

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:

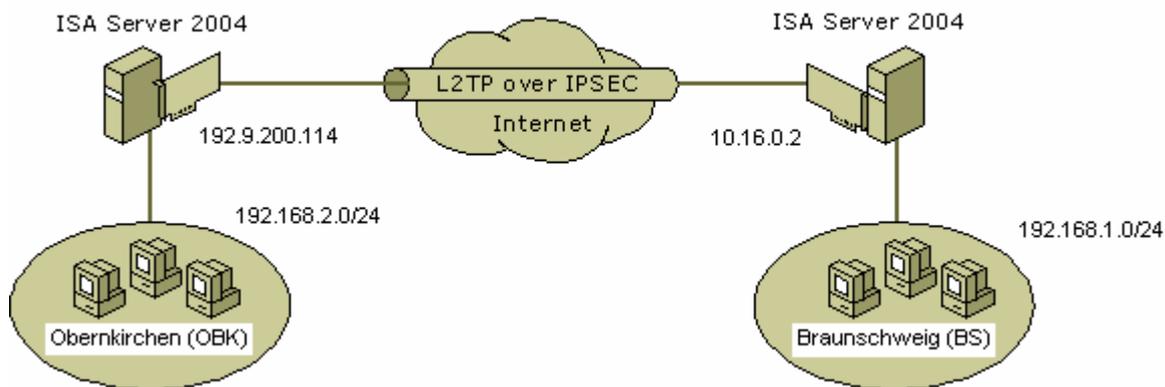
- ? PPTP (Point-to-Point Tunneling-Protokoll)
- ? L2TP (Layer 2 Tunneling-Protokoll) über IPsec (IP Security)
- ? IPsec-Tunnelmodus (IP Security-Protokoll)

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 **Remotestandortnetzwerk 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.

The screenshot shows a Windows XP-style dialog box titled "Assistent für neues Standort-zu-Standort-Netzwerk". The main heading is "VPN-Protokoll" with a sub-instruction: "Wählen Sie das VPN-Protokoll aus, das zum Schützen von Datenverkehr, der zwischen Standorten gesendet wird, verwendet wird." There are three radio button options: "IPSec-Tunnelmodus (IP Security-Protokoll)", "L2TP (Layer Two Tunneling-Protokoll) über IPsec" (which is selected), and "PPTP (Point-to-Point Tunneling-Protokoll)". Each option has a brief description below it. At the bottom, there are three buttons: "< Zurück", "Weiter >", and "Abbrechen".

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*)

The screenshot shows the same dialog box, now at the "Remotestandortgateway" step. The instruction is: "Geben Sie den Namen oder die IP-Adresse des Remotestandort-VPN-Servers an." Below this is a text input field with the label "Name bzw. IP-Adresse des Remote-VPN-Servers:". The field contains the IP address "10.16.0.2". At the bottom, there are three buttons: "< Zurück", "Weiter >", and "Abbrechen".

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.

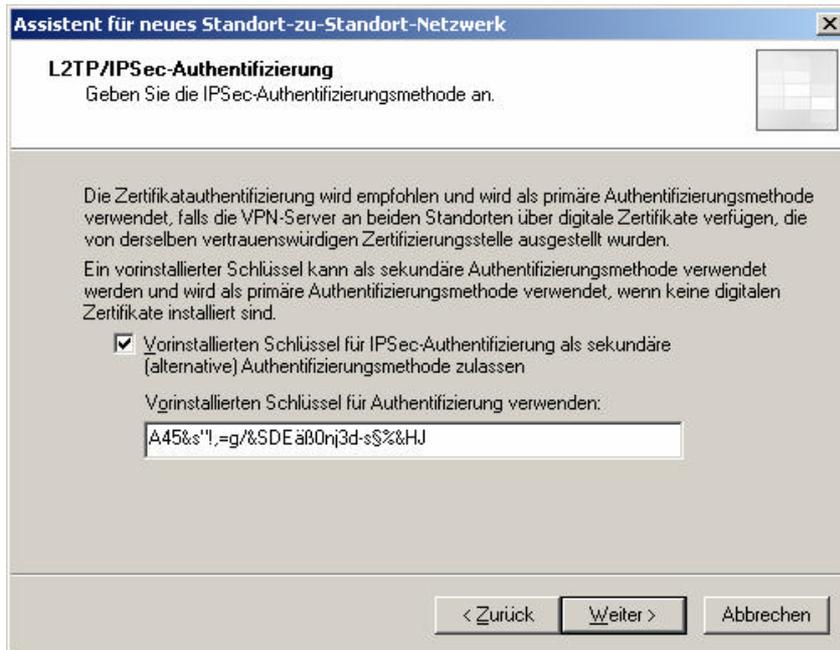
The screenshot shows a Windows dialog box titled "Assistent für neues Standort-zu-Standort-Netzwerk". The current step is "Remoteauthentifizierung". The text reads: "Aktivieren Sie diese Option, falls der lokale Standort Verbindungen mit dem Remoteort initiieren darf. Sie müssen Anmeldeinformationen für diese Verbindung angeben." Below this, there is a checked checkbox: "Lokaler Standort kann Verbindungen mit Remoteort unter Verwendung der folgenden Anmeldeinformationen initiieren:". Underneath the checkbox are four input fields: "Benutzername:" with the value "DBK", "Domäne:" with the value "MSISATEST", "Kennwort:" with seven dots, and "Kennwort bestätigen:" with seven dots. At the bottom, there are three buttons: "< Zurück", "Weiter >", and "Abbrechen".

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

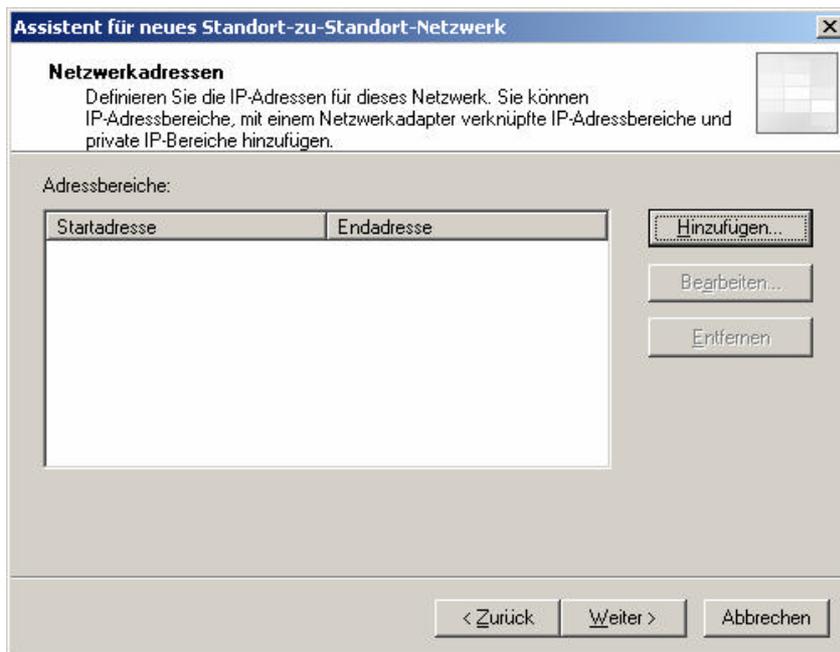
The screenshot shows the same dialog box, but now on the "Lokale Authentifizierung" step. The text reads: "Ein Benutzer muss für eingehende Verbindungen für dieses Netzwerk definiert werden." Below this is an information icon (i) followed by the text: "Ein Benutzerkonto muss auf dem ISA Server-Computer definiert sein, damit der Remoteort eine VPN-Verbindung initiieren kann. Der Name des Benutzerkontos muss mit dem Namen des Remoteortnetzwerkes übereinstimmen und die Einwähleigenschaften müssen Remotezugriff zulassen." Below this text is a link: "Hilfe über [Einwahlkonten](#)". At the bottom, there are three buttons: "< Zurück", "Weiter >", and "Abbrechen".

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.

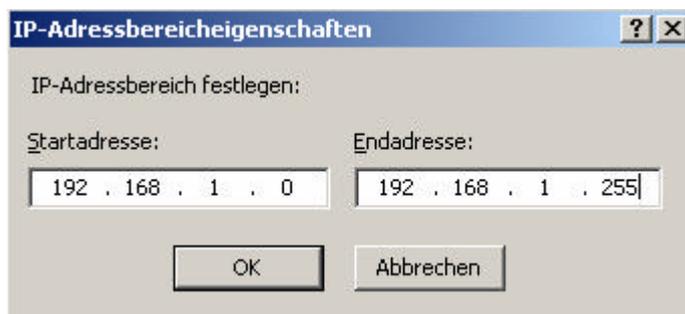
Verwenden Sie für den PSK (Pre Shared Key) eine sehr komplexe, lange und zufällige Zeichenfolge wie in diesem Beispiel.



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)).

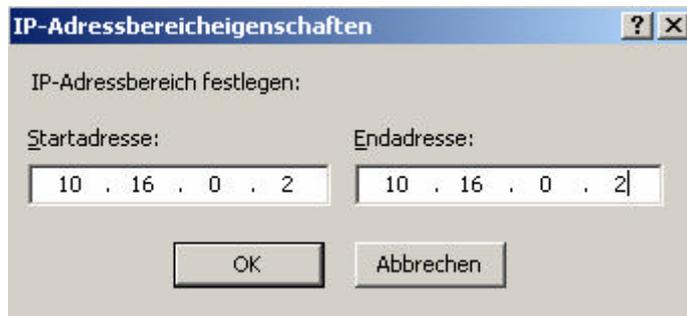


Geben Sie hier den Adressbereich ein.

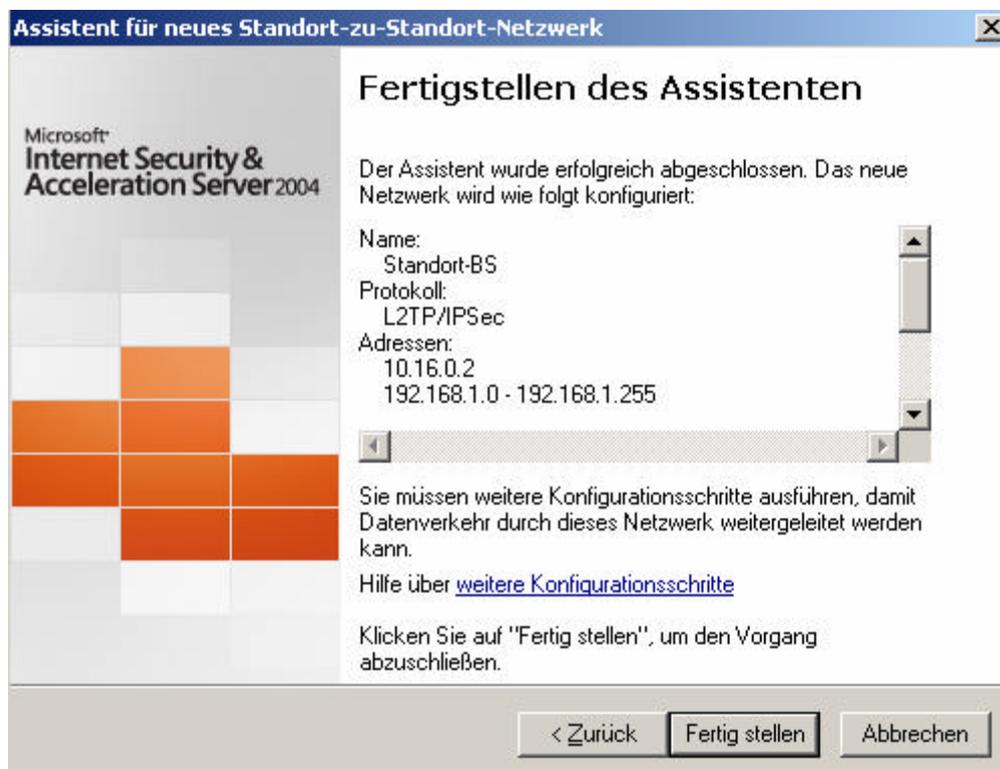


Geben Sie zusätzlich noch die IP-Adresse des externen Interface des Remote ISA Server an. Diese Einstellung ist notwendig, damit Web Proxy Clients auf das Netzwerk zugreifen können.

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.

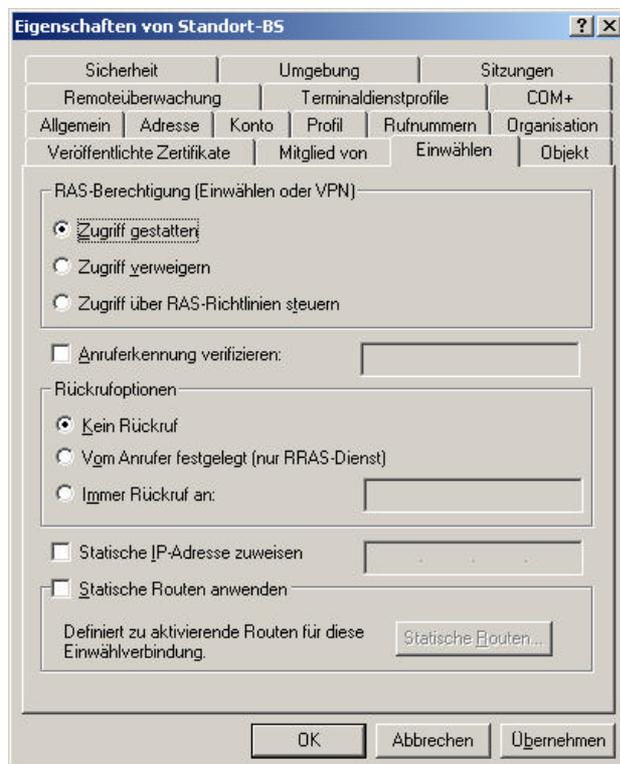
Damit Clients eine Verbindung aus dem VPN über PPTP (Point-to-Point Tunneling-Protokoll) oder L2TP (Layer Two Tunneling-Protokoll) herstellen können, müssen Sie die folgenden Schritte durchführen:

- ? 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

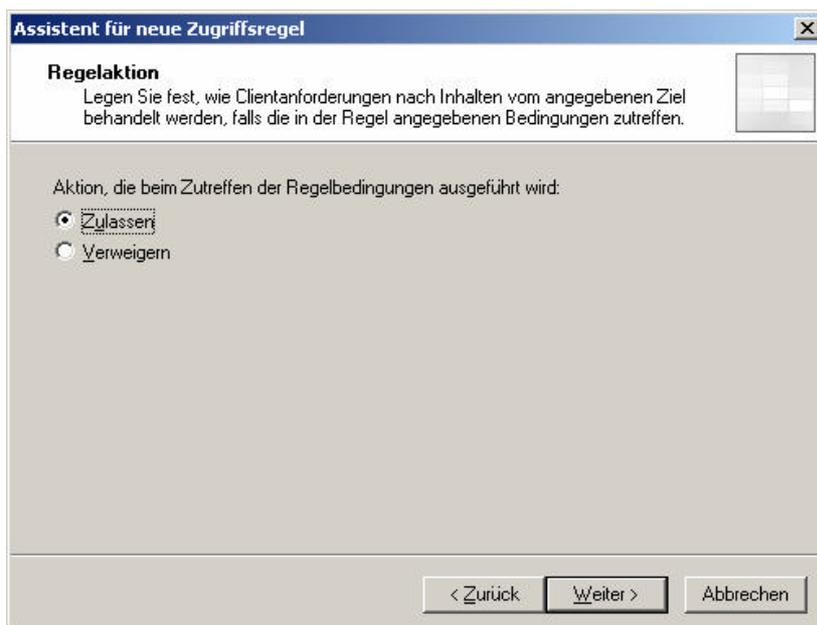
Da es sich bei einem Site to Site VPN in der Regel um ein und dieselbe Firma handelt, ist es nicht notwendig, den Datenverkehr einzuschränken. Wir erstellen eine Regel mit vollständigem Zugriff.

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

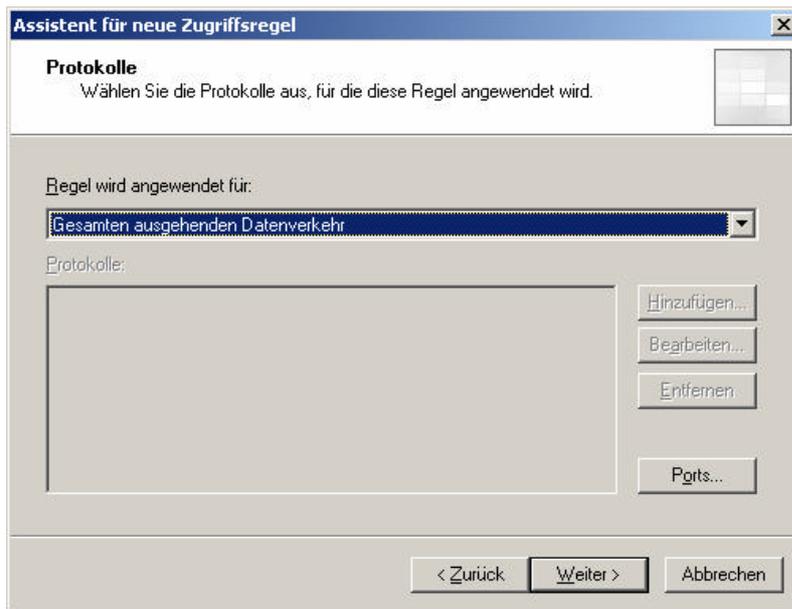
Achten Sie bei der Erstellung eines Site to Site VPN mit Partnern, Lieferanten usw. auf ein angepasstes Firewallregelwerk.



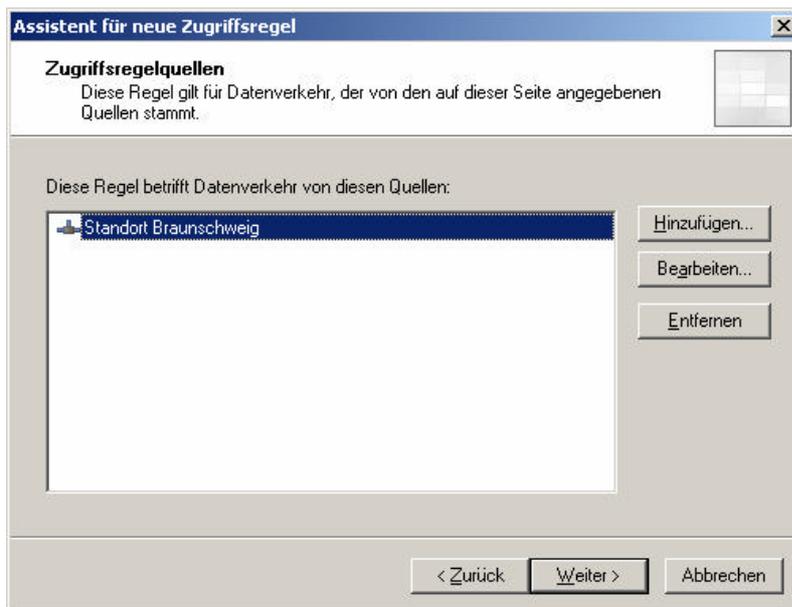
Wir erstellen eine Zulassungsregel



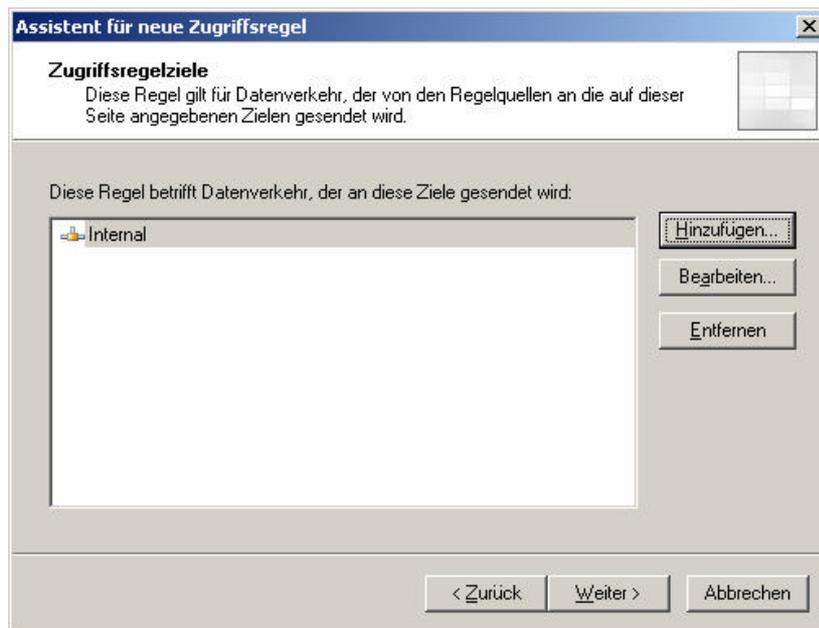
Die Regel wird für den gesamten ausgehenden Datenverkehr angewendet.



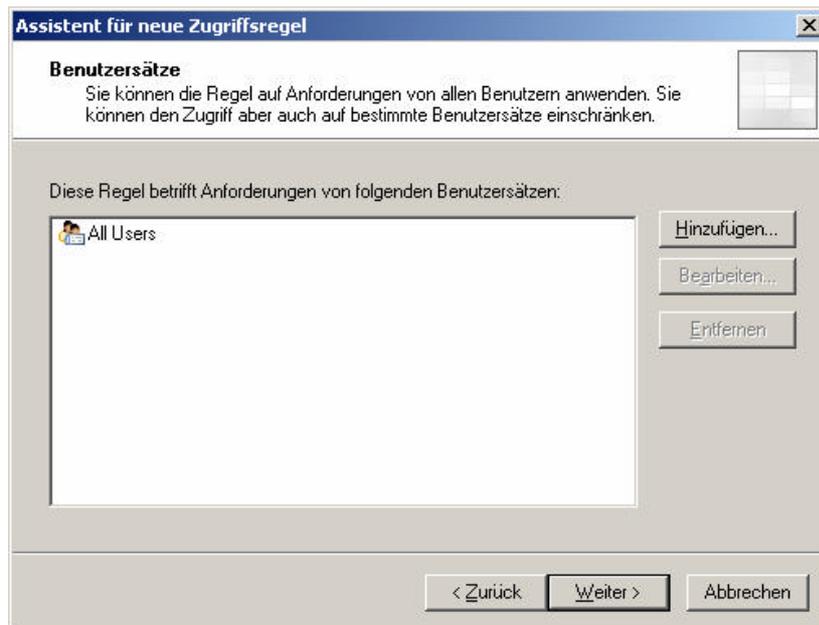
Die Regel betrifft den Datenverkehr vom Standort Braunschweig nach ...



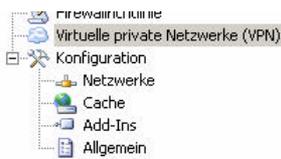
Internal



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



Der Remotestandort ist jetzt konfiguriert.



A screenshot of the 'Remotestandorte' tab in the VPN-Client configuration window. It displays a table with the following data:

Name	Beschreibung	Protokoll	Remoteserver	Status
Remote GW	Dieses Netzwerk ...	L2TP	10.16.0.2	Aktiviert

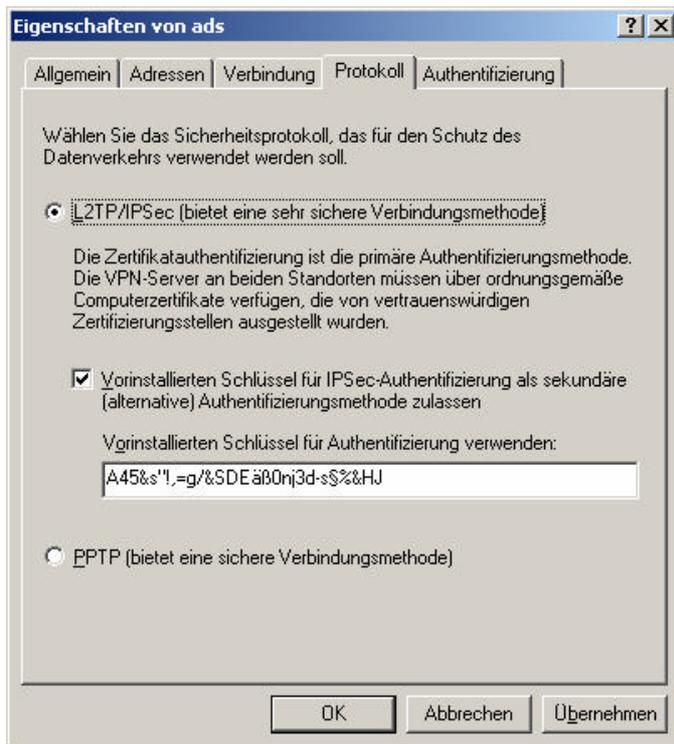
Überprüfen Sie noch einmal die Einstellungen.

A screenshot of the 'Eigenschaften von Remote GW' dialog box, 'Allgemein' tab. The 'Name' field contains 'Remote GW'. The 'Beschreibung (optional):' text box contains 'Dieses Netzwerk stellt eine VPN-Standort-zu-Standort-Verbindung, die L2TP verwendet, dar.' The checkbox 'VPN-Standort-zu-Standort-Verbindung aktivieren' is checked. Buttons at the bottom are 'OK', 'Abbrechen', and 'Übernehmen'.

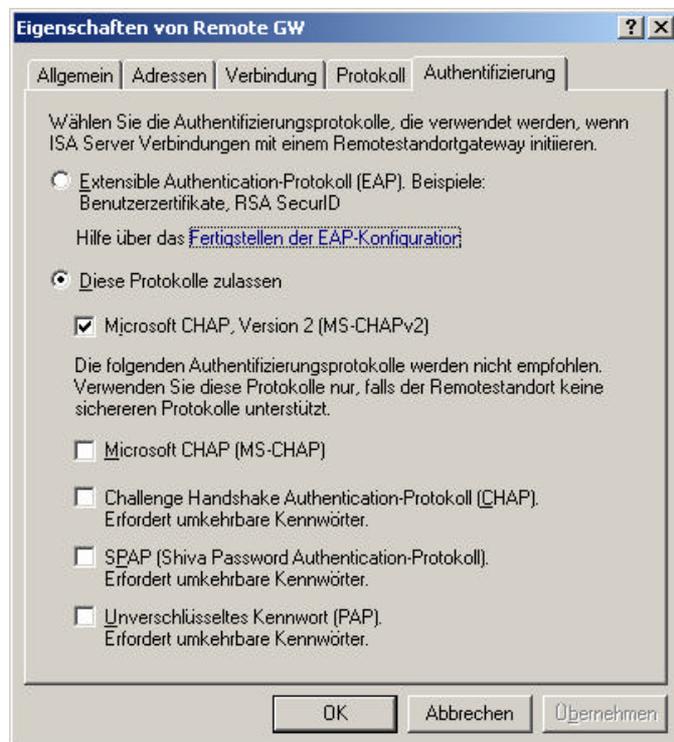
Im Reiter **Verbindungen** können Sie noch einmal die Verbindungsdaten überprüfen und eine Beendigung der Verbindung nach Anzahl X Minuten / Stunden festlegen.

A screenshot of the 'Eigenschaften von Remote GW' dialog box, 'Verbindung' tab. The 'Name bzw. IP-Adresse des Remotegateways:' field contains '10.16.0.2'. The checkbox 'Lokaler Standort kann Verbindungen mit Remotestandort initiieren' is checked. Below it are fields for 'Benutzername:' (OBK), 'Domäne:' (MSISATEST), 'Kennwort:' (masked with dots), and 'Kennwort bestätigen:' (masked with dots). The 'Eingehende Verbindung' section contains a note: 'Ein Benutzer muss für dieses Netzwerk mit aktivierten Einwähleigenschaften definiert sein, damit der Remotestandort eine VPN-Verbindung mit dem lokalen Standort initiieren kann.' and a link 'Hilfe über Einwählkonten'. The 'Inaktive Verbindungen beenden nach:' dropdown is set to 'Niemals'. Buttons at the bottom are 'OK', 'Abbrechen', and 'Übernehmen'.

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.

The screenshot shows the configuration interface of Microsoft Security & Acceleration Server 2004. On the left, a tree view shows the 'Netzwerke' (Networks) folder expanded, with a context menu open over it. The menu options are: Aktualisieren, Exportieren..., Importieren..., Neu (highlighted), Ansicht, and Hilfe. The 'Neu' sub-menu is open, showing: Netzwerk..., Netzwerksatz..., Netzwerkregel... (highlighted), and Webverleittungsregel... The main window displays a network diagram titled 'Edgefirewall' with components: Internes Netzwerk, Lokaler Host, Externes Netzwerk (Internet), and VPN-Clientnetzwerk. Below the diagram, a text box states: 'Sie haben die Netzwerktopologie geändert. Das Netzwerkdiagramm stellt diese Änderungen nicht dar. Alle Netzwerke in der Netzwerktopologie werden auf der Registerkarte "Netzwerke" aufgeführt.' Below this, a table lists the network objects:

Name	Adressbereiche	Beschreibung
External		Für die ISA Server-Netzwerke e... Built-in network object representing the Internet.
Internal	192.9.200.0 - 192.9.200.255	Network representing the internal network.
Local Host		Mit diesem Netzwerk sind keine... Built-in network object representing the ISA Server computer.
Quarantined VPN Cl...		Diesem Netzwerk sind zurzeit k... Built-in dynamic network representing client computers connecting to...
Standort Braunschwi...	10.16.100.2 - 10.16.100.17	Dieses Netzwerk stellt eine VPN-Standort-zu-Standort-Verbindung, d...
VPN Clients		Diesem Netzwerk sind zurzeit k... Built-in dynamic network object representing client computers connect...

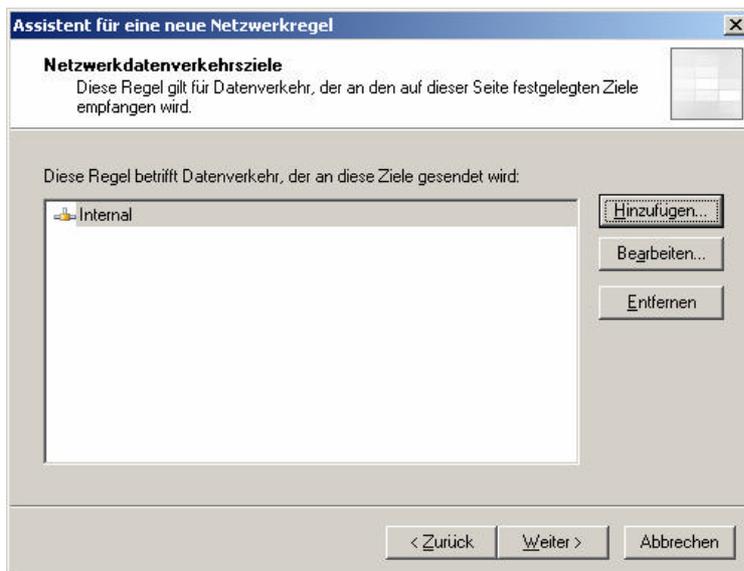
Folgen Sie den Anweisungen des Wizard und vergeben Sie einen Namen für die Netzwerkregel.

The screenshot shows the 'Assistent für eine neue Netzwerkregel' (New Network Rule Wizard) window. The title bar reads 'Assistent für eine neue Netzwerkregel'. The window contains the Microsoft Internet Security & Acceleration Server 2004 logo and a grid of orange squares. The main text reads: 'Willkommen. Mit diesem Assistenten können Sie eine neue Netzwerkregel erstellen. Netzwerkregeln definieren das Verhältnis zwischen Netzwerkidentitäten entweder als Route oder als Netzwerkadressübersetzung (NAT).' Below this, there is a label 'Netzwerkregelname:' followed by a text input field containing 'Braunschweig nach OBK'. At the bottom, there are three buttons: '< Zurück', 'Weiter >', and 'Abbrechen'. A note at the bottom says: 'Klicken Sie auf "Weiter", um den Vorgang fortzusetzen.'

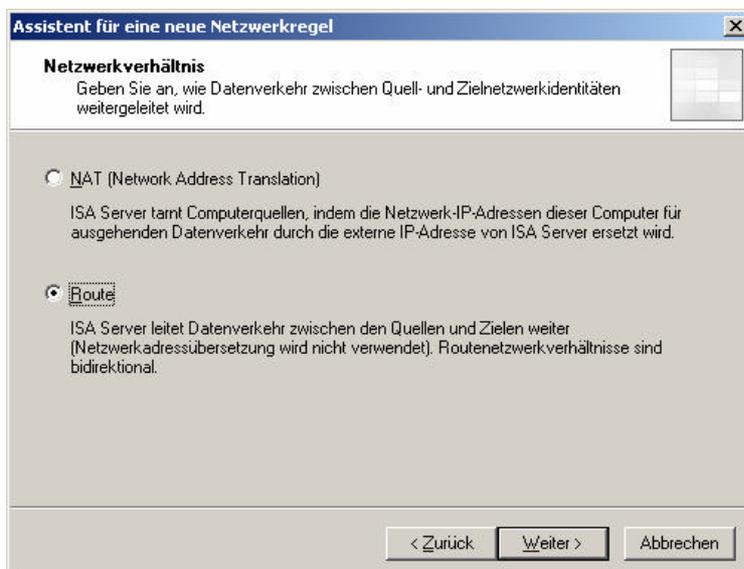
Die Regel betrifft als Quelle den *Standort Braunschweig*



Netzwerkziel ist *Internal*



Das Netzwerkverhältnis muss auf Route stehen, da die Pakete nicht geNATet werden.



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

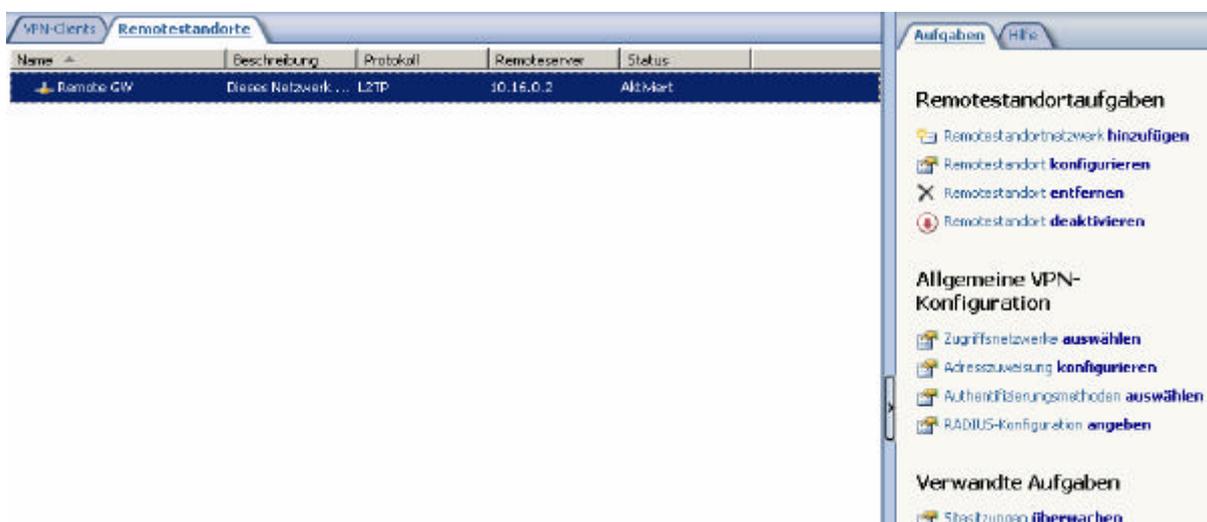


So sieht die neu erstelle Netzwerkregel aus.

Sie haben die Netzwerktopologie geändert. Das Netzwerkdiagramm stellt diese Änderungen nicht dar. Alle Netzwerke in der Netzwerktopologie werden auf der Registerkarte "Netzwerke" aufgeführt.

Netzwerke Netzwerksätze Netzwerkregeln Webverkettung					
R...	Name	Relation	Quellnetzwerke	Zielnetzwerke	
1	Local Host Access	Route	Local Host	All Networks (and ...	
2	VPN Clients to Internal Network	Route	Quarantined VPN Clients VPN Clients	Internal	
3	Internet Access	NAT	Internal Quarantined VPN Clients VPN Clients	External	
4	Braunschweig nach DBK	Route	Standort Braunschweig	Internal	

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>