How-To Enable Forged Email Detection (FED) on Cisco Email Security

Beginning with AsyncOS 10.0
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About This Document</td>
<td>3</td>
</tr>
<tr>
<td>Introduction to Business Email Compromise (BEC)</td>
<td>3</td>
</tr>
<tr>
<td>Cisco Forged Email Detection (FED) Settings</td>
<td>4</td>
</tr>
<tr>
<td>Cisco Forged Email Detection (FED) In Action</td>
<td>6</td>
</tr>
</tbody>
</table>
About This Document

This document is for Cisco® engineers and customers who will deploy Cisco Email Security using AsyncOS.

This document covers:

• Identifying a forged email
• Forged Email Detection
• Forged Email Detection in action

Introduction to Business Email Compromise (BEC)

Email forging (also known as spoofing, CEO fraud, or business email compromise) is the process of altering the message header to hide the real identity of the sender and to make it look like a legitimate message from someone you know.

Briefly described, email forging attacks fall into the following categories:

1. “Envelope From” abuse: This includes making the domain in the sender’s “Mail From” value (also referred to as “Envelope From”) the same as the recipient’s domain. This paper uses the terms “Mail From” and “Envelope From” interchangeably.

2. From header abuse: Using a legitimate domain for the sender’s Envelope From value but using a fraudulent From header.

3. Cousin domain abuse: Sending email from cousin domains that pass Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-Based Message Authentication, Reporting, and Conformance (DMARC) checks. The From value will show a similar sender address that impersonates a real one (for example, using alice@a1pha.com to impersonate alice@alpha.com).

4. Free email account abuse: Using free email (Yahoo, Gmail, etc.) that pass SPF, DKIM and DMARC checks. The From header will show a legitimate sender address with an executive’s name@gmail.com.

The first two categories are abuses of the owner’s domain name in the Envelope From value in the internet headers or the From value in the message body. The basic structure of the second category is shown in Figure 1. Cisco Email Security can remediate these locally by using sender verification and content filters that track and permit only legitimate senders to spoof your domain. Or the same results can be achieved globally by using DMARC, DKIM, and SPF. In this case, your DNS text records must reflect third-party servers that can legitimately send to your employees while spoofing your domain. This allows inbound 401K or health notices while remediating fraudulent ones.

Techniques for addressing categories 1 and 2 are discussed in:

• Forged Email: Detect Spoofing with Cisco Email Security (a white paper)
• SPF / DKIM / DMARC Recommended Deployment (Cisco Email Security Appliance best practices guide)

Figure 1. From Header Abuse

<table>
<thead>
<tr>
<th>mail-from: <a href="mailto:somebodyelse@nottrustworthy.com">somebodyelse@nottrustworthy.com</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>From: Executive Name <a href="mailto:executive.name@company.com">executive.name@company.com</a></td>
</tr>
<tr>
<td>To: Target Name <a href="mailto:target.name@mycompany.com">target.name@mycompany.com</a></td>
</tr>
</tbody>
</table>

The last two categories are not a violation of the domain portion. Malvestors will also construct messages where the mail-from and From values agree, and then publish DKIM and SPF records. So the incoming message is technically legitimate and therefore, cannot be blocked using DNS text records or sender verification. For example, the message may be from a free email account: Executive Name <executive.name@gmail.com>. When viewed on a mobile device, all that is seen is “From: Executive Name”.

Similarly, cousin domains that look like our sample domain could also be registered in DNS with text records as: nycompany.com, mycomqany.com, myc0mpany.com.

Since the last two categories will also spoof the name portion of the message, Cisco® Forged Email Detection (FED) is ideal to remediate these types of spoofs. Given that you know the executive names in your company, you can create a dictionary of these names and then reference that dictionary with the FED condition in message filters or content filters. Before implementing the FED feature, you want to consider a test period for determining who is spoofing your organization, and which spoofers are legitimate. To do so, read the white paper, Forged Email: Detect Spoofing with Cisco Email Security.
Cisco Forged Email Detection (FED) Settings

Step 1. Identify the users in your organization (for example, executives) whose messages are likely to be forged. Create a new content dictionary and add the names of the identified users to it. While creating a content dictionary:

a. Enter the name of the user and not the email address. For example, enter “Olivia Smith” instead of “olivia.smith@example.com”.
b. Do not configure Advanced Matching and Smart Identifiers.
c. Do not choose weight for the terms used.
d. Do not use regular expressions.

To create a dictionary, select: Mail Policies > Dictionaries > Add Dictionary

Figure 2 shows a sample dictionary.

Figure 2. Dictionary

Step 2. Create an incoming content or message filter to detect forged messages and the actions that the appliance must take on such messages.

a. To create a Content Filter, select: Mail Policies > Incoming Content Filters > Add Filter.
b. Use the following: Condition/Rule: Forged Email Detection
c. Select the dictionary that you just created. In our example, our dictionary name is FED.
d. Click OK (See Figure 3.)

Figure 3. FED Condition

Step 3. Add the FED Action

a. Click: Add Action
b. Select: Forged Email Detection
c. Click OK (See Figure 4.)
Step 4. Prepend the subject header with: [WARNING Possible Business Email Compromise]

a. Click: Add Action
b. Select: Add/Edit Header
c. In the Header Name field enter: Subject
d. Select: Prepend to the Value of Existing Header
e. Enter: [WARNING Possible Business Email Compromise]
f. Click: OK
g. Click: Submit (See Figure 5.)

Step 5. Apply the filter to an incoming mail policy

a. Click: Mail Policies > Incoming Mail Policy.
b. Select the policy to which you want to apply the FED filter. In our example it is the default mail policy.
c. Click: Disabled in the Content Filters column.
d. Select: Enable Content Filters (Customize Settings) in the dropdown menu.
e. Check the Enable box for the filter you created (Forged_Email_Detection).
f. Click: Submit and Commit Changes.
Cisco Forged Email Detection (FED) in Action

Removal of From Value

Figure 6 shows two forged emails sent into a fictitious company named Alpha. The message purports to be from an Alpha executive named Chuck Robbins. The first is allowed in without any modification. The second has been modified by the FED filter. Note that by viewing the first in the inbox listing, you see only the name of the sender and not the domain (gmail.com) that it was sent from. But in the second message, the From value, Chuck Robbins, has been replaced with the Envelope From value, chuck.robbins@gmail.com, so that the recipient knows that this is from an external source and what that source is.

Figure 6. Forged Email Samples

BEC Evidence Shared with Recipient

In Figure 7, we show the Internet Mail Headers for the modified message. In Outlook 2010, you can find this by opening the message and then clicking on: File Tab > Properties

The FED action copies the original From value into an X-header called X-original-from. This allows the administrator to verify the effectiveness of the filter and provides a reason to the recipient as to why the message was acted upon.

Figure 7. X-Original-From

Watch this video for more details: Protect Against Email Spoofing with Cisco Forged Email