Configuration Best Practices for CES ESA

Contents

Introduction
Prerequisites
Requirements
Components Used
Configuration Best Practices for CES ESA
Basic Configuration
Recipient Access Table (RAT)
SMTP Routes
Security Services
IronPort Anti-Spam (IPAS)
URL Filtering
Graymail Detection
Outbreak Filters
Advanced Malware Protection
Message Tracking
LDAP
SPF
System Administration
Users
Log Subscriptions
CLI Level Changes
Web Security SDS URL Filtering
URL Logging
Anti-Spoof Filter
Header Stamping Filter
Host Access Table
Mail Flow Policy (Default Policy Parameters)
Security Settings
Incoming Mail Policies
Anti-Spam thresholds
Anti-Virus
AMP
Graymail
Outbreak Filters
Whitelist Mail Policy
Blacklist Mail Policy
Outgoing Mail Policies
Anti-Virus
Policy Quarantines
Other Settings
Introduction

This document provides a summary of recommendations for administrators using Cisco's Cloud Email Security (CES) to configure their Cisco Email Security Appliance (ESA).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- ESA Administration, both CLI and GUI level administration

Components Used

The information in this document is based on best practices and recommendations for CES customers and administrators.

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

Related Products

This document can also be used with these hardware and software versions:

- ESA on-premises hardware and virtual appliances (non-CES) running any version of AsyncOS for Email Security

Configuration Best Practices for CES ESA

Warning: Any changes to configuration(s) based on the best practices as provided in this document should be reviewed and understood prior to committing your configuration changes in a production environment. Please consult with your CES System Engineer or Account Team prior to making configuration changes that you do not 100% understand or have comfort with when administrating.

Basic Configuration

Recipient Access Table (RAT)
Inbound mail domains configured in Recipient Access Table

SMTP Routes

If smtp route destination is Office 365 hosted,

Security Services

IronPort Anti-Spam (IPAS)

- Always scan 1.5 MB and Never scan 2 MB

URL Filtering

- Enable URL Categorization and Reputation
- Enable Web Interaction Tracking

Graymail Detection

- Enable and Maximum Messages size 1 MB

Outbreak Filters

- Enable Adaptive Rules, Max Scan size 1 MB
- Enable Web Interaction Tracking

Advanced Malware Protection

- Enable additional file types after enabling feature

Message Tracking

- Enable Rejected Connection Logging (if required)

LDAP

if using LDAP, recommend using LDAP with SSL enabled.

SPF

Provide instructions on adding CES hosts to customer’s existing SPF record. A macro is published for all CES hosts per the allocation hostname to make it easier to add all hosts:

Place the following macro before ~all or -all within the current TXT / SPF record if it exists.

exists:%{i}.spf.<allocation>.iphmx.com
Note: Ensure the spf record ends with either ~all or -all. Placing this part of the spf record anywhere else may cause errors mail delivery issues. Always validate before making any changes.

Validate the SPF records for the customer's domains before and after any changes

Example tools:

- Validate existing record:
  - https://www.kitterman.com/spf/validate.html?
- Pre-validate a proposed change:

Breakdown of the basic elements of an SPF record.

[v=spf1] This identifies the TXT record as a SPF record.
[exists] Does the record exist
[%{i}] Macro expression that is replaced with the connecting IP.
[-all] Fail: Only allow mail that matches one of the parameters (IPv4, MX, etc) in the record
[~all] SoftFail: Allow mail whether or not it matches the parameters in the record

More SPF Examples

If you are receiving on CES and sending outbound mail from other mail servers, a good start would be the following example. You can use the "a:" mechanism to specify mail hosts.

v=spf1 mx a:mail01.yourdomain.com a:mail99.yourdomain.com ~all
If you are sending only outbound mail through CES, you could use:

v=spf1 mx exists:%{i}.spf.<allocation>.iphmx.com ~all
In this example, the "ip4:" or "ip6:" mechanism is used to specify an IP address or IP address range.

v=spf1 exists:%{i}.spf.<allocation>.iphmx.com ip4:192.168.0.1/16 ~all

System Administration

Users

- Set password policies
- If possible leverage Lightweight Directory Access Protocol (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`

Do you want to disable DNS lookups? [N] > y

Enter the maximum number of URLs that should be scanned: [100] > 20

Enter the threshold value for outstanding requests: [50] > 5

Enter the default time-to-live value (seconds): [30] > 600

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

URL Logging

- [ESA Enabling URL Filtering and Best Practices](#)
- `outbreakconfig`

Logging of URLs is currently disabled.

Do you wish to enable logging of URL's? [N] > y

Logging of URLs has been enabled.

Anti-Spoof Filter

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

Header Stamping Filter

- write and enable the following `message filter`:

Logging of URLs is currently disabled.

Do you wish to enable logging of URL's? [N] > y

Logging of URLs has been enabled.

Host Access Table

Additional Sender Groups

- ESA User Guide: [Creating a Sender Group for Message Handling](#) SKIP_SBRS – Place higher for sources that skip reputation
- SPOOF_ALLOW – Part of Spoofing Filter
- PARTNER – For TLS Forced connections

In the predefined SUSPECTLIST sender group

- ESA User Guide: [Sender Verification: Host](#) enable "SBRS Scores on None" Optionally,
enable "Connecting host PTR record lookup fails due to temporary DNS failure"

Aggressive HAT Sample

- **BLACKLIST [-10 to -2] POLICY: BLOCKED**
- **SUSPECTLIST [-2 to -1] POLICY: HEAVYTHROTTLED**
- **GRAYLIST [-1 to 2 and NONE] POLICY: LIGHTTHROTTLED**
- **ACCEPTLIST [2 to 10] POLICY: ACCEPTED**

**Note**: The above HAT examples show additionally configured Mail Flow Policies. For complete information regarding MFP, please refer to the User Guide of the appropriate version of AsyncOS for Email Security running on your ESA. Example, AsyncOS 10.0: [Host Access Table (HAT), Sender Groups, and Mail Flow Policies](example.com)

**Mail Flow Policy (Default Policy Parameters)**

**Security Settings**

- Set Transport Layer Security (TLS) to preferred
- Enable Sender Policy Framework (SPF)
- Enable DomainKeys Identified Mail (DKIM)
- Enable Domain-based Message Authentication, Reporting and Conformance (DMARC) Verification and Send Aggregate Feedback Reports

**Note**: DMARC requires additional tuning to configure. For complete information regarding DMARC, please refer to the User Guide of the appropriate version of AsyncOS for Email Security running on your ESA. Example, AsyncOS 10.0: [DMARC Verification](example.com)

**Incoming Mail Policies**

**Anti-Spam thresholds**

- Thresholds should be left at default thresholds. Modification of the scoring could result in an increase of false positive.

**Anti-Virus**

- Message Scanning: Scan for Viruses only
- Unscannable Messages, Virus Infected Messages: set "Archive Original Message" to No

**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

- Default threat level is 3, please adjust as per your security requirements. If the threat level for a message equals or exceeds this threshold, the message will be sent to the Outbreak Quarantine. (1=lowest threat, 5=highest threat)
- Enable message modification. Rewrite URL for unsigned message
- Change Subject prepend to: [Possible $threat_category Fraud]

Whitelist Mail Policy

Whitelist mail policies are configured with Antispam and Graymail disabled.

<table>
<thead>
<tr>
<th>Policies</th>
<th>Anti-Spam</th>
<th>Anti-Virus</th>
<th>Advanced Malware Protection</th>
<th>Graymail</th>
<th>Content Filters</th>
<th>Outbreak Filters</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td>BLACKLIST_DROP</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Disabled</td>
<td>(use default)</td>
<td>(use default)</td>
<td>Disabled</td>
<td>(use default)</td>
<td>Retention Time: 1 day Other: 4 hours</td>
</tr>
</tbody>
</table>

Blacklist Mail Policy

Blacklist mail policies are configured with all services disabled and link to a content filter with action of drop.

Blacklist_Drop

Create Content Filter by navigating to GUI > Mail Policies > Incoming Content Filters

Specify No Conditions and an action of Drop()

Link Content filter to Blacklist mail Policy by returning to Mail Policies > Incoming Mail Policies > Blacklist > Content Filters
Outgoing Mail Policies

Anti-Virus

- Message Scanning Scan for Viruses only un-check Include an X-header with the AV scanning results in Message
- For all messages: Advanced > Other Notification, enable "Others" and include admin/SOC contact email address

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
• Rate Limit Your Own Outbound Mail with Destination Control Settings

Content Filters

Note: For complete information regarding content filters, please refer to the User Guide of the appropriate version of AsyncOS for Email Security running on your ESA. Example, AsyncOS 10.0: Content Filters

Inappropriate 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

Related Information

• BRKSEC-2131 - Cisco Email Security: Best Practices and Fine Tuning (2016 Las Vegas)
• BRKSEC-2131 - E-mail Security for Non-E-mail People (2015 San Diego)
• BRKSEC-3770 - (DMARC) - Don't be a phish: deep dive into e-mail authentication techniques (2014 San Francisco)
• CES End User License Agreement
• CES Service Description
- Cisco Universal Cloud Terms
- Technical Support & Documentation - Cisco Systems
- SPF Record Syntax
- Authenticating with SPF: -all or ~all