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). Cisco provides all CES customers with a Security Management Appliance (SMA) in their CES instance. For centralized management purposes, parts of the configuration and best practices direct administrators to use quarantine(s), which are located on the SMA.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- ESA Administration, both CLI and GUI level administration
- SMA Administration, GUI level administration
- CES customers may request CLI access to their CES instances from the following instructions: [CES Customer CLI Access](#)
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
- SMA on-premises hardware and virtual appliances (non-CES) running any version of AsyncOS for Security Management

Policy Quarantines

Quarantines are configured and maintained on the SMA for CES customers. Please log-in to your SMA and view the quarantines and pre-create the following quarantines, as needed:

- ACCOUNT_TAKEOVER
- ANTI_SPOOF
- BLOCK_ATTACHMENTS
- BLOCKLIST
- DKIM_FAIL
- DMARC_QUARANTINE
- DMARC_REJECT
- FORGED_EMAIL
- INAPPROPRIATE_CONTENT
- MACRO
- OPEN_RELAY
- SDR_DATA
- SPF_HARDFAIL
- SPF_SOFTFAIL
- TG_OUTBOUND_MALWARE
- URL_MALICIOUS

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)

Accepted messages for domains are configured in Recipient Access Table. Please review Mail Policies > Recipient Access Table (RAT) to add and manage domains as needed.

SMTP Routes

If SMTP route destination is Office 365 hosted, please see Office365 Throttling CES New Instance with "4.7.500 Server busy. Please try again later".

Security Services

IronPort Anti-Spam (IPAS)

- Enabled and configure Always scan 1M and Never scan 2M

URL Filtering

- Enable URL Categorization and Reputation Filters
- (Optional) Create and configure URL Allowlist named "bypass_urls"
- Enable Web Interaction Tracking

Graymail Detection

- Enable and configure Always scan 1M and Never scan 2M
- Timeout for Scanning Single Message: 60 seconds

Outbreak Filters

- Enable Adaptive Rules
- Maximum Message Size to Scan: 2M
- Enable Web Interaction Tracking

Advanced Malware Protection > File Reputation and Analysis

- Enable File Reputation
- Enable File Analysis
- Review and enable additional file types after enabling feature

Message Tracking

- Enable Rejected Connection Logging (if required)

Additional services to review and consider:

LDAP

- If using LDAP, recommend using LDAP with SSL enabled

SPF

- CES customers, 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 DNS 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 tool:  https://www.kitterman.com/spf/validate.html? If you would like to pre-validate a proposed SPF change:  https://app.dmarcanalyzer.com/dns/spf  Click 'Prevalidate a SPF record update'Enter domain Paste in the SPF TXT record and click 'Validate SPF'
• 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 (System Administration > Users)

• Remember to review and set password policies associated with 'Local User Account & Passphrase Settings'
• If possible, configure and enable Lightweight Directory Access Protocol (LDAP) for authentication (System Administration > LDAP)

Logging (System Administration > Log Subscriptions)

• If not configured, create and enable: Configuration History LogsURL Filtering Logs or URL Reputation Client Logs
• For Global Settings, edit settings and log Headers: To, From, Reply-To, Sender
CLI Level Changes

Web Security URL Filtering

- Please be sure to read our [ESA Enabling URL Filtering and Best Practices](#).
- CLI only, please run the `websecurityadvancedconfig` command and configure the following:

```plaintext
> websecurityadvancedconfig

Enter URL lookup timeout (includes any DNS lookup time) in seconds:
[5]> [5]

Enter the URL cache size (no. of URLs):
[810000]> [810000]

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

Enter the maximum number of URLs that can be scanned in a message body:
[100]> 400

Enter the maximum number of URLs that can be scanned in the attachments in a message:
[25]> 400

Enter the Web security service hostname:
[v2.sds.cisco.com]> v2.sds.cisco.com

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

Do you want to verify server certificate? [Y]>

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

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

Do you want to rewrite both the URL text and the href in the message? Y indicates that the full rewritten URL will appear in the email body. N indicates that the rewritten URL will only be visible in the href for HTML messages. [N]>

Do you want to include additional headers? [N]>

Enter the default debug log level for RPC server:
[Info]>

Enter the default debug log level for URL cache:
[Info]>

Enter the default debug log level for HTTP client:
[Info]>

Note: Starting with AsyncOS 13.5, URL filtering will be handled from Cloud URL Analysis (CUA). The `websecurityadvancedconfig` command will be different and reduce some options for configuration.
> websecurityadvancedconfig

Enter URL lookup timeout in seconds: [15]>

Enter the maximum number of URLs that can be scanned in a message body: [100]>

Enter the maximum number of URLs that can be scanned in the attachments in a message: [25]>

Do you want to rewrite both the URL text and the href in the message? Y indicates that the full rewritten URL will appear in the email body. N indicates that the rewritten URL will only be visible in the href for HTML messages. [N]>

Do you want to include additional headers? [N]>

**URL Logging**

- Please be sure to read our [ESA Enabling URL Filtering and Best Practices](https://www.ironport.com/resources/esa-enabling-url-filtering-and-best-practices).
- CLI only, please run the `outbreakconfig` command and configure the following section as shown, if not already enabled:

```
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**


**HeaderStamping Filter**

- CLI only, please write and enable the following message 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");
}
```

**Host Access Table**

**Additional Sender Groups**
• ESA User Guide: Creating a Sender Group for Message Handling  
  BYPASS_SBRS – Place higher for sources that skip reputation  
  MY_TRUSTED_SPOOF_HOSTS – Part of Spoofing  
  FilterTLS_REQUIRED – For TLS Forced connections  

In the predefined SUSPECTLIST sender group  

• ESA User Guide: Sender Verification: Host  
  enable "SBRS Scores on None" (Optional)  
  enable "Connecting host PTR record lookup fails due to temporary DNS failure"  

Aggressive HAT Sample  

• BLOCKLIST_REFUSE [-10.0 to -9.0] POLICY: BLOCKED_REFUSE  
• BLOCKLIST_REJECT [-9.0 to -2.0] POLICY: BLOCKED_REJECT  
• SUSPECTLIST [-2.0 to 0.0 and SBRS scores of "None"] POLICY: THROTTLED  
• ACCEPTLIST [0.0 to 10.0] 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

HAT example:
Mail Flow Policy (Default Policy Parameters)

Default Policy Parameters

Security Settings

- Set Transport Layer Security (TLS) to preferred
- Enable Sender Policy Framework (SPE)
- 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

Incoming Mail Policies

Default Policy should be configured similar to the following:

Anti-Spam

- Enabled, with thresholds left at default thresholds. (Modification of the scoring could result in an increase of false positive.)

Anti-Virus

- Message Scanning: Scan for Viruses only assure check box for "Include an X-header" is enabled
- Unscannable Messages, Virus Infected Messages: set "Archive Original Message" to No

AMP

- Unscannable Actions on Message Errors: use Advanced and Add Customer Header to Message: "X-TG-MSGERROR", value: "true"
- Unscannable Actions on Rate Limit: use Advanced and Add Customer Header to Message: "X-TG-RATELIMIT", value: "true"
- Messages with File Analysis Pending: use Action Applied to Message as "Quarantine"

Graymail

- Scanning enabled for each Verdict, Prepend Subject and Deliver
- For Action on Bulk Mail, use Advanced and Add Custom Header "X-BulkMail", value = "True"

Content Filters
• Enabled and using URL_QUARANTINE_MALICIOUS, URL_REWRITE_SUSPICIOUS, URL_INAPPROPRIATE, DKIM_FAILURE, SPF_HARDFAIL, EXECUTIVE_SPOOF, DOMAIN_SPOOF, SDR, TG_RATE_LIMIT

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
• URL Rewriting set for "Enable for all messages"
• Change Subject prepend to: [Possible $threat_category Fraud]

### ALLOW_SPOOF Mail Policy

ALLOW_SPOOF mail policy is configured with all default services enabled, and Content Filters enabled for URL_QUARANTINE_MALICIOUS, URL_REWRITE_SUSPICIOUS, URL_INAPPROPRIATE, SDR, or content filters of your choice and configuration.

### ALLOWLIST Mail Policy

ALLOWLIST mail policy is configured with Antispam and Graymail disabled, and Content Filters enabled for URL_QUARANTINE_MALICIOUS, URL_REWRITE_SUSPICIOUS, URL_INAPPROPRIATE, DKIM_FAILURE, SPF_HARDFAIL, EXECUTIVE_SPOOF, DOMAIN_SPOOF, SDR, TG_RATE_LIMIT, or content filters of your choice and configuration.

### BLOCKLIST Mail Policy

BLOCKLIST mail policy is configured with all services disabled, except Advanced Malware Protection, and link to a content filter with action of QUARANTINE.

### Outgoing Mail Policies

Default Policy should be configured similar to the following:

**Anti-Spam**
• Disabled

Anti-Virus

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

Advanced Malware Protection

• Enable File Reputation only
• Unscannable Actions on Rate Limit: use Advanced and Add Customer Header to Message: "X-TG-RATELIMIT", value: "true"
• Messages with Malware Attachments: use Advanced and Add Customer Header to Message: "X-TG-OUTBOUND", value: "MALWARE DETECTED"

Graymail

• Disabled

Content Filters

• Enabled and using TG_OUTBOUND_MALICIOUS, Strip_Secret_Header, EXTERNAL_SENDER_REMOVE, ACCOUNT_TAKEOVER, or content filters of your choice and configuration

Outbreak Filters

• Disabled

DLP

• Enable, based on your DLP licensing and DLP configuration. (This will not be covered with in this document.)

Other Settings

Dictionaries (Mail Policies > Dictionaries)

• Enable and review Profanity and Sexual_Content Dictionary
• Create Executive_FED dictionary for Forged Email Detection, include all executive names
• Create additional dictionary/dictionaries for restricted or other keywords as you see needed for your policies, environment, security control

Destination Controls (Mail Policies > Destination Controls)

• For the Default domain, enable TLS by setting to Preferred
• You may wish to add destinations for webmail domains and set lower thresholds
• Please see our Rate Limit Your Own Outbound Mail with Destination Control Settings guide for more information.
The following content filters have been suggested from the Incoming Mail Policies and Outgoing Mail Policies section. Please review and add if you have followed the guidance from this guide.

**Incoming Content Filters**

**URL_QUARANTINE_MALICIOUS**

Condition: URL Reputation; url-reputation(-10.00, -6.00 , "bypass_urls", 1, 1)

Action: Quarantine: quarantine("URL_MALICIOUS")

**URL_REWRITE_SUSPICIOUS**

Condition: URL Reputation; url-reputation(-5.90, -5.60 , "bypass_urls", 0, 1)
Action: URL Reputation; url-reputation-proxy-redirect(-5.90, -5.60,"",0)

URL_INAPPROPRIATE
Condition: URL Category; url-category (['Adult', 'Child Abuse Content', 'Extreme', 'Hate Speech', 'Illegal Activities', 'Illegal Downloads', 'Illegal Drugs', 'Pornography', 'Filter Avoidance'], "bypass_urls", 1, 1)
Action: Quarantine; duplicate-quarantine("INAPPROPRIATE_CONTENT")

DKIM_FAILURE
Condition: DKIM Authentication; dkim-authentication == "hardfail"
Action: Quarantine; duplicate-quarantine("DKIM_FAIL")

SPF_HARDFAIL
Condition: SPF Verification; spf-status == "fail"
Action: Quarantine; duplicate-quarantine("SPF_HARDFAIL")

EXECUTIVE_SPOOF
Condition: Forged Email Detection; forged-email-detection("Executive_FED", 90, "")
Condition: Other Header; header("X-IronPort-SenderGroup") != "(?i)allowspoof"
* set Apply rule: Only if all conditions match
Action: Add/Edit Header; edit-header-text("Subject", "(.*)", "[EXTERNAL]\1")
Action: Quarantine; duplicate-quarantine("FORGED_EMAIL")

DOMAIN_SPOOF
Condition: Other Header; header("X-Spoof")
Action: Quarantine; duplicate-quarantine("ANTI_SPOOF")

SDR
<table>
<thead>
<tr>
<th>Order</th>
<th>Filter Name</th>
<th>Description</th>
<th>Rule</th>
<th>Policies</th>
<th>Duplicate</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>URL QUARANTINE: MALICIOUS</td>
<td>URL QUARANTINE: MALICIOUS (Domain reputation between 0.00 and 4.00, &quot;good&quot; or &quot;bad&quot;, &quot;success&quot;, 0, 1)</td>
<td>quarantine(&quot;URL MALICIOUS&quot;)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>URL QUARANTINE: QUARANTINE</td>
<td>URL QUARANTINE: QUARANTINE (Domain reputation between 0.00 and 4.00, &quot;good&quot; or &quot;bad&quot;, &quot;success&quot;, 0, 1)</td>
<td>quarantine(&quot;URL QUARANTINE&quot;)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>URL QUARANTINE: MALICIOUS</td>
<td>URL QUARANTINE: MALICIOUS (Domain reputation between 0.00 and 4.00, &quot;good&quot; or &quot;bad&quot;, &quot;success&quot;, 0, 1)</td>
<td>quarantine(&quot;URL MALICIOUS&quot;)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>CHECK QUARANTINE</td>
<td>CHECK QUARANTINE (X-TG-RATELIMIT: &quot;false&quot;)</td>
<td>duplicate-quarantine(&quot;CHECK QUARANTINE&quot;)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>IP HEADER</td>
<td>IP HEADER (X-TG-RATELIMIT: &quot;false&quot;)</td>
<td>duplicate-quarantine(&quot;IP HEADER&quot;)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>EXECUTION</td>
<td>EXECUTION (X-TG-RATELIMIT: &quot;false&quot;)</td>
<td>duplicate-quarantine(&quot;EXECUTION&quot;)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>UPGRADE</td>
<td>UPGRADE (X-TG-RATELIMIT: &quot;false&quot;)</td>
<td>duplicate-quarantine(&quot;UPGRADE&quot;)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>SRC</td>
<td>SRC (X-TG-RATELIMIT: &quot;false&quot;)</td>
<td>duplicate-quarantine(&quot;SRC&quot;)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>TG_RATE_LIMIT</td>
<td>TG_RATE_LIMIT (X-TG-RATELIMIT: &quot;false&quot;)</td>
<td>duplicate-quarantine(&quot;TG_RATE_LIMIT&quot;)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>BLOCKLIST QUARANTINE</td>
<td>BLOCKLIST QUARANTINE (X-TG-RATELIMIT: &quot;false&quot;)</td>
<td>duplicate-quarantine(&quot;BLOCKLIST QUARANTINE&quot;)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Outgoing Content Filters**

**TG_OUTBOUND_MALICIOUS**
Condition: Other Header; header("X-TG-OUTBOUND") == "MALWARE"
Action: Quarantine; quarantine("TG_OUTBOUND_MALWARE")

Strip_Secret_Header

Condition: Other Header; header("PLACEHOLDER") == "PLACEHOLDER"
Action: Strip Header; strip-header("X-IronPort-Tenant")

EXTERNAL_SENDER_REMOVE

Condition: (None)
Action: Add/Edit Header; edit-header-text("Subject", "\[EXTERNAL\\]\s?", "")

ACCOUNT_TAKEOVER

Condition: Other Header; header("X-AMP-Result") == "(?i)malicious"
Condition: URL Reputation; url-reputation(-10.00, -6.00, "", 1, 1)

*Set Apply Rule: If one or more conditions match

Action: Notify; notify ("myit@mycompany.com", "POSSIBLE ACCOUNT TAKEOVER", "", "ACCOUNT_TAKEOVER_WARNING")
Action: duplicate-quarantine("ACCOUNT_TAKEOVER")

For CES customers, we do have example content filters included with-in the pre-loaded, best practices configuration. Please review the "SAMPLE_" filters for more information on conditions and actions associated that may be beneficial in your configuration.
Cisco Live

Cisco Live hosts many sessions globally and does offer in-person sessions and technical breakouts that cover Cisco Email Security best practices. For past sessions and access, please visit ciscolive.com:

- Cisco Email Security: Best Practices and Fine Tuning - BRKSEC-2131
- DMARCate Your Email Perimeter - BRKSEC-2131
- Fixing Email! - Cisco Email Security Advanced Troubleshooting - BRKSEC-3265
- API Integrations for Cisco Email Security - DEVNET-2326
- Securing SaaS Mailbox Services with Cloud Email Security from Cisco - BRKSEC-1025
- Email Security: Best Practices and Fine Tuning - TECSEC-2345
- 250 not OK – Going on the Defensive with Cisco Email Security - TECSEC-2345
- Cisco Domain Protection and Cisco Advanced Phishing Protection: Making the Most of the Next Layer in Email Security! - BRKSEC-1243
- SPF is Not an Acronym for "Spoof"! Let's Utilize the Most out of the Next Layer in Email Security! - DGTL-BRKSEC-2327

Related Information

- CES End User License Agreement
- Cisco Cloud Offer Terms > CES, CRES, DMP, APP and CMD
- Cisco Universal Cloud Terms
- Cisco Support & Downloads
- [EXTERNAL] OpenSPF: SPF Basics and Advanced Information
- [EXTERNAL] Authenticating with SPF: -all or ~all