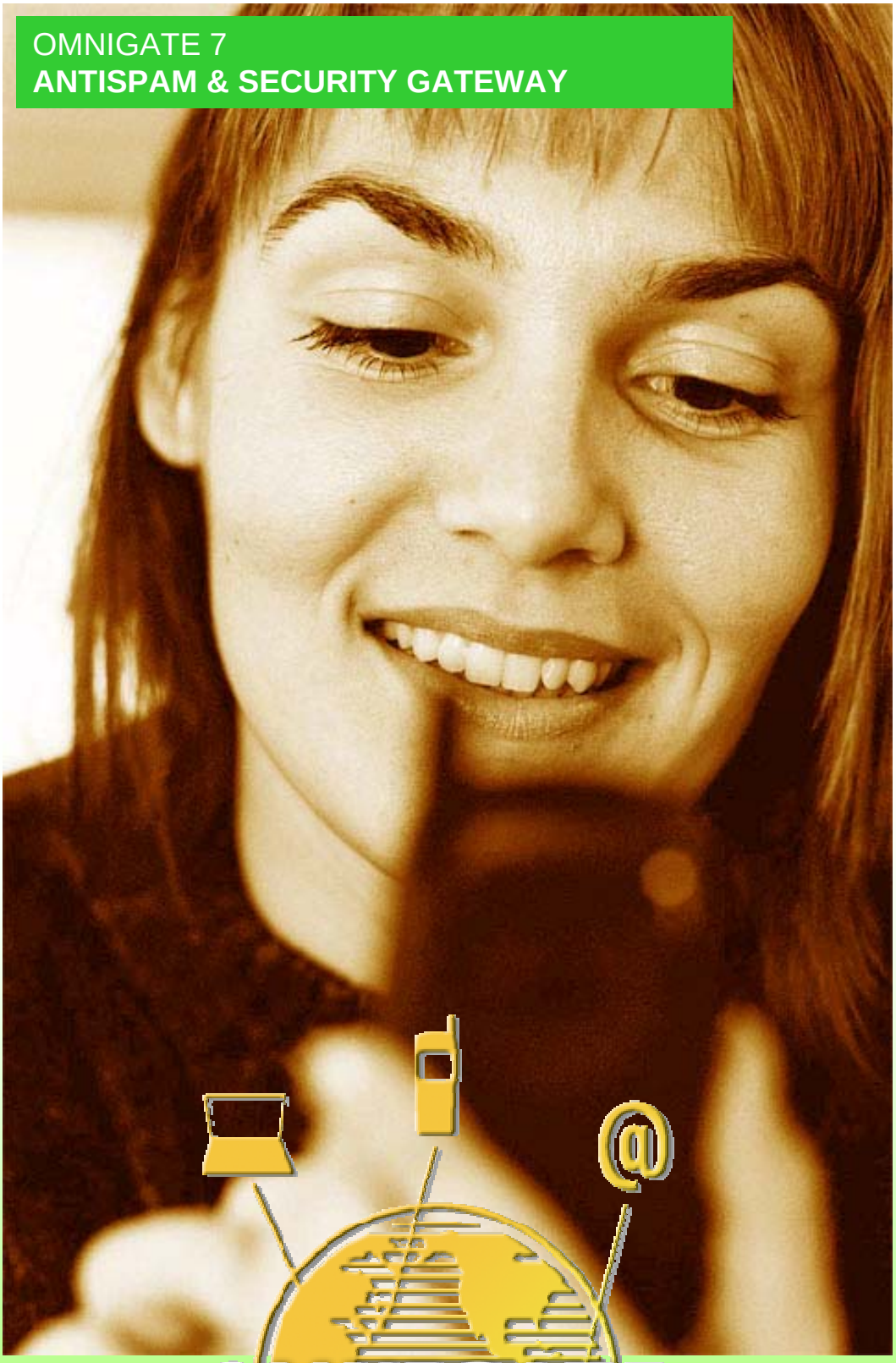
OMNIGATE 7
ANTISPAM & SECURITY GATEWAY



Send anything to anybody anywhere

OMNIGATE 7

OMNIGATE 7 ANTISPAM & SECURITY GATEWAY

OMNIGATE 7
ANTISPAM & SECURITY GATEWAY

Ett nödvändigt säkerhetstillägg till företagets e-postsystem.

Stoppa SPAM

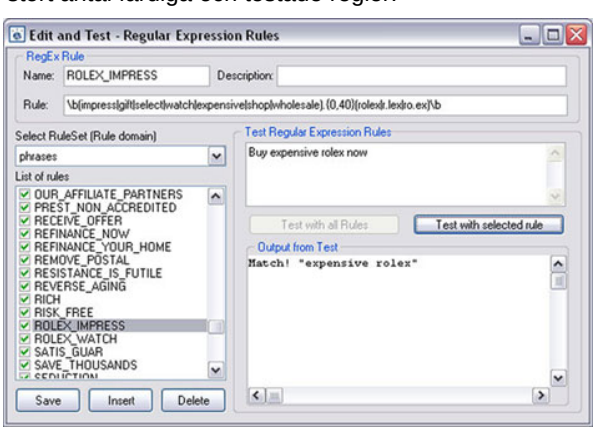
Skydda företaget mot den allt ökande mängden av oönskad e-post, sk spam. Omnigate 7 har en rad oberoende metoder att stoppa spam.

- Graylisting
- Regular expressions
- RBL (realtime blackhole lists)
- E-postregler & filter
- Autentisering och DNS kontroller

Graylisting, Grålistning
När ett e-postmeddelande tas emot av SMTP-server så skickas första gången ett felmeddelande tillbaka till avsändaren om att SMTP-servern inte kan ta emot meddelandet just nu, normalt så gör de flesta e-postservrar då ett eller flera omsändningsförsök. Samtidigt registreras att ett meddelande har skickats från aktuell avsändare och kommer att släppas igenom nästa gång det kommer och ev framtida gånger.

Tekniken fungerar som spam filter genom att många spam utskick sker från "kapade" datorer som normal inte är en SMTP server med möjligheten att hantera ett felmeddelande och göra ett omsändningsförsök. Fördelen med greylistnings tekniken är att den inte drabbar "oskyldiga" som råkat bli svartlistad eller skrivit ett ord/mening i meddelandet som gör att det blockerats av misstag. Samt att graylistnings

Regular Expressions - Antispamfilter som består av register över av kända uttryck och mönster av ord, som ofta används av spammare. Utifrån dessa skapar man regler som används för att filtrera bort liknande meddelanden. Omnigate administratören kan även utöka registret med egna regler eller importera nya från Internet eller från Advox hemsida. Omnigate levereras med ett stort antal färdiga och testade regler.



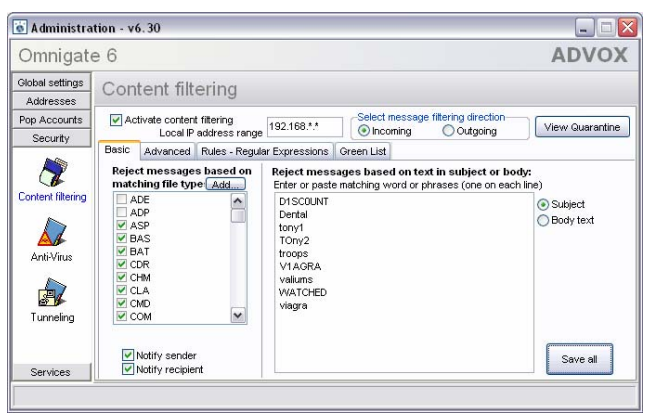
Regular expressions **fungerar för** alla typer av e-postkommunikation t.ex **UUCP, POP3** och SMTP.

RBL - Realtime blackhole lists, är databaser över kända datorer (ip-adresser) som används av spammare. Omnigate kan med automatik och i realtid kontrollera all inkommande e-post och blockera e-post som kommer ifrån dessa datorer.

Omnigate stödjer obegränsat antal RBL-databaser och e-postadministratören kan enkelt lägga upp nya RBL-databaser. Med Omnigates regler och filter kan administratören även skapa egna regler och skydd för att stoppa e-post från en viss domänadress, IP-adress eller avsändare.
RBL - antispamfunktion fungerar hos företag som använder SMTP för att ta emot e-post.

E-postregler & filter - Med ett e-postfilter kan administratören skydda företaget mot obehagliga överraskningar. Med Omnigate får administratören av företagets e-postsystem en rad möjligheter att hantera den e-post som passerar in och ut från Internet. E-postfiltret gör det enkelt att skapa regler för vad som är tillåtet för företaget att ta emot i form av t.ex avsändare, bifogade filer, etc.

På inkommande e-post kan filtrering ske på t.ex enskilda avsändares namn, domänadresser och IP-adresser.



Inkommade e-post med bifogade filer kan virusscannas eller filtreras bort beroende på filtyp. Företaget kan därmed effektivt skydda sig mot vissa filtyper, t ex exe-filer (exekverbara filer), eller specifika filnamn, t ex ”I Love You”.

Karantänfolder - E-post som filtreras bort via regular expression eller med Omnigate e-postregler & filter läggs i en speciell karantänfolder. E-postadminstratören kan sedan bestämma om det skall tas bort efter en viss tid eller om det skall skicka vidare till mottagaren. Mottagaren kan även erhålla en rapport över den e-post som finns i karantänfoldern. Administratören kan sätta upp hur ofta reporten skall skickas, en eller flera gånger per dag.

E-postarkivering
Att arkivera företagets e-post kan vara viktigt om du använder e-posten i dina affärsrelationer.
E-postarkivering kan användas för uppföljning av företagets e-postpolicy och för att bevisa mottagen eller skickad e-post. I Omnigate 7 kan all e-post, både in- och utgående arkiveras. E-posten sparas i ett komprimerat format dag för dag i en separat fil för varje dag.

SMTP inbound relay server
Omnigate kan installeras så att en separat synlig SMTP-server sätts upp utanför företagets brandvägg för att temporärt ta emot e-post och en på insidan som hämtar in e-posten och skickar den vidare till företagets e-postsystem. Detta innebär att brandväggen kan hållas stängd för all inkommande trafik och och endast vara öppen för utgående trafik.

Denna konfiguration höjer väsentligen skyddet för företagets interna nätverk. Detta är den konfigurering som det norska Datatilsynet rekommenderar till norska myndigheter och organisationer (Datatilsynets TV-202).

E-postgateway till Internet
Omnigate kan sköta e-postkommunikationen med Internet via protokollen SMTP, Dial-up SMTP, UUCP, Dial-up UUCP, POP3 (Multipop, Wildcard, POPkonto).

Omnigate fungerar med uppringt modem, ISDN, ADSL, Fastförbindelse, m fl.

SMTP/POP3-autentisering
Omnigate 7 har förstärkt SMTP-säkerhet och autenticering för externa POP-klienter och SMTP-servrar.

Detta innebär t ex att:
– Externa e-postklienter kan logga in och använda företagets e-postserver för att ta emot och skicka e-post.

– Ökad säkerhet för downstreampostkontor och andra interna smtp-servrar, för att t ex hantera företagets externa e-posttrafik via en huvud-SMTP-server.

Omnigate e-postgateways.
Omnigate har inbyggda e-postgateways för transparent integration med marknadens vanligaste e-postsystem.

Microsoft Exchange Server 5.5, 2000, 2003, Small Bussines Server, Lotus Notes/Domino, Novell GroupWise, POP3 och SMTP baserade e-postsystem.

Plattform.
Omnigate 7 är skrivet för och fungerar under Windows NT 4, Windows 2000, 2003 och Microsoft XP. Omnigate kan installeras på separat server eller på samma server som e-postservern.

Hårdvara
Minimum PC, Pentium III, 800 MHz med 256 mb internminne.

Licensiering
Omnigate 7 licenseras på antal användare I företaget.

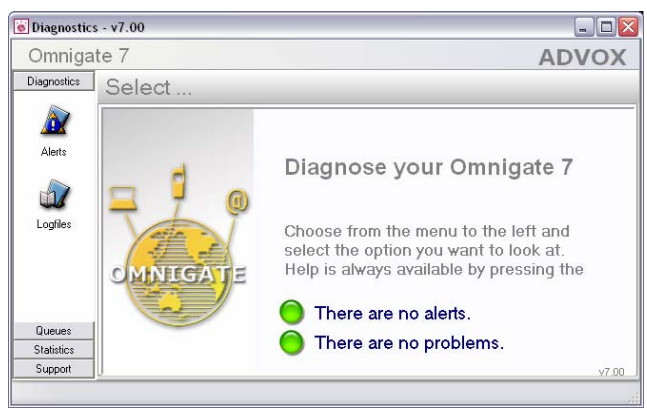
E-postkryptering enligt AES
Kryptera er e-postkommunikation med Omnigate. Omnigate innehåller e-posttunneling och e-postkryptering som gör att Internet kan användas som ett VPN (virtuellt privat nätverk) för företagets e-postkommunikation. Företaget kan använda Internet som om det vore det vanliga företagsnätet och skicka krypterad e-post utan att obehöriga kan läsa den.
All e-post mellan två Omnigate-servrar krypteras och komprimeras automatiskt innan e-posten skickas iväg.

Omnigate 7 använder en krypteringsalgoritm enligt den senaste AES-standarden (advanced encryption standard). Specifikation av algoritmen finns hos US National Institute of Standards and Technology. http://csrc.nist.gov/

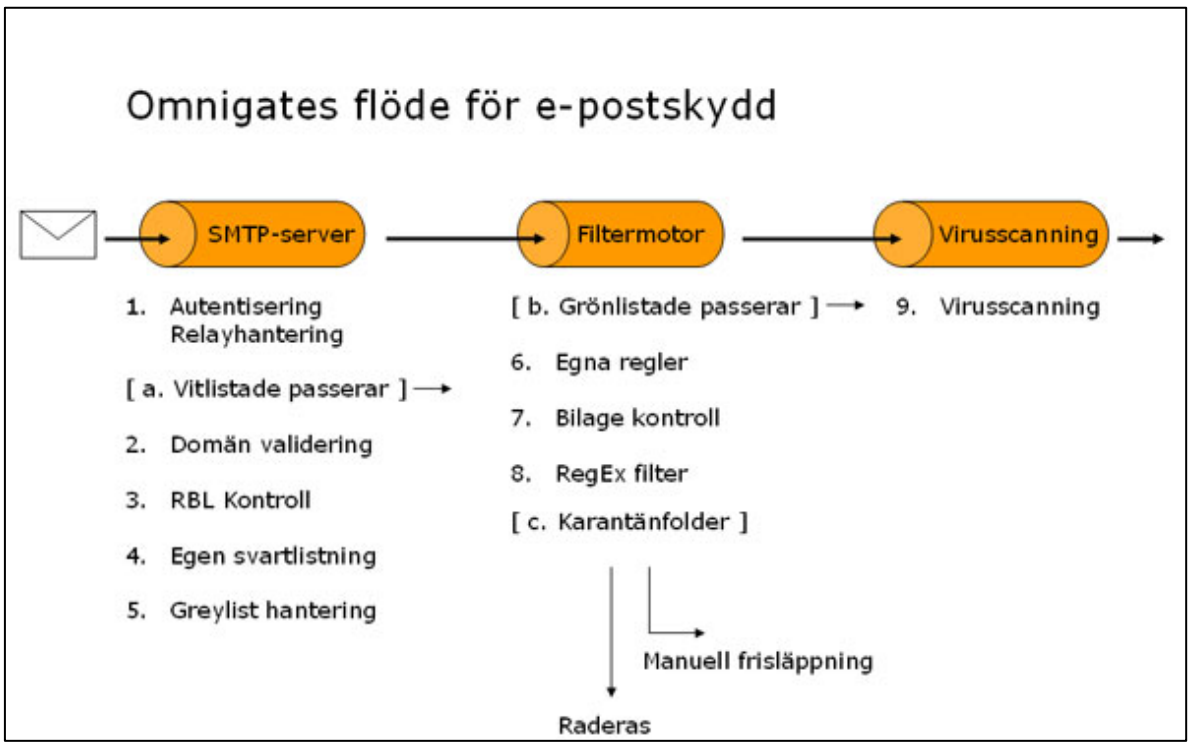
Datavirusskydd
Omnigate kan skydda företaget mot datavirus redan innan de når fram till användaren. Sökning efter virus sker på "gateway"-nivå. Både in- och utgående e-post söks igenom efter virus. Alla bifogade filer packas först upp och genomsöks sedan efter virus. Filerna kan vara packade (t ex winzip) i flera nivåer och kan vara kodade med både UUENCODE och MIME. Om ett virus hittas tas bifogningen bort eller repareras beroende på hur anti-virusprogrammet är konfigurerat. Flera anti-virus program kan köras samtidigt för maximal säkerhet. De vanligaste virusprogrammen, t ex McAfee, F-Prot och Symantec stöds av Omnigate och de inställningar som behövs är förinlagda.

Med Omnigate 7 levereras ClamWin antivirusprogram, som ett komplement till företagets övriga antivirusprogram. För maximalt skydd kan flera virusprogram från olika leverantörer användas parallellt med Omnigates egna filter, se ovan.

E-postövervakning och trafikrapporter
Med hjälp av Omnigate 7 kan företagets e-posttrafik övervakas och snabbt analyseras. Administratören ser vilka som tagit emot resp skickat meddelanden – en effektiv funktion för att t ex identifiera vem som drabbats av ett datavirus. Administratören kan också spåra olika typer av problem eller om någon bryter mot företagets e-postpolicy.



E-posttrafiken kan analyseras utifrån nedanstående sökbegrepp:
– Avsändare, tidsordning, namn, domän
– Mottagare, tidsordning, namn, domän
– Filnamn, tidsordning, filnamn och avsändare



De skyddssteg som ett meddelande passerar igenom Omnigate 7. Där Omnigate administratören kan välja vilka enskilda delar som skall vara aktiva beroende på företagets e-postpolicy. Administratören kan även ange om vissa e-postadresser, ip-adresser och domäner skall vitlistas resp grönlistas för att meddelanden från dessa skall passera igeonom utan kontroller.

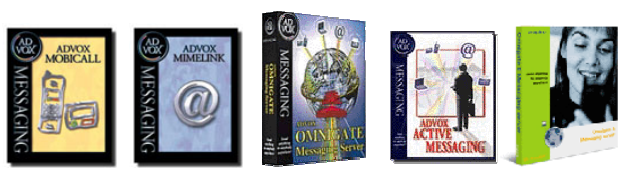
Advox produkter är grundade på erfarenhet

Advox AB är ett svenskt programvaruföretag, som startades hösten 1992.

Advox utvecklar produkter och lösningar för mobil meddelandekommunikation och säker e-post.

Advox var 1993 **först i världen** med att utveckla SMS-produkter, Advox Mobicall. 1994 en av de första att hantera den nya e-poststandarden MIME, Advox Mimelink, flera år före t ex Microsoft.

Advox produkter används idag av GSM-operatörer, Internetoperatörer och mobilportaler för deras inkomstgenererade tjänster**,** av kommuner, skolor, sjukhus och företag för deras verksamhetskritiska e-posthantering.



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

Mer än 6000 företag
Advox produkter används idag av mer än en en miljon användare och har sålts till mer än 6 000 företag i 20 länder världen runt. I Sverige säljs Advox produkter av auktoriserade återförsäljare över hela landet.

För mer information

Azenna Advox AB
Linjalvägen 6a
187 66 Täby

Telefon: 08-54490900
Fax: 08-7324972
E-post: info@advox.se
www.advox.se

Made in Sweden