

# **i**Administrator

Das Magazin für professionelle System- und Netzwerkadministration

**ImTest:**  
**Net at Work Mail Gateway 7.5.71**  
**Sichere Mails garantiert**

**Sonderdruck für**  
**Net at Work**



**Im Test: Net at Work Mail Gateway 7.5.71**

# Sichere Mails garantiert

von Jürgen Heyer



**B**ekannt geworden ist die Net at Work Netzwerksysteme GmbH aus Paderborn durch die Anti-Spam-Lösung NoSpamProxy. Noch relativ neu ist das Programm enQsig zur E-Mail-Verschlüsselung und zum Erstellen qualifizierter elektronischer Signaturen. Der Hersteller hat nun beide Produkte unter einem neuen Namen als Net at Work Mail Gateway vereint, so dass hierfür nur eine Installation notwendig ist. Nur die Lizenzierung bestimmt letztendlich, ob ein oder zwei Produkte aktiv sind. Nutzer beider Funktionen haben den Vorteil, dass so der Ressourcenbedarf geringer ist und die Konfiguration weniger Aufwand erfordert. Für diesen Test haben wir uns auf die Komponente enQsig konzentriert.

Die digitale Signatur bietet dem Empfänger die Sicherheit über die Authentizität des Absenders. Eine Verschlüsselung sorgt dafür, dass nur der Adressat eine Nachricht auch lesen kann. Zudem schreibt das Umsatzsteuergesetz eine Validierung durch eine qualifizierte elektronische Signatur beim elektronischen Rechnungsversand und auch bei der Übergabe an ein Archivsystem vor.

Qualifizierte elektronische Signaturen sind eine zentrale Voraussetzung für den kostensparenden, elektronischen Rechnungsversand. Eine zuverlässige Verschlüsselung ist ebenso wichtig, wenn der Versand vertraulicher Informationen auf der Tagesordnung steht. Mit enQsig bietet Net at Work ein Mail Gateway an, das diese Aufgaben zentral übernimmt und so die einzelnen Anwender entlastet. IT-Administrator hat sich den Ablauf bei der Absicherung des Nachrichtenversands genauer angesehen und verrät, wo die Stärken und Schwächen der Software liegen.

enQsig erledigt diese Aufgaben automatisch. Die Aktionen, die das Gateway auf eine E-Mail anwendet, gliedern sich also in die zwei Bereiche S/MIME-Unterstützung zur Verschlüsselung von E-Mails sowie das Ergänzen und Verarbeiten qualifizierter elektronischer Signaturen.

## Variable Möglichkeiten zur Einbindung ins Netzwerk

Das Mail Gateway arbeitet als SMTP-Proxy und kann auf verschiedene Arten mit dem Mailserver im Unternehmen kombiniert werden. Das Studium der verschiedenen, im Handbuch aufgeführten Szenarien zeigt schnell, dass sich eine bestehende Umgebung erfreulich leicht um das Gateway ergänzen lässt.

## Zuwachs in der DMZ

Bei der so genannten Einzelinstallation wird das Gateway auf einem eigenständigen Server installiert. Zusätzlich muss der Administrator das Routing im Netzwerk so konfigurieren, dass das Gateway die Mails auf Port 25 annehmen kann und erst anschließend an den eigentlichen Mailserver weiterleitet. Beim Versand muss der Mailserver die Mails wiederum zuerst an das Gateway senden, welches diese dann an die Adressaten, also die verschiedenen externen Mailserver, schickt. In einer grö-

ßeren Umgebung mit DMZ empfiehlt es sich, das Gateway in der DMZ aufzustellen. Soll noch ein Virens scanner auf dem Transportweg eingebunden werden, so ist dieser zwischen dem Gateway und dem internen Mailserver anzuordnen. Eine Positionierung zwischen Gateway und Internet ist wenig sinnvoll, da hier Mails eventuell verschlüsselt sind und sich somit gar nicht scannen lassen. Alternativ kann der Virens scanner auch auf dem gleichen Server wie das Gateway laufen.

## Anbindung über SMTP-Relay möglich

Verfügt ein Unternehmen über keine eigene, feste IP-Adresse, kommt meist ein Router mit NAT zum Einsatz. Die notwendige Namensauflösung wird dann am besten durch DDNS (dynamisches DNS) realisiert. Der Router muss nun so konfiguriert werden, dass Verbindungen auf Port 25 an die IP-Adresse des Gateways weitergeleitet werden. Während der Empfang in jedem Fall reibungslos funktionieren sollte, ist beim Versand eine Besonderheit zu beachten: Die meisten Mailserver weisen Mails von Servern mit einer dynamischen IP-Adresse zum Schutz vor Spammern ab. Um diese Tatsache zu umgehen, bietet es sich an, noch einen SMTP-Server beim eigenen Internet-Provider als

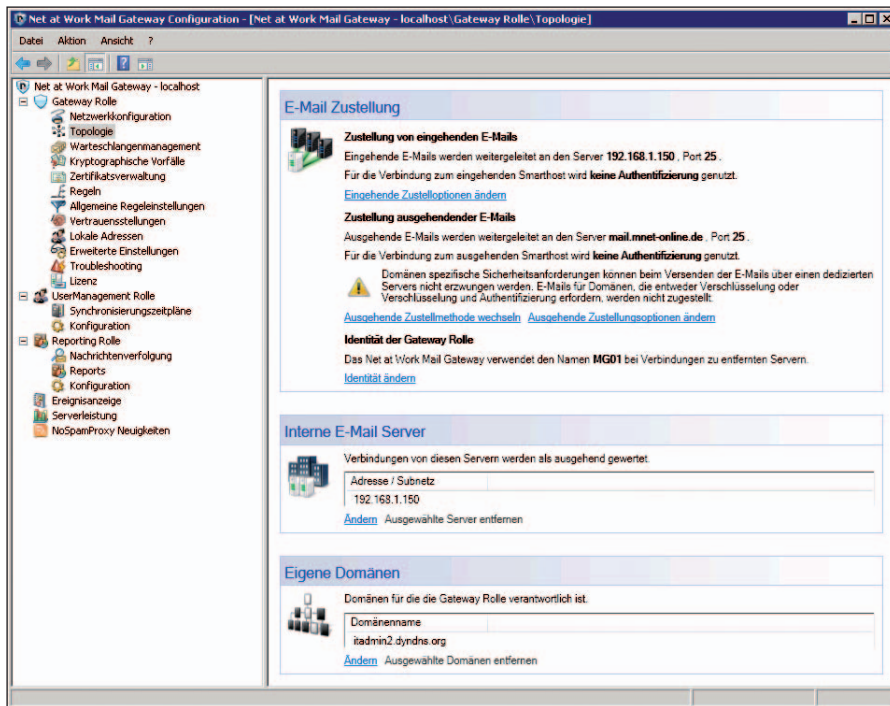


Bild 1: Die Einstellungen wie hier bei der E-Mailzustellung sind recht übersichtlich mit zusätzlichem, beschreibendem Text aufgelistet

SMTP-Relay zu nutzen, welcher dann letztendlich die Mail weitergibt. Das Net At Work Mail Gateway unterstützt diese Betriebsart mit optionaler Anmeldung am Relay ebenso wie den direkten Versand.

Für den kostensparenden Betrieb in kleineren Umgebungen ist es auch möglich, das Mail Gateway und den Mailserver auf dem gleichen System zu installieren. Hierbei muss der Mailserver nur so eingestellt werden, dass er nicht mehr auf Port 25, sondern auf einen anderen Port hört. Dann nimmt das Gateway die Mails selbst auf Port 25 an und gibt sie auf dem anderen Port über localhost weiter.

### Läuft als Cluster und in virtualisierten Umgebungen

Für große Umgebungen und eine höhere Verfügbarkeit lässt sich enQsig als Cluster betreiben, indem das Gateway parallel auf mehreren Servern installiert wird. Die eingehenden Mails sind dann über DNS-RoundRobin, einen SMTP-Load-Balancer der Firewall oder die Windows-Funktion NLBS zu verteilen.

Jedes Gateway arbeitet in diesem Fall eigenständig, die Konfiguration wird pro Server in einer XML-Datei gehalten. Die Betriebsdaten aber werden am besten auf einem zentralen SQL-Server zusammengeführt. Außerdem wird der Betrieb des Mail Gateways auf virtuellen Maschinen unter VMware und Hyper-V offiziell unterstützt. Nicht möglich ist übrigens eine direkte Mailabholung per POP3 oder IMAP, es wird SMTP als Transportprotokoll vorausgesetzt.

### Bedarfsgerechte Installation

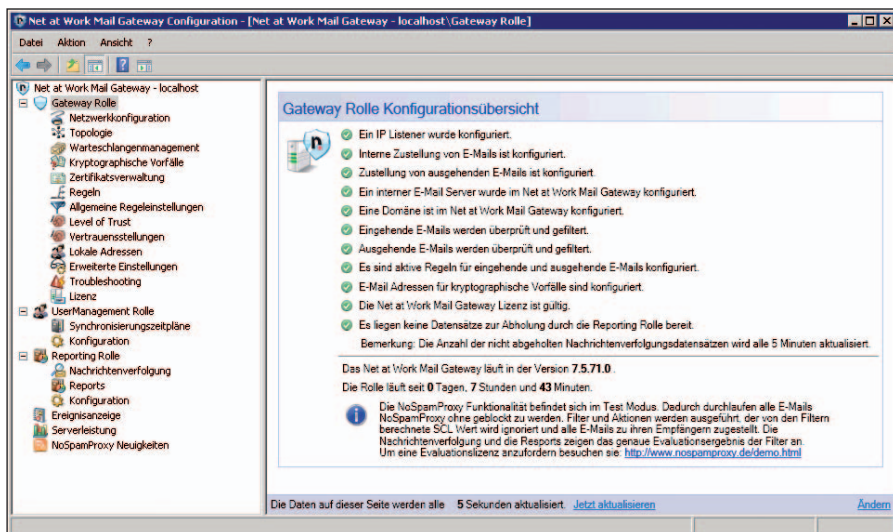
Im Test entschieden wir uns für die Installation des Gateways auf einem eigenständigen Windows 2008-Server, 64 Bit, als virtuelle Maschine. Auf einer weiteren virtuellen Maschine richteten wir einen Mailserver (Kerio Connect) ein. Außerdem konfigurierten wir einen NAT-Router mit DDNS-Unterstützung, so dass die Domäne im Internet aufgelöst wurde und Mails direkt angenommen werden konnten. Ausgehende Mails leiteten wir wie beschrieben über den SMTP-Server eines Internet-Providers als Relay. Das Gateway gliedert sich funktional in

drei Rollen (Gateway, Benutzermanagement und Reporting) sowie eine Management-Konsole, wobei alle Komponenten auf einem Server installiert, aber auch auf mehrere Systeme verteilt werden können. So sprechen Sicherheitsaspekte dafür, in einer größeren Umgebung auf einem oder mehreren Servern in der DMZ nur die Gateway Rolle zu installieren und das User Management sowie das Reporting auf einem Server im LAN. Für den Test installierten wir jedoch alle Komponenten des Gateways zusammen.

Das rund 3,5 MByte große Setup prüft die Installationsvoraussetzung und verlangte in unserem Fall zuerst die Einrichtung des Report Viewer Control 2008 SP1. Der passende Link war mit eingebettet, so dass der Download und die Installation schnell erledigt waren. Anschließend fragte das Setup die gewünschte Datenbank ab. Zur Auswahl stehen entweder ein externer SQL-Server oder SQL Server 2005 Express, zu dessen Setup-Dateien der Administrator den Pfad angeben kann. Alternativ wird die Express-Version bei Microsoft heruntergeladen. Zuletzt fragt das Setup noch ein Passwort für den SA-Benutzer ab, installiert dann alles und richtet auch die notwendige Datenbankinstanz ein. Für die Lizenzierung muss der Administrator abschließend die erhaltene Lizenzdatei in ein Verzeichnis laut Handbuch kopieren.

### Ordnung über Regeln und Rollen

Durch die Verwendung von Rollen für die verschiedenen Funktionsbereiche sowie Regeln für die Beschreibung des Umgangs mit den Mails ist die Konfiguration des Mail Gateways sehr übersichtlich strukturiert und weitgehend intuitiv zu bedienen. Im Rahmen der Erstinbetriebnahme sind diese Rollen und Regeln zu konfigurieren. Vorteilhaft ist, dass in der Dokumentation die notwendigen Schritte für einen Minimalbetrieb stichpunktartig aufgelistet sind. Im Test klappte die Einrichtung anhand dieser Übersicht auf Anhieb. Zuerst ist der Listener für den E-Mailempfang zu konfigurieren, wobei dieser auf alle oder auch



**Bild 2:** Die Konfigurationsübersicht der Gateway-Rolle bietet eine gute Zusammenfassung der bestehenden Einstellungen

nur eine bestimmte IP-Adresse hört. Der Listener unterstützt Tarpitting, um DoS-Attacken abzuwehren. Hierbei wartet der Listener bei ungültigen Anfragen zwischen zwei und zehn Sekunden, um so den Verkehr bewusst zu bremsen.

Der Umgang des Gateways mit ein- und ausgehenden Mails wird über Regeln definiert. Hilfreich ist hier, dass es die Möglichkeit gibt, über einen Link drei vorbereitete Standardregeln einrichten zu lassen. Diese lassen sich nachher bei Bedarf ergänzen oder modifizieren. Weiterhin kann der Administrator aus vier Optionen die gewünschte Transportsicherheit für die komplette SMTP-Verbindung auswählen (keine Anforderung, StartTLS erlauben oder erzwingen, Verwendung von SMTPS). Für eine Verschlüsselung sind entsprechende Zertifikate erforderlich.

### Schwarze Listen in der Domänenverwaltung

Anschließend ist die Zustellung ausgehender Mails an fremde Mail-Server sowie an den oder die internen Mailserver einzurichten. Wichtig ist es hier, alle eigenen Mailserver in eine Liste einzutragen, damit das Gateway weiß, dass Mails von diesen IP-Adressen als ausgehend zu behandeln sind. Auch hier kann optional mit Verschlüsselung und Zertifikaten gearbeitet werden.

Ebenso wichtig ist es, alle eigenen Domänen bei der Domänenverwaltung einzutragen, damit enQsig weiß, welche E-Mails es annehmen und welche es abweisen soll. Darüber hinaus ist es möglich, die SMTP-Adressen über eine Verbindung zum Active Directory, aber auch mittels einer Benutzerliste als Datei abzugleichen. Die Einträge können sowohl in eine Positiv-Liste (zugelassene lokale Adressen) als auch in eine Negativliste (unerwünschte lokale Adressen) fließen.

### Einfacher Import von Zertifikaten

Um das Gateway sinnvoll zu nutzen, sind schließlich noch Zertifikate notwendig, die importiert werden müssen. Eine Partnerschaft besteht hier zwischen Net at Work und TC Trustcenter, so dass ein Anwender auf Wunsch alles aus einer Hand beziehen kann.

Zertifikate können bei enQsig entweder durch öffentliche oder private Zertifikatsdateien importiert werden. Gibt es für eine Domäne beide Zertifikate, so wird das private bevorzugt. Liegt für eine Domäne bereits ein öffentliches Zertifikat vor und wird nun ein privates importiert, so wird das öffentliche entfernt. Gegebenenfalls sind beim Import entsprechende Passwörter anzugeben. Importieren lassen sich die Dateiformate CER, DER, PFX

und P12. Sofern das Gateway eingehende, signierte E-Mails verarbeitet, importiert es die anhängenden, öffentlichen Zertifikate automatisch. Diese wiederum kann es nutzen, um zukünftig diesem Empfänger verschlüsselte Mails zukommen zu lassen.

### Verschlüsselte Verbindung, verschlüsselte Mails

In der Rubrik "Vertrauensstellungen" trägt das Mail Gateway automatisch bei ausgehenden Mails die entsprechende Domäne ein. Die Domäneneinträge für viele große Provider werden bereits im Rahmen der Installation automatisch angelegt. Der Administrator hat nun die Möglichkeit, für jede Domäne eine individuelle Verbindungssicherheit vorzugeben, wobei vier Stufen zur Verfügung stehen, davon drei mit Verschlüsselung. Zu beachten ist hier, dass eine Verschlüsselung (der Verbindung, nicht der Mails) nur bei einer direkten Zustellung zum externen Mailserver möglich ist. Ist das Gateway so konfiguriert, dass es über ein SMTP-Relay, hier Smarthost genannt, Mails verschickt, so kann es nicht sicherstellen, dass die Kommunikation bis zum Empfänger verschlüsselt ist. Ein Mailversand wird dann fehlschlagen.

Um Probleme bei der Signierung gezielt bearbeiten zu können, gibt es einen eigenen Menüpunkt "Kryptographische Vorfälle", in dem alle Probleme in einer Liste aufgeführt sind. Im System ist eine Mailadresse zu hinterlegen, die bei jedem neuen Vorfall benachrichtigt wird.

Im Gegensatz zur Signierung und Verschlüsselung mit einem Mailclient am Arbeitsplatz hat der Einsatz des zentralen Mail Gateways einige deutlich sichtbare Änderungen zur Folge. So hat der Anwender keinen Einfluss darauf, ob seine Mails signiert und/oder verschlüsselt werden, dies entscheidet allein das Gateway anhand des vom Administrator definierten Regelwerks.

### Umfangreiches Regelwerk erfordert Überblick

Im Test haben wir diverse E-Mails mit und ohne Signatur sowie Verschlüsselung



an verschiedene Empfänger versendet, wobei das Gateway von einigen den öffentlichen Schlüssel über eine eingegangene signierte E-Mail gespeichert hatte. Parallel dazu haben wir die Regeln verändert, um zu sehen, wie das Gateway bei verschiedenen Einstellungen arbeitet. Schnell zeigte sich, dass es sehr wichtig ist, die diversen Möglichkeiten genau zu studieren und an die individuellen Anforderungen anzupassen.

Als recht unkritisch erweist sich hier die Signierung. Indem der Administrator ein Zertifikat zu einem Gateway-Zertifikat hochstufte und gegebenenfalls persönliche Zertifikate von Anwendern hinterlegt, kann das Gateway für die Signierung vorrangig das persönliche und ansonsten das Zertifikat des Gateways verwenden. Bezüglich der Verschlüsselung muss der Administrator genauer abwägen, welche Einstellung er wählt. Ist beispielsweise die Verschlüsselung optional, so verschlüsselt das Gateway nur an Adressaten, von denen ein öffentlicher Schlüssel vorliegt, an andere aber nicht. Das passt aber eventuell nicht zu dem Wunsch, dass Mails mit vertrauenswürdigen Inhalt ausschließlich verschlüsselt übertragen werden sollen. Wird nun die Regel auf eine obligatorische Verschlüsselung umgestellt, können keine Mails mehr an Adressaten versendet werden, von denen kein Schlüssel vorliegt. Werden nun in einer Mail mehrere Empfänger aufgeführt und nur von einem liegt kein Zertifikat vor, so wird die Mail an niemanden versendet.

### Plug-In für den Mailclient und PDF-Verschlüsselung geplant

In der jetzigen Version kann ein Anwender das Gateway noch nicht steuern, aber es ist ein Plug-In für Outlook geplant, damit der Versender Signierung und Verschlüsselung selbst vorgeben kann. Wann dieses aber verfügbar sein wird, steht noch nicht fest. Falls übrigens ein Anwender seine Mail gleich am Arbeitsplatz signiert, so hängt es von der Einstellung des Gateways ab, ob es die Signatur wieder entfernt oder nicht. Wird nämlich

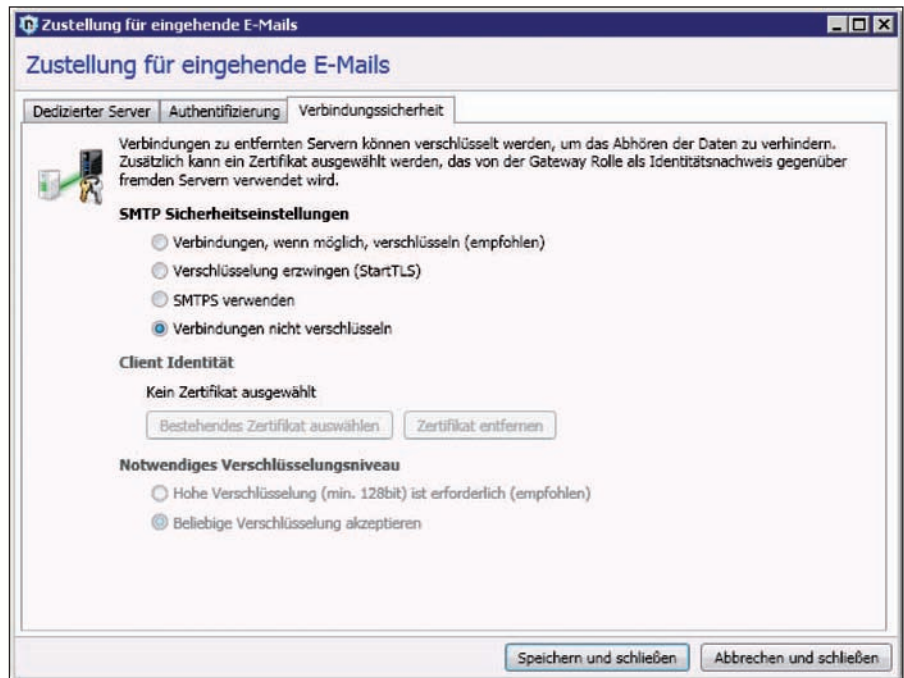


Bild 3: Bei der Verbindungssicherheit für eingehende Mails stehen vier SMTP-Sicherheitseinstellungen zur Verfügung

eine derartige Signatur mitgegeben, so besteht die Gefahr, dass der Empfänger seine Antwort damit verschlüsselt und das Gateway eine Mail erhält, welche es nicht entschlüsseln kann. Je nach Einstellung wird die Mail nun abgewiesen oder dem Anwender verschlüsselt zugestellt. Letzteres hat aber den Nachteil, dass die Mail vor der Zustellung nicht auf Viren gescannt werden kann.

Ob ein Zertifikat bei der Verwendung noch gültig ist, prüft das Gateway mittels der CRL (Certificate Revocation List) des ausstellenden CA. In Zukunft ist eine Überprüfung mittels OCSP geplant, was in der Regel einen etwas aktuelleren Stand liefert als die CRL.

Kommt von einem Absender eine Mail an mehrere Empfänger im Unternehmen, so kann es sein, dass für die Verarbeitung dieser Mail für die Empfänger unterschiedliche Regeln greifen. Aufgrund des SMTP-Protokolls ist es nun nicht möglich, für die unterschiedlichen Empfänger entsprechend unterschiedliche Rückmeldungen zu liefern. Umgehen lässt sich das Problem durch die Ak-

tivierung der so genannten "Strict Single Rule", die den Absender zwingt, jedem Adressaten eine eigene Mail zu schicken. Laut RFC ist das erst ab dem 101. Empfänger erlaubt, aber praktisch kein Mailserver stört sich daran, wenn es weniger Empfänger sind.

In der nächsten Version 7.6 soll eine PDF-Verschlüsselung enthalten sein. Dazu wird das Dokument am Gateway mit einem Zufallscode verschlüsselt, der dem Empfänger parallel per SMS zugeschickt wird.

### Vorbildliche Dokumentation und Reporting

Eine sehr umfangreiche und gut aufgebaute Dokumentation erleichtert sowohl die Installation und anschließende Einrichtung des Mail Gateways als auch die weitere Bedienung. Sehr hilfreich ist im Handbuch die Rubrik "Fehlersuche", die diverse detaillierte Hinweise zur Behebung von Problemen gibt. Dies beginnt mit Tipps, wie das Mail Gateway am besten hinsichtlich seiner Funktion kontrolliert wird. So sollte der Administrator zuerst den Statusbildschirm auf der Überblickseite der Ma-



nagement Konsole betrachten. Hier sind die Rollen mit ihrem Status aufgelistet. Sind dort nicht alle Positionen mit einem grünen Haken versehen, ist dies ein erster Hinweis auf eine Fehlfunktion. Dann kann der Administrator eine einzelne Rolle markieren und erhält wiederum eine detaillierte Übersicht zum Status beziehungsweise zu gefundenen Fehlern.


Neben der Dokumentation und den beschriebenen Statusangaben der Rollen gibt

es im Programm noch weitere Übersichten, die bei der Fehlersuche oder auch der Analyse des Mailverkehrs helfen. So steht dem Administrator eine Nachrichtenverfolgung zur Verfügung, mittels derer er nach bestimmten Kriterien suchen kann. Von der E-Mail sieht er allerdings nur den Betreff, daneben noch Absender, Empfänger und Zeit, aber nicht den Inhalt. Ein unberechtigtes Mitlesen ist also nicht möglich.

Eine Ereignisanzeige liefert Informationen zur Ausführung interner Aktivitäten, außerdem gibt es eine detaillierte Ansicht zur Serverleistung mit diversen statistischen Daten (Ressourcennutzung durch die Rollen, Datenbankgröße, empfangene und versendete Nachrichten sowie Belastung des Systems).

### Fazit

enQsig übernahm in unserem Test fehlerlos die E-Mail-Verschlüsselung und versah Nachrichten bei Bedarf mit einer qualifizierten elektronischen Signatur. Da das Werkzeug als SMTP-Proxy arbeitet, ist es erfreulich einfach in bestehende Mailumgebungen zu integrieren. Dadurch, dass das Gateway bestimmt, inwiefern Mails an bestimmte Adressaten signiert und/oder verschlüsselt werden, lassen sich entsprechende Unternehmensrichtlinien gezielt durchsetzen, ohne dabei von Aktionen der Mitarbeiter abhängig zu sein. Letztendlich spart sich ein Anwender damit auch den Aufwand, seine Mails mit einer qualifizierten elektronischen Signatur zu versehen. Allerdings vermischen wir die Möglichkeit, dass ein Anwender steuern kann, ob signiert und verschlüsselt wird oder nicht. Dieses Feature ist aber für eine spätere Version geplant.

Von Vorteil ist weiterhin die Möglichkeit, die im Gateway angelegten Benutzer unter anderem mit einem Microsoft Active Directory zu synchronisieren. Gefallen haben uns auch die insgesamt intuitive Bedienung und das gute Reporting mit einer Nachrichtenverfolgung, abgerundet durch eine detaillierte Dokumentation, die diverse Hinweise und Tipps zur Analyse und Fehlersuche gibt. (ln) 

#### Produkt

Programm zur E-Mail-Verschlüsselung und qualifizierten elektronischen Signatur, mit zusätzlicher Lizenz auch nutzbar als Anti-Spam-Lösung.

#### Hersteller

Net at Work  
www.enQsig.de

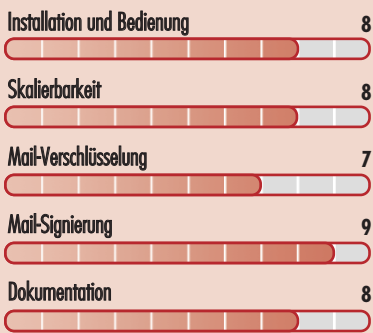
#### Preis

Die Lizenz für enQsig kostet für 25 Benutzer 1.625 Euro.

#### Technische Daten

www.it-administrator.de/downloads/datenblaetter

#### So urteilt IT-Administrator (max. 10 Punkte)



#### Dieses Produkt eignet sich

**optimal** für Unternehmen, die einen eigenen Mailserver betreiben, eine Mailverschlüsselung sowie automatische Signierung benötigen und in diesem Umfeld auf Windows als Betriebssystem setzen.

**bedingt**, falls ein Unternehmen im Internet-Mail-Umfeld auf Linux als Basis setzt. Hier lassen sich keine Funktionen auf einem Server zusammenfassen. Administratoren dürften dann eine durchgängige Linux-Umgebung bevorzugen.

**nicht**, wenn es keinen Bedarf für eine Mailverschlüsselung sowie für signierte Mails gibt.

**Net at Work Mail Gateway 7.5.71**