**Cisco ESA Overview**

(Cisco ESA is a type of firewall and threat monitoring appliance for SMTP traffic, that scans and filters malicious content included in the email messages sent in or out of the organization's networks)

* It is all-in-one appliance defends against spam, advanced malware, phishing, and data loss.
* Cisco ESA scans for malicious threats in email messages by performing deep inspection on the attachments, embedded URLs, and email body content.

(Note ++: When an email with an attachment is received, Cisco ESA inspects the attachment before delivering the email to the user inbox. If a threat is detected, you can configure Cisco ESA to discard the email in its entirety, to forward the email without the attachment, or to rewrite the email subject header with a warning (for example: [Warning: Suspect Attachment]).

* Key email security features of cisco ESA:
  + **threat defense:** provides effective protection against email-transported threats
  + **data security:** Data security offers effective, accurate data loss prevention (DLP) policy enforcement, and email encryption
  + **manageability:** Universal device support, system overview dashboard, and detailed message tracking can all help in better manageability of email traffic

**Cisco ESA AsyncOS Architecture**

* All Cisco ESAs are powered by the unique Cisco AsyncOS for high performance and security
* Cisco Security Management Appliance (SMA): implementing by Cisco ESA AsyncOS to allows you to consolidate reporting, tracking, and quarantine management for multiple Cisco ESAs

**Two major threats to your email:**

* **A flood of unsolicited and unwanted email, called spam**, that wastes your time due to high volume and uses valuable resources such as bandwidth and storage.
* Malicious email, which comes in two basic forms:
  1. **Embedded attacks, which include viruses and malware** that perform actions on the end device when clicked.
  2. T**argeted or directed attacks, such as phishing attacks**, which try to mislead you into releasing sensitive information such as credit card numbers, social security numbers

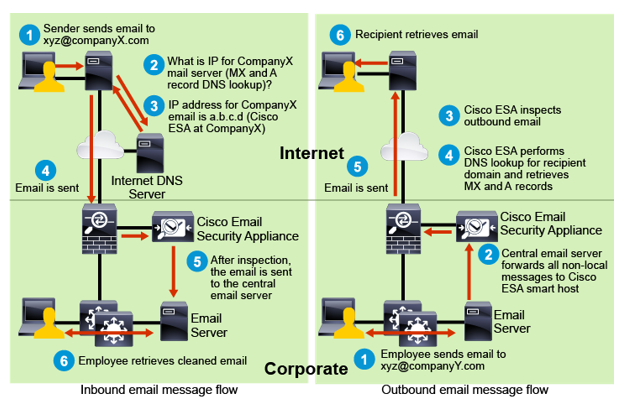
**To protect the email infrastructure:**

* Inbound email is filtering to help prevent spam and malicious mail from being delivered to users.
* Outbound email filtering provides the same benefits as the inbound mail filtering. It prevents malicious email content to be sent to outside recipients

Two different methods to filter spam and combat against phishing of Cisco ESA:

* **Reputation-based filtering:** This type of filtering relies on the likelihood that if a server is a known spam sender, it is more likely that email coming from that server is spam. Reputation filters provide the first layer of defense by looking at the source IP address of the email server and comparing it to the corresponding reputation score downloaded from Cisco SenderBase for the same server
* **Context-based filtering:** These antispam filters in Cisco ESA inspect the entire mail message, including attachments, analyzing details such as sender identity, message contents, embedded URLs, and email formatting.
* If the Cisco AMP feature is enabled on the Cisco ESA appliance, it can also be used for inspecting malware in a more advanced and detailed approach.

**Integrating Cisco ESA into Existing Network**



* Cisco ESA: Acting as a **Mail Transfer Agent (MTA)** within the email-delivery chain. Another name for an MTA is mail relay.

**Implementation options of cisco email security:**

**On-premises solution: Cisco ESA**

* You can deploy Cisco ESA in your organization as a physical (preferred option for large deployments) or virtual appliance (In small deployments).
* . Cisco ESA can be deployed with a single physical interface to transfer emails to and from both the internet and the internal mail servers.
* If desired, two physical interfaces can be used as well, one for email transfer to and from the internet, and another for email communications to the internal mail servers

**Cloud-based solution: Cisco CES**

* Cisco offers a cloud-based solution that is a complete and highly reliable service with software, computing power, and support.
* You get outstanding (exceptionnelle) protection with little administrative overhead and no onsite hardware to monitor and manage.

**Hybrid solution: Cisco ESA and CES**

* The hybrid solution gives you the benefits of the cloud-based email security and provides advanced outbound control of encrypting messages and onsite DLP.
* The cloud-based email security is used for inbound email inspection, while the on-premises Cisco ESA appliances for outbound email inspection.

**SMTP (Simple Middle Transfer Protocol) OVERVIEW**

* SMTP is a communication protocol for passing email between email servers
* it's typically going to occur leveraging TCP over port 25.
* A request and response dialog is going to be used between the client and the server.
  + the SMTP session consists of some commands originated by an SMTP client.
  + And then there's going to be three-digit codes that define the server responses that are actually going to be sent to the client.
* Each message contains envelope **headers:**
* **MAIL FROM**: identifies the sender address
* **RCPY TO:** identifies the recipient address
* We use DNS to get information about multiple records types: **MX record**: provides FQDN for the domain specified in the recipient email address; **A record** provide mapped public ip address for the FQDN
* SMTP heavily relies on the DNS records which provide information about the destination mail servers to which the emails should be sent
* Cisco ESA has the role of the MTA that is responsible for receiving and sending email messages

**Cisco ESA High Availability**

* you can achieve additional resiliency by adding a second Cisco ESA
* High availability is accomplished by enabling two MX records and two A records in the DNS that will point to the two deployed Cisco ESAs in the organization email system. Different priorities are used in the MX records.
* We can use cluster that contains a set of appliances

**Email Pipeline overview**

Email Pipeline: flow of email as it is processed by cisco ESA. IT is in three phases:

* **Receipt:** This phase involves the initial connection from the sender and is responsible for validating the recipient before accepting the email message.
* **Work queue:** In this phase the received email message is processed before being delivered to the delivery phase in the email pipeline. Cisco ESA processing of the email messages includes various tasks, such as masquerading, routing, filtering, safelist/blocklist matching, antispam and antivirus scanning, file reputation scanning and analysis, Outbreak Filters, and quarantining.
* **Delivery:** The final phase of the email pipeline is responsible for sending the email message to the destination SMTP host.

**Incoming Email Processing**

* The incoming mail policy provides the inbound security controls for the incoming email processing.
* This policy includes **six layers of filters**, where each one is designated for a specific protection.
* Some of the filters and engines are optional and disabled by default but can be enabled with appropriate license key installed on Cisco ESA.

The list shows the order in which they are applied to a message when it traverses the appliance from an external source:

1. **Reputation filters:** first layer of spam protection, allowing you to control the messages that come through the email gateway based on sender trustworthiness, which is determined by the Cisco SenderBase Reputation Service.
   1. incoming emails from known bad senders are simply denied.
   2. Known good emails from global organization domains are automatically routed around the spam filters, reducing the chance of false positives.
2. **Message filters:** provides special type of rules that describe how to process messages and attachments as they are received through using a script-like interface with regular expressions.
   1. Various filter actions are supported, such as drop, bounce, archive, quarantine, and so on.
3. **Antispam:** The antispam engine provides antispam scanning on the inbound messages to protect against any type of spam that might be included in the email messages.
4. **Antivirus:** The antivirus protection is achieved by using the integrated virus scanning engines. Virus detection with Sophos or McAfee antivirus engines provides deep virus scanning for viruses, Trojan horses, worms, or other types of malware.
5. **Content Filters:** Content filters are similar to the message filters, except that they are applied later in the email pipeline—after a message has been "splintered" into a number of separate messages for each matching policy.
6. **Outbreak Filters:** Outbreak filters are a special type of filters that provide protection against day-zero attacks. They act proactively to provide a critical first layer of defense against new outbreaks on the internet. Therefore, for any newly released viruses for which the antivirus engines still do not have corresponding definitions, the outbreak filters can block files with infected file characteristics.

**Optional**

* Also, the AMP engine can be enabled, which in turn will provide advanced malware analysis and protection.
* As part of the antispam protection, a graymail protection can also be enabled on Cisco ESA by activating the feature key for this engine.

**Outgoing mail processing**

The outgoing mail processing differs from the incoming mail processing in several aspects:

* Reputation filtering is not used for outgoing emails;
* In the default outgoing mail policy, the antispam scanning and outbreak filters are disabled by default. However, you can enable these engines by editing the outgoing mail policy and configuration applied.
* An outgoing mail policy provides **an additional DLP function** to the process to ensure that unsuitable or unauthorized information does not leak out of the organization. DLP scanning can be performed on outgoing messages only, therefore this feature is available only in the outgoing mail policy on Cisco ESA.

**Public and Private Listeners**

Cisco ESA functions as an email gateway for the email communications. Typical placement of cisco ESA in an enterprise network environment is between a firewall and a local email server

* Inbound email is accepted for local domains
* Outbound email is routed by email server to cisco ESA

**Two types of listeners**:

* **Public**: receives email from the internet and directs messages to a limited number of internal mail servers.
* **Private:** receives email from internal mail servers and directs messages to many external mail hosts

**Host Access Table (HAT) overview**

* HAT defines which hosts are allowed to connect to a listener and every listener has its own HAT
* HAT is defined to take different actions depending on the listener type:
  + Public listener: The HAT is set to accept email from all hosts.
  + Private listener: The HAT is set up to relay email from the host or hosts you specify and reject all other hosts.

To control incoming connections from remote hosts, appropriate information should be defined:

* **Sender groups**: You group remote host definitions into sender groups.
* **Two types of sender groups: predefined and custom**
* You can define multiple remote hosts in a sender group by IP address and hostname or domain name, dns list , SenderBase reputation score (SBRS)
* In a two-interface deployment, Cisco ESA uses two HAT tables, one for the public listener, and one for the private listener

**Predefined sender group**

Hat of the public listener:

* WHITELIST
* BLACKLIST
* SUSPECTLIST
* UNKNOWNLIST
* ALL

HAT table of the private listener contains two sender groups n that are used for outgoing email sent from the local users:

* RELAYLIST
* ALL

NB Cisco is updating products and content to be free of offensive or suggestive language. The predefined sender groups are now named blocked list/allowed list (BLOCKED\_LIST/ALLOWED\_LIST) rather than blacklist/whitelist, respectively

**Recipient Access Table**

* **RAT:** Cisco ESA uses this after the HAT check. This table is responsible for defining recipients (email address, domain, and so on) for which email will be accepted or rejected. RAT is not used on private listeners.
* A recipient address can be defined by : domain name, partial domain, username, full email address
* Cisco ESA can query LDAP servers when accepting email message
  + It is performed after RAT
  + Defines if the messages should be accept or reject

**Mail Flow Policy Overview**

* Cisco ESA enforces organization policies for messages sent to and from users by using mail policies
* Rules defined in policies scan each message and perform corresponding actions and we have incoming and outgoing mail policies
* There are two different types of mail flow policies, predefined and custom.
* Policies can match any of the email pipeline features: antispam, antivirus, AMP, graymail, content filters, outbreak filters, DLP (only for outgoing mail policies)
* Mail policies can be manged from the Gui or the CLi