



Email-Based Threats



Copyright © www.ine.com

Topic Overview

- ▷ Spam
- ▷ Malware
- ▷ Phishing
- ▷ Spear Phishing
- ▷ Threat Statistics

Email-Based Threats: Spam

▷ Spam is unsolicited email that might be:

- ▶ Junkmail (harmless but unwanted)
- ▶ Malicious (designed to trick you into giving private information to people you don't know).

▷ Examples of Spam:

- ▶ Email messages you did not ask for that are from senders you don't know
- ▶ Unsolicited commercial email messages sent in bulk, often to a purchased (or stolen) mailing list that contained your address
- ▶ Counterfeit messages from reliable senders that attempt to trick you into supplying your personal information
- ▶ Misleading messages from people you know whose email accounts have been hacked

Email-Based Threats: Malware

- ▶ Malware is a broad term describing a wide variety of malicious programs.
 - ▶ Malware = **Malicious Software**
- ▶ Designed to compromise computer functions, steal data, bypass access controls, or otherwise cause harm to the host computer.
- ▶ Common forms of email-based malware:
 - ▶ Ransomware
 - ▶ Rootkits
 - ▶ Spyware
 - ▶ Trojan Horse
 - ▶ Virus
 - ▶ Worms



Copyright © www.ine.com

Ransomware is a form of malware that essentially holds a computer system captive while demanding a ransom. The malware restricts user access to the computer either by encrypting files on the hard drive or locking down the system and displaying messages that are intended to force the user to pay the malware creator to remove the restrictions and regain access to their computer.

-

A rootkit is a type of malicious software designed to remotely access or control a computer without being detected by users or security programs. Once a rootkit has been installed it is possible for the malicious party behind the rootkit to remotely execute files, access/steal information, modify system configurations, alter software (especially any security software that could detect the rootkit), install concealed malware, or control the computer as part of a botnet.

-

Spyware is a type of malware that functions by spying on user activity without their knowledge.

-

A Trojan horse, commonly known as a “Trojan,” is a type of malware that disguises itself as a normal file or program to trick users into downloading and installing malware. A Trojan can give a malicious party remote access to an infected computer.

-

A virus is a form of malware that is capable of copying itself and spreading to other computers. Viruses often spread to other computers by attaching themselves to various programs and executing code when a user launches one of those infected programs.

-

Worms are similar to Viruses, but a major difference is that computer worms have the ability to self-replicate and spread independently while viruses rely on human activity to spread (running a program, opening a file, etc). Worms often spread by sending mass emails with infected attachments to users’ contacts.

Email-Based Threats: Phishing

- ▶ Phishing: emails that look like they've come from a legitimate entity but in reality they have not.
- ▶ Intent of phishing is to steal your PII (Personally Identifiable Information).
- ▶ Characterized by emails that contain a generic body without your name and could have been written to anyone.
- ▶ One of the most common entry points for hackers.

Copyright © www.ine.com



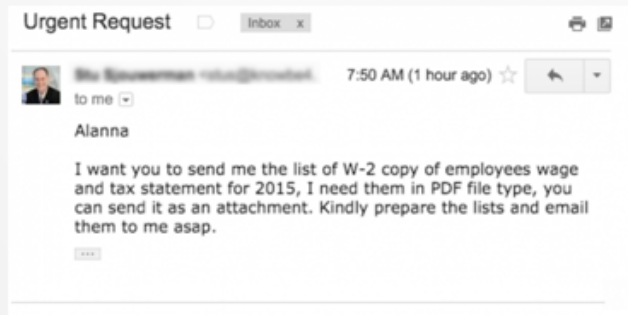
Phishing are emails that have come from a malicious actor with the intent to somehow steal critical information from you such as credit card info, username and password info, etc. Phishing emails are characterized by the fact that they are not addressed directly to you, seem to know nothing about you personally but are more broad in scope.

-

Commonly impersonate a person or organization with a high level of authority—and are urging immediate action.

Email-Based Threats: Spear Phishing

- ▶ **Spear Phishing:** Personal and targeted phishing.
- ▶ Just like phishing, meant to trick you into divulging personal or confidential data for unauthorized use.



Copyright © www.ine.com



Spear Phishing are very similar to regular Phishing emails, except that the attacker has already gained some knowledge about you and makes this email more targeted to you personally. I might be as simple as your name being included in the opening line of the email, or it might contain even more information about you to persuade you that it came from a known, legitimate source.

Threat Statistics

76% of organizations say they experienced phishing attacks in 2017.

Wombat 2018 State of the Phish | [Tweet this stat](#)

By the end of 2017, the average user was receiving 16 malicious emails per month.

Symantec 2018 ISTR | [Tweet this stat](#)

92.4% of malware is delivered via email.

Verizon 2018 DBIR | [Tweet this stat](#)

Copyright © www.ine.com



Almost half of Wombat's "State of the Phish" survey reported that Phishing attacks have been increasing in frequency.

-

According to Symantec's 2018 Internet Security Threat Report (ISTR), a whopping 54.6% of all email is spam. Even more to the point, their data shows that the average user receives 16 malicious spam emails per month, which leads to some scary math.

-

One of the biggest changes has been a shift away from using malicious attachments to a preference for utilizing malicious URLs, instead. In 2017, for example, Proofpoint reported [3 out of 4 malspam emails delivered malware via attachments](#). Fast-forward to Q1 2018 and the firm's data showed that emails with malicious links outnumbered emails with malicious attachments 4 to 1.

-

Quotes are courtesy of <https://blog.barkly.com/phishing-statistics-2018>



The Email Pipeline

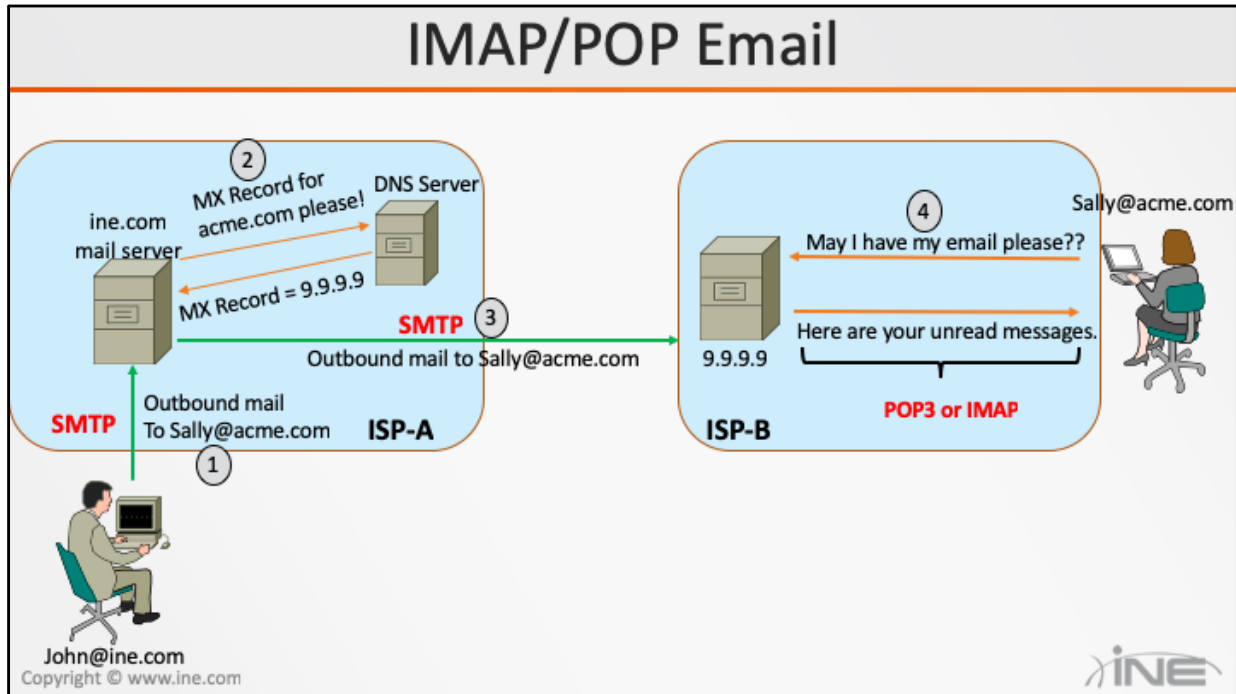


Copyright © www.ine.com

Topic Overview

▶ Review Of The Email Pipeline

IMAP/POP Email

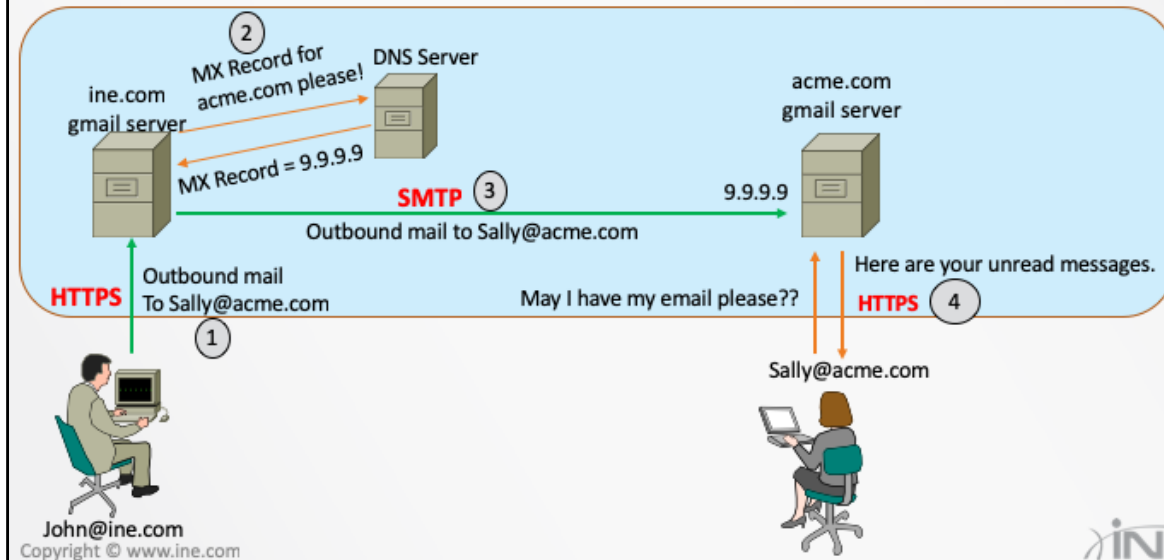


In this example, you would open up an email application on your laptop or PC to send-and-receive emails. This is NOT a web-based solution (like gmail or yahoo mail) but a client-based software solution.

POP3 is used when you are actually downloading the email from the mail server onto your laptop. At that point, the email no longer resides on the server. IMAP is used when you want to be able to view-and-manipulate your emails from multiple clients (smartphone, tablet, PC, etc). In this case, the emails always remain on your mail server, and IMAP is used to view, manipulate, and delete them. Think of IMAP as more of a command language...you're sending IMAP commands to the mail server whereas POP3 is a download language.

If using a web-based email client then when you download emails you're not REALLY downloading the emails (onto your computer) but you're downloading a website (using HTTPS most likely), and then viewing and manipulating the emails on that website. To view and manipulate these emails you are using IMAP. However, SMTP was used to push the email from the sender's Email Server to the Gmail server.

HTTPS-Based Email



The main thing to note in both of these topologies is where the SMTP transactions are happening? This will become relevant when we introduce the Cisco ESA...which only works by inspecting SMTP messages (not POP or IMAP transactions).



Cisco ESA Introduction & Features



Copyright © www.ine.com

Topic Overview

- ▶ Cisco ESA Introduction
- ▶ How ESA Fights Spam, Viruses & Malware
- ▶ ESA Incorporation Of AMP
- ▶ Introducing Cisco Talos
- ▶ Data Loss Prevention (DLP) With The Cisco ESA

Email Security Options

▶ Cisco ESA = Email Security Appliance

▶ Cisco offers several ESA solutions:

- ▶ Cloud-based
- ▶ On-Premises
- ▶ Hybrid



▶ Utilizes the AnySync Operating System.

▶ Filters positively identified spam and quarantines or discards email that has been sent from untrusted or potentially hostile locations. Antivirus scanning is applied to emails and attachments from all servers to remove known malware.

Copyright © www.ine.com



The Cisco ESA is a type of firewall and threat monitoring appliance for SMTP traffic, that means that its ideal position in the network is between MX servers.

-

Cloud-based email security represents a hosted service which can scan emails from mobile employees, and employees working at any location. Email security instances are located in multiple Cisco data centers

Hybrid-based email security is when you have one-or-more ESAs on your premises for scanning of all outgoing email and also utilize a cloud-based ESA for scanning of all incoming email.

Fighting Spam, Viruses & Malware

- ▶ The Cisco ESA has several methods of protecting inbound and outbound email;
- ▶ Filtering SPAM
 - ▶ Reputation-based filtering
 - ▶ Context-based filtering
- ▶ Fighting viruses and malware
 - ▶ Outbreak filters
 - ▶ Antivirus signatures
 - ▶ Outbound email scanning

Copyright © www.ine.com



Reputation filters provide the first layer of defense by looking at the source IP address of the email server and comparing it to the reputation data downloaded from Cisco.

-

Context-Based Filtering: These antispam filters in the appliance inspect the entire mail message, including attachments, analyzing details such as sender identity, message contents, embedded URLs, and email formatting. Using these algorithms, the appliance can identify spam messages without blocking legitimate email.

-

Outbreak filters (for fighting viruses and malware) are similar to reputation filters (for fighting SPAM) in that they are downloaded from the Cisco cloud and contain the latest list of known, malicious email servers. Emails received from a known, malicious server are kept in quarantine until the antivirus signatures are updated to counter the current threat.

-

Antivirus signatures scan quarantined emails.

ESA Incorporation Of AMP

- ▶ The Cisco ESA protects against Spam, Malware and Viruses by utilizing AMP.
- ▶ Advanced Malware Protection (AMP)
 - ▶ Utilizes the cloud security intelligence networks of Cisco Talos
 - ▶ Assists both before, during, and after an attack.
- ▶ Features of AMP
 - ▶ File Reputation
 - ▶ File Sandboxing (quarantining)
 - ▶ File Retrospection

Copyright © www.ine.com



File Reputation: captures a fingerprint of each file as it traverses the Cisco email security gateway and sends it to the AMP cloud-based intelligence network for a reputation verdict.

-

File sandboxing enables you to analyze unknown files that are traversing the Cisco email security gateway. A highly secure sandbox environment makes it possible for Cisco AMP to gather precise details about a file's behavior and to combine that data with detailed human and machine analysis to determine the file's threat level.

-

File retrospection solves the problem of malicious files that pass through perimeter defenses but are later deemed a threat. It allows you to track where a malicious file went, and all devices that either passed that file on, or installed that file.

Cisco Talos

- ▶ “The Talos Security Intelligence and Research Group (Talos) is **made up of leading threat researchers** supported by sophisticated systems to **create threat intelligence** for Cisco products that detects, analyzes and protects against both known and emerging threats. Talos maintains the official rule sets of Snort.org, ClamAV, SenderBase.org and SpamCop.”
- ▶ “**Talos is the primary team that contributes threat information to the Cisco Collective Security Intelligence (CSI) ecosystem.** Cisco CSI is shared across multiple security solutions and provides industry-leading security protections and efficacy. In addition to threat researchers, CSI is driven by intelligence infrastructure, product and service telemetry, public and private feeds and the open source community.”

Quotes courtesy of <https://blogs.cisco.com/author/talos>

Copyright © www.ine.com



A logical question one might ask is, “If all of these Cisco security solutions rely on regular and frequent updates from the Cisco Cloud to keep up-to-date on current and emerging threats...where exactly does this information come from and can I trust it?”

-

Talos updates assist your ESA within identifying SPAM, Viruses and Malware. These updates occur every 3-5 minutes.

ESA Enforcement Of DLP

▶ Email data loss prevention (DLP)

- ▶ Content-level scanning of email messages and attachments to detect inappropriate transport of sensitive information.
- ▶ Built-in rules help identify PII in outgoing email.
- ▶ Ability to create/edit your own rules.

▶ What happens when DLP is detected?

- ▶ You configure the action(s) you want the ESA to take which can include:
 - ▶ Quarantine the email
 - ▶ Drop the email
 - ▶ Encrypt the email

Copyright © www.ine.com



Examples of items that are scanned to protect against DLP include personal identifiers (credit cards or Social Security numbers) or corporate intellectual property (internal or confidential documents).

-

Remember that the ESA is NOT in the pipeline of emails that are exchanged within your company, so it has no ability to scan those messages because it never sees them.

-

Mail policies are created that match against the senders of messages, recipients of messages, or both. So you can have different DLP settings applied against your CEO than against your Marketing Intern.

-

The ESA comes with several, pre-defined DLP templates that you can use or modify. Or you can choose just to create your own filters.



Cisco ESA Deployment Options



Copyright © www.ine.com

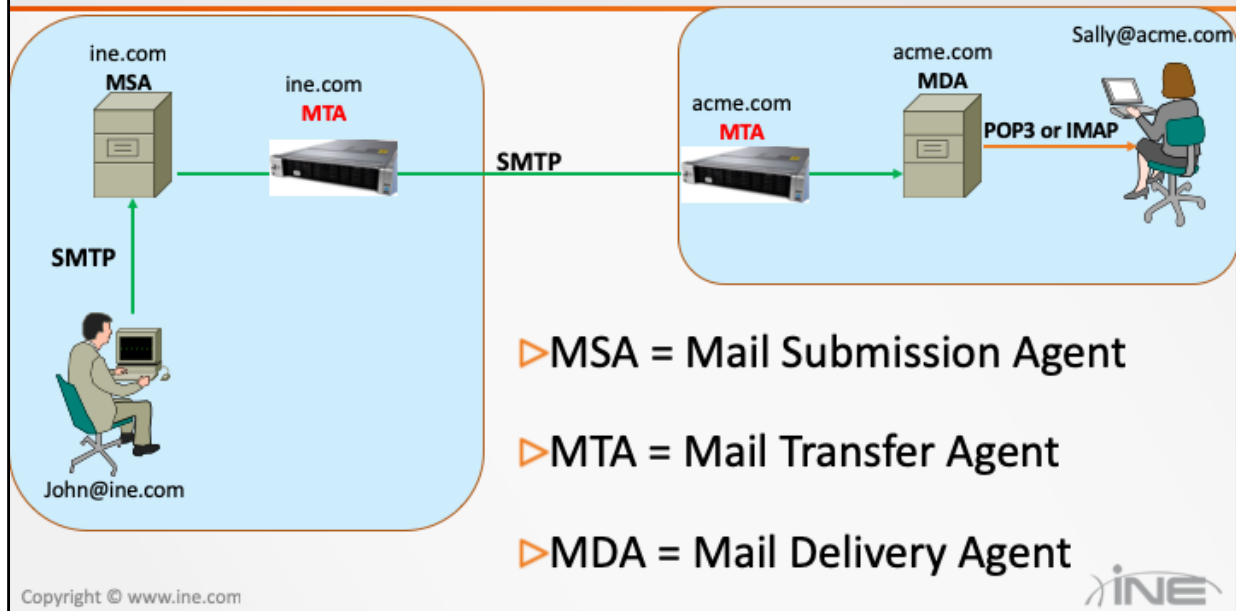
Topic Overview

- ▶ Where The ESA Fits
- ▶ Single-Interface Deployment
- ▶ Dual-Interface Deployment

ESA Deployment

- ▶ Cisco ESA listens on SMTP (TCP port 25)
 - ▶ Does not support POP3
 - ▶ Does not support IMAP
- ▶ ESA is deployed as physical or virtual appliance
- ▶ ESA is deployed as an MTA in the email pipeline

Where The ESA Fits



What you see here is the email pipeline. The Cisco ESA does not speak IMAP or POP3. As such, an end-user would not directly interact with the ESA to download their emails (that is the job of the MDA).

When sending outgoing email, the end-user utilizes SMTP, which the ESA does support. However, the ESA is not designed to function as an MSA so deployment guidelines always display a separate box serving as the MSA (such as an Exchange Server) with the ESA serving as only an MTA.

Key Points About ESA Deployment

- ▶ The Cisco ESA is deployed as the **first** email server for mail coming from the Internet.
- ▶ The Cisco ESA is deployed as the **last** email server for mail going to the Internet.

ESA Single-Interface Deployment

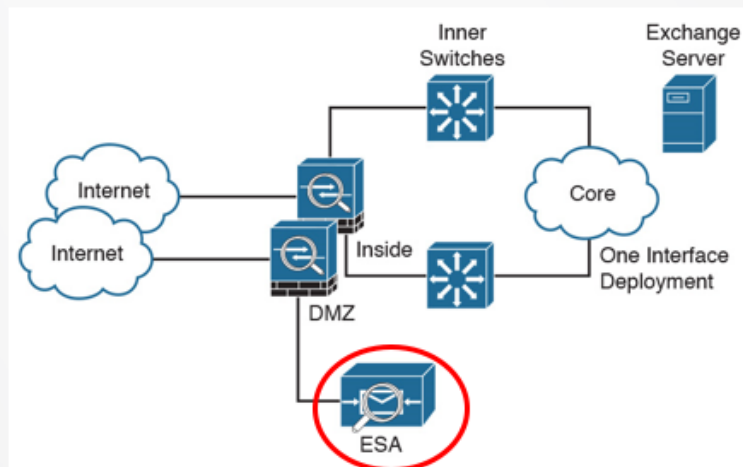


Image courtesy of "31 Days Before Your CCNA Security Exam" by Cisco Press

Copyright © www.ine.com



This is frequently referred to as a "single-arm" deployment.

- Notice that in this deployment, a single interface is connected on your ESA to your Firewall. The firewall's interface would be placed into the DMZ and an ACL or other rule would have to be implemented so that, after the ESA had received emails from the Internet and deemed them safe, it could initiate an inbound connection to the MDA (Mail Delivery Agent) which is the Exchange Server in this graphic.

- This is the most common deployment of an ESA and most Cisco Design Guides and Deployment Guides utilize this model.

ESA Dual-Interface Deployment

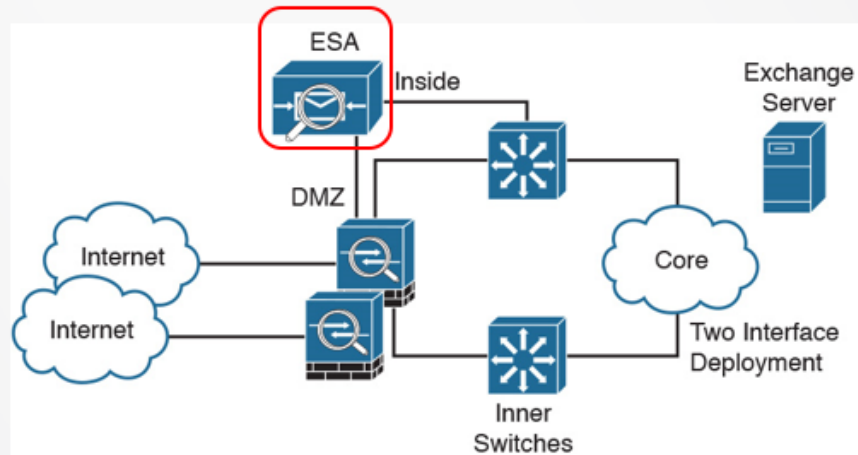


Image courtesy of "31 Days Before Your CCNA Security Exam" by Cisco Press

Copyright © www.ine.com



While it is certainly possible to deploy your ESA using dual-interfaces, most official documents do not reflect this approach.

-

My guess? By having an interface on your ESA connected to the "inside" interface of your Firewall (the interface with the least security restrictions) you are opening yourself to the possibility that, if someone compromised your ESA from the Internet and gained access to it, they would then have easy access to your internal network...essentially bypassing the firewall.



Cisco ESA Processing Rules

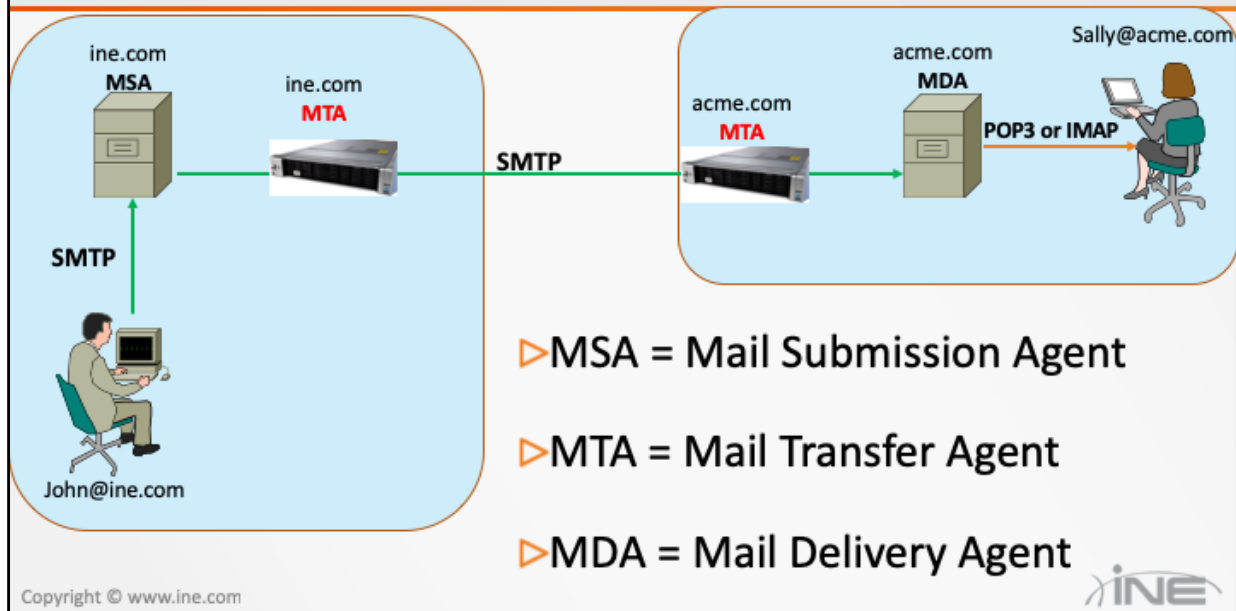


Copyright © www.ine.com

Topic Overview

- ▶ Overview of ESA Deployment
- ▶ Incoming Email & ESA Processing Rules
- ▶ Outgoing Email & ESA Processing Rules

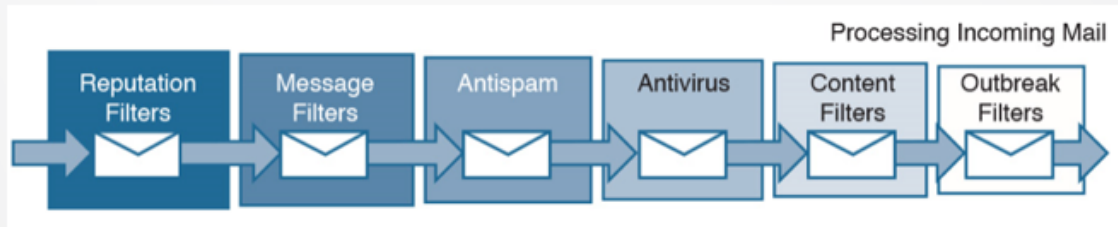
Where The ESA Fits



What you see here is the email pipeline. The Cisco ESA does not speak IMAP or POP3. As such, an end-user would not directly interact with the ESA to download their emails (that is the job of the MDA).

When sending outgoing email, the end-user utilizes SMTP, which the ESA does support. However, the ESA is not designed to function as an MSA so deployment guidelines always display a separate box serving as the MSA (such as an Exchange Server) with the ESA serving as only an MTA.

Incoming Email ESA Pipeline



▷ **R**eliable **M**essages **A**re **A**lways **C**onsidered **O**ptimal

Image courtesy of "31 Days Before Your CCNA Security Exam" by Cisco Press

Copyright © www.ine.com



Above I'm showing a mnemonic that I developed that helped me to remember the stages of this pipeline.

- Reputation filters are for Spam prevention. Reputation filtering is the first layer of spam protection, allowing you to control the messages that come through the email gateway that are based on sender trustworthiness as determined by the Cisco SenderBase Network.

- Message filters are special rules you've manually put in place that are unique to your organizational policy.

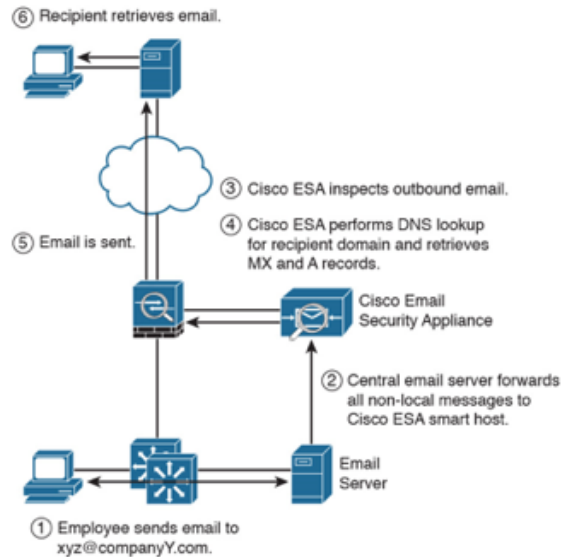
- Antispam: Uses contextual information to determine the email sender's reputation, the message content, the message structure to determine if email contains spam or not.

- Virus detection utilizes Sophos or McAfee antivirus.

- Content filters are used to filter specific file types or content. These are manual filters that you enable and customize.

- Outbreak Filters: Newly released viruses that do not have a published ID can be blocked by stopping files with the infected file's characteristics.

ESA & Outgoing Emails



Copyright © www.ine.com

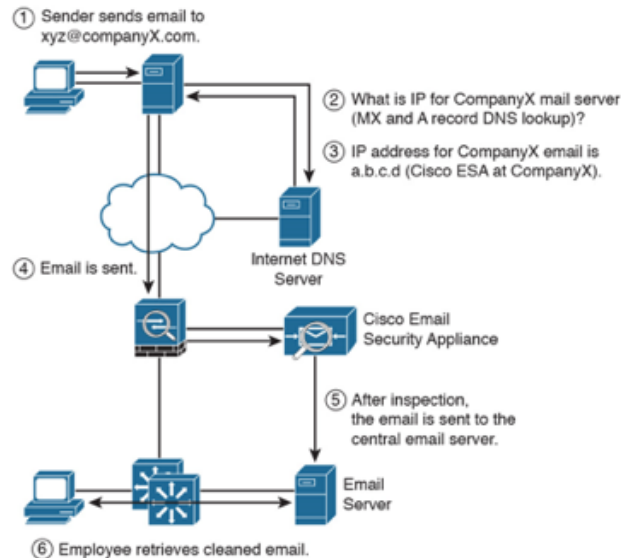
Image courtesy of "31 Days Before Your CCNA Security Exam" by Cisco Press



In this topology, the internal Email Server will need to be configured to forward all non-local outgoing emails to the ESA.

When receiving outgoing email, after processing it to ensure no security rules have been violated, just like any other MTA the Cisco ESA will need to create a DNS Query for the IP address of the next MTA in the email chain. If you are using a corporate, internal DNS server then your Firewall will also need rules to allow DNS transactions from DMZ-to-Inside interfaces.

ESA Receiving Mail



Copyright © www.ine.com

Image courtesy of "31 Days Before Your CCNA Security Exam" by Cisco Press



Notice that in order for this to work, all global DNS entries for your company's MX and A-Records should point to the ESA's IP address (not your actual, internal Email Server).

Additionally, several Firewall policies will have to be implemented such as:

- Allowing SMTP to flow from Outside-to-DMZ

- Allowing SMTP to flow from DMZ-to-Inside

- Allowing HTTP and HTTPS to flow from Outside-to-DMZ only when sourced from...or going to...the Cisco Cloud (these protocols are used by the ESA to send-and-receive security intelligence updates from Cisco).

Outgoing Email ESA Pipeline

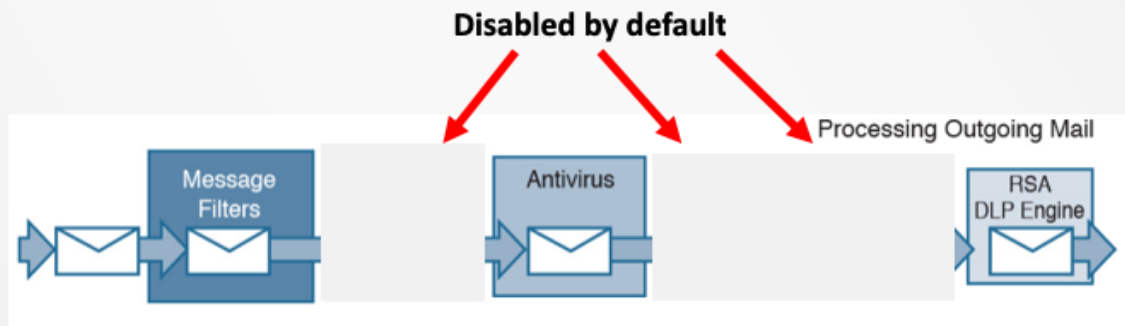


Image courtesy of "31 Days Before Your CCNA Security Exam" by Cisco Press

Copyright © www.ine.com



Notice that Reputation-based filtering is not in the pipeline for outgoing emails.



Email Security Evasion Techniques



Copyright © www.ine.com

Topic Overview

- ▶ Polymorphism
- ▶ Obfuscation
- ▶ Sleep Timers

Detection Evasion

- ▶ No single security solution is 100% effective at blocking malicious emails.
- ▶ There are several, known techniques the Malicious Actors use to avoid detection:
 - ▶ **Obfuscation**: techniques to stay hidden during infection and operation to prevent removal and analysis such as;
 - ▶ Obscuring filenames
 - ▶ Modifying file attributes
 - ▶ Operating under the pretense of legitimate programs and services
 - ▶ **Polymorphism**: a type of malware that constantly changes its identifiable features in order to evade detection
 - ▶ **Sleep Timers**: Malware that intentionally induces lengthy delays between malicious instructions and responses so as to time-out detection techniques.

Copyright © www.ine.com



Sleep Timers: When malware is installed on a system and makes a request of a malicious site on the Internet, typically the response comes back quickly. Most malware detection algorithms aren't designed to wait long periods of time between these requests and subsequent responses. Therefore when malware is intentionally designed to "go to sleep" for a period of time after making a request, the detection algorithms may just timeout and not be aware of the incoming response seconds (or minutes or hours) later.

-

Antivirus emulators and automated analysis systems are designed not to waste CPU cycles and resources. "They are designed to handle tens of thousands of possibly malicious samples, and can't afford to wait on a file that apparently does nothing." - <https://www.csoonline.com/article/2132891/malware-cybercrime/-sleeper--malware-like-nap-trojan-nothing-new.html>

Obfuscation

- ▶ Many anti-malware programs will parse through any downloaded code, attachments, etc looking for recognizable strings:
 - ▶ Known, malicious URLs
 - ▶ Known, malicious words (like “bot”)
- ▶ Obfuscation (in the context of software) is a technique that makes binary and textual data unreadable and/or hard to understand.
- ▶ Can be as simple as manipulating a few bits to as complex as employing cryptographic techniques.

Examples Of Obfuscation

►Applying an Exclusive OR (XOR) operation to hide data:

```
00132E0 61 69 74 46 6F 72 53 69 6E 67 6C 65 4F 62 6A 65 altForSingleObj
00132F0 63 74 00 00 00 00 00 00 00 00 00 00 00 00 00 ct
0013300 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0013310 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0013320 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0013330 00 21 21 21 6F 74 74 74 35 21 35 27 64 64 60 62 ttf0x21h1:dd
0013340 78 30 36 26 21 21 35 21 35 27 78 36 38 38 78 20 (-:5tth1:({6:0x2
0013350 37 38 38 3C 6C 6C 74 78 35 3E 74 37 38 21 78 38 70:cl1z(:>27:t{
0013360 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

XOR encoded against a value of 0x55

```
00132E0 61 69 74 46 6F 72 53 69 6E 67 6C 65 4F 62 6A 65 altForSingleObj
00132F0 63 74 00 00 00 00 00 00 00 00 00 00 00 00 00 ct
0013300 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0013310 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0013320 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0013330 68 74 74 78 38 2F 2F 74 61 74 6F 72 31 31 35 37 http://tator135
0013340 2E 68 6F 78 74 67 61 74 6F 72 2E 63 6F 60 2F 7E .hostgator.com/
0013350 62 65 6E 69 39 39 2F 2E 6F 60 2F 62 6F 74 2E 65 ben199/.ok/bot.e
0013360 74 65 00 00 00 00 00 00 00 00 00 00 00 00 00
```

XOR decoded

►Base64 Encoding

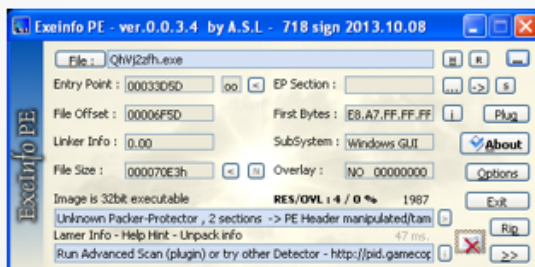
```
1 Plain-text: C:\WINDOWS\system32\svchost.exe
2 Base64 encoded: QzpcV010RE9XU1xeXNOZW0zM1xzdmNob3N0LmV4ZQ==
3 Base64 alphabet: ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/
4
```

Examples Of Obfuscation

▶ ROT13 (uses simple letter substitution)

```
1 Plain-text: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
2 ROT13 output: UXRL_YBPNY_ZNPUVAR\Fbagjner\Zvpebfbag\Jvaqbjf\Pheeragirefvba\Eha
3 Lookup Table: ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz
4               NOPQRSTUVWXYZABCDEFGHIJKLMnopqrstuvwxyzabcdefghijklm
5
```

▶ Runtime Packers



Copyright © www.ine.com



ROT is an ASM (“Assembly Language”) instruction for “rotate”, hence ROT13 would mean “rotate 13”. ROT13 uses simple letter substitution to achieve obfuscated output.

A packer is piece of software that takes the original malware file and compresses it, thus making all the original code and data unreadable. At runtime, a wrapper program will take the packed program and decompress it in memory, revealing the program’s original code.

Malware will make use of commercially available or “homebrewed” packers or cryptors to conceal its malicious code.

Polymorphism

▶ Polymorphic Viruses contain two main elements:

- ▶ Encrypted payload
- ▶ Mutation engine

▶ Encrypted Payload;


- ▶ Hides the malicious payload from scanners and threat detection software
- ▶ Threat detection must resort to identify the virus by its decryption routine

▶ Mutation Engine;

- ▶ Randomly creates a new decryption routine so that when the virus moves to the next target, it appears to be a different file to scanners.
- ▶ May also generate a new filename for the malicious code.

Polymorphic Viruses

- ▶ The first known polymorphic virus was called 1260, or V2PX, and it was created in 1990 as part of a research project.
 - ▶ The author, computer researcher Mark Washburn, wanted to demonstrate the limitations of virus scanners at that time.
- ▶ Recent examples:
 - ▶ Storm Worm
 - ▶ Virlock Ransomware
- ▶ Defense against;
 - ▶ Implement software that utilizes machine learning and behavior-based analytics rather than signature detection.
 - ▶ Employ multiple and diverse layers of information security measures.

Many quotes on this page taken from <https://searchsecurity.techtarget.com/definition/polymorphic-malware>
Copyright © www.ine.com 

Storm Worm: featured a backdoor Trojan and was first discovered in 2007. Spread via email and, once executed, turned infected systems into Bots. This worm was able to change its characteristics every 10-30 minutes.

-
The Virlock ransomware family, which was first discovered in 2014, is considered the first instance of polymorphic ransomware.

-
97% of malware infections employ polymorphic techniques.

-
Machine learning algorithms focus on anomalous behavior of unknown programs as well as other static characteristics such as file names and API calls.

Virlock Ransomware

Unauthorized or pirated software has been detected. Your system has been blocked.



Willful copyright infringement is a federal crime that carries penalties of up to five years in federal prison, a \$250,000 fine, forfeiture and restitution (17 U.S.C. § 506, 18 U.S.C. § 2319)

As a first-time offender you are required by law to pay a fine of 250 USD
If the fine is not paid within three days, a warrant will be issued for your arrest, which will be forwarded to your local authorities.
You will be charged, fined, convicted for up to 5 years.

There are two ways to pay a fine:

1. You can pay your fine online through BitCoin. BitCoin is available nationwide.
Click the tabs below to find the nearest ATM or exchange.
Your computer will be unlocked after you make your payment.
2. (Offline Option) You can come to your local courthouse and pay your fine at the 'Cashiers' window.
Your computer will be unlocked within 4-5 working days.

To regain access now, transfer BitCoin to the following address (click to copy):
172qj3V7g3uqPTXPhIntevkshu8NgGU

After the payment is finished enter Transfer ID below.

Amount

Transfer ID

BTC 0.378

 Online fine payments are securely processed by Chase Paymentech.

NOTE: Files on this computer, including network files, have been encrypted and disabled. Files will be restored after the fine is paid.
Do not attempt to remove this message. This will damage your files, hardware and Windows installation beyond recovery.

[Payment](#) [How to pay a fine](#) [Find nearest ATM](#) [Online Exchanges](#) [Internet Browser](#) [Notepad](#)

[View encrypted files](#)

Office of Criminal Investigations - U.S. Department Of Justice
Cybercrime Investigators Unit (CUI)



Email Encryption Techniques



Copyright © www.ine.com

Topic Overview

- ▶ What Is Email Encryption & Why Use It?
- ▶ Transport Level Encryption
- ▶ End-To-End Encryption
- ▶ Email Encryption With The Cisco ESA

Email Encryption

- ▶ Emails are not encrypted by default.
- ▶ When using a native email client (like MS Outlook) IMAP or POP3 transactions between you and the email server are unencrypted.
- ▶ When using a web-based email service (like Gmail);
 - ▶ IMAP transactions are encrypted by SSL/TLS
 - ▶ SMTP messages between mail exchange points and servers may-or-may-not be encrypted.
- ▶ Securing email messages and attachments with encryption provides for email confidentiality end-to-end.

Email Encryption Deployments

- ▶ There are two, general ways to implement email encryption.
 - ▶ Transport level encryption
 - ▶ End-to-end encryption

Transport Level Encryption

- ▶ Mail transactions between email servers are encrypted
- ▶ Email transactions between end-user and mail server may also be encrypted
- ▶ **Positives:**
 - ▶ No special user-interaction required
 - ▶ Mitigates an eavesdropper snooping on the communication between mail servers
 - ▶ Easy to implement automatic encryption/decryption on all emails between customer sites.
- ▶ **Negatives:**
 - ▶ Does not provide end-to-end encryption
 - ▶ If mail server is compromised, email confidentiality is compromised.
- ▶ **Example protocol(s):**
 - ▶ STARTTLS

Copyright © www.ine.com



The encrypted message is revealed to, and can be altered by, intermediate email relays. In other words, the encryption takes place between individual SMTP relays, not between the sender and the recipient.

-

This has both good and bad consequences. A key positive trait of transport layer encryption is that users do not need to do or change anything; the encryption automatically occurs when they send email. In addition, since receiving organizations can decrypt the email without cooperation of the end user, receiving organizations can run virus scanners and spam filters before delivering the email to the recipient.

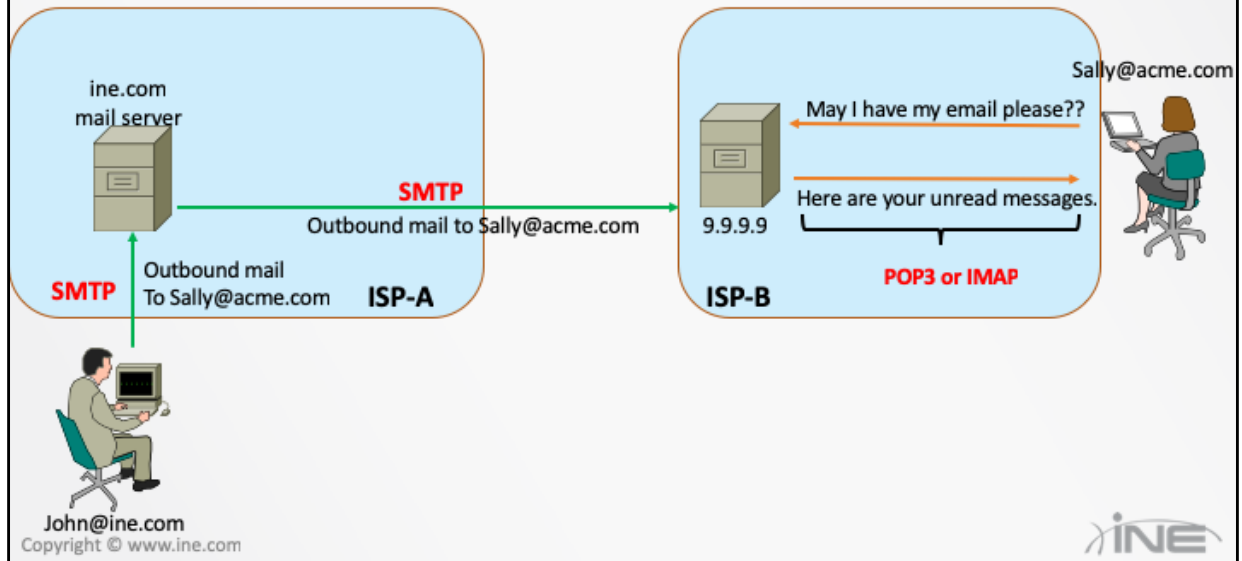
-

However, it also means that the receiving organization and anyone who breaks into that organization's email system (unless further steps are taken) can easily read or modify the email.

-

Google was an early adopter of STARTTLS and now reports that on GMail 90% of incoming email and 90% of outgoing email was encrypted using STARTTLS by 2018-07-24

Email Pipeline



End-To-End Encryption

- ▶ Data is encrypted and decrypted only on the end points.
- ▶ Emails become unreadable to service providers in transit.
- ▶ Examples of end-to-end email encryption protocols:
 - ▶ Bitmessage
 - ▶ GNU Privacy Guard (GPG)
 - ▶ Pretty Good Privacy (PGP)
 - ▶ S/MIME
 - ▶ OpenPGP
- ▶ The methods above require an exchange of Public Keys
 - ▶ Requires users to set up public/private key pairs and make the public keys available widely.

Copyright © www.ine.com

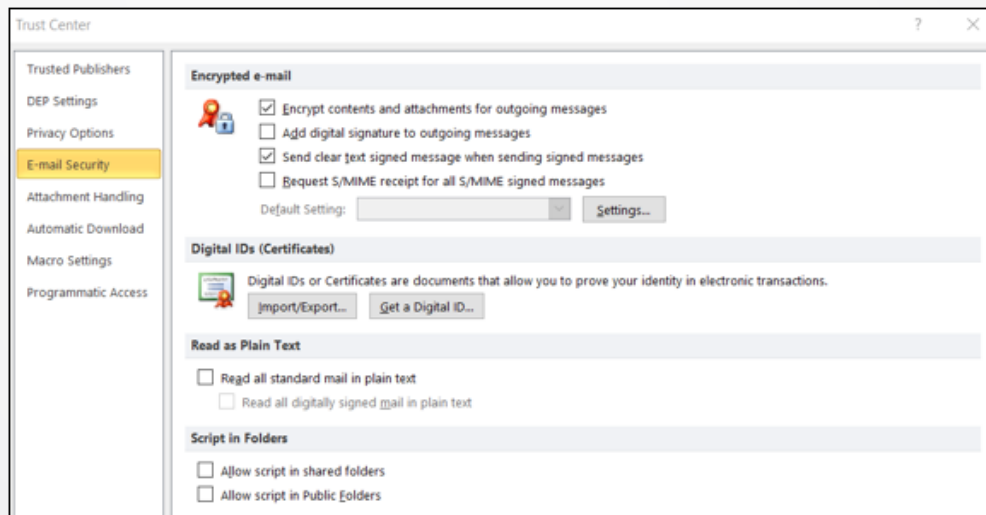


First generation email encryption products rely on PKI, which can be complex and difficult to maintain. Often, users would send the wrong Public encryption key to recipients of their emails. And sometimes, an email user wouldn't have a keypair at all, so they would have to be walked through the process of creating one.

-

Most corporate email encryption services utilize gateway appliances (like the Cisco ESA) to encrypt/decrypt emails for them which keeps all of the key management behind the scenes.

Example Of Encryption Setup



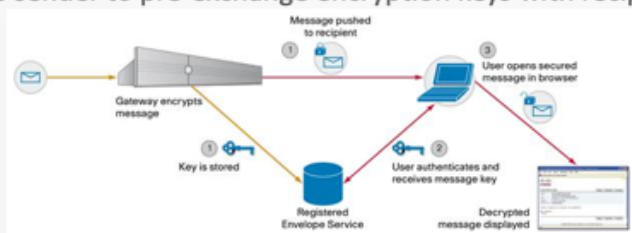
Copyright © www.ine.com



Here you can see an example of configuring Microsoft Outlook for email encryption. Notice that one of the requirements is that you must have your own digital certificate...and you must be able to retrieve the Digital Certificates of other end-users with whom you wish to exchanged encrypted emails. The exchanges of Certificates is what allows you to exchange your Public Encryption Keys.

Email Encryption With Cisco ESA

- ▶ The Cisco Email Security Appliance can be configured to encrypt/decrypt emails.
- ▶ This is considered Transport Level Encryption
- ▶ Utilizes the Cisco Registered Envelope Service
 - ▶ Cloud-based encryption-key service
 - ▶ Encrypted messages can be received by any user
 - ▶ Does not require sender to pre-exchange encryption keys with recipients



Copyright © www.ine.com



The Cisco Registered Envelope service provides some useful features that can be taken advantage of:

Guaranteed read receipts allow users to know exactly when a message was viewed by each recipient.

Message expiration and recall prevents mistakenly sent messages from being opened and automatically secures old messages. The message may be recalled at any time.

Authentication and key delivery typically occurs by identifying user credentials. When a recipient has been authenticated, the key for that message is released and the recipient gets access to the message.

