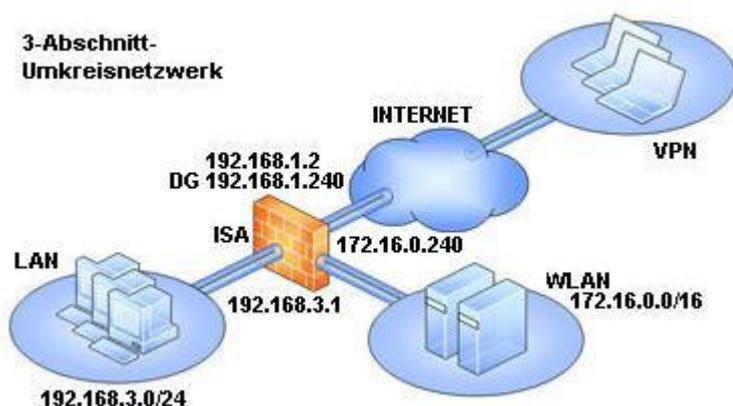


## ISA Server 2004 – ISA Server 2004 Einrichtung eines 3-Abschnitt-Umkreisnetzwerk - Von Marc Grote

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

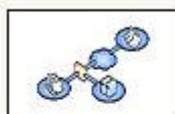
Dieser Artikel beschreibt die Einrichtung eines **3-Abschnitt-Umkreisnetzwerk** mit Hilfe des ISA Server 2004 zum Schutz vor Zugriffen durch Wireless LAN Clients. Die folgende Grafik zeigt den Aufbau der Infrastruktur für diesen Artikel.



ISA Server 2004 stellt verschiedene Netzwerkvorlagen zur Einrichtung einer sicheren Infrastruktur zur Verfügung:

- ✗ Edgefirewall
- ✗ 3-Abschnitt-Umkreisnetzwerk
- ✗ Frontfirewall
- ✗ Backfirewall
- ✗ Einzelner Netzwerkadapter

Wir konzentrieren uns auf die Besonderheiten der 3-Abschnitt-Umkreisconfiguration.



### 3-Abschnitt-Umkreisnetzwerk

Stellt eine Verbindung zwischen dem internen Netzwerk und dem Internet her, schützt das Netzwerk vor Eindringversuchen und veröffentlicht Dienste im Internet sicher von einem Umkreisnetzwerk.

Hilfe zur Einrichtung eines Netzwerkes finden Sie [hier](#). Für erweiterte Fragen zur Netzwerkkonfiguration lesen Sie diesen [Artikel](#).

## Was ist eine DMZ

**DMZ** ist die Abkürzung für **De**Militarisierte **Z**one und beschreibt einen gesonderten, geschützten Bereich innerhalb eines Firewallsystems zur Platzierung von Servern/Diensten wie Webserver, DNS-Server und Mailserver. Sinn einer DMZ ist die Schaffung einer zusätzlichen Sicherheitszone für Dienste, welche von Extern genutzt werden sollen, aber aus Sicherheitsgründen nicht im internen Netzwerk platziert werden soll. Es gibt

verschiedene Arten von DMZ. Klassisch gibt es das hier beschriebene 3-Abschnitt-Umkreisnetzwerk (Trihomed) und die Back-to-Back Firewall. Das 3-Abschnitt-Umkreisnetzwerk wird sehr häufig als [Poor-Man's Firewall](#) bezeichnet, weil ein potentieller Angreifer nur einen Host überwinden muss.

Für weiter führende Informationen zum Thema DMZ, lesen Sie sich folgende [Artikel](#) durch.

## Einrichtung

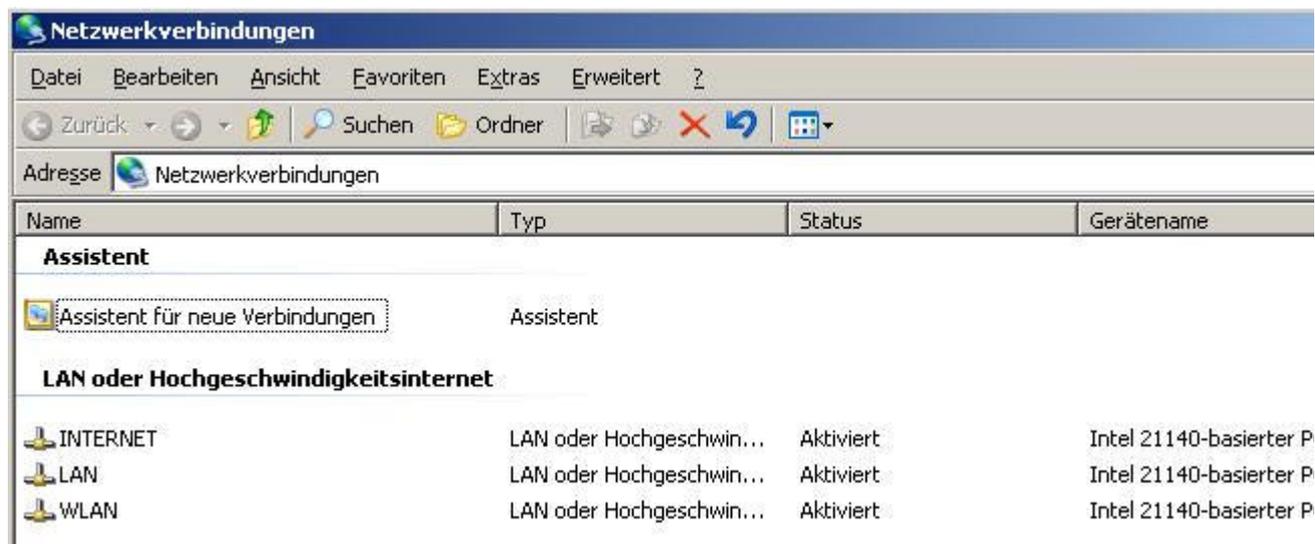
Grundsätzlich bestehen zwei Möglichkeiten bei der Einrichtung eines 3-Abschnitt-Umkreisnetzwerk.

- ✦ Mit Hilfe der vordefinierten Netzwerkvorlage **3-Abschnitt-Umkreisnetzwerk**
- ✦ Händisch mit Hilfe von selbst erstellten Netzwerken, Netzwerkregeln und Firewallregeln.

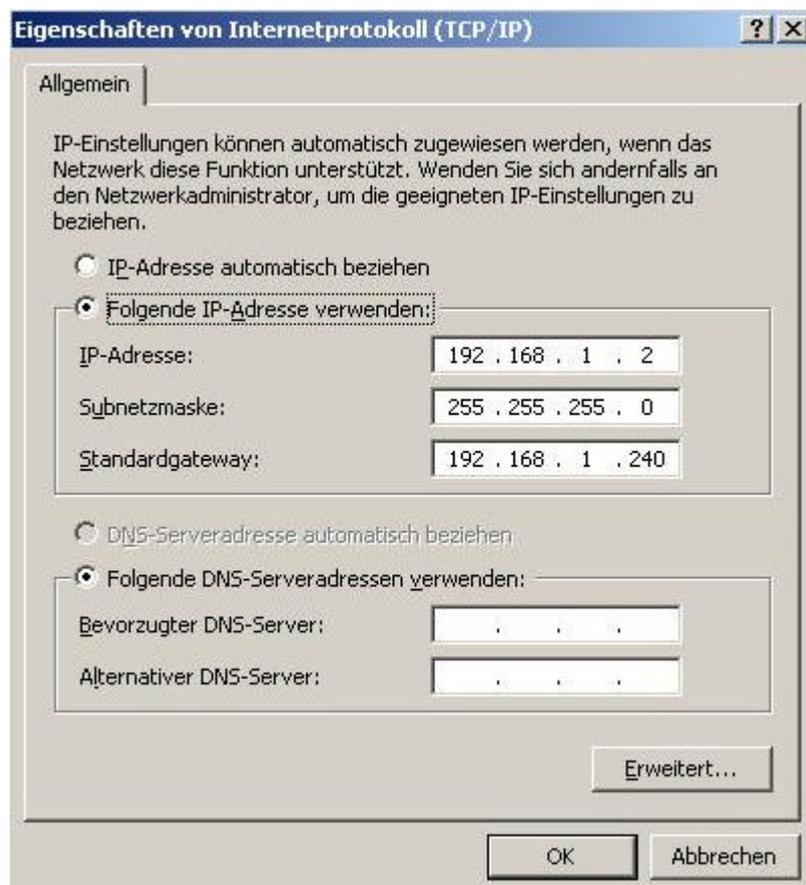
In diesem Artikel wird die Installation zu Demonstrationszwecken mit Hilfe der Netzwerkvorlage vorgenommen, nach erfolgreicher Installation das 3-Abschnitt-Umkreisnetzwerk jedoch weitestgehend auf die Anforderungen in diesem Artikel modifiziert.

Installieren Sie ganz normal einen ISA Server 2004, wie in folgendem [Artikel](#) beschrieben. Nach erfolgter Installation können Sie mit Hilfe der ISA Server Managementkonsole das Netzwerkdesign umstellen.

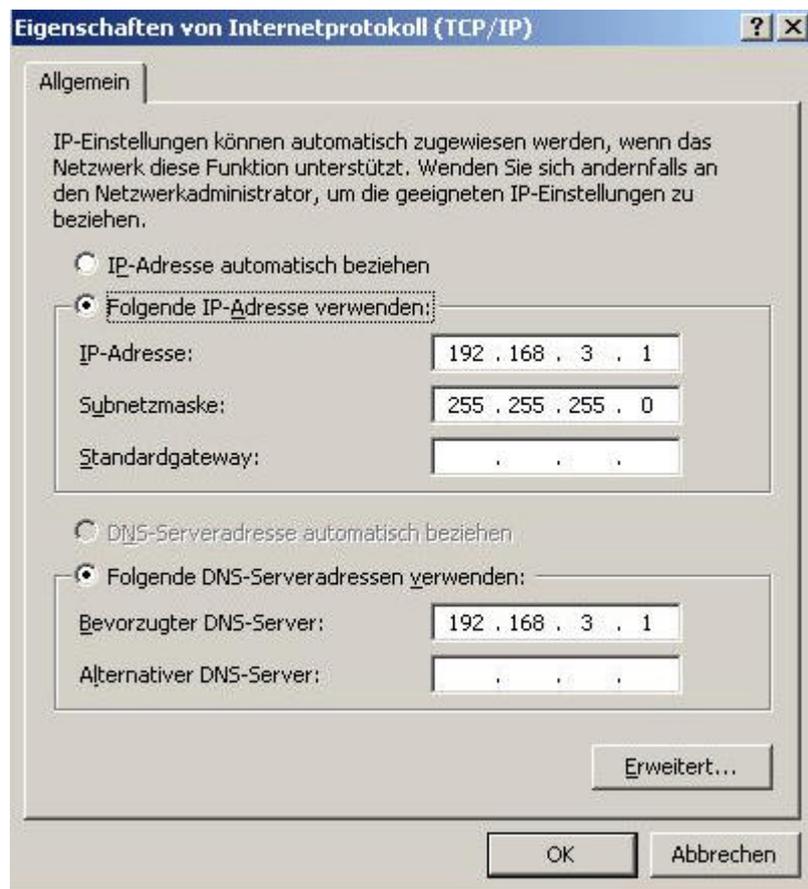
Für die Einrichtung eines 3-Abschnitt-Umkreisnetzwerkes ist ein ISA Server mit drei Netzwerkkarten erforderlich. Benennen Sie jede Netzwerkkarte nach Ihre Funktion, dass erleichtert die spätere Arbeit mit dem ISA erheblich, da Sie immer wissen, welche Netzwerkkarte welche Funktion hat.



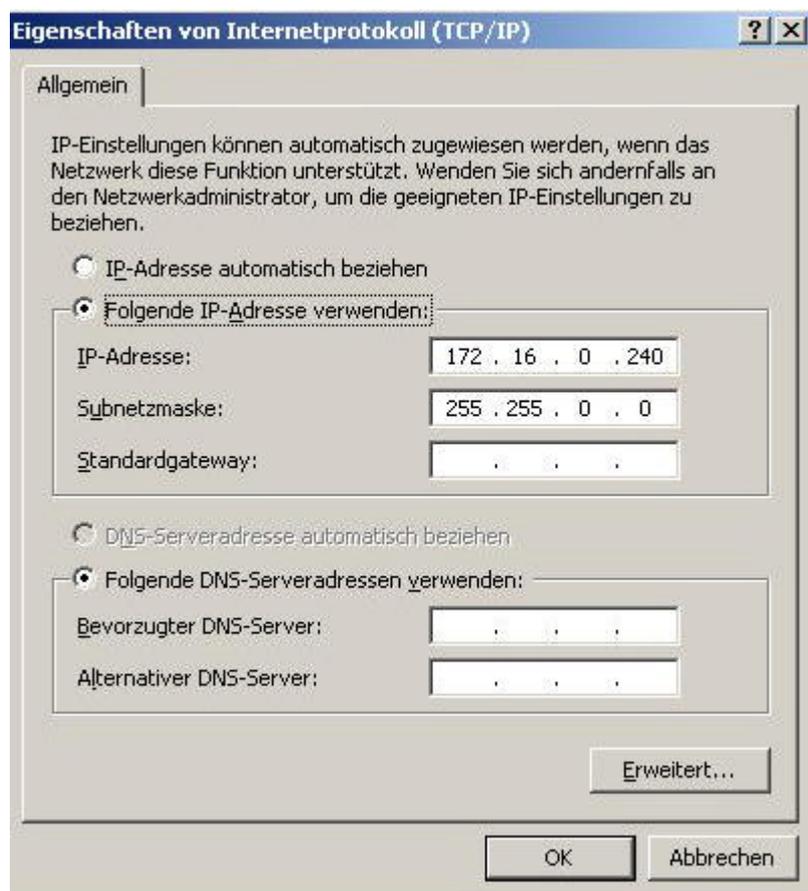
Das Interface **INTERNET** hat ein gesetztes Standardgateway auf einen vorgeschalteten DSL-Router. Die IP-Adresse stammt aus dem Bereich der privaten IP-Adressen.



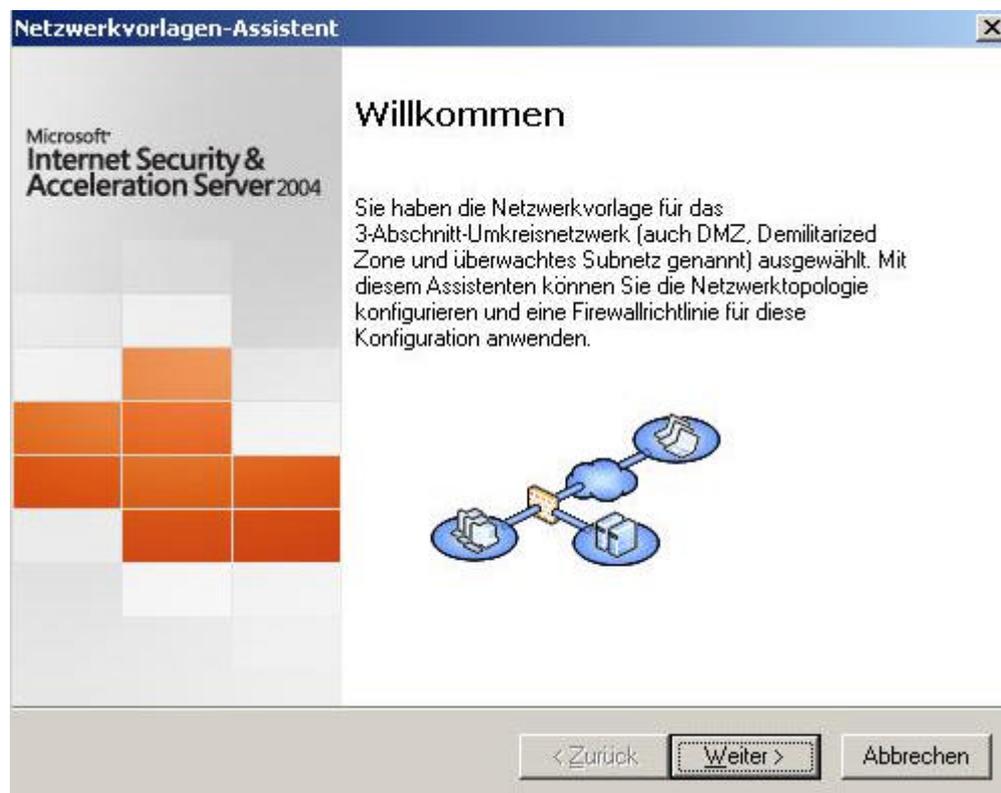
Das Interface **LAN** besitzt eine IP-Adresse aus dem privaten Adressbereich und einen Eintrag für einen DNS Server, welcher auf dem ISA Server installiert ist. Der DNS Dienst auf dem ISA Server leitet DNS Anfragen an einen externen DNS-Server weiter. Es bestehen grundsätzlich mehrere Möglichkeiten zur Einrichtung einer Namensauflösung. Lesen Sie [hier](#) mehr zum Thema DNS-Namensauflösung.



Das Interface **WLAN** besitzt ebenfalls eine IP-Adresse aus dem privaten Adressbereich, aber **KEIN** Standardgateway.



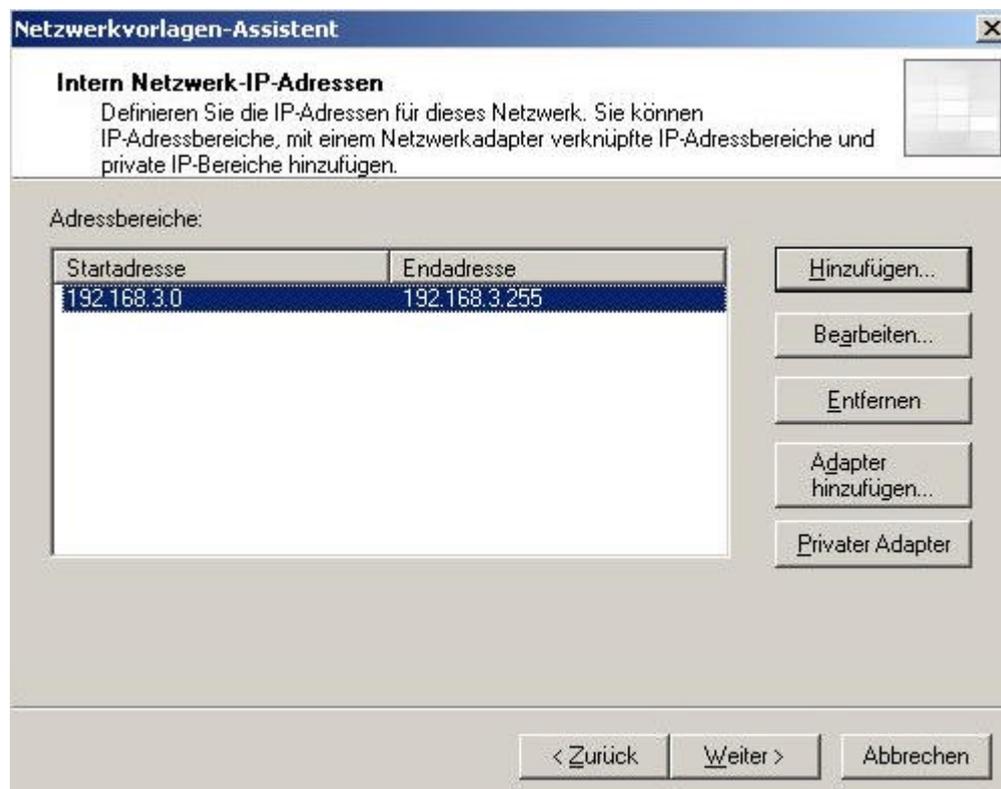
Starten Sie den Netzwerkvorlagen Wizard, indem Sie in der ISA Server Managementkonsole auf **Konfiguration - Netzwerke** klicken und dann im rechten Fenster auf den Reiter **Vorlagen** klicken und dort **3-Abschnitt-Umkreisnetzwerk** auswählen.



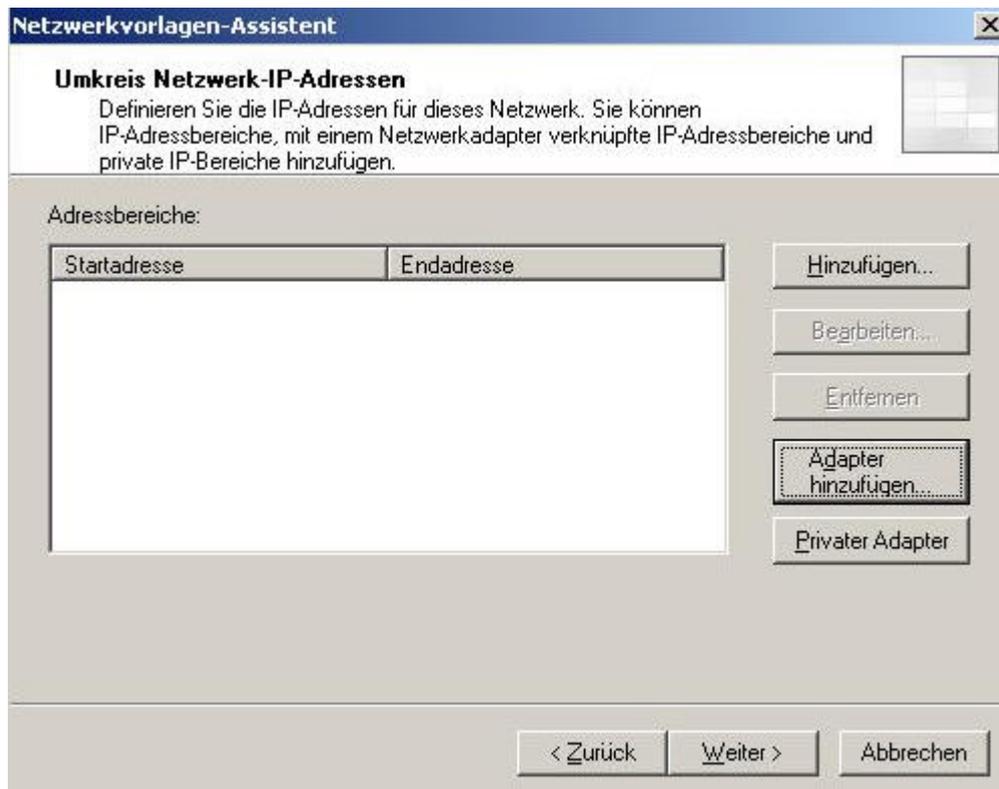
Sie können die vorhandene Konfiguration in eine XML-Datei exportieren um notfalls wieder auf die alte Netzwerkkonfiguration zurückgreifen zu können. Klicken Sie dazu auf **Exportieren** und setzen Sie danach den Vorgang durch Klicken auf **Weiter** fort.



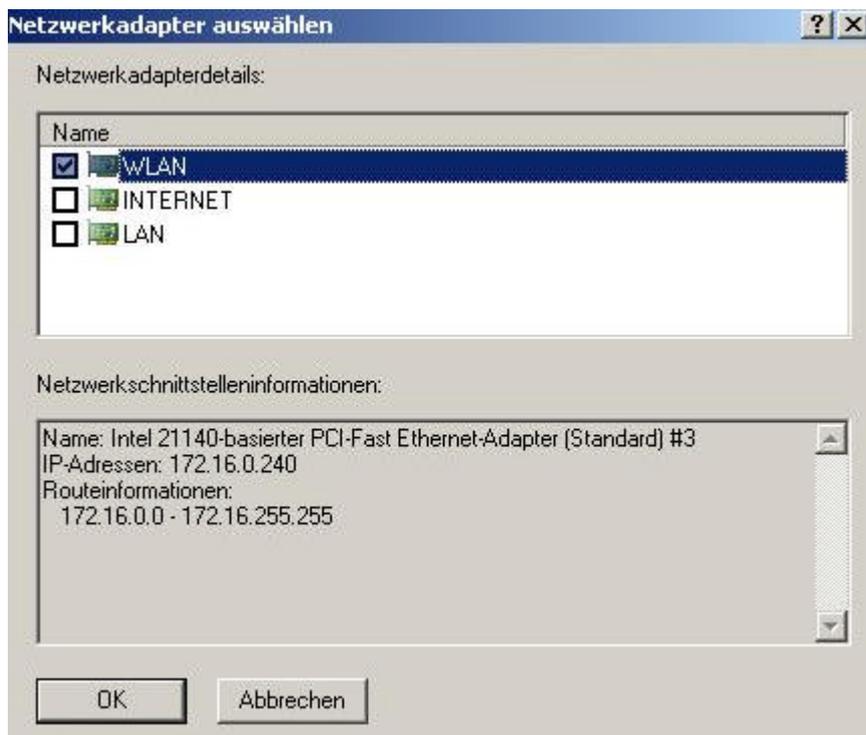
Spezifizieren Sie jetzt den IP-Adressbereich des internen Netzwerkes. Sie können den IP-Adressbereich manuell angeben, oder einen IP-Adressraum auswählen, indem Sie auf **Adapter hinzufügen** klicken und dort den entsprechenden Adapter auswählen (Sie sehen jetzt, warum es Sinn macht, den Netzwerkkarten einen entsprechenden Namen zu vergeben).



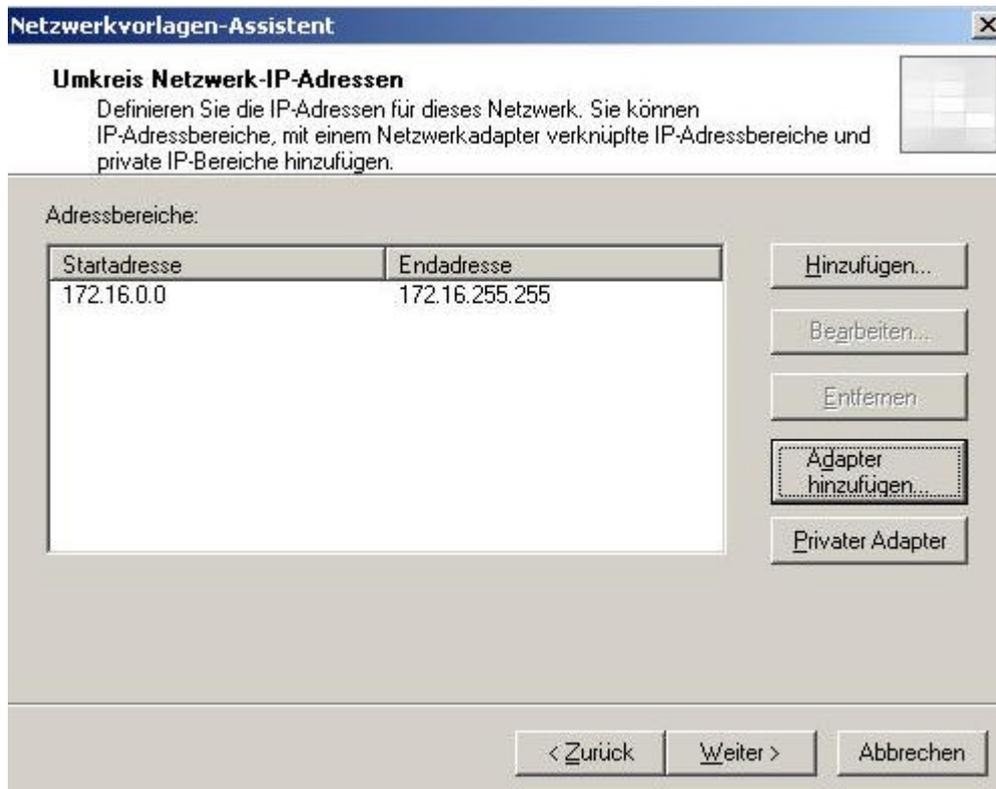
Konfigurieren Sie in diesem Fenster den IP-Adressbereich für das Umkreis Netzwerk (WLAN). Sie können den IP-Adressbereich manuell eingeben oder auf **Adapter hinzufügen** klicken und den Adapter **WLAN** auswählen.



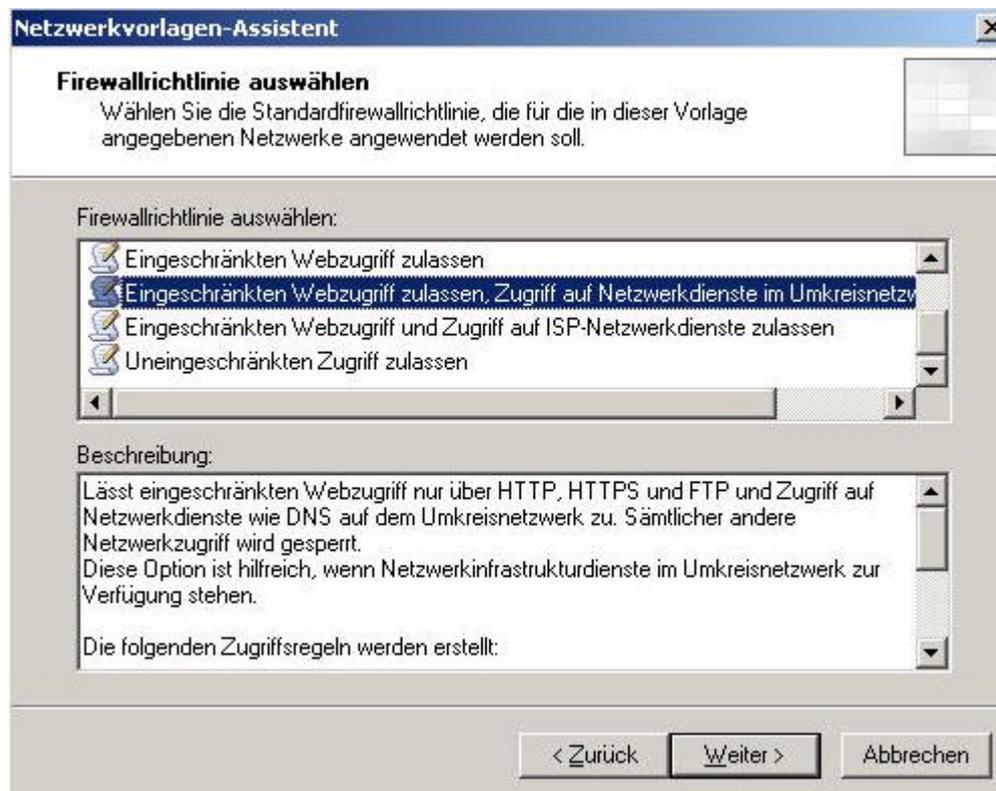
Wählen Sie den Adapter **WLAN** aus.



Nach Auswahl des Netzwerkadapters **WLAN** taucht der korrekte IP-Adressbereich auf.



Der Netzwerkvorlagen-Wizard stellt eine begrenzte Anzahl an Standardfirewallrichtlinien zur Verfügung. Wählen Sie hier die Richtlinie, welche Ihren Anforderungen am gerechtesten wird.



Der Netzwerkvorlagen-Wizard hat seine Arbeit beendet. Überprüfen Sie die Einstellungen und klicken dann auf den Button **Fertig stellen**.



Im Anschluß an die Arbeit des Netzwerkvorlagen-Wizard, müssen Sie die neuen Einstellungen **übernehmen**.

Übernehmen Verwerfen Klicken Sie auf "Übernehmen", um Änderungen zu speichern und die Konfigu...

**Netzwerke**

### 3-Abschnitt-Umkreisnetzwerk

**Aufgaben** **Vorla...**

Stellt eine Verbindung internen Netzwerk ur und schützt das Netz Eindringversuchen.

Stellt eine Verbindung internen Netzwerk ur schützt das Netzwerk Eindringversuchen ur Dienste im Internet s Umkreisnetzwerk.

ISA Server wird als p einer kaskadierten Umkreisnetzwerkkonf Verwenden Sie diese Firewalls zwischen de internen Netzwerk ur verwendet werden.

ISA Server wird als s

**Netzwerke** **Netzwerksätze** **Netzwerkregeln** **Webverkettung**

R...	Name	Relation	Quellnetzwerke	Zielnetzwerke
1	Lokaler Hostzugriff	Route	Lokaler Host	Alle Netzwerke
2	VPN-Clients zum internen Netz...	Route	Quarantänen-VPN-Clients VPN-Clients	Intern
3	Umkreisconfiguration	NAT	Intern Quarantänen-VPN-Clients VPN-Clients	Umkreis
4	Umkreiszugriff	Route	Umkreis	Extern
5	Internetzugriff	NAT	Intern Quarantänen-VPN-Clients VPN-Clients	Extern

Der Netzwerkvorlagen-Wizard hat zahlreiche Einstellungen vorgenommen. Es wurde ein neues Netzwerk mit dem Namen **Umkreis** erstellt, welches wir für diesen Artikel in **WLAN** umbenennen werden.

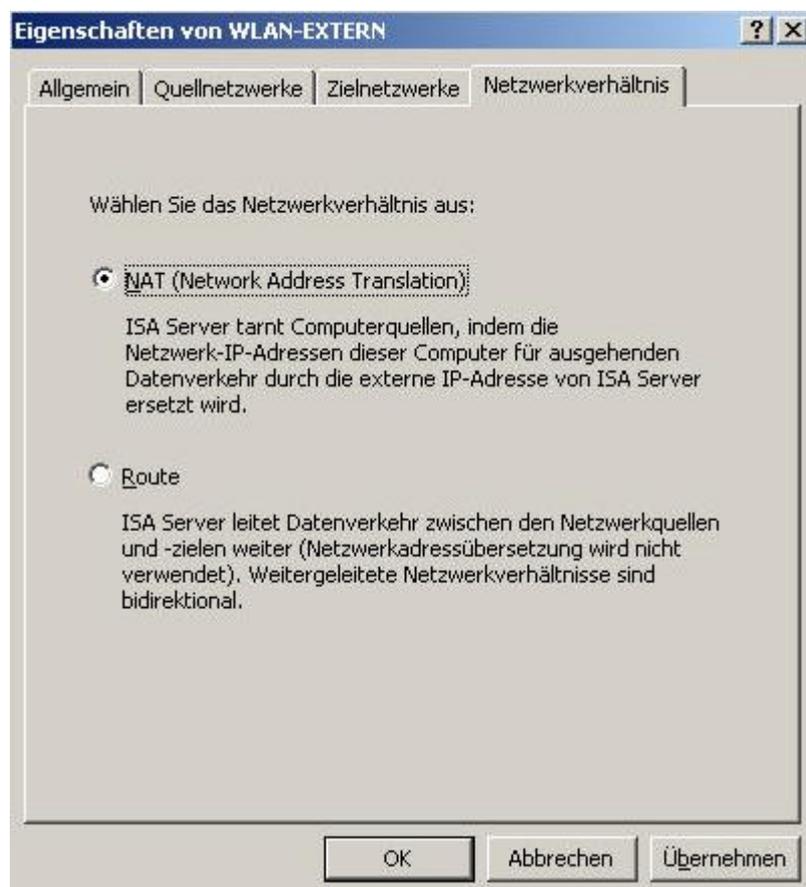
**Netzwerke** **Netzwerksätze** **Netzwerkregeln** **Webverkettung**

Name	Adressbereiche
Extern	Für die ISA Server-Netzwerke externe IP-Adressen
Intern	192.168.3.0 - 192.168.3.255
Lokaler Host	Mit diesem Netzwerk sind keine IP-Adressen assoziiert.
Quarantänen-VPN-Clients	Diesem Netzwerk sind zurzeit keine IP-Adressen zugeordnet.
<b>Umkreis</b>	<b>172.16.0.0 - 172.16.255.255</b>
VPN-Clients	Diesem Netzwerk sind zurzeit keine IP-Adressen zugeordnet.

Wie bereits oben erwähnt, wird das **Umkreis** Netzwerk in **WLAN** umbenannt.

Name	Adressbereiche
Extern	Für die ISA Server-Netzwerke externe IP-Adressen
Intern	192.168.3.0 - 192.168.3.255
Lokaler Host	Mit diesem Netzwerk sind keine IP-Adressen assoziiert.
Quarantänen-VPN-Clients	Diesem Netzwerk sind zurzeit keine IP-Adressen zugeordnet.
VPN-Clients	Diesem Netzwerk sind zurzeit keine IP-Adressen zugeordnet.
WLAN	172.16.0.0 - 172.16.255.255

Für diesen Artikel ändern wir das **Netzwerkverhältnis** für die Netzwerkregel **UMKREISZUGRIFF** auf **NAT**, da wir im Netzwerk **WLAN** nur Access Points und Wireless LAN Clients mit privaten IP-Adressen verwenden. In einem klassischen DMZ-Szenario verwenden die Server in der DMZ öffentliche IP-Adressen, so dass die Auswahl **Route** für das Netzwerkverhältnis angemessen wäre. Zusätzlich wird die Netzwerkregel von **UMKREISZUGRIFF** in **WLAN-EXTERN** umbenannt, damit aus dem Netzwerkregelnamen gleich hervorgeht, welche Konfiguration gemeint ist.



Jetzt wird noch die Netzwerkregel **Umkreisconfiguration** in **WLAN-INTERN** umbenannt und das Netzwerkverhältnis auf **Route** gesetzt, da für diesen Zugriff keine IP-Adressen maskiert werden müssen.

Netzwerke Netzwerksätze <b>Netzwerkregeln</b> Webverkettung				
R...	Name	Relation	Quellnetzwerke	Zielnetzwerke
1	Lokaler Hostzugriff	Route	Lokaler Host	Alle Netzwerke
2	VPN-Clients zum internen Netz...	Route	Quarantänen-VPN-Clients VPN-Clients	Intern
3	Umkreisconfiguration	NAT	Intern Quarantänen-VPN-Clients VPN-Clients	Umkreis
4	Umkreiszugriff	Route	Umkreis	Extern
5	Internetzugriff	NAT	Intern Quarantänen-VPN-Clients VPN-Clients	Extern

Das Ergebnis:

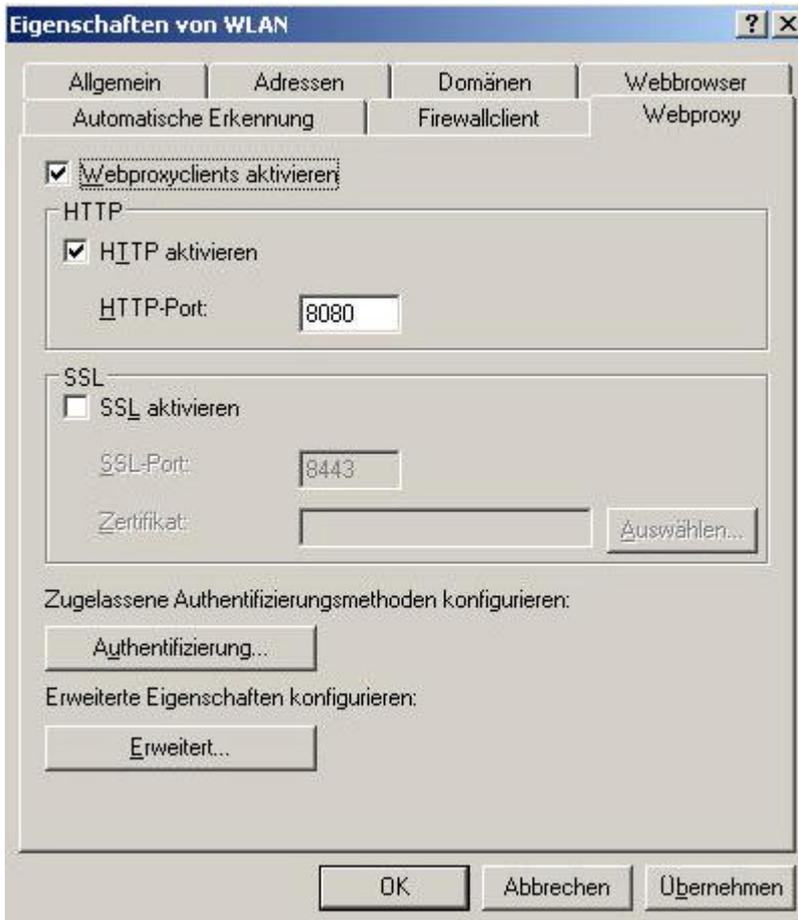
Netzwerke Netzwerksätze <b>Netzwerkregeln</b> Webverkettung				
R...	Name	Relation	Quellnetzwerke	Zielnetzwerke
1	Lokaler Hostzugriff	Route	Lokaler Host	Alle Netzwerke (u
2	VPN-Clients zum internen Netz...	Route	Quarantänen-VPN-Clients VPN-Clients	Intern
3	WLAN-INTERN	Route	WLAN	Intern
4	WLAN-EXTERN	NAT	WLAN	Extern
5	Internetzugriff	NAT	Intern Quarantänen-VPN-Clients VPN-Clients	Extern

### Wichtiger Hinweis:

Netzwerkregeln vom Typ **Route** sind immer bidirektional, müssen also nur einmal eingerichtet werden.

### Webproxy- und Firewall-Client Unterstützung

Sollen Clients aus dem Netzwerk **WLAN** auch **Webproxy** Zugriff erhalten, muss in den Eigenschaften des Netzwerkobjektes **WLAN** im Reiter **Webproxy**, die Unterstützung für **Webproxyclients** **aktiviert** werden. Das selbe gilt auch für die Aktivierung des **Firewallclient**.



Im letzten Schritt müssen Sie nur noch die vom Netzwerkvorlagen-Wizard erstellten [Firewallrichtlinien](#) auf Ihre Bedürfnisse anpassen.

Reihenfolge	Name	Aktion	Protokolle	Von / Listener	Nach
1	Nur Webzugriff	Zulassen	FTP HTTP HTTPS	Intern VPN-Clients	Extern WLAN
2	VPN-Clients zum internen Net...	Zulassen	Gesamter ausgehender Dat...	VPN-Clients	Intern
3	DNS in das Umkreisnetzwerk z...	Zulassen	DNS	Intern VPN-Clients	WLAN
Letzte	Standardregel	Verweigern	Gesamter Datenverkehr	Alle Netzwerk...	Alle Netzwerke

Für diesen Artikel wurden folgende Firewallrichtlinien erstellt:

Firewallrichtlinie					
Reihenfolge	Name	Aktion	Protokolle	Von / Listener	Nach
1	DNS fuer WLAN	Zulassen	DNS	WLAN	Extern
2	PRINT von WLAN nach INTERN	Zulassen	JetDirect	WLAN	Intern
3	INTERN nach WLAN	Zulassen	Gesamter ausgehender Dat...	Intern	WLAN
4	WWW fuer INTERN	Zulassen	HTTP HTTPS	Intern	Extern
5	WWW fuer WLAN	Zulassen	HTTP HTTPS	WLAN	Extern
Letzte	Standardregel	Verweigern	Gesamter Datenverkehr	Alle Netzwerk...	Alle Netzwerk...

Sie haben die Konfiguration eines **3-Abschnitt-Umkreisnetzwerk** erfolgreich abgeschlossen. Dieser Artikel hat Ihnen die notwendigen Kenntnisse zur Arbeit mit dem Netzwerkvorlagen-Wizard vermittelt, aber auch eine Anpassung der vom Wizard erstellten Objekte gezeigt.

Stand: Sonntag, 09. Januar 2005/MG. <http://www.it-training-grote.de>