

**EMAIL MESSAGING SERVICES AND EMAIL MESSAGING PROTOCOLS – AN
INTRODUCTION**

TABLE OF CONTENTS

INTRODUCTION	2
MAIL SERVERS	3
MAIL SERVER SOFTWARE	3
INTRODUCTION TO MICROSOFT EXCHANGE SERVER	4
INTRODUCTION TO IBM LOTUS DOMINO SERVER	5
INTRODUCTION TO NOVELL GROUPWISE	6
INTRODUCTION TO LINUX MAIL SERVERS	6
MAILING AND MESSAGING PROTOCOLS	7
POP3 AND SMTP	8
IMAP	9
MIME	9
LAN PROTOCOLS	10
PORTS	10
PACKETS	10
TRANSPORT – TCP/IP	11
PRACTICAL:	12
EMAIL SECURITY	15
TYPES OF EMAIL ATTACK	15
EMAIL SECURITY RISK MANAGEMENT:	17
EMAIL SECURITY POLICY DOCUMENTS	17
EMAIL SECURITY IMPLEMENTATION	18
GLOSSARY	23

INTRODUCTION

The apparently complex functionality of contemporary email clients such as Microsoft's Outlook, Lotus Notes, or even Linux's FetchMail belies the real simplicity of what actually goes on behind the scenes when sending or receiving email. Although the concept of electronic mailing transactions is, in itself, straightforward to grasp, the surrounding technologies and management strategies are varied and extensive and each of them can, and has, taken up book length studies on their own. As such, any attempt at a comprehensive survey here is impossible. This booklet is intended to offer an introductory grounding in the major issues concerning business email systems, the technologies they employ, and the surrounding issues of email security and email management.

Chris Boswell, 2008

MAIL SERVERS

Every company has to have systems in place to send and receive electronic mail for each of its email users. Just as network servers, file and print servers, FTP (File Transfer Protocol) servers and database servers are employed to handle specific requirements of users and groups of computer users within a company, so mail servers are used to handle electronic mailing requirements, to relay emails between senders and recipients and even to provide mechanisms for archiving mail. As with other servers, mail servers are there to provide a service to clients; i.e. end users.

It may be best to think of mail servers as “communication servers”, since they often provide more services to their clients than electronic mail, such as instant messaging, scheduling calendars, centralised business address books, online meetings, customisable databases and so forth.

MAIL SERVER SOFTWARE

Each proprietary vendor of operating systems and enterprise class servers, such as Linux, IBM, Microsoft and Novell, also tends to have its own mail server/s. However, you will encounter numerous and varied infrastructures out in the real business world: just because a company uses a Windows network server, does not necessarily mean they also use a Windows mail server, and the same goes for Novell Netware. IBM’s Lotus Domino Server (a mail server we will meet shortly) can run alongside a Windows, Novell or a Sun network server, for instance. Evening more confusing, it is also occasionally the case that the mail server used has a different vendor than the email client used, and that two or more different mail servers (either belonging to different vendors or different versions belonging to to the same vendor) may be running together (known as co-existence). It is worth keeping this in mind when asking about the technological infrastructure of prospective clients.

Note that for any decent-sized organisation, mail servers place a high demand upon network resources, since it is to be expected that a high volume of users will be logged on and active at any one time. Since this also represents a pretty continual

flow of data around and into and out of the network, effective backup and storage systems are also business critical for this type of server.

INTRODUCTION TO MICROSOFT EXCHANGE SERVER

Microsoft's Exchange Server is in many ways the protégé of Novell's GroupWise and the two share many similar features. Unlike other mail servers, however, Exchange must be run on a network server from the same vendor (i.e. Windows 2000 Server or Windows Server 2003). This is because it is reliant upon the Windows server administration tool Active Directory for its configuration. Active Directory is the tool used to administer users and groups on a network on every Windows enterprise class server since Windows 2000 Server.

While email accounts are created in Active Directory, administrative functions can be managed using the Exchange System Manager, which can also be used to access user inboxes, calendars and anything else stored on the Exchange server. There are obviously issues of privacy here. Outlook users, however, can also be given personal folders, which are stored either on the hard drive of their client pc or on personal space on a network drive. These offer the option for a degree of user privacy, since users can move (drag and drop) items from their public folders (stored in Active Directory) into their personal folders (stored in allocated user space as user.id files).

The email client of Microsoft Exchange Server is Microsoft Outlook, which offers services such as email, scheduling, calendar, discussion groups and so forth.

Using Exchange server has some administrative advantages, over and above the convenience of being able to create mail user accounts on the same administrative tool upon which network user and group accounts are created (Active Directory).¹ A

¹ Note that versions of Exchange prior to 5.5 could be set up and administered independent of Active Directory.

few automated housekeeping features, for instance, can help to cut down the data storage burden - expiration dates can be set for mail sent, and unread, received mail can be deleted from an inbox after a set period of time.

INTRODUCTION TO IBM LOTUS DOMINO SERVER

Just as Microsoft has a mail server (Exchange) and a mail client (Outlook), so does IBM's Lotus suite. The client is known as Lotus Notes and the server as Lotus Domino Server. The Lotus suite provides a similar group of services to its clients; the ability to send email, set up meetings, schedule appointments and access and administer Notes databases. There is also a global address book, a calendar and the facility to access newsgroups. Notes users also have personal files (these use the file extension .psd).

Although we haven't covered network protocols yet, it is worth saying here that Domino can support communications using a number of different network protocols, as well as the typical TCP/IP; including NetBeau, and IPX/SPX. This makes it a very flexible package, and is one of the reasons why Lotus is found in numerous large organisations, irrespective of technological infrastructure.

Domino server can be administrated using software with a graphical interface (GUI), known as the Domino Administrator. Or, it can be managed from the command line. The administrator software can be installed on any network client, so the administrator does not necessarily have to sit in front of the network server itself to perform his job.

The flexibility of Lotus is also evident in that the Domino server can also be used with a Microsoft Outlook client. This requires the purchase of a package with the unwieldy name, Lotus Domino Access for Microsoft Outlook. The advantage of this is that Domino server functionality can be leveraged within an organisation with only the most minimal changes to the working environment with which users are already familiar.

INTRODUCTION TO NOVELL GROUPWISE

GroupWise, similar to Exchange and Lotus, allows users to send email, provides an address folder and offers instant messaging with the GroupWise Messenger. GroupWise, like Netware (Novell's enterprise server), has the useful feature that it can be configured and administered remotely by anyone on the network with the right user-privileges using the NetWare server's Remote Manager or ConsoleOne. This means that GroupWise is even more flexible than Domino Administrator, since it can be accessed by any client on the network without first having to install client software.

GroupWise runs on a range of enterprise network servers, including the most popular Novell, Linux and Microsoft products such as Linux SUSE enterprise server, Netware, Novell Open Enterprise Server, Windows 2000 Server and Windows Server 2003.

Note that running GroupWise on a network server other than Novell Netware requires the separate installation of Novell's eDirectory and ConsoleOne on the server as well as GroupWise itself.

Note also that the GroupWise mail server will only work with the GroupWise email client.

INTRODUCTION TO LINUX MAIL SERVERS

There are numerous Linux mail servers, as you would expect from an open-source organisation such as this. Among the better known ones are SendMail (client OpenMail) and Postfix. On a Linux server such as SUSE, you can even switch between these using the Mail Transport Agent Switcher. Linux systems can also be set up to run POP3 servers, dedicated to only holding mail until clients request to download it (one often shipped with Linux distributions is the University of Washington POP server, another is Qpopper).

Like their counterparts, Linux mail servers also boast many email security features. A few notable features on Postfix are given here:

PostFix (originally the IBM Secure Mailer) can be configured to manage Unsolicited Commercial Mail (UCM). It also allows the setting of criteria for rejecting, rejecting with reply, deleting mail or providing warnings about suspected Spam. These criteria can be set for both the header and the body of the mail. See also the Mail Abuse Prevention System which uses databases of electronic mail addresses known to be used by email abuses in order to block them.

MAILING AND MESSAGING PROTOCOLS

Protocols are the agreed and standardised methods for sending data between computers. Basically, this means that information sent by one computer also carries information within the protocol that the recipient computer can use in order to determine how this information should be interpreted. The protocol carries some of the following information:

- The type of error checking to use
- The method of data decompression
- How the sending computer will indicate that it has finished sending packets of information
- How the receiving computer will indicate to the sending computer that it has finished receiving the packets of data
- What sort of media files are contained within the data
- The ASCII (American Standard Code for Information Interchange) code being used. ASCII (pronounced ask-ee) is a code for representing textual characters numerically. Knowing which ASCII code is being used is crucial to the interpretation of how data should be displayed in a human-readable format.

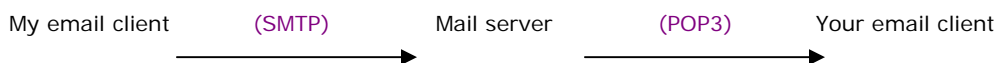
In brief: We use protocols since these provide universal means of deciphering and, if necessary, debugging the information contained within an email message.

POP3 AND SMTP

A common misunderstanding is that email users (email clients) receive electronic mail directly from other email clients. However, as we have seen, the mail must first travel through a mail server or servers, before it reaches its destination. On its journey mail may also travel through, and be forwarded, on by routers, but discussion of these, and network topology in general, falls outside the scope of our interest here. Now, let's take a simplified look at how email travels between senders and recipients.

Email clients often receive mail from their mail server through a TCP/IP protocol known as POP3 (Post Office Protocol version 3). In turn when an email is sent out, it is first sent to a mail server in a TCP/IP protocol known as SMTP (Simple Mail Transfer Protocol).

So electronic mail travels in more-or-less the following way:

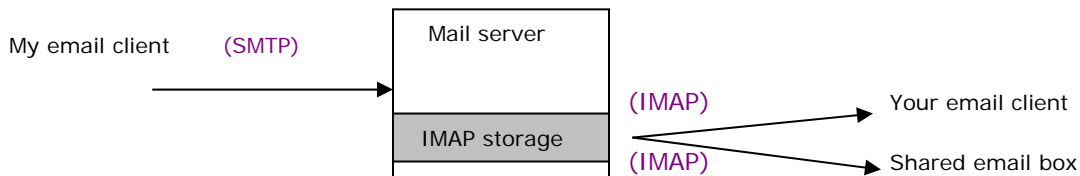


The rationale for using these two different protocols for sending and receiving mail is quite simple. The goal of SMTP is to get the message to a mail server, and it will often try for several days before giving up. This is reliable since mail servers, which often support many thousands of clients, need to have as close to 100% uptime as possible. Mail clients on the other hand might not be open and available to receive electronic mail for weeks at a time. It is impractical to repeatedly try to deliver electronic mail to email clients in this situation. Hence, mail servers receive mail

using the SMTP protocol and store the mail until it receives a request from the client to download it. One other protocol that can be used to store and download mail, other than POP3, is IMAP.

IMAP

Mail servers store received electronic mail ready for when it is requested by a client in one further protocol; IMAP (Internet Message Access Protocol). It is important to note that when mail is downloaded in the IMAP protocol, the mail is still retained in IMAP storage on the mail server. When mail is downloaded from POP3 storage, however, the mail is not retained by the mail server. Thus IMAP has obvious advantages when it comes to storing and archiving all mail in one centralised location, and is useful for email groups where the same mail needs to be downloaded and viewed by more than one person.



MIME

SMTP, POP3 and IMAP only support the sending and receiving of plain text via email, i.e. letters, numbers and other characters without any rich text features such as bold, italic and fonts. Electronic mail as we know it today consists of much more than just plain text and therefore we need a means of sending mails which support the display of rich text, images, audio and video files, e.t.c.

Support for these multimedia file formats (e.g. .MPEG, .GIF, .JPG) is provided by MIME (Multi-purpose Internet Mail Extensions). Each type of data is assigned an RFC MIME type, and this information travels in the header section of the transported data packets, thereby allowing the correct interpretation of the packet's content (the

body) before the content is opened. Much more could be said about the information provided in the header aside from MIME, but this is presently beyond our scope.

LAN PROTOCOLS

Another way of sending email is through propriety protocols – i.e. ones used within a business that may not be interpretable outside of the company’s network or domain. These are known sometimes as LAN (Local Area Network) Protocols. These do not really concern us, since we are involved chiefly in understanding how mail travels into and out of a business network infrastructure. It is worth knowing that these exist, however.

PORTS

Now we have come this far, we need to think about where on client computers and servers these protocols travel into and out of. These points of transit are known as ports. Each method of sending information between computers involves travelling from a port on one computer to a port on another through a LAN (Local Area Network) and/or via the internet. So, for instance, HTTP protocol, the one we use for viewing hypertext on the Internet, usually travels through port 80, SMTP through port 25, POP3 through port 110 and so forth. Where electronic mail is concerned, it is a useful analogy to think of the protocol as a ship, the content of the message as its cargo, and the ports as where this cargo is exported from and imported to.

PACKETS

A packet is the basic unit of data transmission across a network. Any data transmitted over a LAN or the Internet is broken down into separate packets which are shipped out and then reassembled at the destination. These are known as datagrams or IP datagrams. Each datagram carries the unique address of both the sending and receiving computer and does not necessarily pass from just one computer to a mail server to the recipient computer. The datagrams may also pass

through routers along the way, which forward them onwards towards their destination.

TRANSPORT – TCP/IP

Extending the analogy, TCP/IP might be thought of as the ship's engine, that drives the protocol (the ship) and the message (its cargo) from one port to the next, in other words it is the transport mechanism. TCP/IP is, in fact, the standard method by which computers communicate with one another, and it might actually be better thought of as a suite of protocols, some of which we have already encountered. TCP/IP is the foundation protocol, without none of the other protocols could be used.

Let's break TCP/IP down into its component parts:

-- *TCP* (Transport Control Protocol) is the mechanism that sends data in the form of bits and bytes (datagrams) from one computer to another (whether server or client).

-- *IP* (Internet Protocol) addresses are the unique addresses that allow computers anywhere in the world to identify and communicate with one another. They consist of a 32-bit (4 byte) number which is divided into four parts separated by full-points; e.g. 167.205.8.5 (each number is between 0 and 255). Often these numbers are associated with specific domains such as microsoft.com, cnn.com e.t.c. In order to resolve a numeric IP address into a literal domain name made up of roman numerals something called a DNS (Domain Name Server or Domain Name System) is used. By translating IP addresses into domain names and back again, DNS allows computers to communicate in the most efficient way possible, while allowing human beings to interface with this information in the way most familiar to them.

So when put together TCP/IP, is both the transport mechanism used to transmit data between computers (TCP) and the carrier of the information that allows the computers to identify one another and communicate (IP). When two-way communication between computers occurs through TCP/IP they are said to be in a state known as full-duplex. When communication is only in one direction, this is known as half-duplex.

Whenever we communicate with another computer on the internet, such as via email, we open a port. There are many more protocols than we are able to discuss here, and as you probably guessed, there are, therefore, many ports. It is good news that computers are able to communicate with the outside world in so many ways; however this plus has its downside in that each open port is a point of vulnerability through which nasties such as viruses and worms might gain access to a computer or server, and even the rest of the network, if proper measures are not put in place to prevent their entry.

PRACTICAL:

Now let's look at what's happening behind the scenes. We are going to find out which ports are open on our computer, what their status is, and even which protocol is being used.

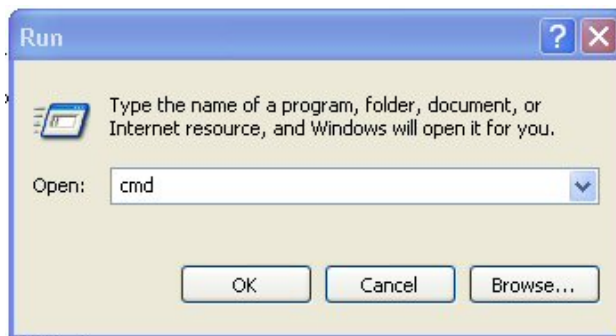
First we will open our email client so that port 25 will start listening for outgoing SMTP requests.

Now try the following. Go to

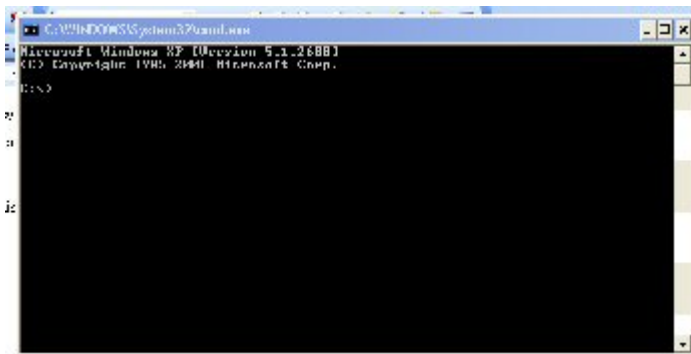
Start > Run



Type **CMD** into the edit box that appears and click **OK**.



In the command line window that opens type the following: `NETSTAT -ANO`



You should now see something like the following:

```

c:\WINDOWS\system32\cmd.exe

Proto Local Address Foreign Address State PID
TCP 0.0.0.0:25 0.0.0.0:0 LISTENING 1940
TCP 0.0.0.0:80 0.0.0.0:0 LISTENING 1828
TCP 0.0.0.0:88 0.0.0.0:0 LISTENING 1940
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING 1096
TCP 0.0.0.0:211 0.0.0.0:0 LISTENING 3668
TCP 0.0.0.0:443 0.0.0.0:0 LISTENING 1940
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING 4
TCP 0.0.0.0:1025 0.0.0.0:0 LISTENING 1868
TCP 0.0.0.0:1026 0.0.0.0:0 LISTENING 1868
TCP 0.0.0.0:1027 0.0.0.0:0 LISTENING 1940
TCP 0.0.0.0:3050 0.0.0.0:0 LISTENING 3364
TCP 0.0.0.0:3306 0.0.0.0:0 LISTENING 296
TCP 127.0.0.1:1028 0.0.0.0:0 LISTENING 3396
TCP 127.0.0.1:1116 127.0.0.1:1117 ESTABLISHED 4644
TCP 127.0.0.1:1117 127.0.0.1:1116 ESTABLISHED 4644
TCP 192.168.0.3:139 0.0.0.0:0 LISTENING 4
TCP 192.168.0.3:1100 212.58.227.11:554 ESTABLISHED 4608
UDP 0.0.0.0:445 *: * 4
UDP 0.0.0.0:500 *: * 884
UDP 0.0.0.0:1030 *: * 1200
UDP 0.0.0.0:1059 *: * 1200
UDP 0.0.0.0:3456 *: * 1940
UDP 0.0.0.0:4500 *: * 884

```

On the first line we can see that a port is actively listening for requests to initiate a TCP conversation – since there is no such request presently both the client IP address and the foreign IP address are empty. We can see that the IP address is made up of four numbers separated by full points, and that the port number is given after the IP address separated by a colon. Our client computer is listening on port 25, the port associated with SMTP.

The column following the Foreign Address shows the port's status - listening, established, or closed (close_wait).

In the final column is the PID (Process IDentification) number, the temporary identification number assigned to the particular process that is using the port. If you want to find out which processes are associated with which ports, and what

particular security risks apply to specific ports, a comprehensive list is provided at <http://www.emsisoft.com/en/kb/portlist/Default.aspx>.

EMAIL SECURITY

To extend our earlier maritime analogy even further, when a ship arrives at a port with imported cargo, it must carry documentation to prove that the cargo is what it is supposed to be and not contraband, and that there are no nasty bugs or infectious creatures lurking within it. For us, this is where email security comes into play. Just as a vigilant customs official will look out for certain discrepancies and clues within the documentation that something is wrong, so will properly configured mail security suites examine what has been received and try to tell if there is anything out of place.

It should be mentioned here that email represents a potentially very big hole in network security. Electronic mail is a high volume instance of opening up a port (port 25, the SMTP port, 110 the POP3 port and 143 the IMAP port) to the outside world. I.e. it is necessary that any and every mail server out there can potentially connect to the mail server used on the network, including those pumping out spam and carrying virus payloads.

TYPES OF EMAIL ATTACK

To give some idea of just how pervasive viruses really are; it has been estimated that a home user with Microsoft XP will be attacked within the first 18 minutes of connecting directly to the internet with no firewall or router as protection. For some more statistics have a look at <http://www.securitystats.com/virusstats.html> and <http://answers.google.com/answers/threadview?id=304308>.

Attacks can come in many forms. The following are some of them, followed by brief definitions:

- Trojan horses: software applications that appear benign but, when launched, trigger behind-the-scenes activities on a computer; e.g. using an email address book to send Spam emails or replications of itself to your contacts or repeatedly shutting down the pc.
- Worms: programs that spread themselves from computer to computer on a network.
- Zero-day attacks: These are attacks that exploit weaknesses not yet identified by the anti-virus community. On the day the attack occurs there is no solution or patch available to seal up the security vulnerability.
- Zombie Machines: computers that have been infiltrated by software packages designed to simultaneously attack a single target such as a web site or mail server by overburdening them with an avalanche of coterminous requests. This is known as a Distributed Denial of Service Attack.

(see, for instance, <http://news.bbc.co.uk/1/hi/technology/3123537.stm>).

- Distributed Denial of Service (DDoS) attack: see above
- Spyware: programs that collect and send data from an infected computer to be used by the hacker (or more precisely "cracker"), for purposes such as fraud, re-selling or unsolicited marketing.
- Adware: any software application that uses advertising banners and popups. Adware is pretty harmless, but its presence upon a client computer on a business network is a good indication that improper usage has taken place and/or that a security vulnerability exists.
- Phishing: This is an identity-theft scam, often whereby an official-looking email makes an urgent request for personal information such as bank account or credit card details.

- Spam: Unsolicited email often sent out by bulk mailers to thousands of individuals at once. These might be relatively benign, but resource consuming, attempts to get the recipient to buy or subscribe to something, to send on chain mail e.t.c. They might also harbour more malignant designs, such as misleading recipients into downloading viruses or spyware through websites linked to from within the email. When any volume of Spam gets through to clients they can add heavily to email administration time and pose a significant cost to businesses.

EMAIL SECURITY RISK MANAGEMENT:

EMAIL SECURITY POLICY DOCUMENTS

Every organisation that uses a mail server should have well-documented email policies, including:

- Security Policies
- Archiving and retention policies – these should stipulate how long emails are to be archived, and what is to be archived i.e. type of file and type of information
- Email usage policies - these should outline responsible email usage to employees regarding such matters as personal e-mails, proliferation of chain letters, legals, abuse and so forth This should include the raising of user awareness about potential sources of viruses and other risks
- Email monitoring/scanning policies – here strategies should be implemented to monitor whether sensitive information is being sent outside the organisation
- Virus scanning policies
- Procedure for reporting abuse

- Company email disclaimer – disclaimers should be carefully considered to avoiding as much liability for emails sent on behalf of the company by employees. Where necessary these should be department or group specific and strategies should also be put in place to ensure that disclaimers are implemented organisation wide.

Where this is applicable, similar policies should also be applied to instant messaging.

Note that whether or not a prospective client has such policies in place, and is able to tell you about them, should provide a useful barometer of just how competent they are at managing their email security in-house.

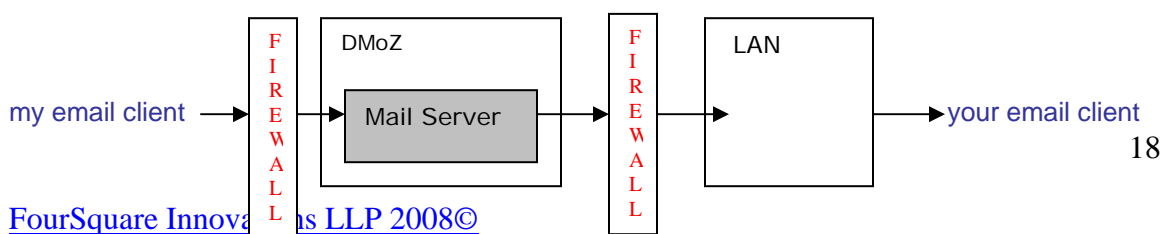
EMAIL SECURITY IMPLEMENTATION

INBOUND PROTECTION

Mail server security

DMZ (Demilitarised Zone): We have already mentioned the problem of mail servers being a hot spot for network security owing to the necessity of allowing open access to external mail servers. Placing the mail server on a DMZ is one solution to this problem. It is a network external to the main network of the company which allows external untrusted hosts to have access to it. If the mail server on the DMZ is attacked, in theory, there should be no impact upon the internal network.

This can be an expensive solution, especially since a firewall is required to sit both in front of the DMZ and between the DMZ network and the main LAN.



Spam filtering: Spam filtering can consist of features including the following:

- Keyword filtering
- Word score – count words associated with known unsolicited email
- Textual analysis – look for word patterns and text-strings associated with unsolicited email, even when spammers attempt to disguise these by inserting special characters or numbers (e.g. Sh!t, v1ag*ra, s3x e.t.c.)
- Lexical analysis – look for words associated with known unsolicited email
- Attachment control - Prevent clients opening mail with attachments of certain file types associated either with large files (e.g. .tiff, .mpeg) or file extensions associated with carry virus threats (e.g. .exe, .zip, .rar)
- Image control (prevent emails downloading external images)
- Limit file sizes of emails received
- Block addresses from which Spam has been previously received
- Block email matching a record from a database of known spammers (as used by Linux Postfix's Mail Abuse Prevention System, discussed above)
- Provide statistical probability that mail is spam based on the above tests and act accordingly –e.g. score of 15 (warn client), 30 (quarantine mail and reply to obtain authentication from sender), 40+ (block sender address)

It is also important to check whether the mail was sent from the domain from which it purports to originate. Some spammers try to cover their tracks by disguising their emails to look like they originated from bogus domains or well-known and trusted domains, including the domain of the recipient – this is known as email spoofing.

[Antivirus security](#)

Antivirus software scans computers and indeed whole networks for known viruses, trojans, worms, spyware and so forth. It is crucial that antivirus software is kept up-to-date so that the network is protected from the most recent manifestations of known viruses and the appearance of new viruses. Crackers often deliberately try to confuse anti-virus software by doing things like morphing – i.e. when two known viruses are combined together to create a new one.

[Firewall security](#)

There are too many different firewall security solutions and firewall vendors to discuss them in any depth here. However, here are a few of the firewall defense strategies you may encounter:

- Protocol rules: a set of rules can be defined preventing protocols not needed by the network to be disabled, or the direction in which these protocols travel can be restricted. This means that the ports used by these protocols can be disabled, thereby decreasing the points of entry available to anyone trying to attack the network. These rules can be set on a firewall or internet security server such as Microsoft's Internet Security and Acceleration Server.
- Block access to intranet server outside of the trusted domain.
- Traffic identification: Examine datagrams in order to identify whether a TCP/IP conversation was initiated locally from inside the domain or externally from outside the domain, and potentially block datagrams initiated from an external address.
- Stateful inspection: Determine whether packets are part of an existing valid TCP/IP conversation and take action accordingly.

[Network Server Security Policies](#)

As well as protecting the server as a point of entry, it is also possible to take action to protect individual clients on the network when configuring a network server. You might, for instance, want to set up a scenario where your client computers can only receive HTTP, FTP and IMAP and only send SMTP and FTP, but not send or receive through the VPN (virtual Private Network) protocol. Here it may be appropriate for a server to accept all these protocols, maybe to accommodate laptop users working offsite who need to establish a VPN connection to mail, application and file servers.

[Application Proxies](#)

Application Proxies sit on an external firewall and handle protocols in the same way as an internal server. The advantage of this is that they can be configured to only let through certain protocols, and extremely rigid validation rules can be employed before letting datagrams through. Only protocol elements that pass these tests will reach the internal server and be passed on to users.

One disadvantage of this method is that versions of Application Proxies need updating regularly in order to work properly and keep up-to-date with new technologies.

Perhaps the best-known Application Proxy is Microsoft's Winsock (short for Windows Socket).

[Managed solutions](#)

One other email security option is a managed solution. These extend the principle of Dmoz and Application proxies and allow the handling of all security issues off site, external to the LAN. In this instance, an external service provider is responsible for the management of all email transactions before they reach the internal mail server, and ensuring their integrity. It is one of these, BlackSpider, for which we will be responsible and we will discuss this vendor in more detail elsewhere. Ideally, managed solutions should not be regarded as a pure alternative to implementing security policies locally, since organisations have less than total control of externally

managed services, they should always make sure that they take measures to protect themselves at source as well.

Note: Enterprise-size organisations may employ any number of network security measures in all sorts of combinations, so it is useful to make a big effort to find out exactly which measures they have in place.

Honeypots

Honeypots are networks set up to deliberately attract crackers, so that their actions can be observed and analysed, often with the objective of designing Intrusion Prevention Systems, which are able to stay ahead of developments in hacking capabilities and strategies.

Intrusion Prevention Systems

IPSs (Intrusion Prevention Systems) are intuitive, behavior-based systems which attempt to prevent threats such as Zero-Day Attacks by identifying crackers' behavior patterns or patterns that would indicate the presence of viruses on the network rather than seeking and destroying known viruses in the way that traditional anti-virus software does. This means that attack can potentially be prevented before anti-virus vendors provide fixes and identify the signature of the virus and provide their software users with the means of identifying the new virus. One of these IPSs is BlackSpider's heuristic Intelligent Threat Prevention system.

OUTBOUND PROTECTION (EMAIL ONLY)

- Use encrypted email for confidential emails
- Use digital signing to verify the authenticity of the sender (avoid releasing confidential information to spoof emailers)
- Limit file sizes of outbound emails
- Use a legal disclaimer

GLOSSARY

- ASCII: American Standard Code for Information Interchange
- DMZ: Demilitarised Zone
- DNS: Domain Name Server or Domain Name System
- IETF: Internet Engineering Taskforce
- FTP: File Transfer Protocol
- GUI: Graphical User Interface
- HTTP: Hypertext Transfer Protocol
- IMAP: Internet Message Access Protocol
- IPS: Intrusion Prevention System
- LAN: Local Area Network
- MIME: Multi-purpose Internet Mail Extensions
- PID: Process IDentification
- POP3: Post Office Protocol version 3
- RFC: Request for Comments: A document outlining the specifications of a proposed technology. Once reviewed and adopted, RFC numbers are retained for the new standard. RFC-822, for instance is the Internet mail-format standard
- SMTP: Simple Mail Transfer Protocol
- SSL - Secure Sockets Layer
- SOAP: Simple Object Access Protocol. This is the protocol often used to send SMS text messages
- TCP/IP: Transport Control Protocol/Internet Protocol
- VPN: Virtual Private Network
- WAN: Wide Area Network

You are free to re-publish this PDF article online so long as the attribution and links remain intact.

Other foursquare innovations articles:

1. [Internet marketing tips - onsite SEO](#) (downloadable pdf opens in a new Window)
2. [Web design - case study](#)
3. [Google marketing tips](#)
4. [SEO/search engine marketing: an integrated approach](#) (multimedia presentation opens in a new window)
5. [How to keep computers out of landfill](#)
6. [Green computing tips](#)
7. [How enterprises can save money on software licensing](#)
8. [How to choose a web designer](#)
9. [How to choose or find a domain name](#)
10. [Intrusion Prevention Systems \(IPSs\) - An introduction](#)