ISA Server 2004 – Mehrfachnetzwerke - Besonderheiten - Von Marc Grote

---

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

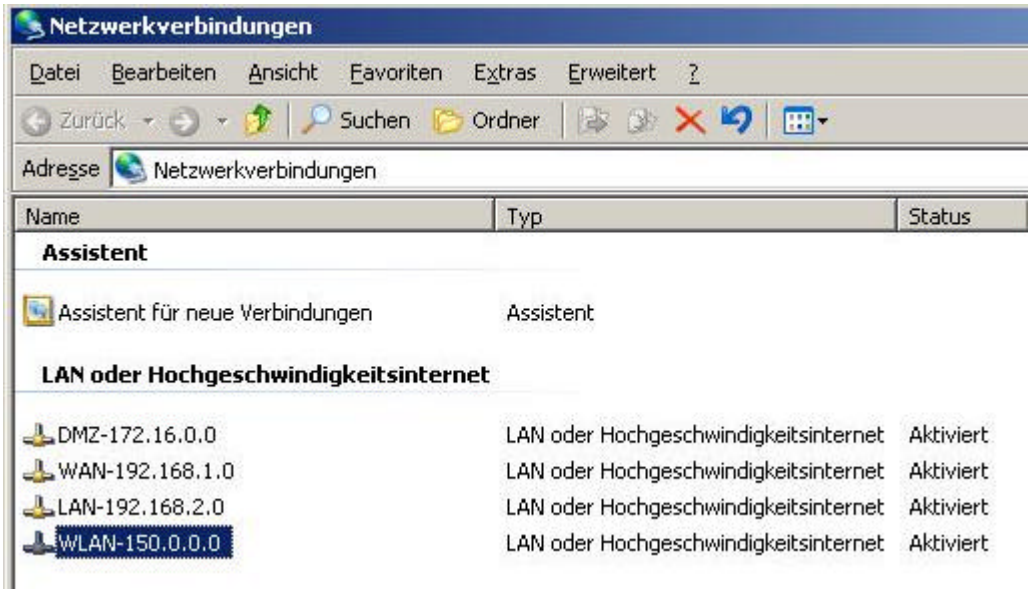
Einleitung

In meinem ersten Artikel habe ich gezeigt, wie man ein Netzwerk mit ISA Server 2004 definiert. Dieser Artikel beschreibt Besonderheiten der Netzwerkkonfiguration. Schwerpunkt dieses Artikels ist die Beschreibung von typischen Konfigurationsfehlern, Erklärung der Beziehung zwischen ISA Server und Routingtabellen, sowie einiger Tipps aus der Praxis.

Basis für diesen Artikel ist ein ISA Server 2004 Standard mit vier Netzwerkkarten auf einem Windows 2003 Standard Server.

Erklärung der Netzwerke:

- DMZ = Netzwerk für die demilitarisierte Zone
  WAN = Verbindung zum Internet
- LAN = Das interne Netzwerk
- WLAN = Spezielles Netzwerksegment für die WLAN Accesspoint Anbindung.



Wie ein Netzwerk konfiguriert wird, lesen Sie bitte hier. Für weitere Informationen zur Einrichtung einer Firewallrichtlinie finden Sie hier.

Zur Auffrischung: Die Konfiguration eines Netzwerkes erfordert folgende Schritte:

- Erstellen des neuen Netzwerkes und Angabe des Netzwerkbereiches
- Erstellen einer Netzwerkregel welche die verbundenen Netzwerke festlegt und den Typ **ROUTE** oder **NAT** festlegt.
- Erstellen einer Firewallrichtlinie welche den Zugriff zwischen den Netzwerken regelt.

Nach der Installation von ISA Server sind fünf Netzwerke konfiguriert

Intern

Bei dem internen Netzwerk handelt es sich um die IP-Adressbereiche des internen Netzwerkes. ISA Server sieht dieses Netzwerk als vertrauenswürdig (mit Ausnahmen - Stichwort: Systemrichtlinie), aber auch als schutzwürdig an. Die IP-Adressbereiche des Netzwerkobjektes intern müssen mit der Windows Routingtabelle für das interne Interface übereinstimmen.

Externes Standardnetzwerk

Das externe Standardnetzwerk beinhaltet alle IP-Adressen, die nicht ausdrücklich zu einem anderen Netzwerk gehören. Nach der Installation beinhaltet das externe Standardnetzwerk alle Adressen, die nicht im internen Netzwerk enthalten sind, die IP-Adresse des lokalen Hostnetzwerks (127.0.0.1) und die IP-Adressen aller anderen Netzwerkadapter des ISA Server-Computers.

Das externe Standardnetzwerk gilt als **NICHT** vertrauenswürdiges Netzwerk. Daher wird das Netzwerkverhältnis zum externen Standardnetzwerk in der Regel als NAT (Network Address Translation) konfiguriert. Dadurch können Clients des Quellnetzwerks auf externe Standardzielnetzwerke zugreifen, das externe Standardnetzwerk jedoch nicht auf das Quellnetzwerk

Lokaler Host

Dieses Netzwerk steht für den ISA Server-Computer. Das lokale Hostnetzwerk kann **NICHT** geändert oder gelöscht werden.

VPN-Clients

Dieses Netzwerk umfasst die Adressen der derzeit verbundenen Clients. Der Bereich der möglichen Adressen wird bei der Konfiguration der VPN-Eigenschaften festgelegt. Das VPN-Clientnetzwerk kann nicht gelöscht werden.

Quarantänen-VPN-Clients

Zu diesem Netzwerk gehören die Adressen von VPN-Clients, die noch nicht aus der Quarantäne entlassen wurden. Das Quarantänen-VPN-Clientnetzwerk kann nicht gelöscht werden.

Netzwerkvorlagen

ISA Server enthält Netzwerkvorlagen, die häufig vorkommende Netzwerktopologien abbilden. Mithilfe der Netzwerkvorlagen konfigurieren Sie die Firewallrichtlinien für den Datenverkehr zwischen den Netzwerken. Die Verwendung von Netzwerkvorlagen ist nicht zwingend vorgeschrieben. Ein erfahrener Administrator kann die Netzwerke/Netzwerkregeln und Firewallrichtlinien auch per Hand konfigurieren.

ISA Server 2004 enthält die folgenden Netzwerkvorlagen (Auszug aus der Online Hilfe leicht modifiziert):

Edgefirewall

Bei dieser Vorlage wird eine Netzwerktopologie angenommen, bei der sich ISA Server an der äußeren Schnittstelle des Netzwerks, dem so genannten Perimeter, befindet. Ein Netzwerkadapter ist hierbei mit dem internen Netzwerk verbunden. Der andere Netzwerkadapter verfügt hingegen über eine Verbindung mit einem externen Netzwerk (Internet). Bei Auswahl dieser Vorlage können Sie den gesamten ausgehenden Datenverkehr zulassen oder den ausgehenden Datenverkehr einschränken, so dass nur der Webzugriff gestattet wird. Eine Edgefirewall gilt nicht als sicherste Firewall Lösung, weil ein Angreifer nur eine Firewall überwinden muß.

3-Abschnitt-Umkreisnetzwerk - (Trihomed Firewall)

Bei dieser Vorlage wird eine Netzwerktopologie angenommen, bei der ISA Server mit dem internen Netzwerk, dem externen Netzwerk und einem Umkreisnetzwerk (auch als DMZ, demilitarisierte Zone oder abgeschirmtes Subnetz bezeichnet) verbunden ist. Eine Trihomed Firewall ist eine Firewall mit drei Netzwerkkarten und wird häufig auch als Poor Man's Firewall bezeichnet.

Frontfirewall-Netzwerkvorlage

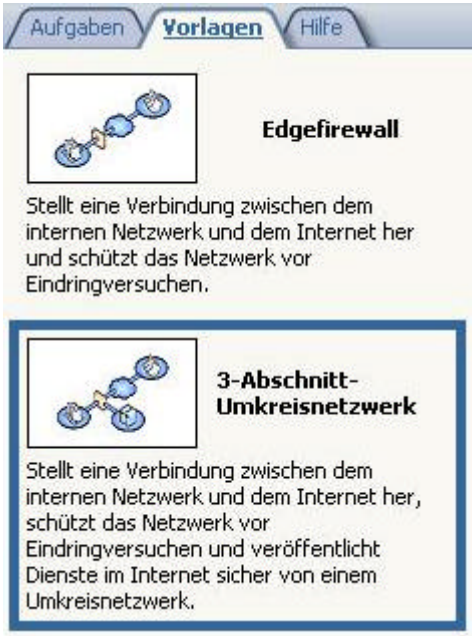
Bei dieser Vorlage wird eine Netzwerktopologie angenommen, bei der sich ISA Server an der äußeren Schnittstelle eines Netzwerks befindet und zum Schutz des internen Netzwerks ein weiterer Firewall am Back-End konfiguriert ist.

Backfirewall-Netzwerkvorlage

Bei dieser Vorlage wird eine Netzwerktopologie angenommen, bei der ISA Server an der Schnittstelle zwischen einem Umkreisnetzwerk und dem internen Netzwerk eingesetzt wird und zum Schutz des internen Netzwerks am Back-End ein weiterer Firewall konfiguriert ist. Weitere Informationen finden Sie unter Backfirewall-Netzwerkvorlage.

Einzelner Netzwerkadapter

Bei dieser Vorlage wird eine Netzwerkkonfiguration mit einem einzelnen Netzwerkadapter angenommen, der sich innerhalb eines Umkreis- oder Firmennetzwerks befindet. In dieser Konfiguration dient ISA Server als Webproxy- und Cacheserver. Diese Netzwerkvorlage entspricht in etwa der Installation eines ISA Server 2000 im Cache Mode.



Hintereinander angeordnete Netzwerke

Sehr häufig stellt sich auch die Frage, wie der ISA Server konfiguriert werden muss, wenn sich die Netzwerke hintereinander angeordnet befinden, dass heißt, sich hinter dem ISA Server weitere Netzwerke als das interne Netzwerk befinden.

Bei einer Konfiguration hintereinander angeordneter Netzwerke verfügt ein Netzwerkadapter über Routen zu einem fremden Netzwerk. In den meisten Fällen unterstützt ISA Server derartige Konfigurationen nicht, wobei jedoch folgende Ausnahmen gelten:

- Ein IPSec-Tunnel der zwischen zwei Standorten besteht.
- Das vordefinierte externe Netzwerk kann sich hinter dem als Standardgateway dienenden Netzwerkadapter befinden.
- Quarantänen-VPN-Clients können niemals direkt mit einem Netzwerk verbunden sein.

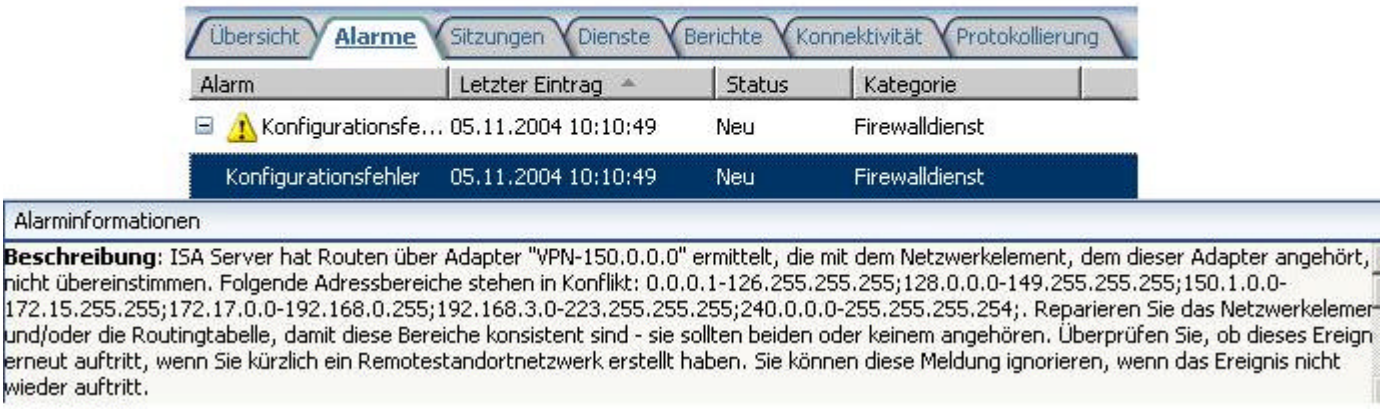
Angenommen, ein Netzwerkadapter mit der Adresse 10.0.0.1 ist das Standardgateway. Außerdem verfügt dieser Netzwerkadapter über Routen zu den Adressen ...
10.X.X.X und
30.X.X.X,
wobei keine Routen (in keinem Netzwerkadapter) für die Adressen 20.X.X.X vorhanden sind. Weiterhin wird in diesem Szenario davon ausgegangen, dass Sie zwei Netzwerke eingerichtet haben:
Netzwerk A: 10.0.0.0–10.255.255.255
Netzwerk B: 30.0.0.0–30.255.255.255
Es sind keine Routen für die Netzwerkadressen im Bereich 20.0.0.0–20.255.255.255 definiert, daher werden diese als Teil des externen Standardnetzwerks angesehen.

Das externe Standardnetzwerk wird als "hinter Netzwerk A befindlich" angesehen, da der Adapter von Netzwerk A eine Route zum externen Standardnetzwerk besitzt, jedoch diesem Netzwerk nicht zugeordnet ist. (Die Adresse des Adapters gehört nicht zum externen Netzwerk.)
Netzwerk B befindet sich dieser Definition nach ebenfalls hinter Netzwerk A. Allerdings ist Netzwerk B nicht das externe Standardnetzwerk. ISA Server betrachtet dies jedoch als eine fehlerhafte Konfiguration und das Netzwerk wird vorübergehend getrennt.

Zur Konfiguration von ISA Server werden die beiden Routen (zu 10.X.X.X und 30.X.X.X) in einem einzelnen Netzwerk zusammengefasst. ISA Server kann diese beiden Adressbereiche nicht als eindeutige Netzwerke auffassen, da beide demselben Netzwerkadapter zugeordnet sind.

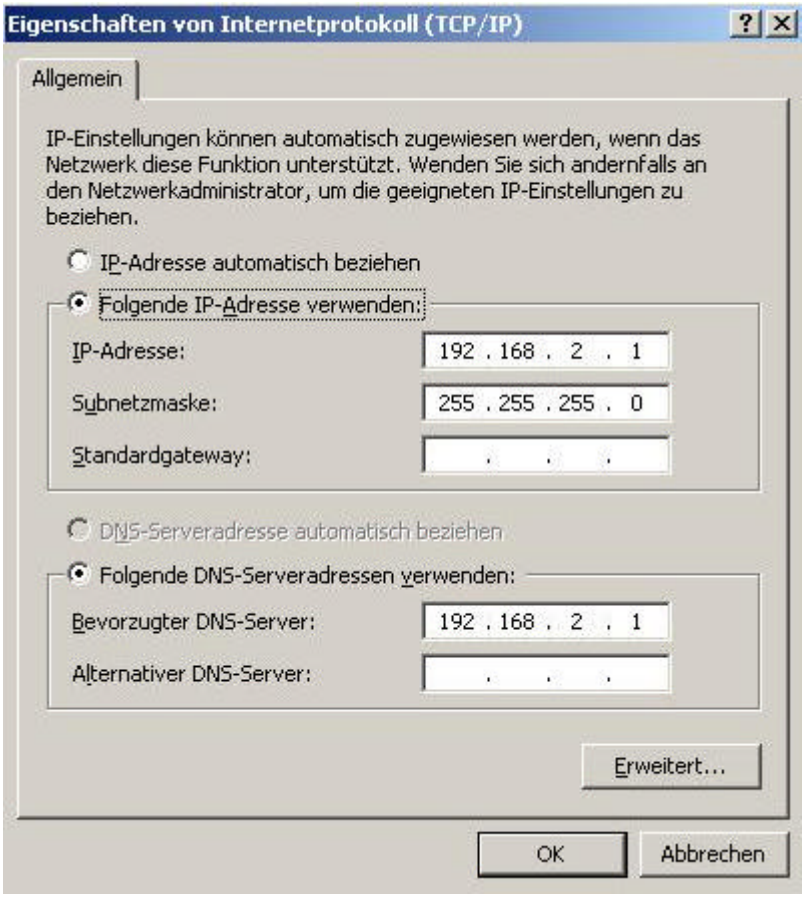
ISA Server Fehlermeldung "ISA Server hat Routen über den Adapter "XXXXX" ermittelt, die mit dem Netzwerkelement, dem dieser Adapter angehört, nicht übereinstimmen."

Auf diese Fehlermeldung suchen viele Administratoren seit Erscheinen des ISA Server 2004 in den Newsgroups eine Antwort zur Lösung des Problems. Aus diesem Anlass sollen hierzu einige klärende Worte gesagt werden.

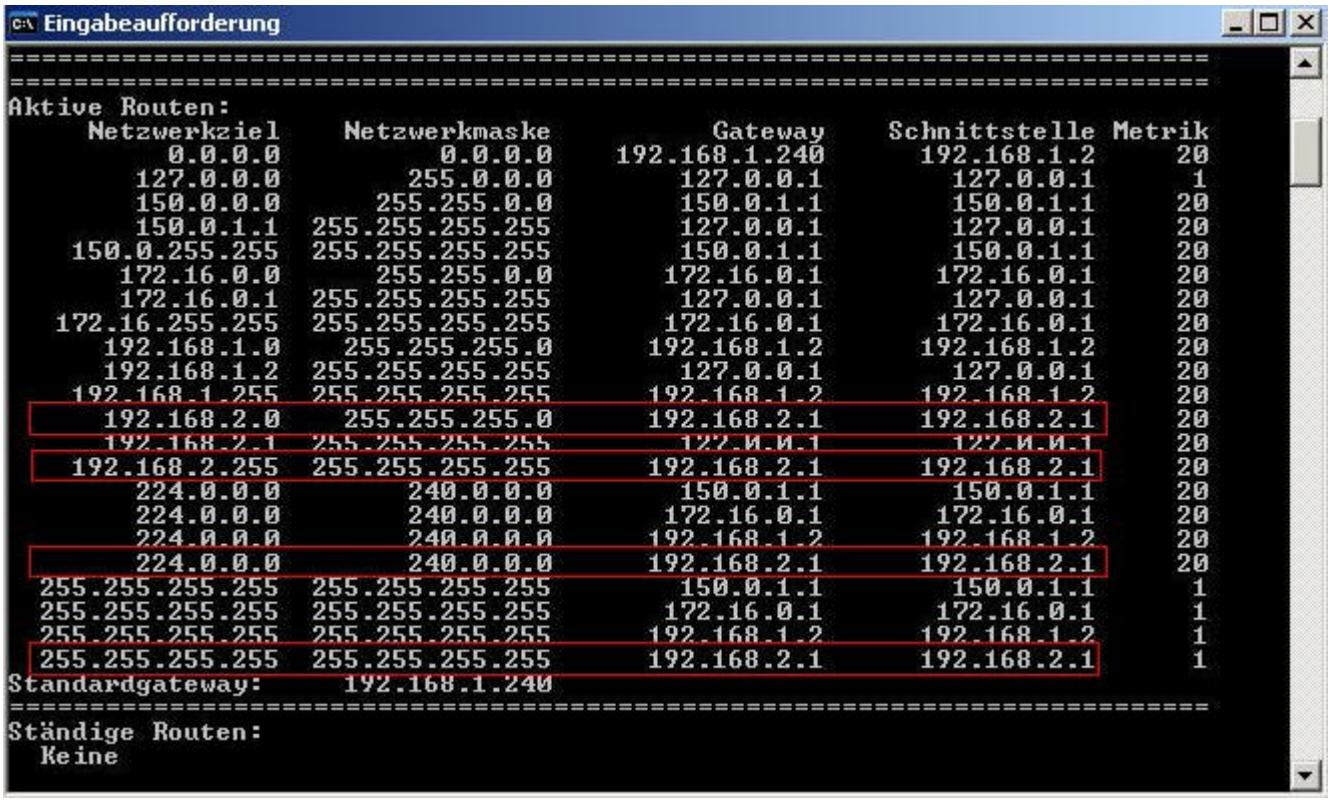


Das (korrekt konfigurierte) interne Netzwerk in diesem Artikel ist wie folgt definiert:

Das interne Netzwerkinterface am ISA hat folgende Konfiguration:



ISA Server versucht bei der Ermittlung des Netzwerkobjektes einen Netzwerkadapter zu finden, der eine IP-Adresse aus diesem Netzwerkbereich hat.
ISA Server ermittelt diese Informationen anhand der Windows 2003 Routingtabelle.
Achten Sie in diesem Beispiel auf die Schnittstelle **192.168.2.1.** Es folgt ein Auszug der Windows 2003 Routingtabelle.



Von Bedeutung für den ISA Server ist hier nur die Route ...

192.168.2.0 255.255.255.0 192.168.2.1 192.168.2.1

Bei den anderen Routen handelt es sich um Multicast / Broadcast Adressen und müssen nicht berücksichtigt werden.

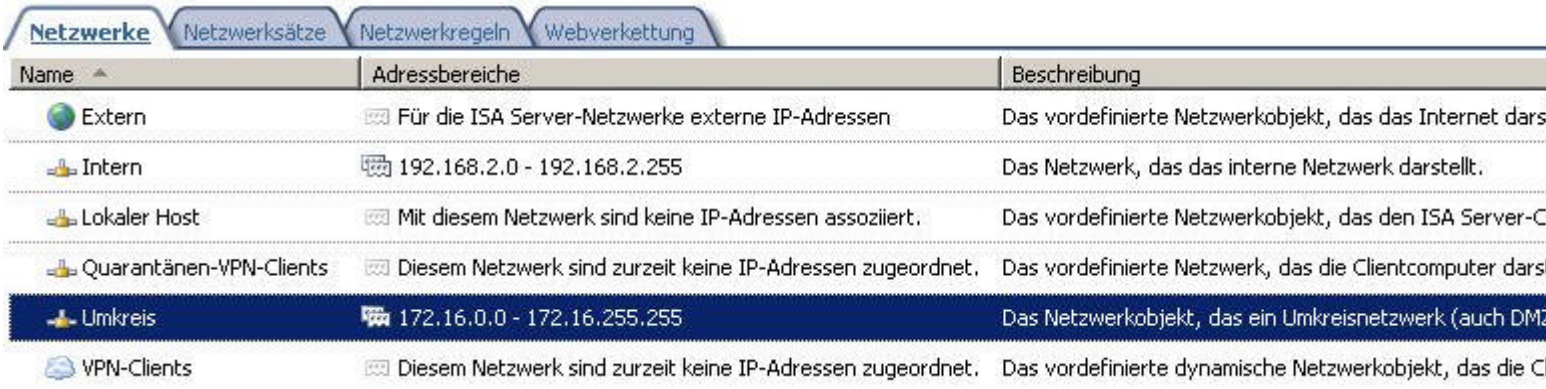
Erläuterung der anderen Routen:
0.0.0.0 ist die Default Route
127.0.0 ist die Loopback-Adresse
192.168.2.0 ist die Netzwerk-Route für das Netzwerk 150.3.0
192.168.2.1 (255.255.255.255) ist die Host-Route des lokalen Hosts
192.168.2.255 ist die Subnetz-Broadcast-Adresse
224.0.0.0 ist für das Multicasting
255.255.255.255 ist für die limitierte Broadcast-Adresse

Die oben beschriebene Fehlermeldung tritt dann auf, wenn Routen nicht mit dem internen Netzwerkobjekt übereinstimmen oder der IP-Adressbereich des internen Netzwerkobjektes nicht richtig definiert wurde. Ein falsch konfiguriertes Netzwerk kann dazu führen, dass ISA Server das Netzwerk nicht schützen kann weil Adressbereiche falsch interpretiert werden.

Eine detaillierte Erklärung zu diesem Thema finden Sie hier.

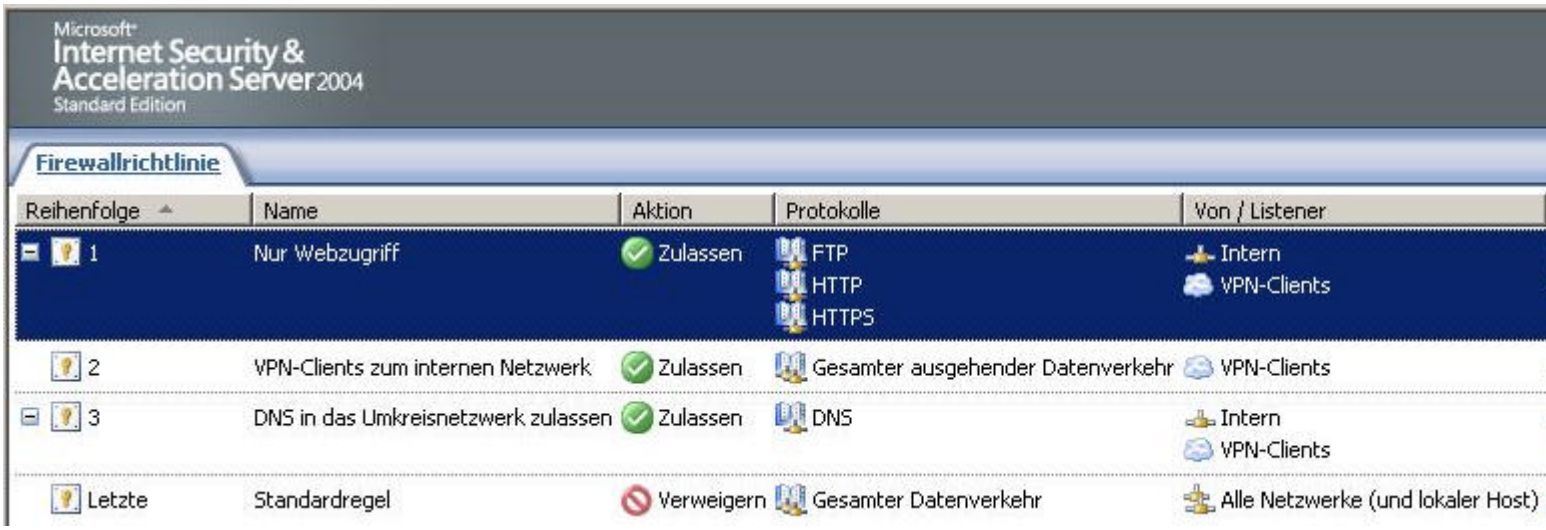
Trihomed DMZ Beispiel

Zum Abschluss dieses Artikels ein Beispiel einer ISA Server 2004 Konfiguration mit der Netzwerkvorlage 3-Abschnitt Umkreisnetzwerk.
Die folgenden Grafiken sollen Ihnen einen Überblick über die Flexibilität des ISA Servers in Bezug auf die Multinetwork-Funktionalitäten geben.
Sie sehen hier ein Netzwerk mit dem Namen Umkreis, welches das Umkreisnetzwerk, auch DMZ genannt, darstellt.



Die Netzwerkregel ist auf **NAT** für interne Kommunikation mit dem Umkreisnetzwerk und **ROUTE** vom Umkreisnetzwerk mit **EXTERN** konfiguriert.

Für das neu erstellte Netzwerk wird basierend auf der gewählten Einstellung des Wizard eine entsprechende Firewallrichtlinie erstellt.



Stand: 07.11.2004/MG. http://www.it-training-grote.de