**Protection Against Spam and Graymail**

**SPAM**

* **Spam email:** an unwanted email for which users have never subscribed before.
* **SenderBase:** as part of Cisco Talos Intelligence Group, is a designed to help email administrators to better manage incoming email streams by providing objective data about the identity of senders. SenderBase is an email reputation service designed to help email administrators research senders, identify legitimate sources of email, and block spammers.
  + SenderBase combines multiple sources of information to determine a "reputation score" for any IP address, known as an SBRS. This information includes:
    - Email volume information provided by tens of thousands of organizations that regularly receive internet email.
    - Spam complaints received by the SpamCop service.
    - Information on other DNS-based blocked lists.
  + The SBRS returns a score based on the probability that a message from a given source is spam. It is essential for the antispam protection on cisco RSA

**Cisco ESA Strategy for Using SBRS**

How you use SBRS scores will depend on how aggressive you want to be in pre-filtering email. Cisco ESA offers three different strategies for implementing SenderBase protection:

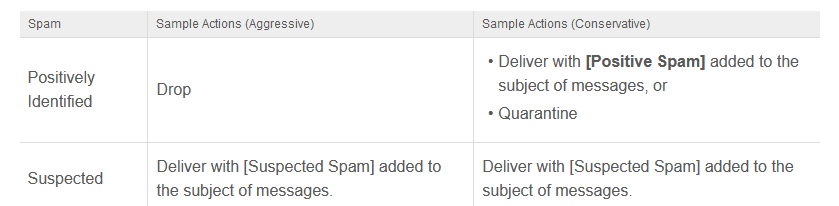
* **Conservative:** A conservative approach is to block messages with a SBRS lower than -10.0, throttle between -4.0 and -2.0, apply the default mail flow policy between -2.0 and +7.0, and apply the trusted policy for messages with a score greater than +7.0.
* **Moderate:** A moderate approach is to block messages with a SBRS lower than -4.0, throttle between -4.0 and 0, apply the default mail flow policy between 0 and +6.0, and apply the trusted policy for messages with a score greater than +6.0. Using this approach ensures a very small false positive rate while achieving better system performance).
* **Aggressive:** An aggressive approach is to block messages with a SBRS lower than -1.0, throttle between -1.0 and 0, apply the default mail flow policy between 0 and +4.0, and apply the trusted policy for messages with a score greater than +4.0

**SBRS Ranges in Sender Groups**

The process of assigning the senders to the sender groups depends on the configured SBRS ranges that are configured for groups that are defined in the HAT and the SBRS assigned to each sender by the SenderBase Reputation Service. Therefore, when SMTP connections are initiated from the sending MTAs, based on the SBRS scores, the senders will be assigned to the appropriate sender groups and corresponding mail flow policies will be applied.

**Antispam Filtering**

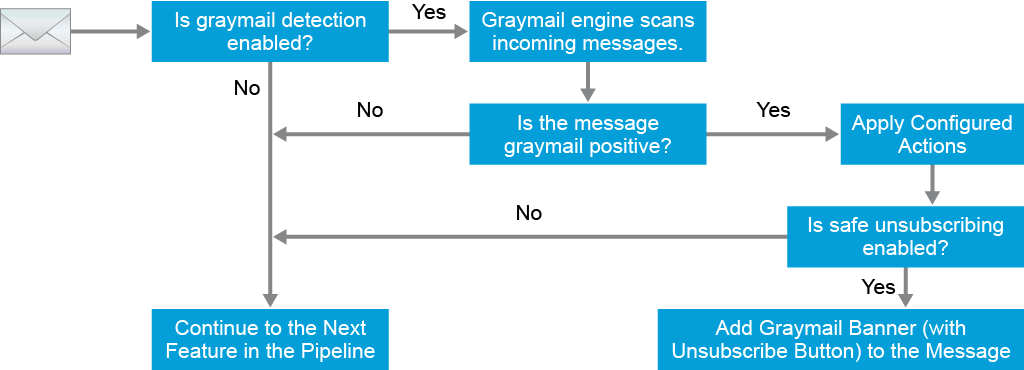
Antispam processes scan email for incoming (and outgoing) email based on the configured mail policies. The antispam filtering can categorize each message as not spam, suspected spam, positively identified spam.

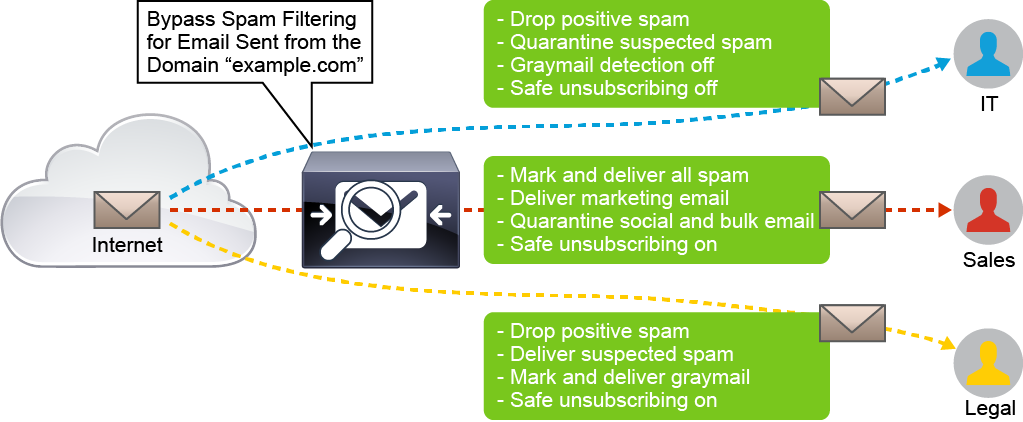


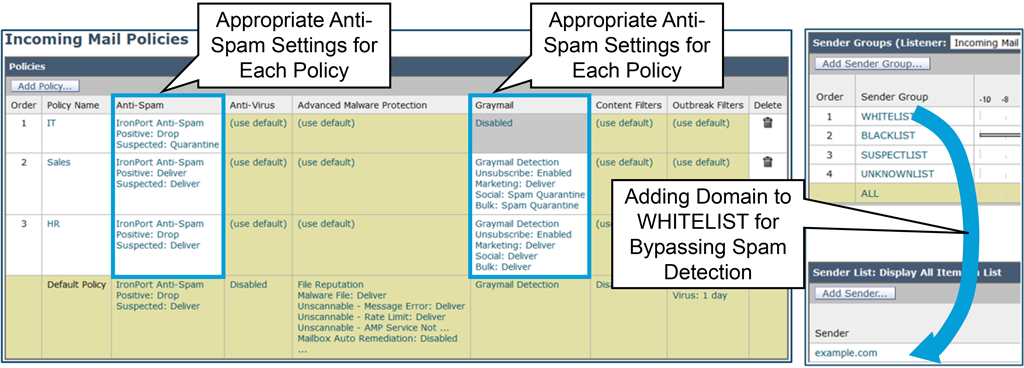
Cisco ESA offers two antispam solutions that can be used for protection against spam email:

* **IronPort antispam:** IronPort antispam analyzes over 100,000 message attributes across the following dimensions:
* **Email reputation:** *Who* is sending you this message?
* **Message content:** *What* content is included in this message?
* **Message structure:** *How* was this message constructed?
* **Web reputation:** *Where* does the call to action take you?
* **Cisco Intelligent Multi-Scan**
* a message is first scanned by third-party antispam engines.
* Cisco Intelligent Multi-Scan then passes the message and the verdicts of the third-party engines to Cisco antispam, which assumes responsibility for the final verdict.
* Low false positive rate

**Graymail overview**

* **It** is another type of spam, although it does not fit the real definition of spam email. Usually, in the beginning this email is wanted by the recipients, however with time it diminishes in value, so users no longer want to receive it.
* Such email messages are newsletters, social media notifications, marketing, bulk email and more.
* The difference between graymail and spam is that the end user intentionally provided an email address at some point (for example, the end user subscribed to a newsletter on an e-commerce website or provided contact details to an organization during a conference) as opposed to spam messages that the end user did not sign up for.
* The graymail management solution in Cisco ESA comprises of two components:
  + **an integrated graymail scanning engine**
  + **a cloud-based Unsubscribe Service.**
* The graymail engine classifies each graymail into one of the following categories: Marketing email, Social network email, Bulk email (**e-** mails publicitaires):
* 





**Antivirus Protection Overview**

* The antivirus feature in the email pipeline provides deep message scanning for viruses, Trojan horses, worms, or other types of malwares included in the email messages.
* Antivirus scanning is performed immediately after the spam scanning
* The Cisco ESA includes integrated virus scanning engines from third-party companies Sophos and McAfee
* Scanning email with Sophos and McAfee provides defense-in-depth by combining the benefits of both scanning engines
* Cisco ESA can use one or both antiviruses scanning engines per mail policy basis
* In multilayer antivirus scanning, McAfee scans first, then Sophos

**Antivirus Settings and Actions**

The virus scanning engines globally on Cisco ESA. Both Sophos and McAfee are optional, so either one or both of them can be licensed on the Cisco ESA appliance.

Several actions for scanning messages are supported on the appliance:

* **Scan for viruses only**
* Scan and repair viruses
* Drop attachments
* Users will always be notified if their messages were modified in any way because they were infected with a bad attachment
* **X-IronPort-AV header**: All messages that are processed by the antivirus scanning engine on the appliance have the header X-IronPort-AV: added to messages. This header provides additional information to you when debugging issues with your antivirus configuration, particularly with messages that are considered unscannable.

After scanning, the malicious messages can be identified as:

* **Repaired message**
* **Encrypted message**
* **Unscannable message:**
* **Virus infected message**

Actions supported for messages identified as malicious:

* **Drop**
* **Deliver as attachment**
* **Deliver as is**
* **Quarantine**

Optional actions:

* **Archive original message**
* **Modify message subject:**
* **Add custom header to message**
* **Send notification when message is delivered as is or as attachment**
* **Modify message recipient:**
* **Send message to alternate destination host:**

**Anti-malware protection Overview**

AMP provides advanced malware analysis and protection across the attack continuum: before, during, and after an attack

* Cisco AMP protects against zero-day threats
* Evaluates most files types
* Available for incoming and outgoing messages
* Cisco ESA and file reputation service communication is encrypted

**Outbreaks filter**

* Outbreak Filters protect your network from large-scale virus outbreaks and smaller, non-viral attacks, such as phishing scams and malware distribution, as they occur.
* For virus outbreaks, analyzes the messages content, context, and structure
* For non-vial threats, scans messages for URLs and uses outbreak rules from Talos to evaluate a message’s threat level
* Three tactics can protect users from outbreaks: delay, redirect and modify
* Outbreak filter rule is basically a threat level associated with a set of characteristics for an email message and attachment
* Each rule is assigned a threat level between 0 and 5

**Content Filters**

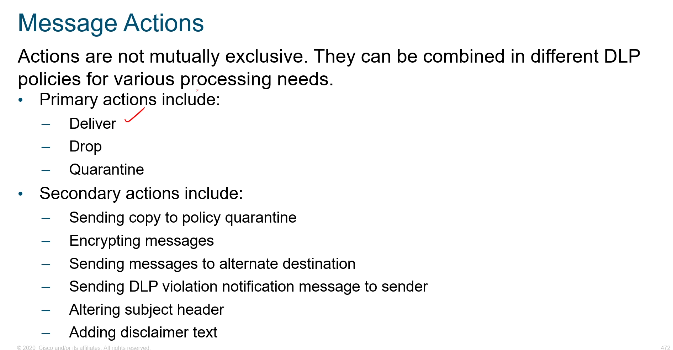
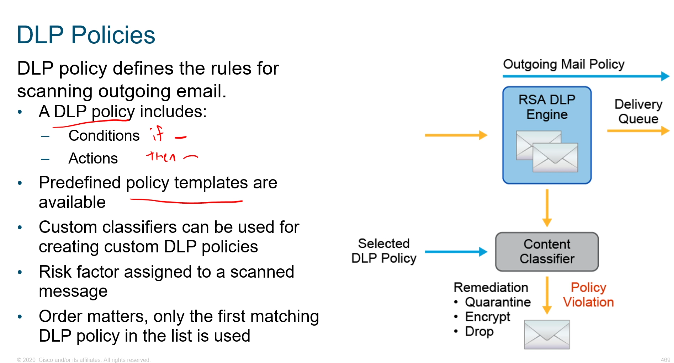
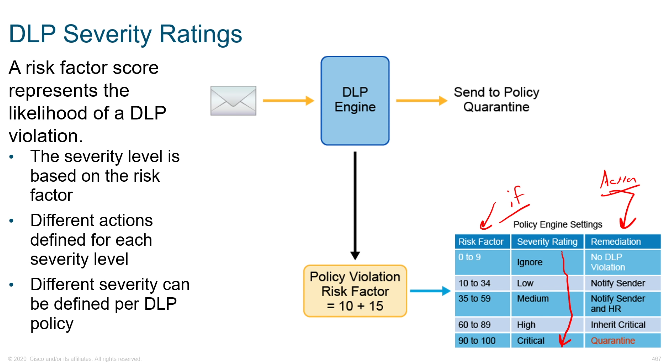
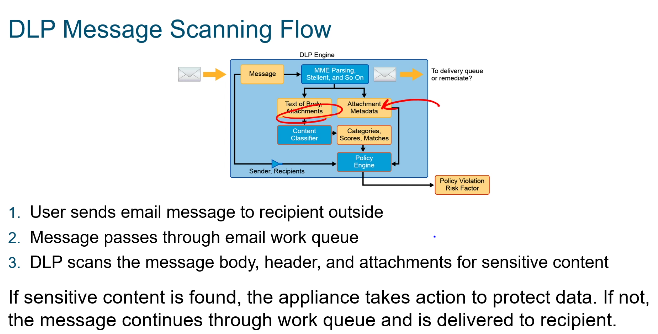
* Content filters allow you to inspect the intricate details of the email messages received by the Cisco Email Security Appliance (ESA) and take appropriate actions on the messages.
* Content filters are similar to message filters. The difference is that they are applied later in the email pipeline

Content filters have the following components:

* **Conditions:** They determine when the Cisco ESA uses a content filter to scan a message.
* **Actions:** When the condition (or conditions) in the content filter is matched, the Cisco ESA applies an action (or actions)
* Two types of content filters: incoming and outgoing content filters

**Data Loss Prevention**

* DLP feature secure users from maliciously or unintentionally emailing sensitive data from the network
* Secures proprietary information and intellectual property
* Defines the types of data that the users are not allowed to email
* Various kinds of sensitive information can be filtered: credit card numbers, bank account numbers, passport numbers…
* DLP feature is off by default and available only for outgoing email



EEmail Encryption

Sending sensitive content via emails cvan be in violation of company policy

They are three available solutions for protecting email:

* **Cisco Email Encryption:** This solution enables the Cisco ESA to encrypt messages and the key needed for decryption is stored on a key server which recipients will connect to in order to retrieve it. The key server can be a locally configured key server, or it might use the Cisco Registered Envelope Service (CRES). CRES is preferred option and is used more frequently.
* **TLS:** This solution offers relaying messages over Transport Layer Security (TLS) instead of encrypting them by using the Cisco email encryption feature with local key server or CRES. TLS is preferred option for protecting emails, in which case the CRES can be used as a backup method.
* **S/MIME Security Services:** This solution allows the Cisco ESA to sign, encrypt, verify, and decrypt messages using a Private/Public key pair. The supported Secure/Multipurpose Internet Mail Extensions (S/MIME) security services on the Cisco ESA can be implemented in Business-to-Business (B2B) and Business-to-Consumer (B2C) scenarios.

