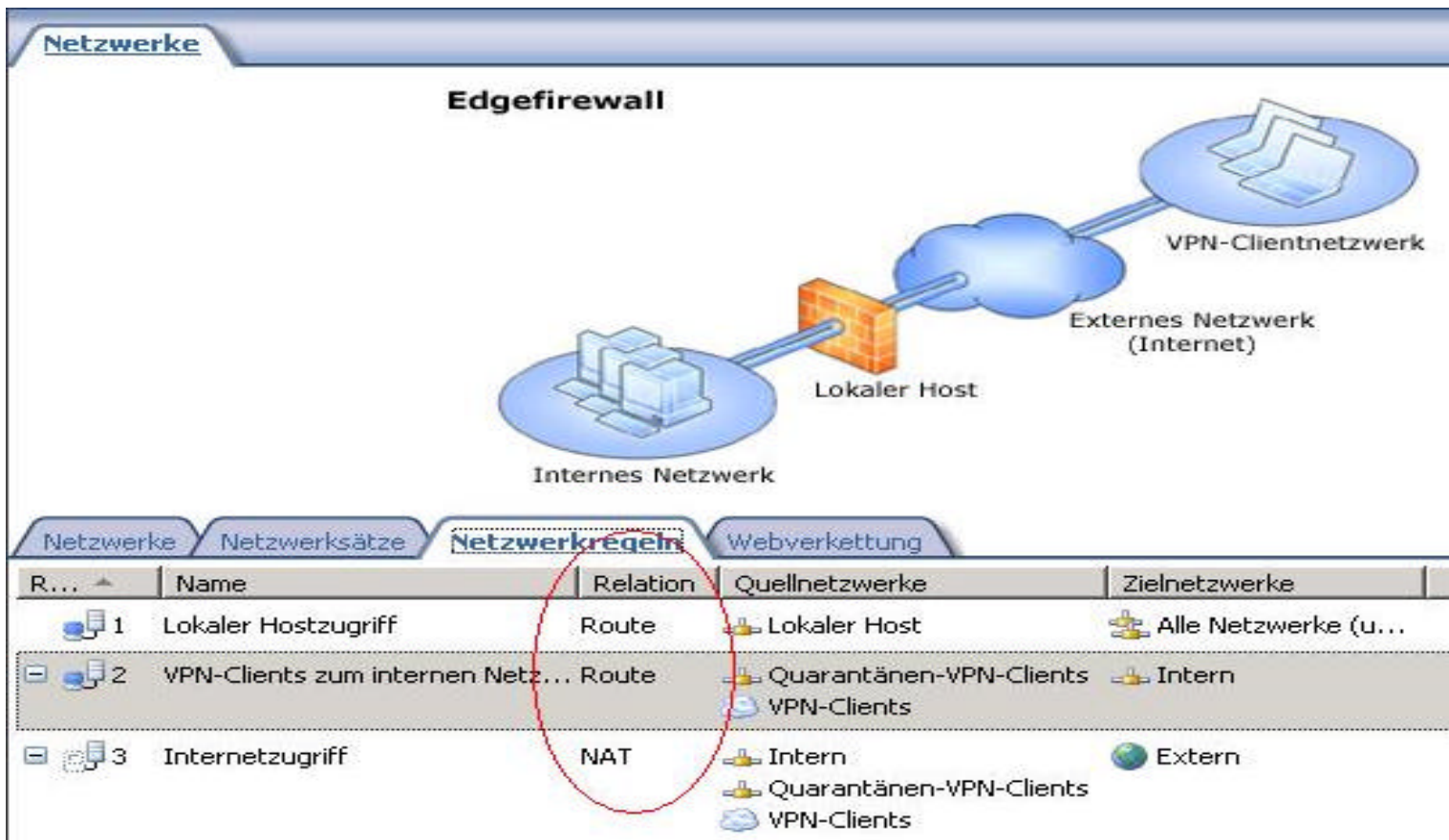
Netzwerke | Netzwerksätze | Netzwerkregeln | Webverkettung

Name	Adressbereiche	Beschreibung
Extern	Für die ISA Server-Netzwerke e...	Das vordefinierte Netzwerkobjekt, das das Internet darstellt.
Intern	192.168.1.2 - 192.168.1.255	Das Netzwerk, das das interne Netzwerk darstellt.
Lokaler Host	Mit diesem Netzwerk sind keine ...	Das vordefinierte Netzwerkobjekt, das den ISA Server-Computer
Quarantänen-VPN-Clients	Diesem Netzwerk sind zurzeit k...	Das vordefinierte Netzwerk, das die Clientcomputer darstellt, die
VPN-Clients	Diesem Netzwerk sind zurzeit k...	Das vordefinierte dynamische Netzwerkobjekt, das die Clientcomp

Diese Netzwerke können vom ISA Administrator in eine ...

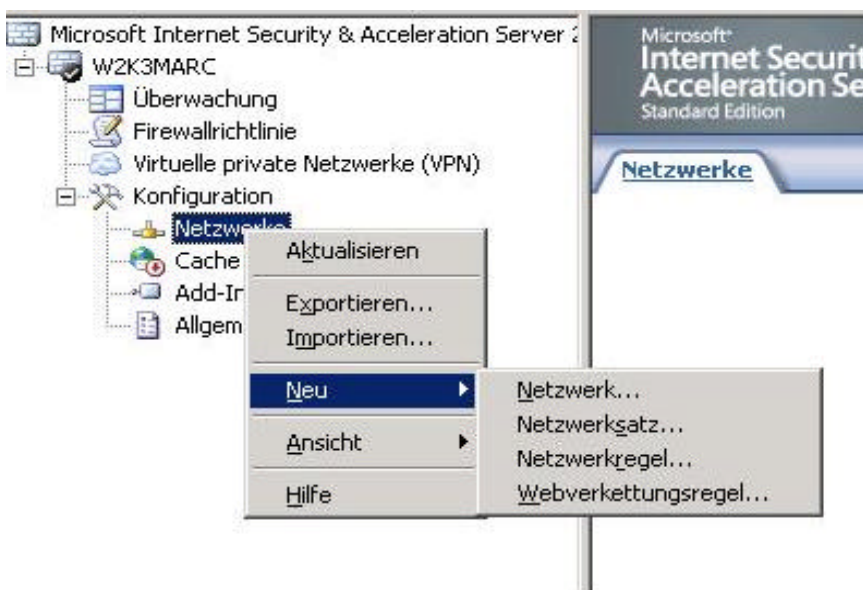
- ⌘ NAT (Network Address Translation) oder
- ⌘ ROUTE

Beziehung zu einander gesetzt werden.



Dieser Artikel beschreibt die Erstellung eines neuen Netzwerkes mit dem Ziel für die Forschungsabteilung, welche sich in einem eigenen IP-Subnetz befindet, ein neues Netzwerk anzulegen, und den PCs in diesem Netzwerk den Zugriff auf Ressourcen im Internet zu ermöglichen.

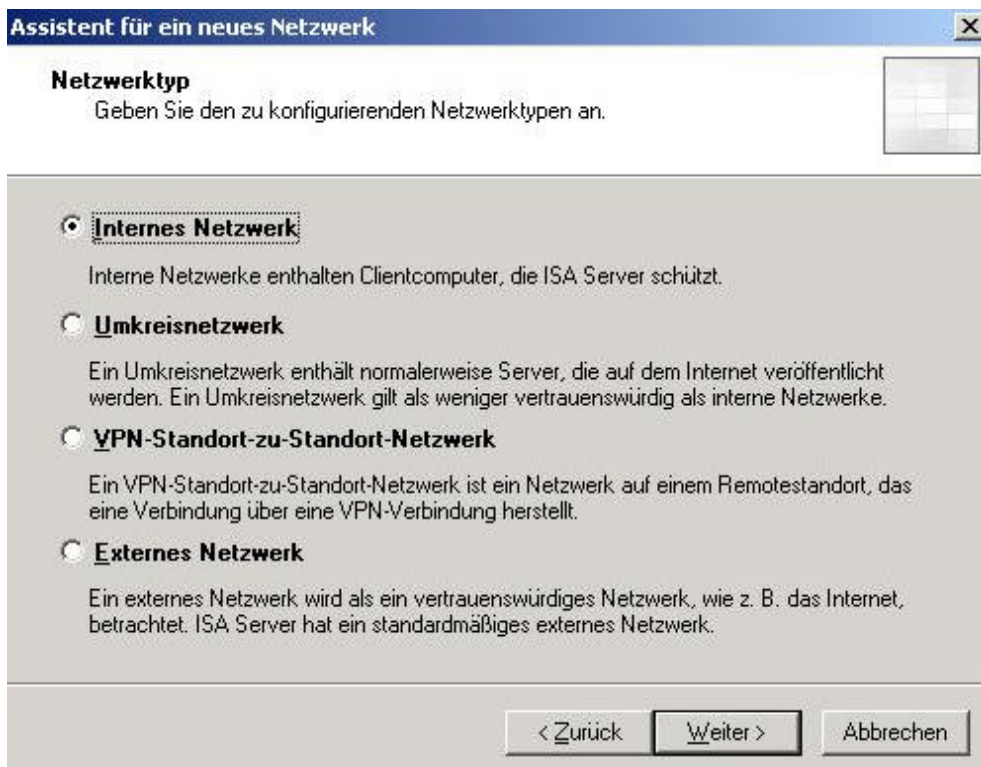
Starten Sie die ISA Server Verwaltungskonsole und klicken Sie mit der rechten Maustaste unterhalb von **Konfiguration** auf **Netzwerke**. Klicken Sie im Kontextmenü auf **Netzwerk**, um ein neues Netzwerk zu erstellen.



Geben Sie dem neuen Netzwerk einen Namen.



Geben Sie jetzt den Typ des zu erstellenden Netzwerkes an. Wir wählen in unserem Beispiel **Internes Netzwerk**.

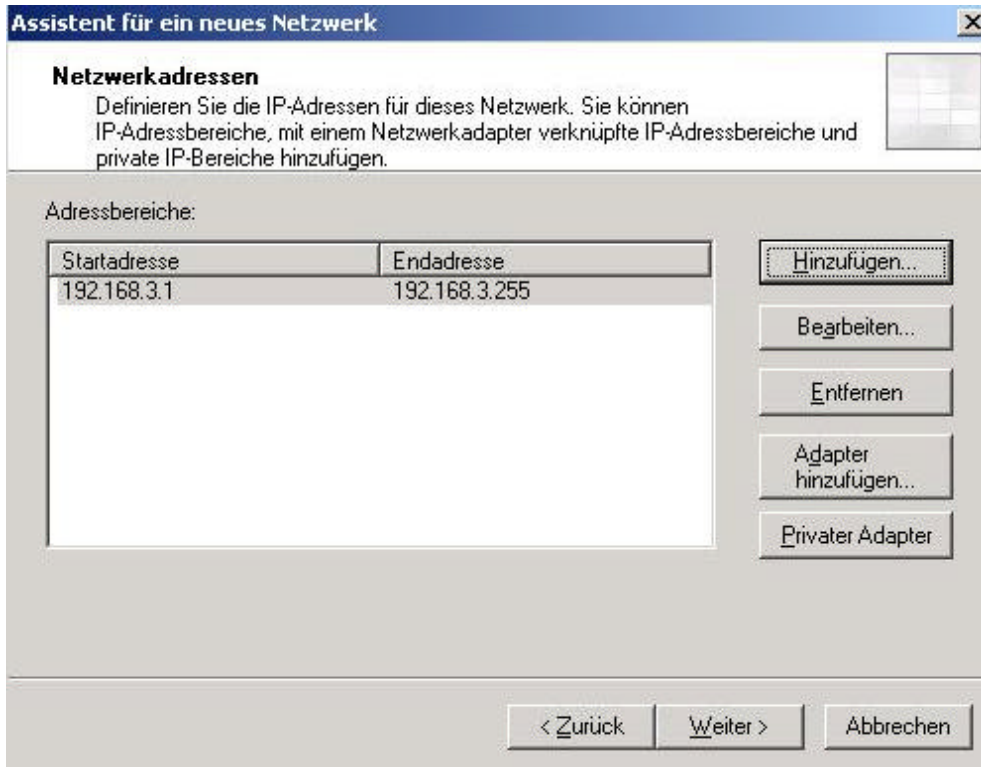


Die Bedeutung der Netzwerke ist selbsterklärend. Es sei hier nur ein Hinweis auf die Bedeutung des Umkreisnetzwerk gegeben.

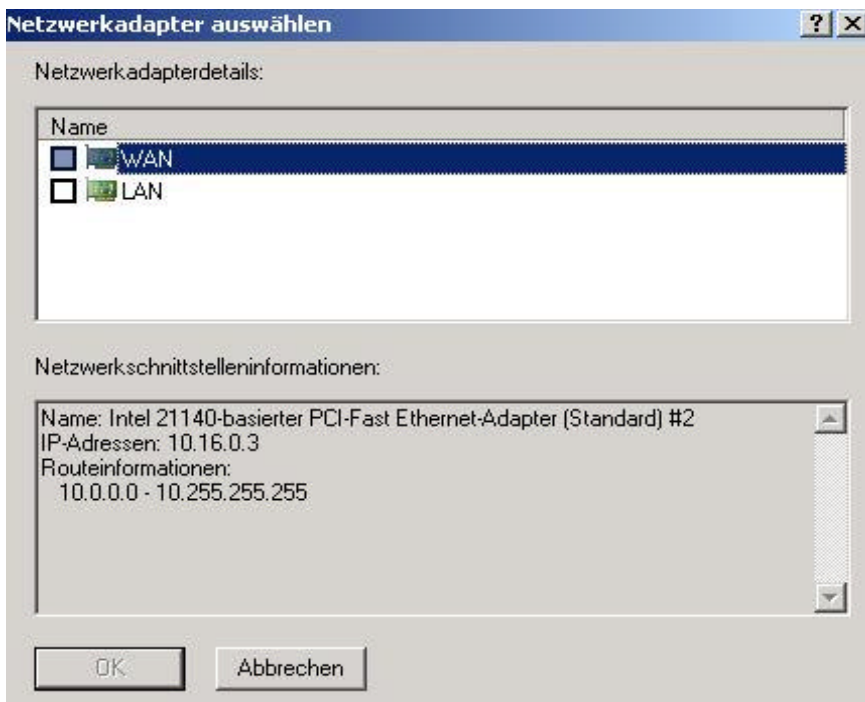
Als Umkreisnetzwerk bezeichnet man auch die DMZ = DeMilitarisierte Zone. Der Begriff DMZ sollte den meisten Lesern geläufiger sein.

Geben Sie jetzt einen IP-Adressbereich für das neue Netzwerk an. in diesem Beispiel wählen wir den

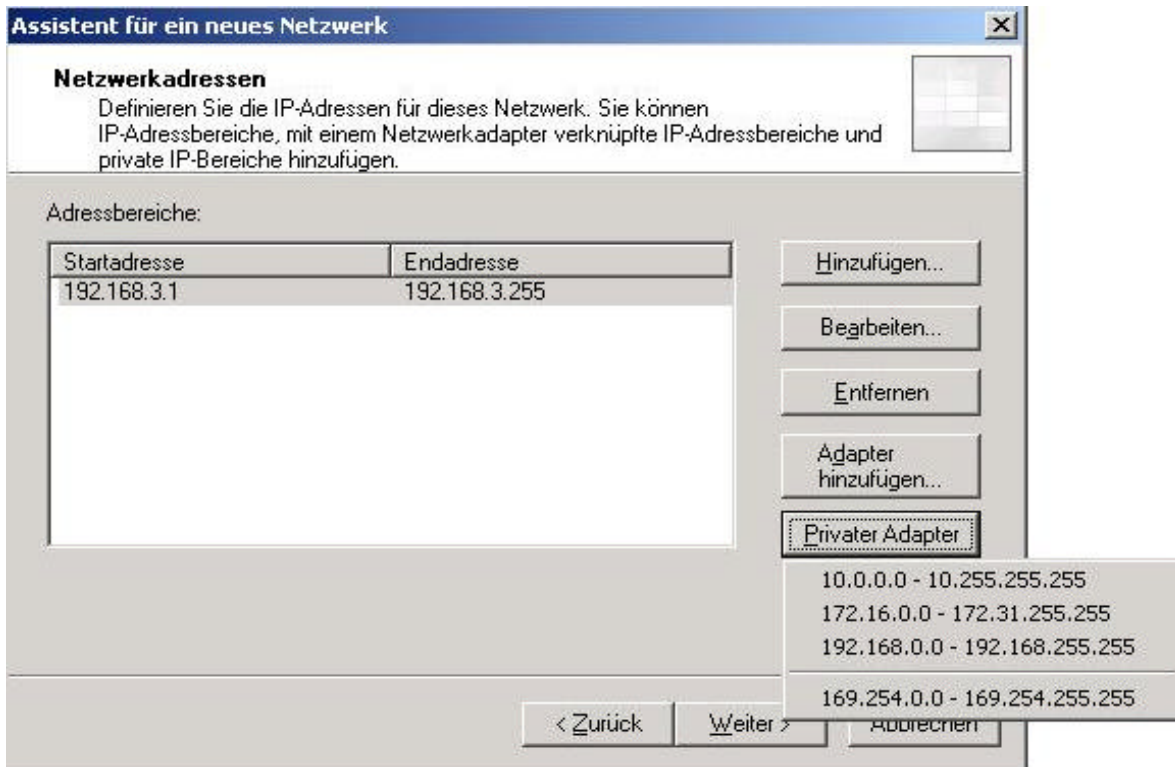
Netzwerkbereich **192.168.3.1 - 192.168.3.255**.



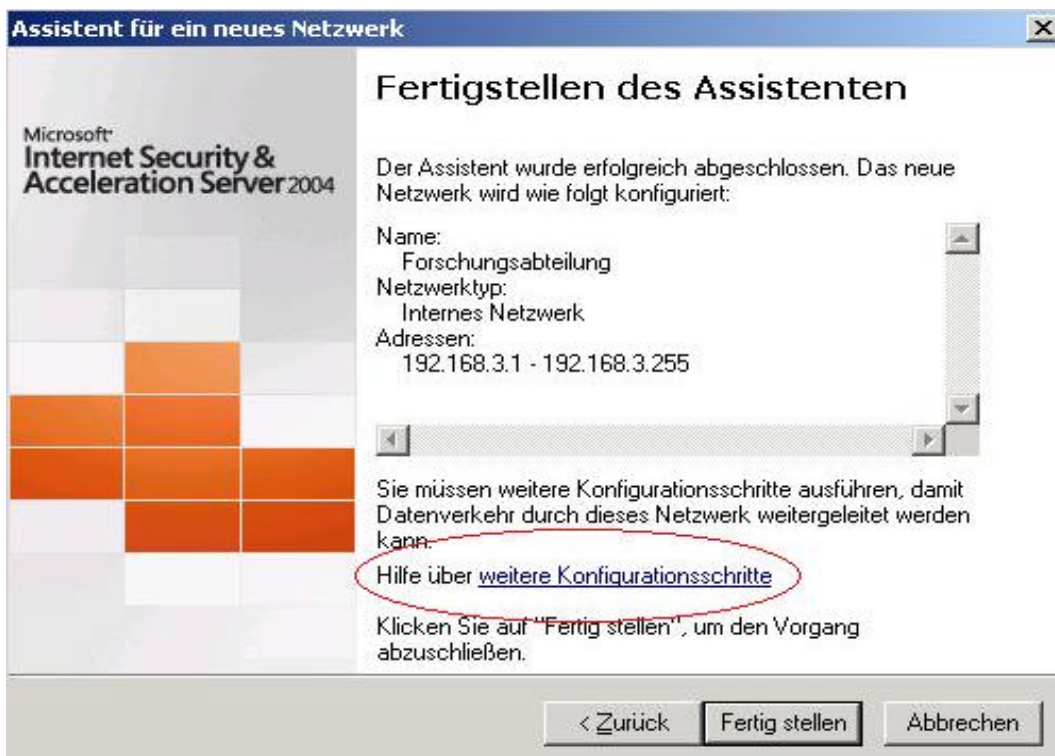
Sie können auch einen Netzwerkadapter auswählen, aus dem der ISA Server Assistent den neuen Netzwerkbereich erstellen soll. Klicken Sie dazu auf **Adapter hinzufügen**.



Haben Sie INTERN einen Standard Netzwerkbereich aus den privaten Netzwerken der Klasse A / B und C, können Sie hier auch auf **Privater Adapter** klicken und den Netzwerkbereich hinzufügen.



Der Assistent hat alle Informationen, welche er zur Erstellung des Netzwerkes benötigt, gesammelt und zeigt Ihnen diese Informationen in einer Zusammenfassung an. Klicken Sie unbedingt auf **Hilfe über weitere Konfigurationsschritte**, denn noch ist die Konfiguration nicht vollständig.



Schritte zur Netzwerkkonfiguration

Damit neu erstellte Netzwerke Datenverkehr senden oder empfangen können, müssen weitere Konfigurationsschritte durchgeführt werden. Diese Schritte sind vom Typ des erstellten Netzwerkes abhängig.

Internes, externes und Umkreisnetzwerk

Damit Clients in diesen Netzwerken Datenverkehr senden und empfangen können, müssen Sie die folgenden Schritte durchführen:

Erstellen Sie eine Netzwerkregel, die Datenverkehr zu und von diesem Netzwerk zulässt. Entsprechende Anweisungen finden Sie unter Erstellen einer Netzwerkregel.

Erstellen Sie Firewallrichtlinienregeln, die Datenverkehr zu und von diesem Netzwerk zulassen. Entsprechende Anweisungen finden Sie unter Erstellen einer Zugriffsregel, Erstellen einer Webveröffentlichungsregel, Erstellen einer Serververöffentlichungsregel oder Veröffentlichen eines Mailservers.

Standort-zu-Standort-VPN mit IPSec

Damit Clients Verbindungen aus einem VPN (Virtual Private Network) mit IPSec (Internet Protocol Security) herstellen können, müssen Sie folgende Schritte durchführen:

Erstellen Sie eine Netzwerkregel, die Datenverkehr zu und von diesem Netzwerk zulässt.

Erstellen Sie Zugriffsregeln, die Datenverkehr zu und von diesem Netzwerk zulassen.

Überprüfen Sie die IPSec-Protokolleinstellungen mithilfe der Eigenschaften des neu erstellten Netzwerks.

Standort-zu-Standort-VPN mit PPTP oder L2TP

Damit Clients eine Verbindung aus dem VPN über PPTP (Point-to-Point Tunneling-Protokoll) oder L2TP (Layer Two Tunneling-Protokoll) herstellen können, müssen Sie die folgenden Schritte durchführen:

Erstellen Sie einen Benutzer mit dem Namen des neuen Netzwerks. Geben Sie dann für die RAS-Berechtigungen Zulassen an. Entsprechende Anweisungen finden Sie unter Erstellen von Benutzern und Gruppen für Remote-VPN-Clients.

Erstellen Sie Netzwerkregeln, die Datenverkehr zu und von diesem Netzwerk zulassen.

Erstellen Sie Zugriffsregeln, die Datenverkehr zu und von diesem Netzwerk zulassen.

Klicken Sie in der ISA Verwaltungskonsole unterhalb von **Konfiguration** auf **Netzwerke** und überprüfen Sie im Reiter **Netzwerke**, ob das entsprechende Netzwerk korrekt erstellt wurde.

Netzwerke Netzwerksätze Netzwerkregeln Webverkettung			
Name	Adressbereiche	Beschreibung	
 Extern	Für die ISA Server-Netzwerke e...	Das vordefinierte Netzwerkobjekt, das das Internet darstellt.	
 Forschungsabteilung	192.168.3.1 - 192.168.3.255		
 Intern	192.168.1.2 - 192.168.1.255	Das Netzwerk, das das interne Netzwerk darstellt.	
 Lokaler Host	Mit diesem Netzwerk sind keine ...	Das vordefinierte Netzwerkobjekt, das den ISA Server-Com...	
 Quarantänen-VPN-Clients	Diesem Netzwerk sind zurzeit k...	Das vordefinierte Netzwerk, das die Clientcomputer darstel...	
 VPN-Clients	Diesem Netzwerk sind zurzeit k...	Das vordefinierte dynamische Netzwerkobjekt, das die Clie...	

Im nächsten Schritt ist die Erstellung einer Netzwerkregel notwendig. Mit Hilfe der Netzwerkregel regeln Sie wie das neue Netzwerk mit dem Zielnetzwerk kommunizieren soll.



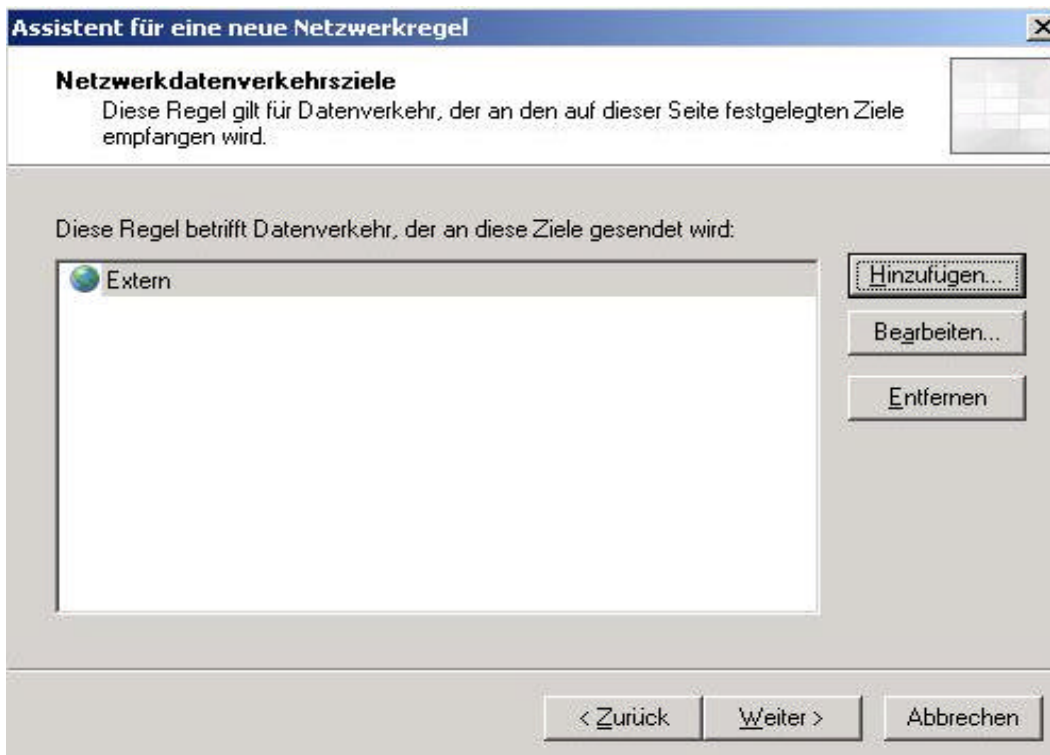
Geben Sie der Netzwerkregel einen sprechenden Namen.



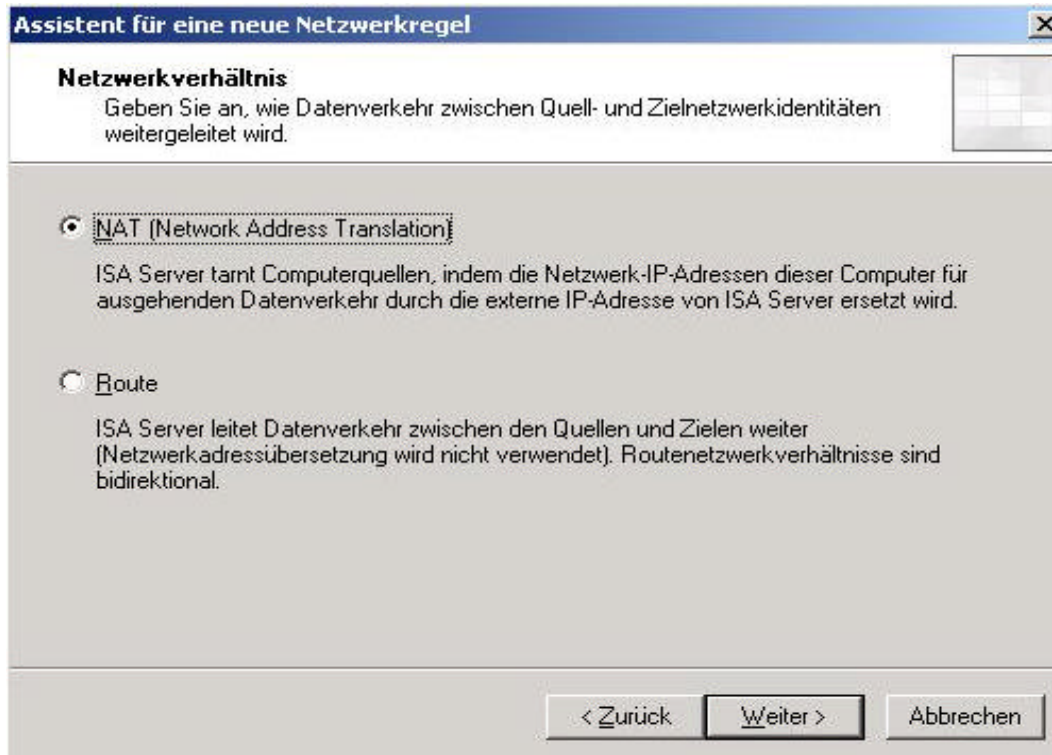
Netzwerkdatenverkehrquelle ist das Netzwerk **Forschungsabteilung**.



Das Netzwerkdatenverkehrsziel ist **Extern**, da eine Internet Verbindung hergestellt werden soll.



Das Netzwerkverhältnis ist **NAT (Network Address Translation)**. Mit Hilfe von NAT maskiert der ISA Server die IP-Adressen der internen Clients mit der externen IP Adresse des ISA Servers.



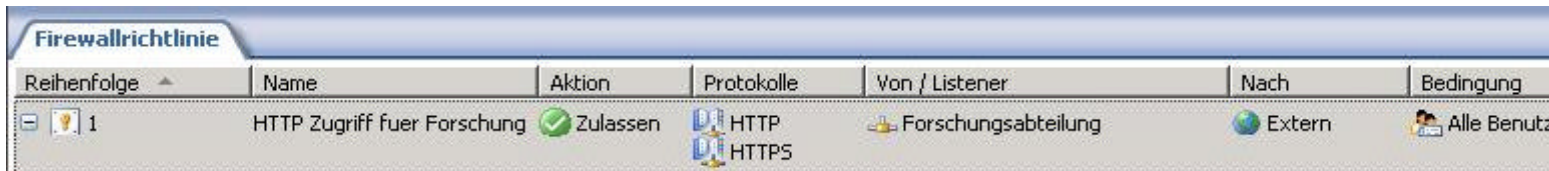
Klicken Sie in der ISA Verwaltungskonzole unterhalb von **Konfiguration** auf **Netzwerke** und überprüfen Sie im Reiter **Netzwerkregeln**, ob die entsprechende Netzwerkregel korrekt erstellt wurde.

R...	Name	Relation	Quellnetzwerke	Zielnetzwerke
1	Lokaler Hostzugriff	Route	Lokaler Host	Alle Netzwerke (u...
2	Forschung-NAT-Internet	NAT	Forschungsabteilung	Extern
3	VPN-Clients zum internen Netz...	Route	Quarantänen-VPN-Clients VPN-Clients	Intern
4	Internetzugriff	NAT	Intern Quarantänen-VPN-Clients VPN-Clients	Extern

Der letzte Schritt ist die Erstellung eine Firewallrichtlinie für das neu erstellte Netzwerk.



Die neue Firewallrichtlinie soll den **HTTP/HTTPS** Zugriff für das Netzwerk **Forschungsabteilung** nach **Extern** für **Alle Benutzer** zulassen.



Stand: 04.09.2004/MG. <http://www.it-training-grote.de>