Marc Grote, Christian Gröbner, Dieter Rauscher

Microsoft ISA Server 2004 – Das Handbuch

Probeseiten

Die beiden vorangegangenen Kapitel haben Ihnen einen detaillierten Einblick in die unterschiedlichen Arten von Serververöffentlichungen gegeben. Neben der Veröffentlichung eines Anwendungsservers haben Sie erfahren, welche umfangreichen Möglichkeiten ISA Server 2004 bei der Veröffentlichung eines Webservers bietet. Das nun folgende Kapitel beschreibt an einem sehr konkreten Beispiel das Zusammenspiel sämtlicher Serververöffentlichungsregeln. Fabrikam Inc. betreibt am Standort München einen Microsoft Exchange Server 2003 (MSX-MUC), der die gesamte Groupware-Funktionalität für das Unternehmen zur Verfügung stellt. Daher müssen Sie sicherstellen, dass der Server MSX-MUC E-Mails empfangen und versenden kann und dass alle internen Clients an beiden Standorten auf ihn zugreifen können. Zusätzlich wollen und müssen Ihre Kollegen mit ihren Firmennotebooks von unterschiedlichen Orten ihr Outlook synchronisieren können. Damit auch Mitarbeiter ohne Firmennotebook von extern ihre E-Mails bearbeiten können, müssen Sie einen Weg finden, diese Zugriffe sicher zu ermöglichen. Dieses Kapitel hilft Ihnen, alle gestellten Forderungen zu erfüllen.

SMTP-Serververöffentlichung

Als Erstes sollten Sie dafür sorgen, dass Fabrikam Inc. E-Mails von externen Geschäftspartnern und Kunden erhalten kann. Dazu sind einige Vorbereitungen notwendig, die zunächst nichts mit ISA Server 2004 zu tun haben. Dennoch sollen Sie hier kurz angesprochen werden. Es gibt zwei unterschiedliche Möglichkeiten, wie ein Mailserver E-Mails empfangen kann. Entweder er bekommt seine E-Mails zugestellt oder er muss sie sich abholen. Vergleichen Sie das einfach mit der Zustellung von Briefpost durch die Deutsche Post AG. Stellen Sie einen Briefkasten auf und teilen dem Postboten mit, wo er ihn findet, somit kann das Postunternehmen fortan alle an Sie adressierte Post direkt in Ihren Briefkasten zustellen. Sie müssen dafür sorgen, dass er erreichbar bleibt und dass immer genügend Platz ist. Übertragen auf den E-Mail-Verkehr entspricht das der E-Mail-Zustellung per SMTP. Dies ist die übliche und empfohlene Vorgehensweise für ein Unternehmen. Sie setzt jedoch voraus, dass der Briefkasten (entspricht dem Mailserver) stets am selben Ort (selbe IP-Adresse) erreichbar ist. Da Sie dafür eine feste statische IP-Adresse benötigen, kommen in der Regel Billiganbieter von DSL-Anschlüssen nicht in Frage, da Sie dort meist alle 24 Stunden eine neue IP-Adresse zugewiesen bekommen. Sollte für Sie dennoch nur eine solche Anbindung möglich sein, können Sie E-Mails auch bei einem Provider abholen. Stellen Sie sich vor, Sie haben bei der Deutschen Post AG ein Postfach. Erhalten Sie Post, die an Ihren Firmennamen adressiert ist, legt das Postunternehmen diese in Ihr Postfach. Dabei wäre es theoretisch egal, an welchem Ort tatsächlich Ihr Firmensitz ist. Denn Sie müssen nur sicherstellen, dass die Post von Ihnen abgeholt wird. Und zwar so regelmäßig, damit das Postfach nicht überläuft. Sonst kann keine neue Post zugestellt werden, sondern geht unzustellbar an den Absender zurück. Übertragen auf den E-Mail-Verkehr entspricht das dem Abholen von E-Mails beim Provider über das POP3-Verfahren (Post Office Protocol). Diese Methode ist aufwändiger und fehleranfälliger und sollte – im Gegensatz zum echten Briefpostverkehr – möglichst nicht verwendet werden. Ein E-Mail-Server wie Microsoft Exchange oder IBM Lotus Notes ist prinzipiell dafür ausgelegt, E-Mails zugestellt zu bekommen. Für das Abholen von E-Mails per POP3 wird meist Zusatzsoftware von Drittherstellern benötigt.

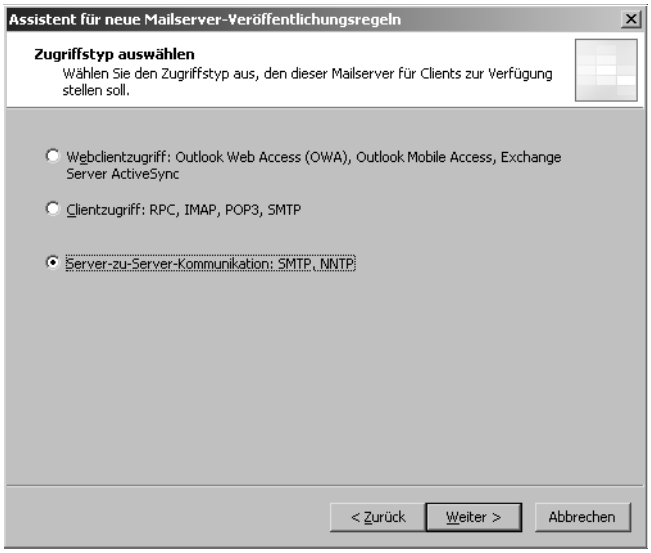
Fabrikam Inc. verfügt über eine Internetanbindung mit festen IP-Adressen und somit ist die E-Mail-Zustellung per SMTP der richtige Weg. Damit der Postbote die Adresse zu Ihrem Briefkasten findet, muss er in einem Straßenverzeichnis nachsehen. Damit ein anderer Mailserver Ihren Mailserver findet, sucht er einen MX-Eintrag in der DNS-Zone für *fabrikam.com*. Beauftragen Sie gegebenenfalls Ihren Internetanbieter, für Sie die entsprechenden Einträge vorzunehmen. Fabrikam Inc. hat einen MX-Eintrag mit der Präferenz 10 auf die IP-Adresse 207.46.130.106 gesetzt. Somit sind alle Voraus-

setzungen erfüllt und Sie können damit beginnen, den Exchange Server mit Hilfe von ISA Server 2004 zu veröffentlichen.

HINWEIS Verfügt Ihr ISA Server 2004 (oder ISA Server 2000) über mehrere externe öffentliche IP-Adressen und möchten Sie einen E-Mail-Server veröffentlichen, sollten Sie dies mit der ersten am Windows Server eingetragenen IP-Adresse tun. ISA Server 2004 verwendet für den Verbindungsaufbau bei externen Verbindungen stets die Standard-IP-Adresse. Veröffentlichen Sie den E-Mail-Server auf der zweiten IP-Adresse, stimmen Sende- und Empfangs-IP-Adresse nicht überein. Somit können Sie Probleme mit E-Mail-Servern bekommen, die ein DNS Reverse Lookup auf den MX-Eintrag machen.

Gehen Sie in den Aufgabenbereich der Firewallrichtlinien und wählen Sie den Punkt *Mailserver veröffentlichen* aus. Sie werden vom *Assistent für neue Mailserver-Veröffentlichungsregeln* begrüßt, dem Sie als ersten den Namen der Regel angeben müssen. Geben Sie **MSX-MUC SMTP-Veröffentlichung** ein und klicken Sie auf die Schaltfläche *Weiter*. Das nächste Dialogfenster (siehe Bild 15.1) fordert Sie auf, den Zugriffstyp auszuwählen.

Bild 15.1 Wählen Sie als Zugriffstyp *Server-zu-Server-Kommunikation: SMTP, NNTP* aus



Die Option *Webclientzugriff* wird dann benötigt, wenn Clients über einen Internetbrowser zugreifen sollen. Dieses Thema wird später in diesem Kapitel beschrieben. Die zweite Option *Clientzugriff* erstellt Zugriffsregeln für Clients, die mit einem Mailclient wie zum Beispiel Outlook oder Outlook Express durch ISA Server 2004 hindurch auf einen E-Mail-Server zugreifen sollen. Da diese Regel für die Serverkommunikation erstellt wird, wählen Sie die letzte Option *Server-zu-Server-Kommunikation: SMTP, NNTP* aus und klicken Sie auf die Schaltfläche *Weiter*. Im nächsten Dialogfenster müssen Sie den zu verwendenden Dienst beziehungsweise das zugehörige Protokoll auswählen. Angeboten werden:

- **SMTP** Diese Option ist für die Standard-E-Mail-Kommunikation notwendig und basiert auf TCP-Port 25 eingehend.

- **Sicheres SMTP** Diese Option nutzt das SMTP-S Protokoll mit TCP-Port 465 eingehend. Dazu müssen aber alle beteiligten Server dieses verschlüsselte Protokoll verwenden. Die Option ist nicht geeignet, um einen E-Mail-Server für alle erreichbar zu machen.
- **NNTP** Der letzte Dienst ist nur für die Kommunikation von Newsservern über TCP-Port 119 eingehend verwendbar. Per NNTP können keine E-Mails zugestellt werden.

Wählen Sie nur die SMTP-Option aus (Bild 15.2).

Bild 15.2 Auswählen des SMTP-Dienstes

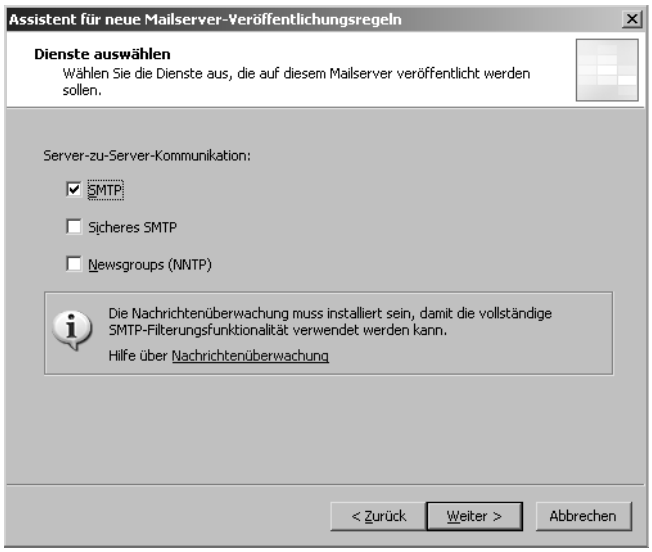
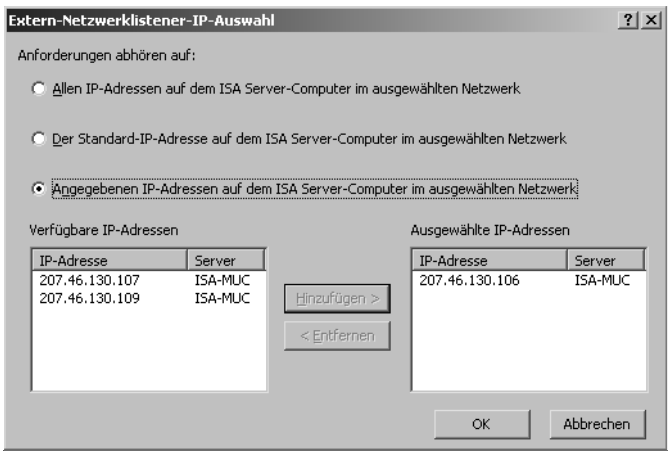


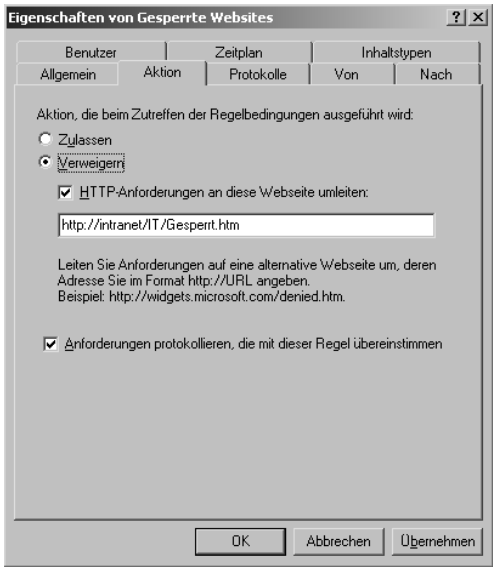
Bild 15.3 Die Serververöffentlichungsregel soll nur an eine bestimmte IP-Adresse gebunden sein



Beachten Sie auch den Hinweis zur Nachrichtenüberwachung. Mit installierter Nachrichtenüberwachung kann der in Kapitel 8 beschriebene SMTP-Filter auch Schlüsselworte und Absender sperren. Diese Möglichkeiten sind im Vergleich zu speziellen E-Mail-Inhaltsfilterlösungen sehr einge-

Als nächstes müssen Sie eine Regel erstellen, die keine Verbindung zu den verbotenen Websites erlaubt. Erstellen Sie dazu eine neue Zugriffsregel und geben Sie ihr den Namen **Gesperrte Websites**. Als Regelaktion geben Sie *Verweigern* an. Fügen Sie im nächsten Dialogfeld *Protokolle* das HTTP-Protokoll hinzu. Klicken Sie auf die Schaltfläche *Weiter* und Sie kommen zum Dialogfeld *Zugriffsregelquellen*. Fügen Sie dort wieder, wie in Bild 16.1 gezeigt, den Computersatz *Interne Workstations* hinzu. Sie können auch das gesamte interne Netzwerk hinzufügen. Ebenso kann der standardmäßig hinzugefügte Benutzersatz *Alle Benutzer* auf der Registerkarte *Benutzer* übernommen werden. Beenden Sie den Assistenten und öffnen Sie anschließend die Eigenschaften der soeben erstellten Firewallrichtlinie. Aktivieren Sie das Kontrollkästchen bei *HTTP-Anfragen an diese Webseite umleiten* auf der Registerkarte *Aktion*. Geben Sie im Eingabefeld eine interne Webseite an, die den Hinweis für die Benutzer über die verbotenen Seiten enthält (siehe Bild 16.2).

Bild 16.2 Umleitungsziel, wenn eine gesperrte Website aufgerufen wird



Sie können zusätzlich zu einzelnen Seiten noch weitere Einschränkungen beim HTTP-Verkehr über den HTTP-Filter vornehmen, was im Laufe dieses Kapitels noch beschrieben wird. Beachten Sie, dass die Verweigerungsregel oberhalb der Zulassungsregel in den Firewallrichtlinien steht (siehe Bild 16.3). Nur dann wird sie angewendet.

Bild 16.3 Reihenfolge der Verweigerungs- und Zulassungsregel für HTTP

Damit die dritte Anforderung (ausgehende VPN-Verbindungen für DHCP-Rechner) erfüllt werden kann, erstellen Sie eine Zugriffsregel. Details dazu lernen Sie in den nächsten beiden Kapiteln.