配置云网关金牌级配置

目录

简介

本文档对思科安全邮件云网关提供的金牌配置进行深入分析。思科安全电邮云客户的金牌配置是云网关和思科安全电邮和网络管理器的最佳实践和零日配置。思科安全邮件云部署同时使用云网关和至少一(1)个邮件和网络管理器。部分配置和最佳实践指导管理员使用位于Email and Web Manager上的隔离区进行集中管理。

先决条件

要求

思科建议您了解以下主题：

- 思科安全邮件网关或云网关，UI和CLI管理
- Cisco Secure Email Email and Web Manager、UI级管理
- 思科安全电邮云客户可以请求CLI访问；请参阅:命令行界面(CLI)访问

使用的组件

本文档中的信息来自针对思科安全电邮云客户和管理员的金牌配置和最佳实践建议。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

相关产品

本文档也适用于以下内容：

- 思科安全邮件网关现场硬件或虚拟设备
- Cisco Secure Email and Web Manager本地硬件和虚拟设备

策略隔离区

在邮件和网络管理器上为思科安全邮件云客户配置和维护隔离区。请登录您的电子邮件和Web管理器以查看隔离区：

- ACCOUNT_TAKEOVER
- 反欺骗
- BLOCK_ATTACHMENTS
- 阻止列表
- DKIM_FAIL
- DMARC_QUARANTINE
- DMARC_REJECT
- FORGED_EMAIL
- INFORECTIVE_CONTENT
- 宏
- OPEN_RELAY
- SDR_DATA
- SPF_HARDFAIL
- SPF_SOFTFAIL
- TG_OUTBOUND_MALWARE
- URL_MALICIOUS

云网关金牌配置

> **警告**：在生产环境中提交配置更改之前，需要查看和了解基于本文档中提供的最佳实践对配置所做的任何更改。更改配置之前，请咨询您的思科CX工程师、指定服务经理(DSM)或客户团队。

基本配置

邮件策略>收件人访问表(RAT)

收件人访问表定义公共侦听程序接受哪些收件人。该表至少指定地址以及是接受还是拒绝。请检查RAT，根据需要添加和管理域。

Network > SMTP Routes

如果SMTP路由目标为Microsoft 365，请参阅Office365 Throttling CES New Instance with "4.7.500 Server busy"。请稍后重试”。

安全性服务

使用提供的值，为所有思科安全邮件云客户配置列出的服务：

IronPort反垃圾邮件(IPAS)

- 启用并配置Always scan 1M和Never scan 2M
- 扫描单个邮件的超时：60 秒

URL 过滤

- 启用URL分类和信誉过滤器
- （可选）创建和配置名为“bypass_urls”的URL允许列表。
- 启用网络交互跟踪
- 高级设置: URL查找超时：15 秒正文和附件中扫描的最大URL数：400重写邮件中的URL文本和HREF:无URL日志记录：启用
- （可选）从AsyncOS 14.2 for Cloud Gateway开始，可以使用URL追溯性裁决和URL补救；请参阅提供的版本说明和为安全邮件网关和云网关配置URL过滤

灰色邮件检测

- 启用并配置Always scan 1M和Never scan 2M
- 扫描单个邮件的超时：60 秒

爆发过滤器

- 启用自适应规则

- 要扫描的最大邮件大小：2米
- 启用网络交互跟踪

高级恶意软件防护>文件信誉和分析

- 启用文件信誉
- 启用文件分析 请参阅“全局设置”以检查文件分析的文件类型

邮件跟踪

- 启用拒绝的连接日志记录（如果需要）

系统管理

用户（系统管理>用户）

- 请记得查看并设置与本地用户帐户和密**码设置关联的密码短语策略**
- 如有可能，配置并启用轻量级目录访问协议(LDAP)进行身份验证**(系统管理> LDAP**)

日志订阅（系统管理>日志订阅）

- 如果未配置，请创建并启用： 配置历史记录日志URL信誉客户端日志
- 在“日志订阅全局设置”(Log Subscriptions Global Settings)中，编辑设置并将信头添加**到、从、回复、发件人**。

其他配置（可选）

需要审查和考虑的其他服务：

系统管理> LDAP

- 如果配置LDAP，思科建议启用了SSL的LDAP

URL防御

- 有关URL防御的最新配置最佳实践，请参阅为安全邮件网关和云网关配置URL过滤。
- 思科还深入研究了URL防御；请参阅URL防御指南。
- URL防御指南中包含的一些示例也包含在本文档中。

SPF

- 发件人策略框架(SPF)DNS记录是在云网关的外部创建的。因此，思科强烈建议所有客户将SPF、DKIM和DMARC最佳实践融入其安全状态。有关SPF验证的详细信息，请参阅SPF配置和最佳实践。
- 对于思科安全电邮云客户，系统会为每个分配主机名发布所有云网关的宏，以便更轻松地添加所有主机。
- 将此项放在~all或 — all之前，放到当前DNS TXT(SPF)记录中（如果存在）：

```
exists:%{i}.spf.<allocation>.iphmx.com
```

注意：确保SPF记录以**~all或 — all结尾**。在任何更改之前和之后验证域的SPF记录！

- 有关SPF的更多信息的推荐信息和工具：
  SPF记录检查器 — 免费SPF查找(dmarcian.com)SPF记录语法表 — 所有SPF - dmarcian.com

其他SPF示例

- SPF的一个极好示例是从云网关接收电子邮件以及从其他邮件服务器发送出站电子邮件。可以使用“a：”机制指定邮件主机：

```
v=spf1 mx a:mail01.yourdomain.com a:mail99.yourdomain.com ~all
```

- 如果仅通过云网关发送出站电子邮件，您可以使用：

```
v=spf1 mx exists:%{i}.spf.<allocation>.iphmx.com ~all
```

- 在本示例中，“ip4：”或“ip6：”机制指定IP地址或IP地址范围：

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

CLI级别更改

- 如必备条件中所述，思科安全电邮云客户可以请求CLI访问；请参阅命令行界面(CLI)访问。

反欺骗过滤器

- 请务必查看防欺骗的最佳实践指南
- 本指南为您提供关于防止邮件欺骗的深层示例和配置最佳实践

添加报头过滤器

- 请仅使用CLI，请编写并启用addHeaders消息过滤器:

```
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");
}
```

主机访问表(邮件策略>主机访问表(HAT))

HAT概述>其他发件人组

- ESA用户指南：创建邮件处理的发件人组 BYPASS_SBRS — 对跳过信誉的源设置较高的值 MY_TRUSTED_SPOOF_HOSTS — 欺骗过滤器的一部分TLS_REQUIRED — 用于TLS强制连接

在预定义的SUSPECTLIST发件人组中

- ESA用户指南：发件人验证：主机 启用“SBRS Scores on None”。（可选）启用“由于临时DNS故障，连接主机PTR记录查找失败”。

主动HAT示例

- BLOCKLIST_REFUSE [-10.0到–9.0]策略：BLOCKED_REFUSE
- BLOCKLIST_REJECT [-9.0到–2.0]策略：BLOCKED_REJECT
- SUSPECTLIST [-2.0到0.0和SBRS评分“无”]策略：已限制
- 接受列表[0.0到10.0]策略：已接受

> **注意**：HAT示例显示了附加配置的邮件流策略(MFP)。 有关MFP的完整信息，请参阅用户指南中的“了解邮件管道>传入/接收”，了解您已部署的思科安全邮件网关的相应版本的AsyncOS。

HAT示例：

Sender Groups (Listener: IncomingMail)

Add Sender Group... | Import HAT...

Order	Sender Group	SenderBase™ Reputation Score -10 -8 -6 -4 -2 0 2 4 6 8 +10	External Threat Feed Sources Applied	Mail Flow Policy	Delete
1	SMA		None applied	RELAYED	
2	CISCO_MONITORING		None applied	ACCEPTED	
3	RELAYLIST		None applied	RELAYED	
4	TLS_REQUIRED		None applied	TLS_REQUIRED	
5	MY_TRUSTED_SPOOF_HOSTS		None applied	ACCEPTED	
6	BYPASS_SBRS_SPAM		None applied	ACCEPTED_NOSPAM	
7	BYPASS_SBRS		None applied	ACCEPTED	
8	BLOCKLIST_REFUSE		None applied	BLOCKED_REFUSE	
9	BLOCKLIST_REJECT		None applied	BLOCKED_REJECT	
10	SUSPECTLIST		None applied	THROTTLED	
11	FREEMAIL		None applied	THROTTLED	
12	ACCEPTLIST		None applied	ACCEPTED	
	ALL		None applied	ACCEPTED	

Edit Order... | Export HAT...

邮件流策略(默认策略参数)

默认策略参数

安全设置

- 将传输层安全(TLS)设置为首选
- 启用发件人策略框架(SPF)
- 启用DomainKey Identified Mail(DKIM)
- 启用基于域的邮件身份验证、报告和一致性(DMARC)验证并发送汇总反馈报告

> **注意：**DMARC需要额外的调整才能配置。有关DMARC的详细信息，请参阅用户指南中的“邮件身份验证> DMARC验证”，了解您已部署的思科安全邮件网关的相应版本的AsyncOS。

传入邮件策略

默认策略的配置类似于：

反垃圾邮件

- 启用，阈值保留为默认阈值。（对评分的修改可能会增加误报。）

防病毒

- 邮件扫描：**仅扫描病毒** 确保“包括X报头”复选框已启用
- 对于**无法扫描的邮件**和**感染病毒的邮件**，请将**存档原始邮件**设置为**否**

AMP

- 对于**无法扫描的邮件错误操作**，请使用**Advanced**和**Add Custom Header to Message**,X-TG-MSGERROR，值：没错。
- 对于**无法扫描的速率限制操作**，请使用**Advanced**和**Add Custom Header to Message**,X-TG-RATELIMIT，值：没错。
- 对于**文件分析处于挂起状态**的邮件，请使用**对邮件应用的**操作：“隔离”。

灰色邮件

- 为每个裁决(Marketing、Social、Bulk)启用扫描，并为**Add Text to Subject**预置，**操作**为**Deliver**。
- 对于**批量邮件操作**，请使用**高级**和**添加自定义信头（可选）**:X-Bulk，值：没错。

内容过滤器

- 已选择ENABLED和URL_QUARANTINE_MALICIOUS、URL_REWRITE_SUSPICIOUS、URL_INFORECTION、DKIM_FAILURE、SPF_HARDFAIL、EXECUTIVE_SPOOF、DOMAIN_SPOOF、SDR和TG_RATE_LIMIT
- 本指南稍后将介绍这些内容过滤器

爆发过滤器

- 默认威胁级别为3;请根据您的安全要求进行调整。 如果邮件的威胁级别等于或超过此阈值，邮件将移至爆发隔离区。（1=最低威胁，5=最高威胁）
- 启用邮件修改
- 为“为所有邮件启用”设置的URL重写。

- 将主题更改为： [可能的$threat_category欺诈]

Policies

Add Policy...

Order	Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters	Advanced Phishing Protection	Delete
1	BLOCKLIST	Disabled	Disabled	(use default)	Disabled	BLOCKLIST_QUARANTINE	Disabled	(use default)	
2	ALLOWLIST	Disabled	(use default)	(use default)	Disabled	(use default)	Disabled	(use default)	
3	ALLOW_SPOOF	(use default)	(use default)	(use default)	(use default)	URL_QUARANTINE_MALICIOUS URL_REWRITE_SUSPICIOUS URL_INAPPROPRIATE SDR	(use default)	(use default)	
	Default Policy	IronPort Anti-Spam Positive: Drop Suspected: Quarantine	Sophos McAfee 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: Disabled Marketing: Deliver Social: Deliver Bulk: Deliver ...	URL_QUARANTINE_MALICIOUS URL_REWRITE_SUSPICIOUS URL_INAPPROPRIATE DKIM_FAILURE SPF_HARDFAIL EXECUTIVE_SPOOF ...	Retention Time: Virus: 1 day Other: 4 hours	Not Available	

策略名称（显示）

- **阻止列表邮件策略**
  BLOCKLIST邮件策略配置为禁用除高级恶意软件防护之外的所有服务，并使用QUARANTINE操作链接到内容过滤器。

- **ALLOWLIST邮件策略**
  ALLOWLIST邮件策略已禁用反垃圾邮件、灰色邮件，并且为URL_QUARANTINE_MALICIOUS、URL_REWRITE_SUSPICIOUS、URL_INFORCISE、DKIM_FAILURE、SPF_HARDFAIL、EXECUTIVE SPOOF、DOMAIN_SPOOF、SDR、TG_RATE_LIMIT或您选择和配置的内容过滤器启用了内容过滤器。

- **ALLOW_SPOOF邮件策略**
  ALLOW_SPOOF邮件策略启用所有默认服务，并且为URL_QUARANTINE_MALICIOUS、URL_REWRITE_SUSPICIOUS、URL_INFORCISE、SDR或您选择和配置的内容过滤器启用内容过滤器。

外发邮件策略

默认策略的配置类似于：

反垃圾邮件

- 禁用

防病毒

- 邮件扫描：**仅扫描病毒** 取消选中“包括X报头”复选框。
- （可选）对于所有消息：**Advanced > Other Notification**，启用“Others”并包含您的管理员/SOC联系人电子邮件地址

高级恶意软件保护

- 仅启用文件信誉
- **速率限制上的不可扫描操作**:使用**Advanced**和**Add Custom Header to Message**:X-TG-RATERLIMIT，值：“正确。”

- **包含恶意软件附件的邮**件：使用**Advanced**和**Add Custom Header to Message**:X-TG-OUTBOUND，值："检测到恶意软件。"

灰色邮件

- 禁用

内容过滤器

- 已启用并选择您选择的TG_OUTBOUND_MALICIOUS、Strip_Secret_Header、EXTERNAL_SENDER_REMOVE、ACCOUNT_TAKEOVER或内容过滤器。

爆发过滤器

- 禁用

DLP

- 根据您的DLP许可和DLP配置启用。

其他设置

词典（邮件策略>词典）

- 启用并审阅**Profanity**和**Sexual_Content**字典
- 使用所有执行名称创建**Executive_FED**词典进行伪造邮件检测
- 根据您对策略、环境、安全控制的需要，为受限或其他关键字创建附加词典

目标控制（邮件策略>目标控制）

- 对于默认域，将TLS支持**配置**为首**选**
- 您可以为Web邮件域添加目标并设置较低的阈值
- 有关详细信息，请参阅[使用目标控制设置限制出站邮件的速率]指南。

Destination Control Table — Items per page 20

Add Destination... | Import Table

Domain ▲	IP Address Preference	Destination Limits	TLS Support	DANE Support ^	Bounce Verification *	Bounce Profile	All Delete
.protection.outlook.com	Default	500 concurrent connections, 50 messages per connection, Default recipient limit	Required	Default	Default	Default	☐
gmail.com	Default	20 concurrent connections, 5 messages per connection, 20 recipients in 1 minutes	Default	Default	Default	Default	☐
hotmail.com	Default	20 concurrent connections, 5 messages per connection, 20 recipients in 1 minutes	Default	Default	Default	Default	☐
yahoo.com	Default	20 concurrent connections, 5 messages per connection, 20 recipients in 1 minutes	Default	Default	Default	Default	☐
Default	IPv4 Preferred	500 concurrent connections, 50 messages per connection, No recipient limit	Preferred	None	Off	Default	

Export Table | Delete

** Bounce Verification settings apply only if bounce verification address tagging is in use. See Mail Policies > Bounce Verification.*
^ DANE will not be enforced for domains that have SMTP Routes configured.

内容过滤器

注意：有关内容过滤器的其他信息，请参阅用户指南中的“内容过滤器”，获取您已部署的思科安全邮件网关的相应版本的AsyncOS。

传入内容过滤器

URL_QUARANTINE_MALICIOUS

条件：URL信誉；url-reputation(-10.00, -6.00, "bypass_urls", 1, 1)

操作：隔离：隔离("URL_MALICIOUS")

URL_REWRITE_SUSPICIOUS

条件：URL信誉；url-reputation(-5.90, -5.60, "bypass_urls", 0, 1)

操作：URL信誉；url-reputation-proxy-redirect(-5.90, -5.60,"",0)

URL_INFORCISE

条件：URL类别； url-category(['Adult', 'Child Abuse Content', 'Extreme', 'Hate Speech', 'Illegal Activities', 'Illegal Downloads', 'Illegal Drugs', 'Copying', 'Filter Avoidance'], "bypass_urls", 1, 1)

操作：隔离；duplicate-quarantine("UNITABLE_CONTENT")

DKIM_FAILURE

条件：DKIM身份验证；dkim-authentication == hardfail

操作：隔离；duplicate-quarantine("DKIM_FAIL")

SPF_HARDFAIL

条件：SPF验证；spf-status检==失败

操作：隔离；duplicate-quarantine("SPF_HARDFAIL")

EXECUTIVE_SPOOF

条件：伪造的电邮检测；伪造的电邮检测("Executive_FED", 90, "")

条件：其他报头；报头("X-IronPort-SenderGroup")!= "(?i)allowspoof"

* set **Apply rule:仅当所有条件都匹配时**

操作：添加/编辑信头；edit-header-text("Subject", "(.*)", "[EXTERNAL]\\1")

操作：隔离；重复隔离(“FORGED_EMAIL”)

DOMAIN_SPOOF

条件：其他报头；header("X-spoof")

操作：隔离；duplicate-quarantine("ANTI_SPOOF")

特别提款权

条件：域信誉;sdr-reputation(['bad'], "")

条件：域信誉;sdr-age (“天”、<、5、“”)

* set **Apply rule:如果一个或多个条件匹配**

操作：隔离；duplicate-quarantine("SDR_DATA")

TG_RATE_LIMIT

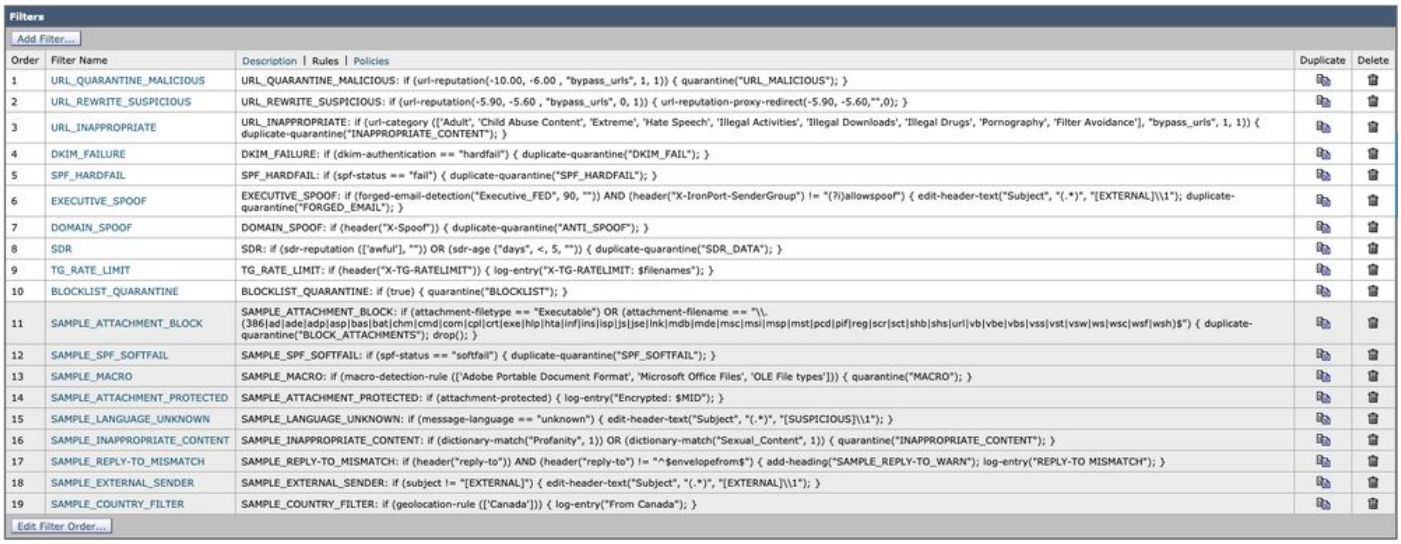
条件：其他报头；报头("X-TG-RATELIMIT")

操作：添加日志条目；log-entry("X-TG-RATELIMIT:$filenames")

BLOCKLIST_QUARANTINE

条件：(无)

操作：隔离；隔离 (“阻止列表”)



Filters

Add Filter...

Order	Filter Name	Description | Rules | Policies	Duplicate	Delete
1	URL_QUARANTINE_MALICIOUS	URL_QUARANTINE_MALICIOUS: if (url-reputation(-10.00, -6.00 , "bypass_urls", 1, 1)) { quarantine("URL_MALICIOUS"); }		
2	URL_REWRITE_SUSPICIOUS	URL_REWRITE_SUSPICIOUS: if (url-reputation(-5.90, -5.60 , "bypass_urls", 0, 1)) { url-reputation-proxy-redirect(-5.90, -5.60,"",0); }		
3	URL_INAPPROPRIATE	URL_INAPPROPRIATE: if (url-category (['Adult', 'Child Abuse Content', 'Extreme', 'Hate Speech', 'Illegal Activities', 'Illegal Downloads', 'Illegal Drugs', 'Pornography', 'Filter Avoidance'], "bypass_urls", 1, 1)) { duplicate-quarantine("INAPPROPRIATE_CONTENT"); }		
4	DKIM_FAILURE	DKIM_FAILURE: if (dkim-authentication == "hardfail") { duplicate-quarantine("DKIM_FAIL"); }		
5	SPF_HARDFAIL	SPF_HARDFAIL: if (spf-status == "fail") { duplicate-quarantine("SPF_HARDFAIL"); }		
6	EXECUTIVE_SPOOF	EXECUTIVE_SPOOF: if (forged-email-detection("Executive_FED", 90, "")) AND (header("X-IronPort-SenderGroup") != "(?i)allowspoof") { edit-header-text("Subject", "(.*)", "[EXTERNAL]\\1"); duplicate-quarantine("FORGED_EMAIL"); }		
7	DOMAIN_SPOOF	DOMAIN_SPOOF: if (header("X-Spoof")) { duplicate-quarantine("ANTI_SPOOF"); }		
8	SDR	SDR: if (sdr-reputation (['awful'], "")) OR (sdr-age ("days", <, 5, "")) { duplicate-quarantine("SDR_DATA"); }		
9	TG_RATE_LIMIT	TG_RATE_LIMIT: if (header("X-TG-RATELIMIT")) { log-entry("X-TG-RATELIMIT: $filenames"); }		
10	BLOCKLIST_QUARANTINE	BLOCKLIST_QUARANTINE: if (true) { quarantine("BLOCKLIST"); }		
11	SAMPLE_ATTACHMENT_BLOCK	SAMPLE_ATTACHMENT_BLOCK: if (attachment-filetype == "Executable") OR (attachment-filename == "\\.(386|ad|ade|adp|asp|bas|bat|chm|cmd|com|cpl|crt|exe|hlp|hta|inf|ins|isp|js|jse|lnk|mdb|mde|msc|msi|msp|mst|pcd|pif|reg|scr|sct|shb|shs|url|vb|vbe|vbs|vss|vst|vsw|ws|wsc|wsf|wsh)$") { duplicate-quarantine("BLOCK_ATTACHMENTS"); drop(); }		
12	SAMPLE_SPF_SOFTFAIL	SAMPLE_SPF_SOFTFAIL: if (spf-status == "softfail") { duplicate-quarantine("SPF_SOFTFAIL"); }		
13	SAMPLE_MACRO	SAMPLE_MACRO: if (macro-detection-rule (['Adobe Portable Document Format', 'Microsoft Office Files', 'OLE File types'])) { quarantine("MACRO"); }		
14	SAMPLE_ATTACHMENT_PROTECTED	SAMPLE_ATTACHMENT_PROTECTED: if (attachment-protected) { log-entry("Encrypted: $MID"); }		
15	SAMPLE_LANGUAGE_UNKNOWN	SAMPLE_LANGUAGE_UNKNOWN: if (message-language == "unknown") { edit-header-text("Subject", "(.*)", "[SUSPICIOUS]\\1"); }		
16	SAMPLE_INAPPROPRIATE_CONTENT	SAMPLE_INAPPROPRIATE_CONTENT: if (dictionary-match("Profanity", 1)) OR (dictionary-match("Sexual_Content", 1)) { quarantine("INAPPROPRIATE_CONTENT"); }		
17	SAMPLE_REPLY-TO_MISMATCH	SAMPLE_REPLY-TO_MISMATCH: if (header("reply-to")) AND (header("reply-to") != "^$envelopefrom$") { add-heading("SAMPLE_REPLY-TO_WARN"); log-entry("REPLY-TO MISMATCH"); }		
18	SAMPLE_EXTERNAL_SENDER	SAMPLE_EXTERNAL_SENDER: if (subject != "[EXTERNAL]") { edit-header-text("Subject", "(.*)", "[EXTERNAL]\\1"); }		
19	SAMPLE_COUNTRY_FILTER	SAMPLE_COUNTRY_FILTER: if (geolocation-rule (['Canada'])) { log-entry("From Canada"); }		

Edit Filter Order...

外发内容过滤器

TG_OUTBOUND_MALICIOUS

条件：恶意软件的其他报头；报头(“X-TG-OUTBOUND”==)

操作：隔离；隔离(“TG_OUTBOUND_MALWARE”)

Strip_Secret_Header

条件：其他标题；标题（“占位符”）==占位符

操作：剥离信头；剥离信头("X-IronPort-Tenant")

EXTERNAL_SENDER_REMOVE

条件：(无)

操作：添加/编辑信头；edit-header-text("Subject", "\\[EXTERNAL\\]\\s?", "")

ACCOUNT_TAKEOVER

条件：其他报头；报头("X-AMP-Result")==(?i)恶意

条件：URL信誉；url — 信誉(-10.00, -6.00, "", 1, 1)

*设置**应用规则：如果一个或多个条件匹配**

操作：Notify;notify ("<插入管理员或通讯邮件地址>", "POSSIBLE ACCOUNT TAKEOVER", "", "ACCOUNT_TAKEOVER_WARNING")

操作：duplicate-quarantine("ACCOUNT_TAKEOVER")

Filters

Add Filter...

Order	Filter Name	Description | Rules | Policies	Duplicate	Delete
1	Stop_O365_OpenRelay	Stop_O365_OpenRelay: if (header("X-IronPort-Tenant") != "placeholder") { duplicate-quarantine("OPEN_RELAY"); }		
2	TG_OUTBOUND_MALICIOUS	TG_OUTBOUND_MALICIOUS: if (header("X-TG-OUTBOUND") == "MALWARE") { quarantine("TG_OUTBOUND_MALWARE"); }		
3	Strip_Secret_Header	Strip_Secret_Header: if (header("PLACEHOLDER") == "PLACEHOLDER") { strip-header("X-IronPort-Tenant"); }		
4	EXTERNAL_SENDER_REMOVE	EXTERNAL_SENDER_REMOVE: if (true) { edit-header-text("Subject", "\\[EXTERNAL\\]\\s?", ""); }		
5	ACCOUNT_TAKEOVER	ACCOUNT_TAKEOVER: if (header("X-AMP-Result") == "(?i)malicious") OR (url-reputation(-10.00, -6.00 , "", 1, 1)) { notify ("myit@mycompany.com", "POSSIBLE ACCOUNT TAKEOVER", "", "ACCOUNT_TAKEOVER_WARNING"); duplicate-quarantine("ACCOUNT_TAKEOVER"); }		
6	ENCRYPT_OUT	ENCRYPT_OUT: if (subject == "(?i)*encrypt*") { edit-header-text("Subject", "(?i)*encrypt*\\s?", ""); encrypt-deferred ("CRES_HIGH", "$Subject", 0); }		
7	TG_RATE_LIMIT	TG_RATE_LIMIT: if (header("X-TG-OUTBOUND-RATELIMIT")) { tag-message ("NOOP"); }		

Edit Filter Order...

对于思科安全电邮云客户，金牌配置和最佳实践建议中确实包含示例内容过滤器。此外，请查看“SAMPLE_”过滤器，了解有关对您的配置有帮助的条件和操作的详细信息。

Cisco Live

Cisco Live在全球托管许多会话，并提供涵盖思科安全电邮最佳实践的面对面会话和技术分组讨论。有关过去的会话和访问权限，请访问Cisco Live（需要CCO登录）：

- 思科电邮安全：最佳实践和优化 — BRKSEC-2131
- DMARC更新您的电子邮件边界 — BRKSEC-2131
- 修复电子邮件！ — 思科邮件安全高级故障排除 — BRKSEC-3265
- 用于思科电邮安全的API集成 — DEVNET-2326
- 通过思科的云邮件安全保护SaaS邮箱服务 — BRKSEC-1025
- 邮件安全：最佳实践和优化 — TECSEC-2345
- 250 NOT OK — 采用思科电邮安全进行防御 — TECSEC-2345
- 思科域保护和思科高级网络钓鱼防护：充分利用邮件安全的下一层！- BRKSEC-1243
- SPF不是“Spoof”的缩写！让我们充分利用邮件安全领域的下一层！- DGTL-BRKSEC-2327

其他信息

思科安全电子邮件网关文档

- 版本说明
- 用户指南

- CLI参考指南
- 思科安全邮件网关的API编程指南
- 思科安全邮件网关中使用的开源
- 思科内容安全虚拟设备安装指南（包括vESA）

安全邮件云网关文档

- 版本说明
- 用户指南

Cisco Secure Email and Web Manager文档

- 版本说明和兼容性列表
- 用户指南
- Cisco Secure Email and Web Manager的API编程指南
- 思科内容安全虚拟设备安装指南（包括vSMA）

思科安全产品文档

- 思科安全产品组合命名架构

相关信息

- 思科安全邮件安全合规性
- 产品说明：安全电子邮件
- 思科通用云术语
- 思科支持和下载
- [外部] OpenSPF:SPF基本信息和高级信息

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。