ISA Server 2004 – Erstellen einer Webverkettung (Proxy-Chain) - Von Marc Grote

---

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

Einleitung

In größeren Firmenumgebungen mit Zweigstellen kommt es häufiger vor, dass in der Zweigstelle ein ISA Server 2004 als Firewall oder Webproxy konfiguriert ist und dieser über den zentralen ISA Server 2004 in der Firmenzentrale eine Verbindung zum Internet herstellt. Diese Art der Anbindung von mehreren Proxy Servern über eine Kaskadierung an das Internet wird als Webverkettung bzw. Proxy Chaining bezeichnet.

Gründe für eine Webverkettung könnten sein:

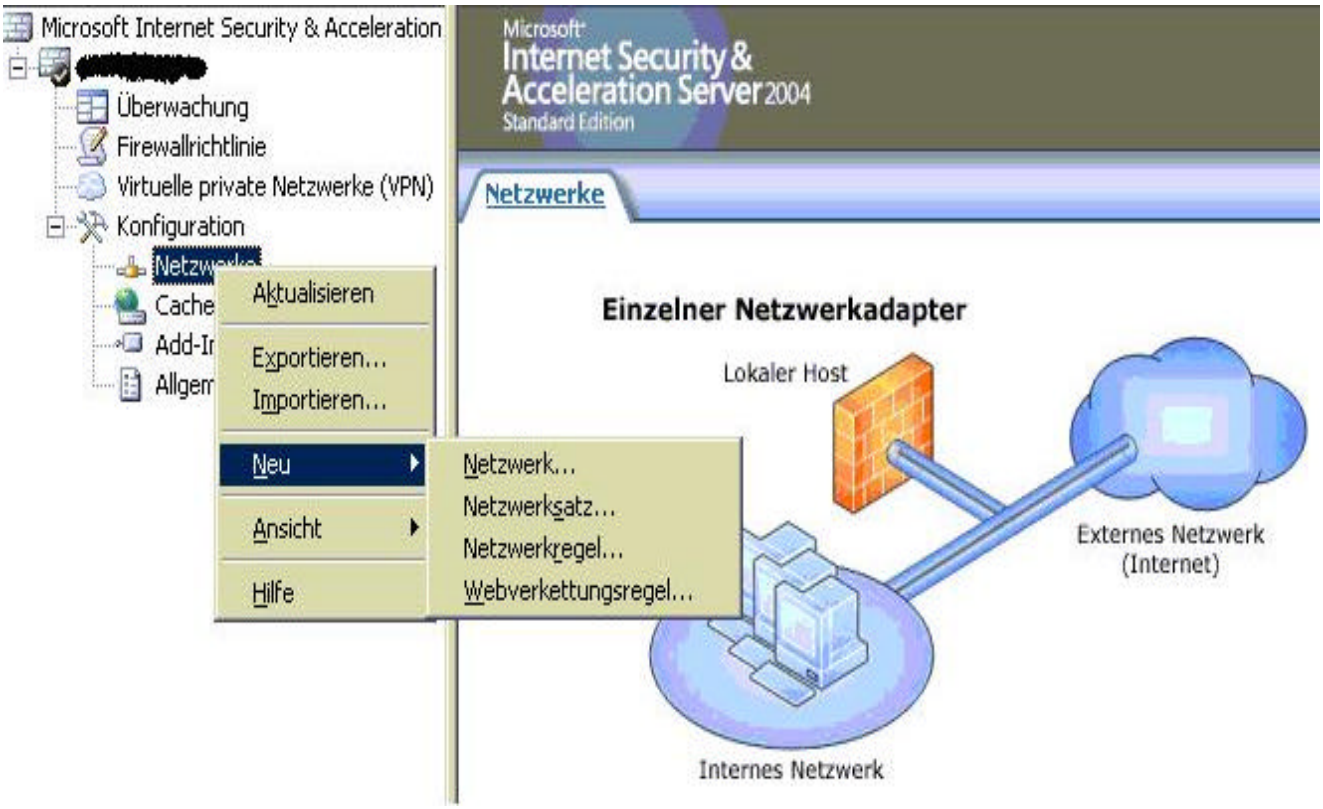
- Ein zentraler Internetzugang aus Sicherheitsgründen, aber Nutzung der Proxy Funktionalitäten zur Reduzierung der Netzwerklast zwischen den Zweigstellen und der Firmenzentrale
- Kaskadierung mit einem weiteren Proxy Server z. B. mit einem Proxy Server eines Rechenzentrums wenn der Firma

Bemerkung:

Eine Webverkettung kann auch zwischen einem ISA Server und einem ***NICHT*** ISA Server hergestellt werden, eine Firewallverkettung hingegen kann ***NUR*** mit ISA Servern durchgeführt werden.

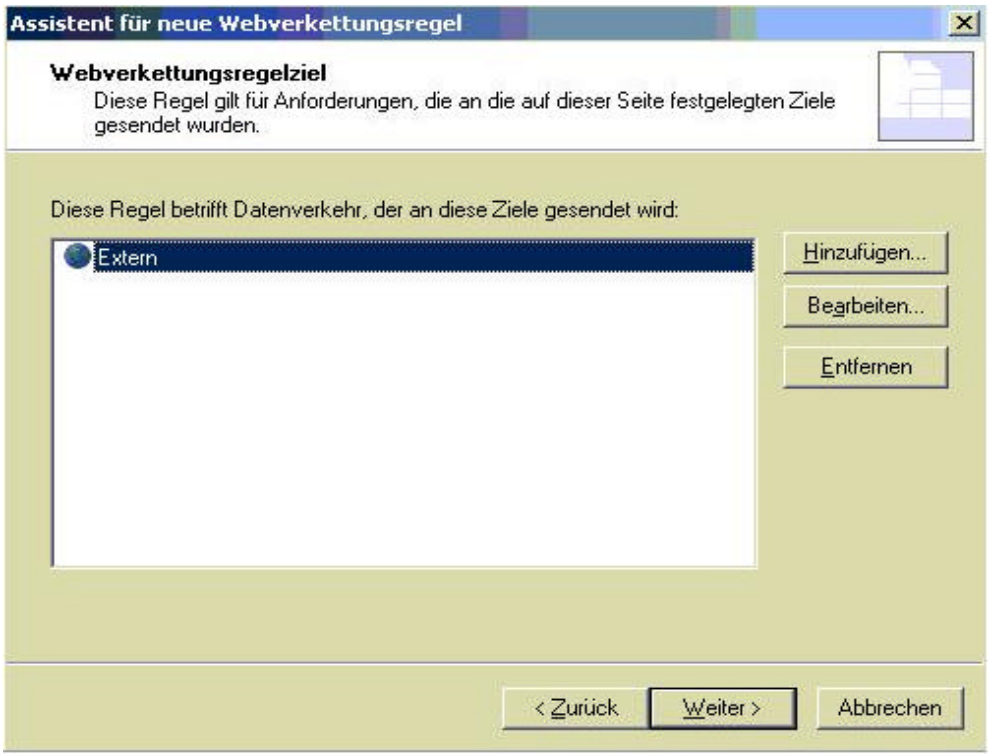
Dieser Artikel beschreibt die Einrichtung einer Webverkettung zwischen einem ISA Server 2004 in einer Zweigstelle und der Firmenzentrale.

Zur Konfiguration der Webverkettung starten Sie die ISA Server Verwaltungskonsole, erweitern den Container ***Konfiguration*** und klicken mit der rechten Maustaste auf ***Netzwerke***. Wählen Sie aus dem Kontextmenü ***Webverkettungsregel*** aus und folgen Sie den Anweisungen des Wizards.



Vergeben Sie einen sinnvollen Namen für die Webverkettungsregel. In diesem Beispiel verwenden wir den Namen ***ISA-Ausstenstelle zu ISA-Firmenzentrale***.

Geben Sie im Fenster ***Webverkettungsregel*** das Ziel für den Datenverkehr an. Da in diesem Beispiel eine Internetverbindung hergestellt werden soll, wählen wir das Netzwerkobjekt ***EXTERN*** aus.



Im Fenster ***Aktion anfordern*** können Sie die Anforderungsverarbeitung konfigurieren. Routingregeln legen fest, ob die Anforderung eines Webproxyclients direkt abgerufen, an einen anderen Upstreamproxyserver oder an ein anderes Ziel gesendet werden sollen.

Anforderungen direkt vom angegebenen Ziel abrufen

Gibt an, dass ISA Server Anforderungen von Webproxyclients direkt an das Internet sendet.

Anforderungen an angegebenen Upstreamserver weiterleiten

Gibt an, dass ISA Server Anforderungen von Webproxyclients zur Verarbeitung an einen Upstreamserver sendet. Der Upstreamserver entscheidet dann, ob die Anforderung zugelassen oder abgewiesen wird.

Delegierung der Anmeldeinformationen für Basisauthentifizierung zulassen

Lässt die Authentifizierung des Clients durch den Webserver zu, an den die Anforderung weitergeleitet wird. Wie der Name vermuten lässt, wird hier nur die Weitergabe der Credentials einer Basisauthentifizierung durchgeführt.

Einstellungen für Upstreamserver

Klicken Sie auf Einstellungen, um den Upstreamserver zu konfigurieren, der die Anforderungen bearbeitet.

Alternativroute

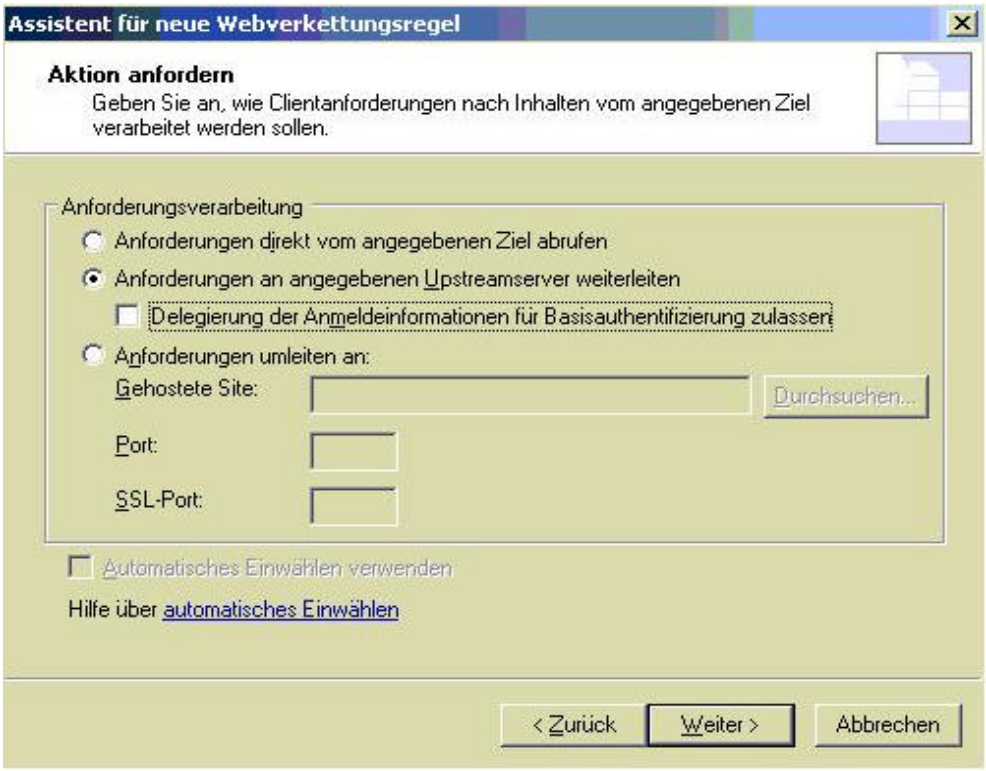
Listet optionale ISA Server-Computer zum Bearbeiten von Anforderungen auf, wenn die Primärroute nicht verfügbar ist. Wenn Sie Upstreamproxyserver auswählen, müssen Sie festlegen, welcher Server verwendet wird.
Klicken Sie auf Einstellungen, um den für die Alternativroute verwendeten Upstreamserver zu konfigurieren.

Anforderungen umleiten an

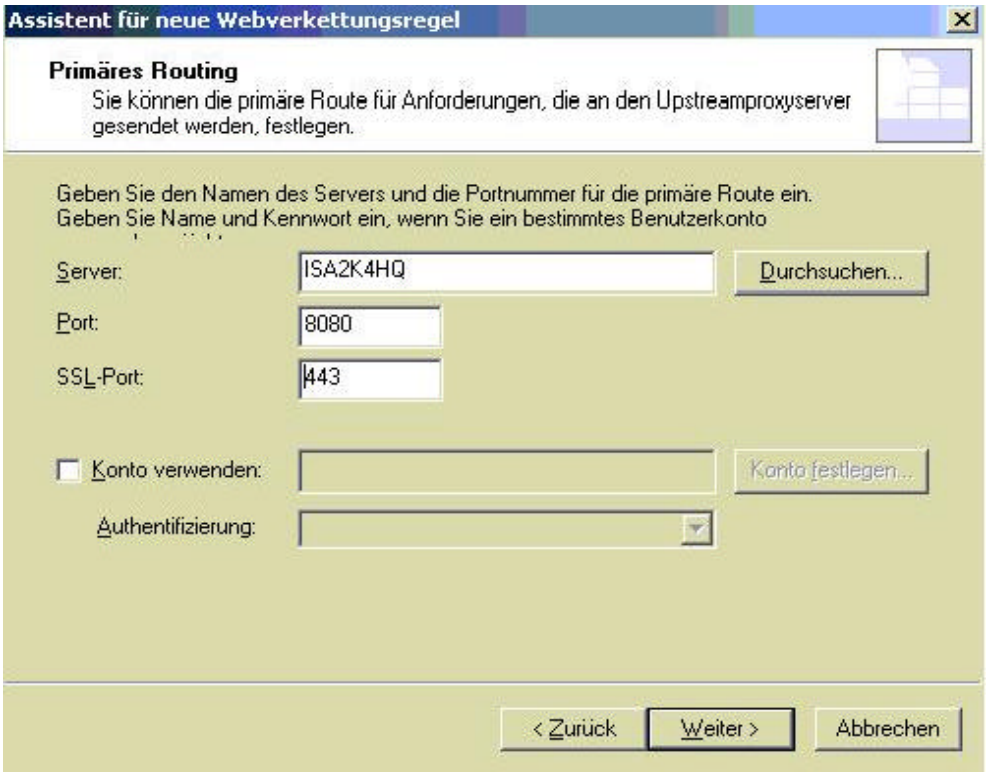
Gibt an, dass ISA Server Anforderungen von Webproxyclients an ein anderes Ziel weiterleitet.
Geben Sie unter Standort die URL des anderen Ziels der Anforderung ein.
Geben Sie unter Port die Portnummer des anderen Ziels ein.
Geben Sie unter SSL-Port die SSL-Portnummer (Secure Sockets Layer) des anderen Ziels ein.

Automatisches Einwählen verwenden

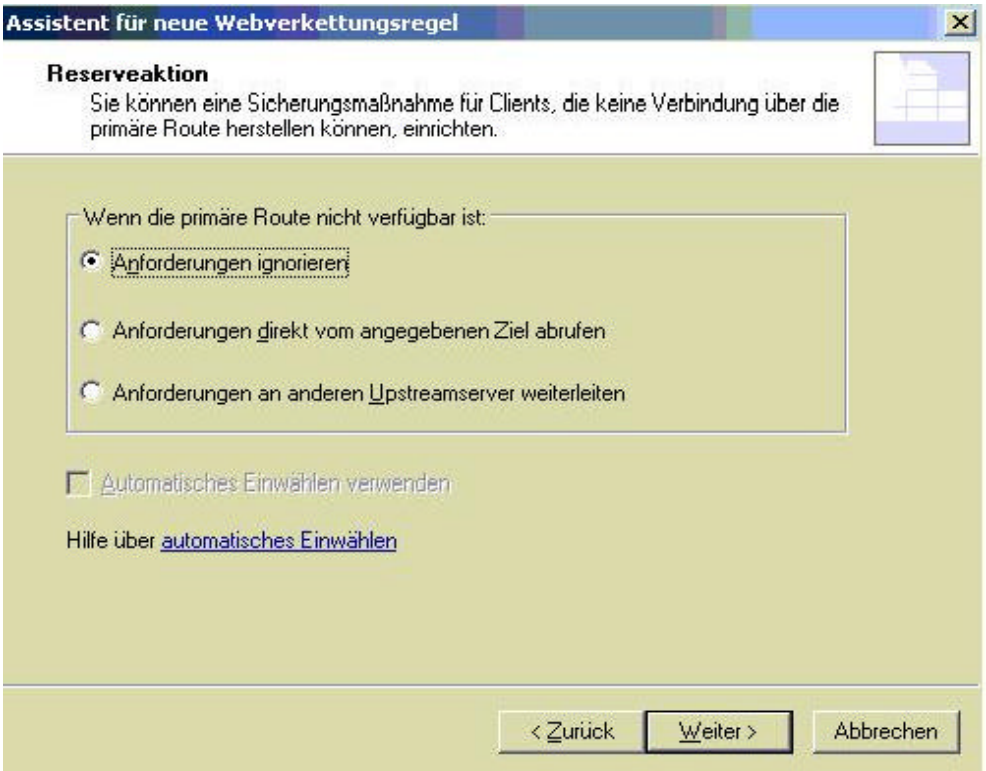
Gibt an, dass ISA Server für die Verbindung zur Primärroute eine DFÜ-Verbindung verwendet. Diese DFÜ Verbindung können Sie ebenfalls in der ISA Verwaltungskonsole erstellen. Ist keine DFÜ-Verbindung vorhanden, bleibt das Feld ausgegraut.



Wenn Sie bei der Anforderungsverarbeitung ***Anforderungen an angegebenen Upstreamserver weiterleiten*** gewählt haben, müssen Sie im Fenster ***Primäres Routing*** den Upstream Proxy und die Port Nummer für HTTP und SSL angeben. Wenn der Upstream Proxy eine Authentifizierung erfordert, müssen Sie auf ***Konto verwenden*** klicken und dort das ***Konto festlegen*** und die Authentifizierungsart (Standard oder WIndows integriert) festlegen.



Im Fenster ***Reserveaktion*** können Sie die Aktion festlegen, wenn die primäre Route nicht verfügbar ist. Aus Redundanzgründen könnten Sie hier einen Reserveserver angeben, indem Sie auf ***Anforderungen an anderen Upstreamserver weiterleiten*** klicken. diesem Beispiel wählen wir ***Anforderungen ignorieren***.



Überprüfen Sie in der Abschlußmeldung des Assistenten noch einmal alle Einstellungen.

Anhand Ihrer Angaben hat der Assistent folgende Webverkettungsregel erstellt.

Zum Schluß können Sie bei Bedarf noch festlegen, wie HTTP- und SSL-Anforderungen weitergeleitet werden sollen. In der Regel ist hier keine Anpassung notwendig.

Klicken Sie zur Anpassung der Weiterleitung mit der rechten Maustaste auf die ***Webverkettungsregel*** und klicken Sie im Kontextmenü auf ***Eigenschaften*** und wählen Sie den Reiter ***Bridging*** aus.

HTTP-Anforderungen umleiten als HTTP-Anforderungen

Legt fest, dass HTTP-Anforderungen als HTTP-Anforderungen umgeleitet werden.

HTTP-Anforderungen umleiten als SSL-Anforderungen

Legt fest, dass HTTP-Anforderungen als SSL-Anforderungen umgeleitet werden. In diesem Fall öffnet ISA Server einen sicheren Kanal zum Server.

SSL-Anforderungen umleiten als HTTP Anforderungen

Legt fest, dass SSL-Anforderungen als HTTP-Anforderungen umgeleitet werden, dass heißt, am ISA Server wird der SSL Tunnel terminiert.

SSL-Anforderungen umleiten als SSL Anforderungen

Legt fest, dass SSL-Anforderungen als SSL-Anforderungen umgeleitet werden. In diesem Fall öffnet ISA Server einen sicheren Kanal zum Server.

Sicherer Kanal (SSL) ist erforderlich

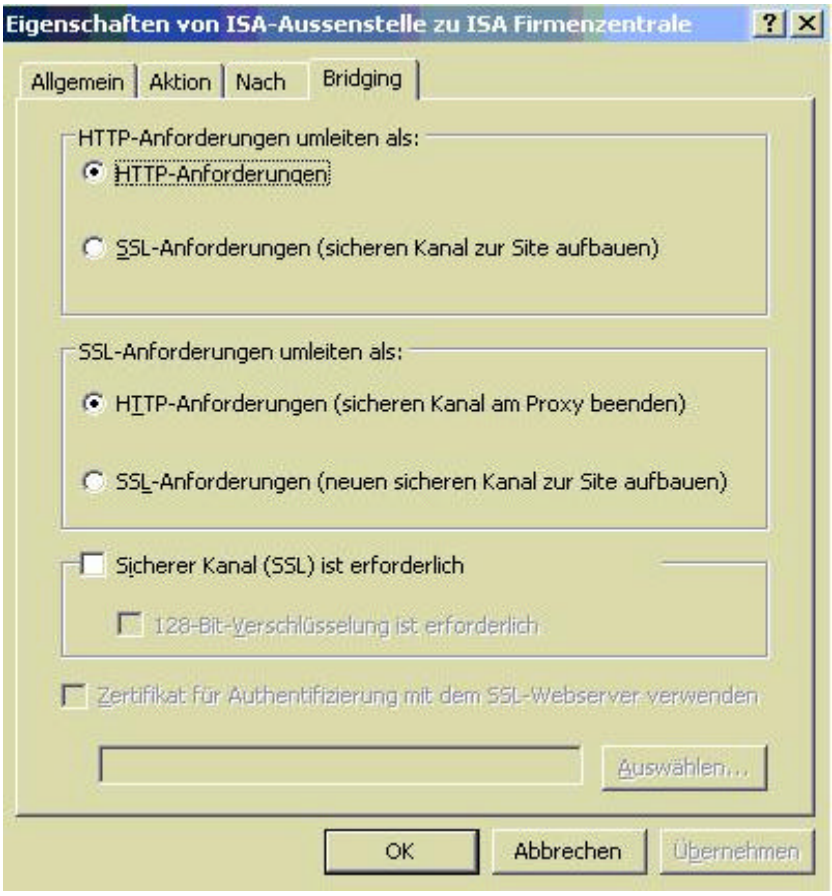
Wählen Sie diese Option aus, um festzulegen, dass der Zugriff nur über einen SSL-Kanal erfolgen darf.

128-Bit-Verschlüsselung ist erforderlich

Klicken Sie auf diese Option, um die 128-Bit-Verschlüsselung auszuwählen.

Zertifikat für Authentifizierung mit SSL-Webserver verwenden

Klicken Sie auf diese Option, um zur Authentifizierung beim SSL-Server ein Zertifikat zu verwenden. Zertifikate fungieren als zusätzlicher Sicherheitsmechanismus zwischen dem ISA Server 2004 und einem SSL-Webserver.



Stand: 05.09.2004/MG. http://www.it-training-grote.de