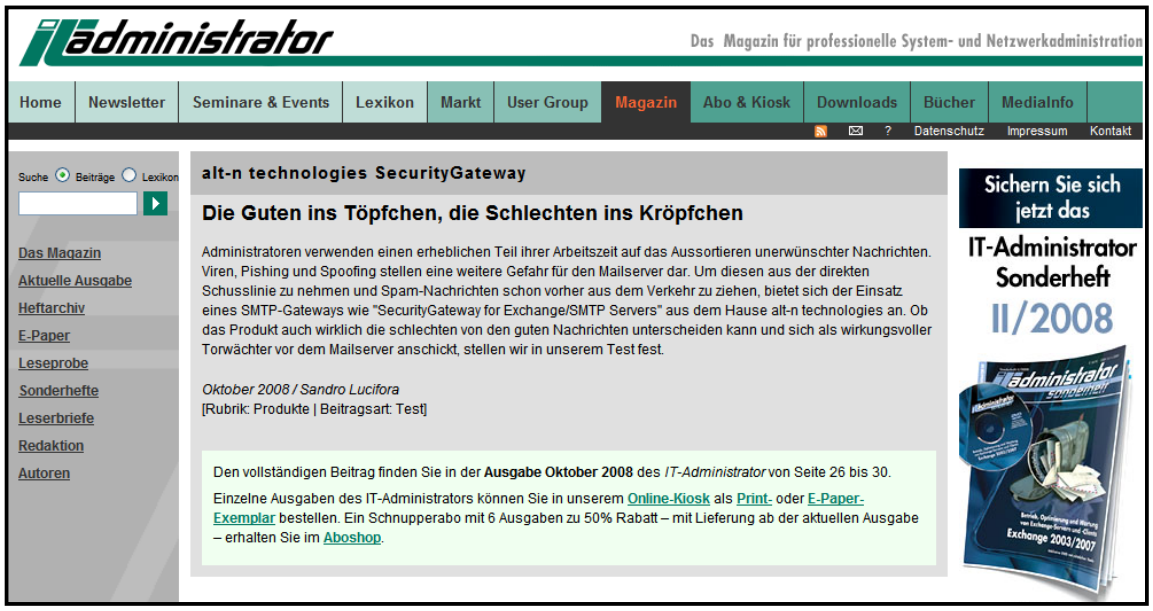
English Translation of SecurityGateway for Exchange/SMTP Servers

Source: IT-Administrator.de

Publication: October 2008



Testing: Alt-N Technologies SecurityGateway

by Sandra Lucifora

Administrators spend a considerable amount of their time on the job on eliminating unwanted messages. Viruses, Phishing, and Spoofing pose further dangers to mail servers. In order to remove the mail server from the direct line of fire, and to eliminate Spam messages before they even reach the server, the use of SMTP gateways, like “SecurityGateway for Exchange/SMTP” by alt-n technologies, seems to be the logical course of action. In our test, we will determine whether this product can really discern the good from the bad messages and whether it acts as a capable gate keeper to protect the mails server.

Electronic mail is transferred from one SMTP server to the next. In order for this data transmission to work properly, an SMTP server must be continuously reachable from the Internet via port 25. If the same server also offers POP3 or even contains the entire message storage, the digital attack surface continues to increase. In order to continue to be able to directly receive e-mail messages and have the e-mail server remain in the secured zone of the intranet, the installation of a separate SMTP

English Translation of SecurityGateway for Exchange/SMTP Servers

Source: IT-Administrator.de

Publication: October 2008

gateway seems the logical course of action. It is only the SMTP gateway that is directly reachable from the internet, and it acts as the upstream SMTP server. In addition, this service scans incoming mail and filters Spam and Viruses.

It is exactly this functionality that “SecurityGateway” by alt-n technologies offers. The software receives e-mail, checks it for validity and quality in a multi-layered process, and transmits the messages found legitimate to the downstream mail server. The advantages of this mode of operation are very apparent: The gateway can be integrated into any existing mail system, regardless of its manufacturer, and the administrator does not need to adapt the configuration of the existing mail server.

Installation and Configuration

After the normal installation procedures were complete, we first defined the method of verification. Exploring this function, we saw the first advantage for the gateway as the option permits to define in advance which e-mail recipients the gateway will accept messages for in the first place. The recipients can be defined manually directly at the gateway server. Most often, however, the e-mail recipients are already defined elsewhere. In larger installations – or just to eliminate unnecessary work – the method of choice is the verification against an Active Directory, an Exchange Server, or any other LDAP server. If another groupware solution is used, the “SMTP call forward verification” eliminates the need for a manual configuration. Using the SMTP protocol, this feature checks, for each incoming message, whether the recipient has a mailbox at the downstream server.

After we had configured the mail domains and the method of verification, we defined the IP address or the host name and the mail server which was to receive messages after verification. Here, we also defined the SMTP port. This setting is important if SecurityGateway and the mail server run on the same hardware server. In this case, both services would monitor port 25 at the same IP address which would disrupt server operations. We therefore had to set the downstream SMTP server to a different port – 10025, for example – (see fig. 2). This results in the gateway accepting external e-mail on port 25; the messages are then scanned and forwarded to, for example, an Exchange Server on port 10025. In this type of configuration it is important to configure the downstream mail server so it only accepts e-mail messages from the same IP, the gateway, and to enforce SMTP authentication. This ensures that the mail server cannot be abused as a relay server. After these steps are complete, the actual installation is concluded, and the services start.

English Translation of SecurityGateway for Exchange/SMTP Servers

Source: IT-Administrator.de

Publication: October 2008

SecurityGateway provides its own web-based administration interface through its own web server, operating parallel to an existing IIS. The interface can be used with all major browsers. If the verification of permitted recipients is done against an Active Directory – Exchange, in effect -, then the only setting still required before the gateway can first be used is that of the permitted recipients' domains. In addition, the gateway should be told which server to authenticate the mailboxes against, and where to deliver the e-mail messages. In our test, we configured different upstream and downstream e-mail servers for various domain names.

Multi-Layer Security

The Security menu of the gateway is subdivided into the sections "Spam", "Virus", "Spoofing", and "Abuse". The Anti Spam features are based on the well-known "SpamAssassin" and work with heuristic rules and Bayesian filtering. The software can use the integrated SpamAssassin engine or a remote SpamAssassin daemon. The second option offers the advantage that one SpamAssassin can be configured centrally for multiple gateways. The DNS blacklist uses the databases of "spamhaus.org" and "spamcop.net"; additional databases can be included. The URI blacklist complements the spam detection routines based on the well-known URIBL.

Effective Spam Protection through Greylisting

Greylisting is one of the most up-to-date features of spam filters. This feature causes SecurityGateway to temporarily refuse the first e-mail message from an unknown sender. If a second attempt is made to deliver the e-mail message (and this is how SMTP servers configured normally and in accordance with RFC operate), the e-mail message is finally accepted. Spam tools will not try to send such e-mail messages a second time because they never received the rejection messages from the protocol dialogue. After the second, regular delivery, SecurityGateway treats the mail server as "good" and stores this information in the local database. If the gateway receives more messages from the same domain and the mail server that has been checked already, these messages will be accepted directly.

The Clam AntiVirus engine takes care of scanning for viruses. The optional extension ProtectionPlus comes with the Kaspersky engine to protect the system against infected messages. We could set the interval for updating the virus definitions between once per hour and once per day, but the hourly update should be the method of choice.

English Translation of SecurityGateway for Exchange/SMTP Servers

Source: IT-Administrator.de

Publication: October 2008

No Change for Spoofing

Spoofing is a mail server's attempt to conceal its true identity, e.g. through forged IP addresses. SecurityGateway contains several effective weapons to check a sender's identity in advance. In addition to the first step, the reverse look-up, the DKMI (sic!) verification and the Sender Policy Framework (SPF), together with a verification of the Sender ID are used on every e-mail message. The additional call-back verification is an additional obstacle to Spam messages. Spam messages are frequently sent without a value in the "from" e-mail header. If, because of this, the sender cannot be verified, the gateway will refuse the e-mail message.

We configured the protection against abuse as a relay server (and thus as a Spam server) by defining the permitted sender addresses. The additional feature of SMTP authentication is an additional protection against misuse.

Additional, customised filters can be created according to rules for message content and attachments. In our test, we could, for instance, have executable files blocked and audio files moved into quarantine automatically. These settings can be applied either globally for all domains, or on a per-domain basis. Individual and manually configurable black and white lists on the basis of single e-mail addresses, domains, and IPs, round off the powerful security configuration.

Scanning of outbound messages increases the rate of detection

The outgoing data traffic is monitored in addition to the incoming traffic. The prerequisite for the use of this feature was that we instructed our mail server to no longer deliver messages directly or via a smart host, but only via SecurityGateway.

The gateway can analyse the outgoing e-mail traffic and learn from it. The classic examples are the use of the words "sex" and "Viagra" in the message body. Upon receipt, these words regularly cause an e-mail message to be classified as Spam and isolated. Nonetheless, the use of these words can be part of daily business, for instance for pharmaceutical companies or the erotic trade. Where the gateway recognises that messages containing such key words are sent, the criteria for receiving e-mail messages are automatically adapted accordingly. This also applies to e-mail senders whose domains or mail servers – for whatever reason – find themselves on a blacklist. The gateway would normally refuse such e-mail messages. Where the software recognises from the outgoing e-mail traffic that e-mail messages are sent to a blacklisted domain, messages originating from that domain will find their way to the recipients.

English Translation of SecurityGateway for Exchange/SMTP Servers

Source: IT-Administrator.de

Publication: October 2008

Outstanding Detection Rates

In our test, we used a web service to have random spam and virus-infected e-mail messages delivered to our test domain. We also blacklisted a domain connected to the Internet on spamhaus.org. After these preparations, we could receive real and manipulated messages for several weeks and test the efficiency of the platform. No unwanted message passed through to our test domain without being quarantined first. Only when we deliberately sent e-mail messages to that domain through our gateway, SecurityGateway acknowledged that the receipt of individual e-mail messages seemed desired.

As already mentioned, the add-on ProtectionPlus, available for a surcharge, extends the security features of SecurityGateway by the Kaspersky AntiVirus engine. While the ClamAV engine did not fail to recognise any infected message during our test, one may assume that, in direct comparison, it could have more difficulties in case of very new viruses. Where the up-to-dateness of virus signatures is concerned, the Kaspersky engine is as good as unbeatable.

Conclusion

As a rule, the use of an SMTP gateway makes sense in order to complement an existing e-mail system by adding powerful Spam and Virus filters, and in order to remove the mail server from the DMZ of the network. During our multi-week test, SecurityGateway did not exhibit any weakness and safely blocked Spam, viruses, and phishing messages. The learning feature showed its first effect after a couple hundred sent e-mail messages. The versatile configuration options can backfire, however. If the security settings of the gateway are set too tightly, legitimate messages could be blocked. Because of this, it is necessary especially during the first weeks and months to regularly review the rules and log files and adapt them accordingly. Contrary to the rule applied to a firewall, to not accept anything initially and then gradually open up individual ports, in the case of SecurityGateway, you should initially rely upon the default configuration and then adapt them after several weeks of learning and analysing log files, step by step.

Those who select the smallest license size for 10 users will typically retrieve the e-mail messages from the internet provider using POP3. Through a workaround and an additional POP3 connector (see tip 2) this implementation can be kept. It would be desirable, however, that such functionality be already included in the Gateway. Aside from this, SecurityGateway is quick to deploy, its configuration can be highly fine-tuned, and it is extremely cost-efficient. At a cost of EUR 50 per user in the first year and EUR 10 in subsequent years, the investment should be quickly amortised.

English Translation of SecurityGateway for Exchange/SMTP Servers

Source: IT-Administrator.de

Publication: October 2008

----------Summary and Evaluation

Product: SecurityGateway for the filtering of Spam and defence against viruses

Manufacturer: alt-n technologies, www.altn.de

Pricing: A license for 10 users is EUR 474 for the first and EUR 100 for each subsequent year. The optional virus protection module ProtectionPlus adds EUR 143 for the first and EUR 100 for each subsequent year for the same number of users. Other license sizes available are 25, 50, and 100 users.

Technical data: www.it-administrator.de/downloads/datenblaetter

This is how IT-Administrator judges (max. 10 points)

Filtering reliability: 10

Individualisation of the filters: 8

Up-to-dateness of the definitions: 8

Time and effort to configure: 8

Time and effort for on-going administration: 9

This product is…

ideally suitable to safeguard existing e-mail systems based on Exchange, using the Active Directory

partially suitable to safeguard smaller e-mail systems without Active Directory, using an LDAP server or the SMTP call-forward verification

not suitable for use on a workstation.

Alt-N Technologies' SecurityGateway

---------- Fig. subtitles

Bild 1: Fig. 1: Schematic overview of the implementation of SecurityGateway by alt-n

Bild 2: Fig. 2: Configuration of the gateway if the target mail server resides on the same hardware

English Translation of SecurityGateway for Exchange/SMTP Servers

Source: IT-Administrator.de

Publication: October 2008

Bild 3: Fig. 3: The comprehensive web interface affords individual security settings

Bild 4: Fig. 4: Excerpt from a log file which documents an unsuccessful attempt at misusing SecurityGateway to send Spam

Bild 5: Fig. 5: Examples for the configuration of a Small Business SMTP Connector, in order to use SecurityGateway for outgoing messages as well

----------Tips

Tip 1: Fast hard drives

As SecurityGateway works in a heavily hard drive-oriented way, the e-mail throughput can be optimised by using fast hard drives. Separate hard drives for the database and the log files further increase performance.

Tip 2: Pull mail in case of dynamic IPs

Those who do not enter their internal mail server as an MX record for their internet domains or use dynamic IP addresses, can poll external mailboxes through a POP3 connector and have the messages forwarded to SecurityGateway through the SMTP protocol. In addition to commercial solutions, the free software “PullMail” is ideal for this task. This tool will probably not continue to be developed, but it can still be retrieved via link [1].

----------Other boxes

System requirements

The system requirements for SecurityGateway depend upon the e-mail traffic. For the average e-mail traffic of 10 to 25 users and in case of an exclusive use of the hardware, the manufacturer specifies the following minimum requirements for the server system: The operating system can only be Microsoft Windows 2000, XP, Vista, or Server 2003. The platform should be equipped with a Pentium 4 processor (multi-core is recommended) and a minimum of 512 MB RAM (2 GByte are better) and an NTFS partition with at least 500 MB of free space. The client must be equipped with a browser such as MSIE 6.0, Firefox 1.5, Opera 8.5, Safari 3.0, and with the Adobe Flash Player, starting from version 8.

English Translation of SecurityGateway for Exchange/SMTP Servers

Source: IT-Administrator.de

Publication: October 2008

We tested the gateway in a virtual machine running in VMWare, and with Windows Server 2008 as the operating system.