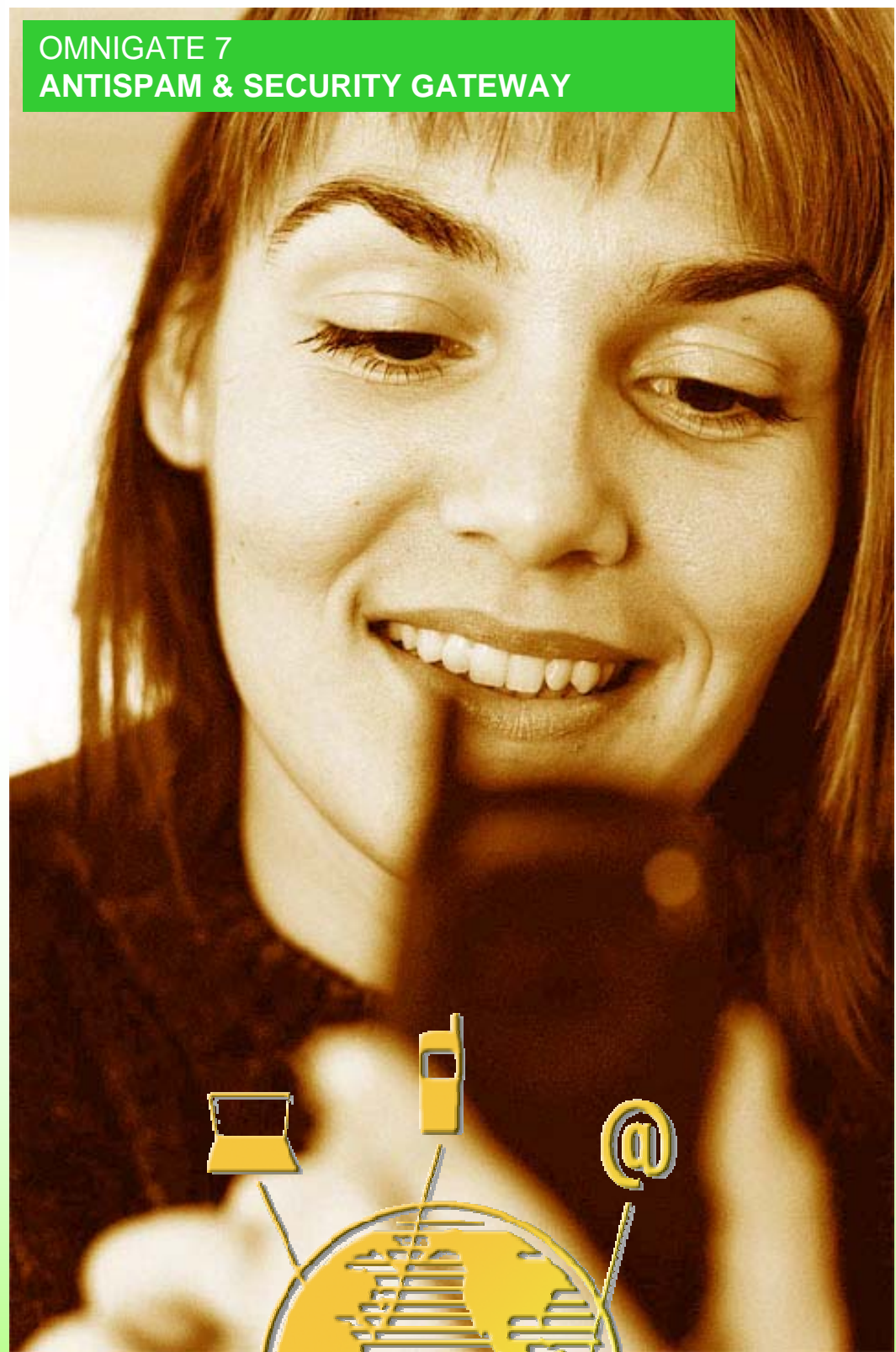




**OMNIGATE 7
ANTISPAM & SECURITY GATEWAY**

**Send
anything to
anybody
anywhere**



**OMNIGATE 7 ANTISPAM
& SECURITY GATEWAY**

OMNIGATE 7 ANTI SPAM & SECURITY GATEWAY

EMAIL SECURITY

Email security has never been simpler than with Omnigate 7. Omnigate adds a range of security functions to your email system.

Omnigate transparently integrates with Microsoft Exchange Server, Microsoft Mail, Lotus Notes, Domino, cc:Mail and Novell GroupWise.

Stop spam!

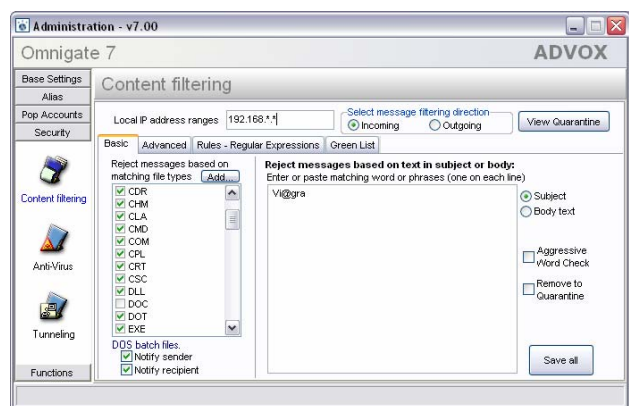
Protects the company against the ever increasing amount of unwanted email, otherwise known as spam.

Graylisting

Graylisting is a effective method of defending e-mail users against spam. In short, Omnigate will temporarily reject any email from a sender it does not recognize. If the email is legitimate, the originating server will try again to send it later, at which time Omnigate will accept it. If the email is from a spammer, it will probably not be retried as most spam are coming from "hijacked" computers and not from e-mail servers.

Regular Expression - A regular expression is a text pattern consisting of a combination of alphanumeric characters and special characters known as metacharacters. A close relative is in fact the wildcard expression which are often used in file management. The pattern is used to match against text strings. The result of a match is either successful or not, however when a match is successful not all of the pattern must match. Regular expressions work with all e-mail communication protocols: UUCP, POP3, Dial-up SMTP and SMTP.

RBL are databases of known servers that are used by spammers. These databases are updated regularly and are both subscription and free services. Omnigate can, with automation and in real time, control all incoming email and block email from known spammers. Omnigate supports unlimited numbers of RBL databases. The administrator can also draw up a list of blocked servers, domains and senders. With Omnigate's rules and filters, the administrator can also create rules and protection to stop email from specific domain addresses, IP addresses or senders. The antispam function is for companies that use SMTP to receive email.



An example of how simple it is to create an email filter. In this case, specific types of attached files are filtered out from all incoming email. Furthermore, a message is sent that explains the company's policy to the sender.

Email rules & filters

Email filters make it simple to create rules for what is permitted for the company to receive, such as senders and attached files.

For incoming email, filtering can only be based on sender's name, domain addresses and IP addresses. Incoming email with attached files can be virus scanned or filtered out dependent on the file type. The company can therefore efficiently protect itself against certain file types, for example exe files (executable files), or specific file names such as 'I Love You'. When a new virus begins to wreak havoc, the administrator can protect the company even before the suppliers of antivirus programs have issued updates.

The administrator can create rules using the variables below :

- | | |
|-----------------------|------------------------|
| - Sender | - Words in the heading |
| - Sender's domain | - Words in the message |
| - Sender's IP address | - File name |
| - Addressee | - File type |

EMAIL SECURITY

Email encryption in accordance with AES

Encrypt your email with Omnigate. Omnigate provides email tunnelling and email encryption that allows the Internet to be used as a VPN (virtual private network) for the company's email communication. The company can use the Internet as if it was the ordinary company network and send encrypted email which unauthorised persons are unable to read. All email between two Omnigate servers is encrypted and compressed automatically before being sent. The user doesn't need to think about security, as the encryption algorithm and password are in Omnigate.

This can be used for companies with several offices, which would like to be able to send emails securely between offices without investing in expensive private networks.

Omnigate uses an encryption algorithm in accordance with the latest AES standard (advanced encryption standard). AES is the encryption standard recommended today for authorities and public organisations in the USA. The algorithm specification is available from the US National Institute of Standards and Technology. <http://csrc.nist.gov/>

Computer virus protection

Omnigate can protect the company against computer viruses before they reach the user. The search for viruses is at the 'gateway' level. Both in and outgoing emails are checked through for viruses. All attached files are unpacked and searched through for viruses. The files can be packed (for example using WinZip) at several levels and can be coded with both UUENCODE and MIME. If a virus is found, the attachment is removed or repaired depending on how the antivirus program is configured. Several antivirus programs can be run simultaneously for maximum security. The most common virus programs, for example McAfee, F-Prot, Sophos Sweep, PC-cillin and Norton Antivirus are supported by Omnigate and the required settings are pre-installed.

For maximum protection, several virus programs from different suppliers can be used in parallel with Omnigate's own filters, see the previous page.

If the programme generates reports, these can included at the bottom of email messages giving detailed information on what was found and removed. The recipient is always informed if a virus has been found .

Communication with the Internet using a closed firewall.

Omnigate can be installed with one separate visible SMTP server set up outside the company's firewall to temporarily receive email and with one on the inside that collects emails and sends them to the company's email system. This means that the firewall can remain closed for all incoming traffic and only be open for outgoing traffic.

This configuration significantly raises the protection of the company's internal network. This is the configuration that the Norwegian Data Inspectorate recommends for Norwegian authorities and organisations (The Norwegian Data Inspectorate TV-202).



Email archiving

Archiving the company's email can be important if you use emails in your business relations. Email archiving can be used for following up the company's email policy and to prove that mails have been received or sent.

In Omnigate, all email both in and outgoing can be archived. The emails are saved in a compressed format every day with a separate file for each day .

SMTP/POP3 authentication

Omnigate 7 has strengthened SMTP security and authentication for external POP clients and SMTP servers. This means for example that:

- External email clients can log in and use the company's email server for receiving and sending email. These email clients receive the same protection, security and functionality as a user within the network.
- Increased security for downstream mail offices and other internal smtp servers, for example by handling the company's external email traffic via a main SMTP server.

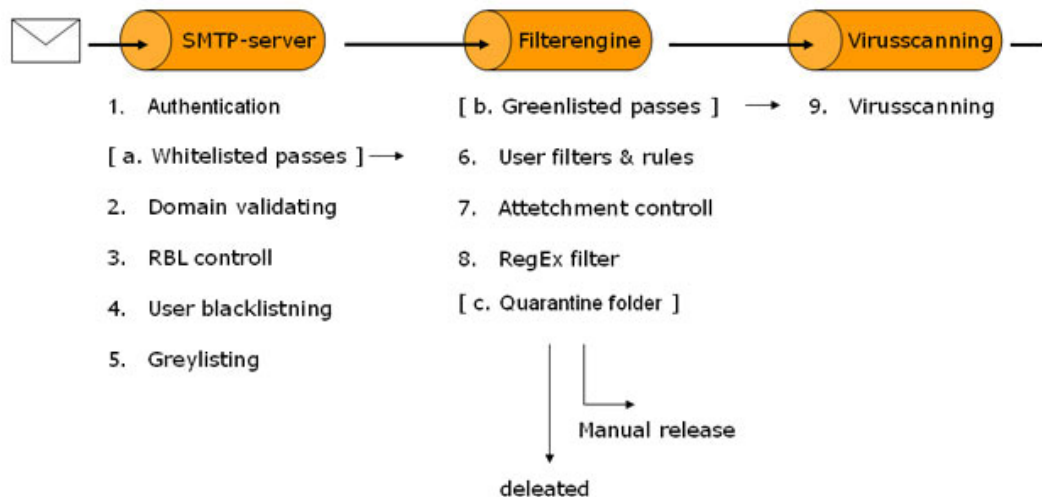
Email monitoring and traffic reports

Using Omnigate, the company's email traffic can be monitored and quickly analysed. The administrator sees who has received specific messages, an efficient function for identifying who has been affected by a computer virus. The administrator can also trace different types of problems or determine whether any user is infringing the company's email policy.

Email traffic can be analysed based on the following search terms:

- Sender, sorted by time, name, domain
- Recipient, sorted by time, name, domain
- File name, sorted by time, file name and sender

Omnigates steps for e-mail security



Omnigate SMTP Server

Below are the controls and security steps preformed in the Omnigate SMTP server. These controls can be activated or deactivated acording to the company e-mail policy.

1. Authentication and relaying

Authentication provides an access control mechanism. It can be used to allow legitimate users to relay mail while denying relay service to unauthorized users.

[a. Whitelisted]

Omnigate administrator can approve certain domains, ip-adresser or e-mailaddresses to pass thru Omnigate SMTP server without being controlled or blocked.

2. Domain valideting

All incomming e-mail validats that it is from a legitim and existing ip-address and domain. Non existing addresses will be blocked.

3. RBL Controll

RBL, Realtme Black List, (or DNSBL, Domain Name System Black List) is a live service to protect your system from known spammers and open relays that potentially may be used by spammers.

4. User blacklisting

There are multiple options to blacklist incoming messages. Omnigate adminstrator may blacklist on the senders domain and on the ip address that is sending the message. He may also blacklist on the name sent by the HELO command.

5. Graylisting

Greylisting is a effective method of defending e-mail users against spam. In short, Omnigate will temporarily reject any email from a sender it does not recognize. If the email is legitimate, the originating server will try again to send it later, at which time Omnigate will accept it. If the email is from a spammer, it will probably not be retried as most spam are comming from "hijacked" computers and not from e-mailservers.

Omnigate Filter Engine

Below are the controls and security steps preformed in the Omnigate Filter Engine.

[b. Greenlist]

Omnigate administrator can approve certain domains, ip-adresser or e-mailaddresses to pass thru Omnigate filter engine without being controlled or blocked. Greenlisted messages passes directly to the virusscan module.

6. User filters and rules

Omnigate filters make it easy to create specific rules for what is permitted for the company to receive, such as senders, e-mail content and attached files. Omnigate can carry out the following measures when a rule is activated:

- Remove the message
- Send the message to a different email address
- Answer the message

7. Attachment controll

Block potential harmful attachments before they reach the end user. An attachment checking rule allows you to block attachments of a certain type.

Its wise to block all executable attachments, in Omnigate 7 its easy to do that.

8. RegEx Filter

A regular expression is a text pattern consisting of a combination of alphanumeric characters and special characters known as metacharacters. A close relative is in fact the wildcard expression which are often used in file management. The pattern is used to match against text strings. The result of a match is either successful or not, however when a match is successful not all of the pattern must match.

[c. Quarantine folder]

All messages filtered by the Omnigate will be automatically placed in a Quarantine folder. Users will receive a daily Quarantine report and may choose to delete or release a message.

9. Virusscanning Omnigate protects the company against computer viruses before they reach the user. The search for viruses is at the gateway level. Both in and outgoing emails are checked through for viruses. Multiple viruscanners can be used.

Advox Omnigate

There are a reason why...

A&H Display Cards Ltd
AB Trav och Galopp
AC Nielsen AS
Acidchem International Sdn Bhd
Aerotech Telub
Akademiska Sjukhuset Uppsala
Arjeplogs Kommun
AT Engineering Sdn Bhd
Autoliv Sverige AB
Avestapolarit AB
Banctec AB
Bankgirocentralen BGC AB
Berkeley Projects UK Ltd
Bid & Ask Fondkommission AB
Biotech Pharma AS
Bostads AB Drott
Bravida AS
City Center of Music & Drama
Connex Sverige
Danshögsolan
Den Norske Lageforeningen
Denon Digital LLC
Det Norske Nobelinstitut
Drammen kommune
EFG Askö OY
Elköp AS
Enosvezia AB
Ernst Gerber AB

Essilor Norge AS
Eurokraft AS
Fabega AB
Fiskars Norge AS
Folksam Auto
Freshfield Lane Brickwork
Gävle Kommun
Gjövik Kommune
Grimaldis Mek Verk AB
Göteborgs Fotbollsforbund
Haninge kommun
Hewlett-Packard, Sverige, AB
HSB Syd IT
Huddig AB
Hufvudstaden AB
Husvarna AB
Hällefors Kommun
Iggesund Tools AB
Infineon WS Sweden AB
Infocus AS
Intrado Ltd
Jamtkraft AB
Karlskoga Kommun
KG Knutsson AB
KKW GOESGEN-DAENIKEN AG
Kockums AB
Korsnas AB
Kriminalvårdsstyrelsen

Kristianstad Kommun
Kungälv Kommun
Lahega Kemi AB
Landstinget Dalarna
Landstinget Kronoberg
Länsförsäkringar Stockholm
Lantmännen
Lardal kommune
Lidkopings kommun
Linder Aluminiumbåtar AB
Lindex AB
Linköpings Universitet
Lomma Kommun
Ludvika Kommun
Mannheimer Swartling AB
Manpower AB
Masonite AB
Micki Leksaker AB
Micromatic Int AB
Mique
Natsteel Chemicals
NCH-Gruppen
Nord-Fron Kommune
Nordtrafikk AS
Norges Blinddeforund
Norges Turistråd
Norpapp AS
Norrköpings Kommun

Norsafe AS
Norsk Bedriftshelsesenter
Norsk Luftambulans
OM Gruppen
Opcon AB
Oppland Vaskeri
Optimal AS
Orkla Trykk AS
Os Kommune
Oslo Kommun Boligbedriften
OZ zorgverzekerings
Pentel (stationary) Ltd
Pfizer AB
Pharma Systems AB
Phil Andreou LTD
Plockmatic Int. AB
Polismyndigheten
Pågen AB
Rederi AB Veritas Tankers
Reko AS
Riksskatteverket IT
Sage Construction Ltd
Sales kommun
SCA Obbola
SCA Packaging Munksund
Scan Coin Industries AB
Scandinavian Aerospace
Scandust AB

Scanraff
Sel Kommune
Siemens Telefonsupport
Skånemejerier
Songdalen Kommune
Sortland Kommune
SSAB Tunplåt AB
Stena Line IT Services AB
Stiftelsen SOS-Barnebyer Norge
Stora Enso
Swedia Networks AB
Svensk Bilprovning AB
Svenska Kraftnät
Söderhamns Kommun
Sör-Fron Kommune
Tana Kommune
Tele2 AB
Telia Sonera Sverige AB
Tilda Toys AB
Toyota Truck Norge AS
Turnbullroofing
Unisys AB
Unite AB
Upplands Väsby Kommun
V&S Åhus
Vasakronan AB
Waterbedrijf Europort
Visual Wireless Europe AB

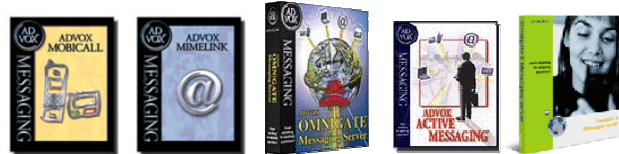
Advox products are based on experience

Advox is a software company founded 1992.

Advox develops products and solutions for mobile message communication and secure email.

Advox was in 1993 **the first in the world** to develop SMS software, Advox Mobicall. In 1994, Advox Mimelink was one of the first to handle the new email standard MIME several years before, for example, Microsoft.

Advox products are used today by GSM operators, Internet operators and mobile portals for their income generating services, by municipalities, schools, hospitals and companies for their company critical email handling.



Advox Mobicall, Advox Mimelink, Advox Omnigate 4, Advox Active Messaging, Advox Omnigate 5.

More than 6000 companies

Advox products are used today by more than one million users and has been sold to more than 6,000 companies in 20 countries around the world.

Advox products are sold by authorised resellers across the world.

For more information

Azena Advox AB
Linjalvägen 6a
187 66 Täby
Sweden

Phone: +46-8-54490900
Fax: +46-8-7324972
email: info@advox.se
www.advox.se



Copyright 1992-2007 Azena Advox AB.
Advox, Omnigate, Mobicall, Mimelink are registered trademarks by Azena Advox AB

TECHNICAL INFORMATION

Platform

Omnigate 7 is written for and operates under Windows NT, 2000, 2003 and Microsoft XP.

Hardware: Minimum PC, Pentium III, 800 MHz with 256 mb internal memory and 50 mb hard disk plus space for messages.

Internet communication

Omnigate can operate email communication over the Internet via the protocols SMTP, Dial-up SMTP, UUCP, Dial-up UUCP, POP3 (Multipop, Wildcard, POPkonto).

Omnigate operates with dial-up modems, ISDN, ADSL, Fixed connection, etc.