# Detect and Prevent Email Spoofing

## Contents

## Introduction

This document describes how to detect and prevent email spoofing when using Cisco Secure Email.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics.

- Cisco Secure Email

### Components Used

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

## About this Document

This document is for Cisco Customers, Cisco Channel Partners, and Cisco Engineers who deploy Cisco Secure Email. This document covers:

## What is Email Spoofing

Email Spoofing is email header forgery where the message appears to have originated from someone or somewhere other than the actual source. Email Spoofing is used in phishing and spam campaigns because people are likelier to open an email when they think a legitimate, trustworthy source has sent it. For more information about spoofing, please refer to What is Email Spoofing and How to Detect It.

Email Spoofing falls into these categories:

| **Category** | **Description** | **Main Target** |
|---|---|---|
| Direct Domain Spoofing | Impersonate a similar domain in the Envelope From as the recipient's domain. | Employees |
| Display Name Deception | The From header shows a legitimate sender with an executive name of an organization. They are also known as Business Email Compromise (BEC). | Employees |
| Brand Name Impersonation | The From header shows a legitimate sender with the brand name of a well-known organization. | Customers / Partners |
| Phish URL-Based Attack | An email with an URL that attempts to steal sensitive data or log in information from the victim. A fake email from a bank that asks you to click a link and verify your account details is an example of a phishing URL-based attack. | Employees / Partners |
| Cousin or Look-alike Domain Attack | The envelope from or From header value shows a similar sender address that impersonates a real one to bypass Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting and Conformance (DMARC) inspections. | Employees / Partners |
| Account Takeover / Compromised Account | Gain unauthorized access to a real email account that belongs to someone, and then sends emails to other victims as the legitimate email account owner. | Everyone |

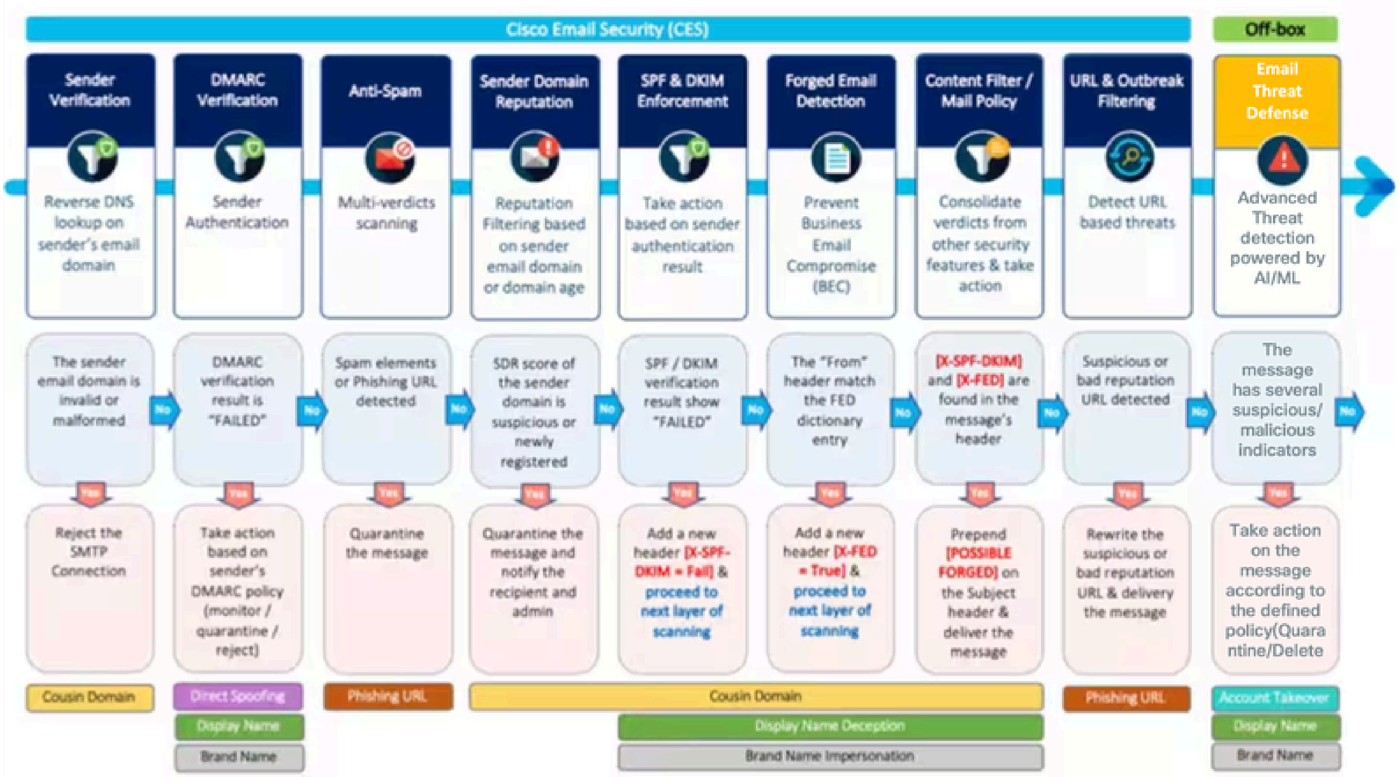
The first category relates to abuses of the owner's domain name in the Envelope From value in the internet header of an email. Cisco Secure Email can remediate this attack using sender Domain Name Server (DNS) verification to permit only legitimate senders. The same result can be achieved globally using DMARC, DKIM, and SPF verification.

However, the other categories only partially violate the domain portion of the sender's email address. Hence, it is not easy to be deterred when you use DNS text records or sender verification only. Ideally, it would be best to combine some Cisco Secure Email features and Cisco Secure Email Threat Defense (ETD) to fight against such advanced threats. As you know, Cisco Secure Email administration and configuration of features can vary from organization to organization, and improper application can lead to a high incidence of false positives. Therefore, to understand the organization's business needs and tailor the features is essential.

## Email Spoofing Defense Workflow

The security features that address the best practices to monitor, warn, and enforce against spoofing attacks are shown in the diagram (Image 1). The details of each feature are provided in this document. The best practice is an in-depth defense approach to detect email spoofing. Attackers can change their methods against an organization over time, so an administrator must monitor any changes and check the appropriate warnings and enforcement.

Image 1. Cisco Secure Email Spoof Defense Pipeline

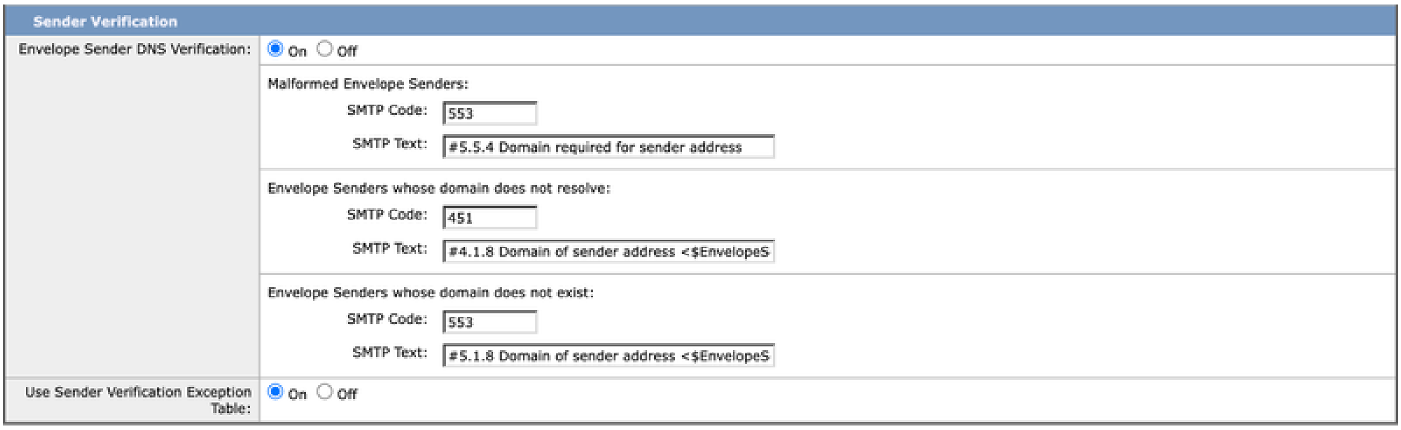

Cisco Email Security (CES)
Off-box
Sender Verification
Reverse DNS lookup on sender's email domain
DMARC Verification
Sender Authentication
Anti-Spam
Multi-verdicts scanning
Sender Domain Reputation
Reputation Filtering based on sender email domain or domain age
SPF & DKIM Enforcement
Take action based on sender authentication result
Forged Email Detection
Prevent Business Email Compromise (BEC)
Content Filter / Mail Policy
Consolidate verdicts from other security features & take action
URL & Outbreak Filtering
Detect URL based threats
Email Threat Defense
Advanced Threat detection powered by AI/ML
The sender email domain is invalid or malformed
DMARC verification result is "FAILED"
Spam elements or Phishing URL detected
SDR score of the sender domain is suspicious or newly registered
SPF / DKIM verification result show "FAILED"
The "From" header match the FED dictionary entry
[X-SPF-DKIM] and [X-FED] are found in the message's header
Suspicious or bad reputation URL detected
The message has several suspicious/ malicious indicators
No
Yes
Reject the SMTP Connection
Take action based on sender's DMARC policy (monitor / quarantine / reject)
Quarantine the message
Quarantine the message and notify the recipient and admin
Add a new header [X-SPF-DKIM = Fail] & proceed to next layer of scanning
Add a new header [X-FED = True] & proceed to next layer of scanning
Prepend [POSSIBLE FORGED] on the Subject header & deliver the message
Rewrite the suspicious or bad reputation URL & delivery the message
Take action on the message according to the defined policy(Quarantine/Delete
Cousin Domain
Direct Spoofing
Display Name
Brand Name
Phishing URL
Cousin Domain
Display Name Deception
Brand Name Impersonation
Phishing URL
Account Takeover
Display Name
Brand Name

### Layer 1: Validity Check on the Sender's Domain

Sender Verification is a more straightforward way to prevent emails sent from a bogus email domain, such as cousin domain spoofing (for example, c1sc0.com is the imposter of cisco.com). Cisco Secure Email makes an MX record query for the domain of the sender's email address and performs an A record lookup on the MX record during the SMTP conversation. If the DNS query returns NXDOMAIN, it can treat the domain as non-existent. It is a common technique for attackers to forge the envelope sender's information so the email from an unverified sender is accepted and processed further. Cisco Secure Email can reject all incoming messages that fail the verification check that uses this feature unless the sender's domain or IP address is pre-added in the Exception Table.

Best Practice: Configure Cisco Secure Email to reject the SMTP conversation if the email domain of the envelope sender field is invalid. Only allow legitimate senders by configuring the mail flow policy, sender verification, and exception table (optional). For more information, visit Spoof Protection using Sender Verification.

Image 2. Sender Verification Section in Default Mail Flow Policy



Sender Verification

Envelope Sender DNS Verification: ● On ○ Off

Malformed Envelope Senders:

SMTP Code: 553

SMTP Text: #5.5.4 Domain required for sender address

Envelope Senders whose domain does not resolve:

SMTP Code: 451

SMTP Text: #4.1.8 Domain of sender address <$EnvelopeS

Envelope Senders whose domain does not exist:

SMTP Code: 553

SMTP Text: #5.1.8 Domain of sender address <$EnvelopeS

Use Sender Verification Exception Table: ● On ○ Off

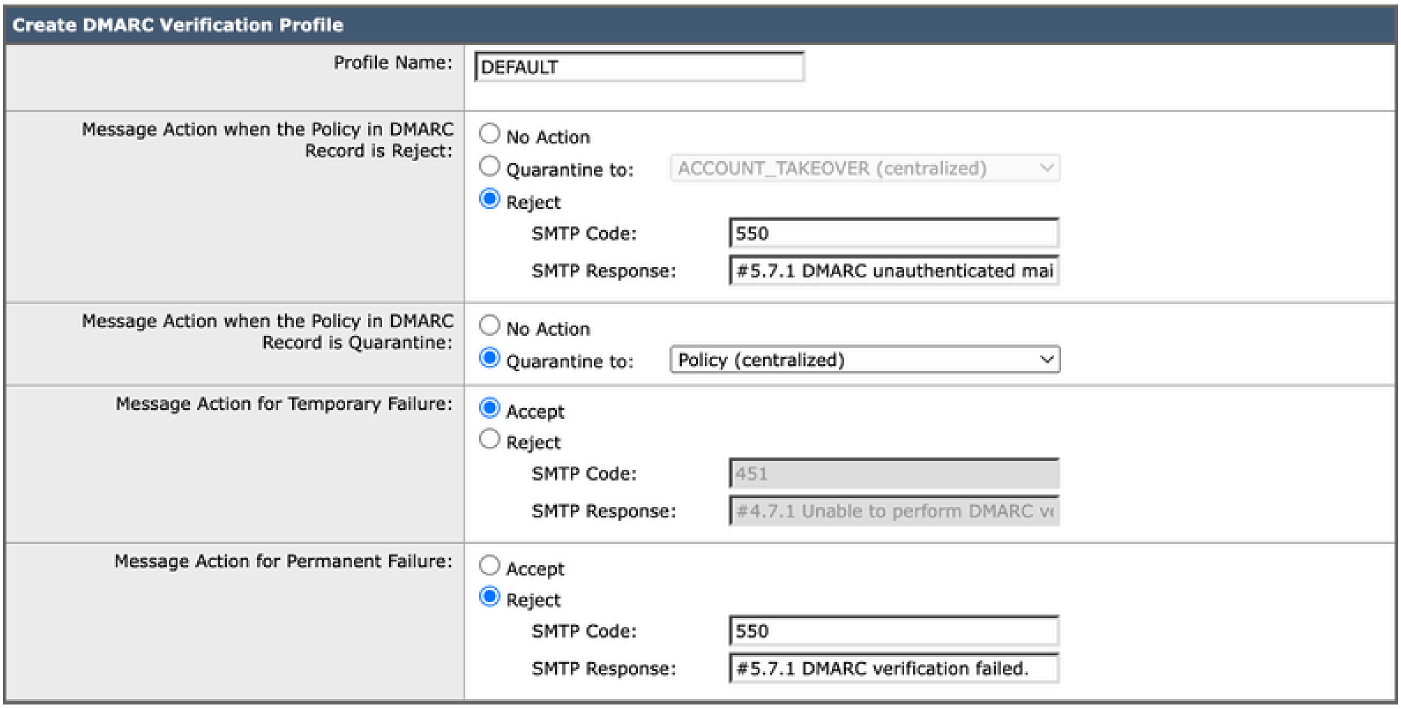
## Layer 2: Verify the From Header Using DMARC

DMARC verification is a much more powerful feature to fight against Direct Domain Spoofing, and also includes Display Name and Brand Impersonation attacks. DMARC ties information authenticated with SPF or DKIM (sending domain source or signature) with what is presented to the end-recipient in the From header and ascertains that SPF and DKIM identifiers are aligned with the FROM header identifier.

To pass DMARC verification, an incoming email must pass at least one of these authentication mechanisms. In addition, Cisco Secure Email also allows the administrator to define a DMARC verification profile to override the domain owner's DMARC policies and send aggregate (RUA) and failure/forensic (RUF) reports to the domain owners. This helps to strengthen their authentication deployments in return.

Best Practice: Edit the default DMARC profile that uses the DMARC policy actions the sender advises. Additionally, the global settings of DMARC verification must be edited to enable correct report generation. Once the profile is configured appropriately, the DMARC verification service must be enabled in the Mail Flow Policies default policy.

Image 3. DMARC Verification Profile



Create DMARC Verification Profile

Profile Name: DEFAULT

Message Action when the Policy in DMARC Record is Reject:
○ No Action
○ Quarantine to: ACCOUNT_TAKEOVER (centralized)
● Reject
SMTP Code: 550
SMTP Response: #5.7.1 DMARC unauthenticated mai

Message Action when the Policy in DMARC Record is Quarantine:
○ No Action
● Quarantine to: Policy (centralized)

Message Action for Temporary Failure:
● Accept
○ Reject
SMTP Code: 451
SMTP Response: #4.7.1 Unable to perform DMARC v

Message Action for Permanent Failure:
○ Accept
● Reject
SMTP Code: 550
SMTP Response: #5.7.1 DMARC verification failed.

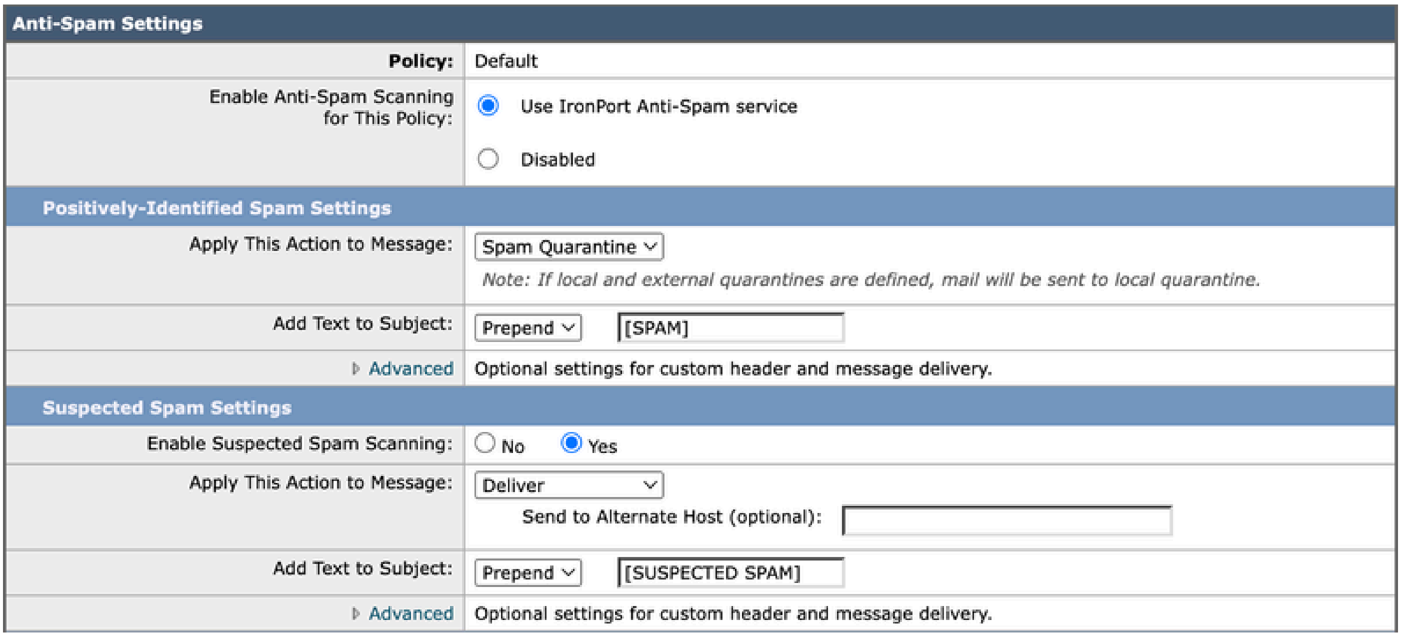
**Note**: DMARC must be implemented by sending the domain's owner in conjunction with a domain monitoring tool, such as Cisco Domain Protection. When implemented appropriately, DMARC enforcement in Cisco Secure Email helps protect against phishing emails sent to employees from unauthorized senders or domains. For more information about Cisco Domain Protection, please visit this link: Cisco Secure Email Domain Protection At-A-Glance.

## Layer 3: Prevent Spammers from Sending Spoofed Emails

Spoofing attacks can be another common form of a spam campaign. Therefore, enabling anti-spam protection is essential to effectively identify fraudulent emails that contain spam/phishing elements and block them positively. Anti-spam, combined with other best practice actions thoroughly described in this document, provides the best results without losing legitimate emails.

Best Practice: Enable anti-spam scanning in the default mail policy and set quarantine action to identify spam settings positively. Increase the minimum scanning size for spam messages to at least 2M globally.

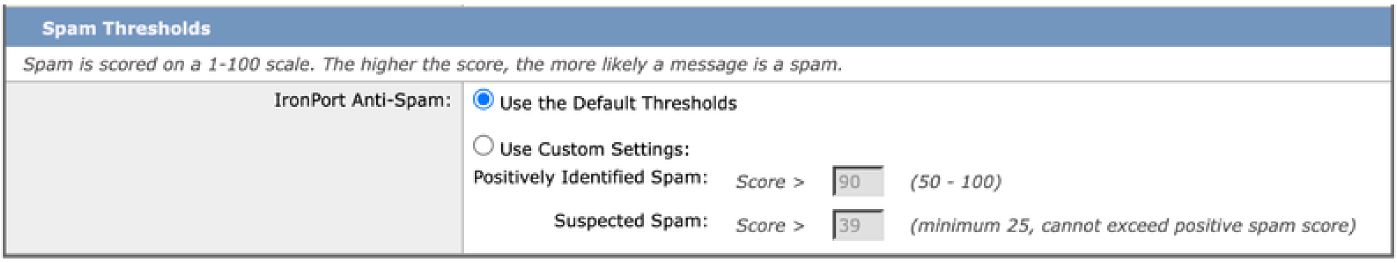
Image 4. Anti-Spam Setting in Default Mail Policy



| | |
|---|---|
| **Anti-Spam Settings** | |
| **Policy:** | Default |
| Enable Anti-Spam Scanning for This Policy: | ● Use IronPort Anti-Spam service<br>○ Disabled |
| **Positively-Identified Spam Settings** | |
| Apply This Action to Message: | Spam Quarantine<br>*Note: If local and external quarantines are defined, mail will be sent to local quarantine.* |
| Add Text to Subject: | Prepend [SPAM] |
| Advanced | Optional settings for custom header and message delivery. |
| **Suspected Spam Settings** | |
| Enable Suspected Spam Scanning: | ○ No ● Yes |
| Apply This Action to Message: | Deliver<br>Send to Alternate Host (optional): |
| Add Text to Subject: | Prepend [SUSPECTED SPAM] |
| Advanced | Optional settings for custom header and message delivery. |

The Spam Threshold can be adjusted for Positive and Suspected Spam to increase or decrease the sensitivity (Image 5); however, Cisco discourages the administrator from doing this and to only use the default thresholds as a baseline unless told otherwise by Cisco.

Image 5. Anti-Spam Thresholds Setting in Default Mail Policy



**Spam Thresholds**

*Spam is scored on a 1-100 scale. The higher the score, the more likely a message is a spam.*

| | |
|---|---|
| IronPort Anti-Spam: | ● Use the Default Thresholds<br>○ Use Custom Settings:<br>Positively Identified Spam: *Score >* 90 *(50 - 100)*<br>Suspected Spam: *Score >* 39 *(minimum 25, cannot exceed positive spam score)* |

**Note**: Cisco Secure Email offers an add-on Intelligent Multi-Scan (IMS) engine that provides different combinations from the anti-spam engine to increase the spam catch rates (most aggressive catch rate).

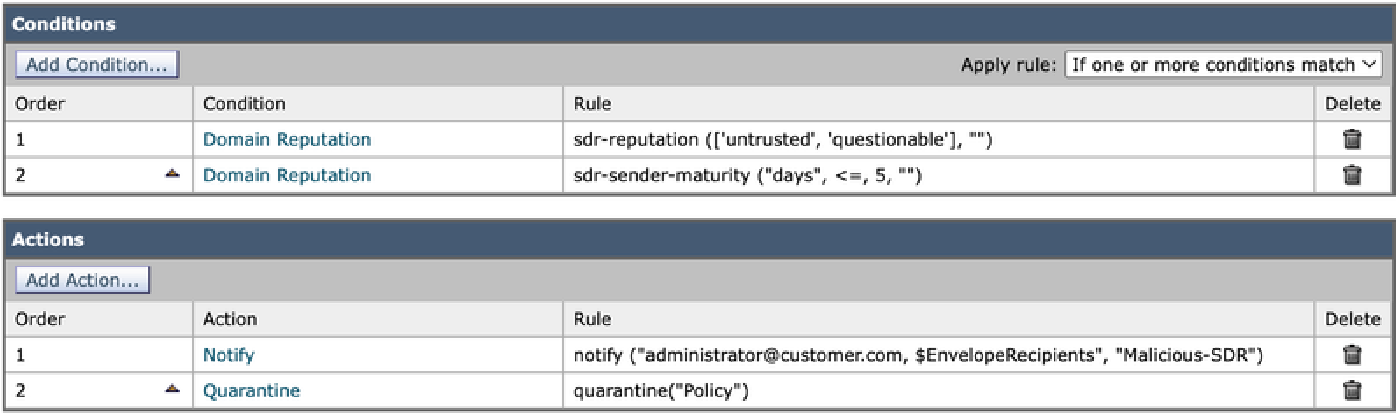
## Layer 4: Determine Malicious Senders via Email Domain

Cisco Talos Sender Domain Reputation (SDR) is a cloud service that provides a reputation verdict for email messages based on the domains in the email envelope and header. The domain-based reputation analysis enables a higher spam catch rate by looking beyond the reputation of shared IP addresses, hosting, or infrastructure providers. Instead, it derives verdicts based on features associated with fully qualified domain names (FQDNs) and other sender information in the Simple Mail Transfer Protocol (SMTP) conversation and message headers.

Sender Maturity is an essential feature to establish the sender's reputation. Sender Maturity is automatically generated for spam classification based on multiple sources of information, and can differ from Whois-based domain age. Sender Maturity is set to a limit of 30 days, and beyond this limit, a domain is considered mature as an email sender, and no further details are provided.

Best Practice: Create an incoming content filter that captures the sending domain in which the SDR reputation verdict falls under either Untrusted/Questionable or the Sender Maturity is less than or equal to 5 days. The recommended action is to quarantine the message and notify the email security administrator and the original recipient. For more information about how to configure SDR, please view the Cisco video at Cisco Email Security Update (Version 12.0): Sender Domain Reputation (SDR)

Image 6. Content Filter for SDR Reputation and Domain Age with Notify and Quarantine Actions.



Conditions

Apply rule: If one or more conditions match

| Order | Condition | Rule | Delete |
|---|---|---|---|
| 1 | Domain Reputation | sdr-reputation (['untrusted', 'questionable'], "") | 🗑 |
| 2 ▲ | Domain Reputation | sdr-sender-maturity ("days", <=, 5, "") | 🗑 |

Actions

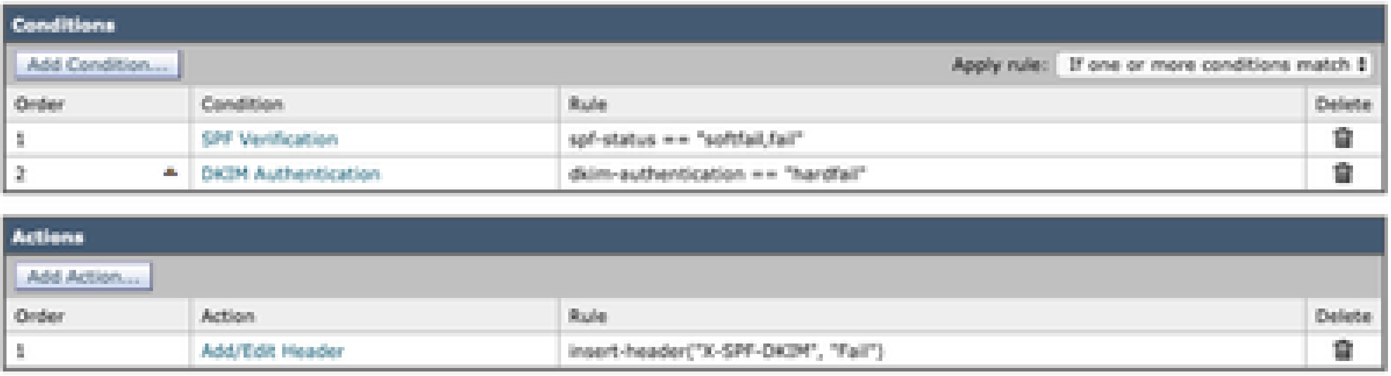
| Order | Action | Rule | Delete |
|---|---|---|---|
| 1 | Notify | notify ("administrator@customer.com, $EnvelopeRecipients", "Malicious-SDR") | 🗑 |
| 2 ▲ | Quarantine | quarantine("Policy") | 🗑 |

## Layer 5: Reduce False Positives with SPF or DKIM Verification Results

It is imperative to enforce SPF or DKIM verification (both or either one) to build multi-layers of spoof email detection for most attack types. Instead of taking a final action (such as drop or quarantine), Cisco recommends adding a new header such as [X-SPF-DKIM] on the message that fails SPF or DKIM verification and co-operate the outcome with the Forged Email Detection (FED) feature, which is covered later, in favor of an improved catch rate of spoofing emails.

Best Practice: Create a content filter that inspects SPF or DKIM verification results of each incoming message that passed through previous inspections. Add a new X-header (for example X-SPF-DKIM=Fail) on the message that fails the SPF or DKIM verification and delivers to the next layer of scanning – Forged Email Detection (FED).

Image 7. Content Filter that Inspects Messages with Failed SPF or DKIM Results



Conditions

Apply rule: If one or more conditions match

| Order | Condition | Rule | Delete |
|---|---|---|---|
| 1 | SPF Verification | spf-status == "softfail,fail" | 🗑 |
| 2 ▲ | DKIM Authentication | dkim-authentication == "hardfail" | 🗑 |

Actions

| Order | Action | Rule | Delete |
|---|---|---|---|
| 1 | Add/Edit Header | insert-header("X-SPF-DKIM", "Fail") | 🗑 |

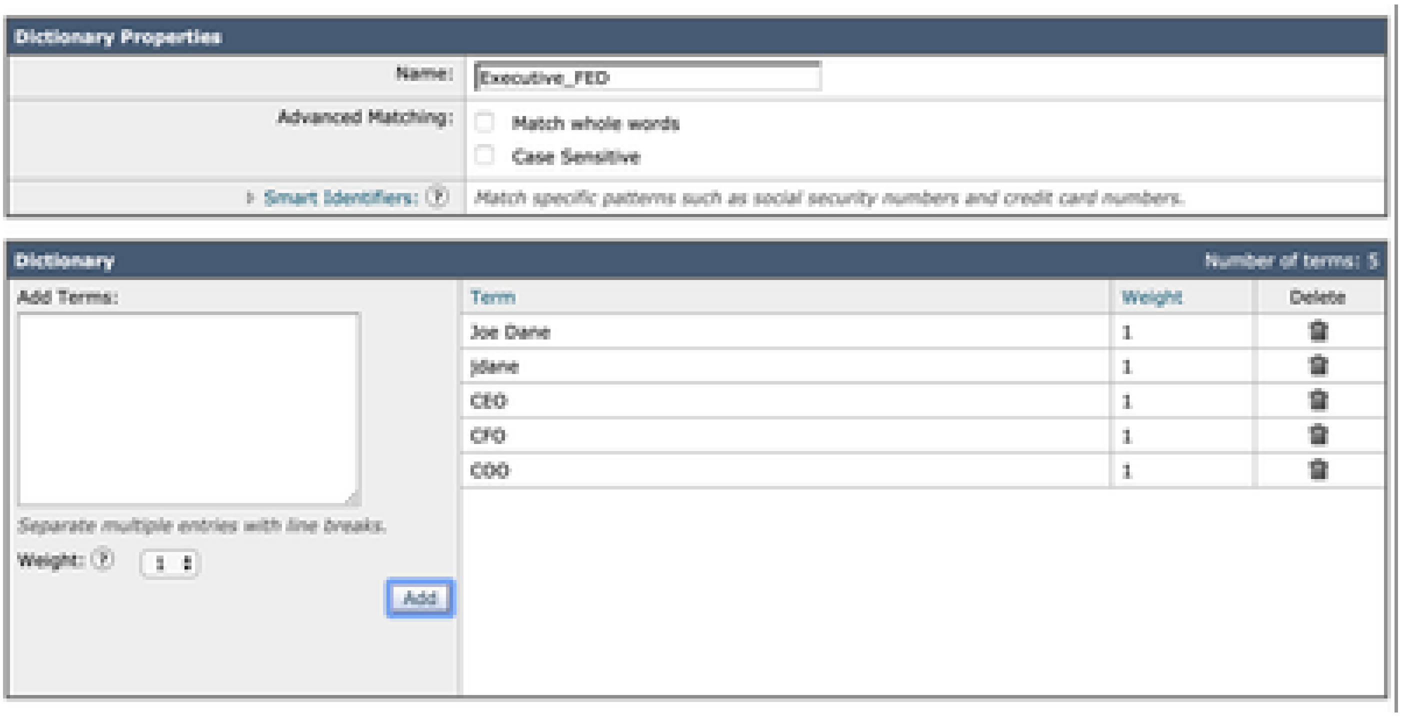
## Layer 6: Detect Messages with Possibly Forged Sender Name

Complementing SPF, DKIM, and DMARC verifications, Forged Email Detection (FED) is another crucial line of defense against email spoofing. The FED is ideal for remediating spoof attacks that abuse the From value in the message body. Given that you already know the executive names within the organization, you can create a dictionary of these names and then reference that dictionary with the FED condition in content filters. Furthermore, apart from executive names, you can create a dictionary of cousin or look-alike domains based on your domain by using DNSTWIST (DNSTWIT) to match against look-alike domain spoofing.

Best Practice: Identify the users in your organization whose messages are likely forged. Create a custom dictionary that accounts for executives. For every executive name, the dictionary must include the username and all possible usernames as terms (Image 8). When the dictionary is complete, use Forged Email Detection in the content filter to match the From value from incoming messages with these dictionary entries.

**Note**: Considering most domains are are not registered permutations, DNS sender verification protects against them. If you choose to use dictionary entries, only pay attention to the registered domains, and make sure not to exceed 500-600 entries per dictionary.

Image 8. Custom Directory for Forged Email Detection



**Dictionary Properties**

| | |
|---|---|
| Name: | Executive_FED |
| Advanced Matching: | □ Match whole words<br>□ Case Sensitive |
| ▸ Smart Identifiers: ? | *Match specific patterns such as social security numbers and credit card numbers.* |

**Dictionary** Number of terms: 5

Add Terms:

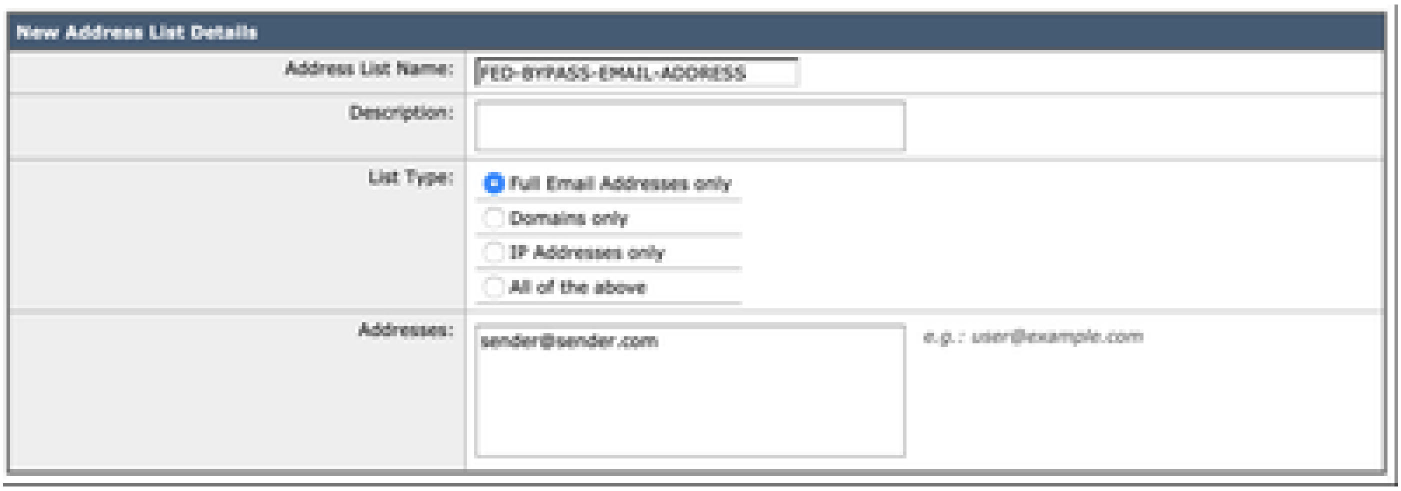
*Separate multiple entries with line breaks.*

Weight: ? 1

| Term | Weight | Delete |
|---|---|---|
| Joe Dane | 1 | 🗑 |
| jdane | 1 | 🗑 |
| CEO | 1 | 🗑 |
| CFO | 1 | 🗑 |
| COO | 1 | 🗑 |

It is optional to add an exception condition for your email domain in the Envelope Send to bypass the FED inspection. Alternatively, a custom Address List can be created to bypass the FED inspection to a list of email addresses that are displayed in the Fromheader (Image 9).

Image 9. Create an Address List to Bypass FED Inspection

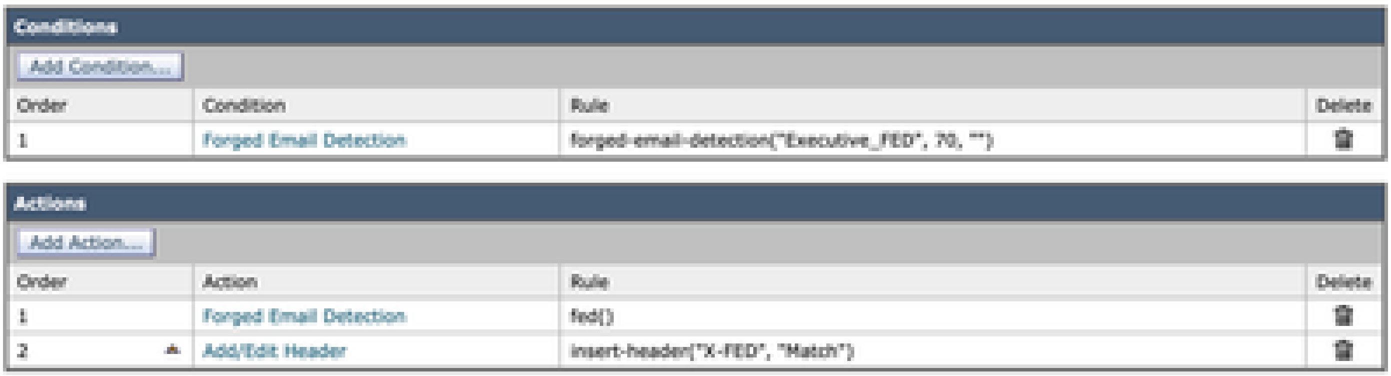


**New Address List Details**

| | |
|---|---|
| Address List Name: | FED-BYPASS-EMAIL-ADDRESS |
| Description: | |
| List Type: | ● Full Email Addresses only<br>○ Domains only<br>○ IP Addresses only<br>○ All of the above |
| Addresses: | sender@sender.com — *e.g.: user@example.com* |

Apply the Forged Email Detection proprietary action to strip the From value and review the actual envelope sender email address in the message inbox. Then, rather than applying a final action, add a new X-header (for example, X-FED=Match) on the message that matches the condition and continue delivering the message to the next layer of inspection (Image 10).

Image 10. Recommended Content Filter Setting for FED



| Order | Condition | Rule | Delete |
|---|---|---|---|
| 1 | Forged Email Detection | forged-email-detection("Executive_FED", 70, "") | 🗑 |

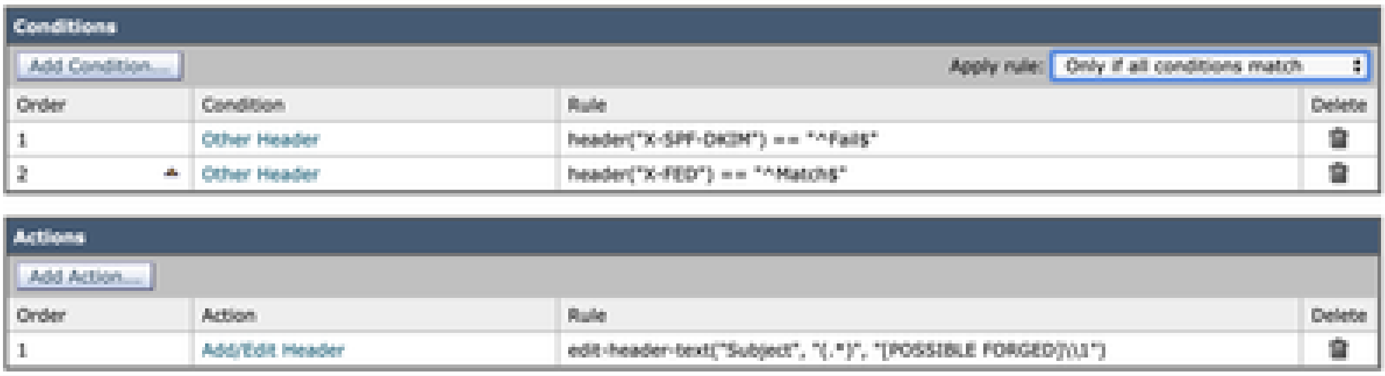
| Order | Action | Rule | Delete |
|---|---|---|---|
| 1 | Forged Email Detection | fed() | 🗑 |
| 2 | Add/Edit Header | insert-header("X-FED", "Match") | 🗑 |

## Layer 7: Positively Identified Spoofing Email

Identifying a real spoofing campaign is more effective by referencing other verdicts from various security features in the pipeline, such as the X-header information produced by SPF/ DKIM Enforcemen and FE. For example, administrators can create a content filter to identify messages added with both new X-headers due to failed SPF / DKIM verification results (X-SPF-DKIM=Fail) and which From header matches the FED dictionary entries (X-FED=Match).

The recommended action can be either to quarantine the message and notify the recipient, or continue delivering the original message but prepending [POSSIBLE FORGED] words to the Subject line as a warning to the recipient, as depicted (Image 11).

Image 11. Combine all X-headers into a Single (final) Rule



Apply rule: Only if all conditions match

| Order | Condition | Rule | Delete |
|---|---|---|---|
| 1 | Other Header | header("X-SPF-DKIM") == "^Fail$" | 🗑 |
| 2 | Other Header | header("X-FED") == "^Match$" | 🗑 |

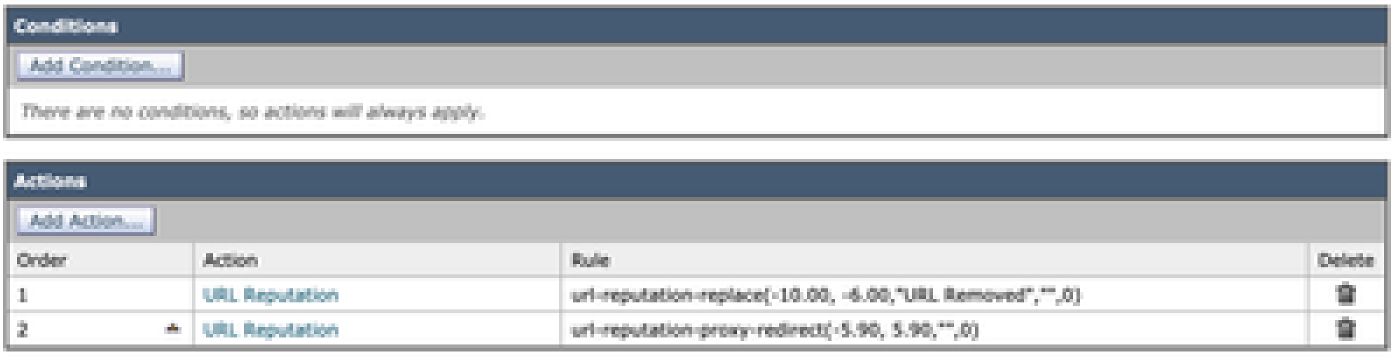
| Order | Action | Rule | Delete |
|---|---|---|---|
| 1 | Add/Edit Header | edit-header-text("Subject", "(.*)", "[POSSIBLE FORGED]\\1") | 🗑 |

## Layer 8: Protecting Against Phishing URLs

Protection against phishing links is incorporated into the URL and Outbreak Filtering in the Cisco Secure Email. Blended threats combine spoofing and phishing messages to look more legitimate to the target. Enabling Outbreak Filtering is critical to help detect, analyze, and stop such threats in real-time. It is worth it to know that URL reputation is assessed inside the Anti-Spam engine, and can be used as part of the decision for spam detection. If the Anti-Spam engine does not stop the message with the URL as Spam, it is evaluated by URL and Outbreak Filtering in the latter part of the security pipeline.

Recommendation: Create a content filter rule that blocks a URL with a malicious reputation score and redirects the URL with a neutral reputation score to Cisco Security Proxy (Image 12). Enable Threat Outbreak Filters by enabling Message Modification. URL Rewrite allows for suspicious URLs to be analyzed by Cisco Security Proxy (Image 13). For more information, visit: Configure URL Filtering for Secure Email Gateway and Cloud Gateway

Image 12. Content Filter for URL Reputations



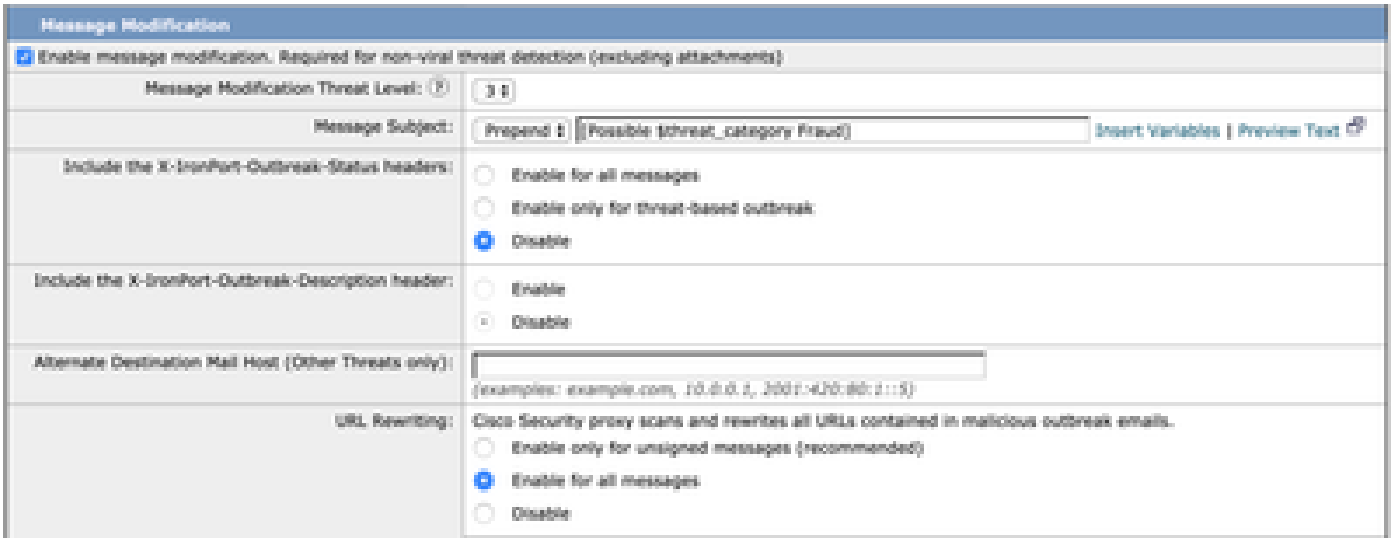
**Conditions**

*There are no conditions, so actions will always apply.*

**Actions**

| Order | Action | Rule | Delete |
|---|---|---|---|
| 1 | URL Reputation | url-reputation-replace(-10.00, -6.00,"URL Removed","",0) | 🗑 |
| 2 ▲ | URL Reputation | url-reputation-proxy-redirect(-5.90, 5.90,"",0) | 🗑 |

Image 13. Enable URL Rewrite in Outbreak Filtering



**Message Modification**

☑ Enable message modification. Required for non-viral threat detection (excluding attachments)

| | |
|---|---|
| Message Modification Threat Level: ⓘ | 3 |
| Message Subject: | Prepend [Possible $threat_category Fraud] Insert Variables \| Preview Text |
| Include the X-IronPort-Outbreak-Status headers: | ○ Enable for all messages<br>○ Enable only for threat-based outbreak<br>● Disable |
| Include the X-IronPort-Outbreak-Description header: | ○ Enable<br>● Disable |
| Alternate Destination Mail Host (Other Threats only): | *(examples: example.com, 10.0.0.1, 2001:420:80:1::5)* |
| URL Rewriting: | Cisco Security proxy scans and rewrites all URLs contained in malicious outbreak emails.<br>○ Enable only for unsigned messages (recommended)<br>● Enable for all messages<br>○ Disable |

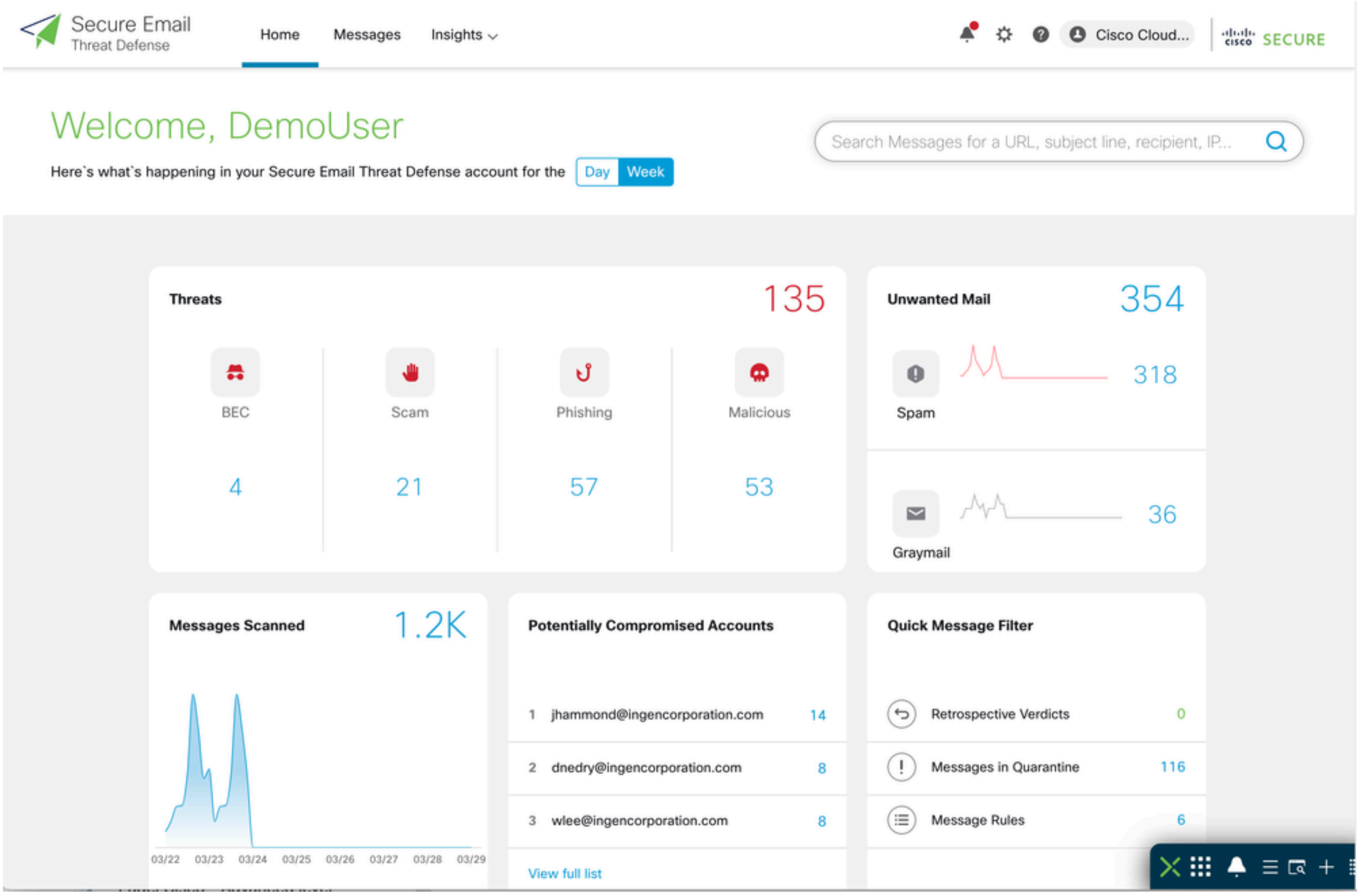
## Layer 9: Augment Spoofing Detection Capability with Cisco Secure Email Threat Defense (ETD)

Cisco offers Email Threat Defense, a cloud-native solution leveraging superior threat intelligence from Cisco Talos. It has an API-enabled architecture for faster response times, complete email visibility, including internal emails, a conversation view for better contextual information, and tools for auto or manual remediation of threats lurking in Microsoft 365 mailboxes. Visit the Cisco Secure Email Threat Defense Data Sheet for more details.

Cisco Secure Email Threat Defense combats phishing using sender authentication and BEC detection capabilities. It integrates machine learning and Artificial Intelligence engines that combine local identity and relationship modeling with real-time behavior analytics to protect against identity deception-based threats. It models trusted email behavior within organizations and between individuals. Among other key features, Email Threat Defense provides these benefits:

- Uncover known, emerging, and targeted threats with advanced threat detection capabilities.
- Identify malicious techniques and gain context for specific business risks.
- Rapidly search for dangerous threats and remediate them in real-time.
- Utilize searchable threat telemetry to categorize threats and understand which parts of your organization are most vulnerable to attack.

*Figure 14. Cisco Secure Email Threat Defense provides information about how your organization is being targeted.*



Welcome, DemoUser

Here`s what`s happening in your Secure Email Threat Defense account for the Day Week

**Threats** 135

| BEC | Scam | Phishing | Malicious |
|---|---|---|---|
| 4 | 21 | 57 | 53 |

**Unwanted Mail** 354

| | |
|---|---|
| Spam | 318 |
| Graymail | 36 |

**Messages Scanned** 1.2K

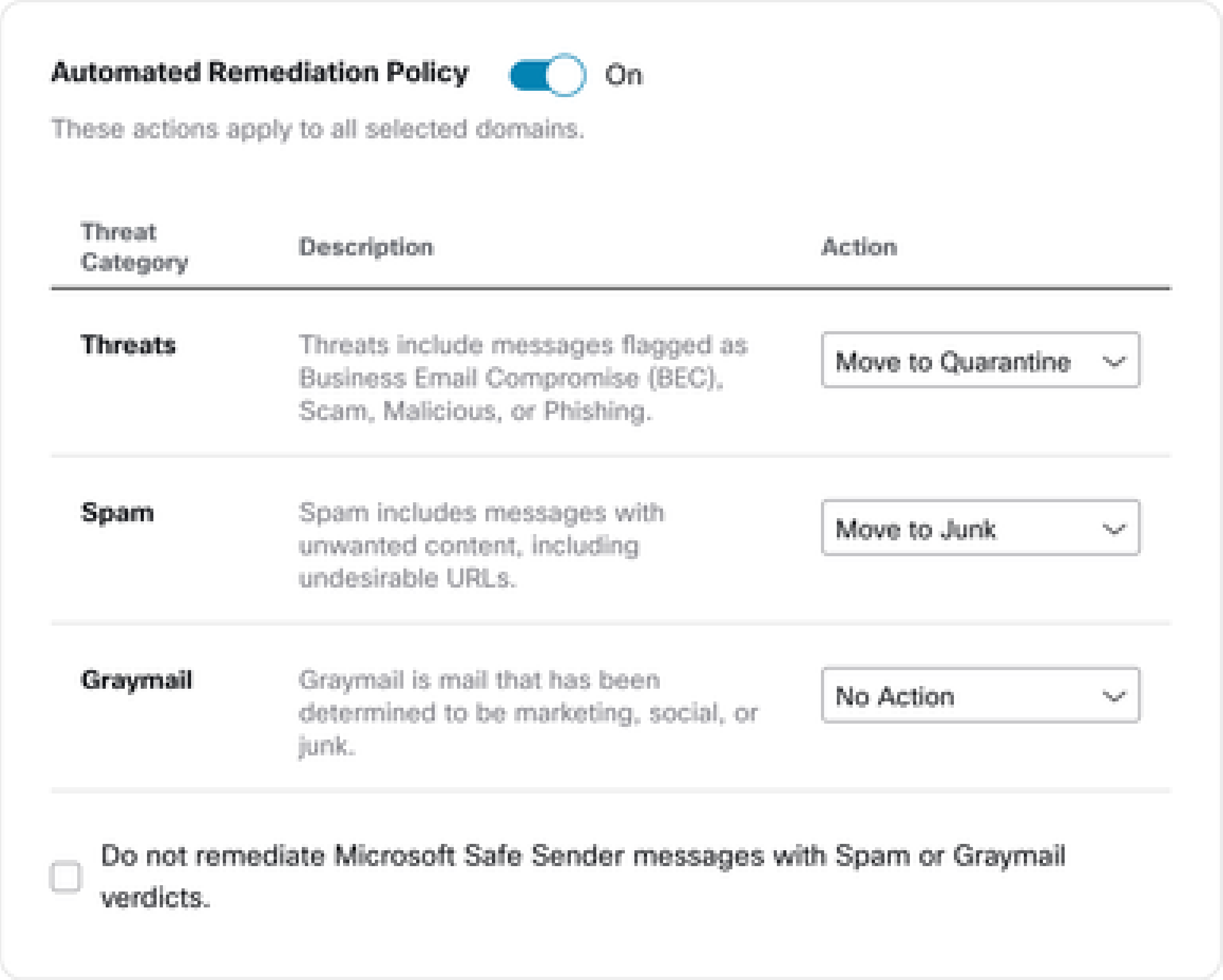
**Potentially Compromised Accounts**

| | | |
|---|---|---|
| 1 | jhammond@ingencorporation.com | 14 |
| 2 | dnedry@ingencorporation.com | 8 |
| 3 | wlee@ingencorporation.com | 8 |

**Quick Message Filter**

| | |
|---|---|
| Retrospective Verdicts | 0 |
| Messages in Quarantine | 116 |
| Message Rules | 6 |

Image 15. The Cisco Email Threat Defense Policy Setting Automatically Determines if the Message Matches the Selected Threat Category



Automated Remediation Policy On

These actions apply to all selected domains.

| Threat Category | Description | Action |
|---|---|---|
| Threats | Threats include messages flagged as Business Email Compromise (BEC), Scam, Malicious, or Phishing. | Move to Quarantine |
| Spam | Spam includes messages with unwanted content, including undesirable URLs. | Move to Junk |
| Graymail | Graymail is mail that has been determined to be marketing, social, or junk. | No Action |

□ Do not remediate Microsoft Safe Sender messages with Spam or Graymail verdicts.

# What More Can You Do with Spoofing Prevention

Many spoofs can be remediated with a few simple precautions that include, but are not limited to these:

- Limit allow listed domains in the Host Access Table (HAT) to very few core business partners.
- Continuously track and update members in the SPOOF_ALLOW sender group if you have created one and use the instructions given in the best practices link.
- Enable graymail detection and place them in the spam quarantine as well.

But most important of all, enable SPF, DKIM, and DMARC and implement them appropriately. However, the guidance on publishing SPF, DKIM, and DMARC records is beyond the scope of this document. For that, refer to this white paper: Email Authentication Best Practices: The Optimal Ways To Deploy SPF, DKIM, and DMARC.

Understand the challenge of remediating email attacks like the spoofing campaigns discussed here. If you have questions about implementing these best practices, contact Cisco Technical Support and open a case. Alternatively, contact your Cisco Account Team for a solution and design guidance. For more information about Cisco Secure Email, refer to the Cisco Secure Email website.