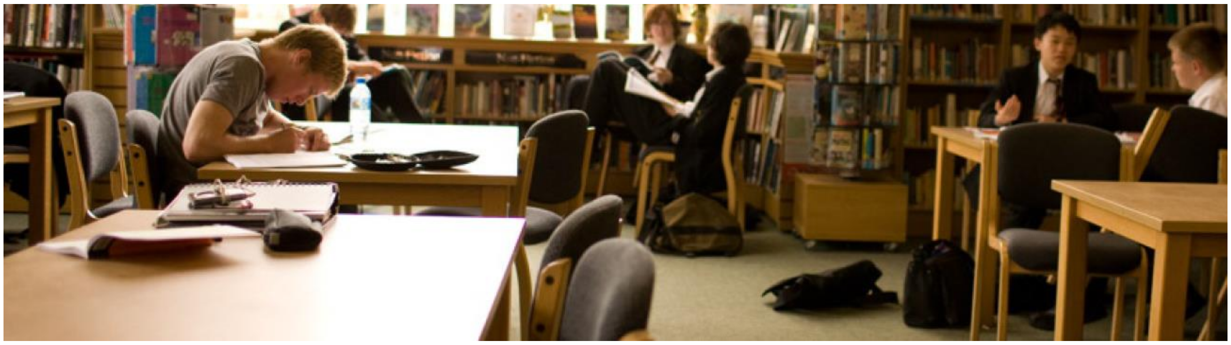
White Paper

Forged Email Detection (FED) With

Cisco Email Security



Forged email, AKA Email spoofing, is the creation of email messages with a forged sender address. It is easy to do because the core protocols do not have any mechanism for authentication. It can be accomplished from within a LAN or from an external environment using Trojan horses.[1] Spam and phishing emails typically use such spoofing to mislead the recipient about the origin of the message.[2] reference: https://en.wikipedia.org/wiki/Email_spoofing.

This Whitepaper is based on AsyncOS 9.7.1. AsyncOS 10.0 has a new feature “Forged Email Detection” that has a dedicated content filter and Executive Dictionary for this purpose. Since the 10.0 feature FED addresses **From** abuse in the message body, it can be used instead of the content and message filters discussed here for 9.7.1. Refer to the 10.0 Admin Guide for specifics on that application. Besides the FED feature application, all other suggestions; General Best Practices etc. apply to both releases.

Table of Contents

Forged Email Problem

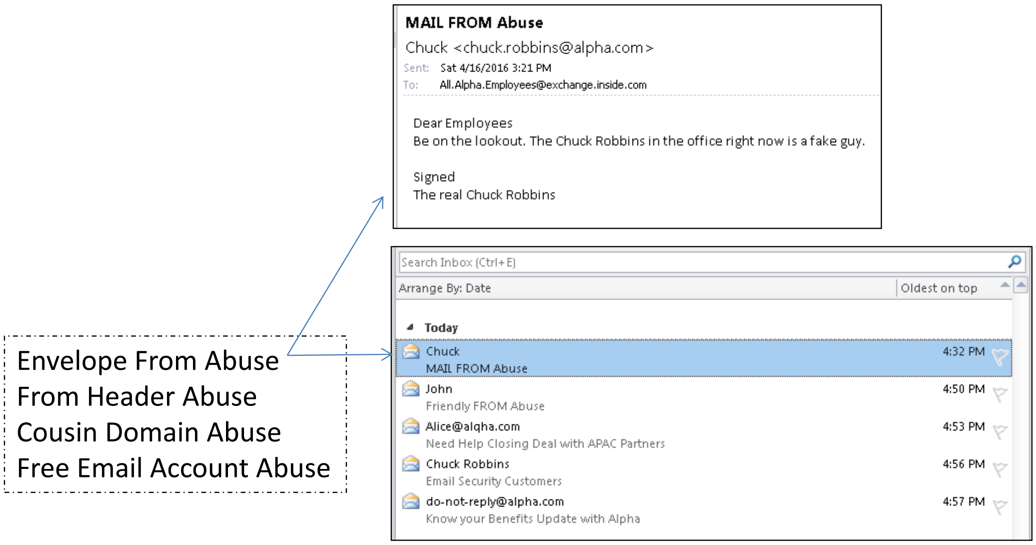
This paper focuses on the resolution of spoofs from outside an organization where the senders are impersonating employees inside the organization. Their purpose is to deceive employees in order to steal money or information. We will discuss four different variants of this attack, and propose solutions for this using Cisco's Email Security Solution running AsyncOS 9.7.1. Addressing circumstances of spoofing where an internal mailbox is compromised is out of scope for this paper. For an introduction to spoofing refer to: http://blogs.cisco.com/security/what-is-email-spoofing-and-how-to-detect-it. In all examples in this document, alpha.com is the example customer domain being spoofed.

Briefly described, spoofing attacks include:

1. Envelope From Abuse: Making the domain in sender's **mail From** value, also referred as "Envelope From" the same as the recipient domain: (This paper uses these terms interchangeably)
2. From Header Abuse: Using a legitimate domain for the sender's **envelope from** value but a fraudulent **From Header**
3. Cousin Domain Abuse: Sending from cousin domains that pass SPF, DKIM and DMARC checks. The **From** value will show a legitimate sender address ie: 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 executives name@gmail.com

The four variants of attacks described above, are shown below in the mailbox alan@alpha.com. The variants are listed from top down in the same order described earlier, along with a legitimate healthcare mailer in Figure 1. Each fraud lists an executives name in the From field. Figure 2 shows the details of an attack similar to the first variant in Figure 1. Our goal is to block any spoofs in these categories, but allow legitimate mailers, like the one sending the healthcare notice, to be delivered.

Figure 1. Forged Mail Attacks on mailbox alan@alpha.com



MAIL FROM Abuse

Chuck <chuck.robbins@alpha.com>

Sent: Sat 4/16/2016 3:21 PM

To: All.Alpha.Employees@exchange.inside.com

Dear Employees
Be on the lookout. The Chuck Robbins in the office right now is a fake guy.

Signed
The real Chuck Robbins

Chuck — MAIL FROM Abuse — 4:32 PM

John — Friendly FROM Abuse — 4:50 PM

Alice@alqha.com — Need Help Closing Deal with APAC Partners — 4:53 PM

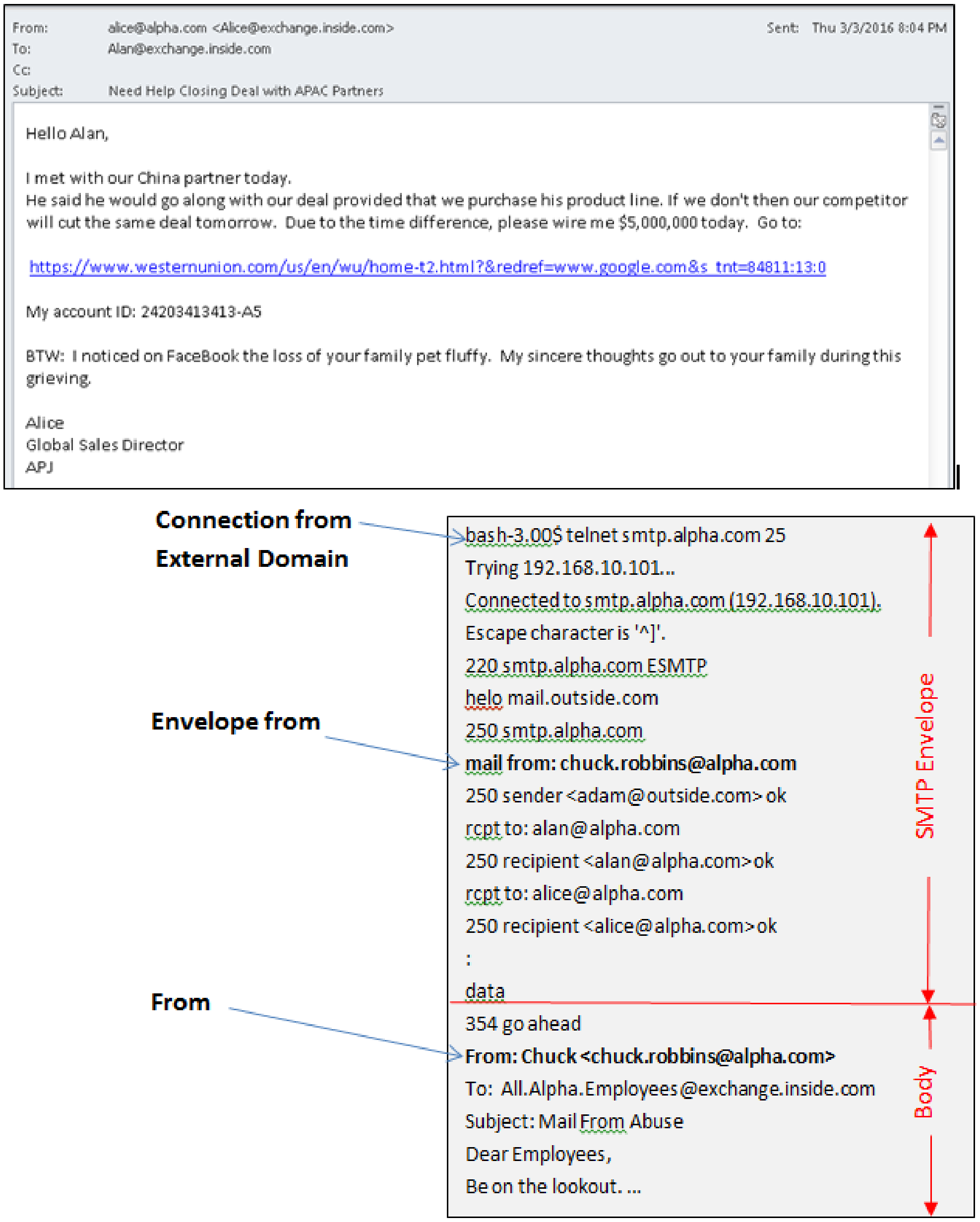
Chuck Robbins — Email Security Customers — 4:56 PM

do-not-reply@alpha.com — Know your Benefits Update with Alpha — 4:57 PM

Anatomy of a Forged Email and its SMTP Details

The structure of the message in Figure 2 is very similar to our first variant in Figure 1. Both are examples of “Envelope From Abuse. The Envelope From field, shown below in the SMTP connection, is illegally using the domain name **alpha.com**. Envelope From abuse is easily remediated with Sender Verification, discussed later. But the problem is that Sender Verification only checks the SMTP Envelope portion shown in Figure 2. The harder to detect spoofs introduced earlier: From abuse, Cousin Domain abuse and Free email account abuse all have legal SMTP Envelope portions, but their Body portions of the message, see Figure 2, are designed to deceive the recipient. These two portions do not have to agree. In fact there are legitimate external mailing lists in which they may not.

Figure 2. SMTP Envelope and Body of “Envelope From Abuse”.



From: alice@alpha.com <Alice@exchange.inside.com> Sent: Thu 3/3/2016 8:04 PM
To: Alan@exchange.inside.com
Cc:
Subject: Need Help Closing Deal with APAC Partners

Hello Alan,

I met with our China partner today.
He said he would go along with our deal provided that we purchase his product line. If we don't then our competitor will cut the same deal tomorrow. Due to the time difference, please wire me $5,000,000 today. Go to:

https://www.westernunion.com/us/en/wu/home-t2.html?&redref=www.google.com&s_tnt=84811:13:0

My account ID: 24203413413-A5

BTW: I noticed on FaceBook the loss of your family pet fluffy. My sincere thoughts go out to your family during this grieving.

Alice
Global Sales Director
APJ

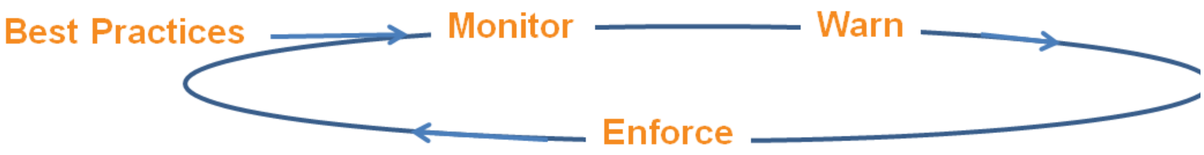
```
bash-3.00$ telnet smtp.alpha.com 25
Trying 192.168.10.101...
Connected to smtp.alpha.com (192.168.10.101).
Escape character is '^]'.
220 smtp.alpha.com ESMTP
helo mail.outside.com
250 smtp.alpha.com
mail from: chuck.robbins@alpha.com
250 sender <adam@outside.com> ok
rcpt to: alan@alpha.com
250 recipient <alan@alpha.com> ok
rcpt to: alice@alpha.com
250 recipient <alice@alpha.com> ok
:
data
354 go ahead
From: Chuck <chuck.robbins@alpha.com>
To: All.Alpha.Employees@exchange.inside.com
Subject: Mail From Abuse
Dear Employees,
Be on the lookout. ...
```

TOC

Forged Email Detection Workflow

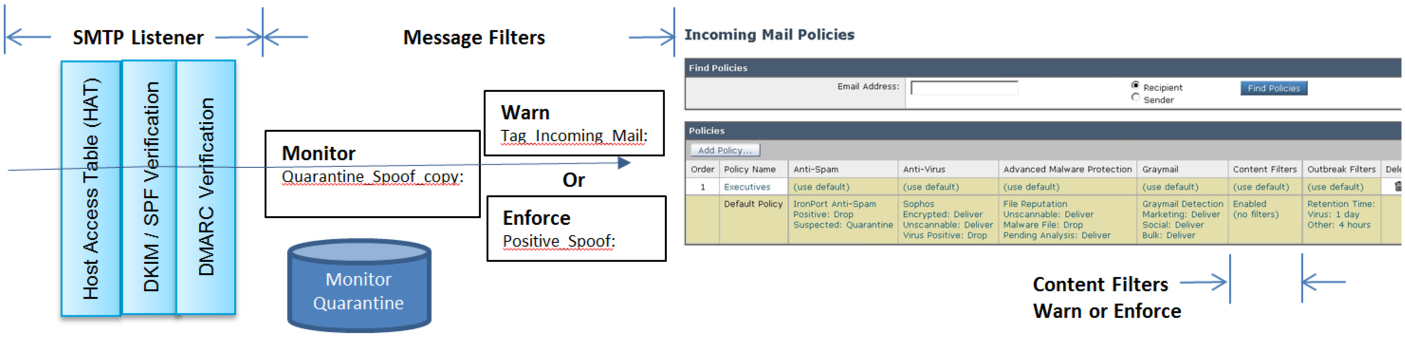
The default settings of Cisco Email Security will prevent broad-based attacks, such as malicious files and snowshoe spam. However spoofing, like other targeted attacks, is tailored for a specific organization. For that reason, preventative tools for spoofing attacks are disabled as their application may vary from one organization to another, and their improper application can lead to a high incidence of false positives. The FED workflow in Figure 3 is a high level view for remediating spoofing attacks on your organization. We will provide details on each step. The final result is a defense in depth approach to Forged Email Detection. Since a targeted attacker will change their methods against an organization over time, the administrator needs to monitor this change and follow up with appropriate warnings and enforcements.

Figure 3. FED Workflow



The elements that address “Best Practice settings”, and filters that monitor, warn and enforce against spoofing attacks are shown below in Figure 4. The Monitor should quarantine copies of all possible spoofs, illegitimate as well as legitimate mailers for one week and then delete. The admin must update the Enforce filter based on what it missed, but was caught by Monitor or by a recipient. We will reference this diagram throughout this whitepaper.

Figure 4. Cisco Email Security Pipeline



Find Policies

Email Address: ● Recipient ○ Sender

Policies

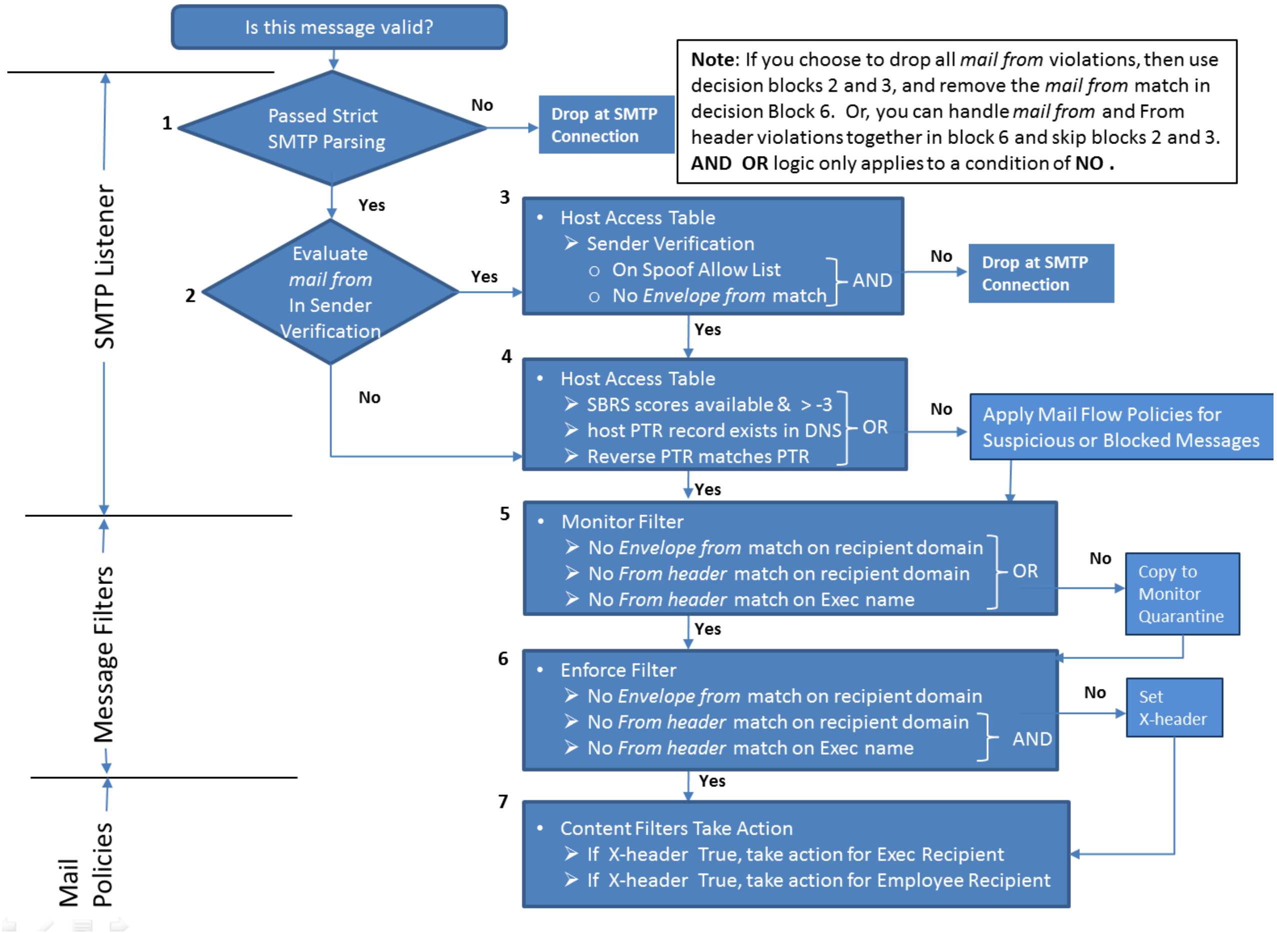
Order	Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters	Dele
1	Executives	(use default)	(use default)	(use default)	(use default)	(use default)	(use default)	🗑
	Default Policy	IronPort Anti-Spam Positive: Drop Suspected: Quarantine	Sophos Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	File Reputation Unscannable: Deliver Malware File: Drop Pending Analysis: Deliver	Graymail Detection Marketing: Deliver Social: Deliver Bulk: Deliver	Enabled (no filters)	Retention Time: Virus: 1 day Other: 4 hours	

TOC

Forged Email Detection Decision Tree

The decision tree in Figure 5 is structured to detect and remediate any of the four spoofs shown in Figure 1. Sender Verification in decision blocks 2 and 3 are redundant to the condition: “No *Envelope from* match on recipient domain” in blocks 5 and 6. If your filters follow this design, then use either one or the other. Dropping *mail from* violations at the SMTP connection assumes that you have no need to analyze the message content for a False Positive. Our Monitor Filter conditions in decision block 5 have a broader range of matches than the Enforce Filter in block 6 due the use of OR and AND logic. Your filter logic may be different than these, but you should follow the same approach: monitor liberally but enforce conservatively. The Enforce filter is a message filter that sets an X-header before policies are applied downstream. This allows us to take action in decision block 7 with those policies by applying content filters within them. For example a message that is tagged with a spoof X-header needs to be handled differently when the recipient is an executive verses a standard employee. This whitepaper will look at these blocks individually by demonstrating how they remediate the specific spoofs discussed at the beginning. At the conclusion we will combine all of these together in a solution described by this decision tree. For the reader, it is a good plan to make a similar decision tree for your email solution before you begin to apply your anti-spoofing polices.

Figure 5. Decision Tree



Is this message valid?
SMTP Listener
Message Filters
Mail Policies
1
Passed Strict SMTP Parsing
No
Drop at SMTP Connection
Note: If you choose to drop all mail from violations, then use decision blocks 2 and 3, and remove the mail from match in decision Block 6. Or, you can handle mail from and From header violations together in block 6 and skip blocks 2 and 3. AND OR logic only applies to a condition of NO .
Yes
2
Evaluate mail from In Sender Verification
Yes
3
Host Access Table
Sender Verification
On Spoof Allow List
No Envelope from match
AND
No
Drop at SMTP Connection
Yes
No
4
Host Access Table
SBRS scores available & > -3
host PTR record exists in DNS
Reverse PTR matches PTR
OR
No
Apply Mail Flow Policies for Suspicious or Blocked Messages
Yes
5
Monitor Filter
No Envelope from match on recipient domain
No From header match on recipient domain
No From header match on Exec name
OR
No
Copy to Monitor Quarantine
Yes
6
Enforce Filter
No Envelope from match on recipient domain
No From header match on recipient domain
No From header match on Exec name
AND
No
Set X-header
Yes
7
Content Filters Take Action
If X-header True, take action for Exec Recipient
If X-header True, take action for Employee Recipient

TOC

General Best Practices to Prevent Spoofing

Before configuring specific filters, recognize that our spoof samples are corner case attacks on Alpha Inc. Many spoofs are remediated by exercising best practices. Referencing the pipeline in Figure 4, these are:

- Limit the use of Whitelisted domains in the Host Access Table (HAT) to a very few core business partners.
- Track and update members in your SPOOF_ALLOW sender group (HAT), if you have one.
- Track and Update Allowed Senders in your SPF records, if you publish them.
- Drop Positively Identified spam
- Enable Gray Mail Detection and flag or place instances in the Spam Quarantine
- Enable URL Filtering to give maximum visibility into URL-based threats
- Enable Message Modification in Outbreak Filters to rewrite Suspicious and Malicious URLs
- Publish your companies DKIM, SPF and DMARC records
- Enable DMARC verification
- Modify your Host Access Table (to address spoofing, see below)

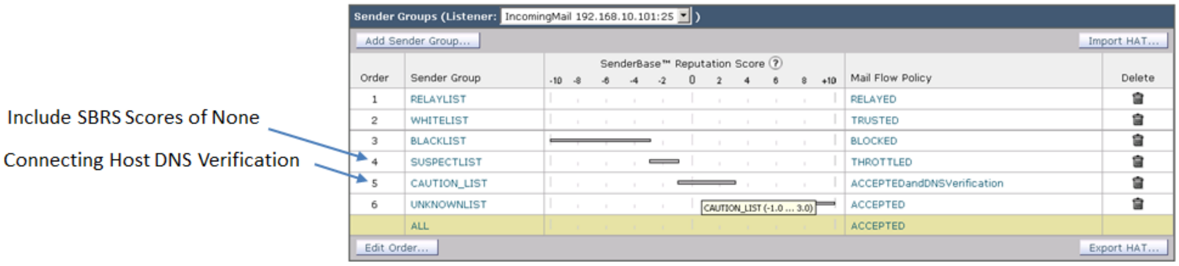
Details on these best practices are available at: http://www.cisco.com/c/en/us/products/collateral/security/email-security-appliance/white-paper-c11-732910.html.

Note: Publishing DNS TXT records for sender authentication allows for greater efficacy in fraud detection than maintaining dictionaries alone. However, methods of publishing these are beyond the scope of this whitepaper.

Host Access Table Modification to Prevent Spoofing

Reference decision blocks 2, 3 and 4 in Figure 5. Incoming messages that fail a DNS check OR do not have any SBRS scores will drop to the UNKNOWNLIST. To avoid that for spoof Envelope From Abuse, here we've segmented off part of the UNKNOWNLIST SBRS range for a CAUTION_LIST below in Figure 5. Lists numbered 4 and 5 have "Include SBRS Scores of None" for 4 and "Connecting Host DNS Verification" for 5 enabled. This allows you to specialize the Mail Flow Policies for messages that fail these checks. You may be introducing delays for some legitimate messages. Not shown here, would be an ALLOWED_SPOOFERs list for legitimate mailers that can send into your organization.

Figure 6. Modified Host Access Table to Address Forged Mail


Include SBRS Scores of None
Connecting Host DNS Verification
Sender Groups (Listener: IncomingMail 192.168.10.101:25)
Add Sender Group...
Import HAT...
-10 -8 -6 -4 -2 0 2 4 6 8 +10
CAUTION_LIST (-1.0 ... 3.0)
Edit Order...
Export HAT...

Order	Sender Group	SenderBase™ Reputation Score	Mail Flow Policy	Delete
1	RELAYLIST		RELAYED	🗑
2	WHITELIST		TRUSTED	🗑
3	BLACKLIST		BLOCKED	🗑
4	SUSPECTLIST		THROTTLED	🗑
5	CAUTION_LIST		ACCEPTEDandDNSVerification	🗑
6	UNKNOWNLIST		ACCEPTED	🗑
	ALL		ACCEPTED	

Manual telnet of the SMTP connection can accidentally break syntax rules in RFC 2821. You can catch these with "Strict" Address Parsing on the Listener, see decision block 1 Figure 5. This will catch some, but the sophisticated attackers won't be dissuaded by this.

Forged Mail Resolution

It is not typical for a Cisco customer to encounter all of these spoofing variants described in the Problem Section, but many are plagued by at least one. As a case study, we will be treating this multi-variant attack on the alpha.com domain for framing our suggested solutions. They come from Cisco Email Security experts with real world experience who have been working to protect customers from these attacks. These are suggestions rather than fixed antidotes for particular problems. The examples and solutions presented are provided as guidelines to assist with remediating these abusive messages. Implement these solutions in an ongoing process of: Monitor, Warn and Enforce.

Monitor

You need to monitor all inbound spoofing traffic, legitimate and illegitimate. For that, identify domain names that should not be values in the **envelope from** or **From** headers and make them members of a dictionary, as we've done in Figure 4 with "No_Spoof_Domains". Create a filter to make a copy of every email where the MAIL FROM or the From header matches domains in the dictionary into a "Spoofs" Quarantine, with a reasonable Delete on Expire policy (possibly 7 days). This gives you visibility into what is being spoofed. Also consider spoofing from legitimate mailer services that are abused by illegitimate clients. Focusing on the From header, make a dictionary for executive names called "Execs". Also, internal group names such as "IT-Support-Services" that should not be in the From header. One form of malware attack is to infect an internal client, thus causing it to harvest the LDAP directory for executive names and group mailing lists. All of the possible violations of **From**, and mail from values resulting from such a query need to be considered in your monitor message filter.   Copy the filter matches to quarantine and possibly notify the admin with a copied attachment, see Figure 7 below. Send the original message to recipient untouched.

Figure 7. Message Filter: Monitor All Spoof

Monitor

```
Quarantine_Spoof_copy:
If sendergroup != "RELAYLIST" AND (
mail-from-dictionary-match("No_Spoof_Domains", 1) OR
header-dictionary-match("No_Spoof_Domains","From", 1) OR
header-dictionary-match("Execs","From", 1))
{
duplicate-quarantine("All_Spoofs");
notify-copy ("brenda@notes.bravo.com");
}
    .
```

TOC

Warn

Modifying the subject header of incoming messages will break digital signatures. However, warning all employees receiving an incoming message with the subject tag [External Sender], Figure 8 below, is suggested until an “Enforecement Policy” is in place. The day that a spoofing attack is realized, you need to begin both warn and monitor phases of your defense. See the relative positions of filters in Figure 8 below in the Pipeline shown in Figure 4. Once the encforcement filter is in place, you can remove the Warning Filter.

Figure 8. Message Filter: Tag All Incoming Messages

```
Warn
Tag_Incoming_Mail:
If sendergroup != "RELAYLIST"
{
edit-header-text("Subject", "(.*)", "[External Sender]\\1");
}
    .
```

TOC

Enforce

Based on what you collect during the monitoring phase, write filters to address the particular spoofing types. Continue to run the monitoring as a separate process and a separate quarantine to catch false negatives. You should monitor aggressively but enforce conservatively. Start your enforcement filters with quarantine copy as your remediation along with modifying the original messages subject with appropriate warning prior to sending to the recipient. As you gain more confidence in your enforcement filter, change to quarantining, or dropping the original message. Maintain your monitor quarantine to catch samples missed by enforcement and update your enforcement filter as needed.

Addressing Envelope From Abuse

Below are the logs from two messages in Alan's mailbox titled: "Mail From Abuse" and "Know your Benefits update from Alpha". wsa.train is an illegitimate sender and mail.outside.com is a legitimate one.

Subject: Mail From Abuse from Alpha

```
New SMTP ICID 147 interface Data 1 (192.168.10.101) address
192.168.42.2 reverse dns host vmware-inside.wsa.train verified no
ICID 147 ACCEPT SG UNKNOWNLIST match sbrs[none] SBRS rfc1918
Start MID 1321 ICID 147
MID 1321 ICID 147 From: <chuck.robbins@alpha.com>
MID 1321 ICID 147 RID 0 To: <alan@exchange.alpha.com>
MID 1321 Subject 'MAIL FROM Abuse'
```

Subject: Know your Benefits update from Alpha

```
New SMTP ICID 151 interface Data 1 (192.168.10.101) address
192.168.10.200 reverse dns host mail.outside.com verified yes
ICID 151 ACCEPT SG UNKNOWNLIST match sbrs[none] SBRS
rfc1918
Start MID 1325 ICID 151
MID 1325 ICID 151 From: <Employee_Benefits@alpha.com>
MID 1325 ICID 151 RID 0 To: <alan@exchange.alpha.com>
MID 1325 ICID 151 RID 1 To: alice@notes.alpha.com
MID 1325 Subject 'Know your Benefits Update with Alpha'
```

Note: In the above logs; the "From" and "To" are actually "mail from" and "rcpt to" respectively in the SMTP envelope. The same is true for Message Tracking reports. The following proceedure using Sender Verification, will drop mail from violations in the SMTP connection. You can also do the same with a message filter.

Recommended Remediation: Identify legitimate and illegitimate in the **mail from** field. Allow legitimate senders while blocking illegitimate ones with configuration in:

1. Configure Mail Flow Policy
2. Configure the HAT
3. Configure the Exception Table

See Techzone article: https://techzone.cisco.com/t5/Email-Security-Appliance-ESA/Spoof-Protection-using-Sender-Verification/ta-p/273384

Or YouTube VoD: https://www.youtube.com/watch?v=mG86aih6Pko&list=PLURIAlKNm1OfUONNsRERA-VtX2WiYNS6P&index=

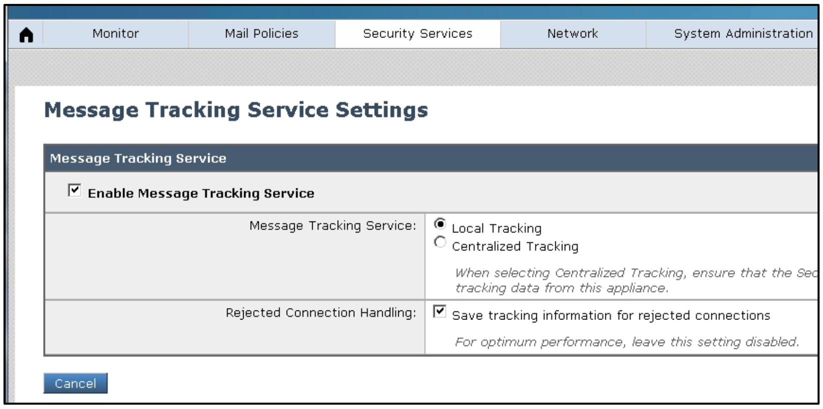
When using Sender Verification, you must know the details of any legitimate mailers so that you can add their domains to your SPOOF_ALLOW Sender Group. Sender Verification will block all domains that use your domain in the Envelope From, including legitimate senders, if you don't implement exceptions for them. Messages that illegitimately use your domain will be dropped at the beginning of the SMTP conversation in the Listener at the HAT. See Figure 4 for this position in the pipeline.

TOC

Verifying Remediation of Envelope From Abuse

After enabling Sender Verification, it is useful to track rejected connections, just in case you missed adding any legitimate mailers in your SPOOF_ALLOW Sender Group. Until you are certain, you may want to enable “Rejected Connection Handling” in Message Tracking shown in Figure 9 for message tracking on legitimate and illegitimate Envelope From Spoofs as shown in Figure 10.

Figure 9. Message Tracking



Message Tracking Service Settings

Message Tracking Service

☑ Enable Message Tracking Service

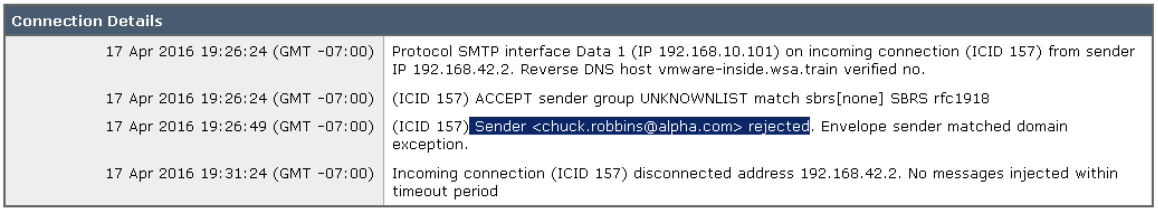
Message Tracking Service: ● Local Tracking ○ Centralized Tracking

When selecting Centralized Tracking, ensure that the Sec tracking data from this appliance.

Rejected Connection Handling: ☑ Save tracking information for rejected connections

For optimum performance, leave this setting disabled.

Figure 10. Rejected Envelope From Abuse



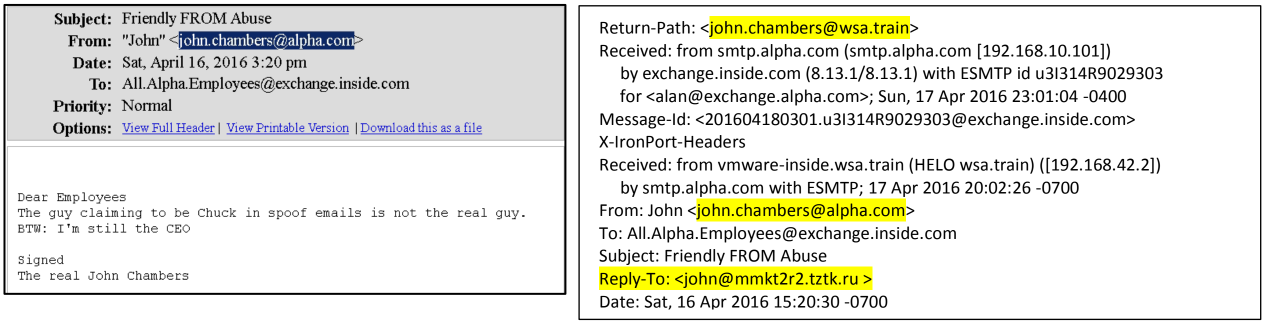
Connection Details	
17 Apr 2016 19:26:24 (GMT -07:00)	Protocol SMTP interface Data 1 (IP 192.168.10.101) on incoming connection (ICID 157) from sender IP 192.168.42.2. Reverse DNS host vmware-inside.wsa.train verified no.
17 Apr 2016 19:26:24 (GMT -07:00)	(ICID 157) ACCEPT sender group UNKNOWNLIST match sbrs[none] SBRS rfc1918
17 Apr 2016 19:26:49 (GMT -07:00)	(ICID 157) Sender <chuck.robbins@alpha.com> rejected. Envelope sender matched domain exception.
17 Apr 2016 19:31:24 (GMT -07:00)	Incoming connection (ICID 157) disconnected address 192.168.42.2. No messages injected within timeout period

Once you are confident that SPOOF_ALLOW Sender Group is correctly populated, you should disable Rejected Connection Handling for optimum performance.

Addressing From Header Abuse

Sender Verification will not stop messages where the Envelope from and From Header values do not agree. The following message was delivered after Sender Verification was enabled. Here is a sample caught by our Monitoring Filter but missed by Sender Verification.

Figure 11. From Header Abuse



Subject: Friendly FROM Abuse
From: "John" <john.chambers@alpha.com>
Date: Sat, April 16, 2016 3:20 pm
To: All.Alpha.Employees@exchange.inside.com
Priority: Normal
Options: View Full Header | View Printable Version | Download this as a file

```
Dear Employees
The guy claiming to be Chuck in spoof emails is not the real guy.
BTW: I'm still the CEO

Signed
The real John Chambers
```

```
Return-Path: <john.chambers@wsa.train>
Received: from smtp.alpha.com (smtp.alpha.com [192.168.10.101])
    by exchange.inside.com (8.13.1/8.13.1) with ESMTP id u3I314R9029303
    for <alan@exchange.alpha.com>; Sun, 17 Apr 2016 23:01:04 -0400
Message-Id: <201604180301.u3I314R9029303@exchange.inside.com>
X-IronPort-Headers
Received: from vmware-inside.wsa.train (HELO wsa.train) ([192.168.42.2])
    by smtp.alpha.com with ESMTP; 17 Apr 2016 20:02:26 -0700
From: John <john.chambers@alpha.com>
To: All.Alpha.Employees@exchange.inside.com
Subject: Friendly FROM Abuse
Reply-To: <john@mmkt2r2.tztk.ru >
Date: Sat, 16 Apr 2016 15:20:30 -0700
```

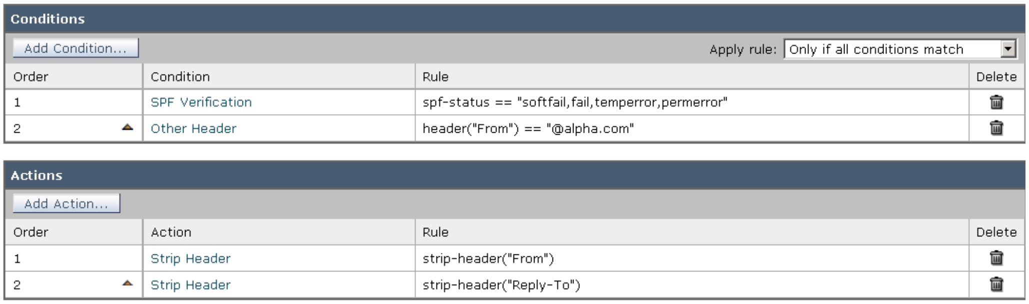
The challenge is the recipient interpreting the **From**: “John” <john.chambers@alpha.com> as an internal sender, and reacting to its call to action. For example, sensitive corporate information could be sent back to Reply-To: <john@mmkt2r2.tztk.ru>. The recipients are unaware of the actual sender’s mailbox john.chambers@wsa.train since they can’t see the Return-Path as well as the Reply-To address in the client (Outlook, for instance), unless viewing the detailed headers. Most mobile devices cannot provide this detail. Outlook hides it by default.

There two methods to detect this From value:

1. Publish SPF records for your domain alpha.com, and enable SPF/SIDF Verification in your default mail flow policy. Set Conformance Level to SIDF Compatible and write either a message filter or content filter that detects SPF failures stamped into the header. See Figure 12 below
2. Create a dictionary that accounts for executives. In this case one entry will be John Chambers. For every executive name, it needs to include their username and all possible surnames as terms. With the Exec_Name dictionary being complete, use a content filter or message filter to match on the From Header value for incoming messages. Your exec dictionary needs to be part of the Monitor filter to catch false postives from external mail expanders. Be sure to run for trial periods before quarantining matches.

Recommended Remediation: Create a Filter that inspects SPF failures, or matches on an Exec dictionary, and removes the **From** header in the body of the message. **From** header removal will cause the **Envelope From** value to automatically be written into the **From** field. This makes the actual senders address viewable in message inbox. Save the original From value in X-header to support your action (shown on next example).

Figure 12. Content Filter Remediate From Header Abuse with SPF



Conditions

Apply rule: Only if all conditions match

Order	Condition	Rule	Delete
1	SPF Verification	spf-status == "softfail,fail,temperror,permerror"	🗑
2	Other Header	header("From") == "@alpha.com"	🗑

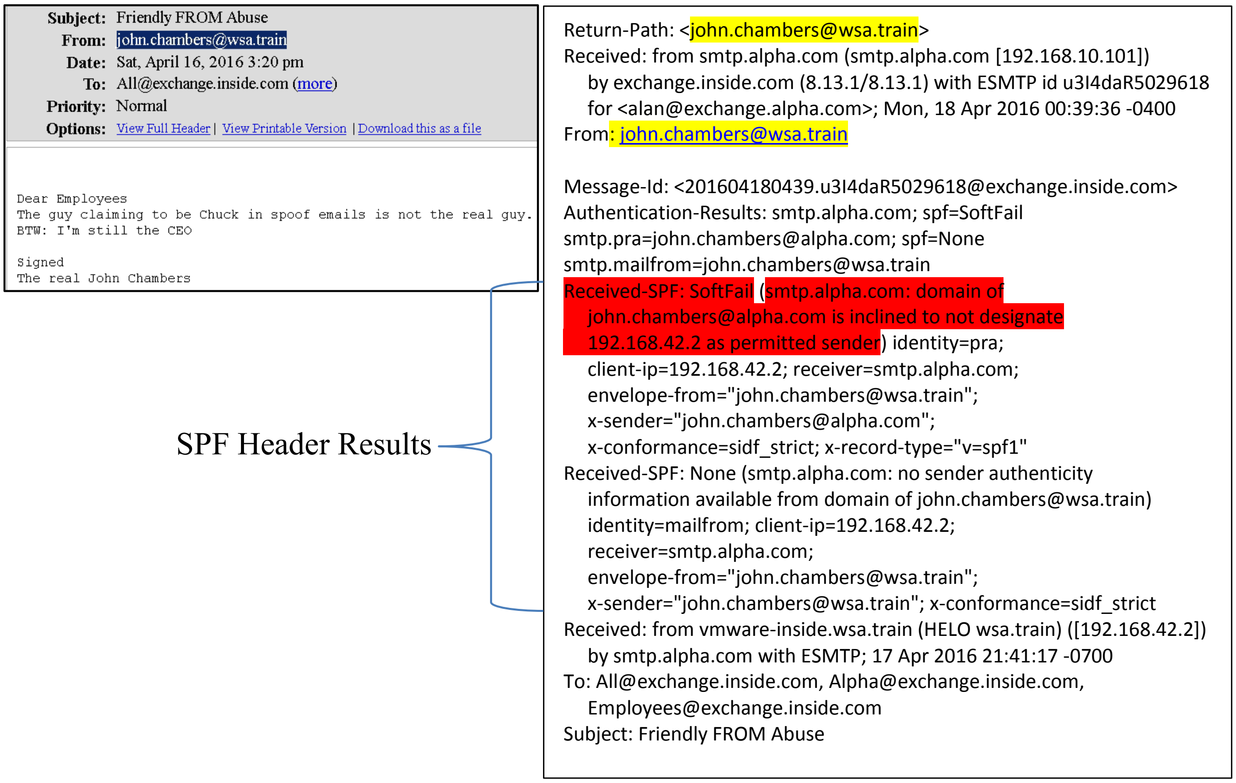
Actions

Order	Action	Rule	Delete
1	Strip Header	strip-header("From")	🗑
2	Strip Header	strip-header("Reply-To")	🗑

From Header Abuse Remediated

Here is the same message that we showed before, but this time it was processed by our filter. The first two conditions were satisfied and both the From and Reply-To fields were removed. This allows the recipient to see the real sender address. That will also be the address that the recipient replies to if they choose to.

Figure 13. Sample of From Header Abuse Remediated with SPF



Subject: Friendly FROM Abuse
From: john.chambers@wsa.train
Date: Sat, April 16, 2016 3:20 pm
To: All@exchange.inside.com (more)
Priority: Normal
Options: View Full Header | View Printable Version | Download this as a file

```
Dear Employees
The guy claiming to be Chuck in spoof emails is not the real guy.
BTW: I'm still the CEO

Signed
The real John Chambers
```

```
Return-Path: <john.chambers@wsa.train>
Received: from smtp.alpha.com (smtp.alpha.com [192.168.10.101])
    by exchange.inside.com (8.13.1/8.13.1) with ESMTP id u3I4daR5029618
    for <alan@exchange.alpha.com>; Mon, 18 Apr 2016 00:39:36 -0400
From: john.chambers@wsa.train

Message-Id: <201604180439.u3I4daR5029618@exchange.inside.com>
Authentication-Results: smtp.alpha.com; spf=SoftFail
smtp.pra=john.chambers@alpha.com; spf=None
smtp.mailfrom=john.chambers@wsa.train
Received-SPF: SoftFail (smtp.alpha.com: domain of
    john.chambers@alpha.com is inclined to not designate
    192.168.42.2 as permitted sender) identity=pra;
    client-ip=192.168.42.2; receiver=smtp.alpha.com;
    envelope-from="john.chambers@wsa.train";
    x-sender="john.chambers@alpha.com";
    x-conformance=sidf_strict; x-record-type="v=spf1"
Received-SPF: None (smtp.alpha.com: no sender authenticity
    information available from domain of john.chambers@wsa.train)
    identity=mailfrom; client-ip=192.168.42.2;
    receiver=smtp.alpha.com;
    envelope-from="john.chambers@wsa.train";
    x-sender="john.chambers@wsa.train"; x-conformance=sidf_strict
Received: from vmware-inside.wsa.train (HELO wsa.train) ([192.168.42.2])
    by smtp.alpha.com with ESMTP; 17 Apr 2016 21:41:17 -0700
To: All@exchange.inside.com, Alpha@exchange.inside.com,
    Employees@exchange.inside.com
Subject: Friendly FROM Abuse
```

Important: Preventing the abuse of a corporate domain name using Sender Verification and Dictionaries can be accomplished with SPF records with significantly less effort (outside of the effort to implement SPF in the first place)! If your records are published, and you specify allowed senders, you can:

- Detect Envelope From Abuse
- Detect From Header Abuse
- Allow legitimate senders

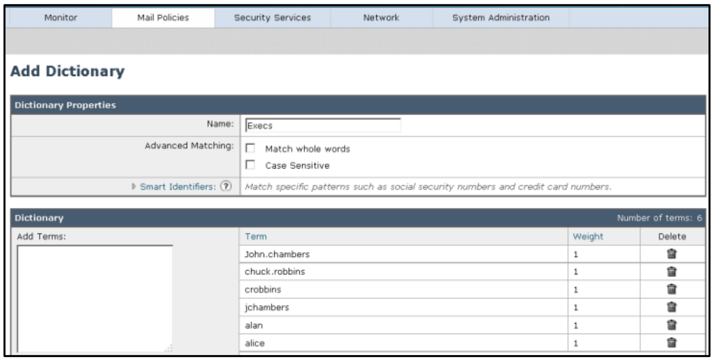
Instead of an SPF check, we could have used an Exec dictionary provided that one of its records is the name “john.chambers”. This is a good alternative if you don’t wish to publish DNS records. If you have a list of legitimate senders, which many enterprises do, then you need to keep the domains updated in your SPF records if using that method, or you need to address those updates in your SPOOF_ALLOW Sender Group if you are using Sender Verification discussed earlier.

TOC

From Header Abuse Remediation (Continued)

For customers that are not implementing SPF, you can define an Executive Name dictionary as follows:

Figure 14. Content Filter Remediate From Header Abuse with Executive and Domain Dictionaries



Add Dictionary

Dictionary Properties

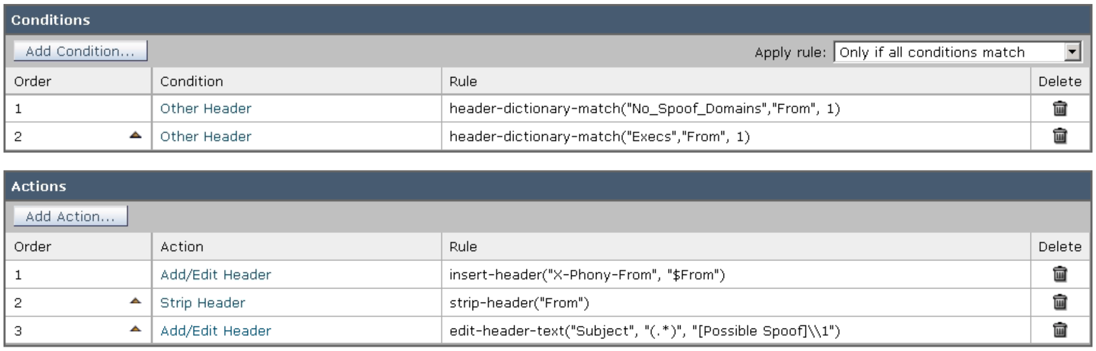
Name:	Execs
Advanced Matching:	□ Match whole words □ Case Sensitive
Smart Identifiers:	*Match specific patterns such as social security numbers and credit card numbers.*

Dictionary Number of terms: 6

Add Terms:

Term	Weight	Delete
John.chambers	1	🗑
chuck.robbins	1	🗑
crobbins	1	🗑
jchambers	1	🗑
alan	1	🗑
alice	1	🗑

In the filter below, SPF condition is replaced with a dictionary match on the **From** field to get the same results, which is our second method discussed earlier. Note: You can exhaustively list all of the variations of executive names and their sur names. Or you can create regular expressions inside of the dictionary. Suggestions on regex syntax is beyond this white paper.



Conditions

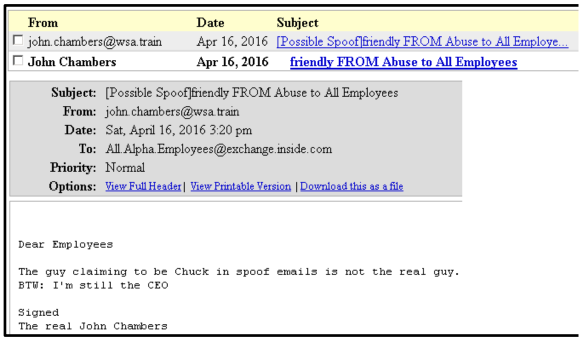
Apply rule: Only if all conditions match

Order	Condition	Rule	Delete
1	Other Header	header-dictionary-match("No_Spoof_Domains","From", 1)	🗑
2	Other Header	header-dictionary-match("Execs","From", 1)	🗑

Actions

Order	Action	Rule	Delete
1	Add/Edit Header	insert-header("X-Phony-From", "$From")	🗑
2	Strip Header	strip-header("From")	🗑
3	Add/Edit Header	edit-header-text("Subject", "(.*)", "[Possible Spoof]\\1")	🗑

Figure 15. Sample of From Header Abuse Remediated with SPF

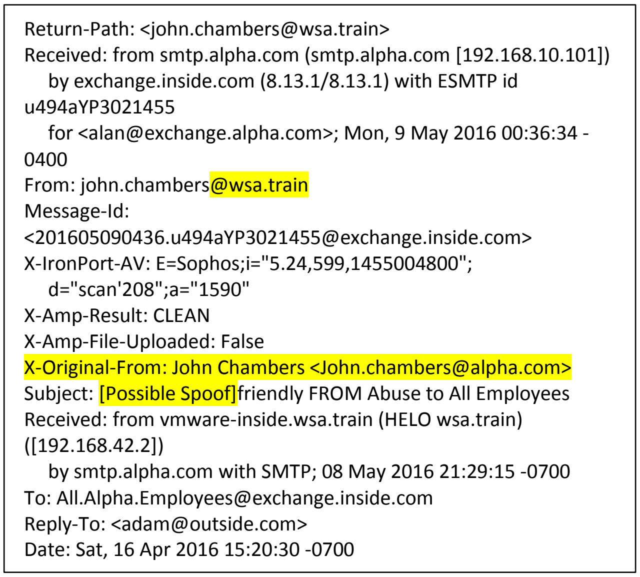


	From	Date	Subject
□	john.chambers@wsa.train	Apr 16, 2016	[Possible Spoof]friendly FROM Abuse to All Employe...
□	**John Chambers**	**Apr 16, 2016**	**friendly FROM Abuse to All Employees**

Subject: [Possible Spoof]friendly FROM Abuse to All Employees
From: john.chambers@wsa.train
Date: Sat, April 16, 2016 3:20 pm
To: All.Alpha.Employees@exchange.inside.com
Priority: Normal
Options: View Full Header | View Printable Version | Download this as a file

```
Dear Employees

The guy claiming to be Chuck in spoof emails is not the real guy.
BTW: I'm still the CEO

Signed
The real John Chambers
```

Figure 15 shows the sample "friendly From Abuse" run with and without applying the filter in Figure 14. The second message in Alan's inbox is the unfiltered message. It's From value is "John Chambers". In the first message, the From value is stripped out and replaced with the Envelope from value john.chambers@wsa.train, and the subject is prepended with [Possible Spoof]. The original From value is recorded in the header X-Original-From.



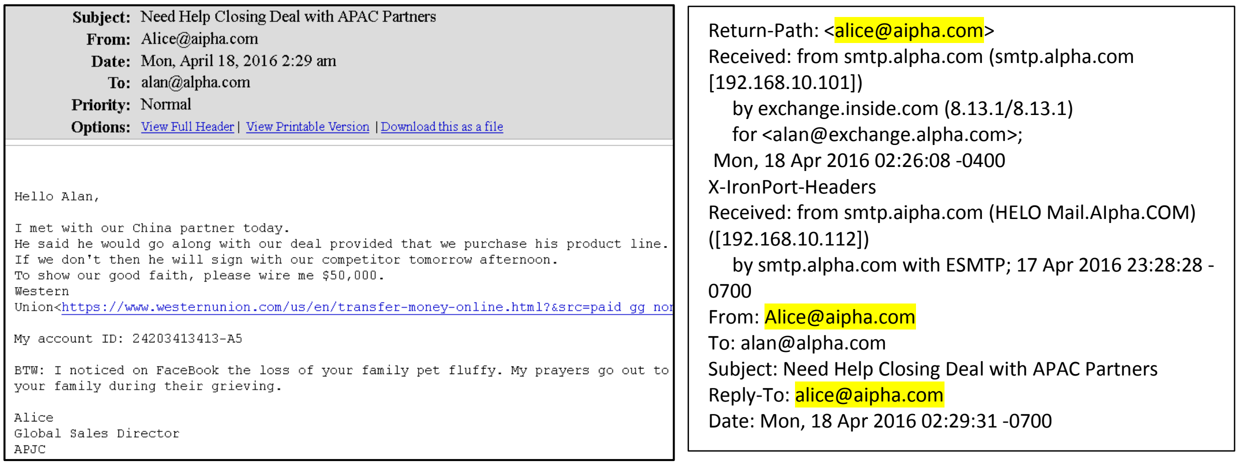
```
Return-Path: <john.chambers@wsa.train>
Received: from smtp.alpha.com (smtp.alpha.com [192.168.10.101])
    by exchange.inside.com (8.13.1/8.13.1) with ESMTP id
u494aYP3021455
    for <alan@exchange.alpha.com>; Mon, 9 May 2016 00:36:34 -
0400
From: john.chambers@wsa.train
Message-Id:
<201605090436.u494aYP3021455@exchange.inside.com>
X-IronPort-AV: E=Sophos;i="5.24,599,1455004800";
    d="scan'208";a="1590"
X-Amp-Result: CLEAN
X-Amp-File-Uploaded: False
X-Original-From: John Chambers <John.chambers@alpha.com>
Subject: [Possible Spoof]friendly FROM Abuse to All Employees
Received: from vmware-inside.wsa.train (HELO wsa.train)
([192.168.42.2])
    by smtp.alpha.com with SMTP; 08 May 2016 21:29:15 -0700
To: All.Alpha.Employees@exchange.inside.com
Reply-To: <adam@outside.com>
Date: Sat, 16 Apr 2016 15:20:30 -0700
```

TOC

Addressing Cousin Domain Abuse

Cousin domain names are visually similar to the victim's domain name; aipha.com looks like alpha.com. But since they are different, they can be uniquely verified with DKIM and SPF. They will not get blocked by Sender Verification. And since their envelope from and From header values agree they'll pass strict DMARC verification. The following message passed the "Enforcement filter" that we created for the From Header abuse, but would have been caught by the Monitor filter provide that a cousin's dictionary was applied:

Figure 16. Sample of Cousin Domain Abuse



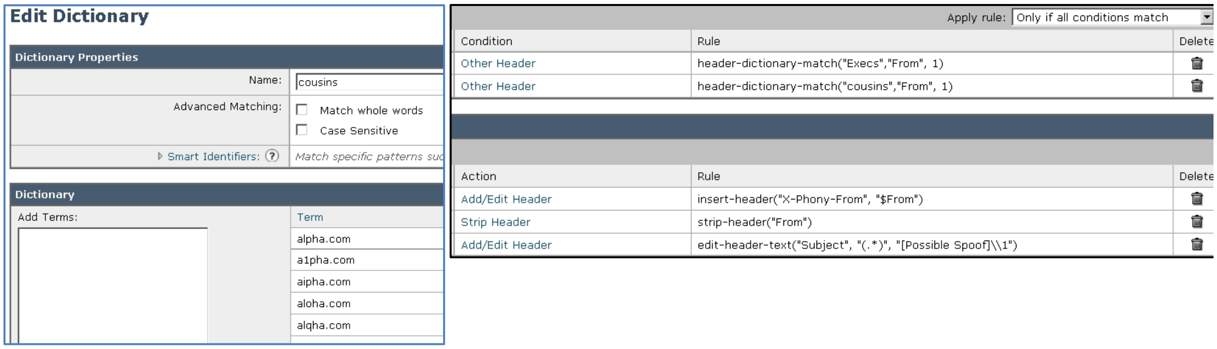
Subject: Need Help Closing Deal with APAC Partners
From: Alice@aipha.com
Date: Mon, April 18, 2016 2:29 am
To: alan@alpha.com
Priority: Normal
Options: View Full Header | View Printable Version | Download this as a file

```
Hello Alan,

I met with our China partner today.
He said he would go along with our deal provided that we purchase his product line.
If we don't then he will sign with our competitor tomorrow afternoon.
To show our good faith, please wire me $50,000.
Western
Union<https://www.westernunion.com/us/en/transfer-money-online.html?&src=paid gg nor

My account ID: 24203413413-A5

BTW: I noticed on FaceBook the loss of your family pet fluffy. My prayers go out to
your family during their grieving.

Alice
Global Sales Director
APJC
```

```
Return-Path: <alice@aipha.com>
Received: from smtp.alpha.com (smtp.alpha.com
[192.168.10.101])
    by exchange.inside.com (8.13.1/8.13.1)
    for <alan@exchange.alpha.com>;
 Mon, 18 Apr 2016 02:26:08 -0400
X-IronPort-Headers
Received: from smtp.aipha.com (HELO Mail.AIpha.COM)
([192.168.10.112])
    by smtp.alpha.com with ESMTP; 17 Apr 2016 23:28:28 -
0700
From: Alice@aipha.com
To: alan@alpha.com
Subject: Need Help Closing Deal with APAC Partners
Reply-To: alice@aipha.com
Date: Mon, 18 Apr 2016 02:29:31 -0700
```

Recommended Remediation: Create a Filter that matches on an Executive dictionary AND a dictionary of cousin domains. You can create a dictionary of cousin domains based on your own domain by going to: https://github.com/elceef/dnstwist and applying their python algorithm. The algorithm will create variants of a domain and then do a DNS lookup to verify that the cousin domain is registered.

Figure 17. Content Filter: Remediate Cousin Domain Abuse



Edit Dictionary

Dictionary Properties

Name: cousins

Advanced Matching: □ Match whole words □ Case Sensitive

Smart Identifiers: Match specific patterns suc

Dictionary

Add Terms:

Term
alpha.com
a1pha.com
aipha.com
aloha.com
alqha.com

Apply rule: Only if all conditions match

Condition	Rule	Delete
Other Header	header-dictionary-match("Execs","From", 1)	🗑
Other Header	header-dictionary-match("cousins","From", 1)	🗑

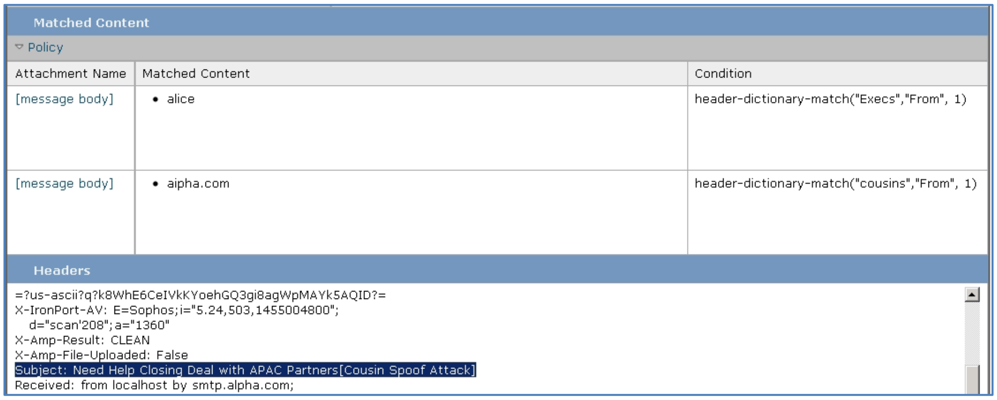
Action	Rule	Delete
Add/Edit Header	insert-header("X-Phony-From", "$From")	🗑
Strip Header	strip-header("From")	🗑
Add/Edit Header	edit-header-text("Subject", "(.*)", "[Possible Spoof]\\1")	🗑

Note: Some of these filter samples use the header X-Phony-From in place of the header X-Original-From. Their usage is identical.

Remediating Cousin Domain Abuse

The following is the matched content from both Execs and Cousins dictionaries. We chose to not apply the rule to remove the friendly From header since it will be replaced with the same field. Instead we modified the subject header and quarantined the message. The following quarantine menu shows the matching conditions.

Figure 18. Sample of Quarantined Cousin Domain Abuse



Attachment Name	Matched Content	Condition
[message body]	• alice	header-dictionary-match("Execs","From", 1)
[message body]	• aipha.com	header-dictionary-match("cousins","From", 1)

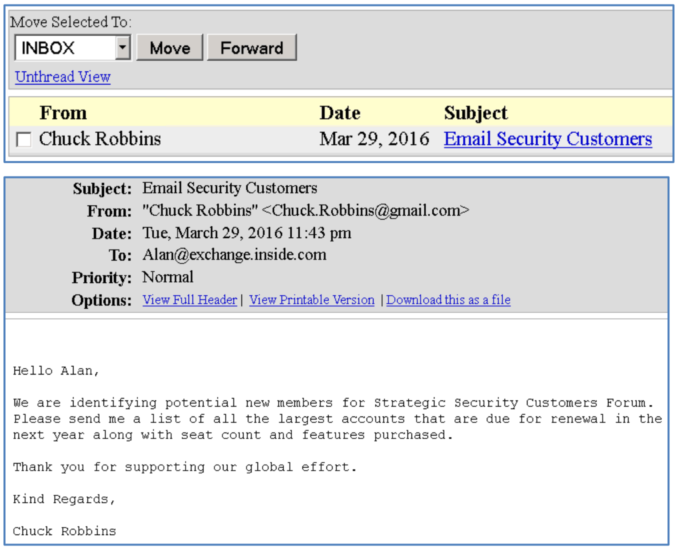
```
=?us-ascii?q?k8WhE6CeIVkKYoehGQ3gi8agWpMAYk5AQID?=
X-IronPort-AV: E=Sophos;i="5.24,503,1455004800";
   d="scan'208";a="1360"
X-Amp-Result: CLEAN
X-Amp-File-Uploaded: False
Subject: Need Help Closing Deal with APAC Partners[Cousin Spoof Attack]
Received: from localhost by smtp.alpha.com;
```

TOC

Free Email Account Abuse

Messages from gmail can be structured so that the senders email address is not shown in the inbox. When we open the message in any email client, you can see more sender information. But the sender’s address isn’t visually available on a mobile device, even when the message is open. Similarly on a mobile device, clicking reply will not populate the “to” field with chuck.robbins@gmail.com . Instead it will be Chuck Robbins or Chuck. In that case, the recipient won’t know that this is an external email. This will also pass all of the sender authentication checks as highlighted here.

Figure 19. Sample of Free Email Abuse



From	Date	Subject
□ Chuck Robbins	Mar 29, 2016	Email Security Customers

Subject: Email Security Customers
From: "Chuck Robbins" <Chuck.Robbins@gmail.com>
Date: Tue, March 29, 2016 11:43 pm
To: Alan@exchange.inside.com
Priority: Normal
Options: View Full Header | View Printable Version | Download this as a file

```
Hello Alan,

We are identifying potential new members for Strategic Security Customers Forum.
Please send me a list of all the largest accounts that are due for renewal in the
next year along with seat count and features purchased.

Thank you for supporting our global effort.

Kind Regards,

Chuck Robbins
```

```
Return-Path: <Chuck.Robbins@gmail.com>
Received-SPF: Pass (smtp.alpha.com: domain of
Chuck.Robbins@gmail.com designates 192.168.10.116 as
permitted sender) identity=mailfrom;
    client-ip=192.168.10.116; receiver=smtp.alpha.com;
    envelope-from="Chuck.Robbins@gmail.com";
    x-sender="Chuck.Robbins@gmail.com"; x-
conformance=spf_only;
    x-record-type="v=spf1"
Authentication-Results: smtp.alpha.com; spf=Pass
smtp.mailfrom=Chuck.Robbins@gmail.com; spf=None
smtp.helo=postmaster@smtp.gmail.com; dkim=pass (signature
verified) header.i=dkim@gmail.com
X-IronPort-Headers
Received: from smtp.gmail.com ([192.168.10.116])
    by smtp.alpha.com with ESMTP; 18 Apr 2016 12:18:44 -0700
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
    DKIM Headers not shown
From: Chuck Robbins <Chuck.Robbins@gmail.com>
To: Alan@exchange.inside.com
Subject: Email Security Customers
```

Recommended Remediation: Create a Filter that matches on the **From** field a dictionary of Exec names, or a list of any internal group names that entice immediate reaction. If the recipients are many employees then, set a condition for multiple recipients. Possible actions are: Save the original **From** value in X-header to support your action, strip the **From** header, notify the admin , append the subject header and either copy-quarantine or quarantine the original message.

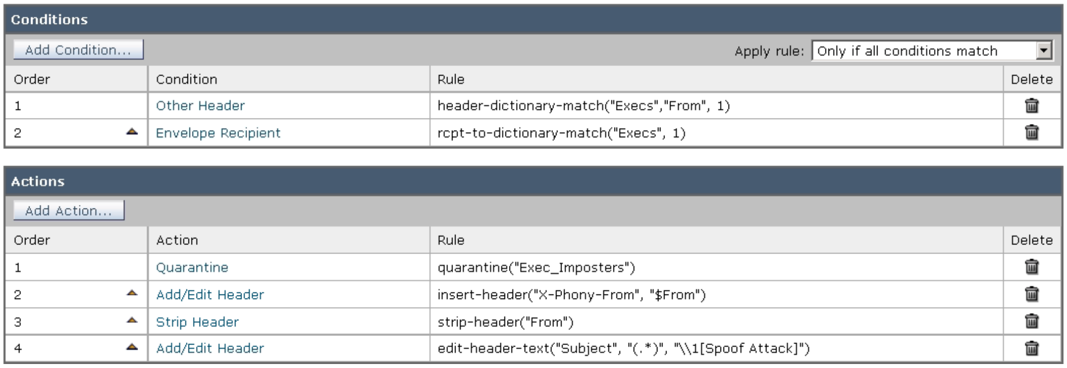
For this case, matching on domain names in the **From** field is ineffective. Free mail spoofs could have the following structures:

- From: named executive <name@gmail.com> To: one executive
- From: named executive <name@gmail.com> To: multiple employees
- From: internal group list <name@gmail.com> To: multiple employees

All of these are rare for incoming business mail. Many admins will warn executives not to send unicast inbound from their free email account. In the following content filter, we match on the first condition above, copy the From information to a new header X-Original-From, strip the friendly From header and quarantine the message. Alternatively, we could send a duplicate message to quarantine and send the modified message to the executive.

Remediation of Free Email Account Abuse

Figure 20. Content Filter Remediation of Free Email Account Abuse



Conditions

Add Condition... Apply rule: Only if all conditions match

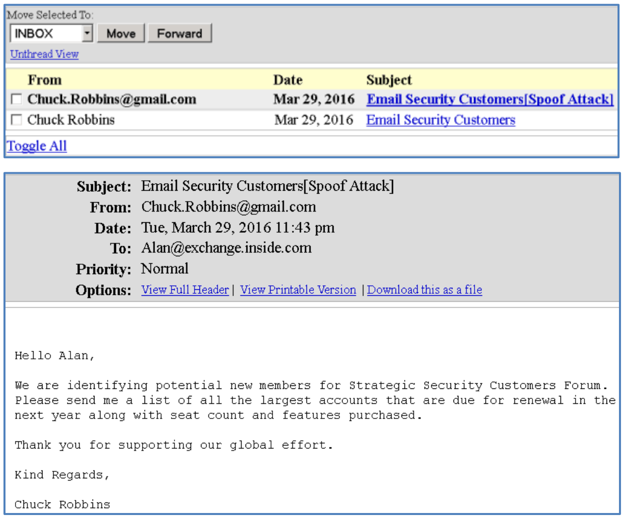
Order	Condition	Rule	Delete
1	Other Header	header-dictionary-match("Execs","From", 1)	🗑
2 ▲	Envelope Recipient	rcpt-to-dictionary-match("Execs", 1)	🗑

Actions

Add Action...

Order	Action	Rule	Delete
1	Quarantine	quarantine("Exec_Imposters")	🗑
2 ▲	Add/Edit Header	insert-header("X-Phony-From", "$From")	🗑
3 ▲	Strip Header	strip-header("From")	🗑
4 ▲	Add/Edit Header	edit-header-text("Subject", "(.*)", "\\1[Spoof Attack]")	🗑

Figure 21. Sample of Remediated Free Email Account Abuse



From	Date	Subject
□ Chuck.Robbins@gmail.com	Mar 29, 2016	Email Security Customers[Spoof Attack]
□ Chuck Robbins	Mar 29, 2016	Email Security Customers

Subject: Email Security Customers[Spoof Attack]
From: Chuck.Robbins@gmail.com
Date: Tue, March 29, 2016 11:43 pm
To: Alan@exchange.inside.com
Priority: Normal
Options: View Full Header | View Printable Version | Download this as a file

```
Hello Alan,

We are identifying potential new members for Strategic Security Customers Forum.
Please send me a list of all the largest accounts that are due for renewal in the
next year along with seat count and features purchased.

Thank you for supporting our global effort.

Kind Regards,

Chuck Robbins
```

Return-Path: <Chuck.Robbins@gmail.com>
Received: from smtp.alpha.com (smtp.alpha.com [192.168.10.101])
    by exchange.inside.com (8.13.1/8.13.1) with ESMTP id u3ILKgcN032691
    for <alan@exchange.alpha.com>; Mon, 18 Apr 2016 17:20:42 -0400
From: Chuck.Robbins@gmail.com
Received-SPF: Pass (smtp.alpha.com: domain of Chuck.Robbins@gmail.com designates 192.168.10.116 as permitted sender) identity=mailfrom;
Authentication-Results: smtp.alpha.com; spf=Pass smtp.mailfrom=Chuck.Robbins@gmail.com; spf=None smtp.helo=postmaster@smtp.gmail.com; dkim=pass (signature verified)
X-Original-From: Chuck Robbins <Chuck.Robbins@gmail.com>
Subject: Email Security Customers[Spoof Attack]
To: Alan@exchange.inside.com

Similar to the other filters, in Figure 20, the **X-Original-From** header receives the value of the original **From** before the value of **From** is stripped out. This is useful when the recipient requests a reason for why the message was acted upon. You could also use X-Original-From to address false positives. You can also create a filter that matches the From value being an executive destined to multiple recipients. But for counting multiple recipients you need to use a message filter. The rcpt-count depends on the organization.

Figure 22

```
Free_Mail_Spoof:
if sendergroup != "RELAYLIST" {
if sendergroup != "SPOOF_ALLOW" {
if (rcpt-count > 1)
 AND
header-dictionary-match ("Execs", "From", 1)
     {
            insert-header("X-Original-From", "$From");
            strip-header("From");
            edit-header-text("Subject", "(.*)", "[Possible Spoof] \\1");
            insert-header("X-IronPort-Quarantine", "");
     }
                                            }
                                 }
```

Comprehensive Configuration to Address all Listed Spoofing Types

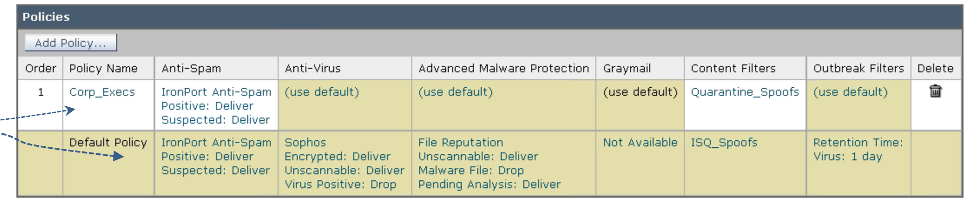
The following filters represent all of the concepts presented in this paper. We've tested the scripts that were presented earlier against this configuration and obtained the same results as the individual filters. Like the earlier material, this is only presented as a suggestion for you environment. We have set the conditions for a positive spoof of envelope from abuse, From Header abuse, cousin domain abuse or free mail abuse in the message filter block and then remediate the matches with content filters. There are different mail policies depending on the recipient being an executive or non-executive as shown below. Spoofs to Execs have their headers modified and "quarantine copied" to a policy quarantine. Any spoofs to non-execs have their headers modified and sent the spam quarantine. As you become more confident of your filter efficacy, change the "quarantine copied" to "quarantine".

Message Filters

Positive_Spoof:
If sendergroup!=..

Free_Mail_Spoof:
If sendergroup!=..

Incoming Mail Policies



Policies

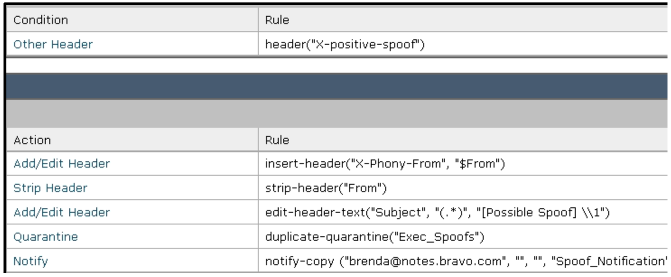
Add Policy...

Order	Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters	Delete
1	Corp_Execs	IronPort Anti-Spam Positive: Deliver Suspected: Deliver	(use default)	(use default)	(use default)	Quarantine_Spoofs	(use default)	🗑
	Default Policy	IronPort Anti-Spam Positive: Deliver Suspected: Deliver	Sophos Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	File Reputation Unscannable: Deliver Malware File: Drop Pending Analysis: Deliver	Not Available	ISQ_Spoofs	Retention Time: Virus: 1 day	

```
Positive_Spoof:
if sendergroup != "RELAYLIST" {
if sendergroup != "SPOOF_ALLOW" {
if  mail-from-dictionary-match("No_Spoof_Domains", 1)
   OR
   (
   header-dictionary-match("No_Spoof_Domains","From", 1)
   AND
   header-dictionary-match ("Execs", "From", 1)
    )
    OR
    header-dictionary-match ("cousins", "From", 1)
       {
             insert-header("X-positive-spoof", "true");
             skip_filters();
       }
                                                  }
                                      }
                         .
```

```
Free_Mail_Spoof:
if sendergroup != "RELAYLIST" {
if sendergroup != "SPOOF_ALLOW" {
if (rcpt-count > 1)
 AND
header-dictionary-match ("Execs", "From", 1)
      {
             insert-header("X-Original-From", "$From");
             strip-header("From");
             edit-header-text("Subject", "(.*)", "[Possible Spoof]
\\1");
             insert-header("X-IronPort-Quarantine", "");
      }
                                                  }
                                      }
                         .
```

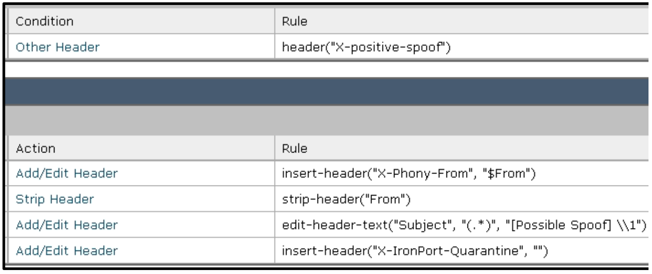
Quarantine_Spoofs



Condition	Rule
Other Header	header("X-positive-spoof")

Action	Rule
Add/Edit Header	insert-header("X-Phony-From", "$From")
Strip Header	strip-header("From")
Add/Edit Header	edit-header-text("Subject", "(.*)", "[Possible Spoof] \\1")
Quarantine	duplicate-quarantine("Exec_Spoofs")
Notify	notify-copy ("brenda@notes.bravo.com", "", "", "Spoof_Notification'

ISQ_Spoofs



Condition	Rule
Other Header	header("X-positive-spoof")

Action	Rule
Add/Edit Header	insert-header("X-Phony-From", "$From")
Strip Header	strip-header("From")
Add/Edit Header	edit-header-text("Subject", "(.*)", "[Possible Spoof] \\1")
Add/Edit Header	insert-header("X-IronPort-Quarantine", "")

TOC

Comprehensive Configuration for all Listed Spoofing Types (Continued)

In the structure for the message filter Positive_Spoof, the operations performed by:

“if sendergroup != "SPOOF_ALLOW" { “ and

“ header-dictionary-match("No_Spoof_Domains","From", 1) “

can be replicated by publishing SPF, DKIM and DMARC records that indicate who can send on your behalf. The DMARC check and remediation can be done in the HAT or you can remediate spoofs in a message filter with an SIDF condition. The added value in this approach is that the DNS text records will limit both mail from and From abuse of the corporate domains. Message filters can then address what is left: Executive names, internal group lists and cousin domains.

Note: Publishing DMARC, DKIM and SPF records, and enabling verification of the these in Cisco Email Security’s solution, is beyond the scope of this WP. For that please reference the following:

- https://dmarc.org/
- http://www.openspf.org/
- http://www.dkim.org/
- Chapter 21 Email Authentication of http://www.cisco.com/c/dam/en/us/td/docs/security/esa/esa9-7/ESA_9-7_User_Guide.pdf

Not shown ahead of the message filters: Positive_Spoof and Free_Mail_Spoof are the message filters: Quarantine_Spoof_copy and Tag_Incoming_Mail. We should remove Tag_Incoming_Mail because that is done by the Enforcement filters. But we should keep the Quarantine_Spoof_copy. If it catches a spoof that Positive_Spoof and Free_Mail_Spoof did not, then we need to adjust accordingly.

Next Steps

We understand the challenge of remediating email attacks, such as the spoofing attacks discussed here. If you are having challenges with implementing these techniques, please contact Cisco Support and open a case. Or reach out to your Cisco account team.

Regards,

Kevin Floyd

Technical Marketing Engineer – Email Security

Security Business Group

Cisco Systems, Inc.

TOC

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA

CXX-XXXXXX-XX 10/11

TOC