09- Email Content Security (ESA)

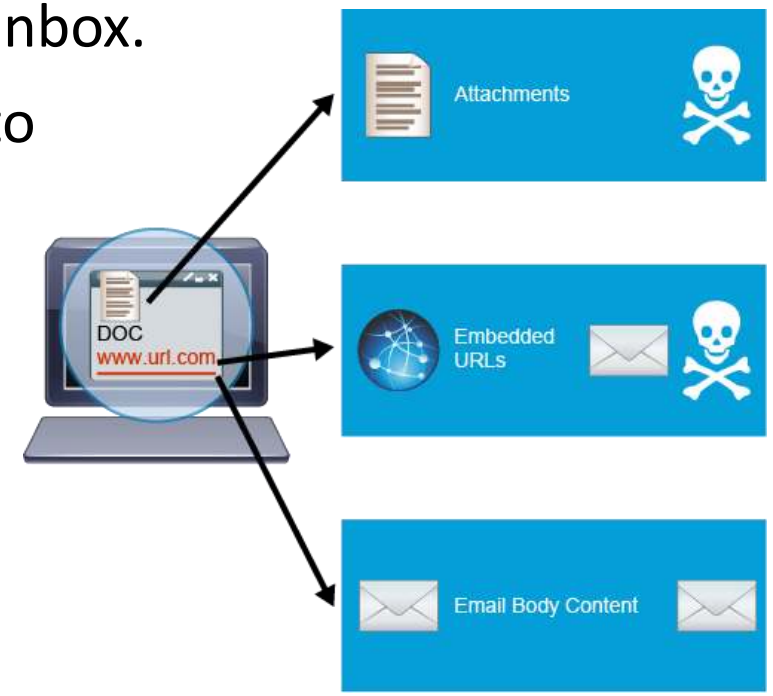
Ahmed Sultan
Senior Technical Instructor
ahmedsultan.me/about

Cisco ESA Overview

- Today's **email-based threats** demand a dedicated array of resources, technologies, and expertise to safeguard systems against existing and evolving attacks.
- Cisco ESA answers the call by staying one step ahead of these advanced threats to keep your inbox highly secure.
- This all-in-one appliance defends against spam, advanced malware, phishing, and data loss.

Cisco ESA Overview (cont.)

- Cisco ESA scans for malicious threats in email messages by performing deep inspection on the attachments, embedded URLs, and email body content.
- 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
  - ✓ Forward the email without the attachment
  - ✓ Rewrite the email subject header with a warning



Cisco ESA Overview (cont.)

- Threat actors know that sending attachments in spam email is a good way to get malicious content inside the network, beyond the firewall.
- However, threat actors also know that several systems can be put in place to inspect or drop emails, and users are being more vigilant against unrecognized emails with attachments.
- If a threat actor can deliver an email with a URL—they can change the equation to be in their favor.
- If a user clicks a URL hyperlink in an email, the user's web browser establishes a connection from the internal network to the URL.

Cisco ESA Overview (cont.)

- Usually, this connection will bypass the perimeter security defenses at the corporate network because the firewall will permit return traffic destined for the user's endpoint.
- Cisco ESA, using **Cisco Talos** threat intelligence, recognizes suspects and known bad URLs, and will warn about or block the connection when something malicious is involved.
- Cisco ESA performs this action by rewriting the URL hyperlink in emails where a suspect URL is detected as the inbound email is processed.

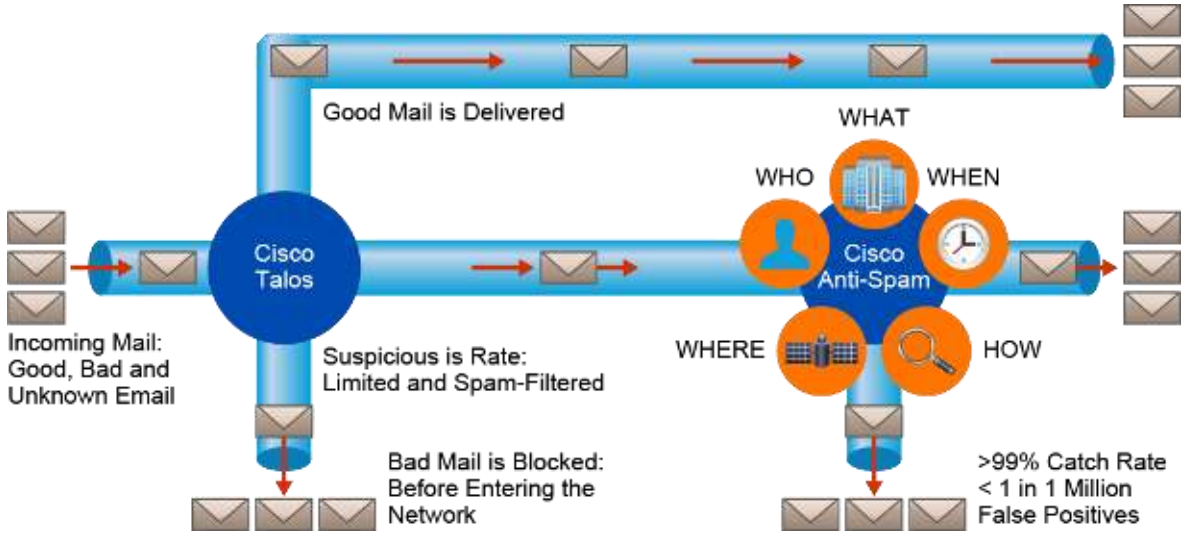
Cisco ESA Overview (cont.)

Cisco ESA can implement some additional security features such as:

- ✓Block, quarantine, or filter incoming email based on sender's geography.
- ✓Identify graymail and tag with "safe unsubscribe" option.
- ✓Comply with industry and government data-loss prevention regulations.
- ✓Track users that have clicked malicious URLs.
- ✓Enforce admin rights with two-factor authentication.

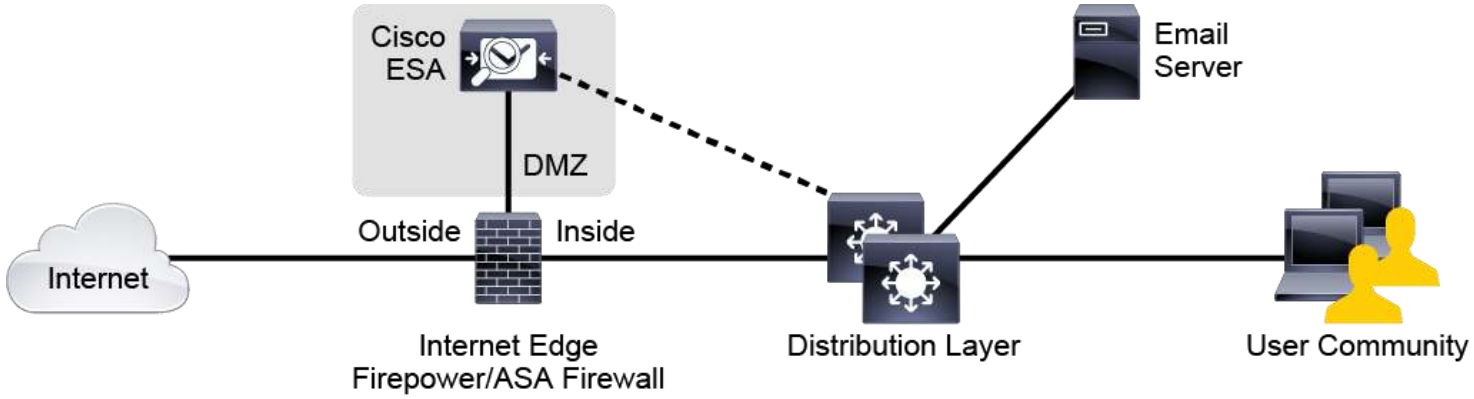
Cisco ESA Overview (cont.)

- **Cisco Talos** service that is integrated into Cisco ESA, provides a 24-hour view into global traffic activity.
- This intelligence enables security analyst to analyze anomalies, uncover new threats, and monitor traffic trends, Automatic policy updates are pushed to network devices **every three to five minutes**.



Cisco ESA Overview (cont.)

- By implementing Cisco ESA in the organization deployment, all email messages will be evaluated and scanned in inbound and outbound direction by the engines and policies configured for filtering out any malicious attachment, email body content or URL links included in the emails.
- In a typical deployment, Cisco ESA is deployed as the first "mail server" for email coming from the internet, and the last "mail server" on the path out to the internet.



Cisco ESA Overview (cont.)

Cisco ESA supports two different methods to filter spam and combat against phishing attacks:

1. **Reputation-based filtering:** 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. For every host on the internet, **Cisco SenderBase** provides a reputation score that depends on the malicious activity performed

2. **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.

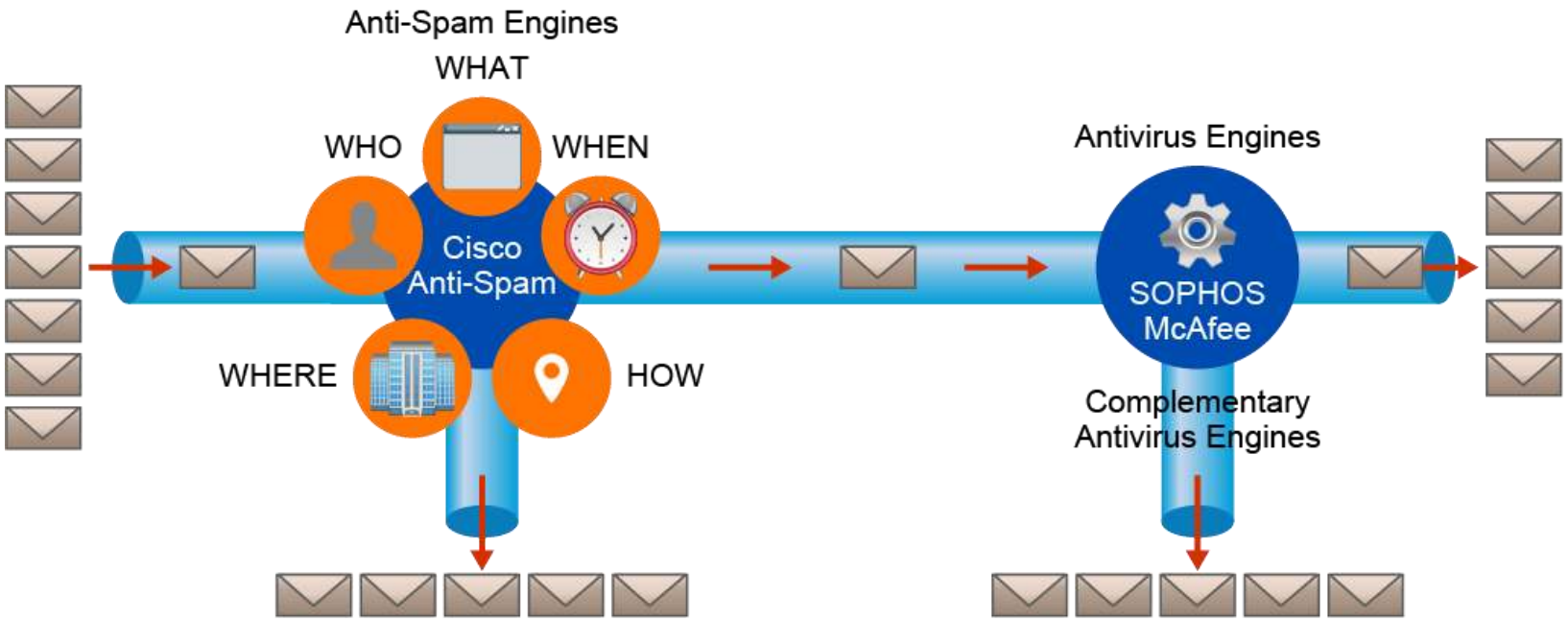
Cisco ESA Overview (cont.)

Cisco ESA uses a multilayer approach to fight Viruses and Malware

- **The first layer of defense** consists of outbreak filters, which Cisco ESA downloads from Cisco SenderBase. They contain a list of known malicious mail servers. These filters are generated by watching global email traffic patterns and looking for anomalies that are associated with an outbreak. When an email is received from a server on this list, it is kept in quarantine until the antivirus signatures are updated to counter the current threat.
- **The second layer of defense** is the use of antivirus signatures (**Sophos** and **McAfee**) to scan incoming emails, and quarantined emails, to ensure that they do not carry malware, such as viruses or worms into the network.

Cisco ESA Overview (cont.)

Cisco ESA uses a multilayer approach to fight viruses and malware (cont.)



Cisco ESA Overview (cont.)

- **Cisco ESA** easily integrates into existing email infrastructures with a high degree of flexibility, It acts as a Mail Transfer Agent (MTA) within the email-delivery chain.