Cisco Live!
July 10-14, 2016 • Las Vegas, NV
Your Time Is Now
Cisco Email Security
Deep Dive & Best Practices

Usman Din, Product Manager Email Security
BRKSEC-2131
Agenda

• Introduction
• Terminology and understanding the Email Pipeline
• Configuration and Best Practices for Anti-Spam Tuning
• Configuration and Best Practices for Spoofing and Phishing detection
• Attachment Control and Defense
• Summary
Introduction – About Me

Trust Me – I’ve been around forever!

• Joined Cisco through IronPort acquisition in 2007.
• On-site SE for Research in Motion, then CSE for Content Security
• Global Lead for the Email Security Advisory Group
• Cisco Live Speaker in US, LATAM and EU
• Distinguished Speaker, Cisco Live Berlin (2016)
• Now part of the Product Management team for Email Security
• Based out of Toronto, Canada
The Email Pipeline
The Email Pipeline

SMTP SERVER
- Host Access Table (HAT)
- Received Header
- Default Domain
- Domain Map
- Recipient Access Table (RAT)
- Alias Table
- LDAP RCPT Accept
- SMTP Call-Ahead
- DKIM / SPF Verification
- DMARC Verification
- S/MIME Verification

WORKQUEUE
- LDAP RCPT Accept (WQ)
- Masquerading (Table / LDAP)
- LDAP Routing
- Message Filters
- Anti-Spam
- Anti-Virus
- Advanced Malware (AMP)
- Graymail, Safe Unsubscribe
- Content Filtering
- Outbreak Filtering
- DLP Filtering (Outbound)

SMTP CLIENT
- Encryption
- Virtual Gateways
- Delivery Limits
- Received: Header
- Domain-Based Limits
- Domain-Based Routing
- Global Unsubscribe
- S/MIME Encryption
- DKIM Signing
- Bounce Profiles
- Message Delivery
Anti-Spam Tuning: HAT, Mail Flow Policies and Workqueue settings
A note about Best Practices…

• Throughout the material we will present options for tuning your environment
• These are meant to be general guidelines, and as each environment is unique, it is recommended that settings be set in monitor mode first
• After a determined time, perform analysis and tuning of rules and settings to achieve the desired result
Host Access Table (HAT) Structure

- HATs are associated per listener, defined as being Public or Private. Once a listener is defined they cannot be changed.
- Private listeners have no Recipient Access Table - best used for outbound facing mail traffic. No restrictions for domains.
- The structure of the HAT is defined by the listener type, once created a default configuration is loaded.
- Mail Flow Policies (MFP) are also created based on the listener type, thus a MFP such as Relayed would not be created until a Private Listener is defined, or created manually.
SenderGroup Structure

- SenderBase score can be attached to the SenderGroups, ensure that the neutral and no score ranges are addressed

<table>
<thead>
<tr>
<th>Order</th>
<th>Sender Group</th>
<th>SenderBase™ Reputation Score</th>
<th>Mail Flow Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>RELAYLIST</td>
<td>-10 -8 -6 -4 -2 0 2 4 0 8 10</td>
<td>RELAYED</td>
</tr>
<tr>
<td>2</td>
<td>WHITELIST</td>
<td></td>
<td>TRUSTED</td>
</tr>
<tr>
<td>3</td>
<td>BLACKLIST</td>
<td></td>
<td>BLOCKED</td>
</tr>
<tr>
<td>4</td>
<td>SUSPECTLIST</td>
<td></td>
<td>THROTTLED</td>
</tr>
<tr>
<td>5</td>
<td>UNKNOWNLIST</td>
<td></td>
<td>ACCEPTED</td>
</tr>
<tr>
<td>ALL</td>
<td></td>
<td></td>
<td>ACCEPTED</td>
</tr>
</tbody>
</table>

- Diagram showing "SUSPECTLIST" with a comment: "Suspicious senders are throttled" and a policy: "THROTTLED".
Host Access Table Structure

- IPs and Hosts are evaluated in the HAT Top Down, First Match
- SenderGroups are containers that define the policy based on match
- Inclusion into a SenderGroup is defined by Reputation Score, DNS, or explicit match

<table>
<thead>
<tr>
<th>Order</th>
<th>Sender Group</th>
<th>SenderBase™ Reputation Score</th>
<th>Mail Flow Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>RELAYLIST</td>
<td>-10 -8 -6 -4 -2 0 2 4 6 8 +10</td>
<td>RELAYED</td>
</tr>
<tr>
<td>2</td>
<td>WHITELIST</td>
<td></td>
<td>TRUSTED</td>
</tr>
<tr>
<td>3</td>
<td>BLACKLIST</td>
<td></td>
<td>BLOCKED</td>
</tr>
<tr>
<td>4</td>
<td>SUSPECTLIST</td>
<td></td>
<td>HEAVY_THROTTLE</td>
</tr>
<tr>
<td>5</td>
<td>GREYLIST</td>
<td></td>
<td>LIGHT_THROTTLE</td>
</tr>
<tr>
<td>6</td>
<td>UNKNOWNLIST</td>
<td></td>
<td>ACCEPTED</td>
</tr>
<tr>
<td></td>
<td>ALL</td>
<td></td>
<td>ACCEPTED</td>
</tr>
</tbody>
</table>
SenderGroup Options

- Within the settings you define the Name, Mail Flow Policy
- Nomenclature is important as it will be displayed in logs and reports
- SBRS scores can be assigned to the group
- RBLs can be leveraged if required.
- Note that SBRS uses multiple sources including honeypots and DNSBLs
SenderGroup Options

- Connecting host PTR record does not exist in DNS.
- Connecting host PTR record lookup fails due to temporary DNS failure.
- Connecting host reverse DNS lookup (PTR) does not match the forward DNS lookup (A).

<table>
<thead>
<tr>
<th>DNS Lists (Optional): ?</th>
</tr>
</thead>
<tbody>
<tr>
<td>(e.g. 'query.blacklist.example, query.blacklist2.example')</td>
</tr>
</tbody>
</table>

Connecting Host DNS Verification:

- Connecting host PTR record does not exist in DNS.
- Connecting host PTR record lookup fails due to temporary DNS failure.
- Connecting host reverse DNS lookup (PTR) does not match the forward DNS lookup (A).
Understanding Email Reputation

- Breadth and quality of data makes the difference
- Real-time insight into this data that allows us to see threats before anyone else in the industry to protect our customers

Spam Traps

Complaint Reports

IP Blacklists and Whitelists

Geo-Location data

Message Composition Data

Compromised Host Lists

Website Composition Data

Host Data

Global Volume Data

Domain Blacklist and Safelists

Other Data

DNS Data

- IP Reputation Score

-10

0

+10
Customizing Reputation on the ESA

Default Settings: Moderate Blocking

<table>
<thead>
<tr>
<th>Order</th>
<th>Sender Group</th>
<th>SenderBase™ Reputation Score</th>
<th>Mail Flow Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>RELAYLIST</td>
<td>.10</td>
<td>RELAYED</td>
</tr>
<tr>
<td>2</td>
<td>WHITELIST</td>
<td>-8</td>
<td>TRUSTED</td>
</tr>
<tr>
<td>3</td>
<td>BLACKLIST</td>
<td>-4</td>
<td>BLOCKED</td>
</tr>
<tr>
<td>4</td>
<td>SUSPECTLIST</td>
<td>0</td>
<td>THROTTLED</td>
</tr>
<tr>
<td>5</td>
<td>UNKNOWNLIST</td>
<td>-10</td>
<td>ACCEPTED</td>
</tr>
</tbody>
</table>

Custom Settings: Aggressive Throttling

<table>
<thead>
<tr>
<th>Order</th>
<th>Sender Group</th>
<th>SenderBase™ Reputation Score</th>
<th>Mail Flow Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>RELAYLIST</td>
<td>.10</td>
<td>RELAYED</td>
</tr>
<tr>
<td>2</td>
<td>WHITELIST</td>
<td>-8</td>
<td>TRUSTED</td>
</tr>
<tr>
<td>3</td>
<td>BLACKLIST</td>
<td>-4</td>
<td>BLOCKED</td>
</tr>
<tr>
<td>4</td>
<td>SUSPECTLIST</td>
<td>0</td>
<td>HEAVY_THROTTLE</td>
</tr>
<tr>
<td>5</td>
<td>GRYLST</td>
<td>-4</td>
<td>LIGHT_THROTTLE</td>
</tr>
<tr>
<td>6</td>
<td>UNKNOWNLIST</td>
<td>-10</td>
<td>ACCEPTED</td>
</tr>
</tbody>
</table>

Incoming Mail Summary

<table>
<thead>
<tr>
<th>Message Category</th>
<th>%</th>
<th>Messages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stopped by Reputation Filtering</td>
<td>98.6%</td>
<td>756</td>
</tr>
<tr>
<td>Stopped as Invalid Recipients</td>
<td>1.4%</td>
<td>11</td>
</tr>
</tbody>
</table>

- Reputation Score determined when connection initiated
- Sender Groups and actions are defined by the administrator
- Reputation can block 80-90% connections on the ESA
Reputation: DNS and caching

- DNS is the most critical external service for the ESA
- By default there are 4 DNS lookups per request: Reverse DNS, 2 SBRS lookups and a Number of requests per connection – default
- With SPF, DKIM and DMARC – 3 or more DNS TXT record lookups
- At least 7 possible DNS lookups per connection (excluding any caching)
- Now factor in outbound destination DNS resolution, LDAP, internal hosts, etc.
- More resolvers in high connection environments
Reputation: Delayed HAT Rejection

- Delayed HAT Rejection allows for additional logs for Reputation based blocks
- 2 additional log lines are added to each connection with details of from and to addresses

esa.teamnorthwind.com> listenerconfig

Currently configured listeners:

1. SMTP-AGGRESSIVE (on Management, 10.10.10.20) SMTP TCP Port 25 Public

[]> setup

By default connections with a HAT REJECT policy will be closed with a banner message at the start of the SMTP conversation. Would you like to do the rejection at the message recipient level instead for more detailed logging of rejected mail? [Y]>

Understanding Connections

- Global limits: Total IPv4 and IPv6 entire appliance, maximum should not exceed 400 concurrent connections (default is 300)
- Per listener limits: Each listener on the appliance should be configured to match your maximum global limit
- Mail Flow Policy limits: Per policy limits are used to rate limit senders, use concurrent connections in conjunction with host and sender rate limits
Understanding Connections

- Limit guidance per model – Model type makes no difference in the number of connections per appliance. Connection limits are based on OS, throughputs between appliances do vary
- In environments that require high number of concurrent connections, recommendation is to increase the number of appliances

Enter the global limit for concurrent connections to be allowed across all listeners.

[300]>

Listener SMTP-POV Policy $RELAYED max concurrency value of 600 will be limited to 300 by this concurrency setting.
MailFlow policies: Host vs Sender Throttling

- By default the only MFP that has any Host limiting is the throttle policy.
- By default, there are no Envelope Sender Limits set on the ESA.
- It is recommended to use Sender Limits in suspect ranges.

### Mail Flow Limits

<table>
<thead>
<tr>
<th>Rate Limit for Hosts:</th>
<th>Max. Recipients Per Hour:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Use Default (Unlimited)</td>
</tr>
<tr>
<td></td>
<td>Unlimited</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Max. Recipients Per Hour Code:</th>
<th>Use Default (E52)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Max. Recipients Per Hour Text:</th>
<th>Use Default (Too many recipients received this hour)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Rate Limit for Envelope Senders:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max. Recipients Per Time Interval:</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

| Sender Rate Limit Error Code: | Use Default (E52) |
|                              | E52                 |

<table>
<thead>
<tr>
<th>Sender Rate Limit Error Text:</th>
<th>Use Default (Too many recipients received from the sender)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Too many recipients received from the sender</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Exceptions:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Default (Ignore Rate Limit for Address List: None)</td>
</tr>
<tr>
<td>Ignore Rate Limit for Address List: None</td>
</tr>
</tbody>
</table>
MailFlow policies: Security Settings

- DHAP is set high on the ESA, recommend to tune it to be lower on suspect ranges
- LDAP enhances DHAP by performing rejection in conservation
MailFlow policies: Security Settings

- TLS Settings are not by default for incoming or outgoing mail
- Three levels of checking, preferred can be set on the default mail flow policy
- Mandatory can be setup as a list or as it’s own SenderGroup

Encryption and Authentication:

<table>
<thead>
<tr>
<th>TLS:</th>
<th>Use Default (Preferred)</th>
<th>Off</th>
<th>Preferred</th>
<th>Required</th>
</tr>
</thead>
</table>

- TLS is Mandatory for Address List: None

A security certificate/key has not been configured and assigned to a listener. (See Network > Certificates.) Enabling TLS will automatically use the “Demo” certificate/key for listeners.

- Verify Client Certificate

SMTP Authentication:

<table>
<thead>
<tr>
<th>Use Default (Off)</th>
<th>Off</th>
<th>Preferred</th>
<th>Required</th>
</tr>
</thead>
</table>

- Require TLS To Offer SMTP Authentication

If Both TLS and SMTP Authentication are enabled:
Host Access Table Tuning

- Before tuning, it is recommended to use the default (moderate) settings to understand the mail flow for your environment.
- Objective of tuning is to block or throttle more messages at the connection level, saving resources for processing legitimate mail.
- The first step is to create content filters to flag messages that are being passed through the default reputation filters with the SBRS and any scanning verdict info.
- Evaluate reporting of Content Filters and adjust HAT settings are required.
Per Policy Scanning

- Per domain policies take place after message filtering and LDAP rewrites
- Triggering Inbound and Outbound policies via Mail Flow policies
- A message is determined to be outbound because of relay mail flow policies (think of the HAT)
- SMTP authentication also triggers outbound regardless of accept policy set.
Policy Engine And Splintering

- If a single message matches multiple policies, it will be splintered
- Splintering *only* occurs if multiple policies are matched
Per Policy Scanning

- Use policies to leverage message splintering to apply rule and scanning as required
- Top down / first match wins, order is very important

<table>
<thead>
<tr>
<th>Order</th>
<th>Policy Name</th>
<th>Anti-Spam</th>
<th>Anti-Virus</th>
<th>Advanced Malware Protection</th>
<th>Graymail</th>
<th>Content Filters</th>
<th>Outbreak Filters</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>IMP.CISCOSECURITYGURU</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>IMP.INTERNETSSINKHOLE</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disclaimer-not-filter</td>
<td>Bypass-relay-internetsinkhole</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>IMP.CSEDEMO</td>
<td>IronPort Anti-Spam Positive; Quarantine Suspected: Quarantine</td>
<td>(use default)</td>
<td>(use default)</td>
<td>(use default)</td>
<td>Enabled (no filters)</td>
<td>(use default)</td>
<td></td>
</tr>
</tbody>
</table>
• Complex conditions inside a policy using AND/OR/NOT

• Multiple conditions can be used inside the same policy

• Move your logic from the filter into the policy and reduce resource consumption
Understanding CASE

- CASE stands for Context Adaptive Scanning Engine
- CASE is the combination of the Anti-Spam, Graymail and Outbreak engines
- Each engine can provide a verdict and depending on the action of the engine will either pass or drop the message
- A non-final action (i.e. Quarantine) will allow a message to continue to process down the workqueue. A final action such as drop will cause an “early exit” condition
- Other scanning blades may take precedence if another engine determines a positive condition
Upgrade, Enable, and Tune!

Enable Antispam – and if possible (based on hardware) increase scanning thresholds to 1M for always scan, 2M for never to scan more.

Enable Graymail – it’s a free engine which helps with Anti-Spam efficacy. Introduced in 9.5 so upgrade!

Enable Outbreak Filters – and if possible (based on hardware) increase scan size to 1M.
Adjusting Thresholds

- You can adjust the thresholds for Suspect / Positive spam to increase or decrease sensitivity
- Don’t do it, unless you really have to
- As we tune spam rules, we use the default thresholds as a baseline, so this may result in undesired results
Enable Graymail Scanning

- Graymail has 2 components: Detection and Unsubscribe
- Detection is free. It comes as part of the base email subscription license
- The graymail engine will provide verdicts to IPAS (final decision), which leads to a better overall email efficacy
Enabling Outbreak Filters

- By default, only Virus Outbreak is enabled.
- Enabling Threat Outbreak (Message Modification) you get additional intelligence being fed into CASE.
- In order to use URL functionality (covered later) Outbreak Filters must be turned on and configured.
Anti-Spam Tuning Checklist

• Assess your Host Access Table – still using the defaults? Time to adjust the scores

• Create more SenderGroups and get gradually more aggressive in your settings

• Check you WhiteLists - entries could be years old, ip changed, etc. Use the comments to keep track and prune regularly

• Check you Mail Flow Policies and turn on Sender limits, Sender Verification, etc.

• Use the new granular policies to create better Incoming Mail Policies

• Move the logic from the filter to the policy to create more efficient settings

• Turn on Graymail, Threat Outbreak Filtering to get more insight and better efficacy

• Upgrade, Upgrade, Upgrade!
Anti-Phishing: Content Filters and Outbreak Filtering
Understanding where URLs are evaluated

- As of version 8.5.6 the ESA can evaluate URLs inside a message – both for Reputation and Categorization

- URL filtering is not enabled by default, you must enable the service and have a valid Outbreak Filter license to perform URL inspection

- Once enabled, URLs are evaluated in three scanning blades:
  1. During IPAS Scan, a URL is used to factor into SPAM scores
  2. Inside a Content Filter for Reputation Score and Category
  3. As part of the Threat Outbreak Filter URL Rewrite function

- 9.7 introduced Web Interaction Tracking for Clicked URLs, which must be enabled after upgrade
URL Evaluation and options

- Enable URL Filtering globally under security settings:

- The Web Reputation Score (WBRS) uses the same -10 to +10 score, however it means something very different than SBRS

- Based on your organization’s security posture you can determine how aggressive you wish to be with URL entering your organization.
URL Evaluation and options

- URL Reputation is assessed inside of the CASE engine and used as part of the decision for Anti-Spam
- If not stopped as Spam the URL can be evaluated inside a content filter for both Category and Reputation

<table>
<thead>
<tr>
<th>Conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Add Condition...</strong></td>
</tr>
<tr>
<td>Order</td>
</tr>
<tr>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Add Action...</strong></td>
</tr>
<tr>
<td>Order</td>
</tr>
<tr>
<td>Final</td>
</tr>
</tbody>
</table>
URL Evaluation and options

Recommendations:

• Block URL: -10 to -6
• URL Remove: -5.9 to -5.8
• Leave the rest for Outbreak Filters
• Use in condition when you want to take an action on the whole message
• Use in action to act on URL only

<table>
<thead>
<tr>
<th>URL Reputation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Disclaimer Text</td>
</tr>
<tr>
<td>Bypass Outbreak Filter Scanning</td>
</tr>
<tr>
<td>Bypass DKIM Signing</td>
</tr>
<tr>
<td>Send Copy (Bcc:)</td>
</tr>
<tr>
<td>Notify</td>
</tr>
<tr>
<td>Change Recipient to</td>
</tr>
<tr>
<td>Send to Alternate Destination Host</td>
</tr>
<tr>
<td>Deliver from IP Interface</td>
</tr>
<tr>
<td>Strip Header</td>
</tr>
<tr>
<td>Add/Edit Header</td>
</tr>
<tr>
<td>Add Message Tag</td>
</tr>
<tr>
<td>Add Log Entry</td>
</tr>
<tr>
<td>S/MIME Sign/Encrypt on Delivery</td>
</tr>
<tr>
<td>Encrypt and Deliver Now (Final Action)</td>
</tr>
<tr>
<td>S/MIME Sign/Encrypt (Final Action)</td>
</tr>
<tr>
<td>Bounce (Final Action)</td>
</tr>
<tr>
<td>Skip Remaining Content Filters (Final Action)</td>
</tr>
<tr>
<td>Drop (Final Action)</td>
</tr>
</tbody>
</table>

URL Reputation is:

- Malicious (-10.0 to -6.0)
- Neutral (-5.9 to 5.9)
- Clean (6.0 to 10.0)
- Custom Range (min to max) [-5.9, -5.8]
- No Score

Use a URL whitelist: None

Action on URL:

- Defang URL
- Redirect to Cisco Security Proxy
- Replace URL with text message
- Perform Action for:
  • All messages
URL Categorization

- URL Categorization on the ESA leverages the same data as the Web Security Appliance (WSA) and Cloud Web Security (CWS)
- Use this to compliment Acceptable Use Policies to prevent inappropriate URLs in email
URL Logging & Tracking

- Logging of URLs can be seen in the mail logs and only if the outbreakconfig command is run.
URL Evaluation and options

- With the 10.0 release, URL information can be shown in message tracking if enabled by role

<table>
<thead>
<tr>
<th>Processing Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>URL Details</strong></td>
</tr>
<tr>
<td><strong>Summary</strong></td>
</tr>
<tr>
<td><strong>13 Jun 2016 13:15:23 (GMT -04:00)</strong></td>
</tr>
</tbody>
</table>
Graymail Unsubscribe

- Graymail Unsubscribe is an additional license
- It provides protection against malicious threats masquerading as unsubscribe links
- A uniform interface for all subscription management to end-users
- Better visibility to the email administrators and end-users into such emails
Graymail Unsubscribe

End-user clicks on the rewritten unsubscribe link in the banner

Click-time check of the rewritten link. If found safe, redirect to UnSubscribe service

Cisco executes un-subscription on behalf of the end-user

Cisco ESA Safe Unsubscribe Service

Graymail Safe Unsubscribe

You have successfully unsubscribed from allgraymail.com
Web Interaction Tracking & Reporting

- On box reporting (batch) can provide valuable insight into who clicked on certain URLs
- More valuable as a training tool and understanding who is being targeted inside your environment
- Reporting and Tracking pages will show the URLs (Tracking in 10.0 for URL details)
Phishing is not just URLs

- Other scams such as Banking, Money Mules, Dating, 419, etc are also used to get information from targets
- Blended threats combine spoofing and phishing in an attempt to look more legitimate to the target
- Threat Outbreak Filters must be enabled in order to help detect and stop these threats
## Threat Outbreak Filters

|----------------|-----------------------------------------|---------------------------|-----------------------------|--------------------------------------|-------------------------------|--------------------------------------|----------------|----------------|----------------------------|----------------|

- Enable Threat Outbreak Filters (not enabled by default) by enabling Message Modification
- URL Rewriting allows for suspicious urls to be analyzed by Cisco Cloud Web Security (Reputation, AV/AM, AMP)
Anti-Spoofing: HAT, Filters and Forged Email Detection
## Anti-Spoofing Overview

<table>
<thead>
<tr>
<th>Simple Spoof</th>
<th>Simple spoof is where the attacker attempts to change or manipulate the envelope from in the headers of an email. This spoof is relatively easy to detect using SPF or DMARC as well as other header validation checks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reply-To Spoof</td>
<td>Reply-To spoof is where the sending address does not match the reply-to address. This is a low spoof indicator and can lead to high false positives.</td>
</tr>
<tr>
<td>Cousin Domain / Typo Squatting</td>
<td>Attacks become more sophisticated by relaying on minor changes to the suffix and / or prefix of the email addresses to trick users. High probability of success and hard to detect due to large number of variations</td>
</tr>
<tr>
<td>Display Name Modification</td>
<td>Also called Business Email Compromise (BEC) is the most complex attack involves the use of legitimate domains (either hijacked or created) with the manipulating message headers to show an accurate Display Name and a Cousin domain/typo in the email address to trick targets into releasing information. This is the most common attack today with a high success rate.</td>
</tr>
</tbody>
</table>
Impact of Social Engineering

• Social Engineering has added to the success rate for spoofing attacks. Attackers will follow targets for months, on social media, news, etc.

• Will craft messages with “history” to add legitimacy to the request being made

• They will look for an event – i.e travel abroad, large deals, vendor agreements and use it to express urgency

• Along with technical controls, user education is key to prevent financial lost, brand damage, or legal ramifications.
MailFlow policies: DKIM/SPF/DMARC

• During connection, the HAT can be configured to validate SPF, DKIM and DMARC records

• No checks are enabled by default in the Mail Flow Policies

• DMARC has the ability to stop / block mail via policy settings, SPF and DKIM mark headers for further action via Content Filters or Message Filters
How it works: SPF

• Sender Policy Framework, specified in RFC4408
• Allows recipients to verify sender IP addresses by looking up DNS records listing authorized Mail Gateways for a particular domain
• Uses DNS TXT Resource Records
• Can verify HELO/EHLO and MAIL FROM identity (FQDN)
• Upon evaluation of SPF records, the following can these results:

<table>
<thead>
<tr>
<th>Result</th>
<th>Explanation</th>
<th>Intended action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pass</td>
<td>The SPF record designates the host to be allowed to send</td>
<td>accept</td>
</tr>
<tr>
<td>Fail</td>
<td>The SPF record has designated the host as NOT being allowed to send</td>
<td>reject</td>
</tr>
<tr>
<td>SoftFail</td>
<td>The SPF record has designated the host as NOT being allowed to send but is in transition</td>
<td>accept but mark</td>
</tr>
<tr>
<td>Neutral</td>
<td>The SPF record specifies explicitly that nothing can be said about validity</td>
<td>accept</td>
</tr>
<tr>
<td>None</td>
<td>The domain does not have an SPF record or the SPF record does not evaluate to a result</td>
<td>accept</td>
</tr>
<tr>
<td>PermError</td>
<td>A permanent error has occurred (eg. badly formatted SPF record)</td>
<td>unspecified</td>
</tr>
<tr>
<td>TempError</td>
<td>A transient error has occurred</td>
<td>accept or reject</td>
</tr>
</tbody>
</table>
SPF Record Semantics

`acmilan.com IN TXT v=spf1 ip4:77.92.66.4 -all`

SPF version

Verification mechanisms
How it works: SPF

• Mechanisms: all, ip4, ip6, a, mx, ptr, exists, include
• Qualifiers: "+" Pass, "-" Fail, "~" SoftFail, "?" Neutral
• Modifiers: redirect, modifier

• Examples:
  • “v=spf1 mx –all” is allow MX to send mail, but no other domain
  • “v=spf1 +all” Nullifies any usefulness of SPF
  • “v=spf1 ip4:192.168.0.1/16 –all” Allow any IP address between 192.168.0.1 and 192.168.255.255
  • “v=spf1 mx/24 mx:offsite.domain.com/24 -all” Domain's MX servers receive mail on one IP address, but send mail on a different
SPF on the ESA

When SPF is enabled, the ESA will stamp headers in the message.

Use the results inside message or content filters to determine the action.

PRA identities are evaluated in the message filters only.

SPF vs SIDF, an interesting read: http://www.openspf.org/SPF_vs_Sender_ID
SPF Best Practices

• Plan to include “-all” in your SPF records
  • Consider all legitimate servers sending e-mail on your behalf
  • Make it part of security policy for roaming users to use authenticated SMTP on your gateways for sending outgoing mail

• Add your relay hosts’ HELO/EHLO identity to SPF records

• Create SPF records for all of your subdomains too
  • Publish null SPF records for domains/hosts that don’t send mail!
    nomail.domain.com. IN TXT "v=spf1 -all"

• Only include “MX” mechanism if your incoming mail servers also send outgoing mail

• (for now) Publish both TXT and SPF DNS Resource Records with your SPF record data.
How it works: DKIM

- Domain Keys Identified Mail, Specified in RFC5585
  - Additional RFC6376 (DKIM Signatures), RFC5863 (DKIM Development, Deployment and Operation), RFC5617 (Author Domain Signing Practices (ADSP))

- In a nutshell: Specifies methods for gateway-based cryptographic signing of outgoing messages, embedding verification data in an e-mail header, and ways for recipients to verify integrity of the messages

- Uses DNS TXT records to publish public keys

20120113._domainkey.gmail.com IN TXT "k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1Kd87/UeJjenpabgbFwh+eBCsSTrqmwIYYvywlbbqoo2DymndFkbj0VIPIldNs/m40KF+yzMn1skyoxcTUGCQs8g3FgD2Ap3ZB5DekAo5wMmk4wimDO+U8QzI3SD0" "7y2+07w1NwWt8svnxdGkVbhz8Y8i+RQ9DpSVpPbF7ykQxtKXkv/ahW3KjViiAH+ghvvlhkx4YS1c9o5wVmA50ctMEeWUwg8Istjqz8BZetWbf41fbNhhte7Y+YqZ0wq1Sd0DbvVAD9NOZK9vlfuac0598HY+vtSBczUiKERHv1yRbcaQtZFHs5wttiRrN04BLUTD21MycBX5jYchJhPY/wIDAQAB"
DKIM Operation

Outgoing msg

Generate keypair

Canonicalize + Sign

Insert DKIM-Signature

DNS TXT RR

Receive msg

Parse DKIM-Signature

Verify b and bh

Deliver/Drop/Quarantine…
How it works: DKIM Signature

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;

d=gmail.com; s=20120113;

h=mime-version:date:message-id:subject:from:to:content-type;

bh=pMD4ZYid1vn/f7RZAy6LEON+d+W+AD1VSR6I0zrYofA=;

b=n3EBxT5DwNbeISSYpKT6zOKHeb8ju51F4X8H2BKhDWk9YpOk8DuU4zgLh
srfFeCv+/2XEPnQaIVtKmE0h7ZTI8yvV61DEQtJQQWqQ/RA7WsN4Tjg4B
JAXPR+yF6xwLLcQqMwzsgLxC3pQAPW3Lp7py9C62naue13nLEM0gLnXYSh
Uvq6IS+qfJBOkeMby9WUsqRecg0AWX8Dfb8gxXHfH8wKfJ96KitB6iPFq
ufI0TaZWMhiFnL+NHt06v0PwsC6hSccuk0eTDu9Uqyf8bDn4opkhg7tZ
SyGhUFeuqwxxJoCJcghGf7edZ00IgZtEcuxLMcg1+mpSje2YIfexgFRg==
DKIM Public Key Retrieval

• DNS query:

\(<selector>._domainkey.<SDID>\)

• For our example:

20120113._domainkey.gmail.com IN TXT “k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1Kd87/UeJjenpabgbFwh+eBCsSTRqmwIYYvywlbhbqoo2DymndFkbjOVIPIIdNs/m40KF+yzMn1skyoxcTUGCQs8g3FgD2Ap3ZB5DekAo5wMmk4wimDO+U8QzI3SD0" "7y2+07w1NWwIt8svnxgdxGkBbhzY8i+RQ9DpSVpPbF7ykQxtKXkv/ahW3KjViiAH+ghvvIhkx4xYS1c9oSwVmA15octMEEwUWg8Istjqz8BZeTWbf41fbNhte7Y+YqZ0wq1Sd0DbvYAD9NOZK9v1fuac0598HY+vtSbczUiKERHv1yRbcaQtZFh5wtiRrN04BLUTD21MycBX5jYchHjPY/wIDAQAB"
DKIM on the ESA

- DKIM Settings in the HAT can be set to verify signatures
- Use a content filter to enforce policy based on DKIM auth result
- Use an action to Policy quarantine to be able to review spoofs
How it works: DMARC

• Both DKIM and SPF have shortcomings, not because of bad design, but because of different nature of each technology

• Thus, DMARC was born:
  • Leveraging great existing technologies, providing a glue to keep them in sync, and allowing senders to mandate rejection policies and have visibility of offending traffic

• Domain-based Message Authentication, Reporting And Conformance
  • Defined in RFC 7489
  • Provides:
    • DKIM verification
    • SPF authentication
    • Synchronization between the two and all sender identities (Envelope From, Header From)
    • Reporting back to the spoofed entity
DMARC Operation

- Publish SPF
- Publish DKIM
- Publish DMARC
- Insert DKIM-Signature
- Outgoing msg
- SPF (or TXT) DNS RR
- DKIM (TXT) DNS RR
- DMARC (TXT) DNS RR
- Check SPF
- Check DKIM
- Check DMARC (TXT) DNS RR
- Apply DMARC Policy
- Fetch DMARC Policy
- Send DMARC Report(s)
- Align Identifiers
- Check SPF on Header From
How it works: DMARC Record Structure

TXT Record for Domain amazon.com

_v=DMARC1; p=quarantine; pct=100; rua=mailto:dmarc-reports@bounces.amazon.com; ruf=mailto:dmarc-reports@bounces.amazon.com

Version of DMARC

Action on Auth Failure

% of messages to apply policy

Aggregate Feedback report URI

Forensic Feedback report URI
DMARC Policy Specification

_dmarc.amazon.com IN TXT "v=DMARC1; p=quarantine; pct=100; rua=mailto:dmarc-reports@bounces.amazon.com; ruf=mailto:dmarc-reports@bounces.amazon.com"
DMARC Policy

- Policies requested by senders:
  - None
  - Quarantine
  - Reject

- Receivers MAY deviate from requested policies, but SHOULD inform the sender why (through Aggregate Report)

- Sampling rate ("p" tag) instructs the receiver to only apply policy to a fraction of messages
How to enable DMARC (inbound)

- DMARC is configured via by creating a profile and then applying the profile to a Mail Flow Policy
- By default the profile is set to Monitor for DMARC violations, however it needs to be applied to a policy for it to evaluate DMARC records
- Monitor and Tune settings and SenderGroups and move to blocking when ready
How to Start With DMARC (outbound)

1. Correctly deploy DKIM and SPF
2. Make sure that your identifiers will align
3. Publish a DMARC record with “p=none”, gather rua and ruf reports for a while
4. Analyze the data and modify your mail streams (or DKIM/SPF parameters)
5. Eventually apply “reject” or “quarantine” policy after running in Monitor mode
## Allowed Spoofing & Sender Verification Table

- Before you begin to block any messages, determine who is allowed to spoof; external marketing firms, vendors, SaaS tools and notifications

- Use a filter to mark and track addresses that match your domains or copy messages into a quarantine for review

- In your HAT create a SPOOF_ALLOW (or similar) to add the host addresses for vendors that are allowed. Use the SPOOF_ALLOW as part of the filter to ensure that those messages are not flagged or stopped

- The Sender Verification Table is enabled within the Mail Flow Policy and can be used to evaluate the mail from is exists and resolvable

- Use the SVT table to set your domains to block and apply to the policies

---

### Sender Verification Table

<table>
<thead>
<tr>
<th>Envelope Sender DNS Verification</th>
<th>On</th>
<th>Off</th>
</tr>
</thead>
</table>

- **Molformed Envelope Senders**
  - SMTP Code: 503
  - 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 <$Env1

- **Envelope Senders whose domain does not exist**
  - SMTP Code: 553
  - SMTP Text: #5.1.8 Domain of sender address <$Env1

### Add Sender Verification Exception Table

<table>
<thead>
<tr>
<th>Sender Verification Exception</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Exception:</strong></td>
</tr>
<tr>
<td><strong>Order:</strong></td>
</tr>
<tr>
<td><strong>Behavior:</strong></td>
</tr>
<tr>
<td>Rejected SMTP Code:</td>
</tr>
<tr>
<td>Rejected SMTP Text:</td>
</tr>
</tbody>
</table>

---

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public
Quick Review: Message Filters

- High-performance scriptable filtering capability
- Accessible from CLI only (filters command)
- Allowing complex logical operators between conditions
- **All** Message Filters are evaluated for **all** messages
- Executed serially
- Apply to **entire** mail flow, incoming and outgoing!
- Message Filters occur before Policy Engine! Filter matches if **any** recipient matches, and **all** actions are executed for **all** recipients!
Message Filters

Name: myFilter

Condition(s):
if (body-contains('word',1)) AND \n(attachment-filetype == 'Document') {

Action(s):
quarantine('Policy');
}
Filter Conditions

- Can be combined using AND, OR, NOT
- ! = equals NOT if condition result can be evaluated
  (not (attachment-filetype == 'Document')) equals (attachment-filetype != 'Document')
- Mostly support regular expressions
- Least expensive conditions evaluated first
- Unneeded tests are not evaluated
- Inactive filters are evaluated!
Message Filter Actions

- Actions are executed in order specified
- Final actions: skip-filters, drop, bounce, encrypt, smime-gateway
  - Just exit message filters and continue down the pipeline (except drop)
- All filter actions across all matching filters are cumulative
  - If a message matches multiple filters which execute the same action, only the last specified action is executed
Filtering & Quarantine Spoofs

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 ("admin@company.com"); 
}

- Above is an example of a message filter that will look to see if the IP is not in the RELAYLIST and is trying to send a message that matches a dictionary of names in the dictionary
- It will duplicate the message and place in quarantine for review
- Modify to include SPOOF_ALLOW list and domains in the From header
Forged Email Detection (New for 10.0)

- Forged Header Detection will look for permutations in the Display Name and the prefix of the email address in the From Header
- Use this rule to look for matches against a dictionary of names that are exact or some form of typo squatting
- i.e: Han S0lo, Han Slo, Han So1o
Forged Email Filters

• In this example, we took the from header and stripped it from the message if the match was 70 or above

• Combined with a warning disclaimer this would expose the bad sender while warning the end user

• Idea here is that for names that are low threshold matches, you can use the strip header to expose envelope sender – if it is legitimate, it won’t disrupt mail flow

• If all else fails, warn the user of a potential issue by using a disclaimer text on top of the message

Info: MID 2089 Forged Email Detection on the From: header with score of 100, against the dictionary entry Han Solo
Phish & Spoofing Checklist

• Enable URL Filtering on the ESA
• Enable Web Interaction Tracking (if permitted by policy)
• Enable certain admin users URL visibility in Message Tracking (if permitted by policy)
• Enable Threat Outbreak Filtering and message modification – warn your users!
• Whitelist your partner URLs, use the scores to create filter for others
• Combine the reputation rules and leverage language detection as part of the logic
• Use the policies to define the level of aggression for rule sets

• Make a plan to enable SPF, DKIM and DMARC
• Know who your allowed external spoofs are by tracking them via filters and policies
• Build the list as the exception, trap all others
• With 10.0 use the Forged Email Detection Feature to look for matches on the display name, if too close to call, drop the From header
• Send a copy of suspected spoofs to a quarantine for review and then tune your rules to start blocking messages
Attachment Handling
Block the unwanted file types

• Within either a content or message filter an organization can define how to handle attachments on a per policy basis.

• Commonly customers will create a content filter to block unwanted file types

• Using the predefined libraries simplifies the process

• The system will detect changed extensions or attempts to hide files within multiple zip levels in order to evade file blocking
### Blocking early in the pipeline

- If files are being outright dropped (i.e. Executables) then doing it earlier in the pipeline would save on AV, AMP and OF cycles.

```javascript
strip_all_exes: if (true) {
    drop-attachments-by-filetype ('Executable', "Removed attachment: $dropped_filename");
}
```

- A non-final action such as quarantine will allow the file to continue processing the file and any other verdict will apply.

<table>
<thead>
<tr>
<th>Anti-Spam</th>
<th>Anti-Virus</th>
<th>Advanced Malware Protection</th>
<th>Graymail</th>
<th>Content Filters</th>
<th>Outbreak Filters</th>
</tr>
</thead>
<tbody>
<tr>
<td>(use default)</td>
<td>Disabled</td>
<td>(use default)</td>
<td>(use default)</td>
<td>(use default)</td>
<td>(use default)</td>
</tr>
<tr>
<td>(use default)</td>
<td>Disabled</td>
<td>(use default)</td>
<td>(use default)</td>
<td>(use default)</td>
<td>(use default)</td>
</tr>
</tbody>
</table>
Block the known viruses

- Sophos comes bundled with the licenses, enable and block known viruses
- Encrypted => Password Protected, Signed
- Unscannable => Too large to scan, malformed
- Do you still repair? Most customers today do not have the repair option enabled for virus infected messages.

|----------------|---------------------------------------------------------------|---------------------------------------------------------------|---------------------------------------------------------------|---------------------------------------------------------------|----------------|----------------------------------|

Top Incoming Virus Types Detected

- Trojan/Docx: AGS
- Trojan/Docx: AJT
- Trojan/Docx: APZ
- Trojan/Docx: SL
- Trojan/Agent: APKJ
- Trojan/Docx: AIE
- Trojan/Docx: J
- Trojan/Fareit: UT
# Enabling AMP

- AMP is an additional license on the ESA and CES

- 4 components to AMP:
  - File Reputation
  - File Analysis
  - File Retrospection
  - Mailbox Auto Remediation (New)

### Table

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

![Incoming files handled by AMP](image)

![Top Incoming Malware Threat Files](image)
How AMP works
Mailbox Auto Remediation

- API integration with Office 365 / Azure for Malware Remediation

- When a retrospective alert is received, the ESA can remove the email from the mailbox automatically

1. Original message delivered with non-malicious verdict
2. Retrospective alert of file that is now deemed malicious received by CES
3. API call to O365 to remove message from the mailbox, or forward to specific mailbox
Enable Virus Outbreak Filters

- VOF is enabled by default
- Provides a significant catch rate for outbreaks over traditional scanning engines
- It's the human element, after signature, heuristics and hash based scanning

http://www.senderbase.org/static/malware/#tab=0
File Handling Checklist

- Create a filter to block, quarantine or strip attachment that are deemed risky for the organization
- Use AV to block the known viruses. Cleaning / Repairing viruses from files may be something you want to turn off…
- Ensure Virus Outbreak is turned on all your policies, it provides an average 10+ hr lead time on 0-day attacks

- Evaluate AMP is you don’t have it already
- AMP will hash all files and ask for file reputation
- Macro inspection is performed by File Analysis on AMP along with other file types
- Retrospection alerts can now do remediation with Office 365
In Summary

• The days of set it and forget it are long gone – continuous monitoring and tuning are required to keep up with today's threats

• Understand what your organization's security posture is and apply it to your appliances

• Keep your appliances updated – we are constantly introducing new features that require upgrades / updates

• We are publishing guides to help with tuning and setup new features on Cisco Email Security
Security Joins the Customer Connection Program
Customer User Group Program

- **Who can join**: Cisco customers, service providers, solution partners and training partners
- **Private online community** to connect with peers & Cisco’s Security product teams
- Monthly **technical & roadmap briefings** via WebEx
- Opportunities to **influence product direction**
- Local **in-person meet ups** starting Fall 2016
- **New member thank you gift* & badge ribbon** when you join in the Cisco Security booth
- **Other CCP tracks**: Collaboration & Enterprise Networks

Join in World of Solutions
Security zone → Customer Connection stand
- Learn about CCP and Join
- New member thank-you gift*
- Customer Connection Member badge ribbon

Join Online
www.cisco.com/go/ccp
Come to Security zone to get your new member gift* and ribbon

* While supplies last
Complete Your Online Session Evaluation

- Give us your feedback to be entered into a Daily Survey Drawing. A daily winner will receive a $750 Amazon gift card.

- Complete your session surveys through the Cisco Live mobile app or from the Session Catalog on CiscoLive.com/us.

Don’t forget: Cisco Live sessions will be available for viewing on-demand after the event at CiscoLive.com/Online
Continue Your Education

• Demos in the Cisco campus
• Walk-in Self-Paced Labs
• Lunch & Learn
• Meet the Engineer 1:1 meetings
• Related sessions
Thank you
# Security Cisco Education Offerings

<table>
<thead>
<tr>
<th>Course</th>
<th>Description</th>
<th>Cisco Certification</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCIE Security</td>
<td>Expert Level certification in Security, for comprehensive understanding of security architectures, technologies, controls, systems, and risks.</td>
<td>CCIE® Security</td>
</tr>
<tr>
<td>Implementing Cisco Threat Control Solutions (SITCS)</td>
<td>Deploy Cisco’s Next Generation Firewall (NGFW) as well as Web Security, Email Security and Cloud Web Security</td>
<td></td>
</tr>
<tr>
<td>Implementing Cisco Secure Access Solutions (SISAS)</td>
<td>Deploy Cisco’s Identity Services Engine and 802.1X secure network access</td>
<td></td>
</tr>
<tr>
<td>Implementing Cisco Secure Mobility Solutions (SIMOS)</td>
<td>Protect data traversing a public or shared infrastructure such as the Internet by implementing and maintaining Cisco VPN solutions</td>
<td></td>
</tr>
<tr>
<td>Implementing Cisco Network Security (IINS 3.0)</td>
<td>Focuses on the design, implementation, and monitoring of a comprehensive security policy, using Cisco IOS security features</td>
<td>CCNA® Security</td>
</tr>
<tr>
<td>Securing Cisco Networks with Threat Detection and Analysis (SCYBER)</td>
<td>Designed for security analysts who work in a Security Operations Center, the course covers essential areas of security operations competency, including event monitoring, security event/alarm/traffic analysis (detection), and incident response</td>
<td>Cisco Cybersecurity Specialist</td>
</tr>
</tbody>
</table>

For more details, please visit: [www.cisco.com/go/securitytraining](http://www.cisco.com/go/securitytraining) or [http://learningnetwork.cisco.com](http://learningnetwork.cisco.com)

Questions? Visit the Learning@Cisco Booth or contact [ask-edu-pm-dcv@cisco.com](mailto:ask-edu-pm-dcv@cisco.com)