

Juli 2004

2 Ausgaben kostenlos lesen



Administrator

Das Magazin für professionelle System- und Netzwerkadministration

Reportage Proxyserver

Appliance löst MS-Proxy ab

**Sonderdruck für
Blue Coat Systems**

Ablösung eines Proxyserver

Vom Zwischenspeicher zum Torwächter

Als zentrales Tor zum Internet sorgen klassische Proxyserver hauptsächlich für die Zwischenspeicherung von Webseiten. Auf diese Weise sparen sie Bandbreite und beschleunigen den Zugriff auf oft gefragte Inhalte.

Zunehmend sollen die Proxies jedoch weitere Aufgaben wie die Durchsetzung von Sicherheitsregeln auf Benutzer- und auf Inhaltsebene übernehmen. Die Omnibusverkehr Rhein-Nahe GmbH, ein mittelständischer Regionaldienstleister im Personennahverkehr, migrierte ihren Internetcache von einem MS-Proxy-Server auf eine Proxy-SG-800-Appliance von Blue Coat Systems und bietet nun ihren rund 100 Anwendern einen sicheren und kontrollierten Internetzugang an – zu vergleichsweise günstigen Kosten.



Der Webzugriff bei der Omnibusverkehr Rhein-Nahe GmbH erfolgt zentral über einen Proxy SG 800 von Blue Coat Systems

Als Dienstleister im öffentlichen Personennahverkehr gehört die Omnibusverkehr Rhein-Nahe GmbH (ORN) auf den ersten Blick nicht unbedingt zur klassischen Zielgruppe für Proxyappliances. Und wie so oft im richtigen Leben spielte auch der Zufall bei diesem Projekt eine gewisse Rolle. Anfang 2003 überlegte das EDV-Team der ORN, den bestehenden Microsoft-2.0-Proxy auszutauschen. Zu diesem Zeitpunkt griffen rund

15 Nutzer über den MS-Proxy, der auf einem Windows-NT-Server 4.0 lief, auf das Internet zu. "Die alten Proxies boten zwar das übliche Caching, aber sonst nicht viel", erklärt Jochen Platz, IT-Administrator und Teamleiter Datenverarbeitung bei der ORN. Mit dieser mangelnden Flexibilität vor allem in Sachen Benutzerauthentifizierung und Administration wollte sich das Tochterunternehmen der Deutsche Bahn Regio AG nicht länger

zufrieden geben. Für Administrator Platz bot das bestehende System keine Perspektive für seine Probleme in der alltäglichen Arbeitspraxis: "Es war beispielsweise nicht möglich, individuelle Policies pro User zu definieren oder einzelne URLs je nach Nutzergruppe (Quell-IP-Adressranges, einzelne Dienste) freizugeben", so Platz. Zudem wünschte sich der IT-Verantwortliche eine einfach zu bedienende Verwaltungsoberfläche am liebsten browserbasiert.

Zufällig bot zu diesem Zeitpunkt der langjährige IT-Dienstleister Sopra eine Kundeninformationsveranstaltung an, die sich für ORN als richtungweisend herausstellte. Auf dem Event des IT-Dienstleisters lernte das EDV-Team von ORN die Secure-Proxy-Appliances des amerikanischen Herstellers Blue Coat Systems kennen. Bei der Veranstaltung selbst ging es dabei nicht nur um die Proxyappliances von Blue Coat. Denn der Hersteller bindet auch zusätzliche Sicherheitsfunktionen seiner Technologiepartner wie Symantec, Trend Micro oder Surfcontrol in seine Proxies ein. Dies geschieht entweder über eine direkte Integration in der Appliances (on box) oder über ICAP (Internet Content Adaptation Protocol) als separates Gerät. "Wir wollten sowieso einen Antivirens Scanner für die Web-

dienste in unser Netzwerk einbinden.“, erinnert sich Jochen Platz und forderte ein Testgerät an. Zusätzlich informierte sich der IT-Administrator über alternative Angebote und zog den Microsoft-ISA-Server in Erwägung.

Kostenvorteil

Eine Woche nach der Veranstaltung von Sopra hielt ORN das Testgerät von Blue Coat in Händen. Für den Test schloss Platz die Proxy SG 800 zunächst nur an einige Rechner des EDV-Teams an. Das Gerät arbeitete sozusagen im Parallelbetrieb mit den bestehenden Proxy-Systemen. Nach und nach zog der Administrator weitere Nutzer hinzu. So testeten nach zwei Wochen insgesamt 10 Nutzer stellvertretend für die insgesamt 100 Anwender innerhalb des Unternehmens die Proxyappliance.

Ein Vergleich der Kosten für Hard- und Software für den ISA-Server von Microsoft und den Kosten für die Proxyappliance von Blue Coat sowie ein Abwägen der Folgekosten in Form von regelmäßigen Updates für die Server-basierende Konkurrenz machten die Entscheidung relativ leicht: Die Kosten für die Proxy-SG-800-Appliance von Blue Coat zusammen mit Consulting und einem 3-Jahresvertrag für die Anbindung eines Virenschanners von Symantec beliefen sich auf rund 8.000 Euro. Im Vergleich dazu hätte ORN nach eigener Rechnung für die ISA-Lösung mit ISA- und Windows-2000-Serverlizenz, 100 Clientlizenzen und Serverhardware anfänglich bereits rund 11.000 Euro bezahlen müssen. Hinzu wären dann noch Folgekosten für regelmäßige Updates und Wartung des Betriebssystems sowie Lizenzkosten für eine Antivirenlösung gekommen. So fiel die Entscheidung zugunsten der Lösung von Blue Coat.

Integration ins Netz

Nach zwei Manntagen lief das Gerät im operativen Betrieb des heterogenen Windows-2000/NT-Netzes der ORN. Der Appliance vorgeschaltet sind ein Paketfilter und eine Firewall. Das interne Netz-

werk erstreckt sich neben der Firmenzentrale in Mainz über sechs Außenstellen und zwei Kundencenter und vier Niederlassungen. Die Netzwerkanbindung innerhalb von Mainz erfolgt über Richtfunk mit 11 MBit/s, die Außenstellen greifen über ADSL auf das Firmennetz zu. Die externen Netzwerkverbindungen sind VPN-getunnelt und mit je einer 128 KBit/s-Wählverbindung abgesichert. Alle Außenstellen greifen dabei ausschließlich über die Zentrale und somit über die Proxyappliance auf das Internet zu. Über ICAP mit der Proxy SG 800 verbunden ist ein Virenschanner von Symantec, der unter anderem alle Webmails, die über Port 80 in das Netzwerk gelangen, kontrolliert. Die Konfiguration aller Policies für die Kontrolle des Webverkehrs erfolgt zentral in der Appliance.

Anfangs nutze ORN das Gerät von Blue Coat vorwiegend als klassischen zentralen Proxy für den Internetzugang der rund 100 Anwender und zur Authentifizierung der verschiedenen Nutzergruppen. Während der Einführungsphase informierte das Unternehmen die Mitarbeiter darüber, dass der Internetzugang protokolliert wird. Dieses Logging ermöglichte es dem EDV-Team festzustellen, welche Inhalte tatsächlich abgefragt wurden und die Sicherheitsregelwerke

Projekt:

Ablösung eines Proxy-Servers

Kunde:

Omnibusverkehr Rhein-Nahe GmbH

Anwender:

ca. 100

Gewähltes Produkt:

Proxy SG 800 Appliance von Blue Coat Systems

Alternative Produkte:

Microsoft ISA Server

Kosten:

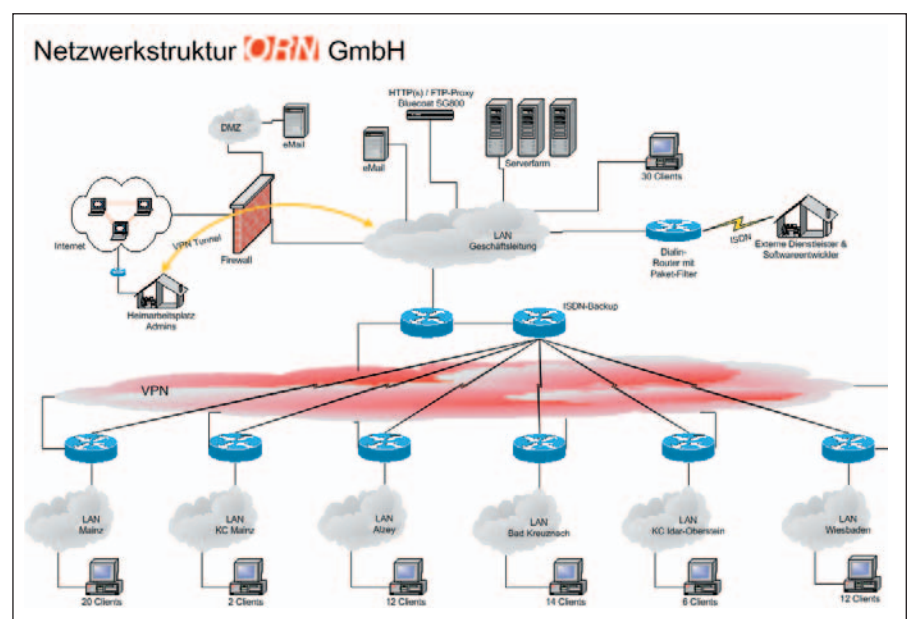
8.000 Euro für Proxy-Appliance, Consulting und 3-Jahresvertrag für Virenschanner

Dauer:

2 Manntage für Einführung

Anwendung in Kürze

nach und nach immer feinkörniger anzupassen. Die Software Blue-Coat-Reporter erzeugt dazu Berichte auf Basis von Seitenzugriffen, Datenvolumen und der Verteilung des Datenverkehrs über die Tageszeit und bringt so Auffälligkeiten oder missbräuchliche Nutzung ans Licht. Zudem geben die generierten Berichte Auskunft über die Stabilität und Performance des Netzwerks. Am wichtigsten waren für IT-Administrator Platz die granularen Konfigurationsmöglichkeiten für den Webzugriff nach Merkmalen wie



100 Anwender greifen bei der ORN, einem Tochterunternehmen der Deutsche Bahn Regio AG, auf das Internet zu

Webadresse, Quell-IP-Adressrange und NTLM/Active-Directory-Nutzergruppe. Je länger das Team sich mit der Appliance beschäftigte, desto mehr Möglichkeiten entdeckten die IT-Verantwortlichen, um die Regelwerke immer weiter zu verfeinern. Die Konfiguration sämtlicher Policies erfolgte dabei zentral über ein Webinterface auf der SG 800 selbst.



„Beim Einsatz eines Proxies mit flexiblem Regelwerk sollte sich der Administrator von Beginn an Gedanken über die Gruppenbildung der Nutzer und die firmenrelevanten Policies machen“ – Jochen Platz, IT-Administrator und Teamleiter Datenverarbeitung bei der ORN

Aufwändige manuelle Änderungen an den Clients waren bei der Umstellung auf die Appliance nicht notwendig. Bei Nutzung der Windows-2000-Server bindet die Proxyappliance das Active Directory über einen so genannten Blue Coat Authentication Authorization Agent ein. Die Unterstützung für die Authentifizierung erfolgt über die von Microsoft empfohlene Methode des Security Support Provider Interface (SSPI). Über die „Einstellungen“ im Internet Explorer wird hierbei die DFÜ-Verbindung entsprechend angepasst und über die Active-Directory-Policies der Windows-2000-Umgebung an alle 100 Clients verteilt. So genügt es, die Proxy-IP-Adresse und die Ports der einzelnen Dienste zu ändern.

Die der Appliance vorgeschaltete Firewall stellt darüber hinaus sicher, dass kein Client die Sicherheitsregelwerke umgeht. Denn die Firewall lässt nur Port 80 und den Port für FTP-Datenverkehr offen. Und Datenverkehr dieser Art muss zwangsweise auch durch die Proxyappliance. Fernzugriffe über Laptops oder die Heimarbeitsplätze der Administratoren werden bei Webzugriffen ebenfalls durch den Proxy geschleust, der Zugang erfolgt hier über ein VPN durch die Firewall auf das LAN von ORN. Manchmal bereiten bestimmte Softwareanwendungen Pro-

bleme, die einerseits auf Onlineupdates angewiesen sind, aber keinerlei Proxyauthentifizierung zulassen. Doch diese Herausforderungen waren schnell gelöst. So gibt es die Möglichkeit, über das Proxylog die benötigten Update-URLs herauszufinden und diese für die einzelnen Systeme, zum Beispiel anhand der Quell-IP-Adresse, freizugeben.


Ausbau

Schnell nahm ORN die URL-Filterfunktion in Betrieb. Zu Beginn regelte das EDV-Team die Zugriffsberechtigungen für den Webzugang wie üblich über die „erlaubt/verboten“-Merkmale für unterschiedliche Nutzergruppen. Doch diese Regelung empfand IT-Administrator Platz ziemlich schnell als überholt: „Inzwischen haben wir unsere Policies wesentlich verfeinert und führen detaillierte Black- und White Lists“, so Platz. Aufgrund dieser Feineinstellungsmöglichkeit hat ORN erst kürzlich zwei so genannte halb-öffentliche PCs in das Netz eingebunden. Die beiden Rechner stehen in den Aufenthaltsräumen der Busfahrer und ermöglichen es den Mitarbeitern, während ihrer Pausen auf Websites zu surfen, die für die Arbeit relevant sind. Hierzu zählen beispielsweise die Fahrplanauskunft der Bahn oder Seiten der Partnerunternehmen aus dem Nahverkehrsverbund. Der Zugriff auf Internetinhalte, die nicht arbeitsrelevant sind, ist hingegen gezielt gesperrt. „So eine Funktionsvielfalt hätte bei Lösungen anderer Hersteller gleich finanzielle Mehraufwendungen für Hardware, Software und Betriebssystem nach sich gezogen“, erklärt Jochen Platz, der solche Terminals in Kürze für das Fahrpersonal in jeder Außenstelle zur Verfügung stellen wird.

Mit der Proxyappliance kann der Administrator zudem verschiedene Nutzergruppen mit unterschiedlichen Rechten einrichten und diese individuell verwalten. So hat eine Gruppe beispielsweise vollen Webzugriff, darüber hinaus gelten nur die Authentifizierungseinstellungen des Active Directory. Eine weitere Gruppe hat nur eingeschränkten Zugang zum

Internet, der über so genannte Denylisten geregelt wird. Die Appliance überprüft dann bei der Anfrage einer URL, ob der Nutzer die entsprechenden Zugriffsrechte hat. Hat er sie nicht, sendet das Gerät eine Nachricht an den Nutzer. Den Inhalt jeder einzelnen Nachricht kann der IT-Administrator bei Bedarf selbst individuell an die Unternehmenspolicy und das Corporate Design anpassen. Dies ermöglichte es, die Fehlermeldungen in Formulierungen umzumünzen, die der Nutzer auch wirklich versteht und nachvollziehen kann. Alternativ sind bestimmte Nachrichten vordefiniert und es existieren kleinere Regelwerke, die für einzelne Systeme gewisse URLs für die Durchführung von Onlineupdates freigeben (Virens Scanner und mehr).

Fazit

Für ORN hat sich die Investition inzwischen mehr als gelohnt. Es fielen auch keine Kosten für eine Schulung des EDV-Teams an. „Während der Implementierung wurden bereits viele unserer Fragen beantwortet, außerdem ist die Appliance in sehr vielen Bereichen geradezu selbsterklärend“, so Platz zufrieden. Anderen IT-Kollegen rät Platz, sich von Beginn an Gedanken über die Gruppenbildung der Nutzer und firmenrelevante Policies zu machen. Denn die Geräte bieten sehr viel Freiraum für flexible Anpassungen und eine Konfiguration, die auf das Unternehmen individuell zugeschnitten ist. 

(Larissa von der Howen/gh)

Omnibusverkehr Rhein-Nahe GmbH

www.orn-online.de

Blue Coat Systems

www.bluecoat.de

Sopra

www.sopragroup.de

ICAP Forum

www.i-cap.org

Microsoft ISA Server

www.microsoft.com/germany/ms/isas

Links