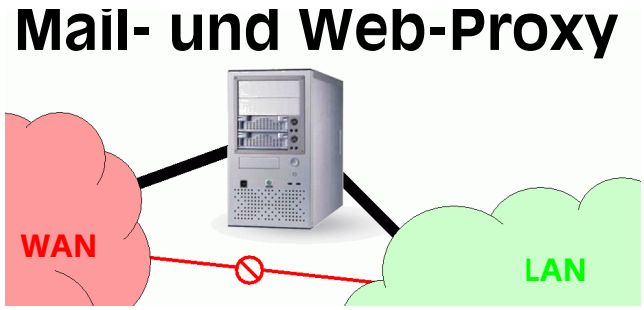
Zur Absicherung des unternehmensinternen EDV-Netzwerk gegen die vielfältigen Gefahren aus dem Internet reichen heute reine Firewallsysteme nicht mehr aus. Es ist vielmehr erforderlich, am Internet-Gateway den Datenverkehr auch inhaltlich einer eingehenderen Prüfung hinsichtlich Viren und Spam zu unterziehen.



Proxy

Ein Proxy-Server ermöglicht die Kontrolle des Datenverkehrs zwischen zwei Netzwerken auf Anwendungsebene, indem im Proxy die Datenpakete der übertragenen Nachricht oder Webseite zusammengesetzt und damit als Ganzes überprüft werden. Es können gegebenenfalls Maßnahmen eingeleitet werden, wenn unerlaubte Dateien heruntergeladen werden beziehungsweise sich in einer Datei z. B. ein Virus befindet.

Darüber hinaus können sogenannte Caching-Proxies die Netzwerklast durch Zwischenspeichern von Inhalten minimieren, indem nur bei der jeweils ersten Anfrage von Inhalten aus dem Internet diese Daten vom Orginalserver bezogen werden. Alle weiteren Anfragen nach demselben Inhalt werden aus dem Zwischenspeicher (Cache) bedient. Hierdurch lassen sich neben der Bandbreitennutzung am Internet-Zugang auch die Zugriffszeiten auf häufig genutzte Seiten reduzieren.

Die von enbiz installierten Proxies basieren auf folgenden Softwarepaketen, die als OpenSource-Software zur Verfügung stehen:

Linuxdistribution Debian:

Debian ist eine Distribution, die zu 100% freie Software einsetzt und sich durch seine Stabilität und schnelle Behebung von Fehlern auszeichnet. Ein Update funktioniert mit einfachen Befehlen und beachtet im Gegensatz zu RPM-basierten Distributionen (wie RedHat und Suse) die Abhängigkeiten zwischen Paketen. Fehlende Pakete werden automatisch nachinstalliert. Debian stellt weiterhin sicher, dass bei Installation und Update die Konfigurationsdateien erhalten bleiben und nicht ohne Nachfrage verändert bzw. überschrieben werden. Damit eignet sich Debian vor allem für angepasste Systeme, bei denen eine individuelle Konfiguration erstellt wurde, die auch bei Aktualisierungen des Systems erhalten bleiben muss.

HTTP-Proxy (Web-Proxy)

Webproxy Squid:

Squid ist der bekannteste OpenSource Webproxy, der unter der GPL-Lizenz verfügbar ist und der Inzwischen auch in vielen kommerziellen Produkten eingesetzt wird. Der Proxy eignet sich sowohl für den Einsatz in kleinen bis mittleren Netzen als auch als hochverfügbares Produkt in Cache-Verbünden. Durch die umfangreichen Konfigurationsmöglichkeiten ermöglicht Squid eine Anpassung an jede Netzwerk-Infrastruktur.

Virenproxy SquidClamAV:

Ergänzend zu Squid kann der Virenproxy SquidClamAV eingesetzt werden. Er bietet die Möglichkeit, mit dem ClamAV-Virenscanner den kompletten Web-Datenverkehr nach Viren zu durchsuchen.

enbiz • engineering and business solutions
Mozartstraße 25 • 67655 Kaiserslautern
http://www.enbiz.de/
info@enbiz.de

SMTP-Proxy (Email-Proxy)

MTA (Mail Transfer Agent) Postfix:

Postfix ist ein OpenSource MTA, der den Transport von E-Mails übernimmt. Durch den modularen Aufbau ermöglicht Postfix die leichte Erweiterung um Viren- und SPAM-Scanner oder auch z. B. das automatische Anhängen von gesetzlichen Angaben (nach EHUG) oder sonstigen Hinweisen und "Disclaimern". Postfix wurde vor allem unter den Gesichtspunkten Sicherheit, Zuverlässigkeit und Stabilität entwickelt und hat sich inzwischen weltweit durchgesetzt.
Postfix unterstützt in der aktuellen Version Graylisting. Dieses Verfahren basiert darauf, eine Mail im ersten Zustellversuch abzulehnen, die Senderadresse zwischenzuspeichern und erst den zweiten Zustellversuch anzunehmen. Durch dieses Vorgehen wird bereits ein großer Teil der SPAM-Mails gar nicht erst angenommen, da die SPAM-Mailer meist nach dem Prinzip "Fire and Forget" arbeiten und die SPAM-Mails nur einmal versandt werden. Das Prinzip von Graylisting ist mit den RFCs für E-Mail zu 100% konform, durch den Einsatz dieses Filters gehen keine EMail verloren, solange der sendende Mailserver die RFC-Standards einhält.

SPAM-Filter SpamAssassin:

SpamAssassin ist ein OpenSource SPAM-Filter, der alle Mails mit mehreren Tests auf SPAM überprüft. Es werden Text- und Header-Analysen, Blacklist-Abgleiche, lernende Filter (Bayes Filter), Vergleich von Mails (mittels Razor und Pyzor) usw. eingesetzt um SPAM zuverlässig zu erkennen und zu kennzeichnen. Mit dieser Kennzeichnung kann der nachgeschaltete Mailserver die SPAM-Mails aussortieren bzw. sie dem Empfänger in einen SPAM-Ordner einsortieren. Auf dem Mailproxy wird bei unseren Installationen zusätzlich ein IMAP-Server betrieben, der es allen Benutzern erlaubt, Mails als SPAM zu bezeichnen und somit durch gezieltes "Training" die Erkennungsrate von SpamAssassin nachhaltig zu steigern.
SpamAssassin wird auch von den meisten Anbietern kommerzieller Appliances (Hard-/Software-Komplettlösungen) eingesetzt.

Virenscanner ClamAV:

ClamAV ist ein komplett unter der GPL entwickelter Virenscanner. Verschiedene Firmen arbeiten inzwischen bei der Entwicklung mit und steuern aktuelle Virenpattern bei. Damit ist ClamAV, als einer von mehreren Virenscanner zur Virenabwehr, für den produktiven Einsatz geeignet. In der Regel setzen wir zusätzlich einen kommerziellen Virenfilter als zweite Stufe ein.

Absicherung und Überwachung

Durch den Einsatz von Linux kann der Server zusätzlich abgesichert und überwacht werden. Möglichkeiten bestehen, eine Software-Firewall mit ipchains bzw. iptables aufzubauen, welche die Zugriffe auf den Proxyserver zusätzlich schützt.
Mit verschiedenen Scripten oder Programmen (z. B. Nagios) kann der Server seine Funktionsweise überprüfen und Störungen automatisch an die Administratoren weitermelden.

Wir bieten Ihnen folgende Dienstleistungen rund um Ihren Proxy:

- Netzwerkanalyse, Beratung, Implementierung, Inbetriebnahme
- Installationsworkshops: "Learning by doing"
- Schulung und Coaching von Administratoren
- Schlüsselfertiger, individueller Aufbau inkl. Dokumentation, Wartung und Support

enbiz • engineering and business solutions
Mozartstraße 25 • 67655 Kaiserslautern
http://www.enbiz.de/
info@enbiz.de