

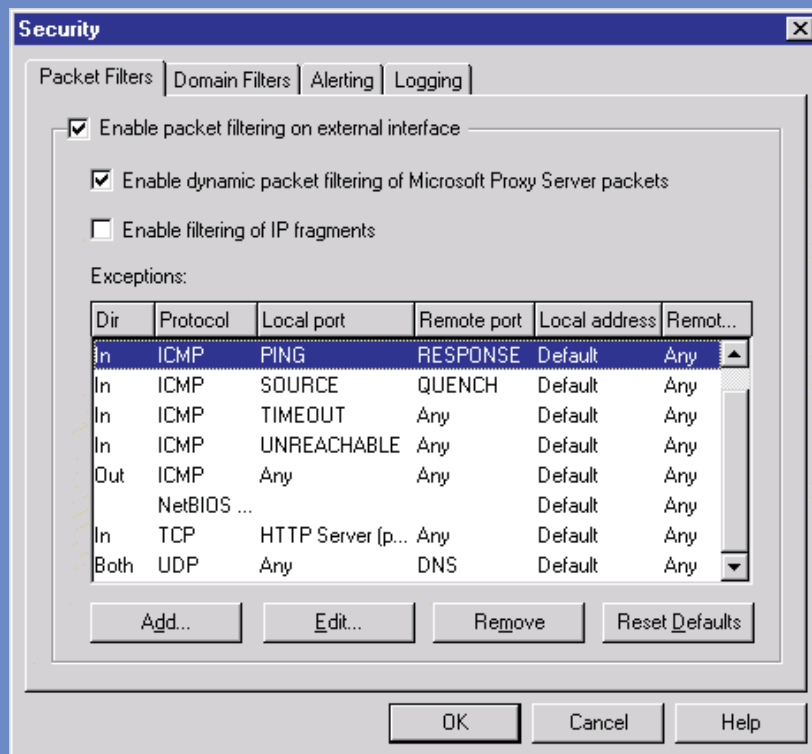
Für immer mehr Unternehmen wird das Internet zu einem wichtigen Werkzeug für das Tagesgeschäft. Jedoch zieht der Anschluß des Firmennetzes an das Internet auch gewisse Sicherheitsrisiken nach sich, gegen die es sich zu schützen gilt. Firewall-Systeme und Proxy-Server haben sich zum Schutz firmeninterner Daten vor Angreifern aus dem Internet gut bewährt. Auch Microsoft hat vor etwas mehr als einem Jahr sein erstes Produkt dieser Kategorie mit dem Namen Proxy-Server vorgelegt und im Herbst 97 die überarbeitete Version 2.0 freigegeben.

VON DIRK PELZER

Paket-Filter

Im Gegensatz zur Version 1.0 verfügt der Proxy-Server 2.0 über einen Paket-Filter-Mechanismus, mit dem der Administrator bestimmte Netzwerk-Pakete auf der IP-Ebene ausfiltern kann, bevor sie höhere Schichten, wie beispielsweise Sockets erreichen können. Wenn man den Paket-Filter des Proxy-Servers einschaltet, werden zunächst einmal alle Pakete, außer denen, die in einer vordefinierten Liste stehen, ausgefiltert. Diese Liste läßt sich beliebig den Erfordernissen des Unternehmens anpassen, so wirklich nur solche Datenpakete zwischen dem internen Netz und dem Internet verkehren

können, die für das Tagesgeschäft relevant sind. Der Proxy-Server verfügt auch über einen dynamischen Paket-Filter, bei dem abhängig von einer bestimmten Protokollsequenz Filter aus- und wieder eingeschaltet werden. So wäre es zum Beispiel für einen FTP-Client möglich, über den Proxy-Server eine Internet-Verbindung zu einem Server anzufordern. Der Proxy-Server wählt dann einen Port aus, über den der ein- und ausgehende Verkehr abgewickelt wird, setzt einen Filter, der eine Kommunikation über den gewählten Port erlaubt und stellt die Verbindung zum gewünschten Internet-Server her. Nach dem Abschluß der Sitzung deaktiviert der Proxy-Server den Filter und unterbindet jede weitere Kommunikation über den zuvor gewählten Port.



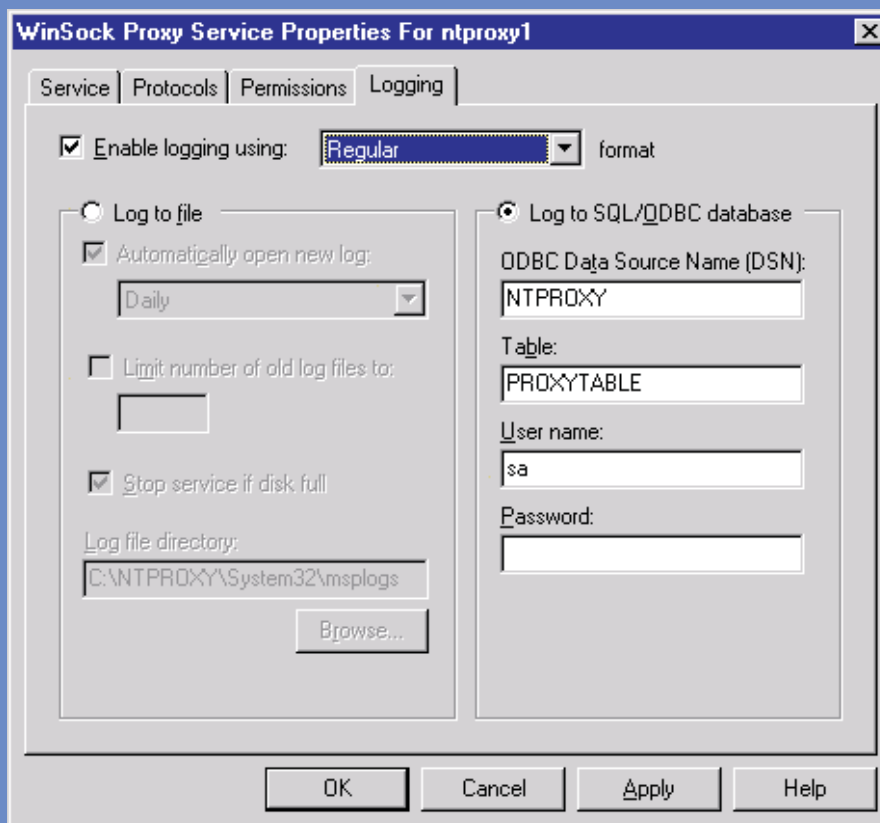
Über die Paket-Filter-Option läßt sich steuern, welche Datenpaket-Typen der Proxy-Server akzeptiert und welche er abweist

Alarmer und Logging

Zusätzlich zu der Möglichkeit, Pakete zu filtern, verfügt der Proxy-Server auch über die Fähigkeit, ein Logging von Ereignissen auf Paket-Ebene durchzuführen. Diese können entweder in eine Textdatei oder über ODBC in eine Datenbank geschrieben werden. Die Informationen, die in der Log-Datei geschrieben werden beinhalten Quell- und Ziel-IP-Adresse, Quell- und Ziel-Port, sowie einen Zeitstempel. Darüber hinaus besteht die Möglichkeit, einen Verbose-Modus zu aktivieren, bei dem erheblich mehr Informationen in die Log-Datei aufgenommen

werden. Die im Verbose-Modus enthaltenen Informationen beinhalten den IP-Header und einen Teil des Datenfeldes im hexadezimalen Format.

Neben der Fähigkeit der Protokollierung, erlaubt der Proxy-Server aber auch eine Alarmierung über Email, falls bestimmte Ereignisse benutzerdefinierte Schwellwerte überschreiten. So kann man sich beispielsweise benachrichtigen lassen, wenn der Proxy-Server mehr als 20 Pakete pro Sekunde abweist. Auf diese Weise kann man sich als Administrator vor möglichen Denial-of-Service-Angriffen warnen lassen und Gegenmaßnahmen einleiten.



Der Proxy-Server gestattet die Protokollierung wichtiger Ereignisse in einer Textdatei, oder aber über ODBC in einer Datenbank

Web- und FTP-Cache

Um den Anwendern Zeit und der Firm Kosten zu sparen, gestattet der Proxy-Server das Caching von HTTP 1.0, 1.1 und FTP-Objekten. Sind in einem Unternehmen mehrere Proxy-Server im Einsatz, so kann man Arrays bilden und den Cache auf alle

Server verteilen und damit einen einzigen großen virtuellen Cache erzeugen. Die Proxy-Server Arrays haben zusätzlich noch den Vorteil, daß sie sich als eine einzige logische Einheit darstellen und administrieren lassen und sie erlauben darüber hinaus noch eine automatische Lastverteilung Internet zugreifen. Über einen Mechanismus, den Microsoft

»Active Intelligent Caching« nennt, ermittelt der Proxy-Server, welche Web-Seiten am häufigsten besucht werden und wie oft sich deren Inhalte ändern. Mit Hilfe dieser Informationen lädt der Proxy-Server proaktiv die neuesten Inhalte in seinen Cache.

Reverse Proxy und Virtual Hosting

Der Proxy-Server gestattet nicht nur Anwendern des Firmennetzes einen sicheren Zugang zum Internet, sondern er erlaubt auch umgekehrt Internet-Benutzern den sicheren Zugriff auf Web-Server, die sich im Unternehmensnetz befinden. Über den »Reverse Proxy«-Mechanismus, kann man den Proxy-Server so konfigurieren, daß er auf URL-Anfragen, die vom Internet hereinkommen wartet und diese Anfragen dann an einen Web-Server im Firmennetz weiterleitet. Der Vorteil dieser Methode ist, daß externe Anwender niemals die richtige IP-Adresse des eigentlichen Web-Servers zu sehen bekommen und dieser somit vor direkten Angriffen auf IP-Ebene besser geschützt ist. Leider kann jeder Proxy-Server auf diese Weise nur einen internen Web-Server schützen. Wenn man mehrere Web-Server hat und diese durch nur einen Proxy-Server schützen möchte, kann man auf den »Virtual Hosting«- Mechanismus zurückgreifen. Mit diesem kann man ausgehend von der Haupt-Proxy-Server-URL mehrere virtuelle Pfade einrichten, die dann wiederum auf die einzelnen Web-Server im internen Netz verweisen. Selbstverständlich werden auch Anfragen von externen Anwendern im Cache des Proxy-Servers abgelegt, um die Antwortzeiten zu verkürzen und Netzwerkverkehr zu reduzieren.

Kommandozeilen-Administration

Für den Proxy-Server 2.0 hat Microsoft nun auch Werkzeuge beigelegt, mit denen man eine Administration auf Kommandozeilenebene durchführen kann. Über das Tool REMOTMSP.EXE lassen sich die Dienste des Proxy-Servers verwalten, Konfigurationen sichern und wieder herstellen, sowie verschiedenen Konfigurations-Paremeter einstellen. Über WSPPROTO.EXE lassen sich Protokoll-Defini-

tionen für den Winsock-Proxy-Service hinzufügen, löschen und ändern.

Fazit

Der Proxy-Server 2.0 bietet sehr viele neue und interessante Features, die aus ihm ein wirklich brauchbares und auch für größere Netze einsetzbares Werkzeug machen. Microsoft hat sich bei der Entwicklung wirklich ins Zeug gelegt und ein Produkt abgeliefert, das, soweit es die komplexe Technologie erlaubt, vergleichsweise einfach zu installieren und zu administrieren ist. Wer auf der Suche nach einer Firewall-Lösung ist, sollte den Proxy-Server 2.0 auf jeden Fall in die Liste der zu evaluierenden Produkte aufnehmen.

Produktdaten / Features

Der Microsoft Proxy-Server 2.0 stellt folgende Funktionen zur Verfügung:

- Proxy-Funktion für FTP, HTTP, HTTP-S, Telnet, Gopher, IRC, RealAudio, VDOLive, POP3, SMTP und NNTP über TCP/IP und IPX/SPX
- Dynamische Paket-Filterung
- Prokollierungs- und Alarmierungsmechanismen zum Schutz gegen Angriffe
- Schutz firmeneigener Internet-Web-Server durch Reverse Proxy und Virtual Hosting
- Lastverteilung und virtueller Cache durch Bildung von Proxy-Server Arrays
- Administration über Kommandozeile möglich
- Erweiterbarkeit durch Internet Server Application Programming Interface (ISAPI)
- Blockieren unerwünschter Internet-Seiten möglich

Hersteller: Microsoft Corp., Redmond, USA

Internet: www.microsoft.com/proxy

Bezugsquelle: Fachhandel

Preis: 995 Dollar

Kurztest: Microsoft Proxy-Server 2.0

So wurde getestet / Equipment

Der Microsoft Proxy-Server 2.0 wurde auf einem englischen Windows-NT Server Version 4.0 mit Service Pack 3 installiert. Als Hardware-Plattform diente ein handelsüblicher Pentium-PC mit 120 MHz Taktfrequenz, 72 MB Hauptspeicher und einer 4,3 Gigabyte Ultra-SCSI Festplatte. Zusätzlich war noch eine 10 Mbit PCI-Ethernet Karte sowie ein analoges Modem mit 33600 Baud Übertragungsrate angeschlossen. Die Netzwerkkarte war mit einem Acht-Port Mini-Hub verbunden, an dem auch ein mit deutschem NT Workstation 4.0 und Service Pack 3 installierter Proxy-Client angeschlossen war. Dieser bestand aus einem 150 MHz Pentium-System mit 64 MB Hauptspeicher, einer 2,5 GB EIDE-Festplatte und einer 10 Mbit PCI-Ethernet Karte. Als Browser wurde der Microsoft Internet Explorer 3.02 verwendet.

Was ist ein Proxy-Server

Unter einem Proxy-Server versteht man einen Rechner, der als Zwischenstation zwischen einem Firmen-Netz und einem externen Netz, wie zum Beispiel dem Internet dient. Ein Proxy-Server gestattet nur bestimmten internen Computern, deren IP-Adresse dem Proxy-Server bekannt ist die Kommunikation mit dem externen Netz. Dabei schirmt der Proxy-Server die IP-Adressen der internen Rechner vor dem externen Netz ab, um potentiellen Angreifern keine Informationen über den firmen-internen Netzaufbau zu geben. Zusätzlich bieten Proxy-Server die Möglichkeit, die Kommunikation auf bestimmte Anwendungen und Protokolle, wie zum Beispiel FTP oder HTTP zu begrenzen und tragen so dazu bei, die Zahl potentieller Risikoquellen klein zu halten.

Zur Person

DIPL. ING. DIRK PELZER arbeitet als freier Consultant und Journalist in München. Er betreibt ein Storage Labor für verschiedene namhafte Fachzeitschriften. Zudem beschäftigt er sich mit Speichernetzen und Hochverfügbarkeit.