

Windows Server 2003: Routing und Firewall

› Neben der Internet-Verbindungsfreigabe über ICS bietet Windows Server 2003 eine weiter gehende und flexiblere Lösung zur Absicherung des Internet-Zugangs - den "Routing and Remote Access Server".

› VON THOMAS WOELFER

Um ein ganzes LAN ans Internet anzuschließen, bietet Windows Server 2003 verschiedene Möglichkeiten: Am einfachsten ist das mit dem Internet Connection Sharing (ICS). Die deutlich flexiblere Variante, die auch über bessere Schutzmöglichkeiten verfügt, ist die Routing-Funktionalität. Diese ist vor allem bei Festverbindungen dem ICS vorzuziehen.

Der "Routing and Remote Access Server" ist eine Komponente von Windows Server 2003 und enthält, wie der Name schon vermuten lässt, einen Software-Router, einen Remote-Access-Server und eine Dial-on-Demand-Komponente. Außerdem unterstützt RRAS auch NAT und verfügt über eine Firewall mit Paketfilter. Damit stellt der RRAS ein perfektes Internet-Gateway für LANs bereit.

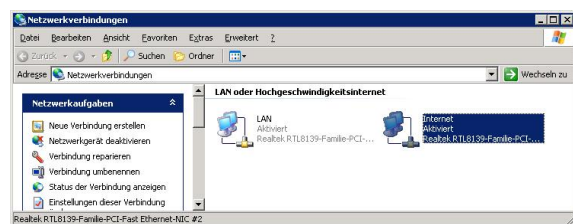
Eine sinnvolle Konfiguration ist dabei ein System mit zwei Netzwerkkarten: Eine verbindet den Server mit dem LAN, die andere mit dem öffentlichen Netz. Dabei hat nur Letztere eine öffentliche IP-Adresse. Diese bekommen Sie vom Carrier oder vom Internet Service Provider.

Eine Konfiguration mit einer privaten und einer öffentlichen Netzwerkkarte können Sie natürlich auch für viele andere Dinge verwenden. So wäre zum Beispiel ein öffentlicher Internet-Server mit dem IIS 6 denkbar. Der Server wäre dann über das öffentliche Interface sichtbar und würde über das private Interface konfiguriert und gewartet. Die Konfiguration ist - abgesehen von der Firewall - in einem solchen Fall mehr oder minder identisch mit der Konfiguration als Internet-Gateway.

› Voraussetzung: Zwei Netzwerkkarten im System

Zunächst brauchen Sie also zwei Netzwerkkarten im Server. Das ist weiter kein Problem, denn Windows Server 2003 kann beliebig viele NICs verkraften. Die Konfiguration der Netzwerkkarten erfolgt wie gewohnt, der Übersicht halber nennen Sie die eine Verbindung "Internet" und die andere "LAN" oder "DMZ" - je nachdem, wie die Verbindung zum internen Interface erfolgt.

Die Verbindung "Internet" bekommt außerdem die öffentliche IP-Adresse, die Sie vom ISP erhalten haben, beziehungsweise die zur vom Webserver betreuten Domain gehörige IP-Adresse. Das private Interface bekommt eine private, nicht-routbare Adresse, wie beispielsweise 192.168.169.1/255.255.255.0.



Doppelverbindung: Zwei Netzwerkkarten müssen es sein, sonst macht RRAS keinen Sinn.

Danach können Sie den RRAS über die Server-Verwaltung installieren. Die Komponente

trägt dort den Namen "RAS/VPN Server". Darin sind Routing, Firewall und NAT enthalten.

Die Verwaltung erfolgt über die "RRAS-Software Management-Konsole". Diese stellt im linken Bereich einen Baum dar, der Informationen über die Netzwerkschnittstellen und über das IP-Routing anzeigt. Um das Routing zu aktivieren, klicken Sie mit der rechten Maustaste auf den Namen des Servers und wählen den Befehl "Routing und Ras aktivieren und konfigurieren". Das startet den Setup-Assistenten für RRAS.

Im Assistenten geben Sie an, welche Art der Konfiguration Sie wünschen. Für ein Internet-Gateway oder einen Webserver mit der oben beschriebenen Konfiguration wählen Sie die Option "Netzwerkadressübersetzung (NAT)". Danach müssen Sie angeben, welche Ihrer Netzwerkkarten das öffentliche und welche das private Interface darstellen soll.

Nach dem Abschluss des Assistenten finden Sie in der Baumdarstellung von RRAS unter dem Ast *NAT/Basisfirewall* drei Einträge: Die "interne" Schnittstelle, die nicht weiter von Belang ist, sowie die Schnittstellen "LAN" und "Internet".

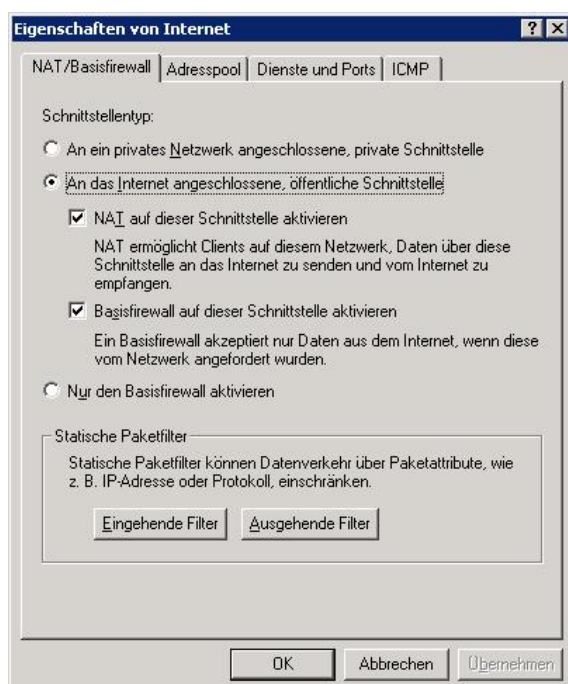
Die Interfaces sind ebenfalls einfach zu konfigurieren - das ist hauptsächlich für das spätere Vorgehen praktisch, denn der Assistent hat alle notwendigen Einstellungen bereits vorgenommen.

› **Basisfirewall: Auf jeden Fall aktivieren**

In den Eigenschaften der Schnittstelle "Internet" unter dem Reiter *NAT/Basisfirewall* aktivieren Sie die folgenden Optionen:

- › "An das Internet angeschlossene, öffentliche Schnittstelle"
- › "NAT auf dieser Schnittstelle aktivieren"
- › "Basisfirewall auf dieser Schnittstelle aktivieren".

"NAT auf dieser Schnittstelle aktivieren" benötigen Sie, damit Sie von allen Rechnern im LAN auf das Internet zugreifen können, da diese normalerweise private - also nicht öffentliche - IP-Adressen haben. Mit einer solchen privaten Adresse kann man aber im Internet nichts anfangen, denn kein Router unterwegs weiß, wohin er die Antwortpakete schicken soll. Auf der anderen Seite verfügt man meist nur über eine einzelne öffentliche IP-Adresse.



Grundsatz: Die Basis-Firewall schützt das System vor dem "bösen" Internet.

Anfragen ans Internet müssen über den NAT-Rechner gesendet werden, damit die Adressumsetzung funktioniert. Das stellen Sie dadurch sicher, dass Sie den NAT-Rechner auf den Workstations im LAN als Default-Gateway eintragen. Wenn Sie einen DHCP-Server verwenden (siehe diesen [tecCHANNEL-Beitrag](http://www.tecchannel.de/betriebssysteme/1222/index.html) (<http://www.tecchannel.de/betriebssysteme/1222/index.html>)), dann können Sie diese Einstellung automatisch im LAN verbreiten lassen.

› NAT-Funktionsweise

Alle Anfragen vom LAN ins Internet laufen über das private Interface des NAT-Servers, denn das befindet sich ja ebenfalls im Subnetz des LAN. Der Rechner merkt sich die (lokale) IP-Adresse sowie den Quellport des anfragenden Rechners und schickt die Anfrage weiter ins Internet.

Dazu verwendet er aber nicht die ursprüngliche Adresse, sondern die öffentliche Adresse des öffentlichen Interface: Die Anfrage wird also von der einen Schnittstelle auf die andere Schnittstelle geroutet. Dabei wird die IP-Adresse von der lokalen in eine öffentliche übersetzt und ein neuer Quellport vergeben.

Kommt die Antwort auf die Anfrage zurück, landet diese Antwort logischerweise wieder auf dem öffentlichen Interface. Der NAT-Rechner sucht anhand der Antwort die ursprüngliche Anfrage aus seinen Tabellen heraus und setzt das Paket entsprechend wieder so auf die lokale IP-Adresse um, dass der Client das Paket als Antwort auf seine ursprüngliche Anfrage interpretieren kann. Somit funktioniert dieser Mechanismus auch, wenn mehrere Rechner gleichzeitig auf denselben Server im Internet zugreifen.

Dieser Mechanismus führt also dazu, dass die Workstations im LAN einen gemeinsamen Internet-Zugang verwenden können, obwohl insgesamt nur eine öffentliche IP-Adresse zur Verfügung steht.

› Grundschutz der Basisfirewall

Die Basisfirewall dient dem Schutz des Rechners: Später werden Sie diese Firewall noch etwas ausführlicher konfigurieren, für den ersten Test ist es jedoch ausreichend, sie zunächst zu aktivieren. Auf dem öffentlichen Interface führt das dazu, dass der Rechner nur noch Pakete annimmt, die als Reaktion auf eine aus dem LAN stammende Anfrage eingehen.

Mit anderen Worten: Verbindungsversuche zu irgendwelchen Diensten auf dem Rechner werden nicht akzeptiert. Das schafft keinen absoluten Schutz, hilft aber gegen gängige Plagegeister wie zum Beispiel SQL-Slammer oder den aktuellen LOVESAN (Win32.Blaster).

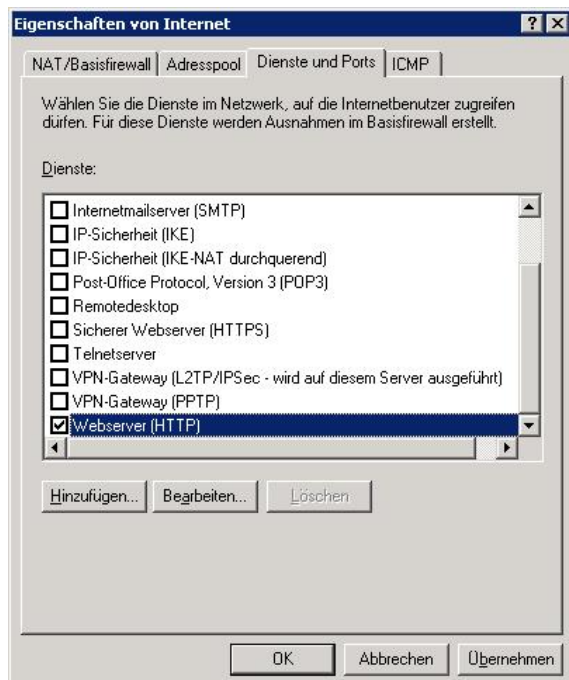
Zusätzlich zu dieser Grundfunktionalität können Sie noch spezielle Filter definieren. Dazu später mehr, denn jetzt soll zunächst einmal das Grundsystem laufen. Wenn Sie nicht nur über eine, sondern über einen Pool von öffentlichen IP-Adressen verfügen, können Sie auch diesen nutzen. Dazu dient der Reiter "Adresspool". Besondere Vorteile bringt das jedoch nur, wenn bestimmte Workstations aus dem LAN nach außen hin immer einer bestimmten öffentlichen Adresse auftreten sollen. Für die typischen Belange eines LANs ist das aber eher nicht von Bedeutung.

› Spezielle Dienste freischalten

Über den Reiter "Dienste und Ports" können Sie die Konfiguration der Basisfirewall beeinflussen. Normalerweise akzeptiert die Firewall keine Verbindungsversuche von außen. Für einen Internet-Gateway-Rechner ist das auch genau das erwünschte Verhalten. Läuft allerdings beispielsweise ein Webserver, müssen Verbindungsanfragen akzeptiert und beantwortet werden.

Genau das erreichen Sie auf diesem Reiter, indem Sie einzelne Dienste freischalten. Aktivieren Sie zum Beispiel die Option "Webserver (http)", dann werden Anfragen von außen akzeptiert, die an den Port 80 des Rechners gesendet werden - Sie können also Webseiten ausliefern lassen. Die vorgeschlagene Liste enthält nur die wichtigsten Standarddienste. Wenn auf dem Server eigene Dienste laufen, die auch im Netz

angeboten werden sollen, ist es möglich, die Liste per "Hinzufügen" selbst zu erweitern. Dabei ist ein Name für den Dienst und das Protokoll sowie der Eingangsport anzugeben. Außerdem können Sie die private Adresse auf der lokalen Maschine und optional einen ausgehenden Port angeben. Letzteren brauchen Sie, wenn der Dienst seine Antworten auf einem anderen Port versendet.



Löcher in der Mauer: Will man spezielle Dienste freischalten, geht das mit diesem Reiter.

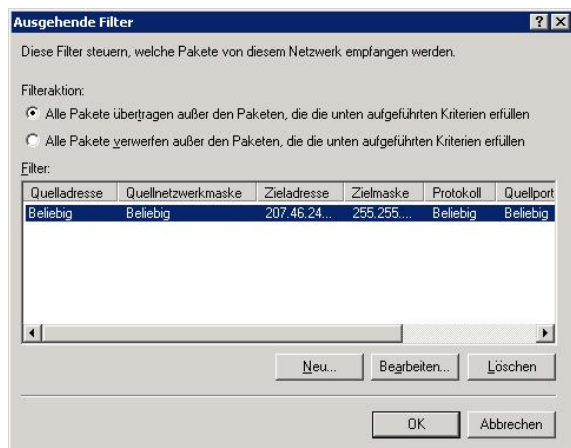
Schließlich gibt es noch den Reiter "ICMP", über den Sie einzelne ICMP-Methoden einschalten: Dies ist hauptsächlich für die Fehlersuche von Interesse. Läuft alles wie geplant, sollten Sie die ICMP-Nachrichten komplett ausschalten. Damit ist der Rechner zum Beispiel für Pings nicht mehr sichtbar. Da die meisten Angreifer zunächst per Ping die Anwesenheit eines Rechners und die verfügbare Bandbreite ermitteln, nehmen Sie diesen Personen auf diese Art und Weise ein wichtiges Hilfsmittel beim Ausloten von Lücken in Ihrem System. Script-Kiddies werden Sie dadurch fast zu 100 Prozent los.

Die Schnittstelle "LAN" muss nicht sonderlich konfiguriert werden. Hier aktivieren Sie einfach die Option "An ein privates Netzwerk angeschlossene, private Schnittstelle". Der RRAS übernimmt dann alle restlichen Aufgaben selbstständig und kümmert sich darum, dass NAT aus dem LAN ins Internet reibungslos funktioniert.

› Statische Paketfilter

Mit den statischen Paketfiltern des Reiters "NAT/Basisfirewall" können Sie die Basisfirewall um spezielle Regeln erweitern. Bei den Filtern handelt es sich um eine einfachere Variante der Paketfilter, die Sie mit IPSec von Windows 2003 einrichten können (Näheres dazu finden Sie in diesem [tecCHANNEL-Beitrag](http://www.tecchannel.de/betriebssysteme/1231/index.html) (<http://www.tecchannel.de/betriebssysteme/1231/index.html>)).

Im Normalfall funktioniert die Basisfirewall so, dass ausgehende Pakete jeder Art zugelassen werden, eingehende Pakete jedoch nur, wenn es sich um Antworten auf eine von innen gestellte Anfrage handelt.



Eingeschränkt: Die statischen Filter sind praktisch, aber wenig flexibel.

Nun will man aber manchmal auch Anfragen von innen blockieren, beispielsweise um bestimmte Webseiten oder Dienste nicht zugänglich zu machen. Andererseits möchte man eventuell auch Anfragen von bestimmten IP-Adressen auf eigene Server-Dienste grundsätzlich ignorieren, etwa um Traffic durch bestimmte Search-Engines abzustellen oder bekannten SPAM-IPs den Zugang zum Mailserver zu verweigern. Das ist mit den statischen Filtern der Basisfirewall ganz einfach.

› Spyware filtern

Angenommen Sie ärgern sich über Traffic, der zu www.gator.com geleitet wird, einem Hersteller von so genannter Spyware. Diesen können Sie abstellen - und damit www.gator.com effektiv blockieren - indem Sie zunächst die IP-Adresse(n) von Gator ermitteln. www.gator.com hat beispielsweise 64.152.73.182.

Wenn Sie diese IP-Adresse haben, klicken Sie auf den Button "Ausgehende Filter". Diese Filter werden auf Datenverkehr angewendet, der aus dem LAN ins Internet gerichtet ist.

Klicken Sie auf "Neu", um einen neuen Filter anzulegen. Jetzt können Sie ein Quell- und ein Zielnetzwerk angeben, um bestimmte Pakete eindeutig zu identifizieren. Wenn Sie sämtlichen Traffic aus dem LAN zu Gator unterdrücken wollen, brauchen Sie kein Quellnetzwerk anzugeben. Wollen Sie hingegen nur Teilen des LAN Verbindungen zu Gator verbieten, spezifizieren Sie diesen Teil des LANs als Quellnetz.

Als Zielnetzwerk geben Sie unter der IP-Adresse die von Gator an. Da es sich um eine einzelne Netzwerkadresse handelt, geben Sie als Subnetz die 255.255.255.255 ein und schließen den Dialog. Daraufhin landen Sie wieder im ursprünglichen Dialog, der nun die spezifizierte Adresse auflistet. Wählen Sie oben die Option "Alle Pakete übertragen außer den Paketen...", und www.gator.com ist aus Ihrem LAN heraus effektiv nicht mehr erreichbar.

Die statischen Paketfilter der Basisfirewall sind jedoch nicht sonderlich flexibel. Sie können entweder jeglichen Datenverkehr erlauben und nur bestimmte Pakete ausschließen oder jeglichen Datenverkehr verhindern und nur ausgewählte Pakete zulassen. Eine Kombination daraus ist nicht möglich - dazu müssen Sie weiter gehende Tools verwenden. Auch die hat Windows Server 2003 zu [bieten](#) (<http://www.tecchannel.de/betriebssysteme/1231/index.html>) .

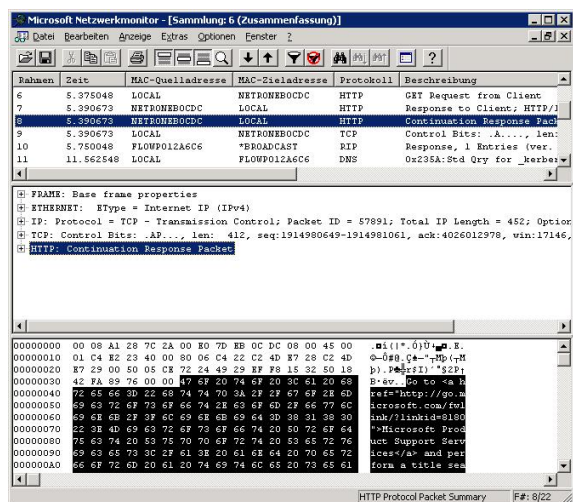
› Der Netzwerkmonitor

Im Zusammenhang mit der Basisfirewall und NAT ist eine weitere Windows-Komponente von Interesse: der Netzwerkmonitor. Mit dem Monitor lässt sich Netzwerk-Traffic auf allen im lokalen Rechner befindlichen Schnittstellen protokollieren und später analysieren. Die Pakete werden einfach in Echtzeit eingesammelt und aufgelistet. Dabei gibt der Netzwerkmonitor die zugehörige Frame-Nummer, die Zeit, die MAC -Quell- und Zieladresse sowie das verwendete Protokoll an. Ferner gibt es eine kurze Beschreibung

zum Paket und weiter gehende Informationen wie zum Beispiel die zugehörigen IP-Adressen, die auch aufgelöst werden.

In der Paketliste kann man auf jedes einzelne Paket klicken und sich den Inhalt des Pakets anzeigen lassen. Der wird sowohl hexadezimal als auch als ASCII dargestellt: Damit kann man zum Beispiel den ungläubigen Kollegen deutlich machen, wie gefährlich es ist, unverschlüsselte Passwörter etwa für ein POP3-Konto zu verwenden. Zusätzlich zur Datenansicht gibt es auch noch eine Baumansicht des Pakets, über die Sie Einsicht in die Header der Pakete erhalten.

Von Haus aus protokolliert der Netzwerkmonitor den kompletten Datenverkehr. Man kann aber auch Filter für die Protokollierung festlegen, um die Menge der eingesammelten Daten zu reduzieren und sich zum Beispiel nur bestimmte interessante Pakete anzusehen. Will man etwa überprüfen, ob Einbruchsversuche stattfinden, so würde man primär die Pakete zum Port 135 untersuchen.



Überblick: Mit dem Netzwerkmonitor sammeln Sie Pakete von ausgewählten Schnittstellen ein.

Damit Sie den Netzwerkmonitor verwenden können, muss der Netzwerkmonitor-Treiber installiert sein. Dabei handelt es sich um eine optionale Netzwerkkomponente der Eigenschaften von Netzwerkkarten. Der Treiber muss für alle Interfaces installiert werden, die Sie mit dem Netzwerkmonitor betrachten wollen, kann aber ganz nach Bedarf ein- und ausgeschaltet werden. Wenn Sie keine Daten mitführen möchten, dann sollten Sie den Treiber auch ausschalten, um die Systemlast nicht unnötig hochzutreiben.

› ICS versus RRAS

Eine Frage bleibt offen: Warum sollte man NAT und die Basisfirewall verwenden, statt einfach die Internet-Verbindungsfreigabe anzuwerfen? ICS ist immerhin deutlich einfacher zu konfigurieren, schließlich braucht man bloß bei den Eigenschaften der Netzwerkkarte eine einzige Option einzuschalten, um mit dem kompletten LAN und ohne eine zusätzliche Server-Software ins Internet zu kommen.

Das ist richtig: ICS ist extrem einfach anzuwenden. Allerdings ist es genauso unflexibel wie einfach. Verwendet man nämlich ICS, dann will es auch die IP-Adressen für die Rechner im LAN vergeben. Man kann also nicht länger den DHCP -Server von Windows Server 2003 benutzen, sondern ist auf das DHCP vom ICS angewiesen. Das ist jedoch nicht konfigurierbar.

Ebenso ist es mit ICS nicht möglich, Adress-Pools zu verwenden. Summa summarum ist ICS wohl die bessere Möglichkeit, ins Internet zu gelangen, wenn man nur über eine Dial-up-Verbindung verfügt. RRAS stellt dagegen die bessere und flexiblere Lösung dar, wenn man eine Festverbindung besitzt.

› Fazit

Mit RRAS haben Sie nicht nur einen Remote-Access- und VPN-Server, sondern auch einen vollwertigen Software-Router zu Ihrer Verfügung, den Sie als gemeinsamen Internet-Zugang mit NAT verwenden können. Die eingebaute Basisfirewall schützt dabei das öffentliche - und bei Bedarf auch das private - Interface und ermöglicht es außerdem, legalen, aber unerwünschten Traffic aus Ihrem LAN und in Ihr LAN zu unterbinden. Wer eine praktische Software-Lösung für den gemeinsamen Internet-Zugang oder eine einfache Methode für die Wartung eines öffentlichen Webservers sucht, der ist mit RRAS von Windows Server 2003 gut bedient. (mha)

› Weitere Themen zu diesem Artikel:

DHCP mit Windows Server 2003 (<http://www.tecchannel.de/betriebssysteme/1222/index.html>)

IPSec in Windows 2003 (<http://www.tecchannel.de/betriebssysteme/1231/index.html>)

So funktionieren TCP/IP und IPv6 (<http://www.tecchannel.de/internet/209/index.html>)

Copyright © 2001
IDG Interactive GmbH
Alle Rechte vorbehalten. Jegliche Vervielfältigung oder Weiterverbreitung in jedem Medium in Teilen oder als Ganzes bedarf der schriftlichen Zustimmung der IDG Interactive GmbH. DPA-Texte und Bilder sind urheberrechtlich geschützt und dürfen weder reproduziert noch wiederverwendet oder für gewerbliche Zwecke verwendet werden. Für den Fall, dass in tecChannel unzutreffende Informationen veröffentlicht oder in Programmen oder Datenbanken Fehler enthalten sein sollten, kommt eine Haftung nur bei grober Fahrlässigkeit des Verlages oder seiner Mitarbeiter in Betracht. Die Redaktion übernimmt keine Haftung für unverlangt eingesandte Manuskripte, Fotos und Illustrationen. Für Inhalte externer Seiten, auf die von tecChannel aus gelinkt wird, übernimmt die IDG Interactive GmbH keine Verantwortung.