Creating a Hardened Internet SMTP Gateway on Exchange 2003

Bret Fisher

GCWN Practical 5.0, Option 2
February 10th, 2005

Abstract

This paper will evaluate a 'locked down' inbound mail gateway (receives email from the Internet) design on Windows 2003 and Exchange 2003, using a set of complementing software products including Microsoft ISA Server 2004 and McAfee SecurityShield for Microsoft ISA Server 1.0. The purpose is to create a more secure Exchange Internet gateway without resorting to using a third party SMTP engine for receiving Internet email. The focus is on hardening the Exchange SMTP engine, increasing the intelligence of mail filtering before entering the internal network, and defending against common types of email-born attacks. Note, topics this paper will not discuss include: OS hardening, email authentication or encryption features, or the security of Exchange back-end systems.

The Windows SMTP Security Issue

Many corporate Windows shops have poor security on their email gateways; usually because even the latest corporate messaging systems do not come hardened as they should for exposure to the Internet. Currently Microsoft Exchange is the most used corporate messaging system[1] and has over 114 million mailboxes worldwide[2]; so, the email community could benefit greatly from a secured gateway design based on Exchange. Administrators often consider disabling open-relays and placing anti-virus at the gateway sufficient. As will be shown here, this is only the first step.

SMTP attacks have the potential to affect more systems and data and more people's productivity than any other single Internet service. Email now ranks as more important than telephones to businesses[3], so this system is to be guarded as such. The exposure risk of a publicly accessible SMTP server can run the full extent of digital threats. Social engineering, phishing, worms, viruses, trojans, denial of service, and buffer overflow attacks can all utilize the SMTP protocols 'trust by default' nature of accepting anonymous email for relay to an internal mailbox.

Large SMTP systems can have a greater attack surface than large web servers. Web servers are usually load balanced DMZ hosts with a few database back-ends; but email systems reach from the DMZ to multiple internal servers down to most user desktops. Attackers do not even need to know the topology of your internal network or what mail system you use. SMTP will often happily direct

[1] Bulkeley, Debra. "Microsoft's share of the corporate messaging market is 31%, compared with 26% for IBM Lotus, according to the Radicati Group". From Exchange is the leader, and rightly so in references.

[2] Bekker, Scott. "[Radicati Group] estimates the worldwide corporate Exchange installed base at 114 million mailboxes.". From After Slow Start, Exchange 2003 Begins to Take Hold in references.

[3] Gonsalves, Antone. E-mail More Important Than the Phone In Business, Study Shows in references.

their payload to servers and desktops inside the perimeter.

Examples of SMTP-Based Attacks

Authentication Denial of Service: Spammers use Exchange's SMTP AUTH command to brute force user passwords, and end up causing a denial of service on user accounts by locking them out. October 2003.
<http://www.winnetmag.com/Articles/ArticleID/40507/40507.html>

SoBig.F Worm: Email-based worm floods millions of systems from only tens of thousands of compromised hosts. August 2003.
<http://antivirus.about.com/cs/emailviruses/a/sobig.htm>

Buffer Overflow: Exchange SMTP command verb 'XEXCH50' vulnerable to buffer overflow. October 2003.
<http://www.microsoft.com/technet/security/bulletin/MS03-046.mspx>

Traditional Approach to Windows SMTP Gateways

The following are two common configurations that Windows administrators have used for email gateways for years, and the security risks taken in choosing these configurations.

1. Default Install of Exchange

Many small- and medium-sized Windows-based networks place their Exchange mail system directly onto an Internet accessible IP (by NAT behind their firewall). This provides no first line of defense against attacks including buffer overflow of the SMTP engine or mail-born viruses. Emails must be downloaded into the internal servers before they can be scanned for hostile, unwanted content. Some of these servers do not use any form of server-side anti-virus protection, usually because of the cost and complexity of such a product.

> *Risks of this configuration:* No tiered defense. Mail gateway has full access to rest of internal network, allowing an attacker to leapfrog onto non-email systems. The full feature set of the internal email server becomes available on the Internet, providing a larger attack surface.

A slightly different approach is to place one of these internal Exchange systems inside the DMZ. This is better than the first security issue, by providing a layer of defense in limiting leapfrog attacks; but, often because of the products' requirements, it still needs to have access to the protected networks Active Directory and Exchange system. This requires at a minimum, IPSec ports open between the DMZ and internal network. If an attacker were to gain access to this box, it may not take much more effort to gain access to the internal email server.

> *Risks of this configuration:* Increased risk from additional ports open from

DMZ to internal. Full SMTP protocol feature set available to Internet.

2. Third Party SMTP Engine

Organizations may often place a SMTP relay from their anti-virus vendor in the DMZ. In fact, anti-virus vendors want you to think their SMTP engine is more secure, based on the sole benefit that it checks for viruses. Often administrators test and evaluate the anti-virus functionality before choosing a product, but never investigate the SMTP engine underneath it. One might even consider this third party SMTP engine a plus because it is a different engine than the internal Exchange system, giving them that 'heterogeneous edge'. The negative side of this strategy is two fold:

Reduced feature set: Some of the features in an Exchange SMTP can actually aid security. Using another engine prevents nearly all of these features from being used, including authentication, SSL-SMTP, account enumeration tar pitting and UCE (spam) blocking at the gateway.

Support of SMTP engine: A big issue that is not usually considered in a third party relay purchase is that anti-virus vendors are not in the business of creating or supporting SMTP engines. Nearly all the anti-virus vendors that sell a SMTP anti-virus scanner force you to use their SMTP engine (or the one they purchased) with the product, rather than allowing you to choose a common engine like IIS. I can only guess this is because it is easier to create an anti-virus scanner if you also control the SMTP engine. Anti-virus SMTP engines never have the full feature set or maturity of an enterprise engine like IIS6. I have witnessed two different major anti-virus vendors who had serious bugs in their SMTP engine, and did not make it a priority to fix them. I do not have this problem of support when choosing a product like IIS6 or Exchange where the product is riding on the quality of its SMTP engine.

One vulnerability, in my experience with third party bundled SMTP engines, was so big it let any email attachments delivered in bulk (from list servers and such) pass through the anti-virus scanner unchecked. This problem was unknown to the manufacture. Once we notified them, they released a patch with little fanfare (In fact the entire product line has but a few vulnerability posts to securityfocus.com or secunia.com, and none include this issue). Such is not the case with IIS.

Another example is McAfee Webshield anti-virus SMTP relay (using its own SMTP engine), which requires nearly a dozen manual entries in the registry to allow proper mail flow. Many of these entries are not documented anywhere except internally at McAfee. The product has poor logging, which is not formatted for automated parsing (it appears to be designed for a human to read it directly from notepad). Again, since Exchange rides on top of IIS, the stability, feature set, and logging are almost always better than a anti-virus vender's SMTP. For these reasons, you would begin with a better security posture if a best-of-breed SMTP engine were used throughout your email system.

Improving the Traditional Approach to Windows SMTP Gateways

So if these two options are no longer the best way in today's Internet climate to protect a corporate Exchange system, then what is? IIS6 is a high quality SMTP engine (Exchange rides on top of it) and has standards-based configurable logging, and decent monitoring when used with Exchange. So why not start with it? Nevertheless, Exchange 'feature bloats' IIS6 beyond what should be available from the Internet, and Exchange also requires network access that is beyond what a DMZ box should have. With all the new features such as SMTP tar pitting and Intelligent Message Filtering, Exchange itself is the best candidate for incoming mail bound for Exchange.

ISA Server 2004 can be a steward for Exchange and sit in the DMZ with only a single port open in one direction to Exchange that sits on the internal network. ISA can reverse-proxy Exchange's SMTP and answer connections from the Internet on Exchange's behalf. ISA can then customize the SMTP feature set it proxies, allowing the administrator a level of customization not previously seen in SMTP for Windows. To be sure this system stops as many attacks before they get through the DMZ, McAfee's SecurityShield for ISA Server 1.0 installs an ISA filter plug-in that gives anti-virus features and further SMTP customization to the application proxy. This creates a "best of both worlds" system: security lock down (DMZ, SMTP command control, anti-virus before internal network) meets the Exchange feature set (Intelligent Message Filter, SMTP tar pit, directory lookup, authentication, Secure SMTP).

Security Issues Mitigated Using This Implementation

If a system is designed and configured as recommended in this document, it will reduce the attack surface of an Internet facing mail server from the following attack scenarios.

1. Zero-day buffer overflow of SMTP commands (using ISA 2004)
2. Known but non-patched buffer overflows of SMTP commands (using ISA 2004)
3. Exploiting unnecessary SMTP commands at the Internet gateway (Using ISA 2004)
4. Known viruses/trojans/worms (Using McAfee SecurityShield 1.0)
5. Account enumeration by read receipt (Using Exchange 2003)
6. Phishing by account enumeration (Using Exchange 2003)
7. Exploiting of third party SMTP engines that are not as mature as IIS6 SMTP (Using Exchange 2003)
8. TCP layer attacks such as port scans, land and ping of death. (Using ISA 2004)
9. UCE denial-of-service (Using Exchange 2003)
10. Spoofed MAIL FROM: fields that lead to Phishing (using Exchange 2003,

SecurityShield 1.0 and DNS)

11. Packet flow or session count denial-of-service (using ISA 2004)
12. Simple exploit scripts that attack based on SMTP banner query (using Exchange 2003)

When each security feature of the system is detailed later in this document, an ‘Issue #’ will be mentioned which refers to the security issues it addresses in this list. For example, search for ‘issue 1’ to find methods to mitigate zero-day buffer overflows.

Non-Compliance Risks

If these or similar steps are not taken on a Windows host performing messaging duties with untrusted hosts, SMTP could become the biggest threat to Internet-born attacks on a private network. Being that email has become an essential business tool, the option to restrict access from unknown hosts is unlikely. Providing as little attack surface on your exposed mail servers as possible is the only way to prevent it from being the attacker’s first choice for gaining unauthorized access into your hosts and network.

Product Evaluation

All of the following products were leading edge software in the Fall of 2004. Several had been on the market less than six months. Products used to build this system:

Windows 2003
IIS6 SMTP
Exchange Server 2003
ISA Server 2004
McAfee SecurityShield 1.0

Detailed Product Description

Windows 2003

2003 Server is the only Windows OS that should be accessible from the Internet. No specific features of Windows 2003 will be used to harden this system, although it is required to install IIS6 SMTP.

IIS6 SMTP

This is the core of Exchange 2003. It is the most popular SMTP engine on Windows, since it’s included in the OS. This can be good for security because Microsoft has one of the most mature patch notification and release processes (though not necessarily the fastest). Every Windows security vulnerability quickly ends up on every OS security web site and mail list, so you have little risk of not knowing when a vulnerability is found. Microsoft provides tools to monitor and manage IIS6 SMTP, as well as free tools to determine if it’s patches are up to date (using Microsoft Baseline Security Analyzer). Also, because IIS6

SMTP runs Microsoft's billion dollar a year Exchange messaging system, it receives a lot of attention from Microsoft and the security community. Addresses Issue 7.

Exchange Server 2003

Exchange the most popular corporate mail platform on Windows. Exchange has some good reasons to be chosen simply on the premise of security. It allows single-sign-on with Active Directory. 100% of its network communications can be encrypted in several ways (IPSec, SSL and MAPI client encryption), and it includes a built-in UCE filter called Intelligent Message Filter. More specific gateway security features will be discussed later.

ISA Server 2004

Even if you do not use ISA Server as your Internet firewall, it can still serve very effectively as an outbound web proxy, a VPN end-point, and as discussed here a reverse application proxy. Since it is the only SMTP proxy with deep protocol inspection and control, and it allows third party products to hook into this inspection, I will not be discussing alternative products to this. To my knowledge, it is an one-of-a-kind product.

McAfee SecurityShield 1.0 for ISA Server

At the time of writing this document (Fall 2004) SecurityShield was the only product released that provided SMTP anti-virus scanning as a plug-in filter for ISA Server 2004. Other vendors have similar products, but they either did not work with the newly released 2004 edition of ISA Server or were not released yet. An anti-virus product with its own SMTP engine built in was not considered. The goal of this analysis was to use a best-of-breed SMTP engine like IIS. SMTP engines in stand-alone anti-virus products mostly use a significantly reduced feature set and have limited SMTP customization, monitoring, and logging.

SecurityShield has its own advanced logging and log searching interface for email scanned and offending content found. Very customizable rules and rule exceptions can be created in the Java management interface which runs outside of the ISA interface. McAfee's filters are seen in the ISA Management program under plug-ins in the form of an incoming and outgoing SMTP filter.

Security Features of Implementation

Recipient Lookup in Active Directory

Because ISA will reverse-proxy an Exchange server, the system can gain the features of Exchange at the gateway. Including the ability to deny any connection with 'rcpt to:' that are not owned by your Exchange system. Addresses issue 9.

Tar Pit 500 Series Responses

This feature was recently released for Exchange in 2004 and the overall affect of its implementation is still being discussed in the engineering community. The Microsoft Knowledge Base article 842851 discusses this feature, but does not go into depth about what will cause it to activate during a SMTP conversation. What is known from the Knowledge Base article is that once a few hotfixes are applied, and a registry value set to a delay time X seconds, the SMTP service will wait that specified delay time before replying to a *rcpt to:* that contains an invalid email address (one that your organization does not have a mailbox for). However, upon testing it actually activates the delay for any command given during a SMTP conversation that generates a 500 series error/response. The intent is to slow down 'directory harvesting', a method spammers use to determine what email addresses exist on a particular email server. By turning on the recipient lookup feature mentioned previously, a server is then open to a harvesting attack. However, this tar pit feature reduces that threat by causing such a lengthy delay followed by '550 5.1.1 User unknown' to requests for unknown email addresses that a spammer would presumably stop an attempted harvest of your mail system because it was 'costing' them too much time. I have found no real-world data to say this is an affective strategy. Many organizations just turn off recipient lookup and accept all incoming mail, and then depend on internal features to bit-bucket (delete) the email once it is found to be illegitimate on an internal system. Both options have the same affect, but recipient-lookup-plus-tar-pitting allows an email server to halt a illegitimate SMTP conversation before it gets past the header, saving CPU cycles and bandwidth. Addresses issue 6.

SMTP Command Size Limiting

Since Exchange is designed to be a very feature rich 'groupware' server, its SMTP engine contains many features, which have commands to interface with them. Typical Internet mail traffic uses a small subset of the known SMTP commands, and all unnecessary commands should be disabled. Exchange does not offer a capability to disable commands (and rightly so, since messing with these would break Exchange-to-Exchange communications inside your network) but ISA Server does in the form of a SMTP filter that inspects the actual commands passed through it (enabled by default when you create a new SMTP publishing rule). Maybe with Exchange's next release (codenamed E12) the new 'Edge Services' will allow you to select a server as the Internet gateway and subsequently have everything but the most necessary SMTP commands turned off[4]. Until then however, we have to control what SMTP features are available to the Internet using ISA.

ISA's SMTP Filter comes with a default list of common SMTP commands and a recommended command size limit for each (in bytes). Below is that list for

[4] Read Microsoft's take on Edge Services at the link in the references

reference. If a command is not on the list, it is allowed through unchecked. You can add too this list, but not delete the defaults (just increase their size so they are never blocked). If you disable a command, the SMTP conversation will be dropped when an incoming host issues that command (so be careful with disabling them). Just as bad, if you set a data length too short and a incoming host exceeds it in a normal conversation, the connection will again be dropped; although you will get a *421 5.5.2 Syntax error (command line too long)* before the connection is dropped. I see no evidence that normal functioning mail hosts can react well to either of these scenarios (e.g., the incoming host receives 5.5.2 and decides 'ok, I'll try to shorten my command to please you'). Most likely, the email will never make it through. Addresses issue 1. Addresses issue 2.

Default ISA SMTP Filter Command List

AUTH	1024
BDAT	20
DATA	6
EHLO	71
EXPN	71
HELO	71
HELP	6
MAIL FROM:	266
NOOP	6
QUIT	6
RCPT TO:	266
RSET	6
SAML FROM:	268
SEND FROM:	268
SOML FROM:	268
STARTTLS	10
TLS	5
VRFY	71

ESMTP Extension (EHLO) Keywords in Exchange 2003

Below is a list of EHLO keywords presented when given an 'Extended Hello' on Exchange 2003. These keywords tell the requesting server what features (also called extensions) are available on the receiving email system. Some should not be available on a standard Internet accessible SMTP gateway. We will use ISA to filter the ones that should not be accessible.

TURN
SIZE
ETRN
PIPELINING
DSN

ENHANCEDSTATUSCODES
8bitmime
BINARYMIME
CHUNKING
VRFY
X-EXPS GSSAPI NTLM LOGIN
X-EXPS=LOGIN
AUTH GSSAPI NTLM LOGIN
AUTH=LOGIN
X-LINK2STATE
XEXCH50

Detailed SMTP Command Filtering Recommendations

NOTE: These recommendations are based on many assumptions about your email environment being rather generic. Do not just arbitrarily apply these on production system without extensive testing. Your mileage may vary. Addresses issue 1, issue 2, and issue 3.

VRFY - Recommend ISA Default

See MS KB 289521 about why this command is a dummy command. It was created by RFC 2821 to verify email addresses, but can no longer be used in the hostile environment of the Internet. It is a 'dummy' because the it still creates a valid response of 550 or 252 (probably because SMTP RFC's require it too), but it will never return a successful result telling the incoming server that an email address exists.

EXPN – Recommend ISA Default

See MS KB article 175842 about why this command is not implemented. It is used to identify members of a mailing list. You can leave it at default on ISA as Exchange will always return a 500 error. If you want to be aggressive, disable it in the ISA filter, as no email server should be sending you this command from the Internet to an Exchange system.

X-LINK2STATE and X-EXPS – Add and Disable

X-LINK2STATE (Exchange site topology) and X-EXPS (Exchange authentication) are proprietary Exchange commands and should not be used for anonymous email from the Internet. It is recommended to add and disable these commands to the ISA filter.

XEXCH50 – Add With 50 Byte Limit

This is a proprietary Exchange command for public folder replication, distribution group email, and other various Exchange functions; but it has had an interesting history, with an Exchange 5.x/2000 bug someone could perform a remote buffer overflow using this command[5]. With a patch, or Exchange 2003, authentication is required before this command will accept data. So normally, it would be recommended to add it to the filter and disable the command, since no authentication will be possible after we disable it later on. However, XEXCH50 has a shady past, where before the patch in Exchange 2000, it would try to use XEXCH50 commands by default over the Internet if it sent an EHLO and a server reported back that it supported XEXCH50[6]. That being said, if there are still unpatched Exchange 2000 systems on the Internet, and you 'Add and Disable' this command (which will not remove it from the EHLO response), you may create a situation where these mail systems cannot communicate with yours. Every time they send a XEXCH50 you will disconnect them and they won't know why. It is recommended to add this command with a 50-byte limit. Aggressive tactics would have you disable it as well, possibly cutting off those few unpatched Exchange 2000 systems sending you email.

NOOP – Increase bytes to 1024

The default is 6, but Exchange 5/2000 may try to use a larger NOOP command[7].

TURN – Do Not Add (Unsupported)

TURN swaps the rolls of SMTP client and server to transfer queued mail from one SMTP server to another. This is not needed in most Exchange gateways, but unfortunately, ISA 2004 does not support adding this command to the SMTP filter.

ETRN – Add and Disable

Provides the same purpose as TURN, and *is* supported by the filter. Typically, you will not be accepting client connections to your Internet facing gateway that will be pulling mail of that system. These verbs are mostly used for disconnected SMTP servers that need to poll for their mail once they come back online (satellite connected systems, dial-up servers, etc). It is recommended to add and disable this command on the ISA filter.

BINARYMIME – Do Not Add

Defined in RFC 3030, this SMTP extension was created to reduce the processing and bandwidth overhead previously associated with sending binary data and the required encoding to other formats for transmission. Its use is common and necessary, and a byte limit is not easily defined. It is recommended not to add this command to the filter[8].

HELP – Disable

I do not know of a SMTP server that uses the HELP command in its normal course of transmission. It is recommended to disable this command in the filter.

[5] See Microsoft Security Bulletin MS03-046

[6] See MS KB article 818222 for how XEXCH50 is used

[7] See MS KB article 312213 for how NOOP is used

[8] See MS KB article 323483 for how this is used

AUTH – Disable

This is a big one. AUTH LOGON should be your nemesis on a SMTP gateway. In the world of non-authenticated email, why is authentication needed? Maybe a better question is why is there not a warning on the front of your Exchange CD that says "Warning! By default, if this SMTP port is accessible from the Internet then the entire world can spend all day brute forcing your Active Directory accounts"[9]. (Now if you support external POP/IMAP users that need a SMTP relay, I recommend using RPC over HTTP with Outlook, RPC Proxy with Outlook, Outlook Web Access, and lastly a SMTP Virtual Server published to TCP port 465 or 587 with AUTH enabled[10].) It is highly recommended to disable this command in the filter. Addresses issue 3.

SMTP Banner Change

A common security (through obscurity) technique is to change the STMP service software information that would normally trail the hostname when a connection is first made to your gateway. Addresses Issue 12. Here is the default string for Exchange 2003:

```
220 exchange.sans.org Microsoft ESMTP MAIL Service, Version:
6.0.3790.211 ready at Wed, 2 Feb 2005 23:40:00 -0500
```

Giving a non-trusted host the .dll version of your SMTP service might not be the best thing to do before you even know them, so there is an easy command to change it. From the IIS adminscripts directory (defaults to C:\inetpub\adminscripts)

```
cscript adsutil.vbs set smtpsvc/1/connectresponse "My Mail
Service .9 Beta"
```

The 1 in smtpsvc/1/ is the virtual server number, which starts at 1 and increments for every new SMTP Virtual Server you create on a machine. To reset the banner, re-enter the command with empty quotes.[11] This will yield the following response after restarting the SMTP service:

```
220 exchange.sans.org My Mail Service .9 Beta ready at Wed, 2
Feb 2005 23:40:00 -0500
```

Personally, I like to rename it to something believable like:

```
220 exchange.sans.org ESMTP ready at Wed, 2 Feb 2005 23:40:00 -
0500
```

[9] See "A New Kind of Attack" in references

[10] 465 is normally for SSL SMTP (STARTTLS) and 587 is for SMTP submit, recently used to get around ISP's blocking 25 outgoing

[11] See MS KB article 836564 for how this is used

‘ESMTP’ as the service name is what some big ISP’s are doing. You could also copy the banner of Sendmail or Qmail. However, using a tool like Nmap, an attacker may determine the OS (or more) of your server using a technique called fingerprinting that looks at the IP packets in depth rather then service info like the SMTP banner. Often they can be successful by connecting to just a few open ports. Therefore, this banner change ‘feature’ will only go so far in protecting your servers’ OS and service identity. A quick test of Nmap 3.81 on ISA 2004 (containing a single rule to publish a default install of Exchange 2003) using –O to perform OS fingerprinting identifies it as NetBSD, but this could change with the next Nmap release, which happens often.

Intelligent Message Filter

There is a lot of information about IMF already available on the Internet. The short version: it is a free server-side UCE filter for Exchange 2003 that works at two levels. First, it monitors the initial connection from the Internet and, second, when it later enters the store (i.e. users mailbox). The part you care about is the initial connection, where you have the ability to disconnect the SMTP session before it is finished (called ‘rejecting’) if IMF determines the email to have a UCE score higher then what you set in Systems Manager. This can save resources, since there is the potential for UCE to be dropped before a large payload of images or binaries are transferred to your server. This feature only works on Exchange (IMF won’t install on IIS6 alone), so publishing it through ISA 2004 is the most effective way to allow highly effective defenses against UCE. If another hop were between IMF and the Internet, then all UCE would be accepted by this first hop and relayed to Exchange before it could be scanned for UCE content. Addresses issue 9.

ISA Intrusion Detection

ISA Server 2004 has some light IDS features built in, including port scans (# of ports is configurable), WinNuke, land, ping of death, IP half scan and UDP bombs. The detection of these known attack patterns is turned on by checkbox, and there is little reason not to do so. Addresses Issue 8.

Anti-Virus Scanning

All the common features should be turned on in SecurityShield. Recommendations include *not* sending notifications about viruses found and to restrict inappropriate file types (by either blacklist or whitelist). Addresses issue 4.

Read Receipts and Mail Loops

In Exchange System Manager under Global Settings > Internet Message Formats, do not be tempted to allow automatic *anything*, out of office responses or non-delivery reports (and optionally do not allow delivery reports either). These settings do not affect internal email, but only email sent from inside out. The out of office and automatic will certainly create mail loops.

Delivery reports are mostly used for spammers. Non-delivery reports can be useful but are constantly abused by email worms and UCE. If you have NDR enabled do not be surprised to see dozens and dozens of outbound domain queues because Exchange is trying to send a NDR to a nonexistent email address. Although there is hope. If you have all the above options enabled, no mail should be entering your system bound for invalid mailboxes. In this case enabling NDR may not be too bad on your queue growth. Also, if you have common organizational partners that you would like these types of emails to get through to, than add their domain as a new record under Internet Message Formats, and select what options are needed just for them. Addresses Issue 5.

Real-time Blacklist

Exchange supports RBL's. They can be good and they can be bad. When they go bad, they REALLY go bad (e.g. blocking any incoming email) so I do not recommend them. Google has plenty of resources on how to chose and implement a RBL.

Sender ID and Sender Policy Framework

Sender Policy Framework is an anti-UCE tool that uses custom formatted DNS TXT records to publicize what gateway servers you allow to send mail from your network. You can do this for a mail domain without any requirements on your email servers, but the best part is the client end. A SMTP server receives an email saying it is from yahoo.com, but how can it be sure it is really from yahoo.com and not someone in China? SMTP headers can be completely forged. Well Sender Policy Framework will quickly lookup yahoo.com's DNS servers and ask if the connecting IP truly has permission to send email from yahoo.com. This is a remarkably simple way to thwart UCE, and does not require a central database of information like blacklists. Unfortunately, it only works if domains that email you implement the custom DNS records. Addresses issue 10.

Currently neither of these 'sender authentication' methods work with this papers selected products out of the box. Exchange 2003 SP2 may contain Sender ID support (which should be a superset of SPF) when it is released. If you cannot wait until then, there is support for SPF in GFI's free version of MailEssentials, which installs on top of an Exchange server. There are also a few IIS 'sink' scripts out there but I do not recommend them.

At a minimum, every responsible email administrator should implement the DNS TXT records that list their outgoing email servers so that others who have implemented SPF can verify if your mail is truly from your servers[12]. The record looks similar to this:

```
v=spf1 mx a:mailhost1.sans.org a:mailhost2.sans.org ~all
```

[12] A DNS record wizard is at http://www.anti-spamtools.org/SenderIDEmailPolicyTool

Two SMTP Virtual Servers

This optional piece will build on a lot previously discussed in this paper. What is required for this security enhancement is to have an Exchange server designated as a Front-End server (so you will need to have more than one Exchange server). This server cannot have any user's mailboxes on it. Now create a second SMTP Virtual Server using System Manager and give it a new IP. You will use this new SMTP queue for incoming mail from the Internet only, so change your ISA SMTP publishing rule to point to the new IP. The original SMTP queue will be used for outgoing and internal mail only. Why separate these out? In addition to all the SMTP command limiting on the ISA Server, now you can turn off features you do not need from the Exchange system itself. On the incoming queue, enable the sender, recipient, and connection filters and customize to taste. Make sure they are disabled on the outgoing queue so 'trusted' mail is not filtered out. Now ensure IMF is enabled only on the incoming queue. Lastly and most important, disable all authentication options except for anonymous on the incoming queue, and then set 'relay after authentication' on the outgoing queue.[13]

Notice the shortened ESMTP extension list below, after the second Virtual Server was created. The size changed, and all authentication features turned off.

Default	Second Virtual Server
TURN	TURN
SIZE	SIZE 10485760
ETRN	ETRN
PIPELINING	PIPELINING
DSN	DSN
ENHANCEDSTATUSCODES	ENHANCEDSTATUSCODES
8bitmime	8bitmime
BINARYMIME	BINARYMIME
CHUNKING	CHUNKING
VRFY	VRFY
X-EXPS GSSAPI NTLM LOGIN	X-LINK2STATE
X-EXPS=LOGIN	XEXCH50
AUTH GSSAPI NTLM LOGIN	
AUTH=LOGIN	
X-LINK2STATE	
XEXCH50	

SMTP Transmission Denial-of-Service

If you create two Virtual Servers as discussed above, the SMTP Virtual Server

[13] For a much more in-depth look at dual SMTP queues, look for "You Had Me At EHLO…" in the references

published to ISA should have its properties changed to prevent Exchange resources being over extended by a mail-flood (it is not recommended to change Virtual Server settings for internal mail routing, so only do this on the incoming Virtual Server as mentioned above). These are often specific to a calculation of hardware resources, Internet connection speed, and the typical amount of mail traffic you receive. Nevertheless, here are some numbers to start with. On the General tab of the Virtual Server Properties, limit connections to 100 (do you normally receive 100 emails from the Internet at the same time on a single server?). On the Messages tab limit the message size to your maximum email attachment setting (default is set in Global Settings, each user can be set in their Active Directory properties, and each Connector can have its own setting as well.). This number will show up now during a EHLO reply as 'SIZE 10039' telling the sending server the max email size your gateway will accept. This can prevent 'orderly' email servers from even trying to send an email over the limit, and non-RFC compliant ones will have their connection dropped by the virtual server as soon as the packet sum hits that number. Otherwise, the email will have to be accepted and dropped within the Exchange system later on when it finds another setting that limits the email size. Just set the session size to slightly higher than the message size. Leave the messages per connection at 20 and reduce the number of recipients per message to something slightly above the total mailbox count this host accepts email for. Change the hop count on the Delivery > Advanced tab to 15 or 20 (reduces the affect of mail loops). These settings should add up to limiting your exposure to a Front-End Exchange server denial-of-service due to resource consumption. Addresses issue 11.

Blocking MAIL FROM: Your Domain

Again, if you create two Virtual Servers as discussed above, a simple yet effective tool for stopping some phishing and UCE is to block all mail at the gateway that has blank senders or a FROM: header that claims it is from your internally hosted domains. This is often used to look like emails coming from administrator@yourdomain.com or support@yourdomain.com to cause users to think it was an internally generated email. Now that you have Sender Filtering enabled on the incoming Virtual Server, you can add a sender rule for blank senders, and for anyone @yourdomain.com. As soon as the sending server enters the offending MAIL FROM: command, the connection is dropped.

NOTE: An important Exchange tip here is that if mail addresses inside your network are spoofed in the from fields on anonymous inbound email, there is an easy way to tell it is not from the internal user: Only authenticated emails will have their name resolved in the From field. This means all authenticated email will have a From line like "Bret Fisher" where anonymous email will be "Bret Fisher [bret.fisher@yourdomain.com]" inside the email. If users are educated about this it may prevent some types of phishing attacks. Addresses issue 10.

Note About Vendor Support

You may notice that every product discussed in this document is a commercial for-profit product. There is a reason behind that choice. The realm of information security has a legality side to it, and in that realm, there is the understanding that an unsupported product (by either the community or the vendor) increases risk and thus decreases security. With these products purchased, you should buy the appropriate amount of support your organization needs. The writer does not mention here nor recommend any unsupported modifications or 'hacking' of these products (e.g., using scripts, small unsupported add-on programs, or reg edits) to make them more secure. To the best of the writers' knowledge, everything in this document is a supported feature of the product it applies to (as of the writing of this document) and should be under warranty of the properly licensed product. As always, if you are unsure, check with your product vendor before making any of these changes. Product support and warranty should be a part of any security professionals buy decision.

Implementation Guide

Physical Network Configuration

For this implementation, you have the choice of two network configurations.

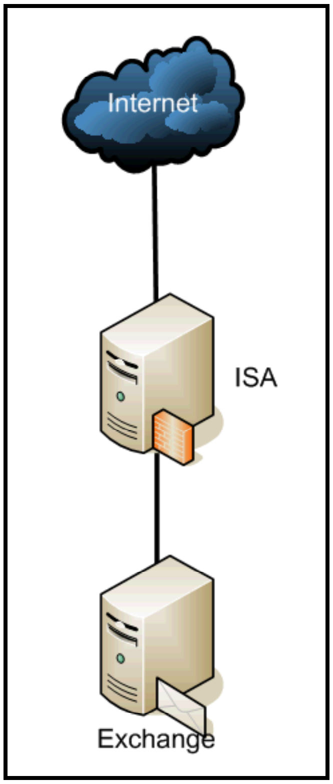

Figure 1

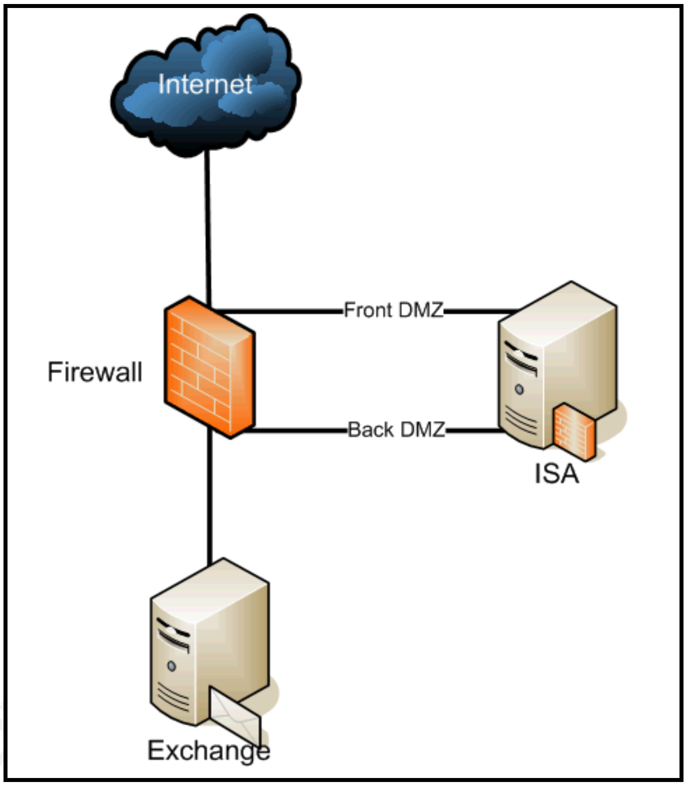

Figure 2

Figure 1 above, is an Exchange system sitting on an internal network, and ISA Server 2004 as the Firewall.

Figure 2 above, is an Exchange system sitting on an internal network, a third party firewall, and ISA sitting between two DMZs. This option is available for networks where a firewall system is already well established and replacing it with ISA Server 2004 is not an option. IP routing is the main difference between these two options, so the system configuration is the same for both designs in respect to SMTP publishing and features for incoming email.

Required on the ISA Server: two network connections that will be referred to as 'Internal ISA NIC' and 'External ISA NIC'. Even sitting in the DMZ configuration of Figure 2, these are necessary as the 'single NIC configuration' of ISA only works for web proxy mode. Most in-place firewall systems have an existing DMZ, so you can either create a new physical DMZ with a separate IP subnet (as indicated by 'Back DMZ' in Figure 2), or have the existing DMZ answer to two different subnets. Whatever the configuration, ISA Server 2004 has to sit on two different subnets and be able to route packets. If NAT is involved somewhere, it is recommended that it take place on the ISA server.[14]

Product Install

Exchange 2003

Installing Exchange is beyond the scope of this paper. Suffice it to say, everything should work on a default install of Exchange. Some security features will specifically require features such as dedicated Front-End and Back-End servers; and they will be clearly indicated when necessary.

Required on Exchange Server(s): Exchange 2003 on Windows 2003. Windows must have hot fixes 831464 (required to install SP1 for Exchange) and 842851 (required for the SMTP tar pit feature) installed. At the time of writing, Windows 2003 SP1 RC1 included both of these hotfixes. Exchange 2003 must have SP1 installed. We will only be referring to the Exchange system that will be your first SMTP hop for incoming mail. It can be a Front-End designated server or the only server in an Exchange environment, but it must be an Exchange host on the Active Directory forest of your users. In addition, the mail path from the gateway to a user's mailbox should always stay in the same Exchange/AD forest. This is to preserve the SCL rating and allow for recipient lookups (read release notes).

Once done patching Exchange, download and install IMF and its update(s) from Microsoft.com/downloads (search for Intelligent Message Filter). It is free as long as you own Exchange. Install it per its deployment guide.[15]

ISA Server 2004

Install ISA Server 2004 on a Windows 2003 server, but make sure not to install the Message Screener component. No IIS components should be installed. No SMTP firewall rules should exist. Ensure there are no ISA updates by checking microsoft.com/isaserver

McAfee SecurityShield 1.0

After ISA Server is installed, install SecurityShield on the same system with all defaults. Check support.mcafee.com for product updates. This does not require a reboot, but starting the Administration Console will require installing Sun Java, which will require a restart.

Product Configuration

Exchange 2003

[14] Refer to isaserver.org for plenty of excellent network designs by Thomas Shinder

[15] Deployment guide listed in references

(Using System Manager)

- Turn on Recipient lookup. Goto Servers > *ServerName* > Protocols > SMTP > *Incoming SMTP Virtual Server* > Properties > Advanced > Edit > And be sure 'Apply Recipient Filer' is enabled. Now look at Global Settings > Message Delivery > Properties > Recipient Filtering tab > enable 'Filter recipients who are not in the Directory'. This takes an SMTP service restart to take affect.
- Tar Pit. You should have already installed Windows 2003 hotfix 842851 or SP1 (once it is out). Recipient lookup was just enabled. Now all that is left is a registry entry. Create a DWORD named TarpitTime in HKLM\SYSTEM\CurrentControlSet\Services\SMTPSVC\Parameters\ And give it a decimal value you are comfortable with, which will be the delay in seconds every time a invalid rcpt to: or SMTP command is sent. 30-45 seconds is recommended.
- Change the SMTP banner. At the command prompt.
  ```
  cscript c:\inetpub\adminscripts\adsutil.vbs set
  smtpsvc/1/connectresponse "ESMTP"
  ```
  Restart the SMTP service to take effect.
- Enable IMF. Under Servers > *ServerName* > Protocols > SMTP > Intelligent Message Filtering > Properties > Enable the Virtual Server that is published through ISA. Now head to Global Settings > Message Delivery > Properties > Intelligent Message Filtering tab, and set SCL ratings to your liking. Be sure that the gateway threshold is set to reject.
- Disable automatic mail and receipts. Under Global Settings > Internet Message Formats > Default > Advanced tab, disable all check boxes except "Allow non-delivery reports" and "Preserve sender's display name on message".

Exchange 2003 Front-End Only (optional)

(Using System Manager)

- Create a second SMTP Virtual Server. Add a second IP to the FE Exchange server. Under Servers > *ServerName* > Protocols > SMTP, right click SMTP and select New > SMTP Virtual Server. Call this one 'Anonymous Incoming', and rename the Default queue to 'Authenticated Outgoing'. Ensure that 'Authenticated Outgoing' is only assigned to the old IP address. Now view the properties of 'Authenticated Outgoing' and ensure that no filtering is running under Advanced. On the Access tab, under Authentication, disable Anonymous access. Click OK and now access the properties of 'Anonymous Incoming'. Ensure all the different types of filtering you will use are enabled under advanced. On the Access tab under Authentication, disable all *but* Anonymous. Under relay, uncheck 'allow all computers which successfully authentication to relay…'.
- SMTP Transmission Denial-of-Service. Go to Servers > *ServerName* > Protocols > SMTP > *Incoming Virtual Server* > Properties and limit the number of connections to 100 (should be a number that you know based

on your typical email traffic). On Messages tab, set maximum message size to the biggest size any mailbox in your organization will accept from the Internet. Make the session size slightly bigger then the maximum message size. Set messages per connection to 20, and number of recipients to slightly larger then the number of mailboxes this server is responsible for. On the Delivery tab, under Advanced, change the max mail hop count to 15 or 20.

- Blocking MAIL FROM: Your Domain. Go to Global Settings > Message Delivery > Properties > Sender Filtering tab and check 'Filter messages with blank sender'. Now add a Sender rule for '@yourdomain.com'. Ensure Sender Filtering is enabled on the incoming Virtual Server. Restart the SMTP service.

ISA Server 2004

(Using ISA Server Management)

- SMTP command size limiting. Under add-ins > SMTP Filter > SMTP Commands tab. (using recommended settings and not aggressive) disable AUTH, disable HELP, change NOOP bytes to 1024, add and disable X-EXPS, add and disable X-LINK2STATE, add and set 50 bytes to XEXCH50, add and disable ETRN. Click OK and 'apply' the new configuration.
- Enable IDS features of ISA. Enable all features under General > Enable Intrusion Detection and DNS Attack Detection. Click OK and 'apply' the new configuration.

McAfee SecurityShield 1.0

You can configure the anti-virus settings to your liking, as we will not be discussing most of them here. Be sure to create an ISA access rule to allow FTP out from the ISA server so SecurityShield can get its updates.

Summary

After finishing the implementation of Exchange 2003, ISA 2004 and SecurityShield 1.0, a mail system will then be a very narrow surface of attack for Internet-born attacks over TCP port 25. DMZ separation, SMTP command limiting, anti-virus, anti-UCE, and connection limiting have all been addressed. The resulting system is one of the most advanced yet secure SMTP systems that can be easily built and maintained on Windows systems.

References

Internet Software Marketing Ltd. ISAserver.org. Feb 9, 2005. <http://www.isaserver.org>

Internet Software Marketing Ltd. Msexchange.org Feb 9, 2005. http://www.msexchagne.org

Robichaux, Paul. "A New Kind of Attack". Windows IT Pro. Oct 9, 2003. Feb 9, 2005. <http://www.winitpro.com/Articles/ArticleID/40507/40507.html>

Landesman, Mary. "Mass Attack of SoBig.F" About, Inc. August 2003. Feb 9, 2005. <http://antivirus.about.com/cs/emailviruses/a/sobig.htm>

Microsoft. "Vulnerability in Exchange Server Could Allow Arbitrary Code Execution (829436)". October 15, 2003. Feb 9, 2005. <http://www.microsoft.com/technet/security/bulletin/MS03-046.mspx>

Microsoft. Using the ISA Server 2004 SMTP Filter and Message Screener. June 7, 2004. Feb 7, 2005. <http://www.microsoft.com/technet/prodtechnol/isa/2004/plan/smtpfilter.mspx>

Gromov, Dmitry. "Installing Tar Pit fix". DGCom's Logging space. Dec 10, 2004. Feb 7 2005. <http://spaces.msn.com/members/dgcom/Blog/cns!1pPLTh53lHpzr6ZzbIN6DYHQ!140.entry>

Bulkeley, Debra. "Exchange is the leader, and rightly so". SearchExchange.com. March 22, 2004. Feb 7, 2005. <http://searchexchange.techtarget.com/originalContent/0,289142,sid43_gci956167,00.html>

Bekker, Scott. "After Slow Start, Exchange 2003 Begins to Take Hold". Redomndmag.com. Nov 2004. Feb 7, 2005. <http://www.redmondmag.com/reports/article.asp?EditorialsID=112>

Gonsalves, Antone. "E-mail More Important Than the Phone In Business, Study Shows". TechWeb. April 22, 2003. Feb 7, 2005. <http://www.techweb.com/wire/story/TWB20030422S0008>

Microsoft. "Exchange Server Edge Services Overview". Feb 24, 2004. Feb 9, 2005. <http://www.microsoft.com/technet/prodtechnol/exchange/2003/edgeservices.mspx>

Microsoft. "Definitions of Verbs That Are Used Between 2 Exchange Servers".

June 13, 2003. Feb 9, 2005. <http://support.microsoft.com/kb/812455>

Microsoft. “VRFY Command Does Not Work in Exchange 2000 or in Exchange 2003” Sep 4, 2003. Feb 9, 2005. <http://support.microsoft.com/kb/289521>

Microsoft. “Enhanced Status Codes for Delivery – RFC 1893”. Oct 9, 2003. Feb 9, 2005. <http://support.microsoft.com/kb/256321>

Networksorcery.com. SMTP, Simple Mail Transfer Protocol. Nov 10, 2004. Feb 9, 2005. <http://www.networksorcery.com/enp/protocol/smtp.htm>

Bernstein, D.J. SMTP: Simple Mail Transfer Protocol. April 26, 2001. Feb 9, 2005. <http://cr.yp.to/smtp.html>

Berrueta, David. A practical approach for defeating Nmap OS-Fingerprinting. Feb 9, 2005. <http://voodoo.somoslopeor.com/papers/nmap.html>

The Exchange Team. “MS IT: Leveraging dual SMTP Virtual server approach for Exchange 2003 gateway perimeter system”. You Had Me At EHLO… Microsoft. Jan 24, 2005. Feb 9, 2005. <http://blogs.msdn.com/exchange/archive/2005/01/24/359677.aspx>

Microsoft. Sender ID. Feb 9, 2005. http://www.microsoft.com/senderid

Microsoft “Microsoft Exchange Intelligent Message Filter Deployment Guide” May 25, 2004. Feb 9, 2005 <http://www.microsoft.com/technet/prodtechnol/exchange/2003/library/imfdeploy.mspx>

IC Group, Inc. Sender Policy Framework. Feb 9, 2005. <http://spf.pobox.com>

Microsoft. Microsoft Exchange Server 2003 Security Hardening Guide. Dec 1, 2004. Feb 9, 2005. <http://www.microsoft.com/technet/prodtechnol/exchange/2003/library/exsecure.mspx>

Software References

Fyodor. Nmap. Feb 9, 2005. <http://www.insecure.org/nmap/index.html>

Microsoft. Microsoft Baseline Security Analyzer. Feb 9, 2005. <http://www.microsoft.com/technet/security/tools/mbsahome.mspx>

Microsoft. Exchange 2003. Feb 9, 2005 < http://www.microsoft.com/exchange/>

McAfee. SecurityShield 1.0 for ISA Server. Feb 9, 2005. <http://www.networkassociates.com/us/products/mcafee/antispam/spk_security

shield.htm>

Microsoft. ISA Server 2004. Feb 9, 2005. <http://www.microsoft.com/ISAServer/>

Microsoft. Intelligent Message Filter. Feb 9, 2005. <http://www.microsoft.com/DOWNLOADS/results.aspx?displaylang=en&freeText=Intelligent+Message+Filter>

GFi. GFi MailEssentials. Feb 9, 2005. <http://www.gfi.com/mes/>

Microsoft. "A software update is available to help prevent the enumeration of Exchange Server 2003 e-mail addresses" Knowledge Base Article 842851. Jan 25, 2005. Feb 7, 2005. <http://support.microsoft.com/?kbid=842851>