



You make **possible**



>250 *not* OK

Going on the defensive with Cisco Email Security

Robert Sherwin, Filipe Lopes

TECSEC-2345

CISCO *Live!*

Barcelona | January 27-31, 2020



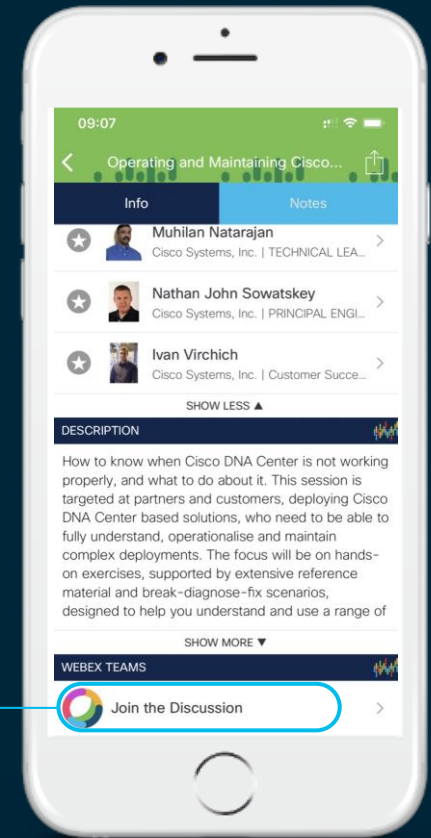
Cisco Webex Teams

Questions?

Use Cisco Webex Teams to chat with the speaker after the session

How

- 1 Find this session in the Cisco Events Mobile App
- 2 Click “Join the Discussion”
- 3 Install Webex Teams or go directly to the team space
- 4 Enter messages/questions in the team space



Agenda

- Introductions
- Understanding the Email Pipeline
- Base Configuration Settings
 - IP & Domain Reputation
 - Sender Group and Mail Flow Policies
 - Engine setup and tuning
 - Delivery recommendations
- Threat Defense Configuration
 - Spoofing and Phishing Detection
 - Attachment Control and Defense
- Cisco Threat Response
- Monitoring & Tools
- Summary & Checklist

Introductions

This sessions speakers

- Technical Marketing Engineer, Email Security
- 12 years at Cisco since CSAP, joined TME team 2019
- MsC degree in Systems Engineering
- Speaker at Multiple Conferences (Portugal Wireless Conference, Smart Mobility Summit, IoT Vodafone Conference)
- Cisco's Technical Lead for Web Summit (~60.000 attendees)
- Part of the Core Team that Designs, Builds and Operates CiscoLive! Europe
- Based out of Lisbon, Portugal (EU)

Filipe Lopes
(jlopes@cisco.com)



- Technical Marketing Engineer, Email Security
- Joined Cisco December 2011
- Cisco Live Speaker in US, EMEA, APJC
- 18 years of combined Network, Data Center, and Security experience
- 6 years in Cisco TAC, joined TME team in 2018
- Based out of Morrisville, NC (US)

Robert Sherwin
(robsherw@cisco.com)



Introductions

Email Security specific sessions this week

250 not OK: Going on the defensive with Cisco Email Security

- TECSEC-2345
- Monday, January 27 | 08:45 AM - 01:00 PM
- Hall 8.1, CC8, Room 8.29/8.30

From Zero to DMARC Hero

- TECSEC-2310
- Monday, January 27 | 02:30 PM - 06:45 PM
- Hall 8.0, Session Room D138

API Integrations for Cisco Email Security

- DEVNET-2326
- Tuesday, January 28 | 10:00 AM - 10:45 AM
- Hall 6 - The Hub, DevNet Classroom 2

SPF is not an acronym for "Spooof"! Let's utilize the most out of the next layer in Email Security!

- BRKSEC-2327
- Thursday, January 30 | 02:45 PM - 04:15 PM
- Hall 8.0, Session Room B115

AsyncOS Release 13.0 - What's new in Email Security

- LTRSEC-2319
- Thursday, January 30 | 09:00 AM - 01:00 PM
- Hall 8.0, Session Room B110

Fixing Email! - Cisco Email Security Advanced Troubleshooting

- BRKSEC-3265
- Friday, January 31 | 09:00 AM - 10:30 AM
- Hall 8.0, Session Room A104

Introductions

Our schedule for this session

- Technical Seminar Agenda – Morning Half Day
 - 08:45 – 10:45 (2 hours)
 - 10:45 – 11:00 Break
 - 11:00 – 13:00 (2 hours)
 - 13:00 – 14:30 Lunch

Audience Questions

We have 4.25 hours... Let's get to know each other!

- Are you new to Cisco Email Security? Or, are you a Pro?
- What is your primary purpose of attending our TECSEC?
- Have you attended our session previous years, or at another Cisco Live?
- What is the top 3 items for Email Security that you want to take away today?
- What tools, software makes your daily life easier?

As we go along – if you have a question or comment, let us know! We are happy to make this an interactive session. We're here to help you. (And, perhaps you will help us, too!) **We hope that you enjoy the session and your week at Cisco Live!**



Versions of AsyncOS

Recommended version(s) that we will discuss today include:

- General Deployment (GD)
 - 12.5.1-037
- Limited Deployment (LD)
 - 13.0.0-375

Email
Security



- General Deployment (GD)
 - 12.5.0-658
- Limited Deployment (LD)
 - 13.0.0-239

Security
Management



Note: Cloud Email Security (CES) ESA and SMA versions are managed by Cisco

Release Notes & User Guide for AsyncOS 12.0

http://cs.co/email_security_support

http://cs.co/12_0_release_notes

http://cs.co/12_0_user_guide



Release Notes for AsyncOS 12.0 for Cisco Email Security Appliances

Published: November 26, 2018

Contents

- What's New In This Release, page 2
- Changes in Behavior, page 6
- Upgrade Paths, page 6
- Installation and Upgrade Notes, page 6
- Known and Fixed Issues, page 11
- Documentation for FCS, page 12
- Related Documentation, page 12
- Service and Support, page 13



Cisco Systems, Inc.
www.cisco.com

Products Support Partners More

Support / Product Support / Security / Cisco Email Security Appliance / End-User Guides /

User Guide for AsyncOS 12.0 for Cisco Email Security Appliances - GD (General Deployment)

Find Matches in This Book

Translations Download Print

Book Table of Contents

- Getting Started with the Cisco Email Security Appliance
 - Accessing the Appliance
 - Setup and Installation
 - Understanding the Email Pipeline
 - Configuring the Gateway to Receive Email
 - Sender Reputation Filtering
 - Defining Which Hosts Are Allowed to Connect Using the Host Access Table
 - Accepting or Rejecting Connections Based on Domain Name or Recipient Address
 - Using Message Filters to Enforce Email Policies
 - Mail Policies

Updated: January 7, 2020

Was this Document Helpful?

Yes No Feedback

Contact Cisco

Open a Support Case (Requires a Cisco Service Contract)

Related Cisco Community Discussions

Cisco Email Security Appliance

Release Notes & User Guide for AsyncOS 13.0

http://cs.co/email_security_support

http://cs.co/13_0_release_notes

http://cs.co/13_0_user_guide






Release Notes for AsyncOS 13.0 for Cisco Email Security Appliances



Published: September 23, 2019

Contents

- What's New In This Release, page 2
- Changes in Behavior, page 8
- Comparison of Web Interfaces, New Web Interface vs. Legacy Web Interface, page 12
- Upgrade Paths, page 15
- Installation and Upgrade Notes, page 15
- Known and Fixed Issues, page 20
- Related Documentation, page 21
- Service and Support, page 22

MENU   

User Guide for AsyncOS 13.0 for Cisco Email Security Appliances - LD (Limited Deployment)

Find Matches in This Book  

Book Table of Contents

- Getting Started with the Cisco Email Security Appliance
- Accessing the Appliance
- Setup and Installation
- Understanding the Email Pipeline
- Configuring the Gateway to Receive Email
- Sender Reputation Filtering
- Defining Which Hosts Are Allowed to Connect Using the Host Access Table
- Accepting or Rejecting Connections Based on Domain Name or Recipient Address
- Using Message Filters to Enforce Email Policies
- Mail Policies
- Content Filters

Updated: September 23, 2019


Was this Document Helpful?

Yes No [Feedback](#)

Contact Cisco

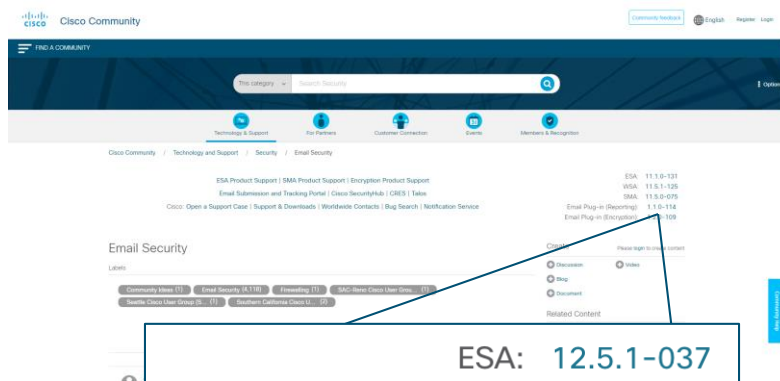
Open a Support Case
(Requires a Cisco Service Contract)

Related Cisco Community Discussions

 Cisco Email Security Appliance
Last Reply 4 years ago

Not getting notifications of new versions?

Cisco Support Community – Email Security
<https://supportforums.cisco.com/community/5756/email-security>



ESA: 12.5.1-037
SMA: 12.5.0-658
Email Plug-in (Reporting): 1.1.0-114
Email Plug-in (Encryption): 1.2.1-118

cisco Live!

Cisco Notification Service:
<https://www.cisco.com/cisco/support/notifications.html>

Add / Edit a Notification

1 Topic Type > 2 Topic > 3 Sub-Topic(s) > 4 Finish >

Choose an alert for your notification topic

- End-of-Sale and End-of-Life Announcements
- Field Notices
- Security Advisories
- Software Updates [New, Certified, Software Advisories, Deferred, Obsolete]
- Known Bugs



Add / Edit a Notification

1 Topic Type > 2 Topic > 3 Sub-Topic(s) > 4 Finish >

Verify your selections below. You may repeat this process and add another topic to the same notification and then choose sub-topic for it. You may also add additional sub-topic to an existing topic with this notification.

When satisfied press 'Finish' button to save your profile.

Software Updates

An Email with links and summaries delivered Daily Summary to

Software Updates

Email Security Appliance

Add another subtopic



Bookmark & Subscribe to these today!

Global Email Issues / Notifications

<https://urgentnotices.statuspage.io/>



SUBSCRIBE TO UPDATES

All Systems Operational

About This Site

Welcome to the Cisco Email and Web Security status page. The purpose of this page is to track issues impacting the Cisco's Email Security Appliance (ESA), Web Security Appliance (WSA) and associated services.

For the status of Cisco Umbrella Service, please visit: <https://status.umbrella.com>

For the status of Cisco Cloud Email Security (CES), please visit: <https://status.ces.cisco.com/>

NOTE: The CES status page is currently under construction and running as a pilot.

Do you have a question or would like to report a status page related issue? Please contact security-urgent-notices@cisco.com.

Uptime over the past 90 days. [View historical uptime.](#)

Advanced Malware Protection (AMP)

File Reputation 🔄

Operational

File Analysis 🔄

Operational

Cloud Email Status

<https://status.ces.cisco.com>

Cloud Email Security



SUBSCRIBE

All Components are operational

Component Summary 🔍

Component Name	Component Status
CES Americas Response Time : 428 ms	✔ Operational
CES Asia Response Time : 250 ms	✔ Operational
CES Canada Response Time : 121 ms	✔ Operational
CES Europe Response Time : 85 ms	✔ Operational
UCS Test Response Time : 51 ms	✔ Operational

The Email Pipeline

Cisco Email Security Mail Flow Pipeline

INCOMING

Connection level protection

Anti-spoof, throttling & verification

Sending domain verdict analysis

Spam protection, URL analysis

Virus protection

Malware protection

Marketing/Social/Bulk email detection

Content protection

Malware, Phishing, URL threat protection

Phishing behavioral analytics & protection



Sender Reputation Filtering (SBRS)



Connection Filtering



Sender Domain Reputation (SDR)

* Message Filtering



Content Scanning (CASE)



Anti-virus Scanning (AV)



Advanced Malware Protection (AMP)



Graymail Detection



Content Filtering



Outbreak Filtering (VOF)



Advanced Phishing Protection (APP)

Per-policy

Cisco Email Security Mail Flow Pipeline

OUTBOUND

Connection level protection

Encryption & authentication enforcement

Spam protection, URL analysis

Virus protection

Malware protection

Marketing/Social/Bulk email detection

Content protection

Malware, Phishing, URL threat protection

Sensitive data protection & encryption

Brand protection, SPF/DKIM/DMARC administration



Sender Reputation Filtering (SBRS)



Connection Filtering

* Message Filtering



Content Scanning (CASE)



Anti-virus Scanning (AV)



Advanced Malware Protection (AMP)



Graymail Detection



Content Filtering



Outbreak Filtering (VOF)



Data Loss Prevention (DLP)



Domain Protection (DP)

Per-policy

Cisco Email Security Mail Flow Pipeline

Post Delivery

Unsubscribe validation and management

URL reporting + end-user click tracking

Verdict change alerting & mailbox administration

Threat detection, investigation, remediation



Graymail Unsubscribe




URL rewrite & tracking



AMP retrospection & remediation



Cisco Threat Response (CTR)



Within these layers of email security,
Cisco Email Security features, and services
that always come with acronyms...

Typical acronyms used in email security

Who loves acronyms? Cisco loves to utilize acronyms a lot...

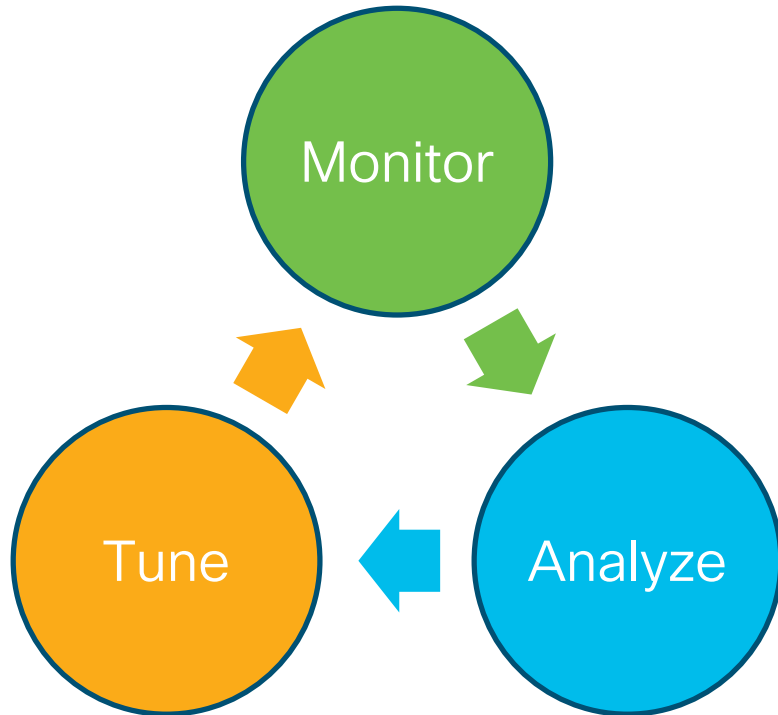
ADFS : Active Directory Federation Services
AMP : Advanced Malware Protection
API : Application Programming Interface
APPC : Advanced Phishing Protection Console
AS (A/S) : Anti-spam
AV (A/V) : Anti-virus
BATV : Bounce Address Tag Validation
BEC : Business Email Compromise
BIMI : Brand Indicator Message Identification
CASE : Context Adaptive Scanning Engine
CDP (DMP) : Cisco Domain Protection
CES : Cloud Email Security
CLI : Command Line Interface
CRES (see RES)
CTR : Cisco Threat Response
DCID : Delivery Connection ID
DHAP : Directory Harvest Attack Prevention
DKIM : DomainKeys Identified Mail
DLP : Data Loss Prevention
DMARC : Domain-based Message Authentication, Reporting and Conformance
DNS : Domain Name System
ESA : Email Security Appliance
ESMTP : Extended (or Enhanced) Simple Mail Transfer Protocol
ETF : External Threat Feed
EUQ : End-user Quarantine (aka Spam Quarantine)
FA : File Analysis (Threat Grid)
FED : Forged Email Detection
FR : File Reputation (AMP)
GUI : Graphical User Interface

HAT : Host Access Table
ICID : Incoming Connection ID
IETF : Internet Engineering Task Force
IMS : Intelligent Multi-Scan
IPAS : IronPort Anti-Spam
ISQ : IronPort Spam Quarantine
LDAP : Lightweight Directory Access Protocol
MAR : Mailbox Auto Remediation
MFP : Mail Flow Policy
MID : Message ID
MX : Mail Exchange (DNS record)
NTP : Network Time Protocol
PoC : Proof of Concept
PoV : Proof of Value
PXE : PostX Encryption
RAT : Recipient Access Table
REPENG : Reputation Engine
RID : Recipient ID
RES : Registered Envelope Service
SAML : Security Assertion Markup Language
SBG : Security Business Group
SBRS : Sender Base Reputation Service
SDR : Sender Domain Reputation
SLBL : Safe List Block List
SMA : Security Management Appliance
S/MIME : Secure/Multipurpose Internet Mail Extensions
SMTP : Simple Mail Transfer Protocol
SNMP : Simple Network Management Protocol
SOC : Security Operations Center
SPF : Sender Policy Framework
SSL : Secure Sockets Layer

TA : Threat Analyzer
TLS : Transport Layer Security
TME : Technical Marketing Engineer
TOC : Threat Operations Center
UI : User Interface
vESA (ESAv/ESAV) : Virtual Email Security Appliance
vSMA (SMAv/SMAV) : Virtual Security Management Appliance
VOF : Virus Outbreak Filtering
WBRS : Web Base Reputation Service
WSA : Web Security Appliance
XML : Extensible Markup Language
2FA : (2) Two Factor Authentication



A note about best practices



CISCO *Live!*

Throughout the presentation, we will present options to **tune** your rules and settings with-in your environment.

These are meant to be general guidelines.

As each environment is unique, it is recommended that settings be set in **monitor** mode first.

After a determined time, **analyze** the rules, settings, or configuration changes and tune to achieve the desired result.

Why telemetry is important to Cisco

- Telemetry provides Cisco Talos insight on targeted attacks.
- Cisco Systems, Inc. gathers limited data on email from customers to improve the efficacy of our products and services, offers extensive and useful threat detection capabilities which can be coupled with dedicated analysis systems to collect, trend and correlate observed activity.
 - This data is anonymized and used to stop email-based threats.
 - By sharing data with us, helps to analyze what is happening broadly across the threat landscape, providing rich context on threat intelligence classification solution by acting on malicious emails rapidly and meaningfully, and driving protection from new threats such as spam, viruses, and directory harvest attacks.

What is sent to Cisco Talos?

- Using the CLI, there is a hidden command to give more details to Talos - **fullsenderbaseconfig**

```
(Machine esa1.hc3033-47.ipmx.com)> senderbaseconfig

Share limited data with SenderBase Information Service: Enabled

Choose the operation you want to perform:
- SETUP - Configure SenderBase Network Participation settings
- CLUSTERSET - Set how SenderBase is configured in a cluster.
- CLUSTERSHOW - Display how SenderBase is configured in a cluster.
[ ]> fullsenderbaseconfig

Enter SenderBase upload hostname.
[phonehome.senderbase.org]>

Enter SenderBase upload port.
[443]>

Enter the frequency to upload information (in seconds):
[300]>

Exclude per-IP statistics? [N]>

Enter the maximum number of IP addresses to aggregate:
[100000]>

Exclude per-msg statistics? [N]>

Enter the maximum number of Messages to aggregate:
[30000]>

Exclude capacity statistics? [Y]>

Enable verbose logging at the TRACE level? [N]>

Enter the upper limit (in percent, up to two places after decimal point) of messages to be
sampled for improving efficacy:
[1.00]>

Do you wish to configure a custom SenderBase lookup? [N]>

Please enter the mode of SenderBase query.
[norm]>
```

What is sent to Talos?

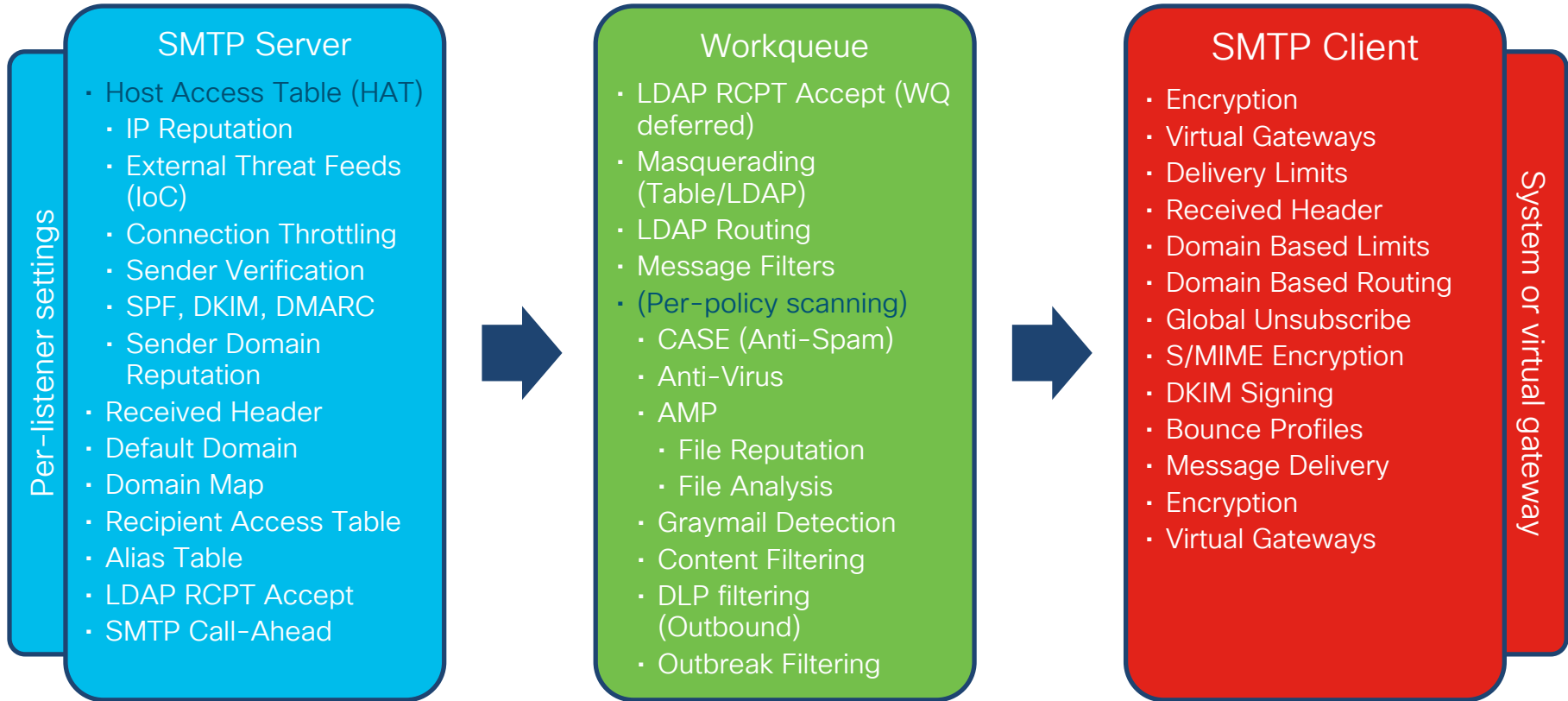
- When enabled, the Context Adaptive Scanning Engine (CASE) is used to collect and report the data (regardless of whether Cisco anti-spam scanning is enabled).
- The data is summarized information on message attributes and information on how different types of messages were handled by Cisco appliances.
- We do not collect the full body of the message.

Item	Sample Data
Message count at various stages within the appliance	Seen by Anti-Virus engine: 100 Seen by Anti-Spam engine: 80
Sum of Anti-Spam and Anti-Virus scores and verdicts	2,000 (sum of anti-spam scores for all messages seen)
Number of messages hitting different Anti-Spam and Anti-Virus rule combinations	100 messages hit rules A and B 50 messages hit rule A only
Number of Connections	20 SMTP Connections
Number of Total and Invalid Recipients	50 total recipients 10 invalid recipients
Hashed Filename(s): (a)	A file <one-way-hash>.pif was found inside an archive attachment called <one-way-hash>.zip.
Obfuscated Filename(s): (b)	A file aaaaaaa0.aaa.pif was found inside a file aaaaaaa.zip.
URL Hostname (c)	There was a link found inside a message to www.domain.com
Obfuscated URL Path (d)	There was a link found inside a message to hostname www.domain.com, and had path aaa000aa/aa00aaa.
Number of Messages by Spam and Virus Scanning Results	10 Spam Positive 10 Spam Negative 5 Spam Suspect 4 Virus Positive 16 Virus Negative 5 Virus Unscannable
Number of messages by different Anti-Spam and Anti-Virus verdicts	500 spam, 300 ham
Count of Messages in Size Ranges	125 in 30K-35K range
Count of different extension types	300 ".exe" attachments
Correlation of attachment types, true file type, and container type	100 attachments that have a ".doc" extension but are actually ".exe" 50 attachments are ".exe" extensions within a zip
Correlation of extension and true file type with attachment size	30 attachments were ".exe" within the 50-55K range
Number of attached files uploaded to the file reputation service (AMP cloud)	1110 files were uploaded to the file reputation service
Verdicts on files uploaded to the file reputation service (AMP cloud)	10 files were found to be malicious 100 files were found to be clean 1000 files were unknown to the reputation service
Reputation score of files uploaded to the file reputation service (AMP cloud)	50 files had a reputation score of 37 50 files had a reputation score of 57 1 file had a reputation score of 61 9 files had a reputation score of 99
Names of files uploaded to the file reputation service (AMP cloud)	example.pdf testfile.doc
Names of malware threats detected by the file reputation service (AMP cloud)	Trojan-Test

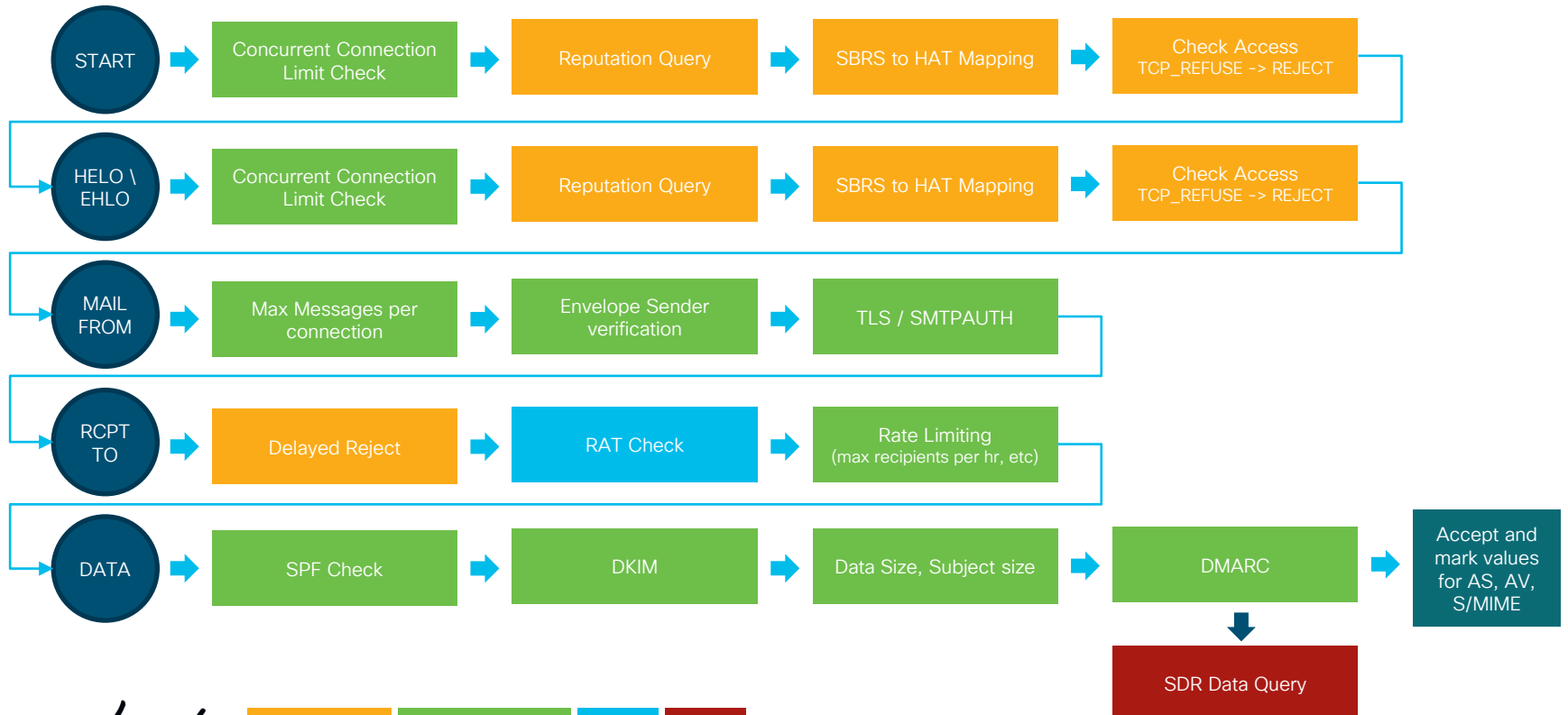


Base Configuration: Connection and Domain Filtering

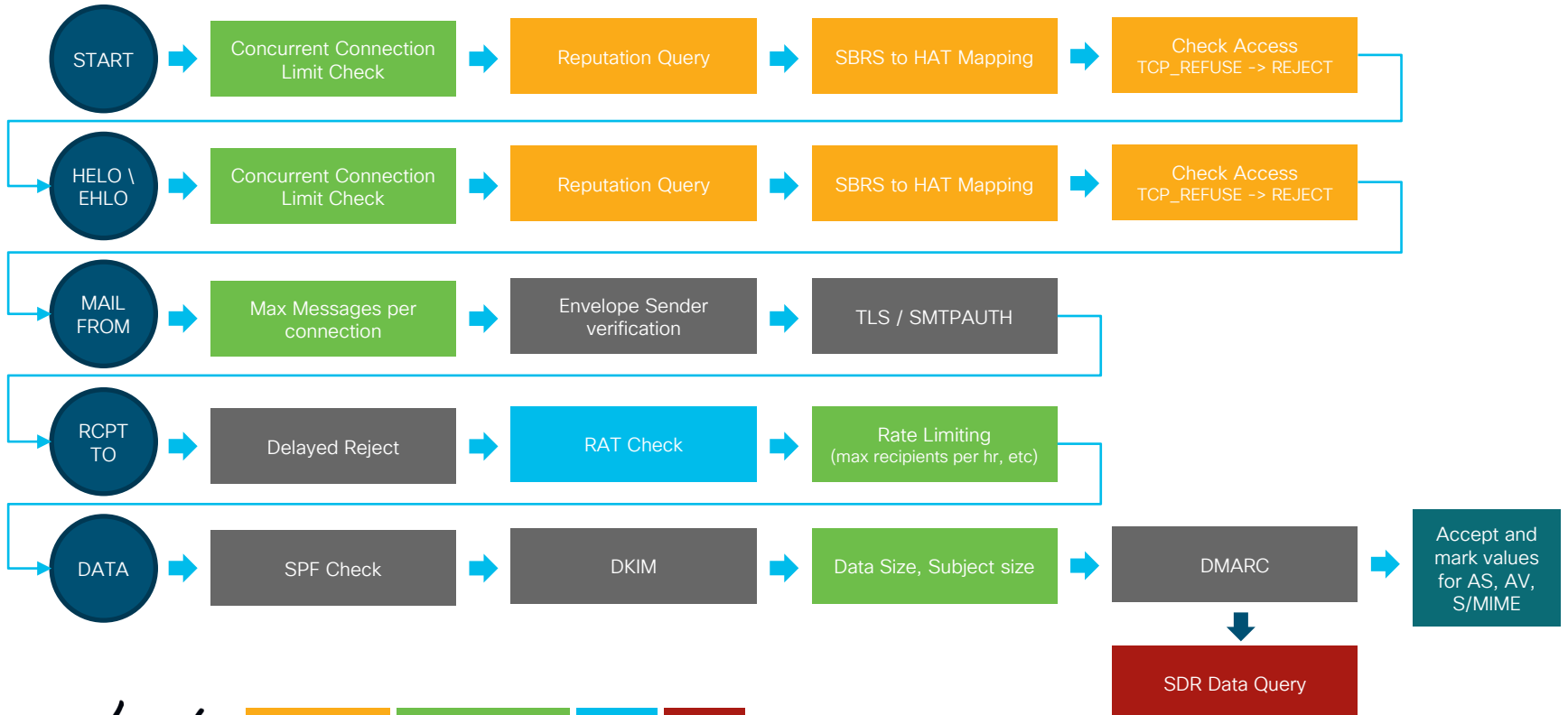
Email pipeline (what happens and where)



Understanding the flow at connection time



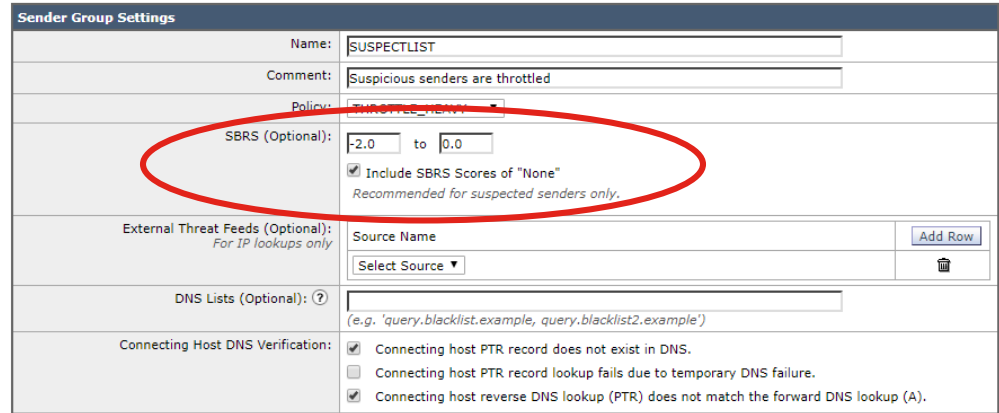
Default flow controls



Sender Group options

SBRS score settings

- SenderBase Reputation Score can be attached to the Sender Groups
- By default, senders with scores of “none” fall in to the “All” Sender Group
- Recommendation is to throttle scores on None



Sender Group Settings	
Name:	SUSPECTLIST
Comment:	Suspicious senders are throttled
Policy:	THROTTLED_SENDER
SBRS (Optional):	-2.0 to 0.0 <input checked="" type="checkbox"/> Include SBRS Scores of "None" <i>Recommended for suspected senders only.</i>
External Threat Feeds (Optional): <i>For IP lookups only</i>	Source Name Select Source <input type="button" value="Add Row"/>
DNS Lists (Optional): ?	<input type="text"/> <i>(e.g. 'query.blacklist.example, query.blacklist2.example')</i>
Connecting Host DNS Verification:	<input checked="" type="checkbox"/> Connecting host PTR record does not exist in DNS. <input type="checkbox"/> Connecting host PTR record lookup fails due to temporary DNS failure. <input checked="" type="checkbox"/> Connecting host reverse DNS lookup (PTR) does not match the forward DNS lookup (A).

```
Info: New SMTP ICID 8 interface Management (10.10.10.90) address 94.46.249.12  
Info: ICID 8 ACCEPT SG SUSPECTLIST match sbrs[-3.0:-1.0] SBRS -2.1
```

Sender Group options

DNS lists, External Threat Feeds (ETF)

- DNS Block Lists (DNSBLs) can be used to include hosts into a specific Sender Group
- Many public DNSBLs are available, however effectiveness is limited as SBRS provides better coverage
- Custom DNSBLs can also be used, but note that entries are cached for 60 mins

The screenshot shows the 'Sender Group Settings' configuration page for a group named 'SUSPECTLIST'. The settings are as follows:

- Name:** SUSPECTLIST
- Comment:** Suspicious senders are throttled
- Policy:** THROTTLE_HEAVY
- SBRS (Optional):** -2.0 to 0.0, with the checkbox 'Include SBRS Scores of "None"' checked. A note below states: 'Recommended for suspected senders only.'
- External Threat Feeds (Optional):** For IP lookups only. It includes a table with one row for 'Source Name' and a 'Select Source' dropdown menu. An 'Add Row' button and a trash icon are also present.
- DNS Lists (Optional):** This field is circled in red. It contains a text input field with a help icon and a placeholder text: '(e.g. 'query.blacklist.example, query.blacklist2.example')'.
- Connecting Host DNS Verification:** Three checkboxes are present:
 - 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).



Let's dive deeper into...
External Threat Feeds (ETF)

External Threat Feeds (ETF)

Why would an Email Administrator use ETF(s)?

Introduced in AsyncOS 12.0 for Email Security, ETF allows an admin to use ETF:

- Pay for a service, such as FS-ISAC, which includes STIX/TAXII feeds directly related to that customer's business.
- SIEM integration runs and provides STIX/TAXII (McAfee, Splunk).
- Open Source, free services (OTX Alien Vault [AT&T], Hailataxii).
- Anyone who wants a "2nd opinion" of IOC(s) that Cisco & Cisco Talos has provided a score, or perhaps that Cisco Talos has not detected and does not have information.

External Threat Feeds (ETF)

Overview

- Structured Threat Information eXpression (STIX)
- Trusted Automated eXchange of Indicator Information (TAXII)

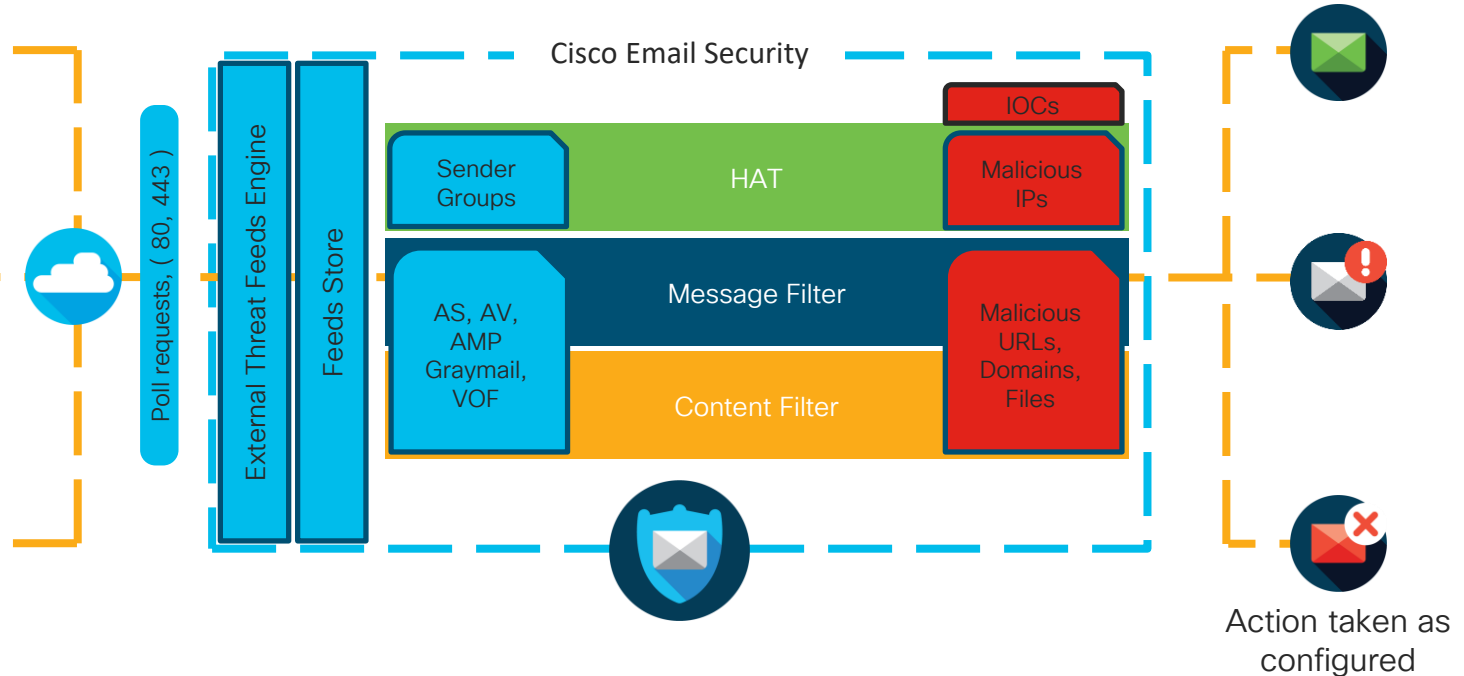
Free/Open Source



PhishTank



Paid \$
Cisco Live!



External Threat Feeds (ETF)

Configuration and usage

- Feed Example: Open Threat Exchange (OTX) Alien Vault
- Indicator of Compromise (IoC): URL
- Service: URL Reputation --> “URL Filtering”
- What would it look like in mail_logs?

```
Mon Oct 14 18:39:32 2019 Info: MID 42261 Threat feeds source 'alienvault' detected malicious
URL: 'http://xmr.btgirl.com.cn' in message body. url-external-threat-feeds-rule
Mon Oct 14 18:39:32 2019 Info: MID 42261 Custom Log Entry: <<<=== EIF_URL_LIST_MATCHED ===>>>
Mon Oct 14 18:39:32 2019 Info: MID 42261 URL http://xmr.btgirl.com.cn has reputation -5.9
matched Condition: URL Reputation Rule
Mon Oct 14 18:39:32 2019 Info: MID 42261 Custom Log Entry: URL_REP
Mon Oct 14 18:39:32 2019 Info: MID 42261 queued for delivery
```

External Threat Feeds (ETF)

Configuration and usage

- Looking at Mail Policies > External Threat Feed Manager... 'alienvault' feed:

Source Details	
Source Name:	<input type="text" value="alienvault"/>
Description (Optional):	<input type="text"/>
TAXII Details	
Hostname: ?	<input type="text" value="otx.alienvault.com"/>
Polling Path: ?	<input type="text" value="/taxii/poll"/>
Collection Name: ?	<input type="text" value="user_AlienVault"/>
Polling interval:	<input type="text" value="0"/> Hours <input type="text" value="15"/> mins <i>(Maximum 24 Hours.)</i>
Age of Threat Feeds: ?	<input type="text" value="365"/> Days <i>(Maximum 365 Days.)</i>
Time Span of Poll Segment ?	<input type="text" value="365"/> Days <i>The maximum time span for a poll segment is the value entered in the 'Age of Threat Feeds' field.</i>
Use HTTPS:	<input checked="" type="radio"/> Yes <input type="radio"/> No Polling Port: ? <input type="text" value="443"/>
Configure User Credentials:	<input checked="" type="radio"/> Yes <input type="radio"/> No <input checked="" type="radio"/> Basic Authentication Username: <input type="text" value="robsherw"/> Password: <input type="password" value="....."/>
Proxy Details	
Use Global Proxy:	<input type="radio"/> Yes <input checked="" type="radio"/> No <i>To configure Proxy Server, go to: Security Services > Security Updates</i>

External Threat Feeds (ETF)

Configuration and usage

- How does the ESA act? Looking at the 'CF ETF_URL' content filter:

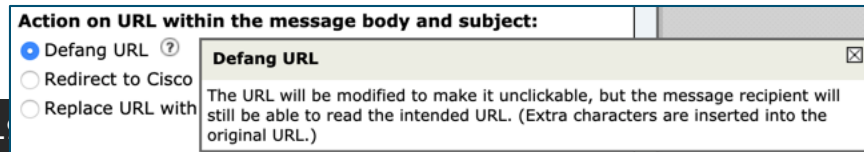
Conditions			
Add Condition...			
Order	Condition	Rule	Delete
1	URL Reputation	url-external-threat-feeds (['SRC_CyberCrime', 'SRC_HATaxii', 'alienvault', 'hailataxii', 'hailataxii_phishtank'], "", 1, 1)	

Actions			
Add Action...			
Order	Action	Rule	Delete
1	Add Log Entry	log-entry("<<<=== ETF_URL_LIST_MATCHED ===>>")	

External Threat Feeds (ETF)

Configuration and usage

- If we did not have any previous/additional URL Filtering content filter in place, we *could* have added action to 'defang' any URL detected by our 'alienvault' feed...



```
Mon Oct 14 19:14:59 2019 Info: MID 42265 Threat feeds source 'alienvault' detected malicious
URL: 'http://xmr.btgirl.com.cn' in message body. url-external-threat-feeds-rule
Mon Oct 14 19:14:59 2019 Info: MID 42265 Custom Log Entry: <<<=== ETF URL LIST MATCHED ===>>>
Mon Oct 14 19:14:59 2019 Info: MID 42265 Threat feeds source 'alienvault' detected malicious
URL: 'http://xmr.btgirl.com.cn' in message body. Action: URL defanged
Mon Oct 14 19:14:59 2019 Info: MID 42265 rewritten to MID 42266 by url-ETF-defang-action filter
'CF ETF URL'
Mon Oct 14 19:14:59 2019 Info: Message finished MID 42265 done
Mon Oct 14 19:14:59 2019 Info: MID 42266 URL http://xmr.btgirl.com.cn has reputation -5.9
matched Condition: URL Reputation Rule
Mon Oct 14 19:14:59 2019 Info: MID 42266 Custom Log Entry: URL_REP
Mon Oct 14 19:14:59 2019 Info: MID 42266 queued for delivery
```

External Threat Feeds (ETF)

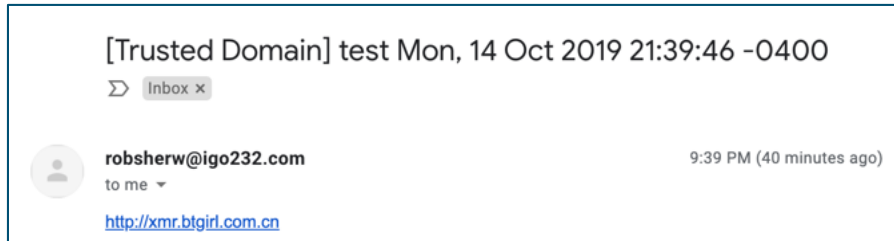
Configuration and usage

- Final result:



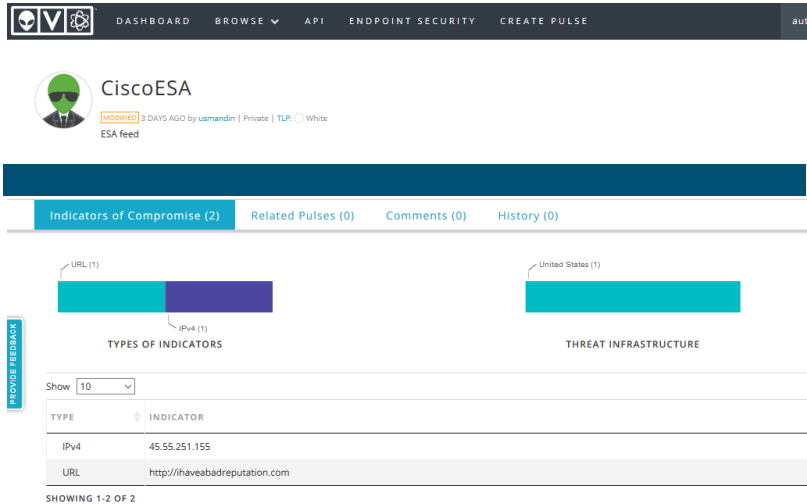
Defanged URL!

- Versus:



External Threat Feeds (ETF)

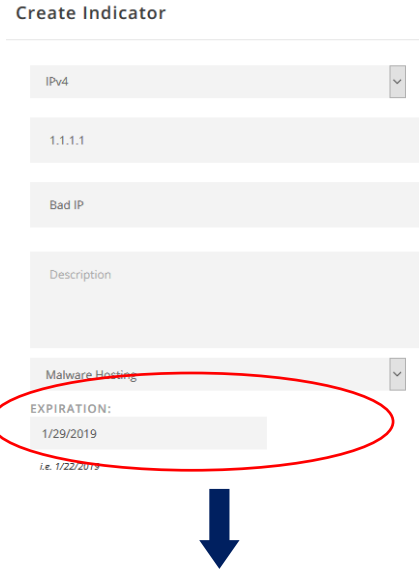
Configuration and usage, HAT automation



The screenshot shows the Cisco ESA dashboard. At the top, there's a navigation bar with 'DASHBOARD', 'BROWSE', 'API', 'ENDPOINT SECURITY', and 'CREATE PULSE'. Below that, the user profile for 'CiscoESA' is visible, along with a 'MOORED 3 DAYS AGO by usmandin' status and 'Private | TLP: White' settings. The main content area has tabs for 'Indicators of Compromise (2)', 'Related Pulses (0)', 'Comments (0)', and 'History (0)'. There are two charts: 'TYPES OF INDICATORS' showing 'URL (1)' and 'IPv4 (1)', and 'THREAT INFRASTRUCTURE' showing 'United States (1)'. A table below shows a list of indicators:

TYPE	INDICATOR
IPv4	45.55.251.155
URL	http://ihaveabadreputation.com

SHOWING 1-2 OF 2



The screenshot shows the 'Create Indicator' form. It has several input fields: 'IPv4' (dropdown), '1.1.1.1', 'Bad IP', 'Description', 'Malware Hosting' (dropdown), and 'EXPIRATION: 1/29/2019'. A red circle highlights the 'EXPIRATION' field, and a blue arrow points down from it.



```
Fri Dec 21 11:19:54 2018 Info: New SMTP ICID 5451 interface Data 1 (216.71.134.24) address 45.55.251.155 reverse
dns host mailbot1.teamnorthwind.com verified yes
Fri Dec 21 11:19:54 2018 Info: ICID 5451 REJECT SG BLOCKED match etf-source: OTX SBRS None country None
Fri Dec 21 11:19:54 2018 Info: ICID 5451 close
```




Now you have seen ETF.
Back to the connection and domain
filtering...

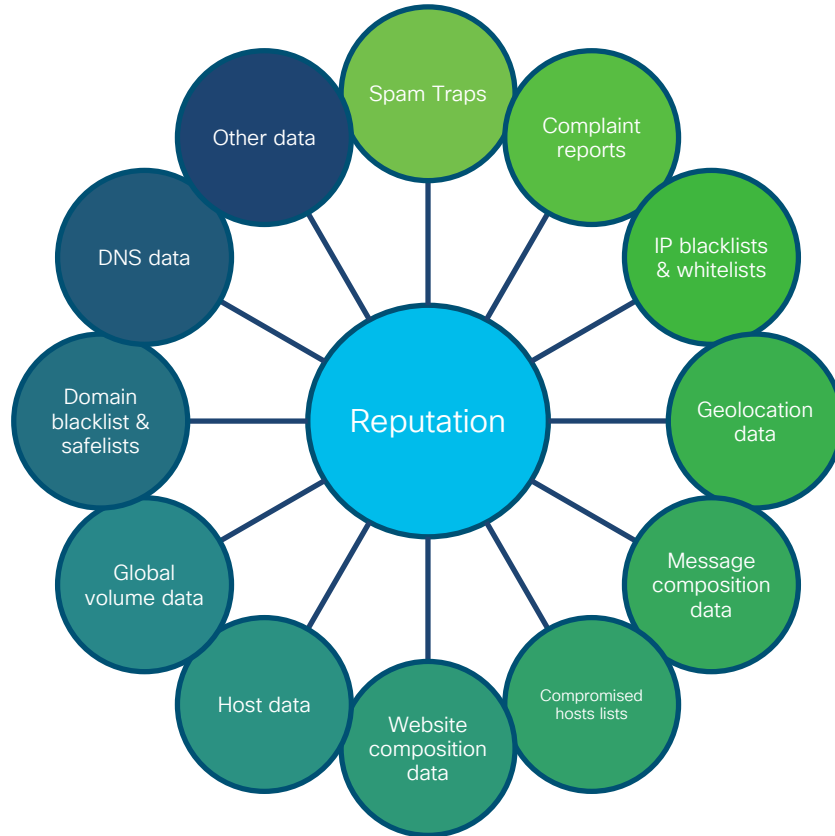
Sender Group options

DNS Settings

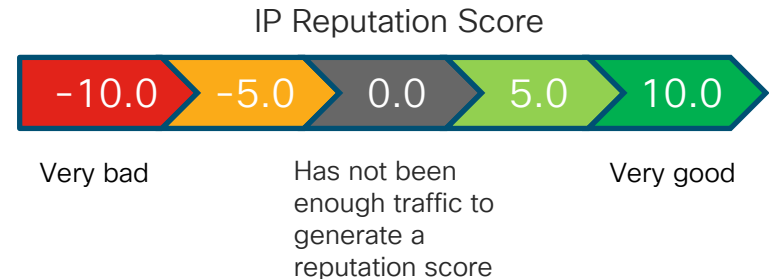
- Is there a Reverse DNS record?
- Is there a DNS failure (temp)?
- Do the A and reverse match?
- At a minimum, select PTR does not exist and A/REV mismatch to fall into suspect senders

DNS Lists (Optional): ?	<input type="text"/> <i>(e.g. 'query.blacklist.example, query.blacklist2.example')</i>
Connecting Host DNS Verification:	<input type="checkbox"/> Connecting host PTR record does not exist in DNS. <input type="checkbox"/> Connecting host PTR record lookup fails due to temporary DNS failure. <input type="checkbox"/> 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.



Customizing the Host Access Table (HAT)

Default Settings: Moderate Blocking

Order	Sender Group	SenderBase™ Reputation Score (?)											Mail Flow Policy	
		-10	-8	-6	-4	-2	0	2	4	6	8	+10		
1	RELAYLIST													RELAYED
2	WHITELIST													TRUSTED
3	BLACKLIST													BLOCKED
4	SUSPECTLIST													THROTTLED
5	UNKNOWNLIST													ACCEPTED
	ALL													ACCEPTED

Incoming Mail Summary		
Message Category	%	Messages
Stopped by Reputation Filtering	98.6%	756
Stopped as Invalid Recipients	1.4%	11

Custom Settings: Aggressive Throttling

Order	Sender Group	SenderBase™ Reputation Score (?)											Mail Flow Policy	
		-10	-8	-6	-4	-2	0	2	4	6	8	+10		
1	RELAYLIST													RELAYED
2	WHITELIST													TRUSTED
3	BLACKLIST													BLOCKED
4	SUSPECTLIST													HEAVY_THROTTLE
5	GREYLIST													LIGHT_THROTTLE
6	UNKNOWNLIST													ACCEPTED
	ALL													ACCEPTED

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

Filtering non-business critical mail

Host Options

Sender Group: WEBMAIL_PROVIDERS - IncomingMail 216.71.129.13:25

Sender Group Settings	
Name:	WEBMAIL_PROVIDERS
Order:	8
Comment:	None
Policy:	THROTTLED
SBRS (Optional):	Not in use
DNS Lists (Optional):	None
Connecting Host DNS Verification:	None Included

<< Back to HAT Overview Edit Settings...

Find Senders

Find Senders that Contain this Text: Find

Sender List: Display All Items in List Items per page 20 ▼

Add Sender... Clear All Entries

Sender	Comment	All Delete
.aol.com	None	<input type="checkbox"/>
.yahoo.com	None	<input type="checkbox"/>
.hotmail.com	None	<input type="checkbox"/>
.google.com	None	<input type="checkbox"/>

<< Back to HAT Overview Delete

- By explicitly adding hosts and IPs to a Sender Group, we can force desired connection behavior.
- The idea here is to limit the attack surface by throttling or blocking noncritical emails.
- Inputs:
 - IP (Range, Subnet, exact)
 - Host (Partial / wildcard)

Filtering non-business critical mail

Geo Filtering

Sender Group: HIGH_RISK_REGION - IncomingMail 216.71.129.13:25

Sender Group Settings	
Name:	HIGH_RISK_REGION
Order:	4
Comment:	None
Policy:	BLOCKED
SBRS (Optional):	Not in use
DNS Lists (Optional):	None
Connecting Host DNS Verification:	None Included

<< Back to HAT Overview Edit Settings...

Find Senders

Find Senders that Contain this Text: (?) Find

Sender List: Display All Items in List		Items per page 20 ▾
Add Sender...		
Sender	Comment	All <input type="checkbox"/>
Canada [ca]	Blame Canada	Delete <input type="checkbox"/>

<< Back to HAT Overview Delete

- Country detection is based on the **connecting** host.
- Country is returned as part of the SBRS query.
- The idea here is to limit the attack surface by throttling or blocking noncritical emails.

```
Info: New SMTP ICID 4246 interface Data 1 (216.71.134.24) address 68.183.144.44 reverse dns host...
Info: ICID 4246 REJECT SG BLOCKED match country[ca] SBRS None country Canada
Info: ICID 4246 close
```

Reputation

DNS and caching

- DNS is the most critical external service for the ESA.
- By default there are 4 DNS lookups per connection:
 - Reverse DNS, 2 SBRS lookups and ASN Number (informational)
- With SPF, DKIM & 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.

```
Tue Dec 19 07:34:05 2017 Info: ICID 394968647 ACCEPT SG SUSPECTLIST match sbrs[none] SBRS unable to retrieve
```

```
Tue Dec 19 07:34:05 2017 Warning: Received an invalid DNS Response: rcode=ServFail  
data="'ev\\x81\\x82\\x00\\x01\\x00\\x00\\x00\\x00\\x00\\x00\\x01m\\x02ag\\x00\\x00\\x01\\x00\\x01'"
```

Mail Flow policies

Host Throttling

- By default the only MFP that has any Host limiting is the **Throttle** policy.
- By default, there are no **Max Recipients Per Hour** Limits set on the ESA.
- It is recommended to set a low threshold (under 100) in suspect ranges.

Rate Limit for Hosts:	Max. Recipients Per Hour:	<input checked="" type="radio"/> Use Default (Unlimited) <input type="radio"/> Unlimited <input type="radio"/> <input type="text"/>
	Max. Recipients Per Hour Code:	<input checked="" type="radio"/> Use Default (452) <input type="radio"/> <input type="text"/>
	Max. Recipients Per Hour Text:	<input checked="" type="radio"/> Use Default (Too many recipients received this hour) <input type="radio"/> <input type="text"/>

Mail Flow policies

Envelope Sender Throttling

- By default, there are no Envelope Sender Limits set on the ESA.
- It is recommended to implement Sender Limits based on the **High-Volume Mail** report. (see: **Monitor > High Volume Mail**)

▼ Rate Limit for Envelope Senders:	Max. Recipients Per Time Interval:	<input checked="" type="radio"/> Use Default (Unlimited) <input type="radio"/> Unlimited <input type="radio"/> <input type="text" value="100"/> Recipients per 60 Minutes. <i>Number of recipients between 1 and 1,000,000 per number of minutes between 5 and 1440</i>
	Sender Rate Limit Error Code:	<input checked="" type="radio"/> Use Default (452) <input type="radio"/> <input type="text" value="452"/>
	Sender Rate Limit Error Text:	<input checked="" type="radio"/> Use Default (Too many recipients received from the sender) <input type="radio"/> <input type="text" value="Too many recipients received from the sender"/>
	Exceptions:	<input checked="" type="radio"/> Use Default (Ignore Rate Limit for Address List: RateLimit_Bypass) <input type="radio"/> Ignore Rate Limit for Address List: <input type="text" value="None"/>

Mail Flow policies

Flow Control

- Flow controls will use SBRS to group similar IP ranges to apply connection limits against networks if Cisco Talos sees a pattern.
- If turned off, you can select the range to enforce limits.
 - For example, a /32 would mean that each IP would have its own throttle limit.

Flow Control:	Use SenderBase for Flow Control:	<input checked="" type="radio"/> Use Default (On) <input type="radio"/> On <input type="radio"/> Off
	Group by Similarity of IP Addresses:	<i>This Feature can only be used if Senderbase Flow Control is off.</i>
		<input checked="" type="radio"/> Off
		<input type="radio"/> <input type="text" value=""/>
		(significant bits 0-32)

Mail Flow 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 conversation.
- Recommendation is set a low max threshold at suspect / throttle levels (5 to 10 max).

Directory Harvest Attack Prevention (DHAP):	Max. Invalid Recipients Per Hour:	<input checked="" type="radio"/> Use Default (25) <input type="radio"/> Unlimited <input type="radio"/> <input type="text" value="25"/>
	Drop Connection if DHAP threshold is Reached within an SMTP Conversation:	<input checked="" type="radio"/> Use Default (On) <input type="radio"/> On <input type="radio"/> Off
	Max. Invalid Recipients Per Hour Code:	<input checked="" type="radio"/> Use Default (550) <input type="radio"/> <input type="text" value="550"/>
	Max. Invalid Recipients Per Hour Text:	<input checked="" type="radio"/> Use Default (Too many invalid recipients) <input type="radio"/> <input type="text"/>

Mail Flow policies

Security settings continued

- By default, TLS Settings are not on for incoming or outbound mail.
- Three levels of checking: Off, Preferred, Required
 - Set **Preferred** on the default mail flow policy.
- **Mandatory** can be set up as a list or as its own Sender Group.

Encryption and Authentication:	TLS:	<input checked="" type="radio"/> Use Default (Preferred) <input type="radio"/> Off <input type="radio"/> Preferred <input type="radio"/> Required
		<input type="checkbox"/> TLS is Mandatory for Address List (TLS_Enforced) <input type="checkbox"/> Verify Client Certificate
	SMTP Authentication:	<input checked="" type="radio"/> Use Default (Off) <input type="radio"/> Off <input type="radio"/> Preferred <input type="radio"/> Required
	If Both TLS and SMTP Authentication are enabled:	<input type="checkbox"/> Require TLS To Offer SMTP Authentication

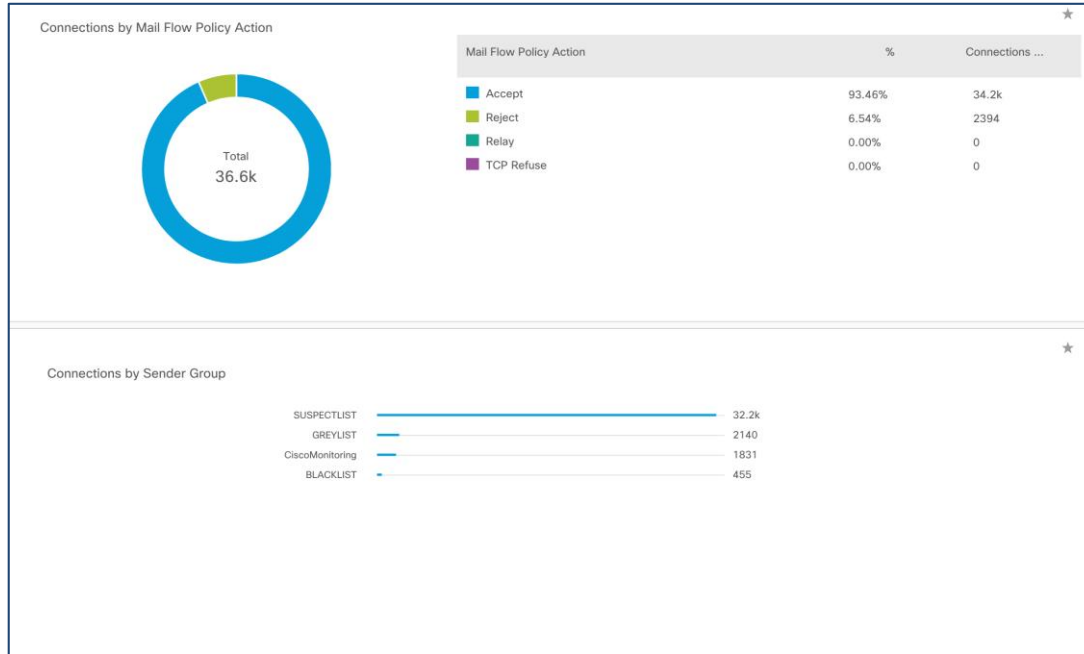
Mail Flow policies

Sender Validation

- Sender Validation is enabled only on the suspect Sender Group.
- These are potent settings to detect spoofing attempts or invalid domains.
- A recommendation is to use these settings (cautiously) to block invalid senders to own domain spoofing.

Envelope Sender DNS Verification:	<input checked="" type="radio"/> On <input type="radio"/> Off
Malformed Envelope Senders:	
SMTP Code:	<input type="text" value="553"/>
SMTP Text:	<input type="text" value="#5.5.4 Domain required for sender address"/>
Envelope Senders whose domain does not resolve:	
SMTP Code:	<input type="text" value="451"/>
SMTP Text:	<input type="text" value="#4.1.8 Domain of sender address <\${EnvelopeSend}"/>
Envelope Senders whose domain does not exist:	
SMTP Code:	<input type="text" value="553"/>
SMTP Text:	<input type="text" value="#5.1.8 Domain of sender address <\${EnvelopeSend}"/>
Use Sender Verification Exception Table:	<input checked="" type="radio"/> On <input type="radio"/> Off

Reporting on Connections



- Connections are a significant consumer of resources on the appliance.
- A poorly configured policy could allow a single host to consume all available connections.
- An ESA can handle between 300-500 connections globally.
- Configure policies and tarpits to ensure no one host takes up too many connections.



Let's dive deeper into...
Sender Domain Reputation (SDR)

Sender Domain Reputation (SDR)

- Traditionally, Cisco Email Security filters mail based on the sending domain's IP reputation by querying SenderBase for the sending domain's SBRS.
- The efficacy of IP reputation would gradually decrease because of various reasons, some listed below:
 - A single IP could be used to host multiple domains, in which case the nature of each domain may be different.
 - With increased penetration of IPv6 addresses, the IP reputation would be less effective.
 - To bypass reputation checks, attackers would prefer to switch IPs, which are not visible to an end-user, then switch domains.

Sender Domain Reputation (SDR)

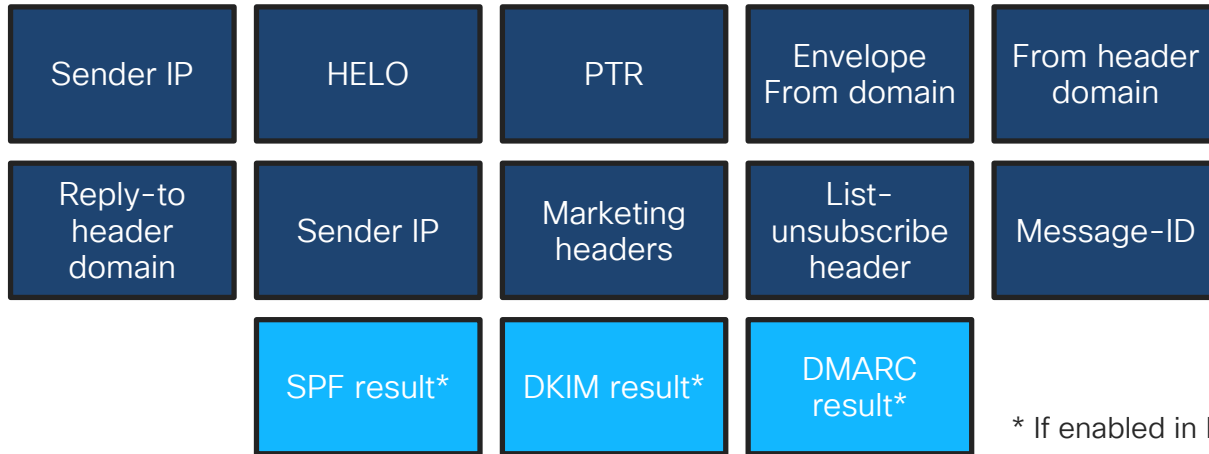
What is SDR?

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

Sender Domain Reputation (SDR)

What is sent to Talos with SDR?

- Starting with AsyncOS 12.0 for Email Security, SDR is enabled by default and the following information is used to help determine verdicts
- For each incoming message, an SDR query is performed and the reputation of the message is retrieved via HTTPs POST request to the SDR service



* If enabled in Mail Flow Policies

Sender Domain Reputation (SDR)

Enable SDR or review SDR service configuration

- SDR is enabled globally and turned on by default when you upgrade to 12.0.
- The default query includes IP, envelope header, and HELO information.

1

Security Services | Network

Domain Reputation Filtering

Domain Reputation

Sender Domain Reputation Overview

Enable Sender Domain Reputation Filtering

Include Additional Attributes: ? **Enable**

Sender Domain Reputation Query Timeout: ? 5 seconds

Match Domain Exception List based on Domain in Envelope From: ? **Enable**

2

Sender Domain Reputation Overview

Sender Domain Reputation:	Enabled
Include Additional Attributes: ?	Enabled
Sender Domain Reputation Query Timeout: ?	5 seconds
Match Domain Exception List based on Domain in Envelope From: ?	Enabled

[Edit Global Settings...](#)

3

Domain Exception List

Domain Exception List: ?	None
--------------------------	------

[Edit Settings...](#)

Sender Domain Reputation (SDR)

Improving SDR efficacy

Domain Reputation

Sender Domain Reputation Overview

Enable Sender Domain Reputation Filtering

Include Additional Attributes

SDR uses headers such as 'Envelope-From:', 'From:' and 'Reply-to:' to determine the reputation of the message. In addition, it also uses the results of the email authentication mechanisms such as SPF, DKIM, and DMARC to decide the reputation. If you enable this option, the following additional attributes of the message are included in the Sender Domain Reputation check to improve the efficacy:

- Username part of the email address present in the 'Envelope-From:', 'From:' and 'Reply-To:' headers.
- Display name in the 'From:' and 'Reply-To:' headers.

Additional Attributes: Enable

Reputation Query Timeout: seconds

Display Name in Envelope From: Enable

Cancel

Copyright © 2003-2020

- You may configure additional attributes to be sent during the data phase to help increase the telemetry to SDR.

```
"headerFrom": [ {  
  "addr": "boa-support@example.com",  
  "friendly": "Bank of America Support"  
} ],  
"headerReplyto": [  
  {  
    "addr": "john@example.com",  
    "friendly": "Bank of America Support"  
  },  
  {  
    "addr": "jane@example.com",  
    "friendly": "Bank of America Support"  
  } ]
```

Sender Domain Reputation (SDR)

SDR Verdicts

- Evaluate domain information of Envelope Sender, From and Reply-to.
- 7 reputation verdicts possible to action on inside a content filter or based on age:

Reputation	Action	Description
Awful	Block	Always Block domains with this reputation
Poor	Block	Recommend blocking level
Tainted	Block	Block with False Positives
Weak	Throttle/Quarantine	Weak reputation, throttle or quarantine
Unknown	Throttle/Delay	Unknown Sender
Neutral	None	Neutral (fair) reputation
Good	None	Good Reputation

Sender Domain Reputation (SDR)

Configuring SDR Actions

Add Condition

Message Body or Attachment
Message Body
URL Category
URL Reputation
Message Size
Message Language
Macro Detection
Attachment Content
Attachment File Info
Attachment Protection
Subject Header
Other Header
Envelope Sender
Envelope Recipient
Receiving Listener
Remote IP/Hostname
Reputation Score
Domain Reputation
DKIM Authentication
Forged Email Detection
SPF Verification
S/MIME Gateway Message
S/MIME Gateway Verified
Duplicate Boundaries Verification
Geolocation

Domain Reputation Help

Does the sender domain match any one of the specified criteria?

Sender Domain Reputation

Sender Domain Reputation Verdict

Verdict: **Awful to Good**

Awful Poor Tainted Weak Unknown Neutral Good

Sender Domain Age

Sender Domain Reputation Unscannable

External Threat Feeds

Use a Domain Exception list: ?

- Although SDR queries during the connection level, actions are configured at the filter level.
- Message Filters and Content Filters can use either the domain age or reputation to take an action.

Domain Reputation Help

Does the sender domain match any one of the specified criteria?

Sender Domain Reputation

Sender Domain Reputation Verdict

Sender Domain Age

Sender Domain Reputation Unscannable ?

External Threat Feeds

This option is not available because no threat feed source is configured. To create one, go to Mail Policies > External Threat Feeds Manager.

Use a Domain Exception list: ?

Sender Domain Reputation (SDR)

SDR in logs and message tracking

- Evaluates domains in the envelope-from, from, and reply-to headers.
- Displays the “worst” verdict, along with domain age.
- Verdicts and domain age can be used in a filter.

21:06:12 (GMT -05:00) ● Start message 3723073 on incoming connection (ICID 1964604).

21:06:12 (GMT -05:00) ● Message 3723073 enqueued on incoming connection (ICID 1964604) from user@gmail.com.

21:06:12 (GMT -05:00) ● Message 3723073 direction: incoming

21:06:12 (GMT -05:00) ● Message 3723073 on incoming connection (ICID 1964604) added recipient (usman@encoresol.com).

21:06:12 (GMT -05:00) ● Message 3723073 scanned by engine SPF Verdict Cache using cached verdict.

21:06:12 (GMT -05:00) ● Message 3723073 SPF: helo identity postmaster@urlrewrt.com None ← Sending domain identified by SPF

21:06:12 (GMT -05:00) ● Message 3723073 scanned by engine SPF Verdict Cache using cached verdict.

21:06:12 (GMT -05:00) ● Message 3723073 SPF: mailfrom identity user@gmail.com SoftFail ← Spoofed address

21:06:12 (GMT -05:00) ● Message 3723073 does not contain DKIM signature.

21:06:12 (GMT -05:00) ● Message 3723073 scanned by engine SPF Verdict Cache using cached verdict.

21:06:12 (GMT -05:00) ● Message 3723073 SPF: pra identity user@gmail.com None headers from

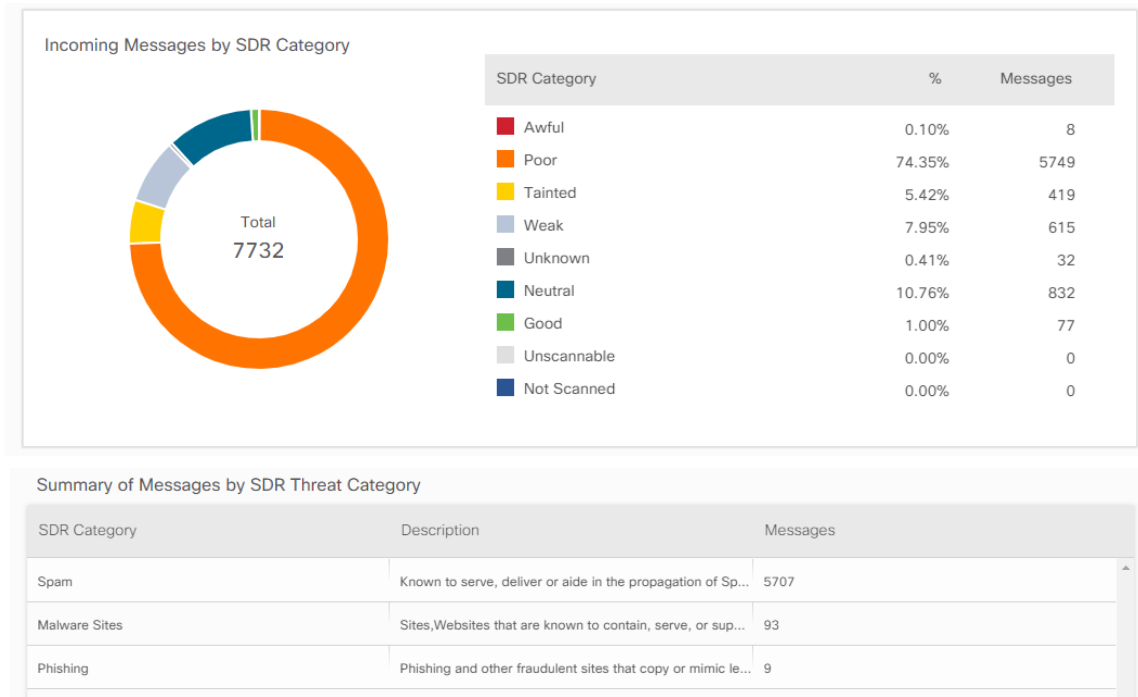
21:06:12 (GMT -05:00) ● Message 3723073: DMARC verification failed. No action taken on the message.

21:06:12 (GMT -05:00) ● Message 3723073 contains message ID header '<201811130206.wAD26AWS026160@urlrewrt.com>'.
21:06:12 (GMT -05:00) ● Message 3723073 Domain Reputation: Poor, Domain Age: 1 year 26 days, Threat Category: Spam ← Verdict and Age

Sender Domain Reputation (SDR)

SDR Reporting

- Two (2) reporting widgets available for SDR:
 1. Breakdown of SDR categories
 2. Breakdown of Threat Category:
 - Spam
 - Malware Sites
 - Phishing
 - Botnets
 - Domain Generated Algorithms
 - Newly Seen Domains



Sender Domain Reputation (SDR)

SDR Exceptions (bypass)

- Full email addresses, IP addresses, and domains may be excluded from SDR checks.
- Create an 'Address List' and specify the email address(es), IP(s), or domain(s) to be excluded.
- If an Address List is configured to be excluded for SDR, the configured email, IP or domain will NOT be got through SDR checks provided:
 - Email authentication checks, such as SPF, DKIM, DMARC pass.
 - When authentication checks are NOT enabled, the domains in the mail-from, friendly-from and reply-to headers MUST match.

Sender Domain Reputation (SDR)

Exception Configuration

Add Address List

New Address List Details

Address List Name:

Description:

List Type:

- Full Email Addresses only
- Domains only
- IP Addresses only
- All of the above

Addresses: e.g.: user@example.com, user@.example.com, @[1.2.3.4], @.example.com

1

Domain Exception List

Domain Exception List: **2**

[Edit Settings...](#)

Edit Domain Exception List

Domain Exception List

Domain Exception List:

The Domain Exception list shows address lists that can contain domains only.
To create a domain exception list, go to Mail Policies > Address Lists

3

Steps to create an exception:

1. Create an address list.
2. Apply to Domain Reputation Global settings.
3. (or) Apply per filter settings.

Domain Reputation

[Help](#)

Does the sender domain match any one of the specified criteria?

- Sender Domain Reputation
 - Sender Domain Reputation Verdict

Verdict: **Awful to Good**



- Sender Domain Age
- Sender Domain Reputation Unscannable
- External Threat Feeds

Use a Domain Exception list:

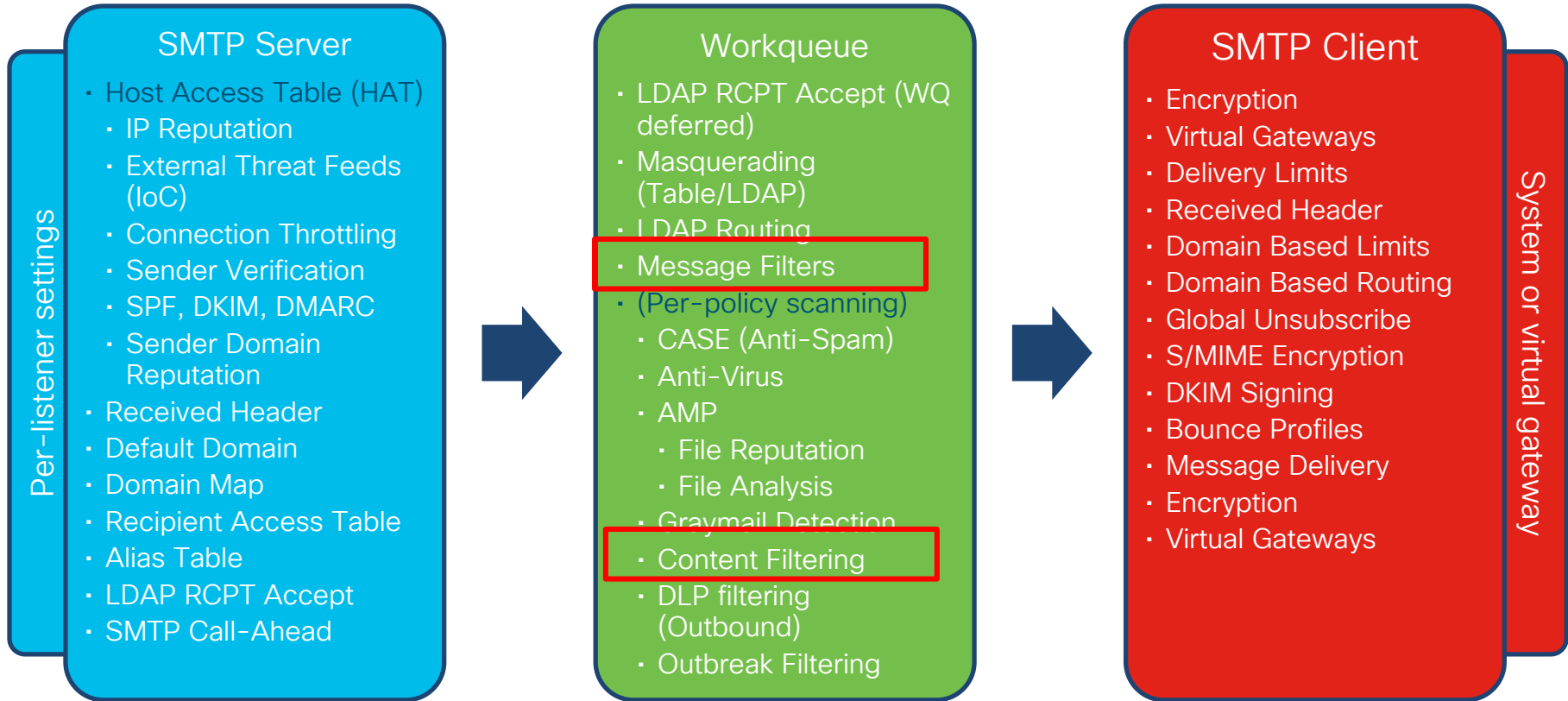


And that is a brief look into SDR!



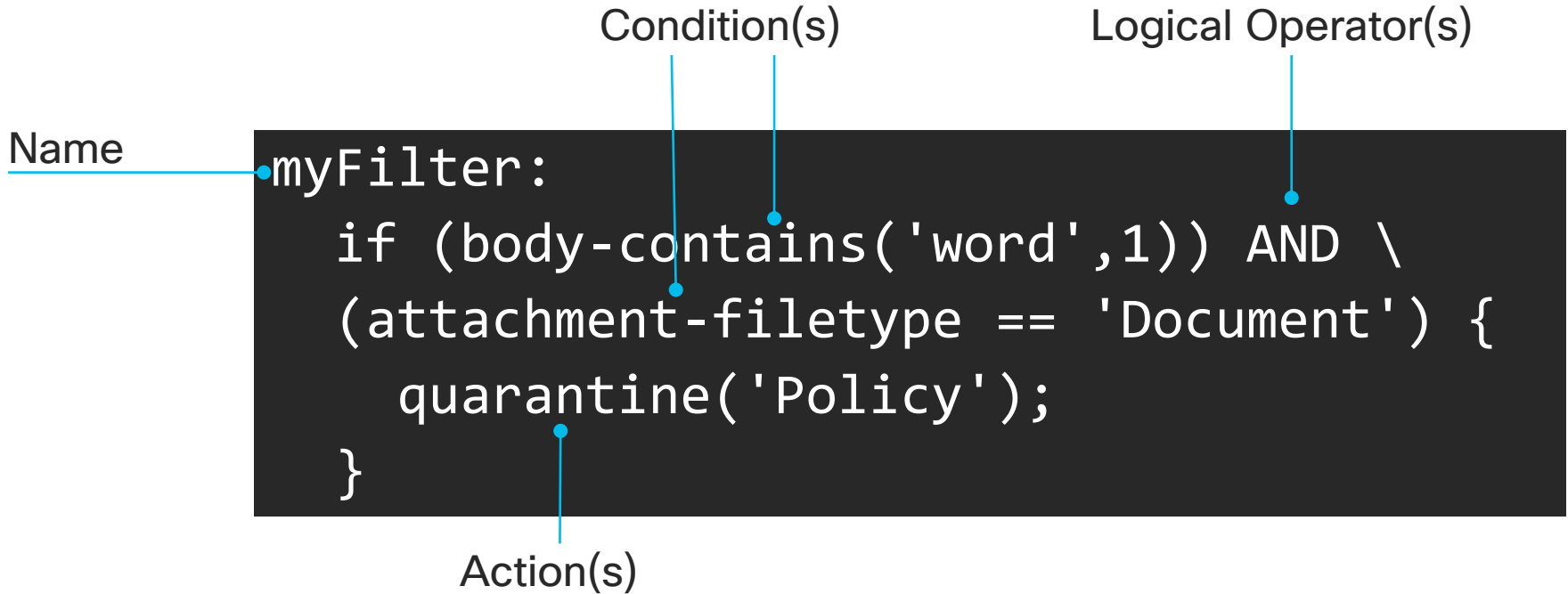
Base Configuration: Pre-policy filtering and Per-policy scanning

Message Filters & Content Filters



Message Filter

Syntax



Message Filter

Conditions and Actions

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!

Actions

- 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 actions is executed

Message Filters

Exclusive conditions to Message Filters

- `sendergroup()`
- `recv-int()`
- `random()`
- `rcpt-count()`
- `addr-count()`
- `attachment_size()`
- `every-attachment-contains()`
- `attachment-binary-contains()`
- `workqueue-count()`
- `dnslist()`
- `smtp-auth-id-matches()`
- `valid()`
- `signed()`
- `header-repeats()`

Message Filters

Better inspection of SPF status

- `spf-status()` with Message Filters allows to check separate posture for
 - HELO SPF identity - `spf-status("helo")`
 - MAIL FROM identity - `spf-status("mailfrom")`
 - PRA identity - `spf-status("pra")`
- `spf-passed()` - faster than `spf-status`, but less granular

- Naturally, multiple “and” and “or” conditions make rule creation much more flexible

Message Filters

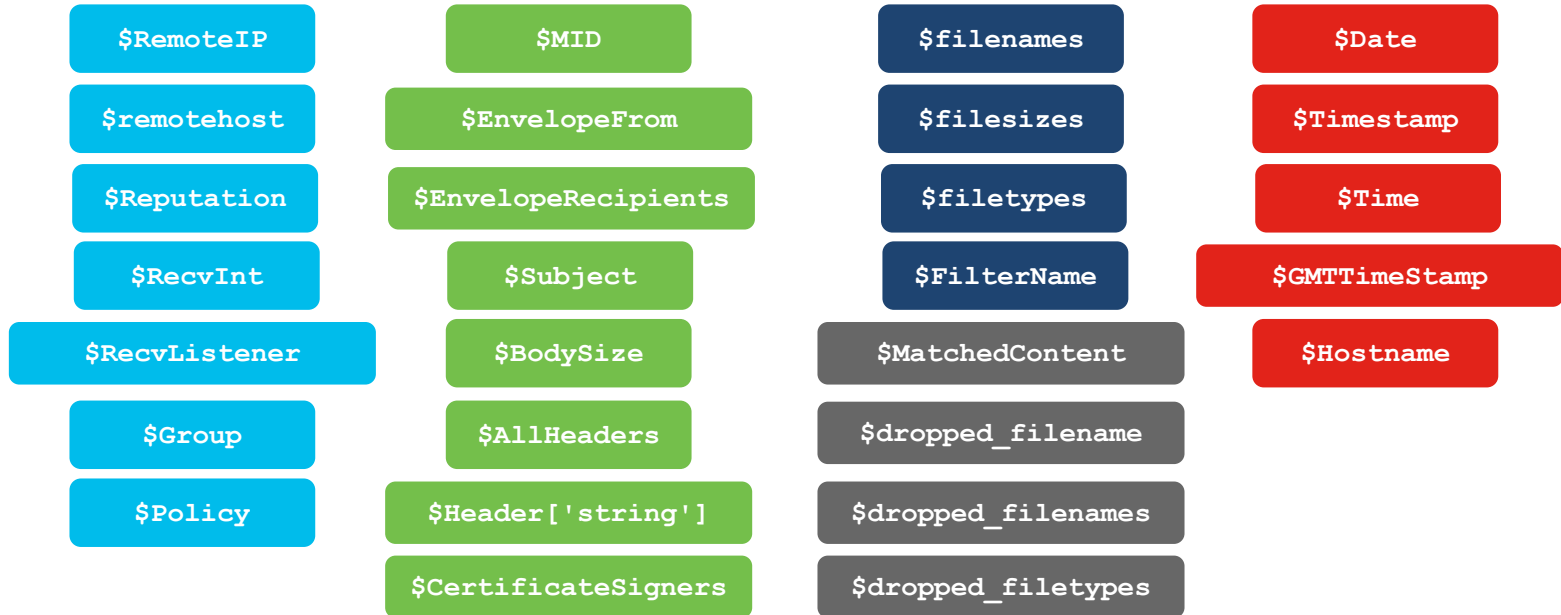
Exclusive actions to Message Filters

- `no-op()`
- `archive()`
- `bcc()`
- `edit-body-text()`
- `html-convert()`
- `bounce-profile()`
- `skip-spamcheck()`
- `skip-marketingcheck()`
- `skip-socialcheck()`
- `skip-bulkcheck()`
- `skip-viruscheck()`
- `skip-ampcheck()`
- `skip-vofcheck()`

Message Filters

Action Variables

- Can be used in `bcc()`, `bcc-scan()`, `notify()`, `notify-copy()`, `add-footer()`, `add-heading()`, `log-entry()`, `insert-header()` and `edit-header-text()`



Message Filters

Example: Adding Informational X-headers

- Use a message filter to stamp X-header that leverages action variables.
- Message Filters may be used to help troubleshoot issues on messages in the user's inbox.
- Can also be used to trigger content filters later in the pipeline.

```
addHeaders: if (sendergroup != "RELAYLIST")
{
    insert-header("X-IronPort-RemoteIP", "$RemoteIP");
    insert-header("X-IronPort-MID", "$MID");
    insert-header("X-IronPort-Reputation", "$Reputation");
    insert-header("X-IronPort-Listener", "$RecvListener");
    insert-header("X-IronPort-SenderGroup", "$Group");
    insert-header("X-IronPort-MailFlowPolicy", "$Policy");
}
```

AND, OR, IF, ELSE and nesting

```
andTestFilter: if (remote-ip == "192.168.100.100" AND rcpt-to-group == "GROUP") { ... }
```

- Because the least expensive test is performed first, switching the order of the items in the test will have no effect. If you want to guarantee the order in which tests are performed, use nested if statements. This is also the best way to ensure that an expensive test is avoided whenever possible:

```
expensiveAvoid: if (<simple tests>) { if (<expensive test>) { <action> } }
```

- Or, a little more complicated:

```
if (test1 AND test2 AND test3) { ... }
```

```
if ((test1 AND test2) AND test3) { ... }
```

Message Filters

Regex vs Dictionaries

```
spooof_filter:
  if (((recv-listener == "InboundMail") AND
      (sendergroup != "SPOOF_ALLOW")) AND
      ((mail-from == "(?i)@elpaso\.com|@epenergy\.com|@elink\.elpaso\.com|
@epglobalnetworks\.com|@epmidstream\.com|@gulfterra\.com|
@alpheuscommunications\.com") OR (header('From')
=="(?i)@elpaso\.com|@epenergy\.com|@elink\.elpaso\.com|
@epglobalnetworks\.com|@epmidstream\.com|@gulfterra\.com|
@alpheuscommunications\.com")))) {
    archive ("spoofedmail");
  }
```

```
CousinDomainSpoof:
  if (mail-from-dictionary-match("DomainCousins", 1)) {
    insert-header("X-Spoof-Potential", "High");
    edit-header-text("Subject", "(.*)", "POSSIBLY FORGED \\1");
    duplicate-quarantine("SenderVerificationFailure");
  }
```

Message Filters

Using LDAP in filters

- The most advanced and most flexible way for complex environments
 - Taking advantage of freeform LDAP group queries in AsyncOS
 - Limited scope, applicable to very specific use cases
 - Very flexible, and mostly light for processing due to LDAP caching
 - Will require LDAP schema modification for most applications

✓ Group Query	
Name:	<input type="text" value="listenerLDAP.group"/>
Query String:	<input type="text" value="&((proxyAddresses=smtp:{a})(countryCode={g}))"/> <input type="button" value="Test Query"/>

```
countryRouter:  
  if (rcpt-to-group == "US") {alt-mailhost("us-exch.domain.com");}
```

Message Filters

Using LDAP in filters

- You can manipulate the LDAP query to make it match any attribute as the “group”
- Regular LDAP configuration allows for several “tokens” – {a}, {u}, {d}, {g}, {f}
- It will return a pass/fail as a result of the query, so in the query we can use the attribute to match as a “group”

Original:

✓ Group Query	
Name:	<input type="text" value="listenerLDAP.group"/>
Query String:	<input type="text" value="(&(memberOf={g})(proxyAddresses=smtp:{a}))"/> <input type="button" value="Test Query"/>

Modified:

✓ Group Query	
Name:	<input type="text" value="listenerLDAP.group"/>
Query String:	<input type="text" value="(&((proxyAddresses=smtp:{a})(countryCode={g}))"/> <input type="button" value="Test Query"/>

Filter:

```
countryRouter:  
if (rcpt-to-group == "US") {alt-mailhost("us-exch.domain.com");}
```


LDAP Considerations

- LDAP queries used by Message Filters must be assigned to the Listeners
- You can still use “regular” LDAP group queries in the Mail Policies
- Add additional LDAP Server Profiles to accommodate “special” Group Queries used by Message Filters

LDAP Server Profiles				
Add LDAP Server Profile... <input type="checkbox"/> using the Active Directory Wizard. ?				
Server Profile	Host Name	Port	Queries	Delete
AD1	198.18.133.1	389	AD1.externalauth, AD1.accept, AD1.group, AD1.masquerade	
listenerLDAP	198.18.133.1	389	listenerLDAP.group	

Advanced

LDAP Queries:

- Accept
 - Accept Query: AD1.accept
 - Work Queue
 - Non-Matching Recipients: Bounce
 - SMTP Conversation
 - If the LDAP server is unreachable:
 - Allow Mail in
 - Return error code:
 - Code: 451
 - Text: Temporary recipient validation error.

Routing

Masquerade

Group

- Group Query: listenerLDAP.group

Add Policy

Policy Name: groupPolicy (e.g. my IT policy)

Insert Before Policy: 1 (Default Policy)

Add Users

Current Users

Sender

Recipient ?

Email Address(es)

(e.g. user@example.com, user@, @example.com, @.example.com)

LDAP Group Query

Query: AD1.group

Group: listenerLDAP.group

Message Filters

Structuring Message Filters, easy tests first!

- Most Message Filters are used to process lists:
 - Email addresses
 - Content keywords
 - IP addresses
 - Filenames
- There are multiple ways to process lists:
 - Nested ifs/multiple rules connected with Boolean operators
 - Regular Expressions
 - Dictionaries
 - LDAP

Message Filters

Filtering in layers, detect with MF & then act with CF!

- Message Filter:

MacroMFilter:

```
if (attachment-filename == "(?i)\\. (xls|doc|ppt|xlsx|docx|pptx)$") \  
AND ((attachment-binary-contains("(?i)x-vba-macros")) OR \  
((attachment-binary-contains("(?i)vba")) AND \  
(attachment-binary-contains("(?i)versioncompatible32")))) {  
  log-entry("$MatchedContent");  
  insert-header("X-Macro", "True");  
}
```

- Content Filter:

Conditions			
Add Condition...			
Order	Condition	Rule	Delete
1	Other Header	header("X-Macro") == "^True\$"	

Actions			
Add Action...			
Order	Action	Rule	Delete
1	Notify	notify ("admin@customer.org", "Macros in attachments")	
2	Quarantine	quarantine("Policy")	

Message Filters

Filtering in Layers, prep in 1st MF & finish in 2nd MF

```
filter1:
  if true {
    insert-header('X-Date-Received', '$date $time');
  }

filter2:
  if (mail-from == "^bob@abc.de$") AND (header('Date') == 'Wed') {
    if ((header('X-Date-Received') == '16 (08|09|10)') OR \ (header('X-Date-Received') == '16
11:(0|1|2)')) {
      strip-header("Subject");
      insert-header("Subject", "Time Limit: $Subject");
    }
  }
}
```

Message Filters

Drawbacks

- Message Filters apply to entire mail flow - incoming AND outbound!
- All Message Filters are evaluated for all messages.
- Message Filters occur before splintering!

Example:

```
devNoExe:
  if (rcpt-to-group=="Development") {
    drop-attachments-by-
filetype("Executable");
  };
salesNoHTML:
  if (rcpt-to-group=="Sales") {
    html-convert();
  };
```

- What happens if a message is sent to two people:
One in Sales group, and one in Development?
- What happens if they are in Development and Management?
- What happens if LDAP server is unavailable?

Message Splintering

Policy Engine And Splintering

MAIL FROM: bob@domain.com
 RCPT TO: joe@remote.org
 RCPT TO: jane@remote.org

SMTP Server	
IP Reputation	Host Access Table
External Threat Feeds (IoC)	
Connection Throttling	
Sender Verification	
SPF, DKIM, DMARC	
Sender Domain Reputation	
Received Header	
Default Domain	
Domain Map	
Recipient Access Table	

MAIL FROM: bob@domain.com
 RCPT TO: joe@remote.org
 RCPT TO: jane@remote.org

Workqueue	
LDAP RCPT Accept (WQ deferred)	
Masquerading (TABLE / LDAP)	
LDAP Routing	
Message Filters	

MAIL FROM: bob@domain.com
 RCPT TO: joe@remote.org

CASE (Anti-Spam)	
Anti-Virus	
AMP	Reputation File Analysis Retrospection Remediation
Graymail Detection	
Content Filtering	
DLP filtering (Outbound)	
Outbreak Filtering	

MAIL FROM: bob@domain.com
 RCPT TO: jane@remote.org

CASE (Anti-Spam)	
Anti-Virus	
AMP	Reputation File Analysis Retrospection Remediation
Graymail Detection	
Content Filtering	
DLP filtering (Outbound)	
Outbreak Filtering	

MAIL FROM: bob@domain.com
 RCPT TO: joe@remote.org

SMTP Client	
Encryption	
Virtual Gateways	
Delivery Limits	
Received Header	
Domain Based Limits	
Domain Based Routing	
...	

MAIL FROM: bob@domain.com
 RCPT TO: jane@remote.org

SMTP Client	
Encryption	
Virtual Gateways	
Delivery Limits	
Received Header	
Domain Based Limits	
Domain Based Routing	
...	

Per-policy scanning

Incoming or Outgoing Mail Policies

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

Policies									
Add Policy...									
Order	Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters	APP Filter	Delete
1	thiachan@bce-demo.com	Disabled	Disabled	Disabled	Disabled	ALEX-SPF-DKIM ALEX-FED ALEX-BEC-CF	Disabled	Forwarding (disabled)	
2	safeprint@bce-demo.net	Disabled	Disabled	Disabled	Disabled	CF_Safe_Print	Disabled	(use default)	
3	BLACKLIST	Disabled	Disabled	(use default)	Disabled	BLACKLIST_DROP	Disabled	(use default)	
4	WHITELIST	Disabled	(use default)	(use default)	Disabled	(use default)	Disabled	(use default)	
5	ALLOW_SPOOF	(use default)	(use default)	(use default)	(use default)	Malicious_URL URL_LOG_ALL_REPUTATION URL_LOG_ALL_CATEGORY URL_QUARANTINE_MALICIOUS URL_REWRITE_SUSPICIOUS URL_INAPPROPRIATE ...	(use default)	(use default)	
	Default Policy	IronPort Anti-Spam Positive: Deliver Suspected: Deliver	Sophos Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	File Reputation Malware File: Drop Pending Analysis: Quarantine Unscannable - Message Error: Deliver Unscannable - Rate Limit: Deliver Unscannable - AMP Service Not	Graymail Detection Unsubscribe: Enabled Marketing: Spam Quarantine Social: Spam Quarantine Bulk: Spam Quarantine ...	URL_LOG_ALL_REPUTATION URL_LOG_ALL_CATEGORY URL_QUARANTINE_MALICIOUS URL_REWRITE_SUSPICIOUS URL_INAPPROPRIATE SPF_DKIM_FAIL ...	Retention Time: Virus: 1 day Other: 4 hours	Forwarding (disabled)	

Per-policy scanning

Policy Match Conditions

- Complex conditions inside a policy using AND/OR/NOT
- Multiple conditions are configurable inside the same policy.
- Move your logic from the filter into the policy and reduce resource consumption.

The screenshot displays the 'Add User' configuration window, which is split into two main sections for defining sender and recipient conditions. The window title is 'Add User'.

Sender Conditions (Left Panel):

- Radio buttons for selection: Any Sender, Following Senders, Following Senders are Not.
- Text input for 'Email Address': 'user@outside.com'. Below it is a note: '(e.g. user@example.com, user@, @example.com, @.example.com)'. A small '.d' icon is at the end of the input.
- 'LDAP Group' section: 'Query: TNW_AD.group' (dropdown), 'Group: []' (input), and 'Add Group' / 'Remove' buttons.
- A large empty list box with a vertical scrollbar at the bottom.

Recipient Conditions (Right Panel):

- Radio buttons for selection: Any Recipient, Following Recipients.
- Text input for 'Email Address': 'ceo@inside.com'. Below it is a note: '(e.g. user@example.com, user@, @example.com, @.example.com)'. A small '.d' icon is at the end of the input.
- 'LDAP Group' section: 'Query: TNW_AD.group' (dropdown), 'Group: []' (input), and 'Add Group' / 'Remove' buttons.
- A large empty list box with a vertical scrollbar at the bottom.
- Checkboxes: Following Recipients are Not.
- Text input for 'Email Address': 'cto@inside.com'. Below it is a note: '(e.g. user@example.com, user@, @example.com, @.example.com)'. A small '.d' icon is at the end of the input.
- 'LDAP Group' section: 'Query: TNW_AD.group' (dropdown).





At the top right of the right panel, there is a dropdown menu set to 'Only if all conditions match'.

Per-policy scanning

Policy Match Priority (10.x, 11.1)

- AsyncOS 10.x allowed us to match a message to a mail policy, the envelope sender and the envelope recipient have a higher priority over the sender header.
- Starting with AsyncOS 11.1, there is now an option to choose which sender header has the priority for matching the incoming or outbound policy (global option).

Mail Policy Settings

Match Priority ?		
Add Priority...		
Priority	Headers	Delete
P1	Envelope Sender	
P2	Header "From"	
P3	Header "Sender"	
P4	Header "Reply-To"	

Per-policy scanning

Using Mail Policies vs. a dictionary

- Customers often use dictionaries to match senders or recipients for Block Lists/Allow Lists.
- By applying a block via content filter + dictionary causes all messages to be scanned, thus using more resources.
- Consider using Mail Policies to splinter and apply actions quickly.
- Be mindful of policy orders, first match wins, top-down.

Edit Policy

Policy Name: ?	<input type="text" value="BLOCKLIST"/> <small>(e.g. my IT policy)</small>
Editable by (Roles):	Cloud Operator
Insert Before Policy:	1 (BLOCKLIST) ▼

Users

[Add User...](#)

Sender	Recipients	Edit	Delete
user@gmail.com	ANY	Edit	
anotheruser@gmail.com	ceo@company.com	Edit	

Edit Policy

Policy Name: ?	<input type="text" value="ALLOWLIST"/> <small>(e.g. my IT policy)</small>
Editable by (Roles):	Cloud Operator
Insert Before Policy:	2 (ALLOWLIST) ▼

Users

[Add User...](#)

Sender	Recipients	Edit	Delete
user@gooddomain.com	ANY	Edit	

Content Filters

- Like message filters, content filters allow for granular filtering based on prior engine results and content scanning/analysis.

Add Condition

Message Body or Attachment

Message Body
URL Category
URL Reputation
Message Size
Message Language
Macro Detection
Attachment Content
Attachment File Info
Attachment Protection
Subject Header
Other Header
Envelope Sender
Envelope Recipient
Receiving Listener
Remote IP/Hostname
Reputation Score
Domain Reputation
DKIM Authentication
Forged Email Detection
SPF Verification
S/MIME Gateway Message
S/MIME Gateway Verified
Duplicate Boundaries Verification
Geolocation

Message Body or Attachment [Help](#)

Does the message body or attachment contain text that matches a specified pattern?

Contains text:
[]*

Contains smart identifier:
[ABA.Routing.Number]

Contains term in content dictionary:
[Executives]

Number of matches required: [1] (1-1000)
For content dictionaries, the number of matches is based on term weight.

Add Action

Quarantine

Encrypt on Delivery
Strip Attachment by Content
Strip Attachment by File Info
Strip Attachment With Macro
URL Category
URL Reputation
Add Disclaimer Text
Bypass Outbreak Filter Scanning
Bypass DKIM Signing
Send Copy (Bcc):
Notify
Change Recipient to
Send to Alternate Destination Host
Deliver from IP Interface
Strip Header
Add/Edit Header
Forged Email Detection
Add Message Tag
Add Log Entry
S/MIME Sign/Encrypt on Delivery
Encrypt and Deliver Now (Final Action)
S/MIME Sign/Encrypt (Final Action)
Bounce (Final Action)
Skip Remaining Content Filters (Final Action)
Drop (Final Action)

Quarantine [Help](#)

Flags the messages to be held in one of the centralized quarantines at "216.71.132.72".

Send message to quarantine: [Policy (centralized)]

Duplicate message
Send a copy of the message to the specified quarantine, and continue processing the original message. Any additional actions will apply to the original message.

Content Filters

Structure

Conditions			
Add Condition...		Apply rule:	If one or more conditions match ▾
Order	Condition	Rule	Delete
1	SPF Verification	spf-status != "none,pass,neutral,softfail,temperror"	
2	DKIM Authentication	dkim-authentication == "hardfail"	

Actions			
Add Action...			
Order	Action	Rule	Delete
Final	Drop (Final Action)	drop()	

- Add multiple conditions and actions into a single filter, use the same methodology as Message Filters & use easy tests first.
- No nesting of multiple conditions, AND/OR statements apply to conditions.
- Order of content filters are essential, each Content Filter in the list will be evaluated based on policy assignment.

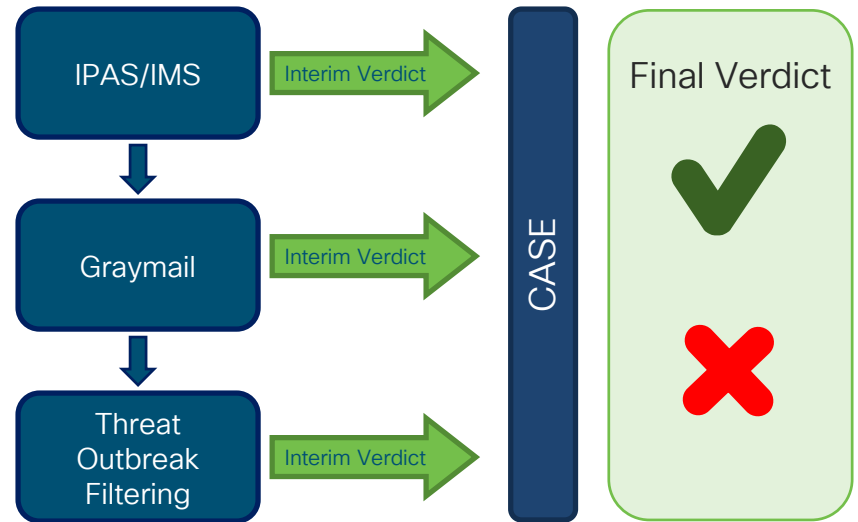
Base Configuration: Scanning Engines



Understanding CASE

Context Adaptive Scanning Engine (CASE)

- CASE is the combination of the **Anti-Spam**, **Graymail**, and **Outbreak** engines.
- Each engine can provide a verdict and depend 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 work queue.
- 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.



CASE & Anti-Phishing Enhancements

- CASE/OF Engine not detecting all URL-based Threats
- SDR verdict is not passed to CASE
- Upon release from OF, only AS/AV rescans the email
- Passing Macro detection, SPF and DKIM verification verdict to CASE
- IMS-NG (Advanced CASE and new spam detection)

12.x

- CASE/OF engine detection improvements
- Pass SDR, URLs in attachments information to CASE/OF
- Re-scan an email by all engines on release from OF quarantine
- New Aggressive scanning profile for IPAS users

13.0

- Cloud URL Analysis for inline URL inspection of anomalies
- Real-time cloud queries for IP and URL reputation
- OF/Re-scan improvements passing intermediate scan results, Suspect spam handling
- Support for additional URL shortened services
- Infrastructure improvements for faster URLs reputation updates
- Improved telemetry and exchanging contextual data across services

13.5

Anti-Spam/IronPort Anti-Spam

Global Settings

- Enable Antispam.
- Increase scanning thresholds for **Always scan messages smaller than to 1M, Never scan messages larger than to 2M.**
- Introduced in AsyncOS 13.0, you can now assign a higher priority on incoming or outgoing messages detected as spam, and to accept a higher chance of false positives with Scanning Profile of **Aggressive.**

IronPort Anti-Spam Global Settings	
<input checked="" type="checkbox"/> Enable IronPort Anti-Spam Scanning	
Message Scanning Thresholds:	<p>Increasing these values may result in decreased performance. Please consult documentation for size recommendations based on your environment.</p> <p>Always scan messages smaller than <input type="text" value="1M"/> Maximum <i>Add a trailing K or M to indicate units. Recommended setting is 1024K(1MB) or less.</i></p> <p>Never scan messages larger than <input type="text" value="2M"/> Maximum <i>Add a trailing K or M to indicate units. Recommended setting is 2048K(2MB) or less.</i></p>
Timeout for Scanning Single Message:	<input type="text" value="60"/> Seconds
Scanning Profile:	<p><input type="radio"/> Normal</p> <p><input checked="" type="radio"/> Aggressive <i>Recommended for customers who desire a stronger emphasis on blocking spam. When enabled, tuning Anti-Spam policy thresholds will have more impact on spam detection than the normal profile with a larger potential for false positives. Do not select the aggressive profile if IMS is enabled on the mail policy.</i></p> <p><input type="radio"/> Regional (China)</p>

Anti-Spam/IronPort Anti-Spam Mail Policies

Anti-Spam Settings	
Policy:	Default
Enable Anti-Spam Scanning for This Policy:	<input checked="" type="radio"/> Use IronPort Anti-Spam service <input type="radio"/> Use IronPort Intelligent Multi-Scan <i>Spam scanning built on IronPort Anti-Spam.</i> <input type="radio"/> Disabled
Positively-Identified Spam Settings	
Apply This Action to Message:	Deliver Send to Alternate Host (optional): <input type="text"/>
Add Text to Subject:	Prepend <input type="text" value="[SPAM]"/>
Advanced	Optional settings for custom header and message delivery.
Suspected Spam Settings	
Enable Suspected Spam Scanning:	<input type="radio"/> No <input checked="" type="radio"/> Yes
Apply This Action to Message:	Deliver Send to Alternate Host (optional): <input type="text"/>
Add Text to Subject:	Prepend <input type="text" value="[SUSPECTED SPAM]"/>
Advanced	Optional settings for custom header and message delivery.
Spam Thresholds	
<i>Spam is scored on a 1-100 scale. The higher the score, the more likely a message is a spam.</i>	
IronPort Anti-Spam:	<input checked="" type="radio"/> Use the Default Thresholds <input type="radio"/> Use Custom Settings: Positively Identified Spam: Score > <input type="text" value="90"/> (50 - 100) Suspected Spam: Score > <input type="text" value="50"/> (minimum 25, cannot exceed positive spam score)
IronPort Intelligent Multi-Scan:	<input checked="" type="radio"/> Use the Default Thresholds <input type="radio"/> Use Custom Settings: Positively Identified Spam: Score > <input type="text" value="90"/> (50 - 100) Suspected Spam: Score > <input type="text" value="50"/> (minimum 25, cannot exceed positive spam score)

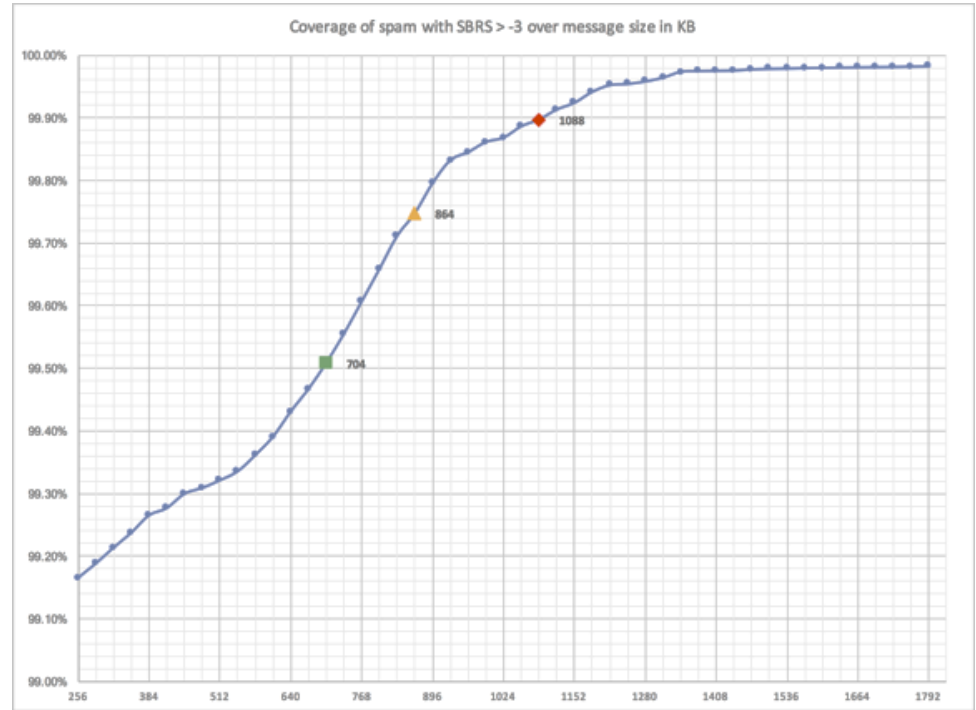
- You can adjust the thresholds for Positively-Identified & Suspected spam thresholds to increase or decrease sensitivity.
- Please don't do it, unless you really must.
- As we tune spam rules, we use the default thresholds as a baseline, so this may result in undesired results.
- Instead, assure that you have enabled the **Aggressive** scanning profile at service level. (See slide before!)

Anti-Spam/IronPort Anti-Spam

Optimal Spam Scanning Size

For your consideration:

- The chart to the right from Talos shows the volume of spam in large message sizes is small compared to spam, overall.
- Most spam is quite small.
- However, by not increasing scan size, you could be giving more extensive spam a free pass.
- Most of the spam captured in the 512KB and 896KB region capture plateaus around 1.3MB.



Anti-Spam/IronPort Anti-Spam

Ironport Intelligent Multi-Scan (IMS)

Cisco Intelligent Multi-Scan incorporates multiple anti-spam scanning engines, including Cisco Anti-Spam, to provide a multi-layer anti-spam solution.

When processed by Cisco Intelligent Multi-Scan:

* IMS is an additional license

- A message is first scanned by third-party anti-spam engines.
- Cisco Intelligent Multi-Scan then passes the message and the verdicts of the third-party engines to Cisco Anti-Spam, which assumes responsibility for the final verdict.
- After Cisco Anti-Spam performs its scan, it returns a combined multi-scan score to AsyncOS.
- Combining the benefits of the third-party scanning engines and Cisco Anti-Spam results in more caught spam while maintaining Cisco Anti-Spam's low false positive rate.

You cannot configure the order of the scanning engines used in Cisco Intelligent Multi-Scan; Cisco Anti-Spam will always be the last to scan a message and Cisco Intelligent Multi-Scan will not skip it if a third-party engine determines that a message is spam.

Using Cisco Intelligent Multi-Scan can lead to reduced system throughput.

Scan Behavior

Attachment Scanning Size and depth configuration

CLI: scanconfig, or from the UI: **Security Services> Scan Behavior**

Field	Description	Default
Action for attachments with MIME types / fingerprints in table above	Choose whether to scan or skip attachments types defined in the attachment type mapping.	Skip
Maximum depth of attachment recursion to scan	Specify the level up to which the recursive attachments are to be scanned.	5
Maximum attachment size to scan	Specify the maximum size of attachments to scan.	5M
Attachment Metadata scan	Specify whether to scan or skip metadata of the attachments.	Enabled
Attachment scanning timeout	Specify the scanning time-out period.	30s
Assume attachment matches pattern if not scanned for any reason	Specify whether to consider unscanned attachments as match to the search pattern.	No
Action when message cannot be deconstructed to remove specified attachments	Specify the action to be taken when a message could not be deconstructed to remove specified attachments.	No
Bypass all filters in case of a content or message filter error	Specify whether to bypass all filters in case of a content or message filter error.	Deliver
Encoding to use when none is specified	Specify the encoding to be used if no encoding is specified.	US-ASCII
Convert opaque-signed messages to clear-signed (S/MIME unpacking)	Specify whether to convert opaque-signed messages to clear-signed (S/MIME unpacking).	Disabled
Action for unscannable messages due to extraction failures	Specify the actions to take when a message cannot be scanned by the Content Scanner because of an attachment extraction failure.	Deliver As Is
Action for unscannable messages due to RFC violations	Specify the actions to take when a message cannot be scanned by the Content Scanner because of an RFC violation.	Disabled



Let's dive deeper into something new from 13.0!
Scan Behavior
Content Disarm and Reconstruction (Safe Print)

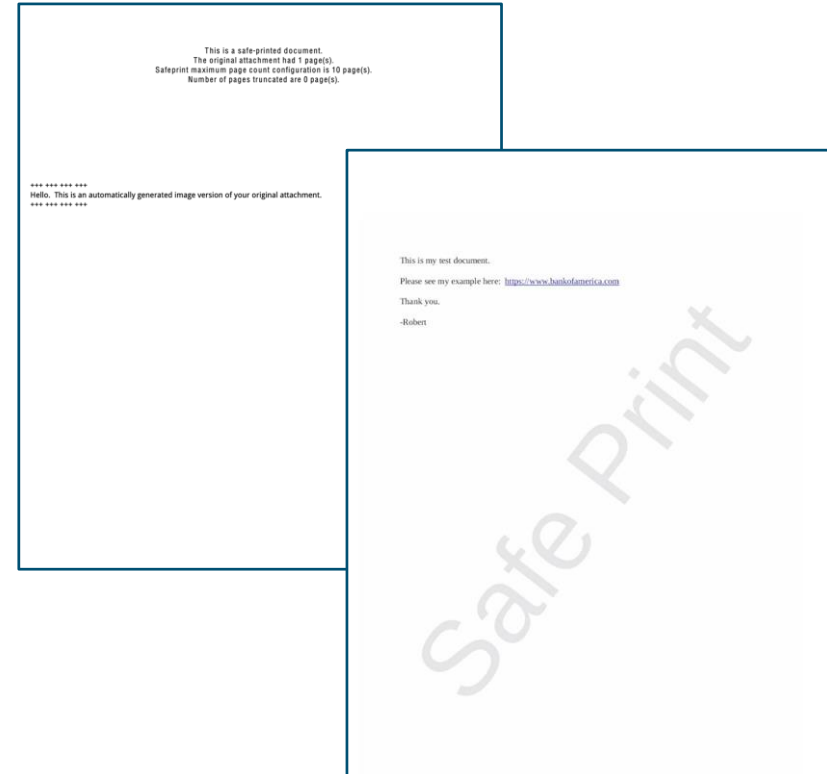
Scan Behavior

Content Disarm and Reconstruction (Safe Print)

- Content Disarm and Reconstruction (Safe Print) allows for malicious attachments to be converted into an image and embedded in a PDF.
- Use the 'Safe Print' content filter action to safe print all message attachments that match a configured content filter condition
- Watermark & cover page are optional

The screenshot shows the 'Safe Print Settings' configuration page. It includes the following settings:

- Maximum File Size:** 5M (with a note: 'Add a trailing K or M to indicate size units')
- Maximum Page Count:** 10
- Document Quality:** Use Default Value (70) and Enter Custom Value: 70
- File Type Selection:** Includes 'Select All', 'Expand All', 'Collapse All', and 'Reset' buttons. A tree view shows 'Document' expanded with 'Microsoft Documents' selected.
- Watermark:** Enabled and Disabled. 'Enter Custom Text:' is set to 'Safe Print'.
- Cover Page:** Enabled and Disabled. 'Enter Custom Text:' contains a preview of the generated image version of an attachment.



Safe Print: Content Filter example

File Types supported in AsyncOS 13.0:

Document

- AcroExch.Document(.pdf)
- Hancom Office File(.hwp)
- Xhtmlfile(.xhtml)
- Xmlfile(.xml)

Microsoft Documents

- PowerPoint.Show.12(.pptx)
- PowerPoint.Show.8(.ppt)
- PowerPoint.ShowMacroEnabled.12(.pptm)
- PowerPoint.SlideShow.12(.ppsx)
- PowerPoint.SlideShowMacroEnabled.12(.ppsm)
- PowerPoint.Template.12(.potx)
- PowerPoint.Template.8(.pot)
- PowerPoint.TemplateMacroEnabled.12(.potm)
- Powerpointxmlfile(.pptxml)
- Word.Document.12(.docx)
- Word.Document.8(.doc)
- Word.Template.12(.dotx)
- Word.Template.8(.dot)
- Word.TemplateMacroEnabled.12(.dotm)
- Wordhtmlfile(.dohtml)

Content Filter Settings	
Name:	CF_Safe_Print
Currently Used by Policies:	Default Policy
Editable by (Roles):	Cloud Operator
Description:	13.0 EFT2 Beta - Safe Print Content Filter
Order:	1 (of 20)

Conditions			
Add Condition...		Apply rule: If one or more conditions match	
Order	Condition	Rule	Delete
1	Attachment File Info	attachment-filename == "docx"	
2	Attachment File Info	attachment-filename == "pdf"	

Actions			
Add Action...			
Order	Action	Rule	Delete
1	Quarantine	duplicate-quarantine("SAFE_PRINT")	
2	Safe Print	safeprint-all-attachments-strip-unscan(1, "Your attachment has been removed from the email message as Cisco Email Security has ruled it as 'unscannable'. Please contact your email administrator.", 0)	
3	Add Log Entry	log-entry("<<< === SAFE PRINT TRIGGERED === >>>")	
4	Add Disclaimer Text	add-heading("SAFE_PRINT_DISCLAIMER")	

(*Use duplicate-quarantine to save a copy of original email and attachment prior to 'Safe Print' re-write

Safe Print (Demo Video)

1min 27sec



The screenshot displays the Cisco C300V Cloud Email Security Appliance management interface. The main content area is titled "Scan Behavior" and is divided into two sections: "Attachment Type Mappings" and "Global Settings".

Attachment Type Mappings

Fingerprint / MIME	Type	Edit	Delete
MIME Type	audio/*	Edit...	
MIME Type	video/*	Edit...	
MIME Type	image/*	Edit...	
Fingerprint	Media	Edit...	
Fingerprint	Image	Edit...	

Global Settings

Action for attachments with MIME types / fingerprints in table above:	Skip
Maximum depth of attachment recursion to scan:	5
Maximum attachment size to scan:	5M
Attachment Metadata scan:	Enabled
Attachment scanning timeout:	30 seconds
Assume attachment matches pattern if not scanned for any reason?	No
Assume zip file to be unscannable if files in the archive cannot be read?	No
Action when message cannot be deconstructed to remove specified attachments:	Deliver
Bypass all filters in case of a content or message filter error:	Yes
Encoding to use when none is specified:	US-ASCII
Convert opaque-signed messages to clear-signed (S/MIME unpacking):	Disabled
Safe Print settings	
Maximum File Size	5M
Maximum Page Count	10
Document Quality	70
Actions for Unscannable Messages due to decoding errors found during URL Filtering Actions:	Disabled
Action when a message is unscannable due to extraction failures:	Deliver As Is
Action when a message is unscannable due to RFC violations:	Disabled

Current Content Scanner files

File Type	Last Update	Current Version	New Update
Content Scanner Tools	28 Jul 2019 02:31 (GMT +00:00)	11.4.14.3263.10.1.1200279	Connecting to update server

CISCO *Live!*

Anti-Virus

Sophos and/or McAfee

Sophos Anti-Virus Overview	
Anti-Virus Scanning by Sophos Anti-Virus:	Enabled
Virus Scanning Timeout (seconds):	60
Automatic Updates: ?	Enabled
Edit Global Settings...	

Message Scanning	
	Scan for Viruses only ▾
	<input type="checkbox"/> Drop infected attachments if a virus is found
	<input checked="" type="checkbox"/> (recommended) Include an X-header with the Anti-Virus scanning results in messages
Repaired Messages:	
Action Applied to Message:	Deliver As Is ▾
Archive Original Message:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Modify Message Subject:	<input checked="" type="radio"/> No <input type="radio"/> Prepend <input type="radio"/> Append
	[WARNING: VIRUS REMOVED]
	Optional settings for custom header and message delivery.
Encrypted Messages:	
Action Applied to Message:	Deliver As Is ▾
Archive Original Message:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Modify Message Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append
	[WARNING: MESSAGE ENCRYPTED]
	Optional settings for custom header and message delivery.
Unscannable Messages:	
Action Applied to Message:	Deliver As Is ▾
Archive Original Message:	<input type="radio"/> No <input checked="" type="radio"/> Yes
Modify Message Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append
	[WARNING: A/V UNSCANNABLE]
	Optional settings for custom header and message delivery.
Virus Infected Messages:	
Action Applied to Message:	Drop Message ▾
Archive Original Message:	<input type="radio"/> No <input checked="" type="radio"/> Yes
Modify Message Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append
	[WARNING: VIRUS DETECTED]
	Optional settings for custom header and message delivery.

- Sophos is on by default, with automatic updates enabled.
- Configure attachment scan size via the **scanconfig** command.
- There are two modes: **Scan for Virus only** or **Scan and Repair**
 - The recommendation is not to Repair viruses.
- What are Encrypted Messages?
 - Encrypted is signed or files that are identifiable but can't be unpacked (i.e., password-protected .zip files)
- What are Unscannable Messages?
 - Unscannable would be corrupt/too large to scan attachments.
- Virus-infected Messages?
 - Configure, if not already, as **Drop**

Advanced Malware Protection (AMP)

File Reputation and File Analysis

The screenshot shows the configuration page for File Reputation and File Analysis in the AMP console. It is divided into several sections:

- File Reputation Filtering:** Includes checkboxes for "Enable File Reputation" and "Enable File Analysis".
- File Analysis:** A tree view showing file types with checkboxes. Checked items include "Archived and compressed", "Configuration", "Database", "Email", "Encoded and Encrypted", "Executables", "Microsoft Documents", and "Miscellaneous". Buttons for "Select All", "Expand All", "Collapse All", and "Reset" are present.
- Advanced Settings for File Reputation:**
 - File Reputation Server: AMERICAS (cloud-sa.amp.cisco.com)
 - AMP for Endpoints Console Integration: Register Appliance with AMP for Endpoints.
 - SSL Communication for File Reputation: Use SSL (Port 443). Tunnel Proxy (Optional) fields for Server, Port, Username, Password, and Retype Password. Relax Certificate Validation for Tunnel Proxy.
 - Heartbeat Interval: 15 minutes
 - Query Timeout: 15 seconds
 - Processing Timeout: 120 seconds
 - File Reputation Client ID: 42cde4d9-16c6-4282-8554-fcb8b52f0c11
 - File Retrospective: Suppress the verdict update alerts.
- Advanced Settings for File Analysis:**
 - File Analysis Server URL: AMERICAS (https://panacea.threatgrid.com)
 - File Analysis Client ID: 01_VLINESA000143_423F898DE7A7ED99CDD2-0D5198CC716E_C100V_00000000
- Cache Settings:** Advanced settings for cache.
- Threshold Settings:** File Analysis Threshold Score: Use Value from Cloud Service (95) or Enter Custom Value: 95.

- File Reputation is SHA based lookups.
- File Analysis is the behavioral analysis engine in the cloud; by default, the list is only 30 file types.
- The recommendation is to review the list and enable additional file types for analysis.
- In 12.0, you have the option to configure the threshold to lower the score of a malicious file. Use this option with caution!

Graymail

Graymail scanning & detection

Common Global Settings	
Message Scanning Thresholds:	Always scan 512K or less. Never scan 2M or more.
Timeout for Scanning Single Message:	60 seconds

- Enable Graymail Detection. Recommendation is to increase scanning thresholds to 2M for Max scan size.

Mail Policies: Graymail

Graymail Settings

Policy: DEFAULT

Enable Graymail Detection for This Policy: Yes No

Enable Graymail Unsubscribing for This Policy: Yes No

Perform this action for: All Messages Unsigned Messages

✓ Action on Marketing Email

Apply this action to Message: (optional):

Add Text to Subject: Append

Advanced

Optional settings for custom header and message delivery:

Add Custom Header (optional): Header: Value:

Send to an Alternate Envelope Recipient (optional): Email Address: (e.g. employee@company.com)

Archive Message: No Yes

✓ Action on Social Network Email

Apply this action to Message: (optional):

Add Text to Subject: No Prepend Append

Advanced

Optional settings for custom header and message delivery:

✓ Action on Bulk Email

Apply this action to Message: (optional):

Add Text to Subject: No Prepend Append

Advanced

Optional settings for custom header and message delivery:

Policy Settings:

- Three (3) verdicts will be returned by Graymail detections: Social, Marketing, Bulk
 - Marketing: Vendor emails, known marketing senders
 - Social: Facebook, Twitter, etc.
 - Bulk: Google Groups, bulk senders
- At a minimum, deliver as-is and mark an X-header for later evaluation and reporting.

Graymail

Using Graymail and Outlook Junk folders

- Two steps: Mark X-header in Graymail, Filter in Exchange to set the SCL value

1

Deliver ▼

Send to Alternate Host (optional):

No Prepend Append

[MARKETING]

Add Custom Header (optional):

Header:	X-GM-VERDICT
Value:	MARKETING

Send to an Alternate Envelope Recipient (optional):

Email Address:

(e.g. employee@company.com)

Archive Message: No Yes

2

Rule - Google Chrome

Secure | https://outlook.office365.com/ecp/RulesEditor/ExchangeTransportRule.aspx?ActivityCorrelationID=c6c9e62a-c7e6-66a8-1fa

GM_TO_JUNK

Name: GM_TO_JUNK

*Apply this rule if...

A message header matches... 'x-gm-verdict' header matches 'social' or 'marketing' or 'bulk'

add condition

*Do the following...

Set the spam confidence level (SCL) to... 6

add action

Except if...

add exception

Properties of this rule:

Priority: 2

Audit this rule with severity level: Not specified

Choose a mode for this rule:

Enforce

Outbreak Filters

Enabling Outbreak Filters

Outbreak Filter Settings

Quarantine Threat Level:

Maximum Quarantine Retention: Viral Attachments: Days
Other Threats: Hours
 Deliver messages without adding them to quarantine

Bypass Attachment Scanning:

Message Modification

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

Message Modification Threat Level:

Message Subject: Prepend [Insert Variables](#) | [Preview Text](#)

Include the X-IronPort-Outbreak-Status headers:
 Enable for all messages
 Enable only for threat-based outbreak
 Disable

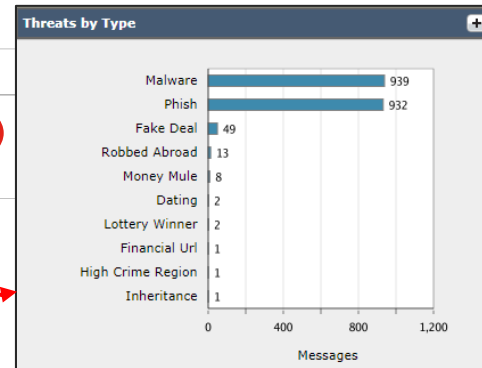
Include the X-IronPort-Outbreak-Description header:
 Enable
 Disable

Alternate Destination Mail Host (Other Threats only):
(examples: example.com, 10.0.0.1, 2001:420:80:1::5)

URL Rewriting: Cisco Security proxy scans and rewrites all URLs contained in malicious outbreak emails.
 Enable only for unsigned messages (recommended)
 Enable for all messages
 Disable

Bypass Domain Scanning:

- By default, Outbreak Filters is enabled.
- Enabling 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.



Summary

CASE engines

IronPort Anti-Spam

IronPort Anti-Spam Overview	
IronPort Anti-Spam Scanning:	Enabled
Message Scanning Thresholds:	Always scan 1M or less. Never scan 2M or more.
Timeout for Scanning Single Message:	60 seconds
Regional Scanning:	Off

- Enable Anti-Spam.
- Increase scanning thresholds to 1M for always scan, 2M for never to scan more.

Graymail Detection and Safe Unsubscribing

Global Settings	
Graymail Detection:	Enabled
Maximum Message Size to Scan:	2M
Timeout for Scanning Single Message:	60 seconds

- Enable Graymail.
- It's a free engine which helps with Anti-Spam efficacy!

Outbreak Filters

Outbreak Filters Overview	
Global Status:	Enabled
Adaptive Rules:	Enabled
Maximum Message Size to Scan:	1M
Receive Emailed Alerts:	No
Web Interaction Tracking	Enabled <small>To track URLs due to Policy rewrites, you have to enable Web Interaction Tracking at Security Services > URL Filtering.</small>

[Edit Global Settings.](#)

- Enable Outbreak Filters.
- Increase scan size to 1M.

Summary

Base Configuration: Scanning Engines

- ❑ Assess your Host Access Table – still using the defaults? Time to adjust the scores
- ❑ Create more Sender Groups and get gradually more aggressive in your settings
- ❑ Check your WhiteLists – entries could be years old, ip changed, etc. Use the comments to keep track and prune regularly
- ❑ Check your 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 and Threat Outbreak Filtering to get more insight and better efficacy
- ❑ Check your file size limits: Defaults are low and could potentially allow threat messages through
- ❑ Running old AsyncOS? (Why?) Upgrade, Upgrade, Upgrade!



Base Configuration: Mail delivery

Outbound Mail scanning

- From the HAT, configuring a mail flow policy as RELAY will mark a message as outbound.
- Outgoing mail policy/policies will then define which security service and scanning are leveraged on the flow and have an additional DLP blade.

Policies									
Add Policy...									
Order	Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters	DLP	Delete
1	INTERNAL	(use default)	Sophos Encrypted: Deliver Unscannable: Deliver Virus Positive: Quarantine	File Reputation Malware File: Deliver Pending Analysis: Deliver Unscannable - Message Error: Deliver Unscannable - Rate Limit: Deliver Unscannable - AMP Service Not	(use default)	MALICIOUS_URL MALICIOUS_FILE_INTERNAL AUP_URL_CATEGORY	(use default)	Merger and Acquisition Code Names	
	Default Policy	Disabled	Sophos Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	File Reputation Malware File: Drop Unscannable - Message Error: Deliver Unscannable - Rate Limit: Deliver Unscannable - AMP Service Not	Disabled	MALICIOUS_URL PROFANITY ENCRYPT_CRES	Disabled	PCI-DSS (Payment Card Industry... US HIPAA and HITECH (Low Threshold)	

Message Delivery settings

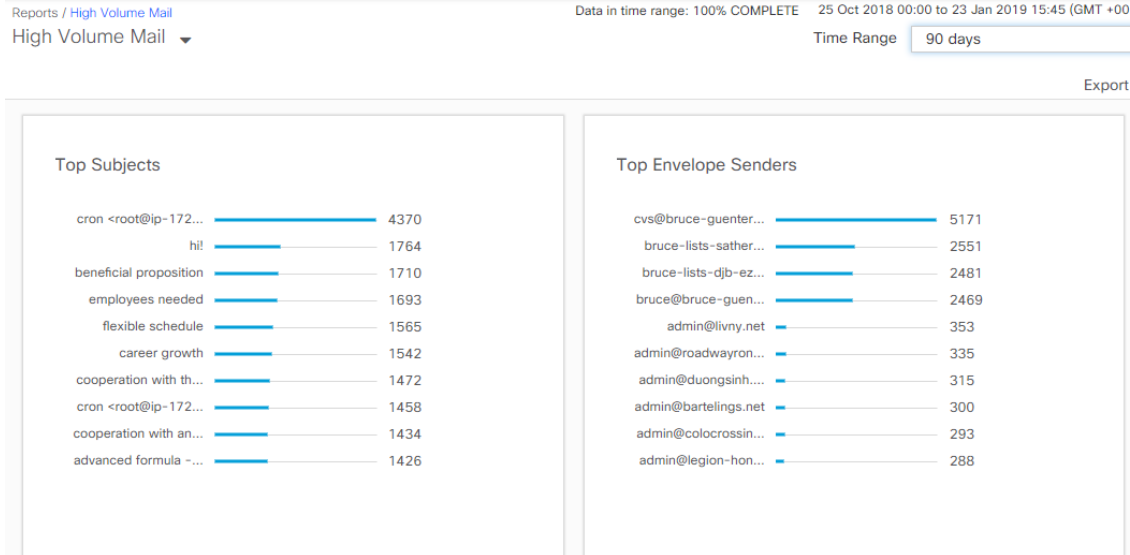
Sender Throttling

Rate Limit for Envelope Senders:	Max. Recipients Per Time Interval:	<input type="radio"/> Unlimited <input checked="" type="radio"/> 100 Recipients per 60 Minutes. <small>Number of recipients between 1 and 1,000,000 per number of minutes between 5 and 1440</small>
	Sender Rate Limit Error Code:	452
	Sender Rate Limit Error Text:	Too many recipients received from the sender
	Exceptions:	Ignore Rate Limit for Address List: <input type="text" value="None"/>
Flow Control:	Use SenderBase for Flow Control:	<input checked="" type="radio"/> On <input type="radio"/> Off
	Group by Similarity of IP Addresses:	<small>This Feature can only be used if SenderBase for Flow Control is off.</small>

- The HAT will define a RELAY policy for the host or IP that is sending email.
- By leveraging the per-sender throttling in the HAT, you can prevent outbound blasts (either purposely or be malicious host) to prevent flooding and potential blacklisting.

Message Delivery settings

High Volume Mail



- The high-volume mail report will report on both external and internal mail.
- This can help identify if there was a blast of email from a sender.
- Consider configuring a high-volume message filter or content filter. This will be useful to help prevent blasts based on a header.

Message Delivery settings

Destination Controls

Destination Controls	
Destination:	<input type="text" value="gmail.com"/>
IP Address Preference:	Default (IPv6 Preferred) ▼
Limits:	Concurrent Connections: <input type="radio"/> Use Default (500) <input checked="" type="radio"/> Maximum of <input type="text" value="20"/> (between 1 and 1,000)
	Maximum Messages Per Connection: <input type="radio"/> Use Default (50) <input checked="" type="radio"/> Maximum of <input type="text" value="5"/> (between 1 and 1,000)
	Recipients: <input type="radio"/> Use Default (No Limit) <input checked="" type="radio"/> Maximum of <input type="text" value="20"/> per <input type="text" value="60"/> minutes <small>Number of recipients between 0 and 1,000,000,000 per number of minutes between 1 and 60</small>
	Apply limits: Per ESA hostname: <input checked="" type="radio"/> System Wide <input type="radio"/> Each Virtual Gateway <small>(recommended if Virtual Gateways are in use)</small>
TLS Support:	Default (Preferred) ▼ DANE Support: ? <input type="text" value="Default (None)"/> ▼
Bounce Verification:	Perform address tagging: <input checked="" type="radio"/> Default (No) <input type="radio"/> No <input type="radio"/> Yes <small>Applies only if bounce verification address tagging is in use. See Mail Policies > Bounce Verification.</small>
Bounce Profile:	Default ▼ <small>Bounce Profile can be configured at Network > Bounce Profiles.</small>

- Self-throttle should be implemented to control outbound mail flow
- Some destinations like webmail providers, have much lower limits for receiving email
- Lowering those limits will help prevent throttling by those destinations
- BATV and Bounce Profiles can be set per destination



Destination Controls Settings

<https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118573-technote-esa-00.html>

Disclaimers and Action Variables

- You can create a wide variety of text resources that can be used in filters as actions for suspected messages.
- Action Variables can be used inside the text resource as well as Message Filters and Content Filters.

Edit Text Resource

The screenshot displays the 'Edit Text Resource' interface for a resource named 'FROM_REPLYTO' of type 'Disclaimer Template'. The HTML editor shows the following code:

```
<table>
<tbody>
<tr>
<td style="text-align: center;">
<p><EXTERNAL_EMAIL><br>&nbsp;</p>Note that this message is from
$EnvelopeFrom.&nbsp;<br>Do not reply to this message if you do not recognize the
sender.&nbsp;<br><span style="color: #ff0000;">Keep the Empire safe!</span></p>
</td>
</tr>
</tbody>
</table>
```

An 'Insert Variables' dialog is open, listing various variables such as 'To', 'Subject', 'Time', 'Internal Message ID', 'Mail Flow Policy', 'File Names', 'File Sizes', 'Receiving Listener', 'Header', 'Envelope Recipients', 'Body Size', 'Matched Content', 'DLP Severity', 'Threat Category', 'Threat Description', 'Threat Verdict', 'From', 'Date', 'GMT Timestamp', 'HAT Group Name', 'SenderBase Reputation Score', 'File Types', 'Remote Host Address', 'All Headers', 'Envelope Sender', 'Hostname', 'Filter Name', 'DLP Policy Name', 'DLP Risk Factor', 'Threat Type', and 'Threat Level'. A yellow arrow points from the 'Code View' button in the HTML editor to the 'Insert Variables' dialog.

A separate 'Code View' window shows the rendered HTML output:

```
<table style="background-color: #FE9A2E; margin-bottom:10px; width: 100%;
text-align: center">
<tbody>
<tr>
<td><span style="font-size:12px; font-family:verdana;">Warning: Replies to this
message will go to $EnvelopeFrom. If you are unsure this is correct please contact
the helpdesk.</span></td>
</tr>
</tbody>
```

The 'Plain Text Alternative' section contains the text: 'A plain text disclaimer is applied when HTML is not supported. The text is automatically generated from the required HTML text above or an alternate to the HTML, can be defined below.' Below this is an 'Edit alternative text' field containing: 'EXTERNAL_EMAIL: Note that this message is from \$EnvelopeFrom. Do not reply to this message if you do not recognize the sender. Keep the Empire safe!'.

Adding warning disclaimers to email

Content Filter Settings	
Name:	<input type="text" value="EXTERNAL_EMAIL"/>
Currently Used by Policies:	Default Policy
Editable by (Roles):	Cloud Operator
Description:	<input type="text"/>
Order:	1 ▼ (of 6)

Conditions
<input type="button" value="Add Condition..."/>
<i>There are no conditions, so actions will always apply.</i>

Actions			
<input type="button" value="Add Action..."/>			
Order	Action	Rule	Delete
1	Add Disclaimer Text	add-heading("FROM_REPLYTO")	

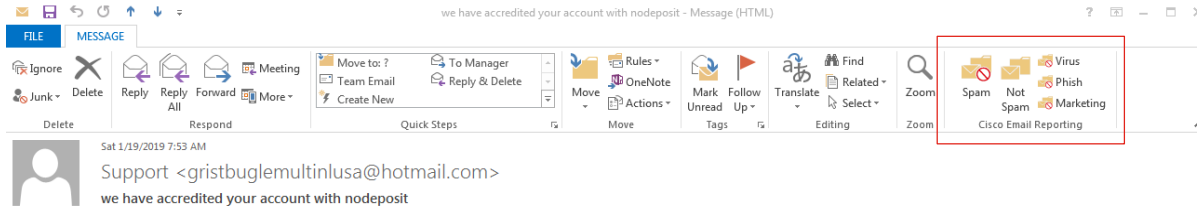
j.hutt@carbonidedepot.com
to ▼

EXTERNAL EMAIL

Note that this message is from j.hutt@carbonidedepot.com. Do not reply to this message if you do not recognize the sender. **Keep the Empire safe!**

Dey bimlio deesah shlong Twass pahs teeka al won roonk. Bas kah!

Submitting misses



- Reporting plug-in allows for end-users to directly submit missed threats to Cisco
- Can be mass-deployed via installers and GPOs
- Edit the manifest file to send administrators to get a copy to a specific address



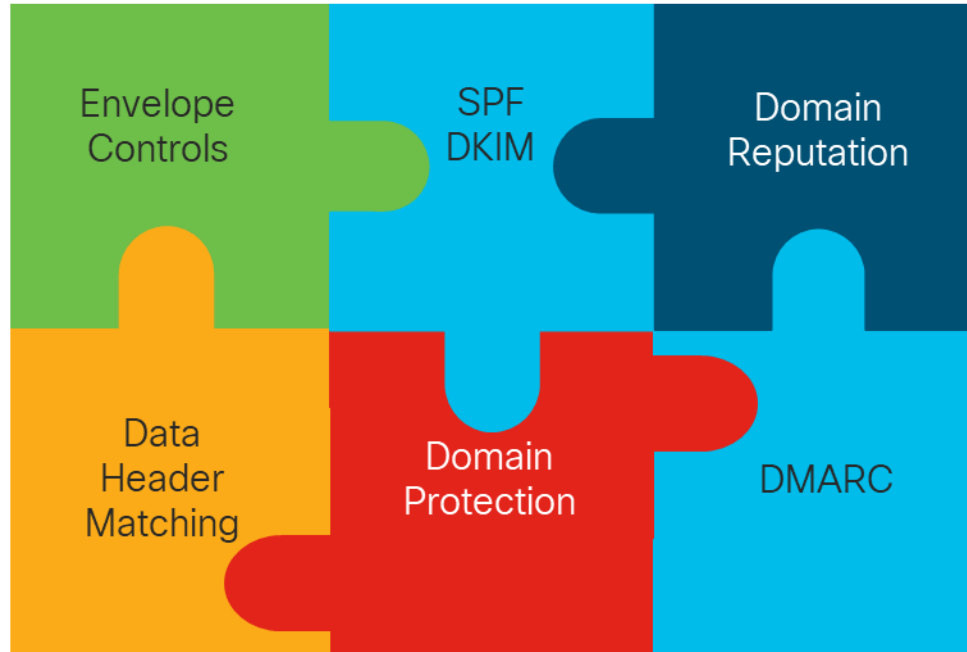
Download the Reporting Plug-In:

<https://software.cisco.com/download/home/284900944/type/283090986/release/1.2.0.109>



Defensive Configuration: Anti-Spoofing & Phishing

Putting together the anti-spoofing puzzle



Spoofing Targets

Type	Who are they spoofing?	Spoof Target	Description
Simple Spoof	External Parties	Your Users	Simple spoof is where the attacker attempts to change or manipulate the envelope from in the headers of an email, or change the reply-to to redirect email.
Cousin Domain / Typo Squatting	Your Brand	Your Customers	Attacks become more sophisticated by relying 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
Display Name Modification	Your Executives	Financial Controllers	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.

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 the key to prevent financial loss, brand damage, or legal ramifications.

Sources of spoofs

- The advent of shared services such as Office 365 and G Suite has made it easy to use mail servers that have a “good” reputation.
- Compounding the issue, these services will mix free mail with corporate or paid services, making it harder to distinguish threat messages based on the source.

```
Wed Jan 23 19:53:59 2019 Info: New SMTP ICID 2053153 interface Data 1 (216.71.132.15) address 209.85.128.51 reverse dns host mail-wm1-f51.google.com verified yes
Wed Jan 23 19:53:59 2019 Info: ICID 2053153 ACCEPT SG SUSPECTLIST match sbrs[none] SBRS not enabled country not enabled
Wed Jan 23 19:54:00 2019 Info: Start MID 2262917 ICID 2053153
Wed Jan 23 19:54:00 2019 Info: MID 2262917 ICID 2053153 From: <jango@tatooineexpress.com>
Wed Jan 23 19:54:00 2019 Info: MID 2262917 ICID 2053153 RID 0 To: <boba@carbonitedepot.com>
...
Wed Jan 23 19:54:00 2019 Info: MID 2262917 Message-ID '<CAAkPH0t7Rzakh5akrYw+oHEe3UWY8XmWX_CQ0wTRNJZ5UzZSaA@mail.gmail.com>'
```

```
Wed Jan 23 19:57:11 2019 Info: New SMTP ICID 2053155 interface Data 1 (216.71.132.15) address 209.85.167.50 reverse dns host mail-lf1-f50.google.com verified yes
Wed Jan 23 19:57:11 2019 Info: ICID 2053155 ACCEPT SG SUSPECTLIST match sbrs[none] SBRS not enabled country not enabled
Wed Jan 23 19:57:11 2019 Info: Start MID 2262919 ICID 2053155
Wed Jan 23 19:57:11 2019 Info: MID 2262919 ICID 2053155 From: <greedo@gmail.com>
Wed Jan 23 19:57:11 2019 Info: MID 2262919 ICID 2053155 RID 0 To: <jhutt@carbonitedepot.com>
...
Wed Jan 23 19:57:11 2019 Info: MID 2262919 Message-ID '<CAKSeP1NwiBMK+v2NNCnbGB5Wj2oaCXxH9BJM11jJgDN9LRMjDw@mail.gmail.com>'
```

Addressing the Simple SpooF

```
Sun Jan 27 04:52:01 2019 Info: New SMTP ICID 33038 interface Data 1 (216.71.134.24) address
68.183.144.44 reverse dns host mailbot2.teamnorthwind.com verified yes
Sun Jan 27 04:52:01 2019 Info: ICID 33038 ACCEPT SG BYPASSLIST match .teamnorthwind.com SBRS
None country United States
Sun Jan 27 04:52:01 2019 Info: Start MID 139 ICID 33038
Sun Jan 27 04:52:01 2019 Info: MID 139 ICID 33038 From: <j.hutt@carbonitedepot.com>
Sun Jan 27 04:52:01 2019 Info: MID 139 ICID 33038 RID 0 To: <boba@carbonitedepot.com>
Sun Jan 27 04:52:01 2019 Info: MID 139 Subject 'Re:Missing Shipment (Tracking: SOLO-BSPN-
001)'Sun Jan 27 04:52:02 2019 Info: MID 139 ready 836 bytes from <j.hutt@carbonitedepot.com>
Sun Jan 27 04:52:02 2019 Info: MID 139 matched all recipients for per-recipient policy DEFAULT
in the inbound table
Sun Jan 27 04:52:02 2019 Info: ICID 33038 close
```

- Typically will be a compromised host, on a hosting service or dynamic IP or compromised host.
- In this example, an obvious spooF of a domain owned by the target.
- Without any connection-level verification, little info to use to help convict the message.

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 placed in quarantine for review.
- Modify to include SPOOF_ALLOW list and domains in the From header.



Anti-Spoofing Whitepaper

http://www.cisco.com/c/en/us/products/collateral/security/email-security-appliance/whitepaper_C11-737596.html

Envelope Spoofing (for owned domains)

- There are two types of headers in an email, envelope and data headers.
- Envelope spoofing is one of the simplest and easiest ways to trick users by manipulating the headers to show whatever the attacker desires.

```
Info: ICID 1840489 ACCEPT SG ACCEPT match 45.55.251.155 SBRS None country United States
Info: Start MID 3481407 ICID 1840489
Info: MID 3481407 ICID 1840489 From: <jango@tatooineexpress.com>
Info: MID 3481407 ICID 1840489 RID 0 To: <boba@carbonitedepot.com>
Info: MID 3481407 ready 653 bytes from <boba@carbonitedepot.com>
Info: MID 3481407 matched all recipients for per-recipient policy DEFAULT in the inbound table
Info: MID 3481407 queued for delivery
Info: Delivery start DCID 0 MID 3481407 to RID [0]
Info: Message done DCID 0 MID 3481407 to RID [0] [('from', 'jango@tatooineexpress.com')]
```

Envelope spoof of a domain that you own

Recipient is of the same domain

From header inherits Envelope if not specified

Controlling domains with Sender Exception Tables

Envelope Sender DNS Verification: On Off

Malformed Envelope Senders:

SMTP Code:

SMTP Text:

Envelope Senders whose domain does not resolve:

SMTP Code:

SMTP Text:

Envelope Senders whose domain does not exist:

SMTP Code:

SMTP Text:

Use Sender Verification Exception Table: On Off

Sender Verification Exception Table

[Add Sender Verification Exception...](#) [Clear All Sender Verification Exceptions](#)

Order	Exception	Behavior	SMTP Response	Delete
1	@carbonitedepot.com	Reject	553, Envelope sender <\$EnvelopeSender> rejected	

- Sender Exception Table can be used to allow senders to bypass DNS verification controls
- Can also be used to outright block envelope sender domains, such as your own domain, or variations of them

```
Info: ICID 1840469 ACCEPT SG ACCEPT match 45.55.251.155 SBRS None country United States
Info: ICID 1840469 Address: <boba@carbonitedemo.com> sender rejected, envelope sender matched domain exception
```


Allowed Spoofing Sources

- There are legitimate use cases for outside or 3rd party organizations to send mail to your users or on your organization's behalf.
- Focusing on allowing spoofing to your users, rules would need to be in place to bypass connection verification checks, and any header checks.
- Create a Mail Flow Policy to bypass SBRS, DMARC, SPF, and DKIM.
- You can leverage the X-headers stamped to make policy decisions based on the Sender Group match.

Sender Group Settings

Name:	SPOOF_SENDERS
Order:	1
Comment:	None
Policy:	ACCEPTED_SPOOF
SBRS (Optional):	Not in use
DNS Lists (Optional):	None
Connecting Host DNS Verification:	None Included

[<< Back to HAT Overview](#) [Edit Settings...](#)

Find Senders

Find Senders that Contain this Text: [Find](#)

Sender List: Display All Items in List Items per page 20

[Add Sender...](#)

Sender	Comment	All Delete
.salesforce.com	None	<input type="checkbox"/>

[<< Back to HAT Overview](#) [Delete.](#)

Conditions

[Add Condition...](#)

Order	Condition	Rule	Delete
1	Other Header	header("X-IronPort-SenderGroup") == "^SPOOF_SENDERS\$"	<input type="checkbox"/>

Actions

[Add Action...](#)

Order	Action	Rule	Delete
1	Skip Remaining Content Filters (Final Action)	skip-filters()	<input type="checkbox"/>

SPF

How it works

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

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

DKIM

How it works

- Domain Keys Identified Mail, Specified in RFC5585.
- In a nutshell: Specifies methods for gateway-based cryptographic signing of outbound messages, embedding verification data in an e-mail header, and ways for recipients to verify integrity of the messages.
- Additional RFC RFC6376 (DKIM Signatures), RFC5863 (DKIM Development, Deployment and Operation), RFC5617 (Author Domain Signing Practices (ADSP)).
- DKIM uses DNS TXT records to publish public keys. Example:

```
20120113._domainkey.gmail.com IN TXT "k=rsa\; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCQAQ8AMIIBCgKCAQEA1Kd87/UeJjenpabg  
bFwh+eBCsSTRqmwIYYvyw1bhbqoo2DymndFkbjOVIPIldNs/m40KF+yzMn1skyoxcTUGCQs8g3FgD2Ap3ZB5DekAo5wMmk4wimDO+U8QzI3SD  
0""7y2+07w1NwWIt8svngxgdxGkVbbhzY8i+RQ9DpSVpPbF7ykQxtKXkv/ahW3KjviiAH+ghvvIhkx4xYSIc9oSwVmAl50ctMEeWUwg8Istjqz  
8BZeTWbf41fbNhte7Y+YqZ0wq1Sd0DbvYAD9NOZK9v1fuac0598HY+vtSBczUiKERHv1yRbcaQtZfH5wtiRrN04BLUTD21MycBX5jYchHjPY/  
wIDAQAB"
```

SPF

Enable SPF Verification

Message Body or Attachment

Message Body

URL Category

URL Reputation

Message Size

Attachment Content

Attachment File Info

Attachment Protection

Subject Header

Other Header

Envelope Sender

Envelope Recipient

Receiving Listener

Remote IP/Hostname

Reputation Score

DKIM Authentication

SPF Verification

S/MIME Gateway Message

S/MIME Gateway Verified

SPF Verification

Help

What are the SPF Verification results to match?

SPF Verification:

<input type="text" value="Is"/>	<input type="checkbox"/> None
<input type="text" value="Is"/>	<input type="checkbox"/> Pass
<input type="text" value="Is not"/>	<input type="checkbox"/> Neutral
	<input type="checkbox"/> SoftFail
	<input type="checkbox"/> Fail
	<input type="checkbox"/> TempError
	<input type="checkbox"/> PermError

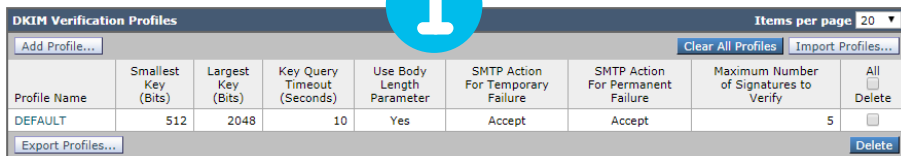
- When SPF is enabled, the ESA will stamp headers in the message
- Use the results inside message or content filters to determine the action
- PRA identities are evaluated in the message filters only
- SPF vs SIDF, an interesting read:
http://www.openspf.org/SPF_vs_Sender_ID

SPF/SIDF Verification:	<input checked="" type="radio"/> Use Default (On) <input type="radio"/> On <input type="radio"/> Off
	Conformance Level: <input type="text" value="Default (SIDF Compatible)"/>
	Downgrade PRA verification result if 'Resent-Sender:' or 'Resent-From:' were used: <input checked="" type="radio"/> Use Default (No) <input type="radio"/> No <input type="radio"/> Yes
	HELO Test: <input checked="" type="radio"/> Use Default (On) <input type="radio"/> Off <input type="radio"/> On

DKIM

Steps to enable DKIM verification

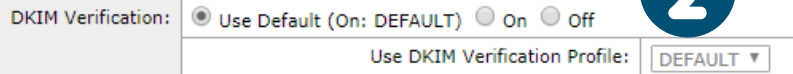
1



Profile Name	Smallest Key (Bits)	Largest Key (Bits)	Key Query Timeout (Seconds)	Use Body Length Parameter	SMTP Action For Temporary Failure	SMTP Action For Permanent Failure	Maximum Number of Signatures to Verify	All Delete
DEFAULT	512	2048	10	Yes	Accept	Accept	5	<input type="checkbox"/>

1. Create profile for action on DKIM
 - Default is Monitor
2. Enable DKIM Verification in Mail Flow Polices.
3. Act on failures via a content filter. Use an action to Policy quarantine to be able to review spoofs.

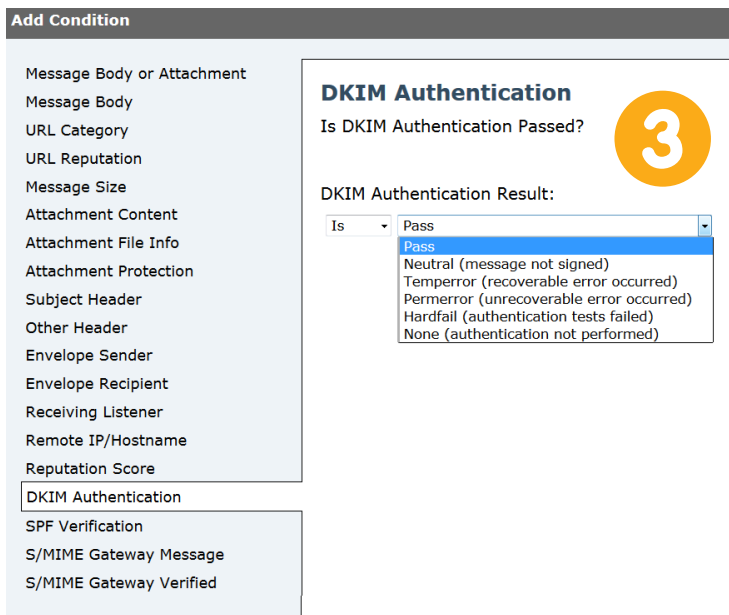
2



DKIM Verification: Use Default (On: DEFAULT) On Off

Use DKIM Verification Profile:

3



Add Condition

- Message Body or Attachment
 - Message Body
 - URL Category
 - URL Reputation
 - Message Size
 - Attachment Content
 - Attachment File Info
 - Attachment Protection
 - Subject Header
 - Other Header
 - Envelope Sender
 - Envelope Recipient
 - Receiving Listener
 - Remote IP/Hostname
 - Reputation Score
- DKIM Authentication
- SPF Verification
- S/MIME Gateway Message
- S/MIME Gateway Verified

DKIM Authentication

Is DKIM Authentication Passed?

DKIM Authentication Result:

Is

- Pass
- Neutral (message not signed)
- Temperror (recoverable error occurred)
- Permerror (unrecoverable error occurred)
- Hardfail (authentication tests failed)
- None (authentication not performed)

After enabling SPF

```
Sun Jan 27 07:01:00 2019 Info: New SMTP ICID 33127 interface Data 1 (216.71.134.24) address
68.183.144.44 reverse dns host mailbot2.teamnorthwind.com verified yes
Sun Jan 27 07:01:00 2019 Info: ICID 33127 ACCEPT SG BYPASSLIST match .teamnorthwind.com SBRS
None country
Sun Jan 27 07:01:00 2019 Info: Start MID 144 ICID 33127
Sun Jan 27 07:01:00 2019 Info: MID 144 ICID 33127 From: <root@gmail.com>
Sun Jan 27 07:01:01 2019 Info: MID 144 ICID 33127 RID 0 To: <boba@carbonitedepot.com>
Sun Jan 27 07:01:01 2019 Info: MID 144 SPF: helo identity postmaster@smtp.teamnorthwind.com
None
Sun Jan 27 07:01:01 2019 Info: MID 144 SPF: mailfrom identity root@gmail.com SoftFail (v=spf1)
Sun Jan 27 07:01:01 2019 Info: MID 144 SPF: pra identity dvader@gmail.com None headers from
```

SPF Record: TXT="gmail.com descriptive text "v=spf1 redirect=_spf.google.com"

- By enabling SPF, you gain additional intelligence on the sender.
- We still accepted the message but can use the verdict later to decide to convict the message.
- Effectiveness is bound by participation – you need to invest time to ensure SPF records are up to date.

Logging additional headers

Global Settings		
System metrics frequency:	60 seconds	
Logging Options:	Message-ID headers in Mail Logs:	On
	Original subject header of each message:	On
	Remote response text in Mail Logs:	On
	Headers:	from, reply-to, cc, authentication-results
Edit Settings...		

```
Sat Jun 17 05:29:54 2018 Info: MID 94398 ICID 188033 From: <kenobi@gmail.com>
Sat Jun 17 05:29:54 2018 Info: Message done DCID 1496 MID 94399 to RID [0] [('from', 'Uncle Ben
<kenobi@gmail.com>')]
```

- Under Log Subscriptions Settings or the logconfig command in the CLI, you can configure additional headers to be logged.
- These will be displayed in the mail_logs and message tracking output upon creation of a DCID (Delivery Connection ID).

Cousin domains and typo-squatting

- It is typically targeted to a specific well-known brand.
- Uses various techniques in the attempt to fool the end user into trusting the sender.
- Will register the domain and create SPF, DKIM and DMARC records.
- Will legitimize the sending host with proper DNS and rDNS records.

Example: cisco.com

Addition: ciscoo.com

Bitsquatting: cicco.com

Homoglyph: c1sco.com

Insertion: ciseco.com

Omission: cico.com

Repetition: cissco.com

Replacement: cizco.com

Subdomain: c.isco.com

Transposition: csico.com

Display name modification

The image shows a Gmail interface. On the left is a sidebar with folders: Compose, Inbox (1), Starred, Snoozed, Sent, Drafts, Categories, and More. The main area shows an email in the Primary tab with the subject 'RE:Shipment status?'. The sender is listed as 'Boba Fett'. A red oval highlights 'Boba Fett' in the sender field. A red arrow points from this oval to a callout box on the right. The callout box contains the text 'RE:Shipment status??' with an 'Inbox x' button, and below it, 'Boba Fett <dvader@gmail.com>', which is also circled in red.

Forged Email Detection (FED)

Header fuzzy matching

1

Dictionaries	
Name	Terms
Executives	Usman Din, Jabba Hutt, Boba Fett (3)

2

Conditions			
Order	Condition	Rule	Delete
1	Other Header	header("authentication-results") == "fail"	
2	▲ Forged Email Detection	forged-email-detection("Executives", 70, "")	

Actions			
Order	Action	Rule	Delete
1	Add Log Entry	log-entry("***Potential BEC attack***)	
2	▲ Quarantine	quarantine("Policy")	

Forged Email Detection on the From: header with score of 100, against the dictionary entry Boba Fett
MID 115 Custom Log Entry: ***Potential BEC attack***

- The idea behind Forged Email Detection is to provide a method to match the Display Name in the From Message header to executives or high-value personnel.
- This feature can help narrow down targeted spoofs, that can leverage any action inside a content or message filter and can also strip the From header to expose the envelope from.
- Using it alone is prone to false positives! Use in conjunction with other conditions.

What are we matching?

- Forged Email Detection focuses on matching the Header From (RFC5322) and specifically the Display Name (i.e **First Last** <user@domain.com>).
- Fuzzy Matching samples:

```
Boba Fett -> Forged Email Detection on the From: header with score of 100
B0ba Fett -> Forged Email Detection on the From: header with score of 89
B.Fett -> Forged Email Detection on the From: header with score of 80
Boba Fettt -> Forged Email Detection on the From: header with score of 95
Bob Fett -> Forged Email Detection on the From: header with score of 94
Boba. Fett -> Forged Email Detection on the From: header with score of 100
```

Getting Started with FED

- FED will only create a log entry for a score that is the same or higher than what is configured.
- Start by creating a filter with a low threshold (50) and log the results for each score above that threshold.
- Enable logging of From and Reply-To headers.

1

Conditions			
Add Condition...		Apply rule: Only if all conditions match	
Order	Condition	Rule	Delete
1	Other Header	header("authentication-results") == "fail"	
	▲ Forged Email Detection	forged-email-detection("Executives", 70, "")	

Actions			
Add Action...			
Order	Action	Rule	Delete
1	Add Log Entry	log-entry("****Potential BEC attack****")	
2	▲ Quarantine	quarantine("Policy")	

2

Message-ID headers in Mail Logs:	On
Original subject header of each message:	On
Remote response text in Mail Logs:	On
Headers:	from, reply-to, cc, authentication-results

Edit Settings...

Forged Email Detection (FED)

Filter example

Before fed()

Boba Fett <dvader@gmail.com>

to boba ▾

After fed()



root@rebellion-hoth-mailserver.teamnorthwind.com

to boba ▾

Strip From header

Conditions			
Add Condition...		Apply rule: Only if all conditions match ▾	
Order	Condition	Rule	Delete
1	Other Header	header("authentication-results") == "fail"	
2	▲ Forged Email Detection	forged-email-detection("Executives", 70, "")	

Actions			
Add Action...			
Order	Action	Rule	Delete
1	Add Log Entry	log-entry("****Potential BEC attack****")	
2	▲ Forged Email Detection	fed()	

- In this example, we look for an auth fail with a FED match.
- By leveraging Forged Email Detection, we can take action to strip the headers and any additional actions that may be required.

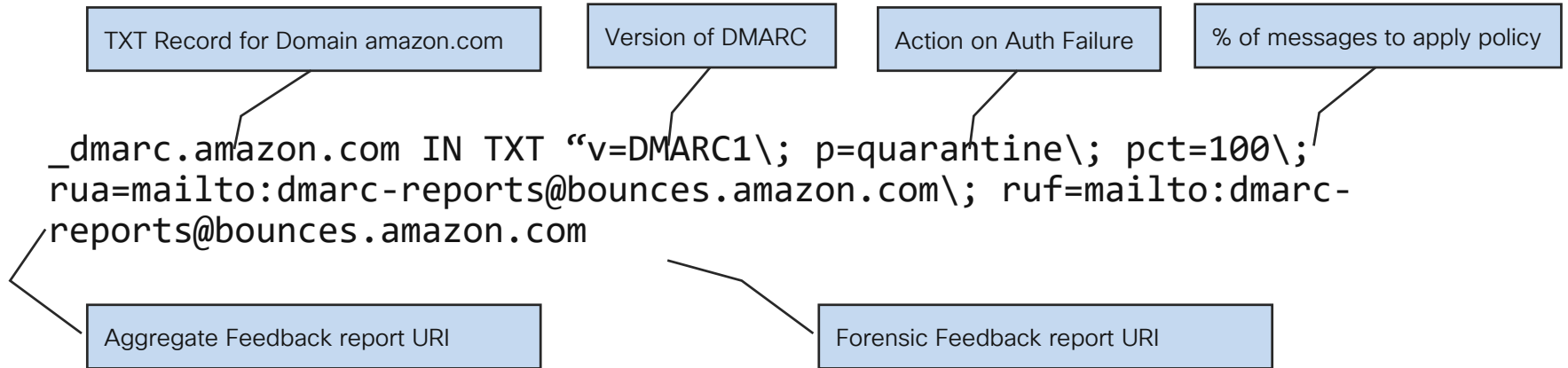
DMARC

How it works

- 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 all sender identities (Envelope From, Header From).**
 - Reporting back to the spoofed entity.

DMARC record structure

How it works



How to enable DMARC (Monitor)

1

DMARC Verification Profiles					Items per page 20
Add Profile...					Import Profiles...
Profile Name	Reject Policy Message Action	Quarantine Policy Message Action	SMTP Action for Temporary Failure	SMTP Action for Permanent Failure	All Delete
DEFAULT	No Action	No Action	Accept	Accept	Delete
Export Profiles...					Delete

2

DMARC Verification	<input type="radio"/> Use Default (On: DEFAULT) <input checked="" type="radio"/> On <input type="radio"/> Off
	Use DMARC Verification Profile: <input type="text" value="DEFAULT"/>
	DMARC Feedback Reports: ? <small>* DMARC reporting message must be DMARC compliant. * Recommended: Enable TLS encryption for domains that will receive reports. Go to Mail Policies > Destination Controls.</small>
	<input checked="" type="checkbox"/> Send aggregate feedback reports

- 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 Sender Groups and move to block when ready.

Honor thy tag

DMARC Verification Profiles					Items per page 20
Profile Name	Reject Policy Message Action	Quarantine Policy Message Action	SMTP Action for Temporary Failure	SMTP Action for Permanent Failure	All <input type="checkbox"/> Delete
BLOCKING	Reject	Quarantine	Accept	Accept	<input type="checkbox"/>
DEFAULT	No Action	No Action	Accept	Accept	<input type="checkbox"/>

v=DMARC1; p=reject; pct=100; rua=mailto:dmarc_y_rua@yahoo.com

```
ICID 33136 From: <anakin@yahoo.com>  
ICID 33136 RID 0 To: <boba@carbonitedepot.com>  
helo identity postmaster@smtp.teamnorthwind.com None  
mailfrom identity root@gmail.com SoftFail (v=spf1)  
pra identity dvader@yahoo.com None headers from  
DMARC: Message from domain yahoo.com, DMARC fail, (SPF aligned False, DKIM aligned False) DMARC  
policy is reject, applied policy is reject  
MID 148 DMARC: rejected by DMARC policy
```

Use DMARC pass/fail as a factor in filters

- DMARC results are stored in the **authentication-results** header.
- This can be leveraged inside a Message Filter or Content Filter if DMARC is not being used to block during the connection phase.
- Use the header results along with other factors such as Geo-Location, Forged Email Detection, etc. to increase the accuracy of a possible threat.

Conditions			
Add Condition...		Apply rule: If one or more conditions match ▼	
Order	Condition	Rule	Delete
1	Other Header	header("authentication-results") == "dmarc=fail"	
2	▲ Forged Email Detection	forged-email-detection("Executives", 70, "")	

Actions			
Add Action...			
Order	Action	Rule	Delete
1	Add Log Entry	log-entry("DMARC FAIL")	



For your review!

Email: Click with Caution
How to protect against phishing, fraud, and other scams

Email: Click with Caution

How to protect against phishing, fraud, and other scams

- Download:
http://cs.co/email_ClickWithCaution

Phishing tips

Protect you and your business

- Security begins with YOU!
- It only takes one wrong click for cyber-criminals to access your company's data.



Phishing tips

Protect you and your business – steps for the end-user

- Avoid strangers, check name and email address
- Don't rush, be suspicious of emails marked "urgent"
- Notice mistakes in spelling and grammar
- Beware of generic greetings, "dear sir/ma'am"
- Don't be lured by incredible "deals"
- Hover over the link before you click to ensure it has a secure URL (https://)
- Never give out personal or financial information based on an email request
- Don't trust links or attachments in unsolicited emails



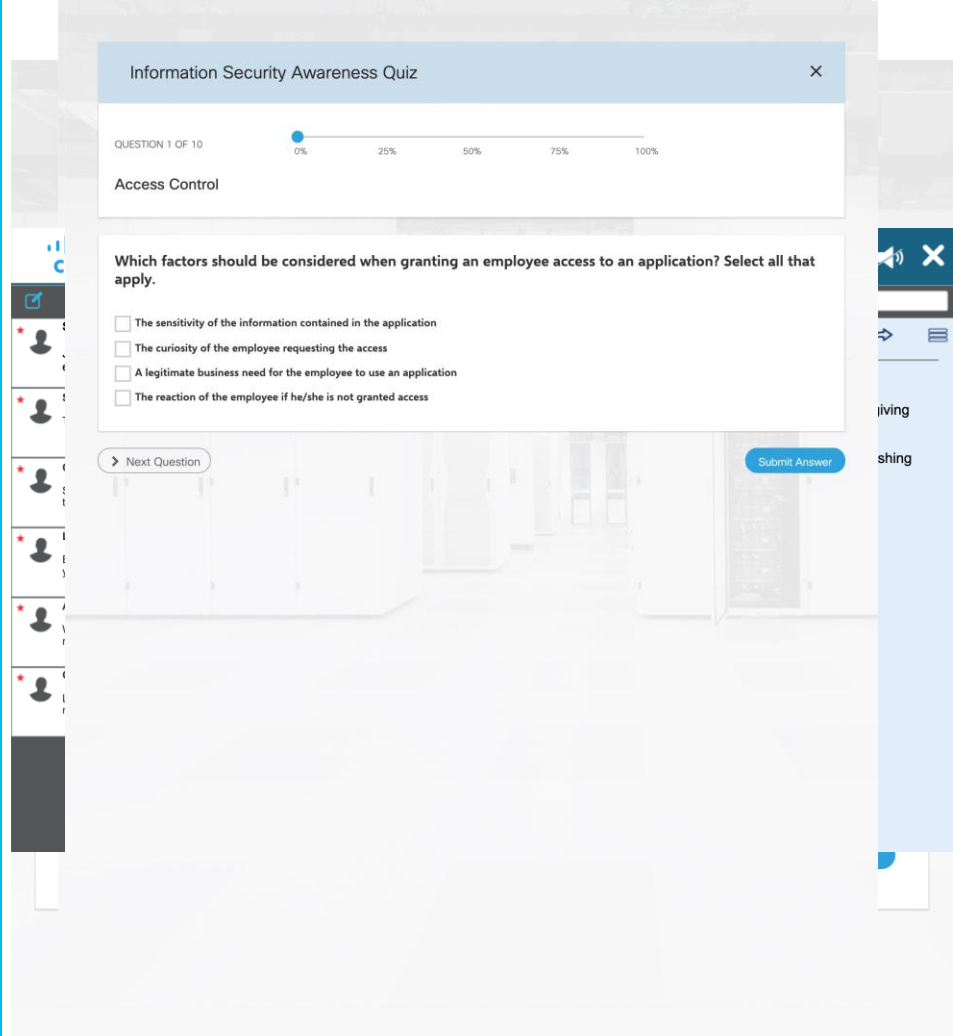
Phishing tips

Training end-users – steps for Email Administrator

- Even with all the controls available, there will be threats that still come though.
- An effective training strategy for end users is important along with the technical controls.
- The technical controls can be extended to end users with the use of in-message banners and notifications.
- Leveraging plug-ins for Outlook can also help train users to be diligent and submit suspicious emails.

Introducing Cisco Security Awareness

- Providing flexibility and support to effectively deploy phishing simulations, awareness training, or both – and measure and report results.
- Empowering security operations teams with the ability to focus on real time threats and not end user mitigation.
- Security training providing the education that helps employees to work smarter and safer.



Cisco Security Awareness

Available in the GLP starting mid-February

- High-quality content is central to any security awareness program and a pre-requisite to provide a training experience that is fun, compelling and relevant.
- Our content is developed by a team of experts using a proven pedagogical approach and methodology for adult learning that ensures the highest degree of engagement.
- Your users will learn about cyber security in a way that expands user knowledge and increases their affinity for your organization to help protect it.

Cisco Security Awareness

Available in the GLP starting end-of-January

Content

- 150+ learning modules
- Micro and nano learning
- Course builder
- Customization of content available
- Role based
- High degree of interaction
- Gamification

Simulation

- Simulation of real threats
- Integrated with training content
- Just in time feedback

Multilingual

- 40+ languages
- Narration + text
- Further customization available

Communication/ Reinforcement

- Internal campaign promotion
- Videos, posters, newsletters

Consultation

- CISO coaching
- Deploy, measure, and report
- Customer success program

Cisco Domain Protection (CDP)

- Protect your brand:
 - Easily analyze, update and act against those misusing your domain to send malicious email.
 - Validate those who use your domain appropriately.
- Automate DMARC authentication:
 - Compliant with new government requirements.
 - Drive to DMARC Enforcement with proven tools and services.
 - Keep records up to date with hosted records.

CDP

Monitoring your senders

- If you have not created SPF or DMARC records, you'll need to implement them in monitoring mode to get an idea of who is sending as your domain.

The screenshot shows the Cisco CDP interface. At the top, there is a navigation bar with the Cisco logo and menu items: Status, Diagnostics, Analyze, Configure, Tools, and Admin. Below this is a section titled 'Verify you are the owner of domains' with a subtitle 'Ensure each domain's DMARC record correctly points to Cisco.' and a help icon. The interface includes a search bar labeled 'Search Domains', a 'Resubmit' button, and buttons for 'Manage DMARC' and 'Download CSV'. A table displays the following data:

<input checked="" type="checkbox"/>	Domain	Verification Status	DMARC	Date Added
<input checked="" type="checkbox"/>	carbonitedepot.com	Failed	No DMARC	2019-01-21

Email Posture

- Because of the feedback loop provided by DMARC, analytics on the number of legitimate vs. spoofed emails can be displayed.
- This information is valuable as most of the information seen is from external recipients sending aggregate reports.

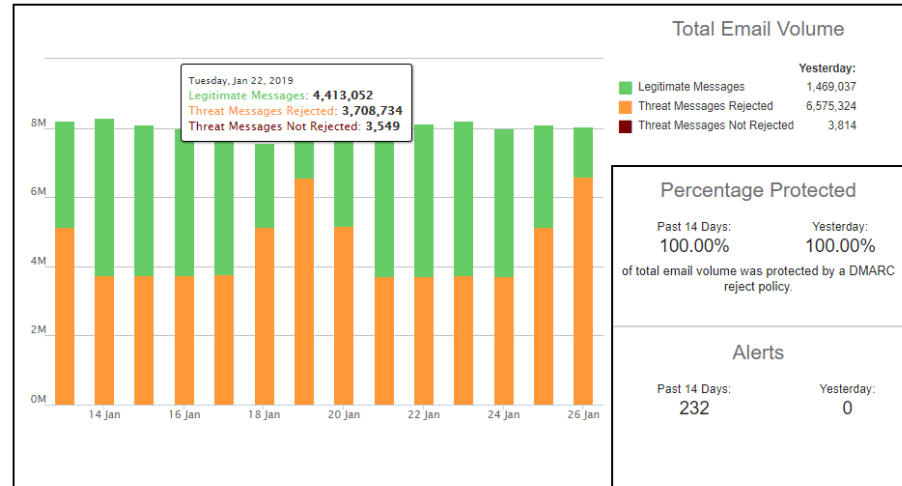
Current Threats 01/26/19 to 01/27/19

Consider the most common subjects and from addresses in current threats.

Recent Occurrences	Subject	From	DMARC Policy
9,753	Account security update please read	"CiscoFunds" <account_security@account.ciscoventurecapital.com>	Reject
1	Account security update please read	"CiscoFunds" <account_security@account.ciscoventurecapital.com>	Reject

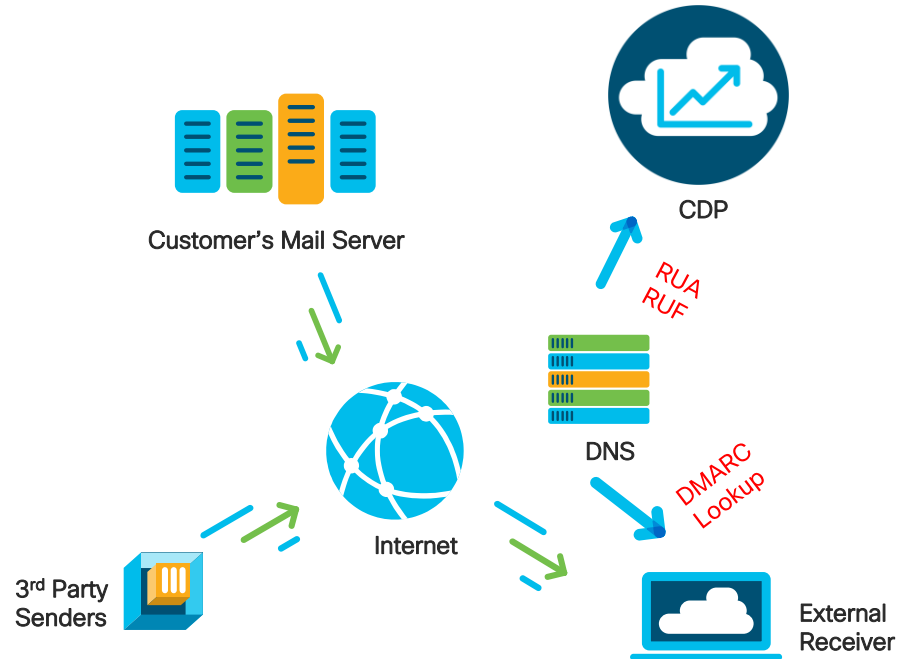
Protection Summary for: All Domains

Analyze the DMARC protection level of the messages sent from your domains.



CDP Deployment

- Cisco Domain Protection (CDP) is designed to identify and protect all of the customers, and it's third party domains that use the customer brand to send an email out to the general Internet. This includes legitimate sending infrastructure owned by the customer, contracted 3rd parties, as well as malicious and unauthorized senders.
- CDP provides workflow tools to understand and remediate authentication problems with legitimate senders. It also provides a mechanism to proactively prevent malicious use of the customer domains by partnering with the most significant email receivers of the world, to prevent malicious mail from ever reaching it's intended targets.



CDP Setup

Creating your records

The screenshot displays the Cisco CDP Setup interface. At the top, there is a navigation bar with the Cisco logo and menu items: Status, Diagnostics, Analyze, Configure, Tools, and Admin. A notification bell icon indicates 'What's New • Filipe L...'. Below the navigation bar, a main heading reads 'Identify your next steps to deploy an... DMARC.' followed by a 'Domain Progress Meter' section. This section includes a 'Verified (12)' tab and a progress bar chart with three categories: 'Configuration Completed' (75%), 'I Am Working On' (17%), and 'Ready To Start' (8%). Below the progress meter are 'To-Dos' and 'Alerts' sections. A dropdown menu is open over the 'Configure' tab, listing options: 'Manage Custom Senders', 'Manage Domains', 'Add Domains', 'Unverified Domains', 'Reports', and 'Whitelists'. A red arrow points from the 'Add Domains' option to a modal dialog titled 'How do you want to add your domains?'. The modal has two radio buttons: 'Type in your domain(s):' (selected) and 'Upload a file of domain names (text or csv):'. The first option has a text input field containing 'testdomainFL.com'. Below this is an 'Advanced Settings' section with a dropdown for 'Add to these Custom Domain Groups:' and checkboxes for 'Mark as Defensive', 'Mark as Third Party', and 'Mark as Primary' (checked). An 'Add your domains' button is at the bottom of the modal.

What's New • Filipe L...

Status Diagnostics Analyze Configure Tools Admin

Identify your next steps to deploy an... DMARC.

Domain Progress Meter

See the progress you have made towards implementing DMARC.

Verified (12)

Category	Progress	Count
Configuration Completed	75%	9 of 12 domains
I Am Working On	17%	2 of 12 domains
Ready To Start	8%	1 of 12 domains

To-Dos

Review the tasks that need to be completed. [View All 14 To-Dos](#)

- Fix DMARC Record for whoissecure.me
- Incorrect DMARC reporting address for jobs.cisconfunds.com
- Incorrect DMARC reporting address for pwm.cisconfunds.com
- Incorrect DMARC reporting address for cisconfunds.com

Alerts

Understand important changes with your domains. [Subscribe](#)

- About 7 hours ago DMARC Record Changed: whoissecure.me. The DMARC record for whoissecure.me has changed.
- About 5 hours ago DMARC Record Changed: whoissecure.me. The DMARC record for whoissecure.me has changed.

How do you want to add your domains?

Type in your domain(s):
Separate each domain name with a comma

Upload a file of domain names (text or csv):
 No file chosen

Advanced Settings

Add to these Custom Domain Groups: [?](#)

Mark as Defensive

Mark as Third Party

Mark as Primary

CDP

Approved & unapproved senders

- To effectively stop spoofing attacks using DMARC, understanding which 3rd parties that send an email on your behalf is mandatory
- CDP automates that process by identifying, tracking, and managing all 3rd party senders.
- Also, CDP maintains governance and helps to identify 3rd party sender risk.

The screenshot displays the Cisco CDP interface for managing email senders. It is divided into two main sections: 'Approved' and 'Unapproved'. The 'Approved' section is currently active.

Well-known Senders

These Well-Known (to Cisco) Senders sent messages on your behalf. When there are multiple domains using a sender, you can view the per-domain breakdown by viewing details. Data shown are based on the top 100 IPs by volume; click the links for additional data where available.

Search:

Sender Name	Domains	Volume	SPF Pass	DKIM Pass
Office 365	dinconsulting.com	0	0%	0%

Sender Profile
✔ SPF Alignment
✔ DKIM Alignment

Displaying 1-1 of 1 Well-Known Senders Previous 1 Next Well-known Senders Per Page: 10

Custom Senders

These senders are either not known to Cisco or are infrastructure within your organization. You can group and label IP addresses in the Unassigned sender group in the [Manage Custom Senders](#) page.

Search:

Sender Name	Domains	Volume	SPF Pass	DKIM Pass
Unassigned	2 (total) teamnorthwind.com & 1 more Details	0	0%	0%

CDP Setup

Moving to Reject

Create and manage your DMARC records

Use this tool to lookup your DMARC records or to create new ones with specific policies.

- 1 Look Up Record
- 2 Create/Modify Record
- 3 View New Record

Enter a domain name to either view its current DMARC record or create a new one.

Domain:

[Look up](#)

There is no DMARC record for testdomainfl.com

[Create new DMARC Record »](#)

[View Hosted DMARC Record @ Cisco »](#)

Domain(s): testdomainfl.com

Policy: Monitor
 Quarantine
 Reject

Send Aggregate Data to:
additional email address (optional)

Send Forensic Data to:
additional email address (optional)

▼ Advanced Settings

Report Format: afrr iodef

DKIM Identifier Alignment: relaxed strict

SPF Identifier Alignment: relaxed strict

Apply to: % of Policy

Reporting Interval: hours

Subdomain Policy:

Forensic Report Options: Send reports for any SPF or DKIM failure
 Send reports only if both SPF and DKIM fail

[« Back](#) [Continue »](#)

DNS-based Authentication of Named Entities (DANE)

- DNS-based Authentication of Named Entities (DANE) is an internet security protocol to allow X.509 digital certificates, commonly used for Transport Layer Security (TLS), to be bound to domain names using Domain Name System Security Extensions (DNSSEC).
- It is proposed in RFC 6698 as a way to authenticate TLS client and server entities without a certificate authority (CA). It is updated with operational and deployment guidance in RFC 7671. Application specific usage of DANE is defined in RFC 7672 for SMTP and RFC 7673 for using DANE with Service (SRV) records.

How DNSSEC Works

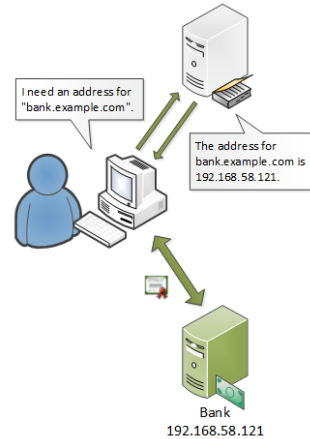
<https://www.internetsociety.org/deploy360/dnssec/basics/>

DNSSEC

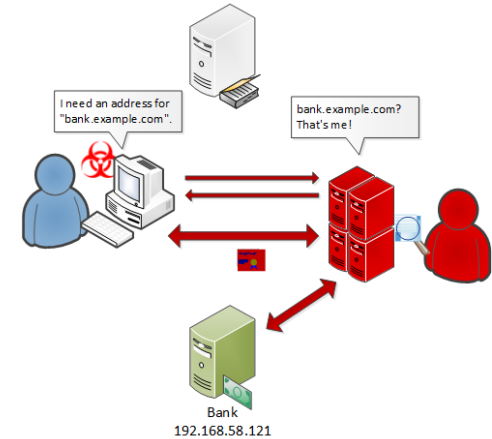
Background

- Conventional DNS is susceptible to man-in-the-middle attacks. A man in the middle can spoof the DNS response, and misdirect the resolver.
- DNSSEC is a secure way to do DNS lookups.
- With DNSSEC, DNS records are signed by the name server and can be authenticated by the resolver.

- Normal:
1. Ask DNS for address of bank's server
 2. DNS gives actual address
 3. Establish secure online banking session at correct IP address



- Hacked:
1. Infected PC asks rogue DNS for address of bank's server
 2. Hacker says he's the bank, so connect to him instead
 3. Hacker stays in the middle of the online banking session, between the user and the real bank server



MTA DANE

- SMTP over TLS between MTAs is susceptible to man-in-the-middle attacks too. The man in the middle can intercept and strip-off STARTTLS, thus making it look like the peer MTA does not support TLS.
- DANE allows a domain to declare its TLS policy out-of-band.
- With DANE, the TLS policy is reflected in a domain's TLSA record secured by DNSSEC.
- If an MTA host for a domain has a secure TLSA record, it shows that the host enforces TLS and the contents of the TLSA record map to the certificate being used for TLS by the host.

ESA support for MTA DANE

- DANE support being added for outbound SMTP connections to peer MTAs. Inbound DANE from peer MTAs, with its own domain being DANE capable, already works.
- DANE support policy configurable per destination domain, or for the DEFAULT set of destination domains.
- DANE support policy configured per domain but applies per host MTA for the domain.
- DANE can be configured to be Mandatory or Opportunistic per destination domain.
- DNSSEC capable DNS server is needed for DANE to work.

```
> daneverify
```

```
Enter the domain to verify DANE support:  
[ ]> huque.com
```

```
SECURE MX record(mail.huque.com) found for  
huque.com
```

```
SECURE A record (50.116.63.23) found for  
MX(mail.huque.com) in huque.com
```

```
Connecting to 50.116.63.23 on port 25.
```

```
Connected to 50.116.63.23 from interface  
139.138.56.31.
```

```
SECURE TLSA record found for MX(mail.huque.com)  
in huque.com
```

```
Checking TLS connection.
```

```
TLS connection established: protocol TLSv1.2,  
cipher ECDHE-RSA-AES256-GCM-SHA384.
```

```
Certificate verification successful
```

```
TLS connection succeeded huque.com.
```

```
DANE SUCCESS for huque.com
```

```
DANE verification completed.
```

DANE configuration

Destination Controls	
Destination:	<input type="text" value="gmail.com"/>
IP Address Preference:	Default (IPv6 Preferred) ▾
Limits:	Concurrent Connections: <input type="radio"/> Use Default (500) <input checked="" type="radio"/> Maximum of <input type="text" value="20"/> (between 1 and 1,000)
	Maximum Messages Per Connection: <input type="radio"/> Use Default (50) <input checked="" type="radio"/> Maximum of <input type="text" value="5"/> (between 1 and 1,000)
	Recipients: <input type="radio"/> Use Default (No Limit) <input checked="" type="radio"/> Maximum of <input type="text" value="20"/> per <input type="text" value="1"/> minutes <small>Number of recipients between 0 and 1,000,000,000 per number of minutes between 1 and 60</small>
	Apply limits: Per ESA hostname: <input checked="" type="radio"/> System Wide <input type="radio"/> Each Virtual Gateway <small>(recommended if Virtual Gateways are in use)</small>
TLS Support:	Default (Preferred) ▾ DANE Support: ? <input type="radio"/> Opportunistic ▾
Bounce Verification:	<input type="text" value="Applies only if bounce verification"/> verification.
Bounce Profile:	Default ▾ <small>Bounce Profile can be configured</small>


DANE Support

- If you configure DANE as 'Opportunistic' and the remote host does not support DANE, opportunistic TLS is preferred for encrypting SMTP conversations.
- If you configure DANE as 'Mandatory' and the remote host does not support DANE, no connection is established to the destination host.
- If you configure DANE as 'Mandatory' or 'Opportunistic' and the remote host supports DANE, it is preferred for encrypting SMTP conversations.


Copyright © 2003-2018 Cisco Systems, Inc. All rights reserved. | [Privacy Statement](#)

- DANE support for policy configurable per-destination domain, or the DEFAULT set of destination domains.
- DANE support for policy configured per-domain but applies per host MTA for the domain.
- It can be configured to be Mandatory or Opportunistic per destination domain.

DANE reporting








 Security Management Appliance Email ▾ Monitoring Tracking Quarantine jolopes ? ⚙️

Reports / [TLS Encryption: Outgoing](#) Data in time range: 99.98% COMPLETE 27 Nov 2017 12:00 to 30 Nov 2018 00:00 (GMT -08:00)

TLS Encryption ▾ View Data For Hosted_Cluster ▾ Time Range Custom Range... ▾ Export 

Incoming Outgoing

TLS Connections Summary

Connection Category	%	Connections
 TLS Required Success	0.00%	0
 TLS Preferred Success	3.70%	36
 TLS Required Failed	0.00%	0
 TLS Preferred Failed	0.00%	0
 Unencrypted Connections	80.27%	781
 DANE Failure	15.42%	150
 DANE Success	0.62%	6

DANE results in Message Tracking

Summary

27 Jan 2019

- 01:00:02 (GMT -08:00) Incoming connection (ICID 137291) has sender_group: SMA, sender_ip: 139.138.56.44 and sbrs: None
- 01:00:02 (GMT -08:00) Protocol SMTP interface Data 1 (IP 139.138.56.31) on incoming connection (ICID 137291) from sender IP 139.138.56.44. Reverse DNS host sma1.hc3033-47.ipmx.com verified ye
- 01:00:02 (GMT -08:00) (ICID 137291) RELAY sender group SMA match sma1.hc3033-47.ipmx.com SBRS None country 139.138.56.44
- 01:00:02 (GMT -08:00) Message 16490 Sender Domain: ces.cisco.com
- 01:00:02 (GMT -08:00) Start message 16490 on incoming connection (ICID 137291).
- 01:00:02 (GMT -08:00) Message 16490 enqueued on incoming connection (ICID 137291) from noreply@ces.cisco.com.
- 01:00:02 (GMT -08:00) Message 16490 direction: outgoing
- 01:00:02 (GMT -08:00) Message 16490 on incoming connection (ICID 137291) added recipient (esa-tme@cisco.com).
- 01:00:02 (GMT -08:00) Message 16490 contains message ID header '<8bb9ea\$6e3fa25=ca5321d809caaa58@sma1.hc3033-47.ipmx.com>'
- 01:00:02 (GMT -08:00) Message 16490 original subject on injection: Cisco Report: Sender Domain Reputation (sma1.hc3033-47.ipmx.com)
- 01:00:02 (GMT -08:00) Message 16490 was released from Spam Quarantine, IP address 139.138.56.44.
- 01:00:02 (GMT -08:00) Message 16490 released from Spam Quarantine. Work queue skipped.
- 01:00:02 (GMT -08:00) Message 16490 queued for delivery
- 01:00:02 (GMT -08:00) MID 16490 (DCID 0) DANE failed for cisco.com. Reason: A record INSECURE.

Phishing

Understanding where URLs are scanned

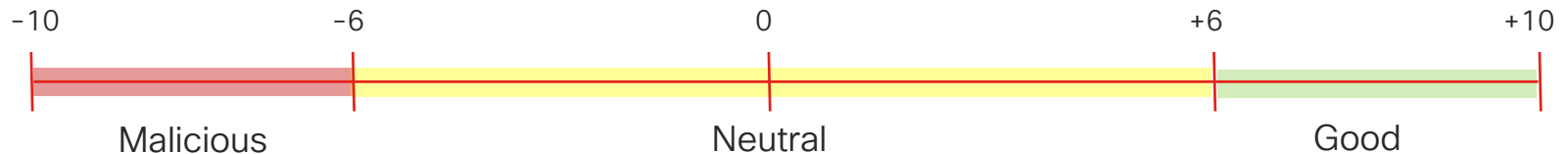
- Cisco Email Security can evaluate URLs inside a message, both for URL Reputation and URL Categorization
- By default, URL Filtering is NOT enabled. You must enable the service and have a valid Outbreak Filter license to perform URL inspection.
- Once enabled, URLs are evaluated in three scanning blades:
 - During IPAS Scan, a URL is used to factor into SPAM scores.
 - Inside a Message Filter or Content Filter configured for Reputation Score and Category.
 - As part of the Threat Outbreak Filter URL Rewrite function.
- URL Filtering also configures Web Interaction Tracking for Clicked URLs, which must be enabled.

Workqueue

- LDAP RCPT Accept (WQ deferred)
- Masquerading (Table/LDAP)
- LDAP Routing
- Message Filters
- (Per-policy scanning)
 - CASE (Anti-Spam)
 - Anti-Virus
 - AMP
 - File Reputation
 - File Analysis
 - Graymail Detection
 - Content Filtering
 - DLP filtering (Outbound)
 - Outbreak Filtering

URL evaluation and options

- The Web Reputation Score (WBRS) uses the same -10.0 to +10.0 score, however it means something very different than SBRS.
- Based on your organizations security posture you can determine how aggressive you wish to be with URL entering your organization.



Enabling URL Filtering

1

URL Filtering Overview	
URL Category and Reputation Filters:	Enabled
Cisco Web Security Services connection status:	Connected
URL Whitelist:	None
Web Interaction Tracking:	Enabled <i>To track URLs due to Outbreak Filter rewrites, you have to enable Web Interaction Tracking at Security Services > Outbreak Filters.</i>
Edit Global Settings...	

Enable URL filtering for URL DB in CASE

Tracking User Clicks of CF/MF re-written URLs

2

Outbreak Filters Overview	
Global Status:	Enabled
Adaptive Rules:	Enabled
Maximum Message Size to Scan:	1M
Receive Emailed Alerts:	No
Web Interaction Tracking	Enabled <i>To track URLs due to Policy rewrites, you have to enable Web Interaction Tracking at Security Services > URL Filtering.</i>
Edit Global Settings...	

Tracking User Clicks of TOF re-written URLs

URL Logging & Tracking

Logging of URLs can be seen in the mail logs and only if:

- Message Tracking must be enabled.
- Outbreak filters and/or content filters based on URL reputation or URL Category must be operational.
- For outbreak filters, URL Rewriting must be enabled.
- URL logging must be enabled in CLI via `outbreakconfig` command.

```
> outbreakconfig
Outbreak Filters: Enabled
Choose the operation you want to perform:
- SETUP - Change Outbreak Filters settings.
[ ]> setup
...
Logging of URLs is currently disabled.
Do you wish to enable logging of URL's? [N]> y
Logging of URLs has been enabled.
...
```

URL Filtering Enablement and Best Practices
<http://cs.co/9002Dcy60>

URL Visibility

- URL information can be shown in message tracking if enabled by role.

Tracking Privileges		
User Roles	View information caught by Data Loss Prevention filters: ?	View details for URLs caught by URL filter: ?
<i>Predefined</i>		
Administrator	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Operator	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Read-Only Operator	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Help Desk User	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<i>Custom Roles</i>		
Cloud Help Desk	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Cloud Operator	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Processing Details

Summary	URL Details
13 Jun 2016 13:15:23 (GMT -04:00)	Message 740 rewritten URL u'http://tara.walletbest.info/jk/j/54/'.

```
Info: MID 3999805 antivirus negative
Info: MID 3999805 AMP file reputation verdict : CLEAN
Info: MID 3999805 using engine: GRAYMAIL negative
Info: MID 3999805 URL http://www.keyfuture.com/ has reputation -7.94499005274 matched url-reputation-rule
Info: Message aborted MID 3999805 Dropped by content filter 'BLOCK URL' in the inbound table
Info: Message finished MID 3999805 done
```

Enabling Shortened URL Expansion

- This feature will allow for URLs that are using a shortening service will be pre-expanded to get base the URLs.
- The ESA will query the service directly to get the base URL.
- Up to 10 redirections/queries will be supported before the URL is marked as malicious.
- This must be enabled via the CLI.

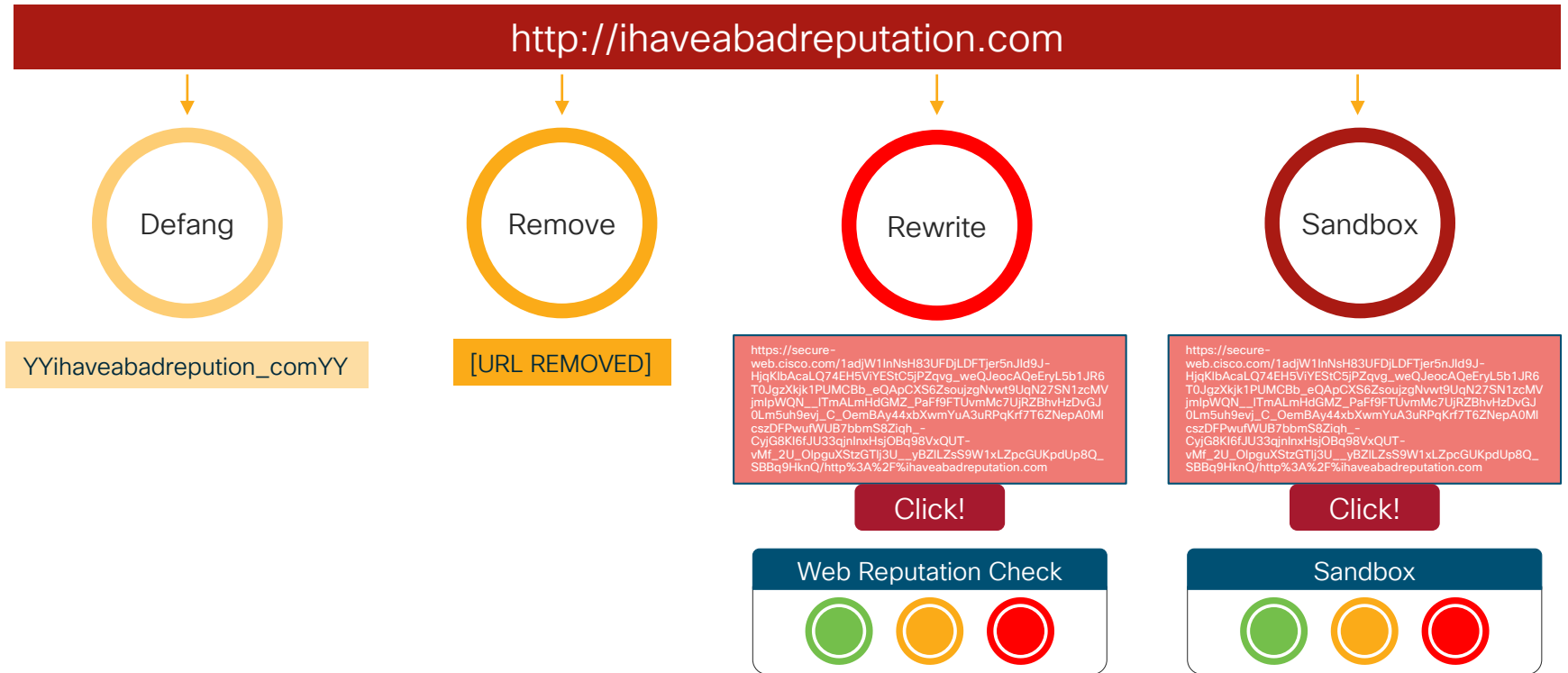
```
websecurityadvancedconfig > Do you want to enable  
URL filtering for shortened URLs? [Y]> Y
```



Services supported (23):


- bit.ly
- tinyurl.com
- ow.ly
- tumblr.com
- formspring.me
- ff.im
- youtu.be
- chatter.com
- tl.gd
- plurk.com
- url4.eu
- j.mp
- goo.gl
- yfrog.com
- su.pr
- wp.me
- post.ly
- tiny.cc
- ustre.am
- tr.im
- ur.ly
- fb.me
- alturl.com


Actions to take on URLs



URL evaluation and options in the message body

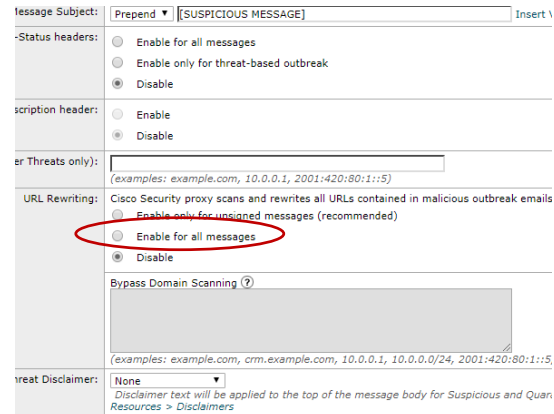
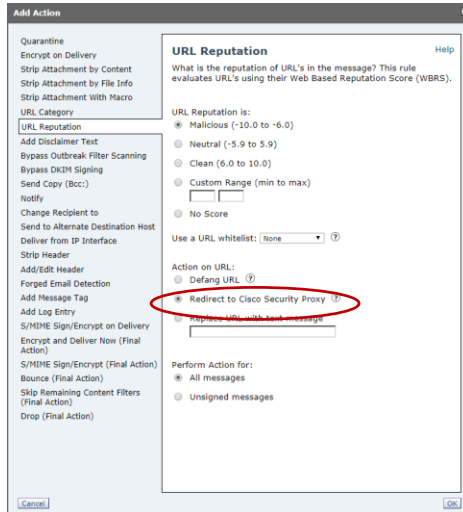
- URL Reputation is assessed inside of the CASE engine and used as part of the decision for Anti-Spam.
- If not stopped as spam, the URL can be evaluated inside a content filter for both Category and Reputation.

Conditions			
Add Condition...			
Order	Condition	Rule	Delete
1	URL Reputation	url-reputation(-10.00, -6.00 , "")	

Actions			
Add Action...			
Order	Action	Rule	Delete
Final	Drop (Final Action)	drop()	

Understanding URL Modification

- URL modification can happen in two places depending on policy settings, inside a Message Filter or Content Filter, and as part of an Outbreak Filter verdict.
- URLs modified by a filter with a re-direct action will only do a reputation check at click time.
- URLs modified by Outbreak Filters will go through a more in-depth inspection, including Malware scanning and AMP in the cloud.



Clean URL Re-writes

- Use the option to do “clean” URL rewrites where only the HREF tag would be rewritten, leaving the email looking unmodified.
- The option is enabled only through the CLI – All URLs refer to both HREF and text; by saying N, it only targets HREF tag.

```
websecurityadvancedconfig > Do you want to rewrite all URLs with secure proxy URLs? [Y]> n
```

Before Clean URL Rewrites:

Hi,

Click on the link below for your special offer!

https://secure-web.cisco.com/1adjW1InNsH83UFDjLDFTjer5nJld9J-HjqKlbAcalQ74EH5ViYEstC5jPZqvg_weQJeocAQeEryL5b1JR6T0JgzXkik1PUJMCBb_eQApCXS6Zsoujzgnvwt9UqN27SN1zcMvjmlpWQN_ITmALmHdGMZ_PaF9FTUvmMc7UjRZBhvHzDvGJ0Lm5uh9evj_C_OemBAy44xbXwmYuA3uRPqKrf7T6ZNepA0MlcszDFPwufWUB7bbmS8Ziqh_-CvjG8Kl6fJU33qjnlxHsjOBq98VxQUT-vMf_2U_OlpguXStzGTij3U_yBZILZsS9W1xLZpcGUKpdUp8Q_SBBq9HknQ/http%3A%2F%randomofferurl.com

After Clean URL Rewrites:

Hi,

Click on the link below for your special offer!

<http://randomofferurl.com>



https://secure-web.cisco.com/1adjW1InNsH83UFDjLDFTjer5nJld9J-HjqKlbAcalQ74EH5ViYEstC5jPZqvg_weQJeocAQeEryL5b1JR6T0JgzXkik1PUJMCBb_eQApCXS6Zsoujzgnvwt9UqN27SN1zcMvjmlpWQN_ITmALmHdGMZ_PaF9FTUvmMc7UjRZBhvHzDvGJ0Lm5uh9evj_C_OemBAy44xbXwmYuA3uRPqKrf7T6ZNepA0MlcszDFPwufWUB7bbmS8Ziqh_-CvjG8Kl6fJU33qjnlxHsjOBq98VxQUT-vMf_2U_OlpguXStzGTij3U_yBZILZsS9W1xLZpcGUKpdUp8Q_SBBq9HknQ/http%3A%2F%randomofferurl.com
Click or tap to follow

URL Categorization & Reputation

- URL Categorization on the ESA leverages the same data as the Web Security Appliance (WSA) and Cloud Web Security (CWS).
- OpenDNS Blocked domain information included in WBRS.
- Use this to compliment Acceptable Use Policies to prevent inappropriate URLs in email.

URL Reputation [Help](#)

What is the reputation of the URL in the message body, subject or the message attachments? This rule evaluates the URL using either the Web Based Reputation Score (WBRS) or using information from the External Threat Feed engine.

Matching Condition

- URL Reputation
 - Malicious (-10.0 to -6.0)
 - Neutral (-5.9 to 5.9)
 - Clean (6.0 to 10.0)
 - Custom Range (min to max)
 - No Score
- External Threat Feeds

Use a URL whitelist: [?](#)

Check URLs within [?](#)

- Message Body and Subject
- Attachments
- All (Message Body, Subject and Attachments)

URL Category [Help](#)

Does the URL in the message body, subject or attachment belong to any one of the selected URL categories?

Available Categories:

Adult	
Advertisements	
Alcohol	
Arts	
Astrology	
Auctions	
Business and Industry	
Chat and Instant Messa	
Cheating and Plagiarism	
Child Abuse Content	
Computer Security	
Computers and Interne	
DIY Projects	
Dating	
Digital Postcards	

Selected Categories:

Use a URL whitelist: [?](#)

Check URLs within [?](#)

- Message Body and Subject
- Attachments
- All (Message Body, Subject and Attachments)

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.

URL Reputation

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

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)
- No Score

Use a URL whitelist: ?

Action on URL:

- Defang URL ?
- Redirect to Cisco Security Proxy ?
- Replace URL with text message

Perform Action for:

- All messages

URLs in Attachments

- Enable lookups in attachments via a Message Filter or Content Filter to perform URL reputation of links in documents.
- Office/OLE objects can be analyzed (i.e., doc, docx, xls, ppt, pdf).
- If a malicious URL is found, action is taken on the message, not just the attachment.
- Default limit of URLs scanned is 25, can be configured via CLI.
- URLs in attachment will not be re-written.

URL Reputation

[Help](#)

What is the reputation of the URL in the message body, subject or the message attachments? This rule evaluates the URL using either the Web Based Reputation Score (WBRS) or using information from the External Threat Feed engine.

Matching Condition

- URL Reputation
 - Malicious (-10.0 to -6.0)
 - Neutral (-5.9 to 5.9)
 - Clean (6.0 to 10.0)
 - Custom Range (min to max)
 - No Score
- External Threat Feeds

Use a URL whitelist: [?](#)

Check URLs within [?](#)

- Message Body and Subject
- Attachments
- All (Message Body, Subject and Attachments)

Structuring rules for URLs in Attachments

Message Body or Attachment
Message Body
URL Category
URL Reputation
Message Size
Message Language
Macro Detection
Attachment Content
Attachment File Info
Attachment Protection
Subject Header
Other Header
Envelope Sender
Envelope Recipient
Receiving Listener
Remote IP/Hostname
Reputation Score
DKIM Authentication
Forged Email Detection
SPF Verification
S/MIME Gateway Message
S/MIME Gateway Verified
Duplicate Boundaries Verification
Geolocation

URL Reputation Help

What is the reputation of URL's in the message? This rule evaluates URL's using their Web Based Reputation Score (WBRS).

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)
- No Score

Use a URL whitelist: ?

Include Attachments
Select this to look for URLs included within the attachments of the message.

Conditions			
Add Condition...			
Apply rule: Only if all conditions match			
Order	Condition	Rule	Delete
1	Reputation Score	reputation <= 0.0	
2	URL Reputation	url-reputation(-10.00, -6.00, "", 1)	

- Reputation lookups are low on resources; however care should still be taken when crafting rules.
- Target attachments from untrusted/unknown sources for further analysis.
- Use message filters to eliminate globally unwanted/restricted file types to reduce the number of files being analyzed.

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.

Global Settings	
Graymail Detection:	Enabled
Maximum Message Size to Scan:	2M
Timeout for Scanning Single Message:	60 seconds
Safe Unsubscribe:	Graymail Safe Unsubscribing is currently disabled. Enable

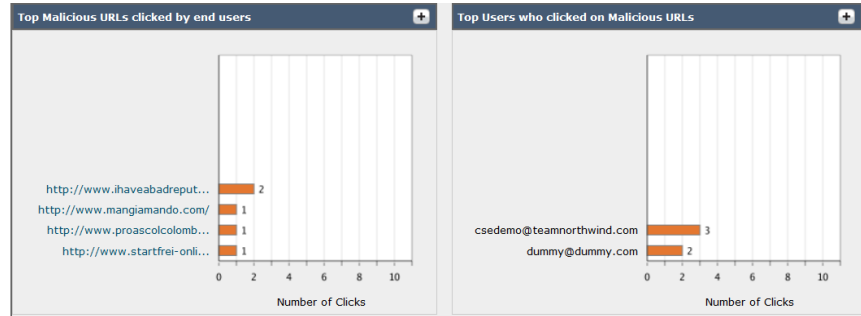
Graymail Settings	
Policy:	DEFAULT
Enable Graymail Detection for This Policy:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable Graymail Unsubscribing for This Policy:	<input checked="" type="radio"/> Yes <input type="radio"/> No
	Perform this action for: <input checked="" type="radio"/> All Messages

Graymail Unsubscribe



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).



Web Interaction Tracking

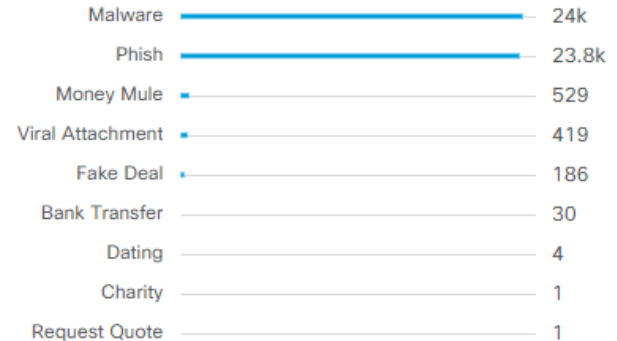
URL Clicked:
(example: http://www.domainname.com)

Mail Flow Direction: Incoming Outgoing

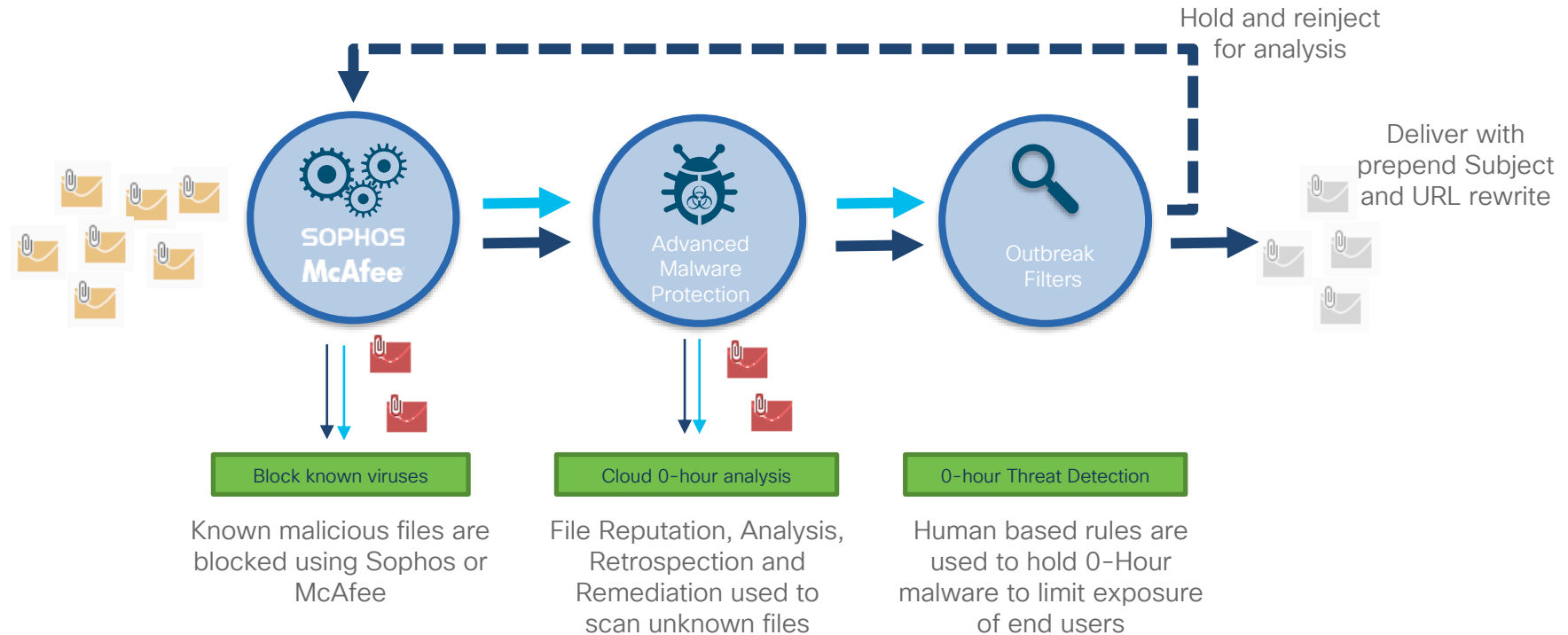
Phishing is not just URLs

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

Threats by Type



Dynamic/Delay Quarantines



Threat Outbreak Filters


Default Policy	IronPort Anti-Spam Positive: Quarantine Suspected: Quarantine	Sophos Encrypted: Deliver Uncannable: Deliver Virus Positive: Drop	File Reputation Uncannable: Deliver Malware File: Drop Pending Analysis: Quarantine MAR Action: Delete ...	Graymail Detection Marketing: Deliver Social: Deliver Bulk: Deliver	FED_LOGHEADER	Retention Time: Virus: 1 day Other: 4 hours
----------------	---	---	---	--	---------------	---

- 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).

The screenshot shows the configuration interface for Message Modification. The 'Enable message modification' checkbox is checked and circled in red. Below it, the 'Message Modification Threat Level' is set to 3. The 'Message Subject' field contains 'Prepend - [[SUSPICIOUS MESSAGE]]'. There are three sections with radio button options: 'Include the X-IronPort-Outbreak-Status headers' (set to Disable), 'Include the X-IronPort-Outbreak-Description header' (set to Disable), and 'Alternate Destination Mail Host (Only for threats only)' (empty). The 'URL Rewriting' section is circled in red and has 'Enable for all messages' selected. The 'Bypass Domain Scanning' checkbox is unchecked.

Preventing Data from leaving

- There will always be a patient 0, nothing will block all incoming phishing attempts.
- We can put in rules to block, quarantine or encrypt data that is leaving that is sensitive using Cisco Data Loss Prevention (DLP) or Content Filters.
- Content Filters can detect based on regular expression, dictionary of keywords and combined with destination domains.

Policies									
Add Policy...									
Order	Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters	DLP	Delete
1	HR SENDERS	(use default)	(use default)	(use default)	(use default)	(use default)	(use default)	HR SSN POLICY	
	Default Policy	Disabled	Sophos Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	File Reputation Unscannable: Deliver Malware File: Drop Pending Analysis: Deliver	Disabled	Disabled	Disabled	DEFAULT SSN POLICY	

Phish & Spoofing Checklist

- ❑ Enable URL Filtering on the ESA
- ❑ Enable Web Interaction Tracking (if permitted by policy)
- ❑ Enable certain admin user's 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

Cisco Advanced Phishing Protection (CAPP)



Who is sending the email?

What Identity is being claimed here?

Who does this sender claim to be?

The science behind it – a phishing attack

The screenshot displays an email client interface with the following details:

- Date:** 31-Jan-2018 15:30:40 EST
- From:** DocuSign Inc <dse@dse.com>
- Reply-To:** dse@dse.com
- To:** [Redacted]
- Subject:** Your document Receipt 03142 for [Redacted] is ready for signature!
- Message ID:** <CC214880.FD9626EB@dse.com>

Message Trust Score: 0.5 (Untrusted)

- Low Trust Domain: dse.com is not a trusted domain
- This message was moved to the folder 'Junk Email'.
- Matched policies: PROD: Low Trust, PROD: Zero-Day, PROD: Low SBRS

Message Trust Score Reasons

- Authenticity Score:** 0.1 (Very low Authenticity Score)
- MAIL FROM:** dse.com
- DKIM 'd=' tag:** none
- Authentication result:** No SPF record for the domain, Not DKIM signed, DMARC check unavailable
- Sending Domain:** dse.com
- Domain Reputation:** 0.5 (Likely Zero-Day Domain, No Consistent Sending History)
- Sending IP Address:** 24.229.13.112 – (cpe-static-raysautorepair-rtr.cmts.mlf.ptd.net)
- SBRS:** -5.3 (Very low SBRS)

Search for similar messages

OK

The science behind it – a legitimate email


Date: 11-May-2017 11:26:17 EDT ⓘ

From: "DocuSign" <docusign@docusign.com>

Reply-To: docusign@docusign.com

To: egiammona@agari.com

Subject: Live Webinar: Turbocharge How You Use Salesforce (final reminder)

Message ID: <0abbc2b251b14182aed99ac48fa9d8b0@566810826> 

Message Trust Score: 6.7 (Trusted)

✓ Authentic mail from highly trusted domain

Message Trust Score Reasons

Authenticity Score: 1.0	Sending Domain: docusign.com
✓ Very high Authenticity Score	Domain Reputation: 6.7
MAIL FROM: esign.docusign.com	Sending IP Address: 204.92.114.26 — (mail03.esign.docusign.com)
DKIM 'd=' tag: docusign.com	SBRS: 3.5
Authentication results:	✓ Very high SBRS
✓ SPF Pass	✓ IP address is in Sender Model for this domain
✓ DKIM Pass	
✓ DMARC Pass	

CAPP Policies

- Policies can be used to report and take actions on messages that been found to be malicious.
- Multiple policies based on Subject, To/From addresses, and verdicts of the email can be created.
- Actions such as move or delete, can be taken.

Policies

Policies

On-Demand Policies System Notifications Policy Log

Configure Policies based on message content.

[Create Policy](#) [Configure Policy Text for Original Recipients](#)

Show policies:

Displaying 1 - 9 of 9 Policies

Name	Conditions	Enabled?	Action	Notify Recipients?	Last Triggered	Number of Times Triggered (in last 7d) ↓
Low Message Trust and Low Server Reputation	<ul style="list-style-type: none">• Message Trust Score is between 0.0 and 2.5• SBRS is between -10.0 and -2.0	Y	Delete	Y	19-Jun-2018 21:45:50 UTC	2
Demo	<ul style="list-style-type: none">• To: address:<ul style="list-style-type: none">◦ contains scbowser• Sending Domain is cisco.com	Y	Move	N	Never	0
[Demo] - Quarantine on Subject	<ul style="list-style-type: none">• Subject: contains Quarantine on Subject	Y	Move	N	Never	0
subject test	<ul style="list-style-type: none">• Subject: contains subject match test very specific	Y	None	N	Never	0
Rapid DMARC (Manage Senders)	<ul style="list-style-type: none">• Domain's Tags include internal• Authenticity Score is between 0.0 and 0.4	Y	None	N	Never	0
Executive Imposters	<ul style="list-style-type: none">• From: address:<ul style="list-style-type: none">◦ matches a Display Name in Executives	Y	None	N	Never	0

CAPP Enforcement

- Enforcement is done through API calls
- Office 365 is supported through the Graph API and on-prem Exchange through the EWS API
- Message trajectory is found through journaling of emails which allows for metadata to be collected on the message

The screenshot shows the CAPP enforcement interface. At the top, a red circle highlights the "Enforce selected" button, and a yellow box highlights the "1 messages selected. Select all 21 messages. Cancel" text. Below this is a table of messages with columns for "Enforced?", "Trust Score", "Date", and "Subject". The first row has a checked "Enforced?" checkbox (circled in red) and a "Trust Score" of 1.5 (boxed in red). A dialog box titled "Enforce Now" is open, asking "Enforce 1 selected messages immediately?". The "Enforcement action:" dropdown is set to "Move to folder 'Cisco APP'", and a "Delete" option is highlighted in blue.

Enforced?	Trust Score	Date	Subject
<input checked="" type="checkbox"/>	1.5	20-Jun-2018	Hello Robert
<input type="checkbox"/>	1.6	20-Jun-2018	[BULK] Would you like to receive emails from Cisco on Mailgun?
<input type="checkbox"/>	1.6	20-Jun-2018	Congrats! is now verified
<input type="checkbox"/>	4.1	20-Jun-2018	[MARKETING] [Live Webinar] Best Practices for Mitigating Web Risks
<input type="checkbox"/>	4.8	20-Jun-2018	Re: Robert - Demisto Community!
<input type="checkbox"/>	5.7	20-Jun-2018	Trial Registration Confirmation



Separating the trees from the forest

Overview - Dashboard

4,794
Top Sending Domains

582
Enforced Messages

577 Moved
5 Deleted

31
Individual Display Name Impostors

11
Brand Display Name Impostors

1
Compromised Accounts

126
Domain Spoofs

21
Look-alike Domains

2.18 K
Spam or Graymail



Separating the trees from the forest

Overview - Dashboard

4,794

Top Sending Domains

582

Enforced Messages

577 Moved

5 Deleted

Show messages...

31

Individual Display Name Impostors

11

Brand Display Name Impostors

1

Compromised Accounts

126

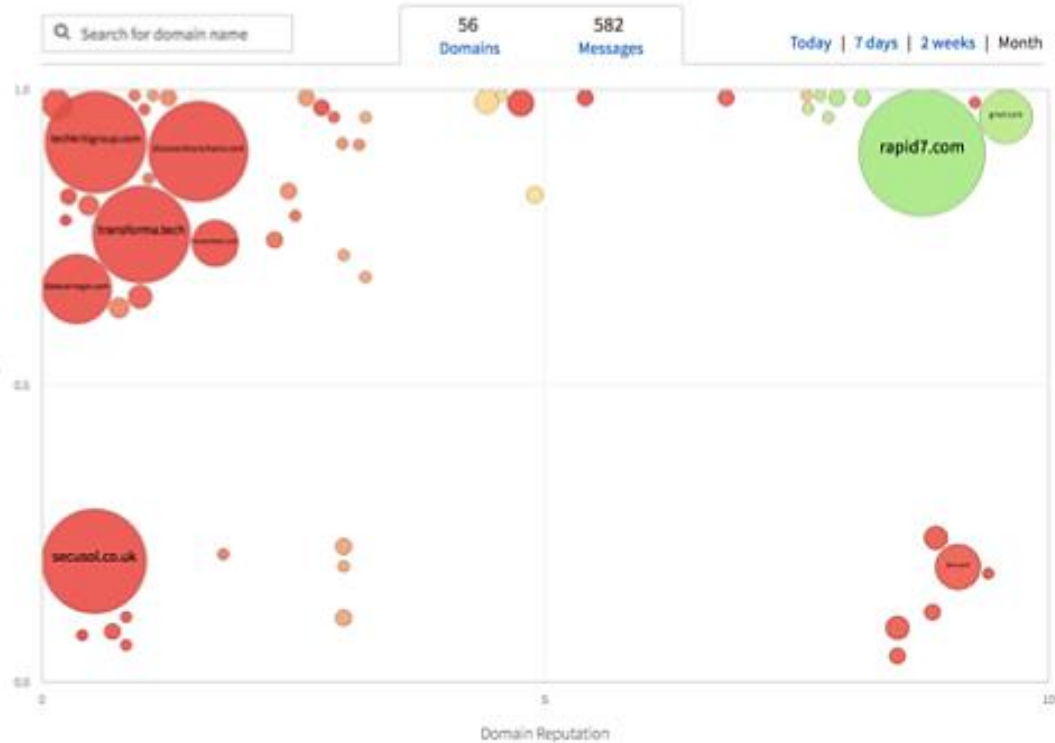
Domain Spoofs

21

Look alike Domains

2.18 K

Spam or Graymail





Defensive Configuration: Attachment Control & Defense

Block the unwanted file types

- Within either a Message Filter or a Content 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 to evade file blocking.

Attachment File Info [Help](#)

Does the message contain an attachment of a filetype matching a specific filename or pattern based on its fingerprint (similar to a UNIX file command)? Does the declared MIME type of an attachment match, or does the IronPort Image Analysis engine find a suspect or inappropriate image? Is the attachment corrupt?

- Filename:**
Contains *
- Filename contains term in content dictionary:**
PHISH_KEYWORDS
- File type is:**
Is Compressed
 - ole
 - pdf
 - ppt, pptx
 - pub
 - rtf
 - torrent
 - wps
 - x-wmf
 - xls, xlsx
 - Executables
 - exe
 - java
 - mrc
 - msi
 - pif
 - sis
 - Images
 - bmp
 - cdr
 - cr2
- MIME type:**
Is
- Image Analysis:**
This condition is unavailable because the feature for Image Analysis is unavailable. See the IronPort Security Center documentation for more information.
- Attachment Content:**
(*) accepts regular expressions

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:

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

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

Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters
(use default)	Disabled	(use default)	(use default)	(use default)	(use default)
(use default)	Disabled	(use default)	(use default)	(use default)	(use default)
IronPort Anti-Spam Positive: Quarantine Suspected: Quarantine	Sophos Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	File Reputation Unscannable: Deliver Malware File: Drop Pending Analysis: Quarantine MAR Action: Delete ...	Graymail Detection Unsubscribe: Enabled Marketing: Deliver Social: Deliver Bulk: Deliver ...	FED_LOGHEADER FED_STRIPHEADER LOG_URL BLOCK_URLS BLOCK_FILETYPES ...	Retention Time: Virus: 1 day Other: 4 hours

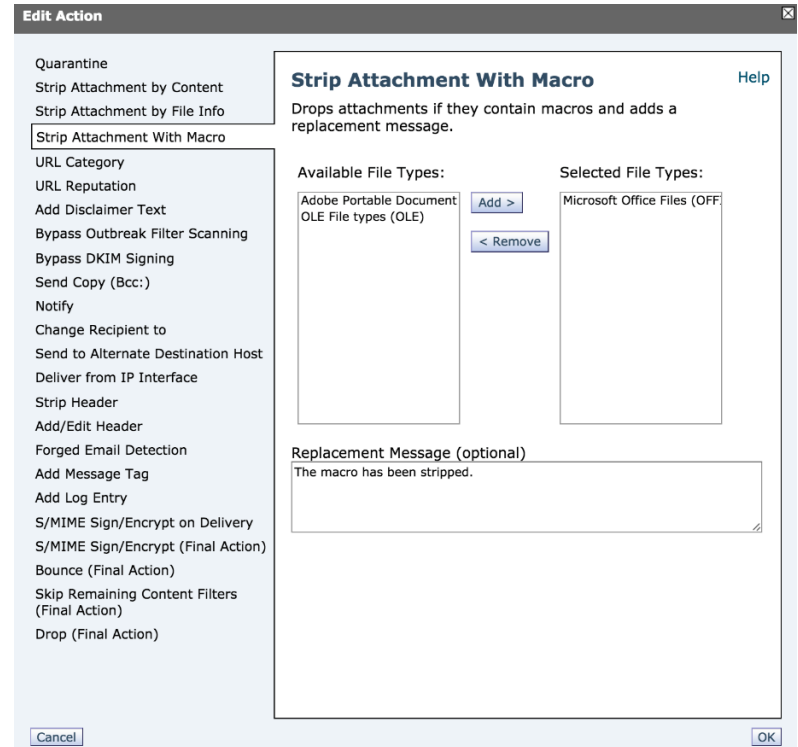
Workqueue

- LDAP RCPT Accept (WQ deferred)
- Masquerading (Table/LDAP)
- LDAP Routing
- Message Filters
- (Per-policy scanning)
 - CASE (Anti-Spam)
 - Anti-Virus
 - AMP
 - File Reputation
 - File Analysis
 - Graymail Detection
 - Content Filtering
 - DLP filtering (Outbound)
 - Outbreak Filtering

Macro

Macro Detection

- Macro enabled document detection allows Message or Content Filters to detect a condition and act for email attachments containing macros or scripts and take the actions of:
 - Quarantine the message
 - Strip the attachment
 - Strip the attachment and add notification text to the message body
 - Modify the subject
 - Add header
 - Forward to another address



Content Filters

Combine factors for effective blocking

Conditions			
Add Condition...		Apply rule: Only if all conditions match	
Order	Condition	Rule	Delete
1	Geolocation	geolocation-rule (['Canada'])	
2	▲ Macro Detection	macro-detection-rule (['Adobe Portable Document Format', 'Microsoft Office Files', 'OLE File types'])	

Actions			
Add Action...			
Order	Action	Rule	Delete
1	Quarantine	quarantine("Policy")	

Think about conditions:

- X-headers that were stamped
- Verdicts from other engines
- Reputation Score of the Sender
- Reputation score of the URL
- Geo-location
- Etc..

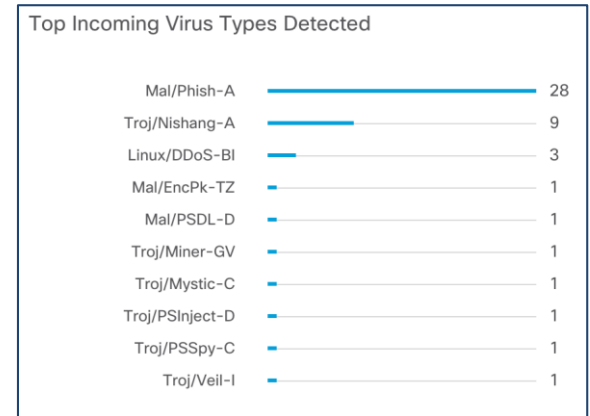
- Use a combination of source and content to create security rules that fit your organizations security posture.
- Can be done inside a message or content filter.
- Combine actions to quarantine and notify or send the message without the attachment to user.

Anti-virus

Sophos and McAfee

Default Policy	IronPort Anti-Spam Positive: Quarantine Suspected: Quarantine	Sophos Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	File Reputation Unscannable: Deliver Malware File: Drop Pending Analysis: Quarantine MAR Action: Delete ...	Graymail Detection Marketing: Deliver Social: Deliver Bulk: Deliver	FED_LOGHEADER	Retention Time: Virus: 1 day Other: 4 hours
----------------	---	---	--	--	---------------	---

- Sophos comes bundled with the licenses, enable and block known viruses. (McAfee is available for \$ license.)
- What are Encrypted Messages?
 - Attachments that are password protected or signed
- What are Unscannable Messages?
 - Messages with attachments that are too large to scan or malformed.
- *Do you still repair?* Most customers today do not have the repair option enabled for virus infected messages.

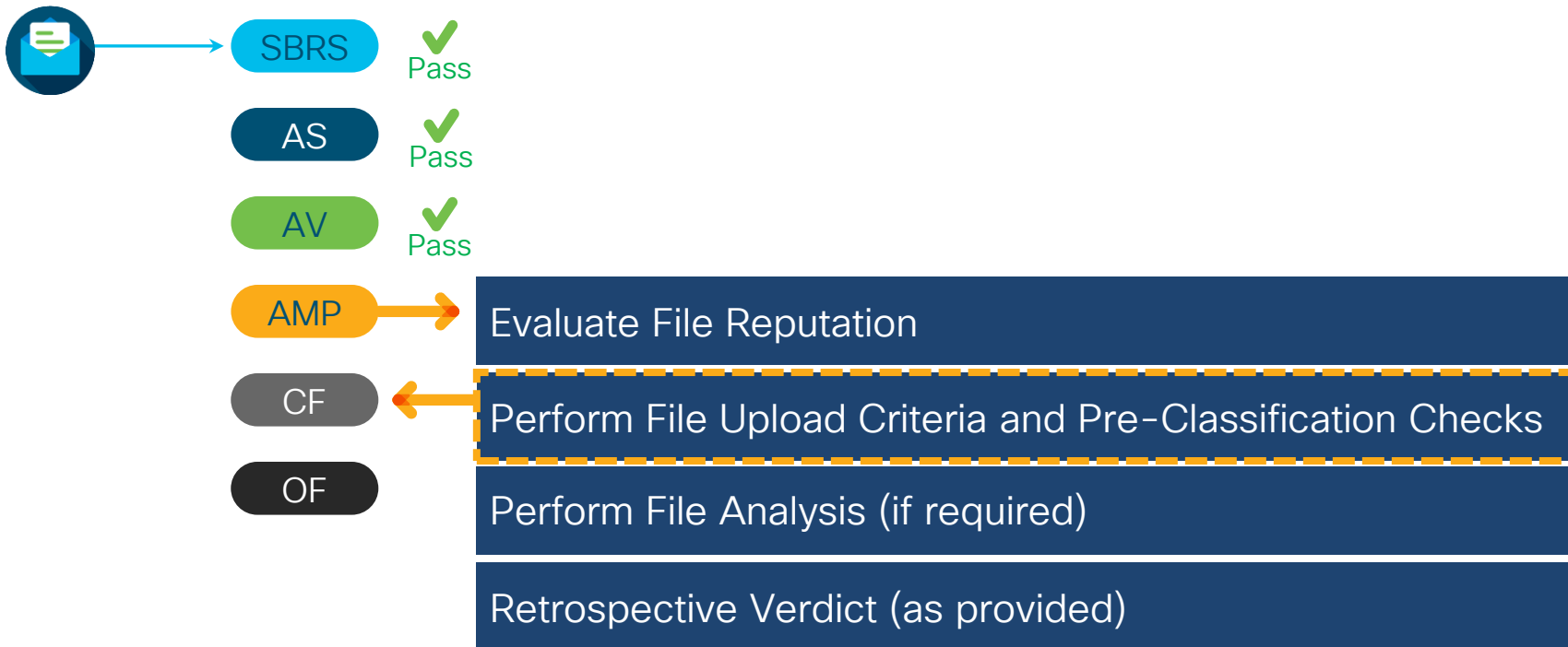




Let's dive deeper into...
Advanced Malware Protection (AMP)

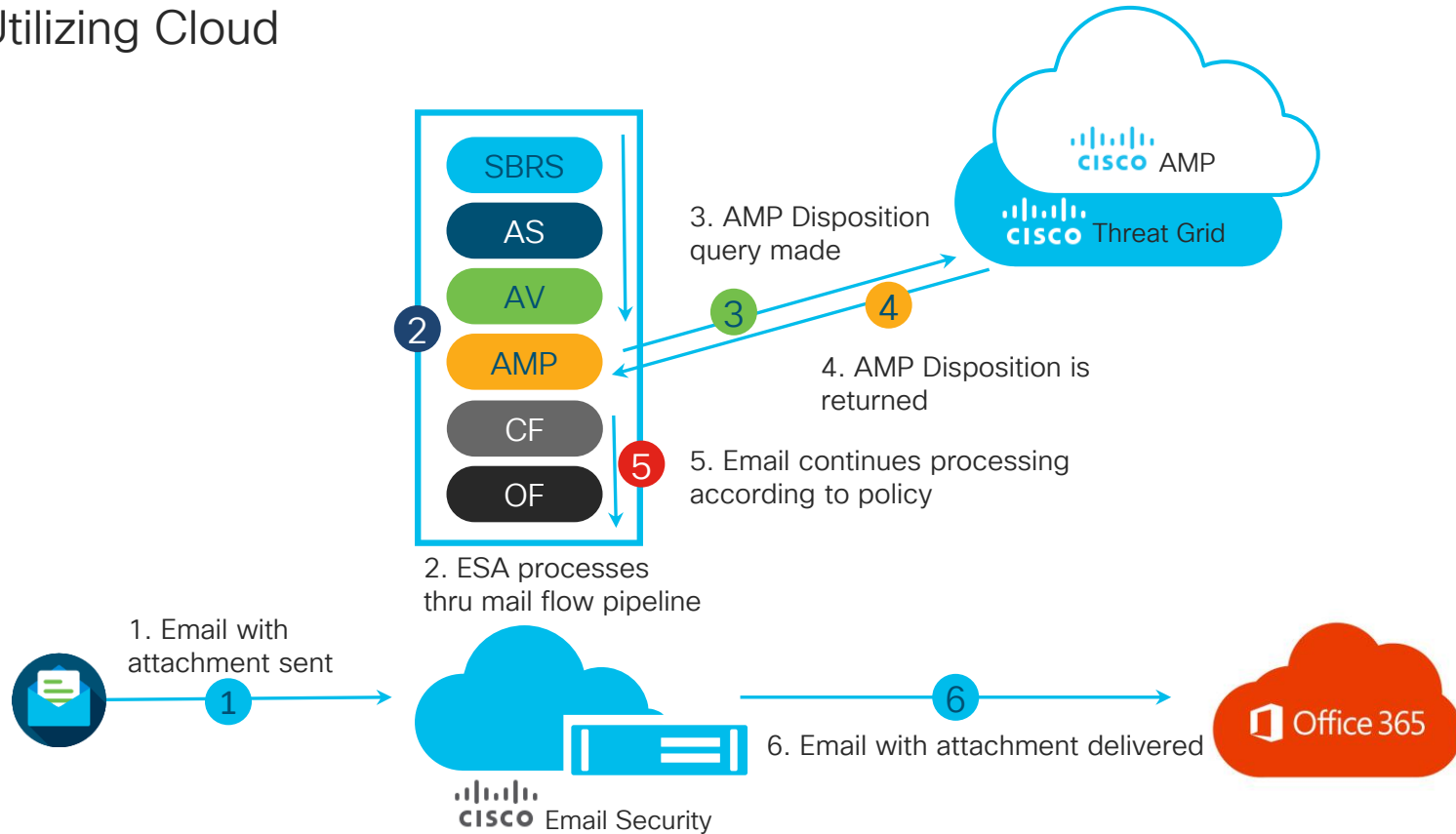
How AMP Works

AMP Order of Processing



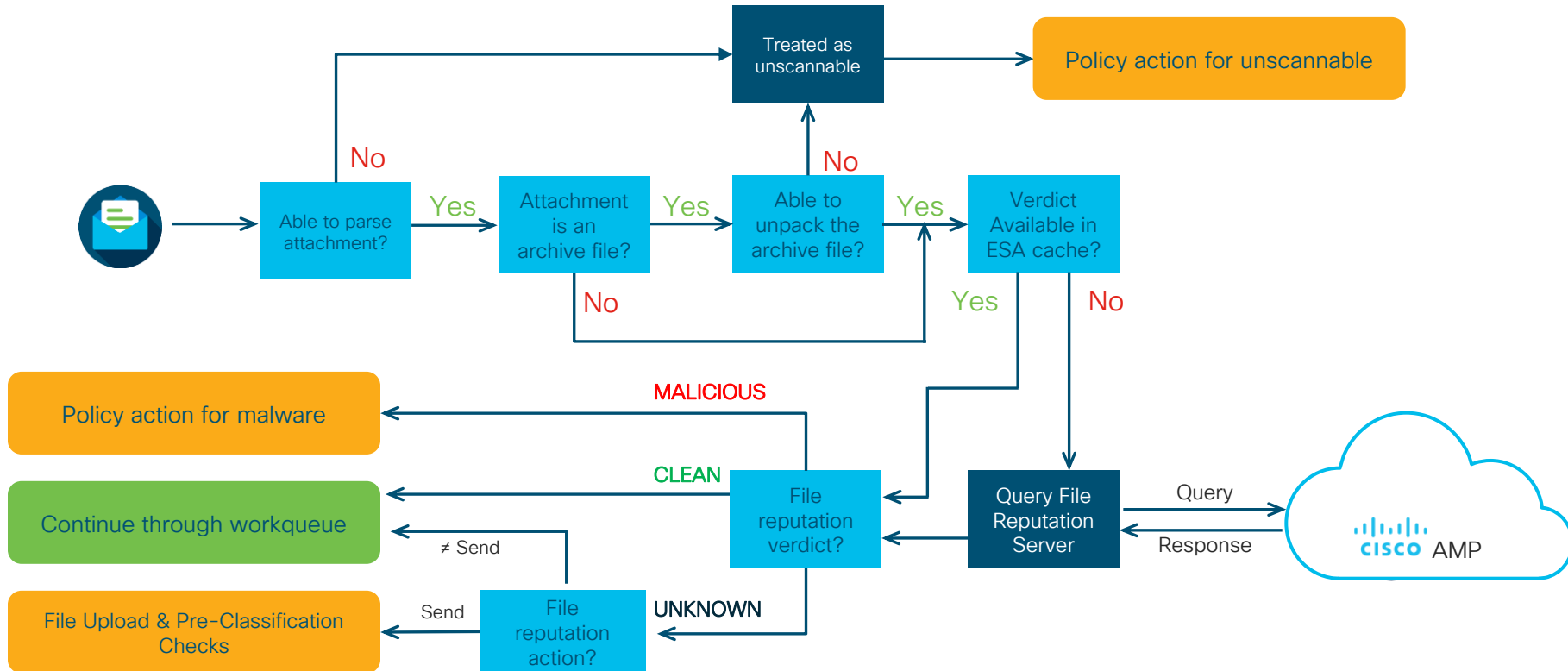
AMP & Threat Grid Process Flow

Utilizing Cloud

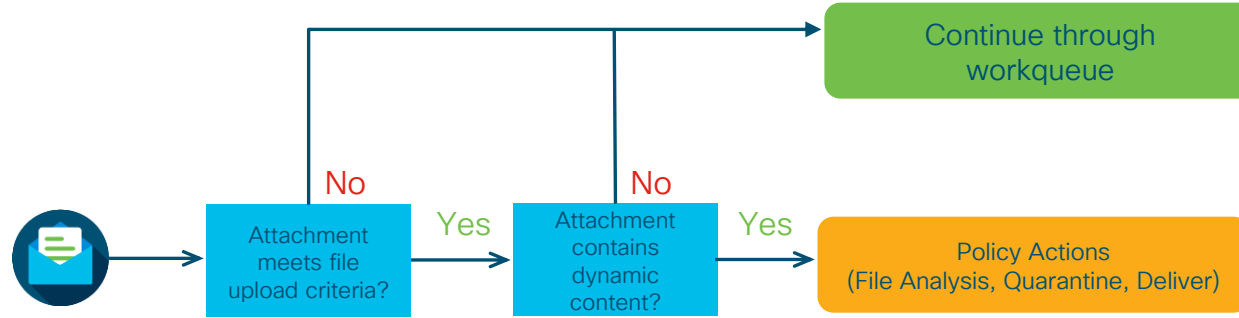


AMP (File Reputation) Workflow

Utilizing Cloud



File Upload Criteria & Pre-Classification Check Workflow



File Upload Criteria:

- Supported File Types
- Attachment size \leq 100 MB

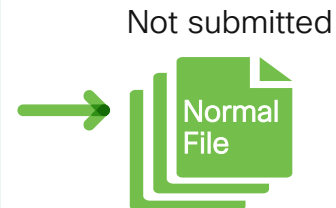
AMP on ESA

File Pre-classification

ClamAV Pre-classifier

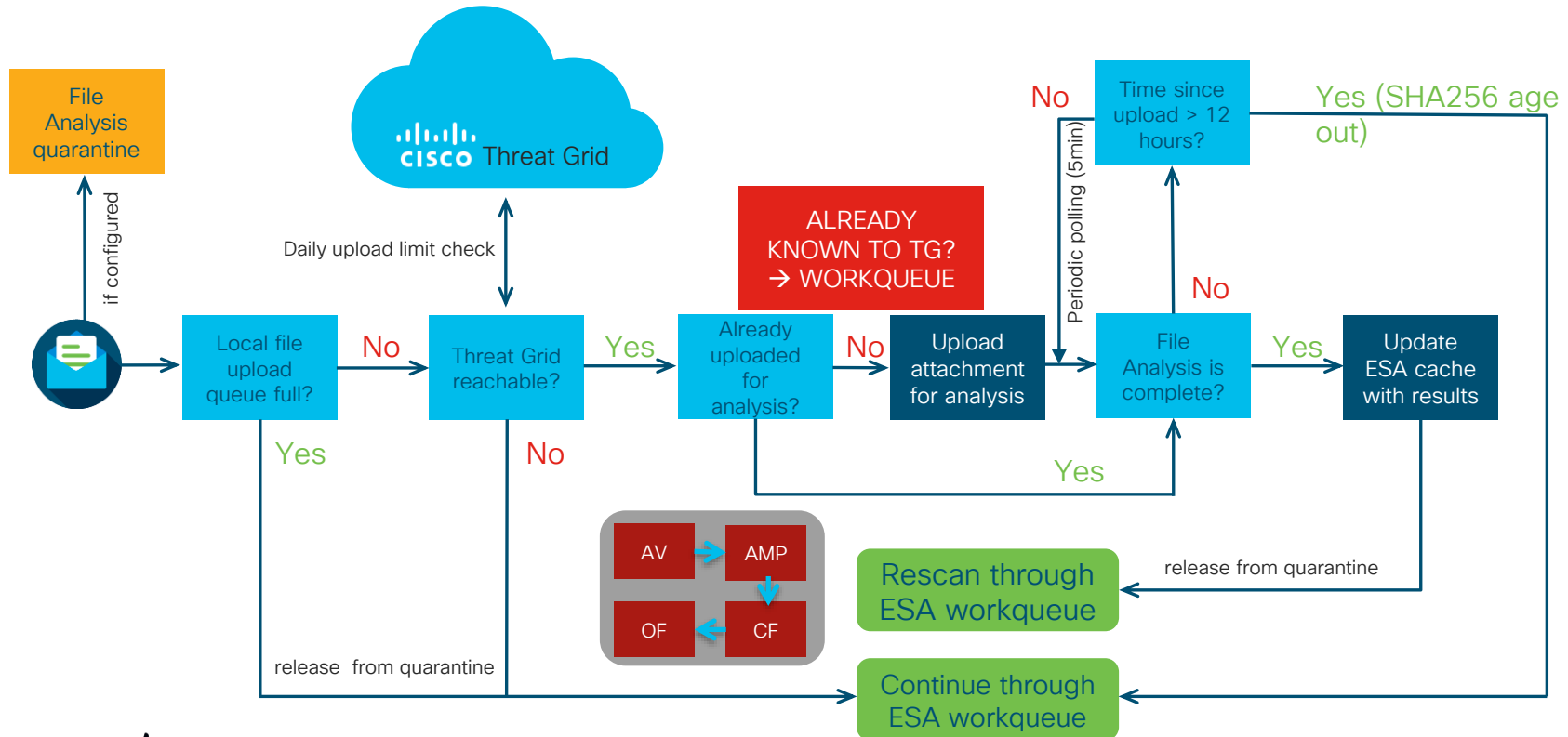


- CL_TYPE_EXE,
- CL_TYPE_UNKNOWN,
- CONTAINS_EMBEDDED_EXE,
- CONTAINS_EMBEDDED_HTML,
- CONTAINS_EMBEDDED_MACROS,
- CONTAINS_FLASH_OBJECT,
- CONTAINS_NUMEROUS_OBJECTS,
- EXE_ABNORMAL_ENTRYPOINT,
- EXE_NUMEROUS_SECTIONS,
- EXE_PACKED,
- EXE_PARSER_FAILURE,
- JSON_INACTIVE,
- OLE_MACRO,
- OLE_PARSE_ERROR,
- OLE_VBA,
- PDF_ACRO_FORM,
- PDF_BAD_TRAILER,
- PDF_JAVASCRIPT,
- PDF_NO_EOF,PDF_OPEN_ACTION

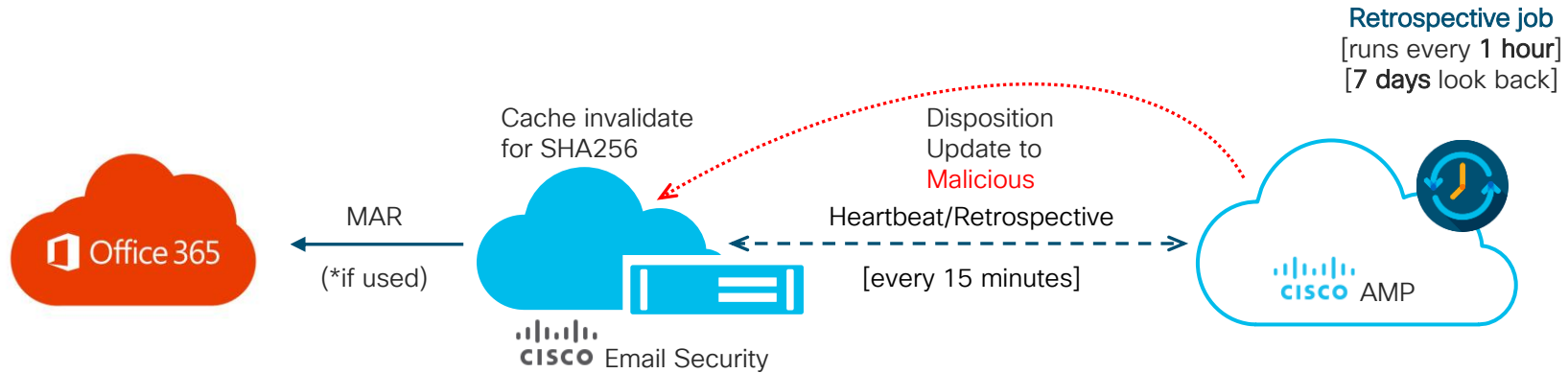


Threat Grid (File Analysis) Workflow

Utilizing Cloud



Retrospective Verdict Workflow



Retrospective verdict received for eicar2.pdf.

```
SHA256: c621544ac86f79f111de866b5e0c2ac272bfb09fcda1bf03b064037a7bf46751
Timestamp: 2017-04-13T10:33:35Z
Verdict: MALICIOUS
Reputation Score: 0
Spyname: Auto.C62154.201750.in02
Total users affected: 1
```

AMP Retrospection Alerts

Two (2) styles of alerts now generated by AMP for retrospective events:

Change in disposition, message not delivered

The Info message is:
Retrospective verdict received.
SHA256:
7c48eb3b1fea5705fc70539f2a0539a3be794d6b70408a31c9ea461855657cd0
Timestamp: 2016-09-19T19:39:13Z
Verdict: MALICIOUS
Reputation Score: 0
Spyname: W32.Auto:7c48eb3b1f.in05.Talos
Version: 10.0.0-124
Serial Number: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Timestamp: 19 Sep 2016 14:39:13 -0500

Reputation Threshold:	<input checked="" type="radio"/> Use Value from Cloud Service (60)
	<input type="radio"/> Enter Custom Value:
	(Valid range 1 through 100)
Query Timeout:	<input type="text" value="15"/> seconds
Processing Timeout:	<input type="text" value="120"/> seconds
File Reputation Client ID:	f88bb5d6-b7d7-4e0a-be5c-dbbeee60a07a
File Retrospective:	<input checked="" type="checkbox"/> Suppress the verdict update alerts ?
Advanced settings for File Analysis	
Advanced settings for Cache	

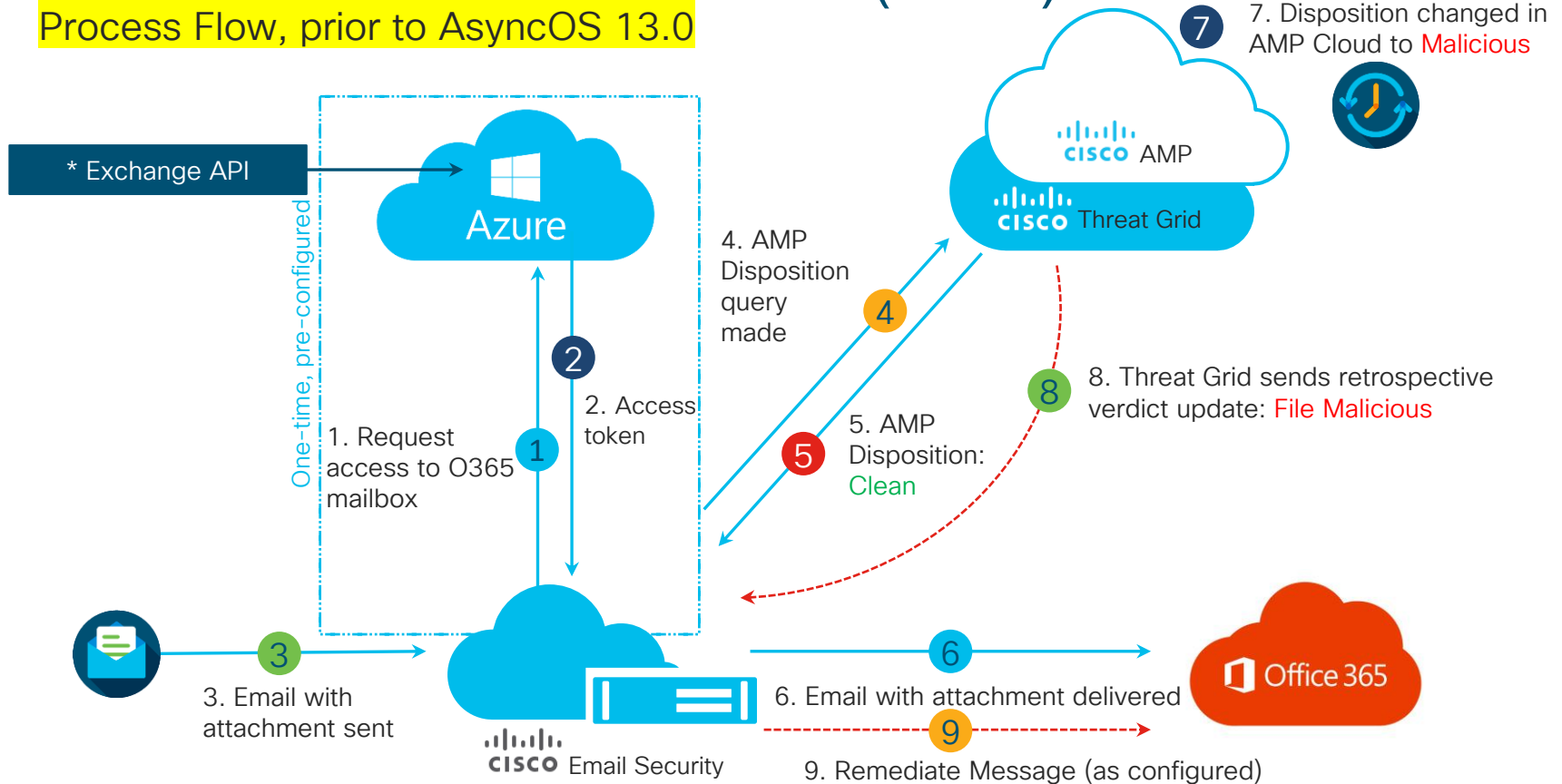
Suppression of non-delivered retro alerts is enabled in the File Retrospective settings.

Change in disposition and message delivered

The Info message is:
Retrospective verdict received for NEW SAMPLE ORDER 1.doc.
SHA256: ce49d65659304dcb7ae63182e17aa4b6f09740caaf77f1565a682bd2bb4e2bf4
Timestamp: 2016-09-19T19:39:12Z
Verdict: MALICIOUS
Reputation Score: 0
Spyname: RTF.CE49D65659.agent.tht.Talos
Total users affected: 1
----- Affected Messages -----
Message 1
MID : 20045
Subject : Sample Pictures and Letter of Intent as shown on attached files (3)
From : alfredo@comerquim.com.ec
Bcc : LAURA.LEWIS@somecustomername.com
File name : NEW SAMPLE ORDER 1.doc
Parent SHA256 : ,
Parent File name : ,
Date : 2016-09-19T05:35:48Z

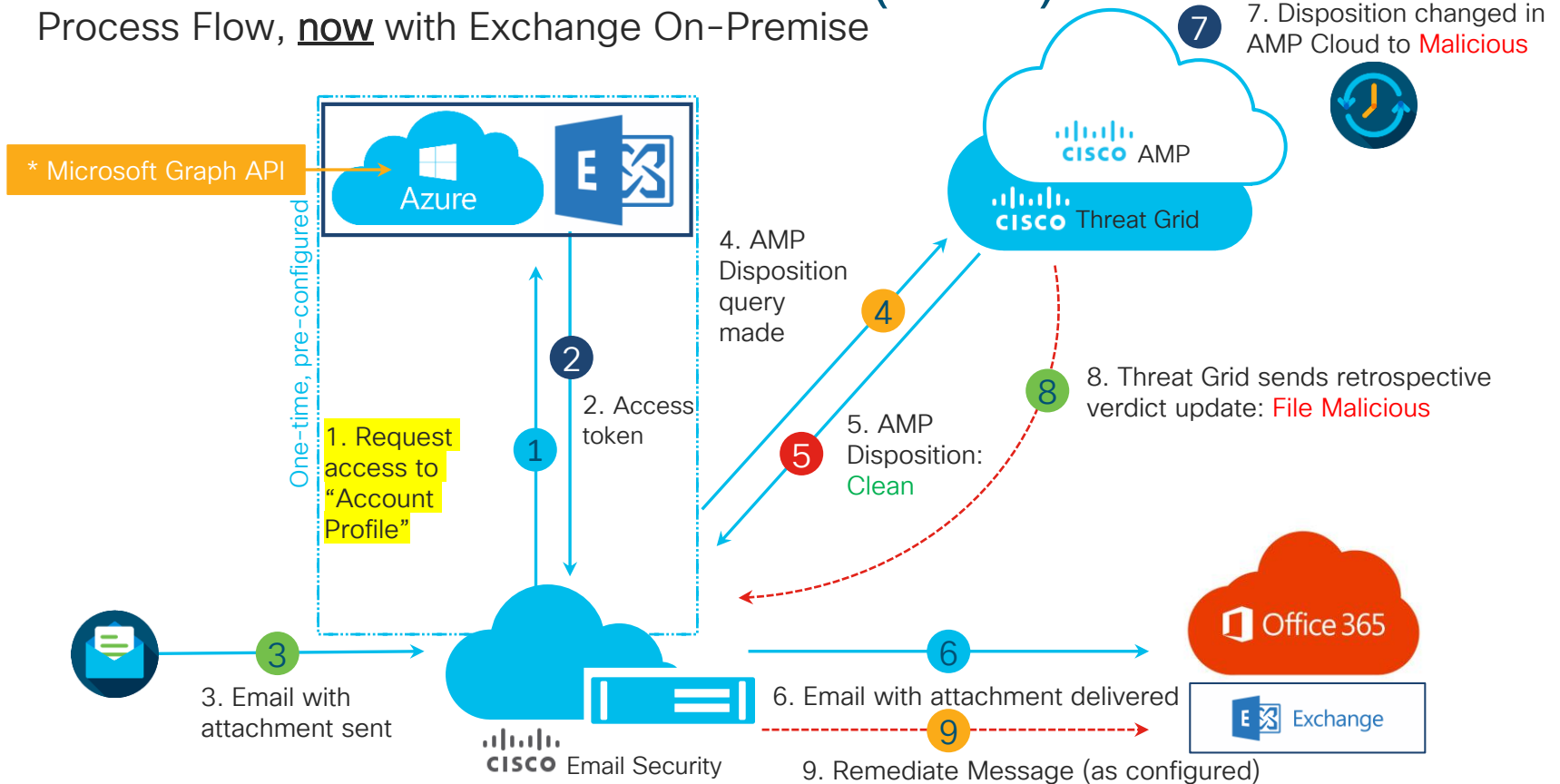
Mailbox Auto Remediation (MAR)

Process Flow, prior to AsyncOS 13.0



Mailbox Auto Remediation (MAR)

Process Flow, now with Exchange On-Premise

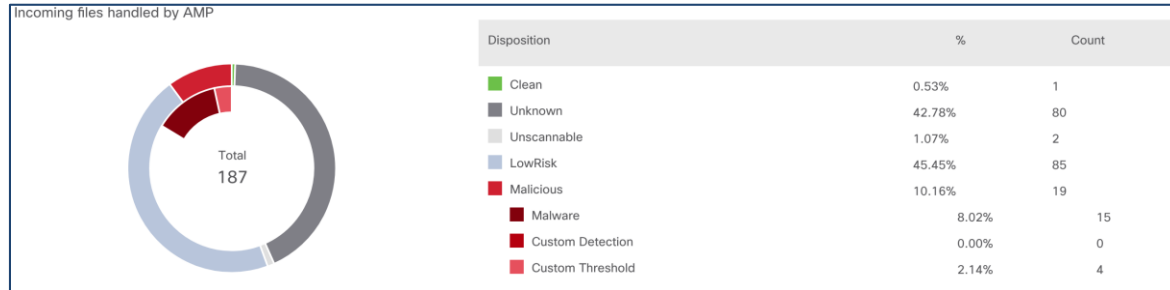


AMP

Enable AMP for Incoming or Outgoing Mail Policies

Default Policy	IronPort Anti-Spam Positive: Quarantine Suspected: Quarantine	Sophos Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	File Reputation Malware File: Drop Pending Analysis: Deliver Unscannable - Message Error: Deliver Unscannable - Rate Limit: Deliver Unscannable - AMP Service Not	Graymail Detection Marketing: Deliver Social: Deliver Bulk: Deliver	LOG_FED_SCORE REPLY-TO_CHECK FED_WARN BAD_URL_IN_DOC SPF_CHECK ...	Retention Time: Virus: 1 day Other: 4 hours
----------------	---	--	---	--	---	---

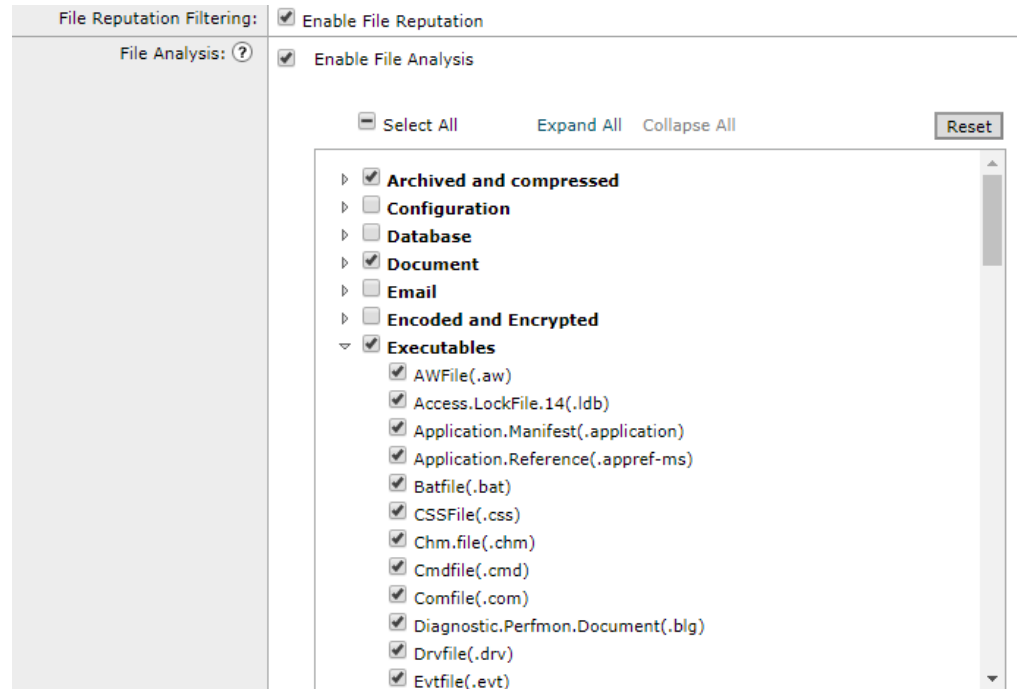
- AMP should be an included license on the ESA and CES.
- Can be enabled for both incoming and outgoing mail policies.
- Four (4) components to AMP:
 1. File Reputation
 2. File Analysis
 3. File Retrospection
 4. Mailbox Auto Remediation



AMP File Analysis

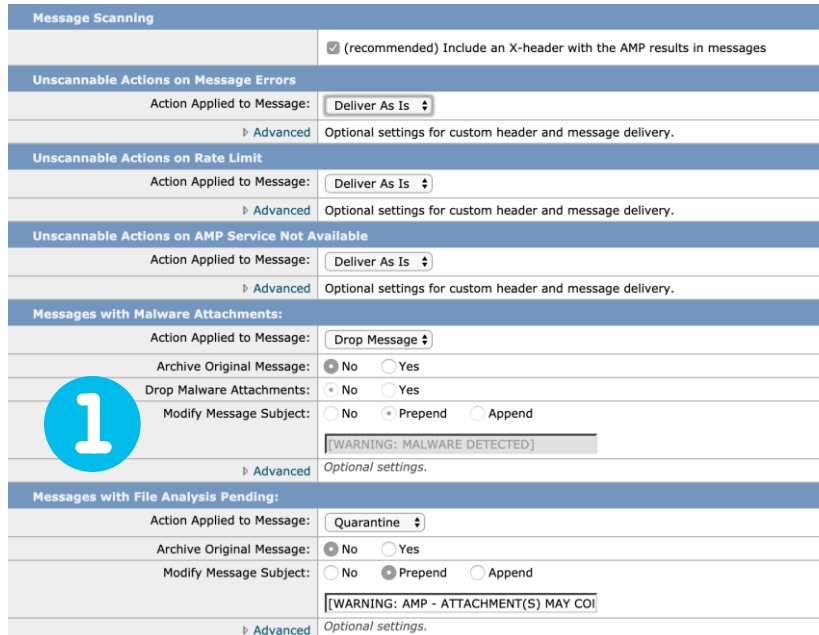
File Types

- Cisco Email Security provides parity with Threat Grid file support.
- AsyncOS 11.1 introduced a new pre-classification engine, allowing for additional file types to be supported for analysis.
- Pre-classification in the cloud allows for greater intelligence on files to be gathered.
- Be sure that you recheck the file types you are scanning!



AMP Dynamic Quarantine

- Recommended to use the quarantine to delay files and wait for analysis results.
- Typically file results are returned in under 10 minutes, default setting is to wait up to 1 hr. before releasing.



Message Scanning

(recommended) Include an X-header with the AMP results in messages

Unscannable Actions on Message Errors

Action Applied to Message:

Advanced Optional settings for custom header and message delivery.

Unscannable Actions on Rate Limit

Action Applied to Message:

Advanced Optional settings for custom header and message delivery.

Unscannable Actions on AMP Service Not Available

Action Applied to Message:

Advanced Optional settings for custom header and message delivery.

Messages with Malware Attachments:

Action Applied to Message:

Archive Original Message: No Yes

Drop Malware Attachments: No Yes

Modify Message Subject: No Prepend Append

Advanced Optional settings.

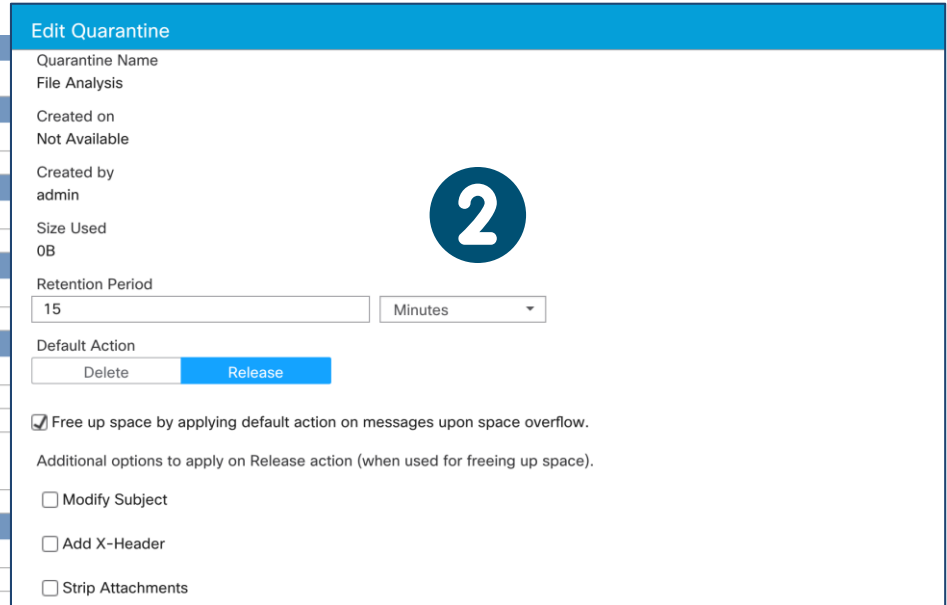
Messages with File Analysis Pending:

Action Applied to Message:

Archive Original Message: No Yes

Modify Message Subject: No Prepend Append

Advanced Optional settings.



Edit Quarantine

Quarantine Name
File Analysis

Created on
Not Available

Created by
admin

Size Used
0B

Retention Period

Default Action

Free up space by applying default action on messages upon space overflow.

Additional options to apply on Release action (when used for freeing up space).

Modify Subject

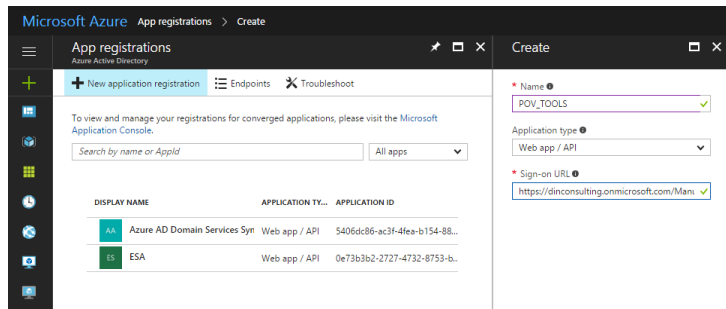
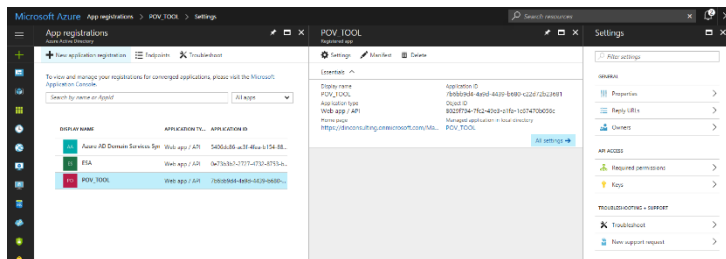
Add X-Header

Strip Attachments

Mailbox Auto Remediation (MAR)

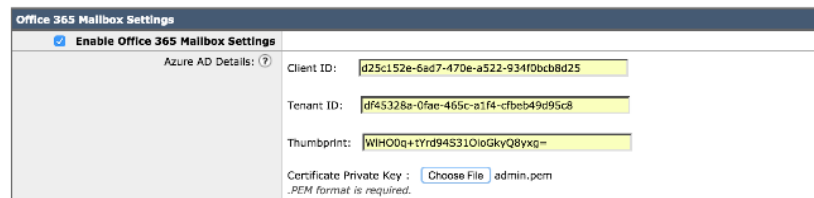
Configuration of Mailbox Remediation

Step 1: Create Azure Web Application in your tenant



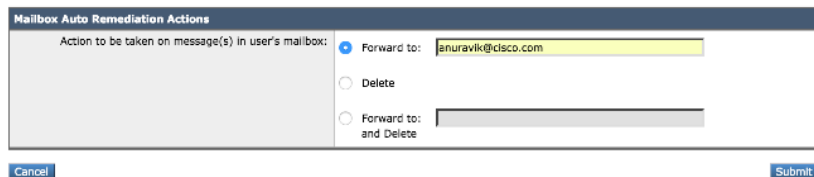
Step 2: Link Application to ESAs / CES


Mailbox Settings



Step 3: Set Policy for Remediation

Mailbox Auto Remediation



 **Mailbox Auto Remediation Setup Guide**
<https://www.cisco.com/c/dam/en/us/products/collateral/security/email-security-appliance/guide-c07-738370.pdf>

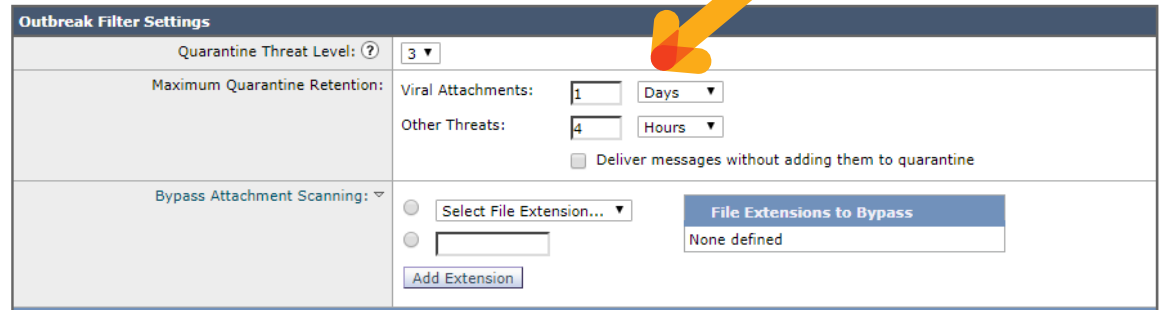


That wraps up our review of AMP!

Enabling Outbreak Filters (OF)

Order	Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters	Delete
	Default Policy	Disabled	Sophos Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	File Reputation Malware File: Drop Pending Analysis: Quarantine Unscannable - Message Error: Deliver Unscannable - Rate Limit: Deliver Unscannable - AMP Service Not ...	Graymail Detection Unsubscribe: Enabled Marketing: Deliver Social: Deliver Bulk: Deliver ...	CF_robsherw_fed CF_robsherw_fed_2 CF_robsherw_fed_3 CF_SDR_OK URL_REWRITE_SUSPICIOUS URL_LOG_ALL_REPUTATION ...	Retention Time: Virus: 1 day Other: 4 hours	

- OF is enabled by default and provides a dynamic quarantine (also called DELAY quarantine).
- Based on rules, OF can continue to hold or release back though AV and AMP for additional scans.



Outbreak Filter Settings

Quarantine Threat Level: ?

Maximum Quarantine Retention:

Viral Attachments: Days

Other Threats: Hours

Deliver messages without adding them to quarantine

Bypass Attachment Scanning:

File Extensions to Bypass

None defined

Benefits of Outbreak Filters

- It provides a significant catch rate for outbreaks over traditional scanning engines as it allows for the “human” element after signature, heuristics, and hash-based scanning.
- On average, it provides a 9+ hr. lead time over AV engines for 0-day Outbreaks.

20 MOST RECENT VIRUS OUTBREAKS FROM EMAIL

MALWARE NAME	CISCO	SOPHOS	MCAFFEE
Mal/Generic-S	+0d 20h 25m	+0d 20h 30m	1 st Mon, 20 Jan 2020 15:45:00 GMT
Mal/Fareit-VB-X	+0d 15h 55m	+0d 14h 40m	1 st Mon, 20 Jan 2020 15:45:00 GMT
Mal/Fareit-VB-X	1 st Mon, 20 Jan 2020 12:55:00 GMT	+0d 23h 20m	+0d 3h 10m
Mal/Generic-L	+0d 13h 50m	+1d 6h 55m	1 st Sun, 19 Jan 2020 17:30:00 GMT
Mal/Generic-S	+0d 12h 5m	+0d 6h 35m	1 st Sun, 19 Jan 2020 17:30:00 GMT
Troj/Fareit-JMA	+0d 20h 55m	+1d 0h 55m	1 st Thu, 16 Jan 2020 16:10:00 GMT
Mal/Generic-L	+0d 20h 39m	+3d 7h 55m	1 st Thu, 16 Jan 2020 16:10:00 GMT
Troj/Zbot-OBV	+0d 15h 55m	+2d 7h 25m	1 st Thu, 16 Jan 2020 16:10:00 GMT
Mal/Generic-S	+3d 14h 47m	+3d 13h 5m	1 st Mon, 13 Jan 2020 17:10:00 GMT
Mal/Generic-L	+0d 15h 16m	+3d 14h 25m	1 st Thu, 16 Jan 2020 16:10:00 GMT
Mal/Generic-S	+0d 15h 13m	+1d 12h 45m	1 st Thu, 16 Jan 2020 16:10:00 GMT
Mal/Generic-S	+0d 15h 12m	+1d 12h 45m	1 st Thu, 16 Jan 2020 16:10:00 GMT
Mal/Generic-S	1 st Thu, 16 Jan 2020 07:29:00 GMT	+0d 9h 16m	+0d 8h 1m
Mal/Generic-S	+0d 12h 46m	+1d 11h 35m	1 st Wed, 15 Jan 2020 18:40:00 GMT
Mal/Generic-S	1 st Thu, 16 Jan 2020 06:10:00 GMT	+0d 4h 25m	+0d 10h 0m
Mal/Fareit-VB-X	+0d 9h 5m	+1d 4h 50m	1 st Tue, 14 Jan 2020 20:45:00 GMT
Troj/TeslaAg-IL	+0d 19h 6m	+0d 21h 25m	1 st Mon, 13 Jan 2020 16:20:00 GMT
Troj/VB-KQI	1 st Tue, 14 Jan 2020 10:41:00 GMT	+4d 0h 4m	+3d 5h 44m
Mal/Generic-L			
Mal/Fareit-V			

http://cs.co/email_MalwareRep

Attachment Control & Defense Checklist

- ❑ Create a filter to block, quarantine or strip attachments that are deemed too risky for the organization.
- ❑ Use AV to block the known viruses. Turn off cleaning/repairing viruses from files.
- ❑ Ensure Outbreak Filters is turned on for all your policies, it provides an average 9+ hr. lead time on 0-day attacks.
- ❑ Use the Macro Filter to detect and take an action on unwanted files.
- ❑ Evaluate AMP if you don't have it already.
- ❑ AMP will hash all files and ask for file reputation.
- ❑ Set the File Analysis pending action to Quarantine to hold the message until a verdict is available.
- ❑ Macro inspection is performed by File Analysis on AMP along with other file types.
- ❑ Remediation is now available with Office 365 with the Azure API.

Cisco Threat Response

Threats are becoming more complex...

Understand what happened requires stitching information together



Cisco Threat Response (CTR)

Defense in depth – Attacking the Cyber Kill Chain!



Cisco Threat Response (CTR)

- Cisco Email Security (ESA) and Cisco Security Management (SMA) now allow pivoting to CTR on an observable anywhere from the UI.
 - ESA requires 13.0
 - SMA requires 12.5
- This provides Security Operations Control (SOC) & email administrators more context about specific observables to understand the associated risk.

The screenshot displays the Cisco Security Management Appliance (SMA) interface. At the top, it shows 'Security Management Appliance' with a 'Monitoring' tab selected. Below this, there are statistics for 'Advanced Malware Protection':

Metric	Value	Change
Avg. Analysis Time	6m 25s	-2% prior period
Avg. Threat Score	56	-2% prior period
Convicted	3	-25% prior period

Below the statistics, there are tabs for 'Incoming' and 'Outgoing'. A 'Mailbox' tab is also visible. The main content area shows 'Advanced Malware Protection Retrospective Security' with a table of files. One file is selected, and a context menu is open, showing various actions:

File SHA-256	Filename	Action Taken
edc9870a4054b0248f82f8624...	2019061701.pdf	Delete


The context menu for the selected file includes the following options:

- Malicious SHA-256
- Copy to Clipboard
- Add to New Case
- AMP for Endpoints
 - File trajectory
 - Search for this SHA256
 - Add SHA256 to custom detections Email Sec...
 - Add SHA256 to custom detections Quick SCD
 - Add SHA256 to custom detections SCD-SEC...
- Threat Grid
 - Browse edc9870a4054b0248f82f8624a8684...
 - Search edc9870a4054b0248f82f8624a8684...
- Umbrella
 - Sample view for edc9870a4054b0248f82f86...
- Threat Response
 - Investigate this SHA-256

Cisco Email Security + Cisco Threat Response

Reducing Time-to-Detection (TTD)



+  Threat Response

1

Out-of-box integrations

2

Designed for your Security Operations Center (SOC)

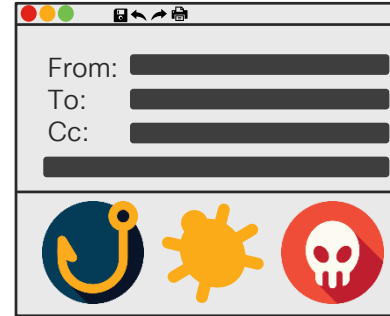
3

Saves time and effort

4

Free

Did you know that email is still the #1 threat vector?



8%

Of employees fall victim to phishing or email attacks

75% of companies cite one or more direct, significant operational impacts like **lost productivity, project delays, time-intensive remediation & data loss**

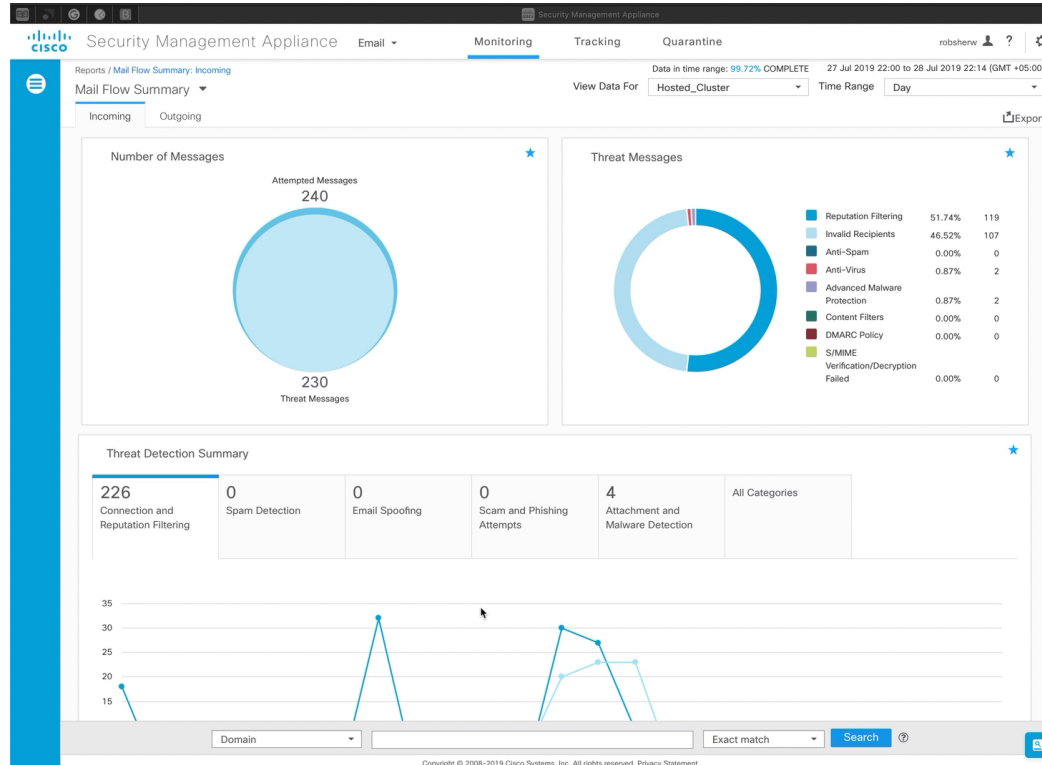
Now with Cisco Threat Response, 60% of surveyed organizations report that CTR has reduced the time they spent on threat investigations by at least 50%



“I am able to visualize threats within my environment and take action in half the time it use to take me.” – Security Engineer, Large Banking Company

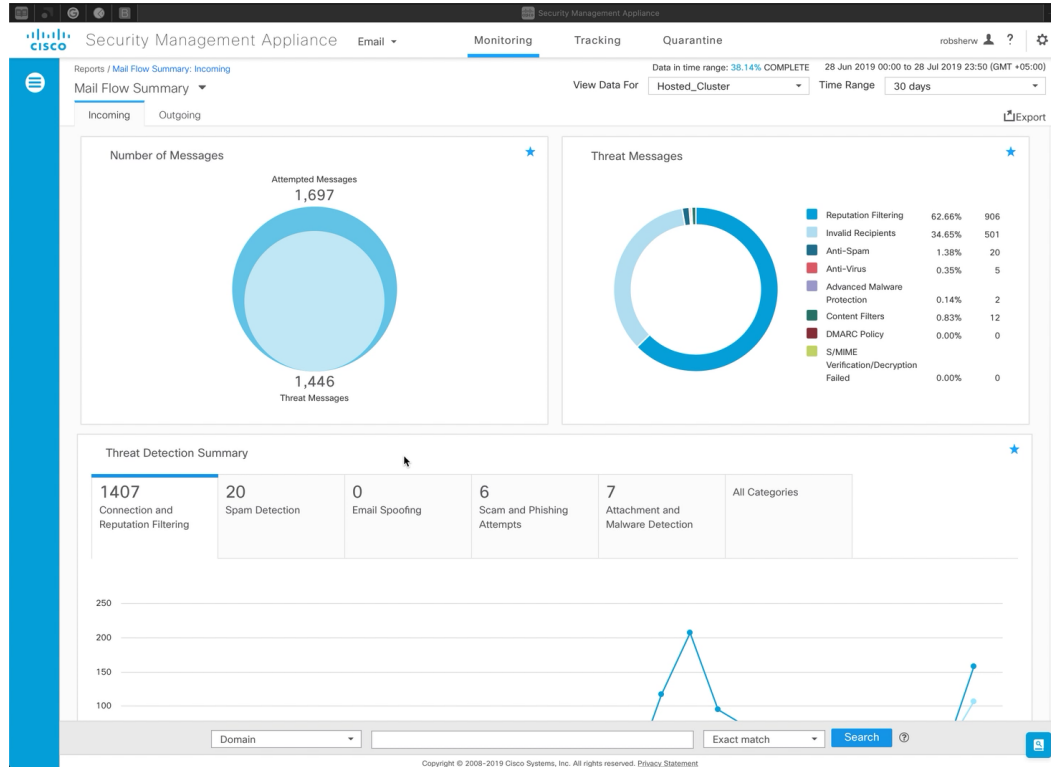
CTR: Enable Casebook/Pivot (Demo Video)

1min 01sec



CTR: Casebook/Pivot Usage (Demo Video)

2min 38sec



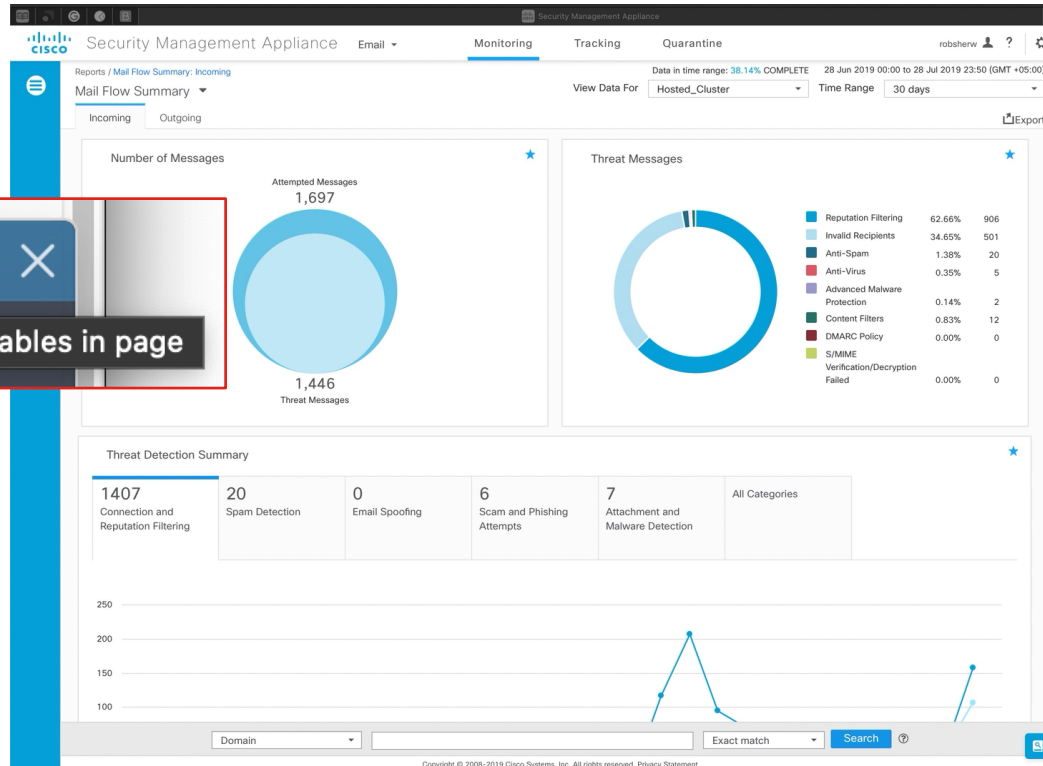
CISCO Live!

CTR: Casebook/Pivot Usage (Demo Video)

1min 01sec



Find observables in page



Monitoring & Tools

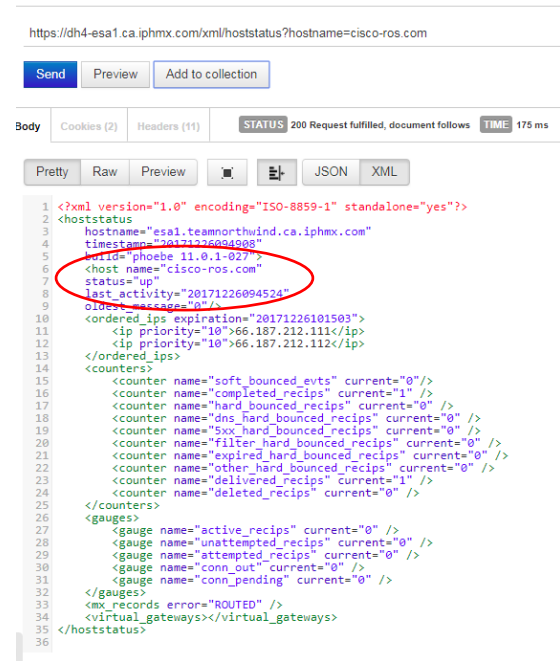
Using the XML pages

- Navigating to <https://hostname/xml/status> will provide a point in time view of all the gauges and health of the system
- Additional pages exist for:
 - Host Status: <https://hostname/xml/hoststatus?hostname=host>
 - DNS Status: <https://hostname/xml/dnsstatus>
 - Top Incoming Domains: <https://hostname/xml/topin>
 - Top Outgoing Domains: <https://hostname/xml/tophosts>

```
▼<counters>
<counter name="inj_msgs" reset="275178" uptime="92859" lifetime="275178"/>
<counter name="inj_recips" reset="275178" uptime="92859" lifetime="275178"/>
<counter name="gen_bounce_recips" reset="17" uptime="9" lifetime="17"/>
<counter name="rejected_recips" reset="517" uptime="123" lifetime="517"/>
<counter name="dropped_msgs" reset="37218" uptime="12236" lifetime="37218"/>
<counter name="soft_bounced_evts" reset="0" uptime="0" lifetime="0"/>
<counter name="completed_recips" reset="218665" uptime="61286" lifetime="218665"/>
<counter name="hard_bounced_recips" reset="23" uptime="11" lifetime="23"/>
<counter name="dns_hard_bounced_recips" reset="0" uptime="0" lifetime="0"/>
<counter name="5xx_hard_bounced_recips" reset="22" uptime="10" lifetime="22"/>
<counter name="filter_hard_bounced_recips" reset="0" uptime="0" lifetime="0"/>
<counter name="expired_hard_bounced_recips" reset="1" uptime="1" lifetime="1"/>
<counter name="other_hard_bounced_recips" reset="0" uptime="0" lifetime="0"/>
<counter name="delivered_recips" reset="218642" uptime="61275" lifetime="218642"/>
<counter name="deleted_recips" reset="0" uptime="0" lifetime="0"/>
<counter name="global_unsub_hits" reset="0" uptime="0" lifetime="0"/>
</counters>
<current_ids message_id="1503978" injection_conn_id="352044" delivery_conn_id="407"/>
▼<rates>
<rate name="inj_msgs" last_1_min="0" last_5_min="459" last_15_min="627"/>
<rate name="inj_recips" last_1_min="0" last_5_min="459" last_15_min="627"/>
<rate name="soft_bounced_evts" last_1_min="0" last_5_min="0" last_15_min="0"/>
<rate name="completed_recips" last_1_min="11" last_5_min="240" last_15_min="240"/>
<rate name="hard_bounced_recips" last_1_min="0" last_5_min="0" last_15_min="0"/>
<rate name="delivered_recips" last_1_min="11" last_5_min="240" last_15_min="240"/>
</rates>
▼<gauges>
<gauge name="ram_utilization" current="1"/>
<gauge name="cpu_utilization" current="39"/>
<gauge name="av_utilization" current="0"/>
<gauge name="case_utilization" current="0"/>
<gauge name="bm_utilization" current="0"/>
<gauge name="disk_utilization" current="0"/>
<gauge name="resource_conservation" current="0"/>
<gauge name="log_used" current="17"/>
<gauge name="log_available" current="135G"/>
<gauge name="conn_in" current="0"/>
<gauge name="conn_out" current="0"/>
<gauge name="active_recips" current="0"/>
<gauge name="unattempted_recips" current="0"/>
<gauge name="attempted_recips" current="0"/>
<gauge name="msgs_in_work_queue" current="0"/>
<gauge name="dsts_in_memory" current="5"/>
<gauge name="kbytes_used" current="0"/>
<gauge name="kbytes_free" current="8388608"/>
<gauge name="msgs_in_policy_virus_outbreak_quarantine" current="19358"/>
<gauge name="kbytes_in_policy_virus_outbreak_quarantine" current="239654"/>
<gauge name="reporting_utilization" current="0"/>
<gauge name="quarantine_utilization" current="0"/>
</gauges>
</status>
```


Out of Band (OOB) Monitoring with XML

- Popular monitoring software such as SolarWinds offer templates to use the XML status page for OOB monitoring: <https://thwack.solarwinds.com/docs/DOC-174863>
- Use the Host Status: <http://hostname/xml/hoststatus?hostname=mydomain.com> to monitor downstream servers such as Exchange or Office 365 instances to watch for delivery issues
- Custom scripts using cURL over HTTPS can be leveraged to get fast metrics / health status of appliances with out of band alerting
- XML status pages does not require any additional ports to be opened and will work for both on-prem ESA and Cloud Email environments
- Status is per individual server, not cluster or pool of servers



```
1 <?xml version="1.0" encoding="ISO-8859-1" standalone="yes"?>
2 <hoststatus
3   hostname="esa1.teamnorthwind.ca.iphmx.com"
4   timestamp="20171226094908"
5   brid="phoebe 11.0.1-027"
6   <host name="cisco-ros.com"
7     status="up"
8     last_activity="20171226094534"
9     oldest_message="0" />
10   <ordered_ips expiration="20171226101503">
11     <ip priority="10">66.187.212.111</ip>
12     <ip priority="10">66.187.212.112</ip>
13   </ordered_ips>
14   <counters>
15     <counter name="soft_bounced_evts" current="0" />
16     <counter name="completed_recips" current="1" />
17     <counter name="hard_bounced_recips" current="0" />
18     <counter name="dns_hard_bounced_recips" current="0" />
19     <counter name="5xx_hard_bounced_recips" current="0" />
20     <counter name="filter_hard_bounced_recips" current="0" />
21     <counter name="expired_hard_bounced_recips" current="0" />
22     <counter name="other_hard_bounced_recips" current="0" />
23     <counter name="delivered_recips" current="1" />
24     <counter name="deleted_recips" current="0" />
25   </counters>
26   <gauges>
27     <gauge name="active_recips" current="0" />
28     <gauge name="unattempted_recips" current="0" />
29     <gauge name="attempted_recips" current="0" />
30     <gauge name="conn_out" current="0" />
31     <gauge name="conn_pending" current="0" />
32   </gauges>
33   <mx_records error="ROUTED" />
34   <virtual_gateways></virtual_gateways>
35 </hoststatus>
36
```

API

Why would an Email Administrator use an API or API tool(s)?

- Application Programming Interface (API) is popular way to extract data, automate 3rd party tools & programs
- Provide secure and authenticated access to reports, report counters, and tracking
- Data, data, data...

API – Swagger

Available on ESA and SMA!

All Categories	771	1	0	0	4
Connection and Reputation Filtering		Spam Detection	Email Spoofing	Scam and Phishing Attempts	Attachm Malware

message-tracking

- GET /esa/api/v2.0/message-tracking/amp-details
- GET /esa/api/v2.0/message-tracking/connection-details
- GET /esa/api/v2.0/message-tracking/details
- GET /esa/api/v2.0/message-tracking/dlp-details
- GET /esa/api/v2.0/message-tracking/messages
- GET /esa/api/v2.0/message-tracking/uri-details

spam quarantine

- DELETE /esa/api/v2.0/quarantine/blocklist
- GET /esa/api/v2.0/quarantine/blocklist
- POST /esa/api/v2.0/quarantine/blocklist
- DELETE /esa/api/v2.0/quarantine/messages



API – Swagger

monitoring

GET /esa/api/v2.0/reporting/mail_amp_file_analysis_by_filename mail amp file analysis by filename completed timestamp

Parameters

Name	Description
startDate string (query)	2019-10-01T19:00:00.000Z
endDate string (query)	2019-10-15T19:00:00.000Z
device_type string (query)	esa
top string (query)	top

Responses

Request URL

```
https://sh3048-esa1.iphmx.com/esa/api/v2.0/reporting/mail_amp_file_analysis_by_filename?startDate=2019-10-01T19%3A00%3A00.000Z&endDate=2019-10-15T19%3A00%3A00.000Z&device_type=esa
```

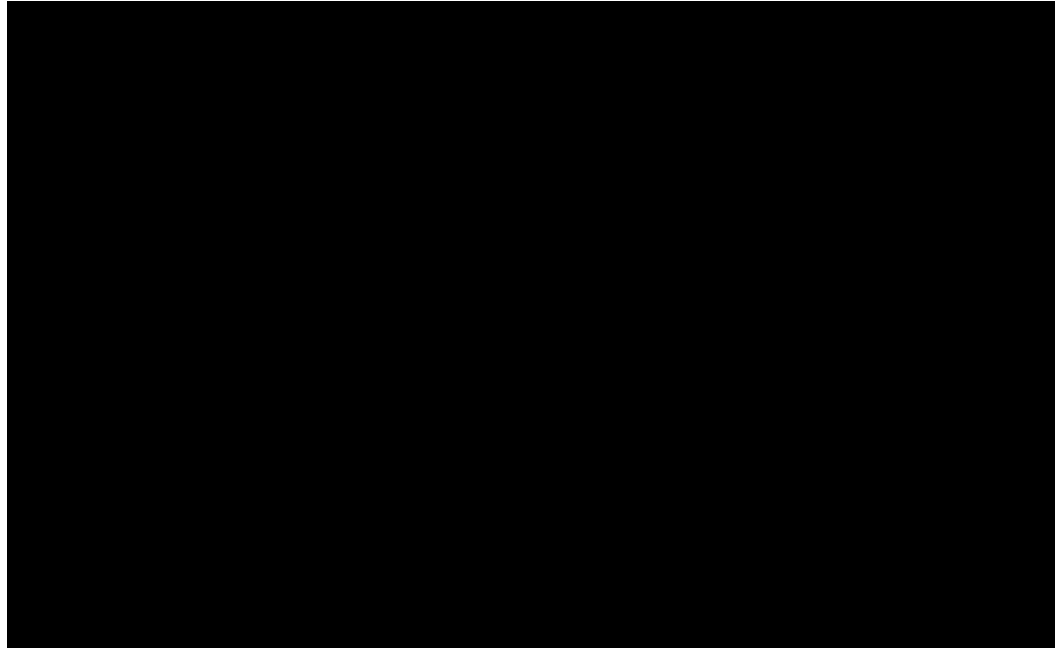
Server response

Code	Details
200	<p>Response body</p> <pre>{ "meta": { "totalCount": 1 }, "data": { "type": "mail_amp_file_analysis_by_filename", "resultSet": [{ "status": [{ "13e801424312cb27a7abbc2ea1f1ba12847d12ac8d85289d14c061708d0d4d2": { "file_name": "2010100101.pdf", "value": 1 }, { "7ba862c494f20e0547011c6c4b435b30a7e3d9aa944e1d40f860befdb8cdd9d": { "file_name": "2019100102.pdf", "value": 1 } }] }, "submit_timestamp": [{ "13e801424312cb27a7abbc2ea1f1ba12847d12ac8d85289d14c061708d0d4d2": { </pre>

Execute

Download

API – Swagger + Postman – Demo



API – Swagger

- 3rd party API tool such as Postman, etc.
- Want to see more on API on Cisco Email Security & Security Management?

AsyncOS Release 13.0 – What's new in Email Security

- LTRSEC-2319
- Thursday, January 30 | 09:00 AM – 01:00 PM
- Hall 8.0, Session Room B110



<https://docs.ces.cisco.com/docs/api>

Batch commands in the CLI

- CLI has all commands that are available in GUI, plus more.
- Some commands can be batched into a single line, you can type “**help <command>**” to see all the options.
- Summary of commands found in the CLI reference guide:

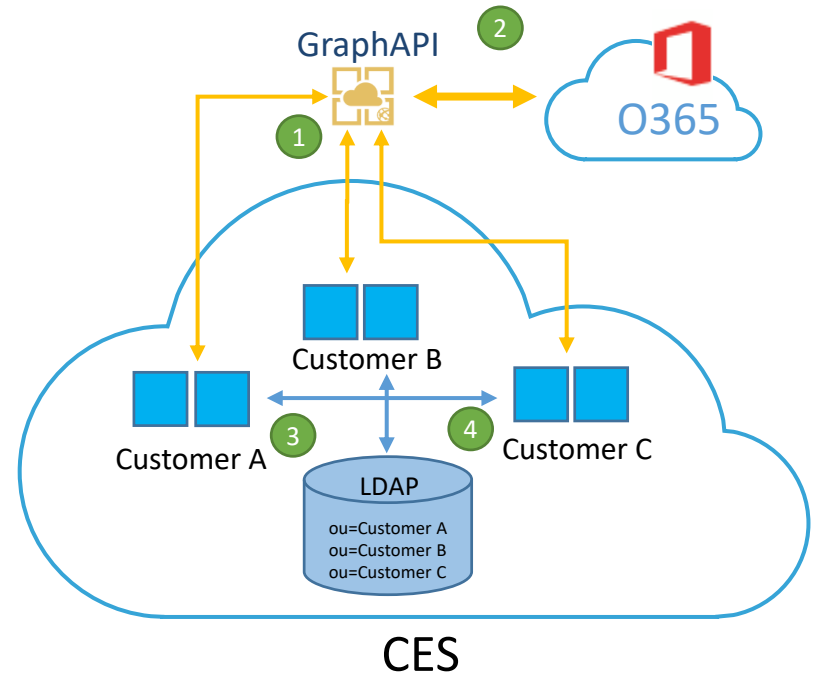
http://cs.co/email_ReferenceGuideCLI

Examples:

- Add an entry to SMTP Route:
 > **smtproutes new mynewdomain.com 215.55.66.77, 215.55.66.88**
- Add an entry to a HAT table:
 > **listenerconfig edit IncomingMail hostaccess new sendergroup REDLIST possible_spammer.com**
 Policy: “THROTTLED”

O365 to LDAP Sync in CES

- The connector provides the customer the ability to use native LDAP and Mailbox Access functionality in CES with Azure.
- It will sync recipient and group information inside Azure AD with a CES LDAP server that is locked by OU to each customer that requests it.
 1. Customer creates Mailbox Access Link with O365 enabling a MS GraphAPI Web Application (read-only)
 2. GraphAPI requests all recipient and group information from Azure for the tenant
 3. Customer CES instance pushes data to assigned OU in the LDAP server (mapped by OPs request)
 4. Customer can then query their specific OU with the assigned user/pass for recipient validation and group membership
- Customers will be provided read-only access to the directory to review and verify records.



<https://docs.ces.cisco.com/docs/azure-to-ldap-connector>

Summary & Checklist

Summary of Recommendations

Security Services

- IronPort Anti-Spam
 - Always scan 1MB and Never scan 2MB
- URL Filtering
 - Enable URL Categorization and Reputation
 - Enable Web Interaction Tracking
- Graymail Detection
 - Enable and Maximum Messages size 2 MB
- Outbreak Filters
 - Enable Adaptive Rules, Max Scan size 2 MB
 - Enable Web Interaction Tracking
- Advanced Malware Protection
 - Enable additional file types after enabling feature
- Message Tracking
 - Enable Rejected Connection Logging (if required)

System Administration

- Users
 - Set password policies
 - If possible leverage LDAP for authentication
- Log Subscriptions
 - Enable Configuration History Logs
 - Enable URL Filtering Logs
 - Log Additional Header 'From'

CLI Level Changes

- Web Security SDS URL Filtering
 - websecurityadvancedconfig >
 - disable_dns=1 , max_urls_to_scan=20 , num_handles=5 , default_ttl=600
 - Do you want to enable URL filtering for shortened URLs? [Y]> Y
- URL Logging
 - outbreakconfig> Do you wish to enable logging of URL's? [N]> y
 - <http://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118775-technote-esa-00.html>
- Clean URL Rewrites
 - websecurityadvancedconfig > Do you want to rewrite all URLs with secure proxy URLs? [Y]> n
- Anti-Spoof Filter
 - https://supportforums.cisco.com/sites/default/files/attachments/discussion/for_ged_email_detection_with_cisco_email_security.pdf
- Header Stamping Filter

```
addHeaders:  if (sendergroup != "RELAYLIST")
{
    insert-header("X-IronPort-RemoteIP", "$RemoteIP");
    insert-header("X-IronPort-MID", "$MID");
    insert-header("X-IronPort-Reputation", "$Reputation");
    insert-header("X-IronPort-Listener", "$RecvListener");
    insert-header("X-IronPort-SenderGroup", "$Group");
    insert-header("X-IronPort-MailFlowPolicy", "$Policy");
}
```

Summary of Recommendations

Host Access Table

- ❑ Additional SenderGroups
 - ❑ SKIP_SBRS – Place higher for sources that skip reputation
 - ❑ SPOOF_ALLOW – Part of Spoofing Filter
 - ❑ PARTNER – For TLS Forced connections
- ❑ In SUSPECTLIST
 - ❑ Include SBRS Scores on None
 - ❑ Optionally, include failed PTR checks
- ❑ Aggressive HAT Sample
 - ❑ BLACKLIST [-10 to -2] POLICY: BLOCKED
 - ❑ SUSPECTLIST [-2 to -1] POLICY: HEAVYTHROTTLE
 - ❑ GRAYLIST[-1 to 2 and NONE] POLICY: LIGHTTHROTTLE
 - ❑ ACCEPTLIST [2 to 10] POLICY: ACCEPTED

Mail Flow Policy (default)

- ❑ Security Settings
 - ❑ Set TLS to preferred
 - ❑ Enable SPF
 - ❑ Enable DKIM
 - ❑ Enable DMARC and Send Aggregate Feedback Reports

Incoming Mail Policies

- ❑ Anti-Spam thresholds
 - ❑ Positive = 90, Suspect = 39
- ❑ Anti-Virus
 - ❑ Don't repair, Disable Archive Message
- ❑ AMP
 - ❑ Add "AMP" to Subject Prepend for Unscannable, Disable Archive Message
- ❑ Graymail
 - ❑ Scanning enabled for each Verdict, Prepend Subject and Deliver
 - ❑ Add X-header for Bulk email header = X-BulkMail, value = True
- ❑ Outbreak Filters
 - ❑ Enable message modification. Rewrite URL for unsigned message.
 - ❑ Change Subject prepend to: [Possible \$threat_category Fraud]

Outgoing Mail Policies

- ❑ Anti-Virus
 - ❑ Anti-Virus Virus Infected: Prepend Subject: Outbound Malware Detected: \$Subject.
 - ❑ Other Notification to Others: Order form admin contact
 - ❑ Anti-virus Unscannable don't Prepend the Subject
 - ❑ Uncheck Include an X-header with the AV scanning results in Message

Summary of Recommendations

Policy Quarantines

- ❑ Pre-Create the following Quarantines
 - ❑ Inappropriate Inbound
 - ❑ Inappropriate Outbound
 - ❑ URL Malicious Inbound
 - ❑ URL Malicious Outbound
 - ❑ Suspect Spoof
 - ❑ Malware

Other Settings

- ❑ Dictionaries
 - ❑ Enable / Review Profanity and Sexual Terms Dictionary
 - ❑ Create Forged Email Dictionary with Executive Names
 - ❑ Create Dictionary for restricted or other keywords
- ❑ Destination Controls
 - ❑ Enable TLS for default destination
 - ❑ Set lower thresholds for webmail domains
 - ❑ <http://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118573-technote-esa-00.html>

Content Filters

- ❑ Inappropriate language Content Filter
 - ❑ Conditions Profanity OR Sexual dictionary match, send a copy to the Inappropriate quarantine.
- ❑ URL Malicious Reputation Content Filter
 - ❑ Send a copy to the URL Malicious (-10 to -6) to quarantine.
- ❑ URL Category Content Filter with these selected
 - ❑ Adult, Pornography, Child Abuse, Gambling.
 - ❑ Send a copy to the Inappropriate quarantine.
- ❑ Forged Email Detection
 - ❑ Dictionary named "Executives_FED"
 - ❑ FED() threshold 90 Quarantine a copy.
- ❑ Macro Enabled Documents content filter
 - ❑ if one or more attachments contain a Macro
 - ❑ Optional condition -> From Untrusted SBRS range
 - ❑ Send a copy to quarantine
- ❑ Attachment Protection
 - ❑ if one or more attachments are protected
 - ❑ Optional condition -> From Untrusted SBRS range
 - ❑ Send a copy to quarantine

Complete your online session survey



- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Content Catalog on ciscolive.com/emea.

Cisco Live sessions will be available for viewing on demand after the event at ciscolive.com.

Continue your education



Demos in the
Cisco Showcase



Walk-In Labs



Meet the Engineer
1:1 meetings



Related sessions



Thank you





You make **possible**