ISA Server 2004 – Site – to – Site VPN mit L2TP/IPSEC - Von Marc Grote

---

Die Informationen in diesem Artikel beziehen sich auf:

- Microsoft ISA Server 2004

Einleitung

Dieser Artikel beschreibt die Einrichtung eines Site to Site VPN Netzwerkes zwischen zwei über SDSL verbundenen Standorten Obernkirchen (OBK) und Braunschweig (BS). Beide Standorte verwenden einen ISA Server 2004 Standard.

Überblick über Site to Site VPN

Große Unternehmen verfügen häufig über mehrere Standorte, die untereinander kommunizieren müssen, z. B. eine Unternehmenszentrale in Obernkirchen München und eine Schulungsniederlassung in Braunschweig. Die beiden Standorte können mithilfe einer Site to Site VPN Verbindung sicher über das Internet verbunden werden.

ISA Server 2004 enthält drei VPN-Protokolle für Site to Site Verbindungen:

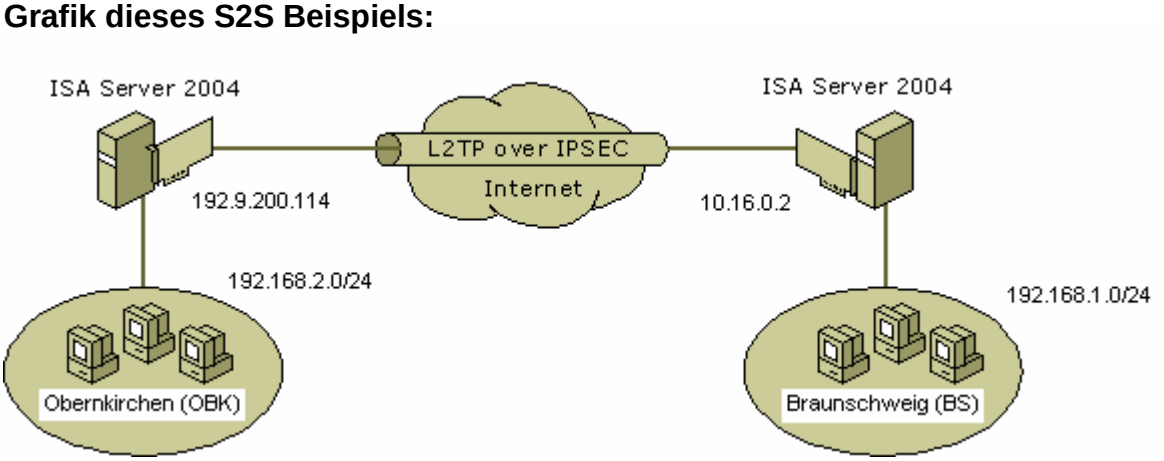
- PPTP (Point-to-Point Tunneling-Protokoll)
- L2TP (Layer 2 Tunneling-Protokoll) über IPSec (IP Security)
- IPSec-Tunnelmodus (IP Security-Protokoll)

Die Verfahren zum Konfigurieren von Remote-VPN-Netzwerken unterscheiden sich je nach ausgewähltem Tunneling-Protokoll. Bei allen Remotestandortnetzwerken muss das Netzwerk konfiguriert, eine Netzwerk- und Firewallrichtlinie für das Remotenetzwerk eingerichtet und das Remotestandortgateway (VPN-Server) konfiguriert werden.

Für IPSec-Netzwerke können darüber hinaus die Sicherheitseinstellungen auf dem ISA Server 2004 Computer konfiguriert werden. Außerdem müssen die IPSec-Richtlinieneinstellungen auf dem Remotestandortgateway konfiguriert werden.

Ein Site to Site VPN mit IPSEC sollte nur aus Abwärtskompatibilitätsgründen mit anderen Firewalllösungen verwendet werden. Site to Site VPN mit IPSEC ist auch ein neues Feature des ISA Server 2004.

Grafik dieses S2S Beispiels:

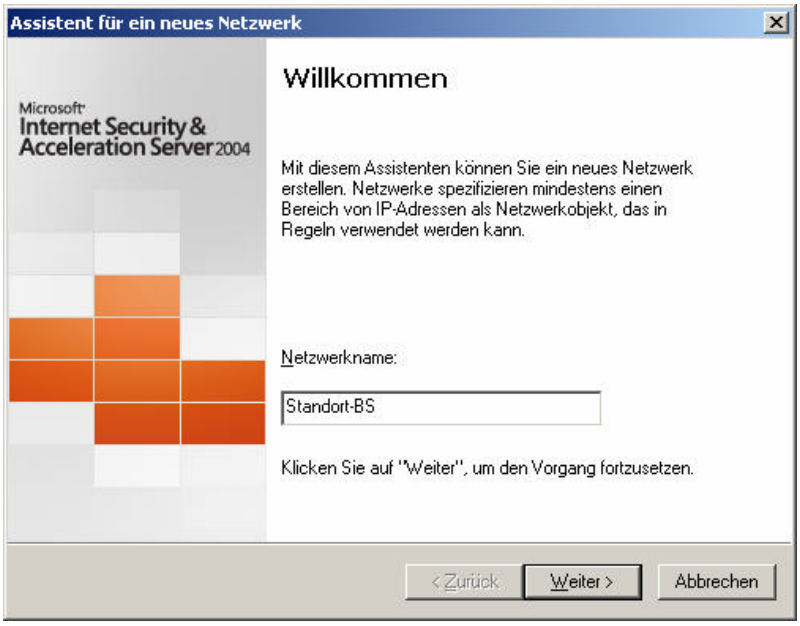


Starten Sie mit der Erstellung des S2S VPN auf dem ISA Server in Obernkirchen.

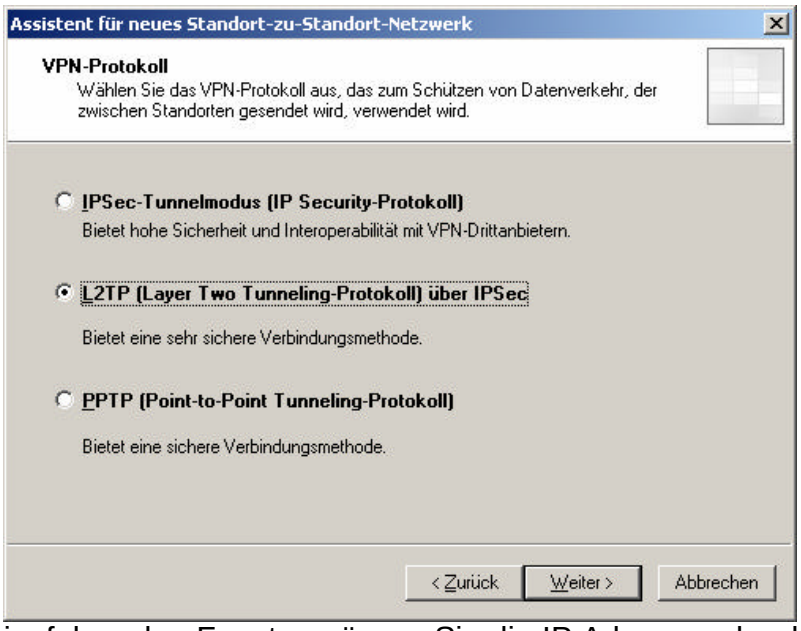
Zur Erstellung eines Site to Site VPN starten Sie die ISA Server Verwaltungskonsole und klicken Sie unterhalb des ISA Server ***Firewallobjektes*** auf ***virtuelle private Netzwerke (VPN)*** und dort auf den Reiter ***Remotestandorte***.

Dort klicken Sie auf der rechten Seite in den ***Remotestandortaufgaben*** auf ***Remotestandortnettwerk hinzufügen.***

Folgen Sie den Anweisungen des Assistenten und vergeben einen Namen für den Remotestandort.

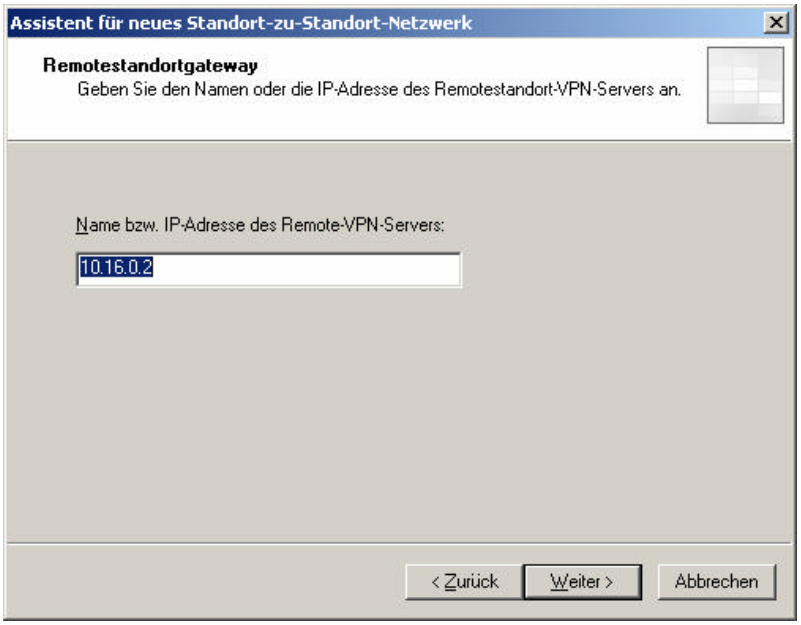


Als Protokoll wählen Sie ***L2TP über IPSEC***. Dabei handelt es sich um das zurzeit bevorzugte Protokoll für eine VPN / Site to Site Verbindung.

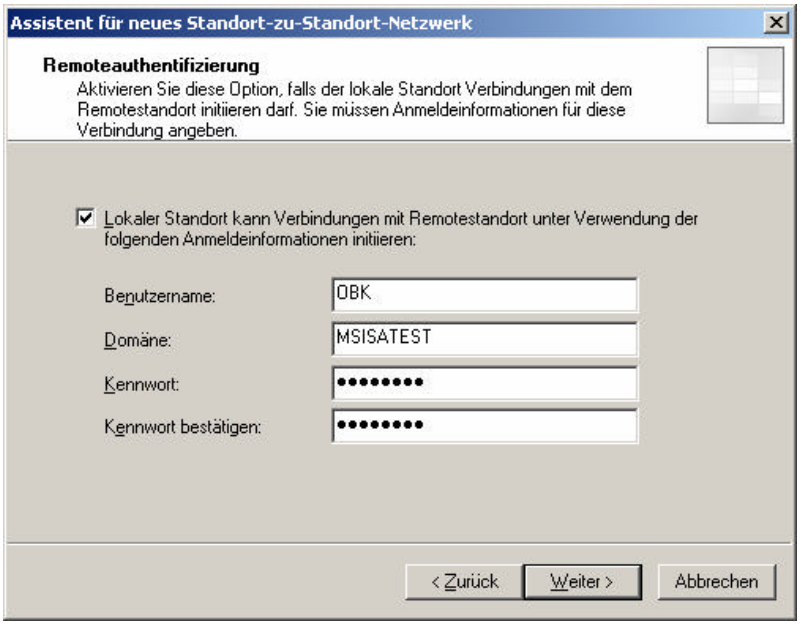


im folgenden Fenster müssen Sie die IP Adresse oder den Namen des Remote ISA Servers angeben.

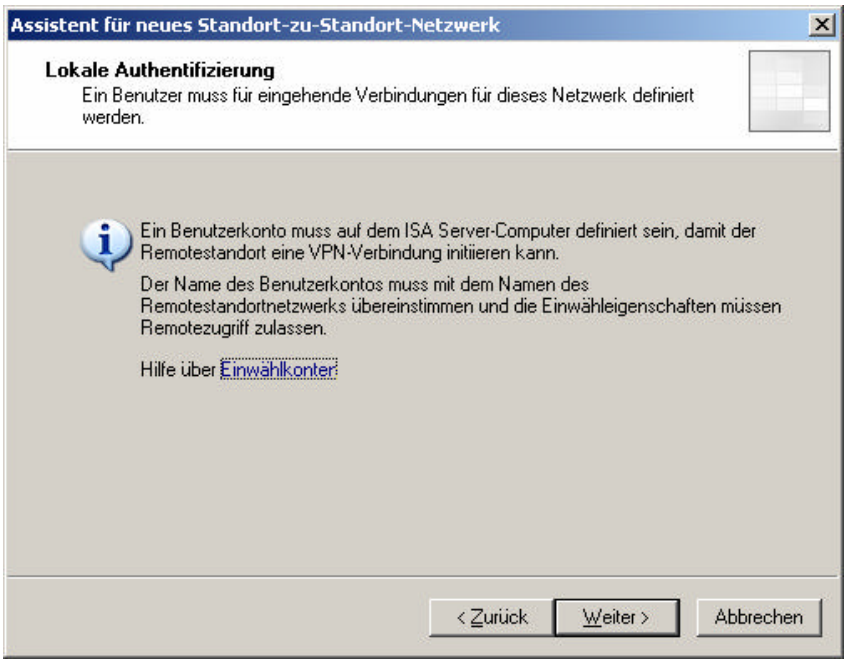
Bemerkung: *Bei nicht statischen IP Adressen müssen Sie hier Verfahren wie DYNDNS einsetzen und im Remotestandortgateway einen Namen angeben (z. B. ISA-Remote.dyndns.org)*



Soll der lokale Standort Verbindungen mit dem Remote Standort aufbauen dürfen, geben Sie in folgender Dialogbox den Benutzernamen, Domänennamen und das Kennwort für die Verbindung an.

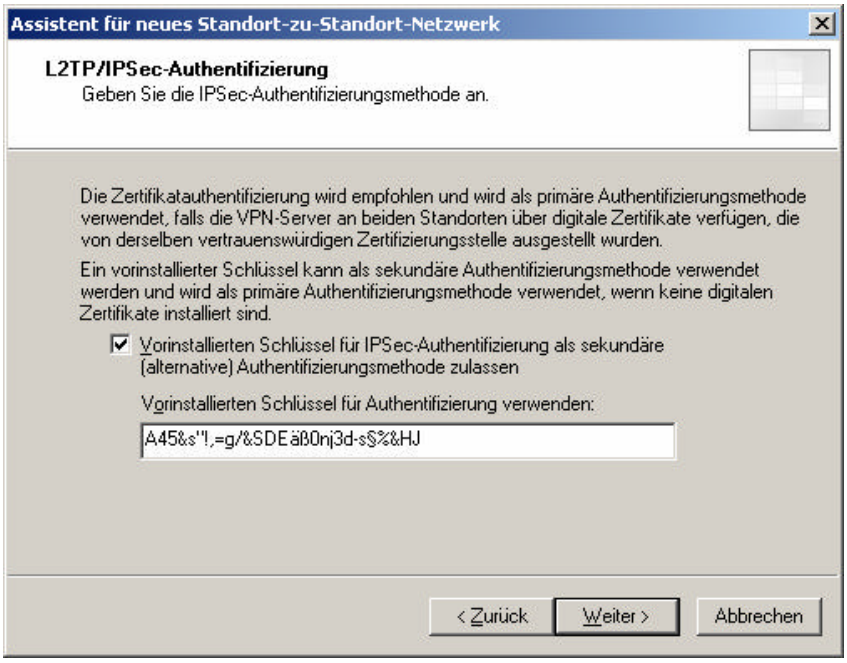


Für eingehende Verbindungen müssen Sie auf dem ISA Server Computer einen Benutzer definieren, welcher mit dem Namen des Remotestandortnetzwerkes übereinstimmen muss. Dieser Account muss auch das Recht zur Remoteeinwahl haben (Das Benutzerkonto wird am Ende des Artikels gezeigt).

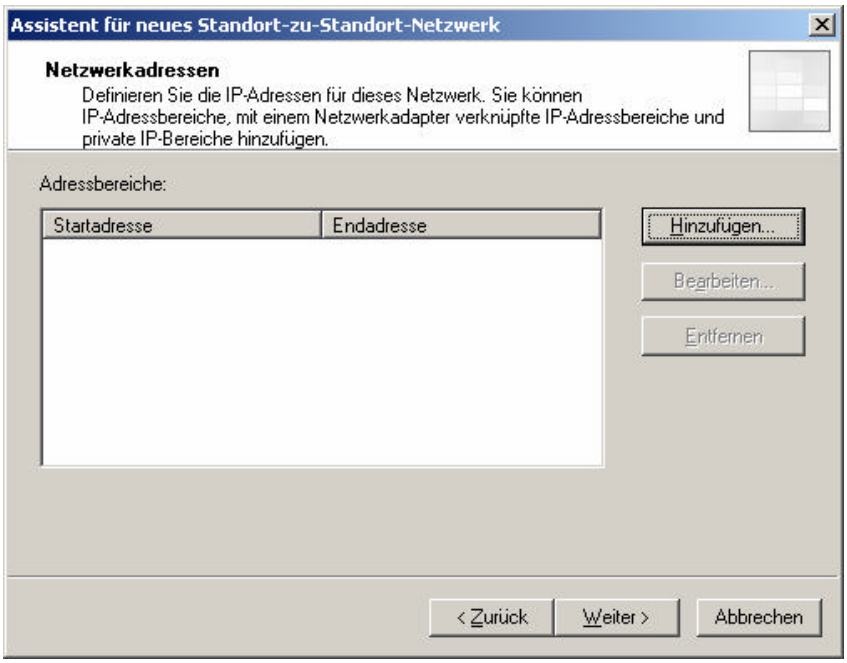


In großen Umgebungen mit zahlreichen Standorten ist es sinnvoll, eine Zertifikatsauthentifizierung einzurichten. Hierfür ist jedoch die Einrichtung einer Inhouse Zertifizierungsstelle erforderlich, welche jedoch sehr viel Verwaltungsaufwand erfordert. In unserem Beispiel verwenden wir keine Zertifizierungsstelle sondern einen vorinstallierten Schlüssel zur Authentifizierung, den so genannten Preshared Key.

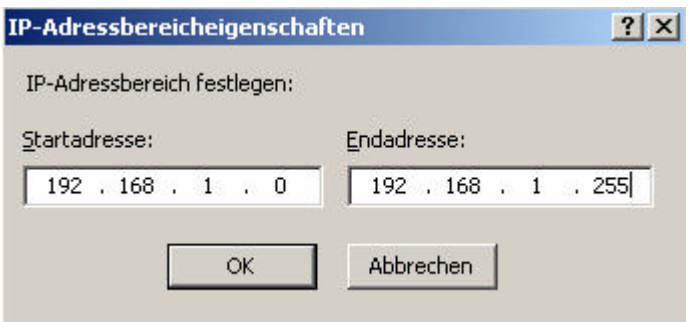
Verwenden Sie für den PSK (Pre Shared Key) eine sehr komplexe, lange und zufällige Zeichenfolge wie in diesem Beispiel.



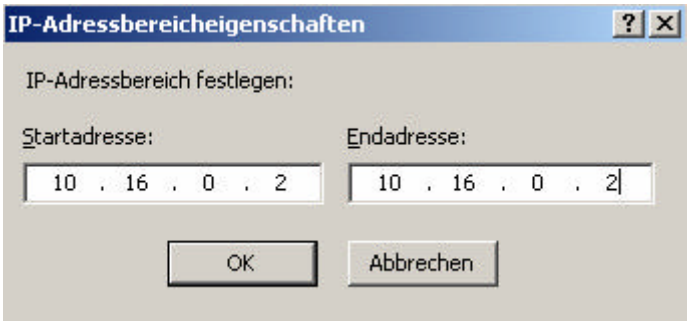
Für das Site to Site Netzwerk müssen Sie jetzt noch den internen IP-Adressbereich der Clients hinter dem Remote ISA Server angeben (Standort Braunschweig (BS)).



Geben Sie hier den Adressbereich ein.



Geben Sie zusätzlich noch die IP-Adresse des externen Interface des Remote ISA Server an. Diese Einstellung ist notwendig, damit Web Proxy Clients auf das Netzwerk zugreifen können.
Quelle: http://www.isaserver.org/tutorials/2004ipsectunnelmode.html



Die Konfiguration ist beendet. Sie können den Assistenten fertig stellen.

Schritte zur Netzwerkkonfiguration

Damit neu erstellte Netzwerke Datenverkehr senden oder empfangen können, müssen weitere Konfigurationsschritte durchgeführt werden. Diese Schritte sind vom Typ des erstellten Netzwerks abhängig. Wir konzentrieren uns auf das Site to Site Netzwerk mit L2TP.

Site to Site VPN mit L2TP

ISA Server 2004 verwendet Windows Routing und RAS um eine L2TP over IPSEC Verbindung herzustellen.

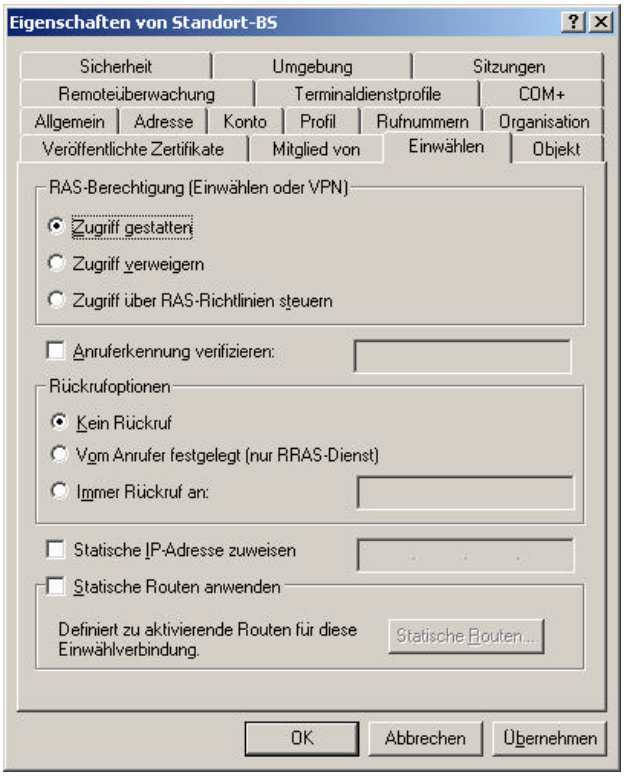
Damit Clients eine Verbindung aus dem VPN über PPTP (Point-to-Point Tunneling-Protokoll) oder L2TP (Layer Two Tunneling-Protokoll) herstellen können, müssen Sie die folgenden Schritte durchführen:

- Erstellen Sie einen Benutzer mit dem Namen des neuen Netzwerks. Geben Sie dann für die RAS-Berechtigungen Zulassen an.
- Erstellen Sie Netzwerkregeln, die Datenverkehr zu und von diesem Netzwerk zulassen.
- Erstellen Sie Zugriffsregeln, die Datenverkehr zu und von diesem Netzwerk zulassen.

L2TP over IPSEC und reine IPSEC Verbindungen erfordern entweder die Verwendung von Zertifikaten oder so genannten Pre Shared Keys (PSK). Die Verwendung von Zertifikaten ist zu bevorzugen, allerdings ist hierfür im Idealfall eine PKI (Public Key Infrastructure) erforderlich.

Erstellen eines Benutzers

Bei der Erstellung eines Benutzer ist der Reiter ***Einwählen*** wichtig. An dieser Stelle muss dem Account die Einwahlberechtigung erteilt werden.



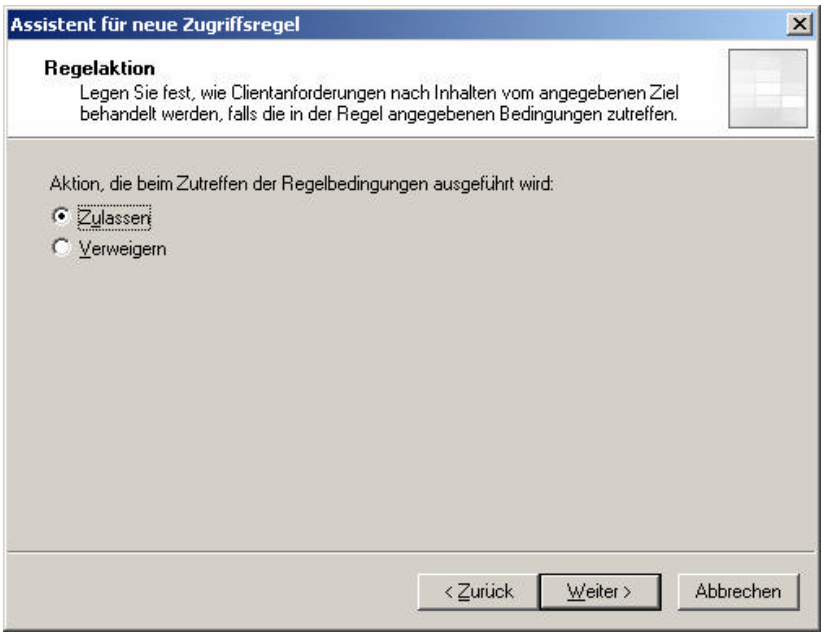
Erstellen einer Zugriffsregel

Da es sich bei einem Site to Site VPN in der Regel um ein und dieselbe Firma handelt, ist es nicht notwendig, den Datenverkehr einzuschränken. Wir erstellen eine Regel mit vollständigem Zugriff.

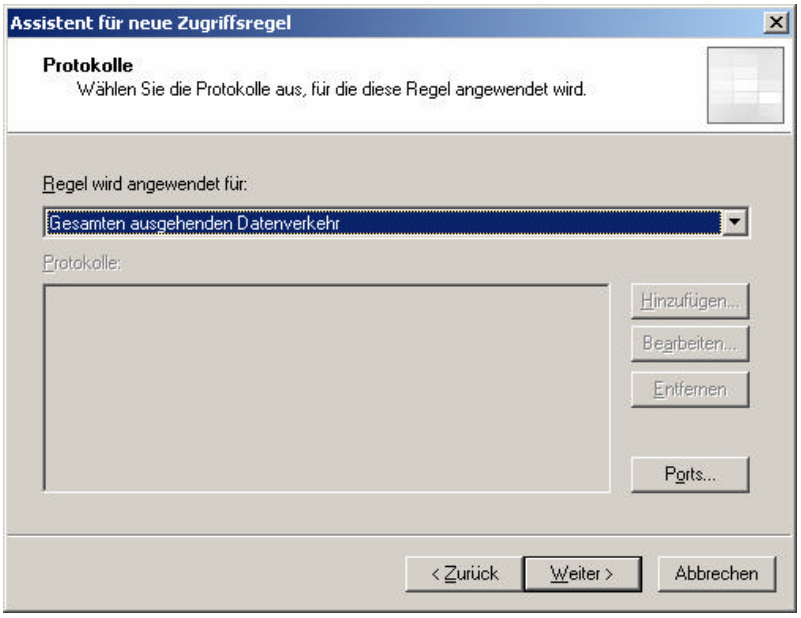
Hinweis: Sie müssen eine Zugriffsregel in beide Richtungen des jeweiligen Remotestandortes erstellen.

Achten Sie bei der Erstellung eines Site to Site VPN mit Partnern, Lieferanten usw. auf ein angepasstes Firewallregelwerk.

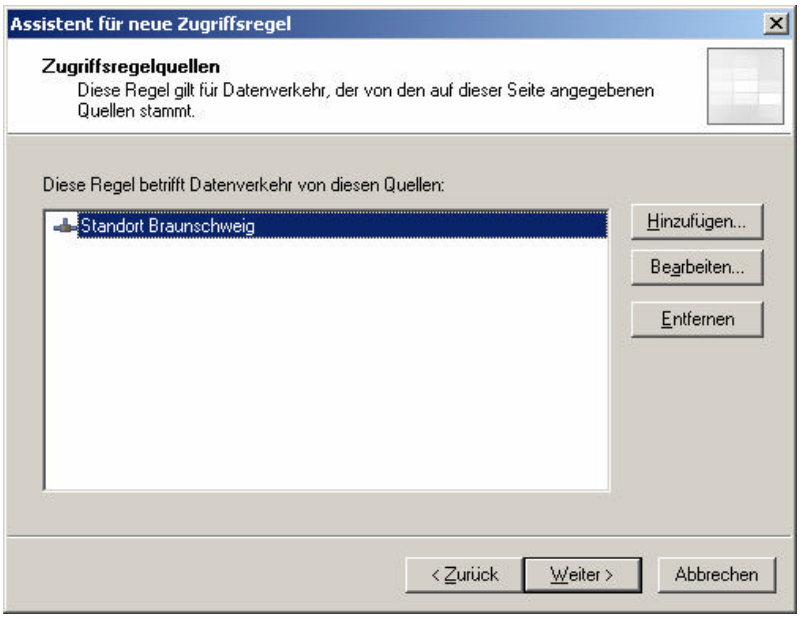
Wir erstellen eine Zulassungsregel



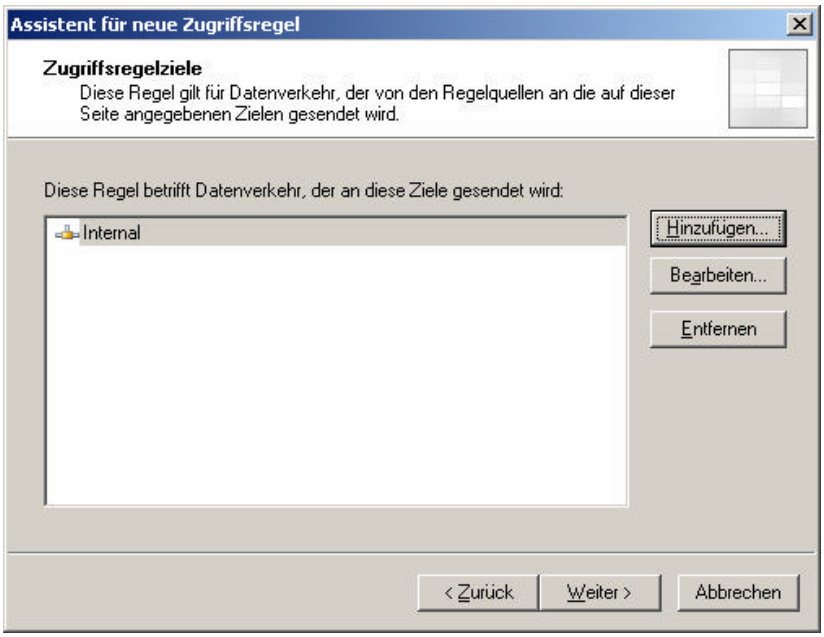
Die Regel wird für den gesamten ausgehenden Datenverkehr angewendet.



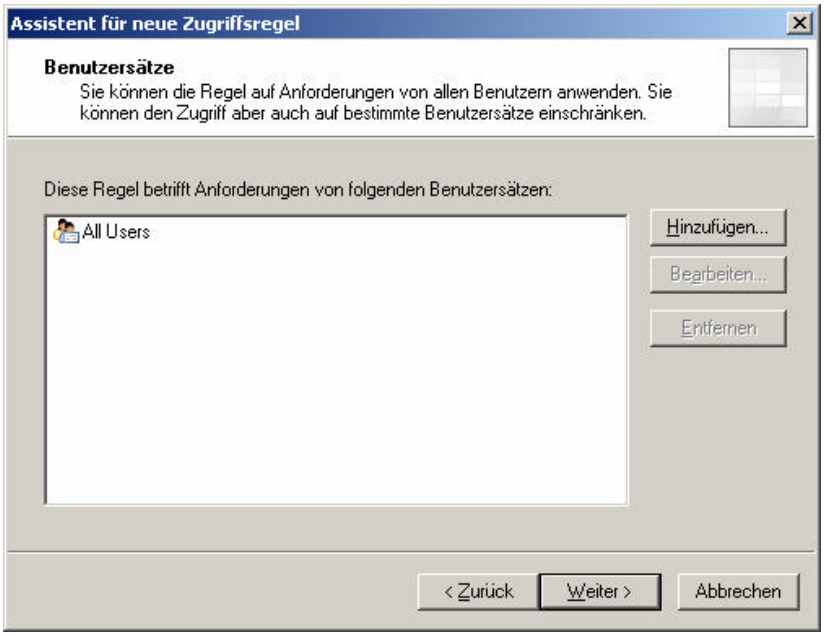
Die Regel betrifft den Datenverkehr vom Standort Braunschweig nach …



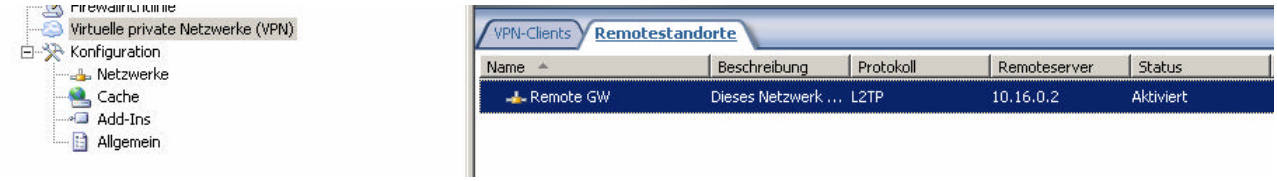
Internal



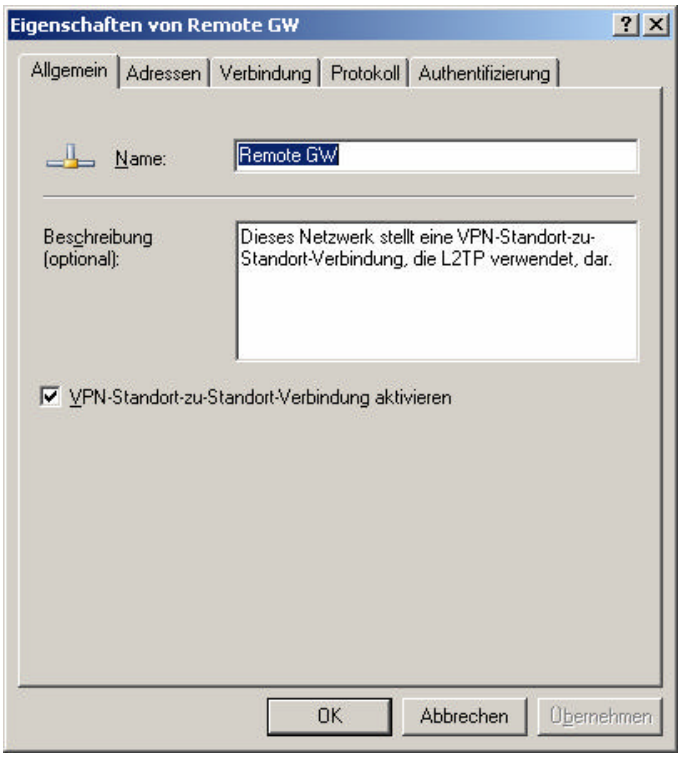
Die Regel betrifft Anforderungen von folgenden Benutzersätzen ***All Users***.



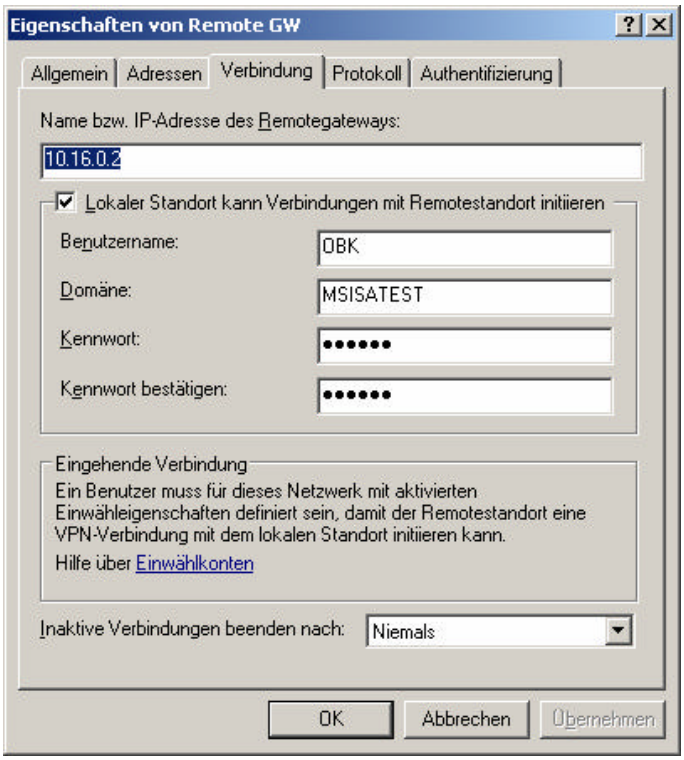
Der Remotestandort ist jetzt konfiguriert.



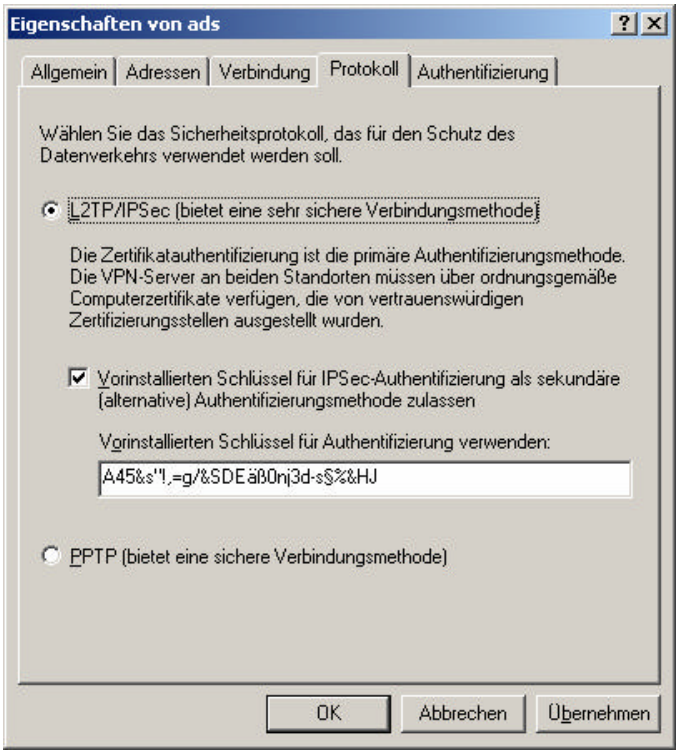
Überprüfen Sie noch einmal die Einstellungen.



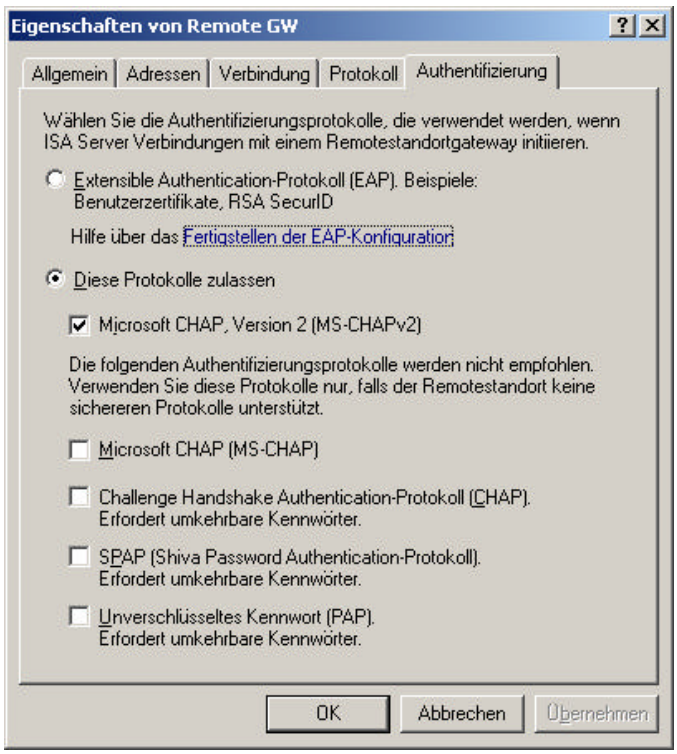
Im Reiter ***Verbindungen*** können Sie noch einmal die Verbindungsdaten überprüfen und eine Beendigung der Verbindung nach Anzahl X Minuten / Stunden festlegen.



Hier können Sie das VPN Protokoll einstellen und den PSK ändern (Vorsicht: Muss auf beiden Seiten geändert werden).

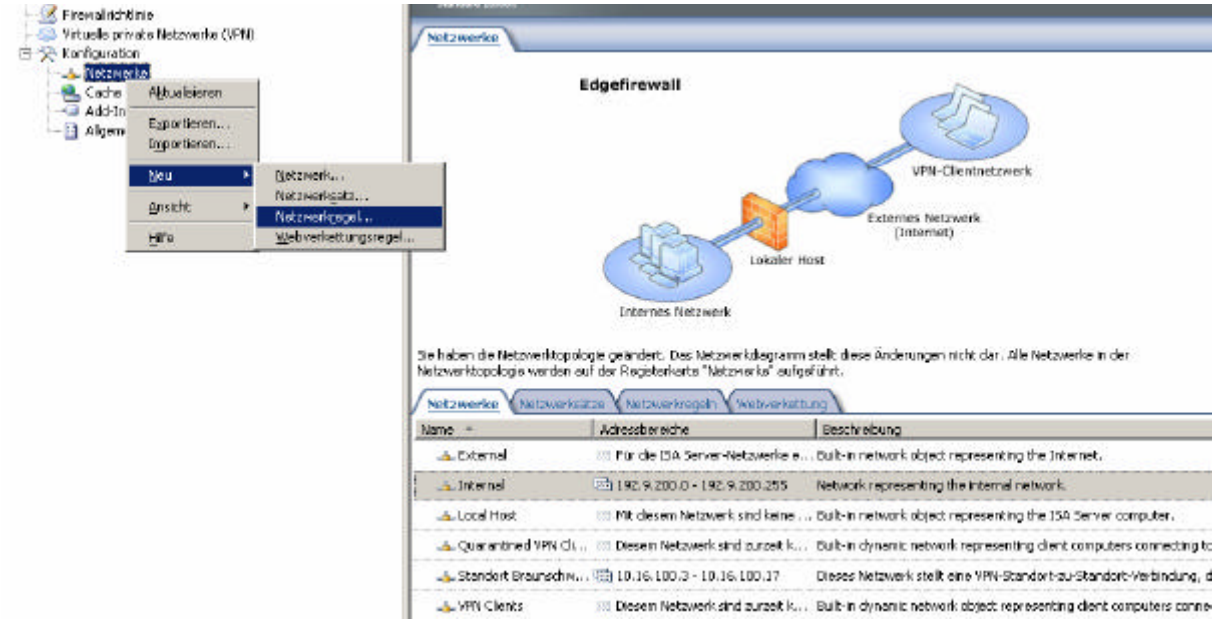


Im Reiter ***Authentifizierung*** können Sie die Authentifizierungsprotokolle festlegen. PPTP/L2TP erfordern im Gegensatz zu IPSEC eine Authentifizierung.

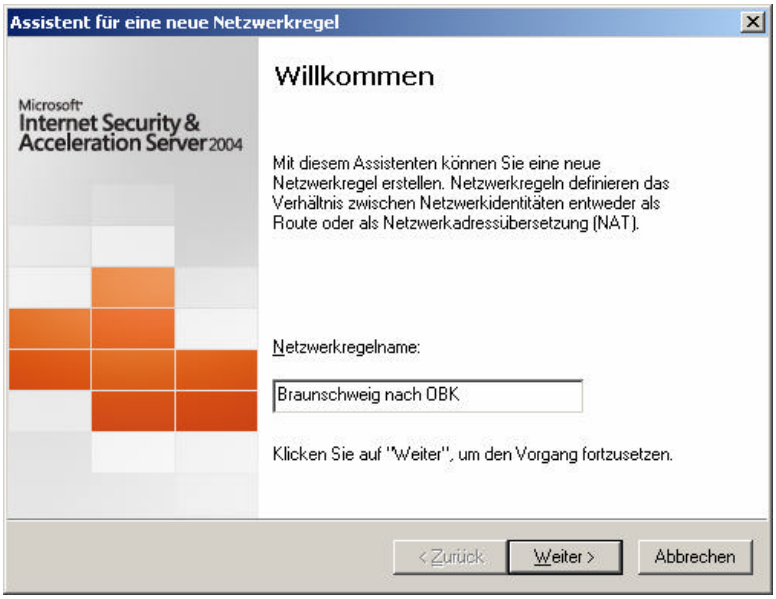


Erstellen eine Netzwerkregel

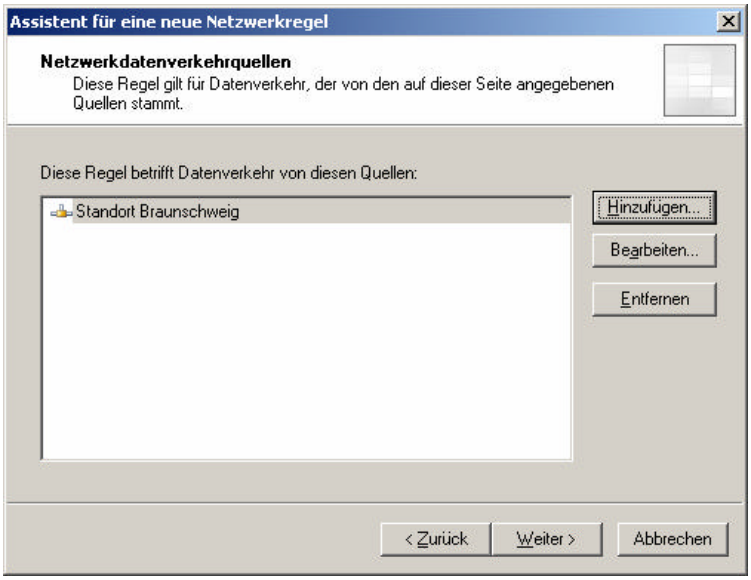
Der letzte Schritt ist die Erstellung einer Netzwerkregel, welche die beiden Standorte mit einander verbindet.



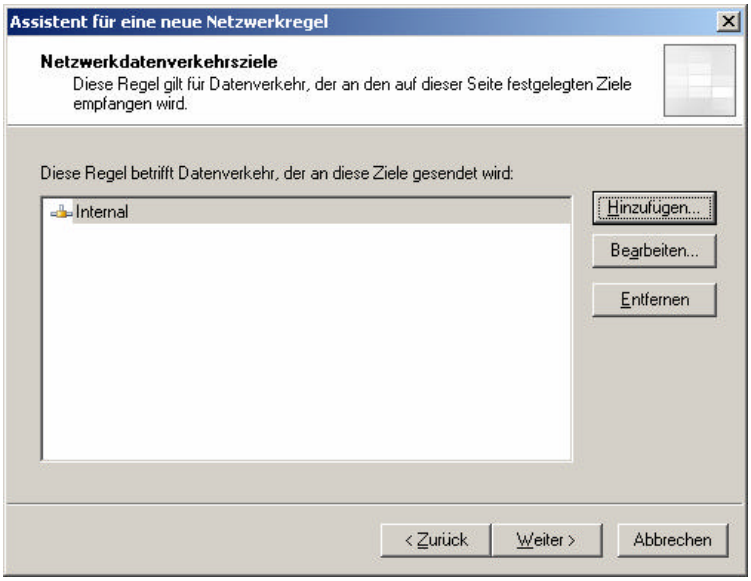
Folgen Sie den Anweisungen des Wizard und vergeben Sie einen Namen für die Netzwerkregel.



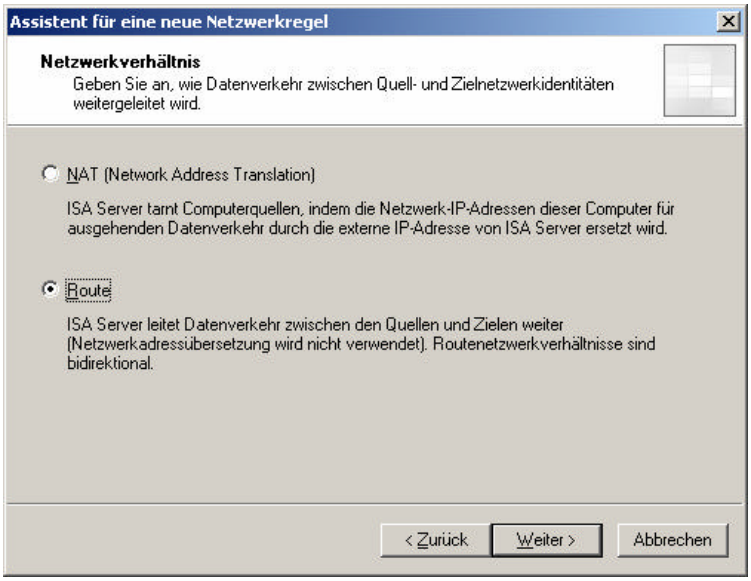
Die Regel betrifft als Quelle den *Standort Braunschweig*



Netzwerkziel ist *Internal*



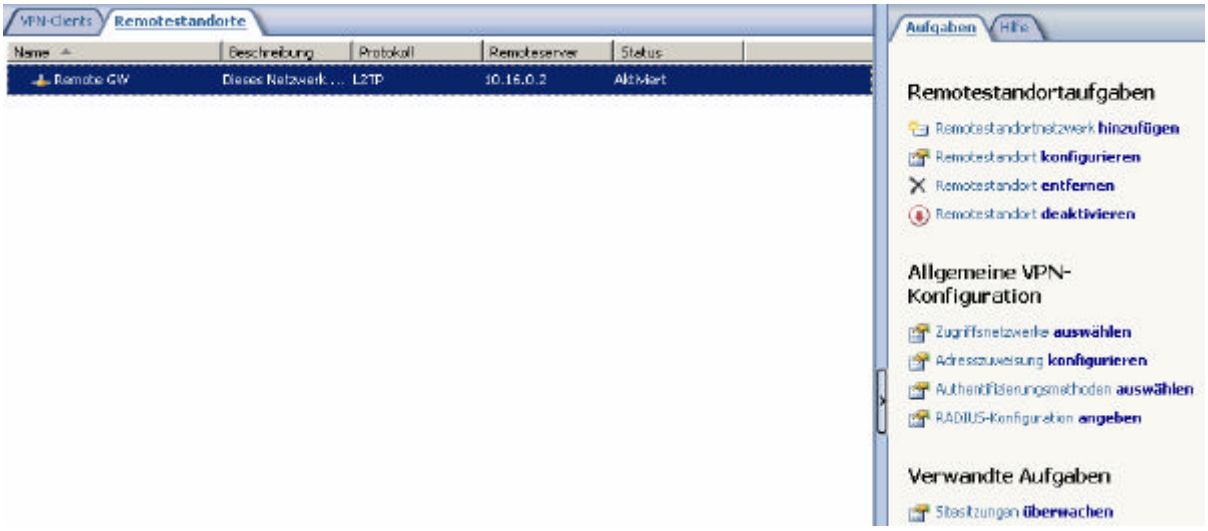
Das Netzwerkverhältnis muss auf Route stehen, da die Pakete nicht ge**NAT**et werden.



Überprüfen Sie noch einmal alle Einstellungen und beenden dann den Assistenten.

So sieht die neu erstelle Netzwerkregel aus.

Sie können die Verbindungen von und zum Remotestandort überwachen, indem Sie auf der rechten Seite im *Aufgabenfenster* unter Verwandte Aufgaben *Sitesitzungen überwachen* anklicken. Die Daten werden dann im Protokollfenster angezeigt.



Stand: 28.12.2004/MG. http://www.it-training-grote.de