Interested in learning more about security?

SANS Institute InfoSec Reading Room

Securely Connecting Your Email System To the Internet - A Primer

For many, it's hard to imagine life before electronic mail. Billions of SMTP messages a day zoom through cyberspace between friends, businesses, and people trying to make a quick buck. The 'S' in SMTP stands for 'simple' - that's one of the reasons it has become the standard protocol for message transfer. Unfortunately, with that simplicity comes poor security. The lack of built in authentication and transmission in clear text are two major examples of the problems you face when using SMTP email. This paper examines th...

Securely Connecting Your Email System To the Internet – A Primer

Stephen Cottrell
GSEC Assignment v1.4b, Option 1

Introduction

For many, it's hard to imagine life before electronic mail. Billions of SMTP messages a day zoom through cyberspace between friends, businesses, and people trying to make a quick buck. The 'S' in SMTP stands for 'simple' – that's one of the reasons it has become the standard protocol for message transfer. Unfortunately, with that simplicity comes poor security. The lack of built in authentication and transmission in clear text are two major examples of the problems you face when using SMTP email.

This paper examines the basics that need to be considered when building a secure email connection to the Internet using an SMTP gateway. As with many security topics, hard and fast answers are not always provided – many of the decisions you make are based on the level of risk you are prepared to accept, and on the amount of money you are willing to spend. However, making a few informed decisions early on can help in mitigating many security issues such as viruses, spam, spoofing and intrusion. Confidentiality, integrity, and availability of your email system are addressed through discussion of policy, available technologies, and architecture.

Where to start?

As boring as it sounds, it has been my experience that the most secure and well functioning systems are those that are built on a foundation of solid, enforceable (and enforced) policies. Without a doubt, the first thing that needs to be determined for your email system is the policies that you will live by. This may be the most difficult part of the design, especially since it is often done after the fact once the bad habits have set in. It is these policy decisions that will dictate how the rest of your design will occur. Unfortunately, it is unlikely that there will be unanimous agreement on many of the policies. What will work great for the Sales department may be the opposite for Research. Also, when you are making policies you have to be able and prepared to enforce them, otherwise they are useless. Clearswift Ltd., a provider of electronic communication security software, identifies three key steps required to implement policy:

1. Establish the policies – this must be a cooperative process with contribution, and most importantly, buy-in from all levels of management, security, and information technology staff.
2. Educate your users – this is the process of explaining what the policies are, the reasons behind them, the ramifications of violating policy and obtaining acknowledgment and consent that they will be adhered to. The policy document should always be easily found, current, and accessible, such as on a corporate intranet, or as a regularly distributed, dated

document. Accepting the policy should be part of the orientation package for all new employees.

3. Enforcement – there must be a way to make sure that your policies are being honored. Some policies can be put in place by making certain restricting configuration settings to your email servers, but often other technologies are required to monitor for breaches. Policy violations always need to be acted on.[i]

When establishing your polices, some of the questions that you will need to ask and other points to ponder include:

Is email considered 'business-critical'?
This will be one of the first questions you will want to have answered. If email is determined to be critical, all sorts of related design issues will be introduced (and of course the price tag can rise dramatically). These issues may include backups, redundant hardware and connections (both internal and external), hot site availability etc. Be careful. Some levels of management may see email only as a convenience, however more and more businesses are integrating email into their processes each day. The question needs to be asked, "If email goes down for any length of time (an hour, 4 hours, a day…), could money in some form (e.g. revenue, reputation) be lost?"

Will you allow email to be used for personal use?
This is a tough one. There are many statistics that indicate productivity and liability losses associated with inappropriate email and Internet use is bad and getting worse. For example, a Computer Security Institute survey showed an average organization's loss jumped over 35% between 2001 and 2002 to $536,000.[ii] While the initial reaction may be "Yikes! Business use ONLY," it would be unrealistic to enforce - who in the world has never sent a personal email through their work systems? However, it may be possible to put some restrictions on the type of content and attachments that personal emails contain. The wording of a policy may want to allow for *reasonable* personal use.

What kind of attachments can be sent/received?
The answer to this question will be closely related to the preceding question. If you are allowing personal use, then will you allow MP3 files to be sent? How about AVI's? Screensavers? Executables? The stricter this policy is, the more you will be automatically protected from things such as lost productivity (if you receive a 2 minute AVI file, you have to watch it and forward it to your friends, don't you?), and many types of viruses and trojans. Obviously some attachments will be required (usually spreadsheets, text documents etc.), and it will be the policy creation team's job to figure out where to draw the line. A list of 37 potentially dangerous file types as identified by Microsoft can be found at http://office.microsoft.com/Assistance/2000/Out2ksecFAQ.aspx.

How large can messages be?

While we're talking about attachments, you will also need to determine (if you're going to allow them) how big they can be. It is possible for email transports to check the size of a message before sending or receiving it. You will need to determine the impact of sending and receiving large files. If you allow large files, you may be opening yourself up for a couple of different types of denial of service attacks (not always the malicious type). The time it takes to receive and process a ten megabyte message will take resources away from sending and receiving hundreds of smaller text-only messages, which are typically less than ten kilobytes. If someone attempts to send many large messages, the problem compounds. Depending on how large people's mailboxes are allowed to be, it could be easy to fill them up, causing other email to be rejected.

Do you require email or their attachments to be encrypted?
This is another one of those tricky questions. It might seem obvious that you would want to maintain confidentiality of email by encrypting it. However many businesses require all email to be audited for legal compliance, which would require it to be in readable format. Also, if an attachment has been encrypted, it cannot be scanned for viruses. There are technological options that solve some of these issues and this is discussed in further detail in the 'Technology' section.

Do messages need to be archived? If so, for how long?
Again, this can be a legal requirement. Archiving for seven years or more[iii] is not uncommon. Will you use off-site storage?

Do you require legal disclaimers to be on all outbound email?
This question deals with more legal protection that should definitely be considered. Lawyers should be consulted for adequate wording of any disclaimers, should you decide this is required.

Will you allow auto-forwarding of email outside of your organization?
Many people like to forward their email to other accounts, especially if they are on vacation, or have mobile devices that have a separate account. There are certain ramifications with allowing this. Since it is widely accepted that Internet email is inherently insecure, such automatic distribution is dangerous. Some messages are confidential, sent for internal use only, which if exposed outside of the organization would be damaging. There is also the possibility of another type of denial of service. If the account that messages are being forwarded to fills up and starts bouncing the messages back to the originating account, a loop will be created filling up the original mailbox and wasting considerable bandwidth and other resources in the process.

Can mailboxes be shared?
Ideally, each person should have their own mailbox that only they can access and therefore be accountable for all messages that are sent from it. In some cases, such as a departmental mailbox, several people may require simultaneous access.

How large can mailboxes be?
Ask most people if they think their mailbox is big enough, and I can almost guarantee you the answer will always be "No". People love saving their email, and for good reason. It is very convenient to go back and find discussions or documents from years ago that you were involved with. Many email systems offer fantastic searching and sorting functions. However, large mailboxes also mean large storage requirements. Large storage requirements mean extended backup and restore times.[iv] A balance needs to be struck between convenience and availability.

What will you do with spam?
Spam - the scourge of the email world. What is spam? Like its pseudo-meat namesake, "Nobody wants it or ever asks for it." Webopedia further defines spam as "Electronic junk mail or junk newsgroup postings."[v] This is another one of those problems that is bad and is getting worse. MessageLabs reports that a staggering 15% of email is spam.[vi] However, the same report goes on to say that the root of the problem is determining what is and what isn't spam. Needless to say, you will want to consider if you are going to deal with spam on an enterprise level. There are many technologies available that offer to come to your rescue. Some of these will be discussed later.
You will also need to make sure that you have a policy forbidding spam originating from your users within your network. Consent should be obtained from recipients before including them on a distribution list and they should always be given an easy way to remove themselves. Mass emailings should be carefully controlled. Being declared a spammer could be disastrous for your organization, both in terms of email service and reputation. Again, more on this topic later.

How will viruses be handled?
It goes without saying that you want to stop any viruses from entering your email system. Most of the latest virus outbreaks (Klez, SoBig, Sircam, Lirva, Nimda) have used email as one of their transport vectors.[vii] It only makes sense to scan for viruses at your front door – your gateway servers. This will be discussed later. However, you will also need to consider your notifications (if any). Will you notify the sender that they sent a virus, and/or will you notify the intended recipient that someone tried sending them one? (You would probably only want to do that for internal recipients…) Will you attempt to clean the virus and send it on its way, or simply quarantine/delete the entire message? On the same topic, you should also consider how you handle any virus outbreak that does occur within your organization. Who is responsible for issuing alerts? When and how will an alert be issued? Who will do the clean up?

Access to web-based email providers and instant messaging
The use of web-based email providers such as Hotmail, Yahoo!Mail and countless others is synonymous to a backdoor to many of the measures you may choose to put in place to help enforce your policies. If you have a sophisticated

gateway scanner that checks your outbound company email for sensitive documents, and blocks inbound email containing pornography, MP3s and viruses, but you allow unrestricted port 80 web-surfing (and therefore web-based email), there's a very good chance that all your efforts are being thwarted. On a related note, policies regarding instant messaging (ICQ, AIM etc.) should also be considered. It is difficult (from a technological point of view) to totally block all forms of instant messaging and web-based mail if you allow port 80 access to the Internet due to the fact that there are hundreds (if not thousands) of sites offering those services.

Remote access to email

Because more people are working from remote locations, demand for remote access to email is growing.[viii] Traditional dial-up access is gradually being replaced by VPN access and web-enabled email. Mobile devices like Research In Motion's BlackBerry are popular. These technologies each have their own associated costs and risks (discussed later). If this is a requirement, a policy will be needed to determine to outline who can have access and how the access will be achieved.

The Technology

In the past few years, thanks to some infamous virus outbreaks and high profile legal battles, the offering of email security software has flourished. They range in functionality from virus scanning to content scanning to encryption to spam blocking to archiving, and all the possible combinations therein.

Content Scanning

A content scanner's most basic purpose is to parse messages and documents for words and/or phrases and/or attachments that it has been configured to search for. This functionality can be used for detection of spam, profanity, confidential information, malicious scripts – basically anything you want to look for. Of course, as with other security detection products, when searching for words or phrases there is a fine line between catching too many false positives and missing too many bad messages. Again, defense in depth is critical. Do not rely totally on scanning for attachment types or file names or keywords to protect you. Have strict policies and obviously run antivirus everywhere.

In their desperate attempts to get questionable attachments through the system, some people will try tricks like:

- Renaming a file (e.g. Shania.mp3 becomes budget.doc), or
- Naming a file so that it appears safe, taking advantage of GUIs that have been configured to hide the real extension (e.g. happy.doc is really happy.doc.exe), or
- Compressing the file with a utility such as pkzip (e.g. so naughty.jpg becomes nice.zip).

A good content scanner will ignore the file extension when determining the file type, and actually examine the file headers (the first bytes of the file). The better scanners are capable of opening many layers of containers (e.g. a document

inside a zip inside a zip inside a zip etc.). MAILsweeper (one of Clearswift's products), which is a combination content scanner, email gateway, and facilitator for virus scanning, is capable of recursively disassembling up to 50 layers of embedded containers, as long as they aren't encrypted.

Anti-virus

If there's one thing that gets an email administrator shaking in her boots (especially a Microsoft Exchange administrator), it's a virus outbreak. Fortunately, there is a lot of anti-virus help out there, and if there's one thing you can't have too much of, it's anti-virus protection. Using a 'defense in depth' strategy, it should be installed at every step of the email path: your gateway, your mailbox server, and your desktop. If possible, use different anti-virus vendors at the different levels. The major vendors offer complete enterprise protection for the major email platforms (like MS Exchange and Lotus Notes) such as Network Associate's WebShield (gateway), Groupshield (mailbox) and VirusScan (desktop) or Symantec's more simply named 'Antivirus' product line.[ix]

Encryption

Many excellent Reading Room papers are available on the topic of secure transmission of email by encryption. It is far from a simple topic and requires considerable resources and commitment to implement. Some solutions may require a public key infrastructure (PKI) to be in place. Some offer point-to-point encryption, to allow secure transmission between two pre-configured sites over the Internet (the messages get encrypted and decrypted at the gateways). As pointed out earlier, one of the problems with encrypting a message is the inability for it to be scanned for viruses and inappropriate content. The MAILsweeper product offers a clever way around this, using its SECRETsweeper[x] plug-in. The general idea is that all encrypted messages must be cc:'d to SECRETsweeper, who will hold the message in escrow, decrypt its copy of the message, scan it and then release/deliver the escrowed message if has been determined to be clean. Currently SECRETsweeper only supports S/MIME.

Spam

There are a number of ways to battle the war against spam. Some have to do with stopping it from even reaching your systems, and others catch it and dispose it after being received. Ideally, you will use a combination of both methods (good old defense in depth). To stop the problem before it even gets in, there are a couple of things you can try. One is the 'reverse lookup'. This method does a reverse DNS lookup on the source IP address of the SMTP conversation and compares it with the sender's domain name. If these two don't match, the conversation is discontinued. This is not a very effective means of prevention, not because it doesn't stop spam, but because it stops a lot of legitimate email as well. Many companies host multiple domain names, however a reverse lookup of an IP can only return a single domain name. All of the other domains that they host will appear invalid.

Another method is by maintaining your own list of spam-sending IP's and domains by manually entering them each time you receive spam, and configuring your gateway to reject any further mail coming from those sources. This can be a time intensive undertaking, not to mention an administrative nightmare. A more popular option is to use the Realtime Black List (RBL).[xi] This is a regularly updated database of IP addresses known to be sources of spam. The MAILsweeper gateway provides a simple checkbox to use this service. If an incoming message originates from an IP that is listed in the database, the message will be rejected. This too may result in legitimate emails being denied, if the originating company has a poorly configured gateway (open-relay, to be discussed later), or if they obtain and use an IP from their ISP that had been used by a spammer in the past.
Your last chance you, as an anti-spam warrior, have to stop the enemy before it reaches your user community, is by content scanning the actual message. If the text in the message has something to do with increasing certain body part sizes, or getting rich quick, or cheap ink jet cartridges, known spam websites, or <fill in your favorite spam subject here>, then it just might be spam. Content scanners work by comparing phrases, that you have defined and given values to, with the text within the message, and if a threshold value is reached (adding up all the found-phrase values), it classifies the message as spam and processes it as you have configured it to (delete, quarantine, etc.).

Spoofing

Spoofing is simply the act of making a message appear that it is coming from somewhere/someone other than the actual sender. By default, most SMTP servers will accept email that comes from any sender - even senders that have the same domain as you. For example, a malicious person could connect to your gateway server, and craft an email from *your.boss@yourcompany.com* to *you@yourcompany.com*. When the message arrives in your mailbox, it would appear that it was just another message from 'your boss', but you might wonder why she's making all those strange suggestions. This is what is known as address spoofing, and can easily happen with SMTP mail because it has no built-in authentication mechanism. Obviously, spoofing should be prevented. With MAILsweeper for SMTP, this can be achieved by specifying valid combinations of domains, and how to handle them:

1. **@yourcompany.com* to **@yourcompany.com* = spoof, do not deliver, send alert.
2. *@* to **@yourcompany.com* = inbound, deliver
3. **@yourcompany.com* to *@* = outbound, deliver

Any valid internal emails that would have the first combination would never get routed to your gateway servers (they would stay internal), so anything that the gateway server does see with that combination is flagged as a spoofed message. (With MAILsweeper, even though *@* could be the same as **@yourcompany.com*, scenario 1 wins because it uses fewer wildcards.)

Cert offers other suggestions[xii] for prevention of spoofing such as using cryptographic signatures to ensure authenticity or using SSL/TLS in your mail transfer software, however this would only be effective if both parties in the email transfer are using the same precautions. At this point in time cryptographic applications have not achieved wide acceptance and would be difficult to use on a large scale. Note that digitally signed messages do not need to be encrypted, so they can still be scanned for undesirable content.

Remote Access to Email

Since everyone has this uncanny need to be connected, demand for remote access to email is at an all time high. Other than traditional dial-up or VPN access that uses the standard email client, mobile devices and web-based access are among the technologies that are gaining popularity.

Anyone that has a Hotmail or Yahoo email account knows the convenience of being able to access your email from anywhere that Internet browsing is available. It is this convenience that is driving the demand for web-based access of enterprise email systems. Both Microsoft Exchange and Lotus Notes offer add-ons to enable web-based access (Microsoft's Outlook Web Access (OWA)[xiii] and Lotus iNotes Web Access[xiv]). Other Reading Room papers are available dedicated to this topic since they pose large security concerns and have many factors to consider when implementing. Remember, this is essentially Internet access to your confidential data and, as such, needs to have all the protection that you would provide for any of your other web sites that access internal data i.e. proper firewall protection, authentication, confidentiality, availability and integrity. Both Microsoft and Lotus provide methods for strong authentication, such as SecurID's two-factor authentication, and encrypted https sessions but have many configuration issues that will require careful planning and implementation. These are beyond the scope of this document.

For the truly connected among us, devices are available that allow you to send and receive emails (including attachments) through a handheld wireless unit. One of the leaders in mobile messaging is the BlackBerry from Research In Motion (RIM)[xv]. If you are considering allowing BlackBerry's to be used with your email system, be aware that all BlackBerry's are not created equal. RIM offers two types: an Internet version, which comes with its own separate email account, and an Enterprise version that integrates with your enterprise email system. Currently they only support Microsoft Exchange and Lotus Notes installations. If a user wants to receive their company email on their Internet version, they will require auto forwarding to be enabled, which was discussed above. Also, the messages are sent in plain text raising confidentiality issues again. The Enterprise version, which also requires a BlackBerry server to communicate with your email servers, uses 128-bit 3DES to encrypt all messages before sending them to the device. It should also be remembered that since all email that is sent or received by an Enterprise version BlackBerry is virtually coming from the users company email account, it will be subject to all of the same policies, monitoring and protection that have been put in place. The Internet version will be using that squeaky backdoor again.

Building It

According to research performed by Ferris Research, Microsoft Exchange accounted for 50% of the corporate mailboxes in use in 2000. Lotus Notes had 25% and the rest was split between Groupwise, HP OpenMail, cc:Mail and others.[xvi] These products all provide ways of sending SMTP messages to the Internet. Email architecture does not have to be extremely complex to offer a respectable degree of security. In fact the 'Keep It Simple' adage certainly applies. There are a few golden rules however that should be adhered to. This brings us to our first rule:

Protect your email servers from the Internet.

Under no circumstances should you allow a server with mailboxes on it direct access to or from the Internet. All mail being sent to or from the Internet should be through dedicated servers in your demilitarized zone (DMZ)(You have a DMZ, right?). See diagram 1.

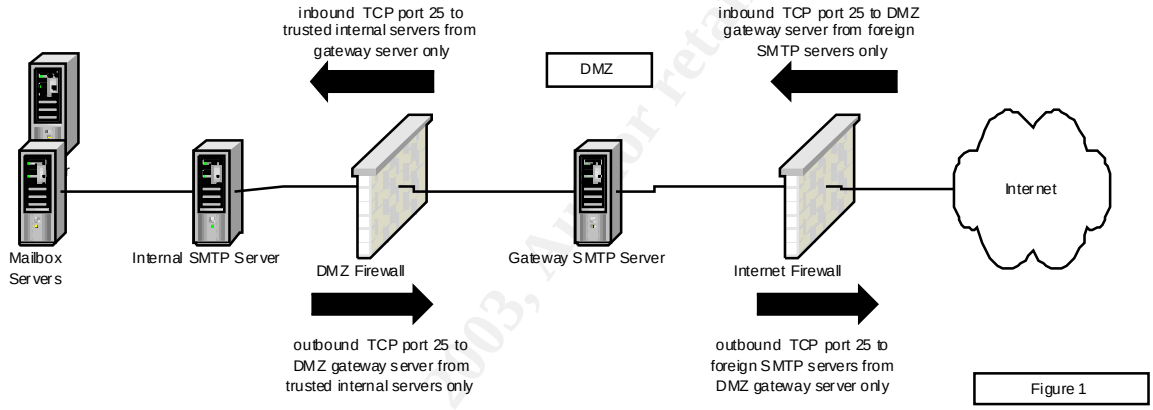

Figure 1

All email destined for the Internet should be sent from your trusted network, through a firewall configured to only allow port 25 connections to and from your DMZ SMTP servers. All email coming from the Internet should flow through the Internet firewall configured to only allow port 25 connections to and from your DMZ SMTP servers.

Since these DMZ servers are only allowed port 25 access, remote administration can be an issue. Ideally, all administration should be done at the console. If remote administration is absolutely necessary, be sure to only allow access from trusted workstations on the trusted internal network. Never allow remote control or remote administration tools to come in through the Internet firewall (that's pretty close to a hard and fast rule!). These servers need to be as hardened as possible, running only a minimum set of services and should be dedicated to processing mail. It also goes without saying that you should make sure they are always fully patched. Since they are going to be sending email to the Internet, they will need access to a DNS server. Ideally, you will have one on the same network segment so as not to introduce any more firewall rules or bandwidth bottlenecks. Complex firewall rules are susceptible to holes (keep it simple!).

Since all Internet mail flows through these servers, they are referred to as gateway servers. It is on these servers that content scanners such as MAILsweeper or GFI MailSecurity, discussed in the Technology section, are often applied. It is also these servers that are advertised on the Internet in your DNS MX records.
Figure 2 illustrates how a redundant set of servers might be set up to provide load balancing and/or backup in case of failure of either your primary ISP connection, or gateway server.

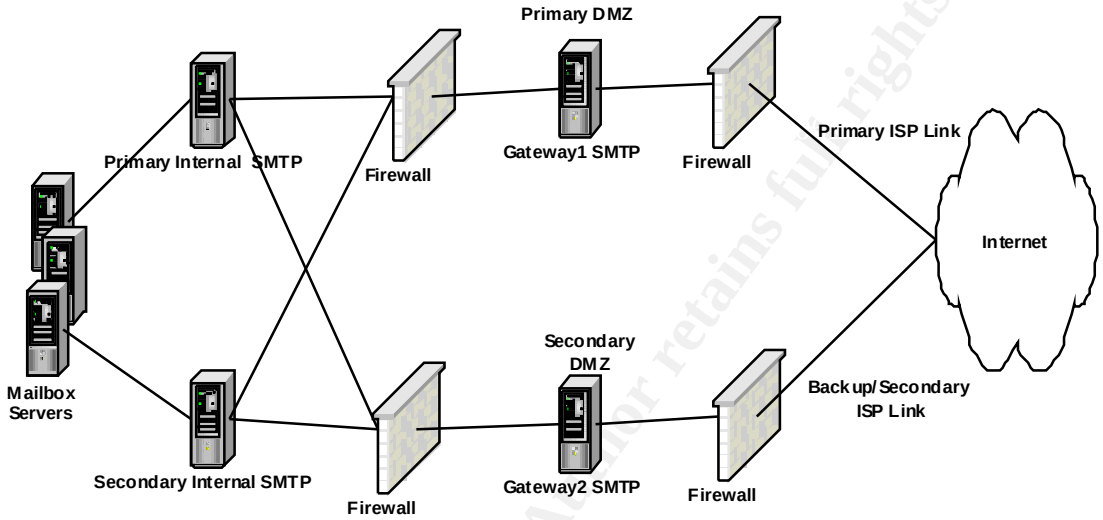

Figure 2

Whether it is functioning as a load balancing or redundant site will partially depend on your MX record values. If they share the same value, incoming mail will usually be split between the two. If your primary site has a lower MX value, it will receive all the mail until it becomes unavailable, at which point mail will start flowing to the secondary server/site. It is a good idea, if possible, to use different ISP's for your primary site and your secondary site, to remove another single point of failure.

Intrusion Detection

It is prudent to place Host Intrusion Detection agents on all Internet facing servers, and your gateway servers are just that. You should monitor these servers for unauthorized login attempts, strange port access attempts (only port 25 should be accessed), file tampering, critical log file entries, and audit tampering.
Network intrusion detection sensors (NIDS) should also be placed in your DMZ. Ideally you will have one on the Internet side of the firewall too. This will allow you to monitor the effectiveness of you firewall rules in preventing malicious access by intruders.

Banners
One of the most common methods of information gathering is done through 'banner grabbing'. This is simply starting a session with the mail server to see how it answers. Very often, the default banner contains the type and version of SMTP server you are running. A quick check on BugTraq for known vulnerabilities can give an attacker all sorts of ammunition to try against you. For this reason, it is strongly advised to change the banner to something very generic. You might consider replacing the default with a warning banner, a similar idea to the login banner that, for legal reasons, informs anyone connecting that it is for "Authorized use only".

Open Relaying (a.k.a. third-party relay, insecure relay)
Relaying of email is what gateway servers do. They take outbound email from your internal servers and relay them to their foreign destination servers. They take inbound email from foreign systems and relay them to your internal servers. An open relay is an SMTP server that will take mail from foreign systems and relay them to other foreign systems. Spam mailers love open relays for obvious reasons because they are able to hide behind your servers. The spam appears to be coming from you!
This can easily be prevented by carefully specifying who (by IP address) is allowed to send outbound email through your SMTP servers. These will typically be your trusted internal email servers. This can be further protected with your firewall rules by limiting who on your internal network can talk to your DMZ servers. With MAILsweeper you can also specify what domains untrusted systems are allowed to email to. Typically this will be limited to the domain(s) that you host.
Mail-abuse.org provides an excellent resource on how to prevent open relays on almost every flavor of SMTP server. This can be found at http://mail-abuse.org/tsi/ar-fix.html.
You will definitely want to make sure that you pay close attention to this issue. As discussed earlier, some companies subscribe to 'blacklists' such as MAPS Relay Spam Stopper (http://work-rss.mail-abuse.org/rss/) or Realtime Blackhole List (http://mail-abuse.org/rbl/) who maintain databases of open relays. If your mail server's IP address appears on one of these blacklists, none of the subscriber companies will accept mail from you. You will stay on the blacklist until you fix the open relay and prove to the blacklist owner that it has been fixed.

Spoof Protection
As discussed earlier, spoofed messages are messages that come from someone other than they appear. While it is difficult to ensure that all messages coming from the outside are authentic, it is absolutely necessary and (fortunately) fairly easy to ensure that no one sends messages from outside appearing to come from inside. Similar in concept to an access control list on a router, you just want to make sure that everything coming in does NOT have your domain as the sender, and everything going out does have your domain as the sender.

Special Email Accounts
Just like their famous cousin *webmaster@yourcompany.com*, there are a few special email accounts that all domains should have and monitor:

- *postmaster@…* Your email administrators should monitor this account. People wanting to report strange email behavior or who have email system related questions associated with your domain will send to this account.
- *abuse@…* and *security@…* These accounts should be monitored by your security group. This is where reports of security incidents or apparent system abuse involving your domain may be sent.

Conclusion

The information presented here is only the tip of the email iceberg. New technologies promising more secure email are appearing each day, and the challenges of keeping your internal systems secure are persistent challenges for all email and security analysts. However, if you have well-documented and thorough policy, and the basic defense-in-depth security architecture is followed, you will be well on your way to providing your users with a stable, safe email experience.

References

[i] Clearswift, "Putting best practice e-policy into action",
URL: http://www.clearswift.com/info/bestpractice.asp

[ii] Clearswift, "Computer Security Institute Survey",
URL: http://www.clearswift.com/info/keyissues_prod_stats.asp (2002)

[iii] Educom, "Statutory Retention Periods",
URL: http://www.exchangearchivesolution.co.uk/HTML/EASlegal_p2.asp

[iv] C2C, "Mailbox Size Management – A guide to control in Exchange and Outlook", URL: http://www.c2c.com/solutions/whitepapers/msm_jul_02.pdf

[v] Webopedia, URL: http://www.webopedia.com/TERM/s/spam.html

[vi] MessageLabs Press Release, "US business drowning in spam and UK set to follow suit as problem escalates",
URL: http://www.messagelabs.com/viewNewsPR.asp?id=103&cmd=Pr, (July 29 2002)

[vii] GFi Products – MailSecurity,
URL: http://www.gfi.com/mailsecurity/antivirus.htm

[viii] CipherTrust Press Release, "CipherTrust raises the bar in providing comprehensive protection for enterprise web-enabled mail", URL: http://www.ciphertrust.com/press/releases/iwm2_release.htm (Aug 19 2002)

[ix] Symantec Products and Services, URL: http://enterprisesecurity.symantec.com/content/productlink.cfm

[x] Clearswift Mimesweeper Products - CS SECRETsweeper, URL: http://www.MAILsweeper.com/products/msw/SECRETsweeper/default.asp

[xi] Mail-abuse.org, URL: http://mail-abuse.org/rbl/

[xii] CERT Coordination Center, "Spoofed/Forged Email", URL: http://www.cert.org/tech_tips/email_spoofing.html

[xiii] Microsoft, "Exchange 2000 Outlook Web Access", URL: http://www.microsoft.com/exchange/techinfo/outlook/2000/0WA2000.asp

[xiv] IBM, "Lotus iNotes", URL: http://www.lotus.com/products/inotes.nsf

[xv] Research In Motion, "About the BlackBerry Wireless Solution", URL: http://www.blackberry.com/products/blackberry/index.shtml

[xvi] Michael Sampson and David Ferris, "The Corporate Email Market, 2000-2005", URL: http://www.microsoft.com/exchange/evaluation/compare/MrktShar.pdf , (March 2001)

Last Updated: December 11th, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS SEC460: Enterprise Threat Beta	San Diego, CAUS	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS Security East 2018	New Orleans, LAUS	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS Amsterdam January 2018	Amsterdam, NL	Jan 15, 2018 - Jan 20, 2018	Live Event
Northern VA Winter - Reston 2018	Reston, VAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SEC599: Defeat Advanced Adversaries	San Francisco, CAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS Dubai 2018	Dubai, AE	Jan 27, 2018 - Feb 01, 2018	Live Event
SANS Las Vegas 2018	Las Vegas, NVUS	Jan 28, 2018 - Feb 02, 2018	Live Event
SANS Miami 2018	Miami, FLUS	Jan 29, 2018 - Feb 03, 2018	Live Event
Cyber Threat Intelligence Summit & Training 2018	Bethesda, MDUS	Jan 29, 2018 - Feb 05, 2018	Live Event
SANS Scottsdale 2018	Scottsdale, AZUS	Feb 05, 2018 - Feb 10, 2018	Live Event
SANS London February 2018	London, GB	Feb 05, 2018 - Feb 10, 2018	Live Event
SANS Southern California- Anaheim 2018	Anaheim, CAUS	Feb 12, 2018 - Feb 17, 2018	Live Event
SANS Secure India 2018	Bangalore, IN	Feb 12, 2018 - Feb 17, 2018	Live Event
Cloud Security Summit & Training 2018	San Diego, CAUS	Feb 19, 2018 - Feb 26, 2018	Live Event
SANS Dallas 2018	Dallas, TXUS	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS Brussels February 2018	Brussels, BE	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS Secure Japan 2018	Tokyo, JP	Feb 19, 2018 - Mar 03, 2018	Live Event
SANS New York City Winter 2018	New York, NYUS	Feb 26, 2018 - Mar 03, 2018	Live Event
CyberThreat Summit 2018	London, GB	Feb 27, 2018 - Feb 28, 2018	Live Event
SANS London March 2018	London, GB	Mar 05, 2018 - Mar 10, 2018	Live Event
SANS Cyber Defense Initiative 2017	OnlineDCUS	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced