配置Cloud Gateway Gold配置

目錄

簡介

本文檔對為思科安全電子郵件雲網關提供的Gold配置進行了深入分析。思科安全電子郵件雲客戶的Gold Configuration是雲網關和思科安全電子郵件和網路管理器的最佳實踐和零日配置。思科安全電子郵件雲部署同時使用雲網關和至少一(1)個電子郵件和網路管理器。部分配置和最佳實踐指導管理員使用位於郵件和Web管理器上的隔離區進行集中管理。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco Secure Email Gateway或Cloud Gateway，UI和CLI管理
- Cisco Secure Email Email and Web Manager， UI級別管理
- Cisco Secure Email Cloud客戶可以請求CLI訪問；請參閱：命令列介面(CLI)訪問

採用元件

本文檔中的資訊來自針對思科安全電子郵件雲客戶和管理員的金牌配置和最佳實踐建議。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

相關產品

本檔案也適用於以下專案：

- 思科安全電子郵件網關內部硬體或虛擬裝置
- Cisco Secure Email and Web Manager本地硬體和虛擬裝置

策略隔離區

在Email and Web Manager上為Cisco Secure Email Cloud客戶配置和維護隔離區。請登入您的電子郵件和Web管理器以檢視隔離區：

- ACCOUNT_TAKEOVER
- 反欺騙
- BLOCK_ATTACHMENTS
- 阻止清單
- DKIM_FAIL
- DMARC_QUARANTINE
- DMARC_REJECT
- FORGED_EMAIL
- INADEQUATE_CONTENT
- 宏
- OPEN_RELAY
- SDR_DATA
- SPF_HARDFAIL
- SPF_SOFTFAIL
- TG_OUTBOUND_MALWARE
- URL_MALIOUS

雲網關Gold配置

> **警告**：在生產環境中提交配置更改之前，需要檢查和瞭解基於本文檔中提供的最佳做法對配置所做的任何更改。更改配置之前，請諮詢您的Cisco CX工程師、指定服務經理(DSM)或客戶團隊。

基本配置

郵件策略>收件人訪問表(RAT)

收件人訪問表定義公共偵聽程式接受哪些收件人。該表至少指定地址以及是接受還是拒絕。請檢查RAT以根據需要新增和管理域。

網路> SMTP路由

如果SMTP路由目標為Microsoft 365，請參閱Office365 Throttling CES New Instance with "4.7.500 Server busy。請稍後再試」。

安全服務

所列服務是針對所有思科安全電子郵件雲客戶配置的，其值如下：

IronPort反垃圾郵件(IPAS)

- 啟用並配置Always scan 1M和Never scan 2M
- 掃描單個郵件超時：60秒

URL篩選

- 啟用URL分類和信譽過濾器
- （可選）建立和配置名為「bypass_urls」的URL允許清單。
- 啟用網路互動跟蹤
- 高級設定： URL查詢超時：15秒正文和附件中掃描的最大URL數：400重寫消息中的URL文本和HREF:否URL記錄：已啟用
- （可選）自適用於雲閘道的AsyncOS 14.2起，已提供URL追溯判定和URL修正；請參閱提供的版本說明和為安全電子郵件網關和雲網關配置URL過濾

灰色郵件檢測

- 啟用並配置「始終掃描1M」和「從不掃描2M」
- 掃描單個郵件超時：60秒

爆發過濾器

- 啟用自適應規則

- 要掃描的最大郵件大小：2米
- 啟用網路互動跟蹤

高級惡意軟體防護>檔案信譽和分析

- 啟用檔案信譽
- 啟用檔案分析 請參閱「全域性設定」以檢視「檔案分析」的檔案型別

郵件跟蹤

- 啟用拒絕的連線記錄（如果需要）

系統管理

使用者（系統管理>使用者）

- 請記得檢視並設定與本地使用者帳戶和密**碼設定關聯的密碼策略**
- 如果可能，配置並啟用輕量級目錄訪問協定(LDAP)進行身份驗證**(系統管理> LDAP**)

日誌訂閱（系統管理>日誌訂閱）

- 如果未配置，請建立並啟用： 配置歷史記錄日誌URL信譽客戶端日誌
- 在「日誌訂閱全域性設定」(Log Subscriptions Global Settings)中，編輯設定並將標頭新增到**到**、**從**、**回覆**、**發件人**。

其他配置（可選）

需要審查和考慮的其他服務：

系統管理> LDAP

- 如果配置LDAP，思科建議啟用了SSL的LDAP

URL防禦

- 有關URL防禦的最新配置最佳實踐，請參閱為安全電子郵件網關和雲網關配置URL過濾。
- 思科也深入研究URL防禦；請參閱URL防禦指南。
- URL防禦指南中包含的一些範例也會包含在本檔案中。

SPF

- 發件人策略框架(SPF)DNS記錄是在雲網關外部建立的。因此，思科強烈建議所有客戶將SPF、DKIM和DMARC最佳實踐融入其安全狀態。有關SPF驗證的詳細資訊，請參閱SPF配置和最佳實踐。
- 對於Cisco Secure Email Cloud客戶，系統會為每個分配的主機名發佈所有雲網關的宏，以便更輕鬆地新增所有主機。
- 將此項放在~all或 — all之前，放到當前DNS TXT(SPF)記錄中（如果存在）：

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

註：確保SPF記錄以~all或-all結尾。在任何更改之前和之後驗證域的SPF記錄！

- 有關SPF的更多資訊的建議資訊和工具：
  SPF記錄檢查器 — 免費SPF查詢(dmarcian.com)SPF記錄語法表 — 所有SPF - dmarcian.com

其他SPF示例

- SPF的一個絕佳示例是，您從雲網關收到電子郵件並從其他郵件伺服器傳送出站電子郵件。可以使用「a：」機制指定郵件主機：

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

- 如果您僅通過雲網關傳送出站電子郵件，可以使用：

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

- 在本示例中，「ip4：」或「ip6：」機制指定IP地址或IP地址範圍：

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

CLI級別更改

- 如前提條件中所述，思科安全電子郵件雲客戶可以請求CLI訪問；請參閱指令行介面(CLI)存取。

反欺騙濾波器

- 請務必檢視防偽的最佳實踐指南
- 本指南為您提供電子郵件欺騙預防的深層示例和配置最佳實踐

新增標題篩選器

- 請僅使用CLI，然後寫入並啟用addHeaders消息過濾器:

```
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");
}
```

主機訪問表(郵件策略>主機訪問表(HAT))

HAT概述>其他發件人組

- ESA使用手冊：建立郵件處理的發件人組 BYPASS_SBRS — 對跳過信譽的源設定更高位置 MY_TRUSTED_SPOOF_HOSTS — 欺騙過濾器的一部分TLS_REQUIRED — 用於TLS強制連線

在預定義的SUSPECTLIST發件人組中

- ESA使用手冊：發件人驗證：主機 啟用「SBRS無分數」。（可選）啟用「由於臨時DNS故障，連線主機PTR記錄查詢失敗」。

積極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評分「無」]策略：已限制
- ACCEPTLIST [0.0到10.0]策略：已接受

> **附註**：HAT示例顯示了附加配置的郵件流策略(MFP)。 有關MFP的完整資訊，請參閱使用手冊中的「瞭解郵件管道>接收/接收」，瞭解您已部署的思科安全郵件網關的相應版本的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...

郵件流策略(默認策略引數)

預設策略引數

安全設定

- 將傳輸層安全(TLS)設定為首選
- 啟用發件人策略框架(SPF)
- 啟用DomainKeys Identified Mail(DKIM)
- 啟用基於域的報文驗證、報告和一致性(DMARC)驗證並傳送彙總反饋報告

> **附註**：DMARC需要額外的調整才能配置。有關DMARC的詳細資訊，請參閱使用手冊中的「電子郵件驗證> DMARC驗證」，瞭解您已部署的思科安全電子郵件網關的相應版本的AsyncOS。

傳入郵件策略

預設策略配置如下：

反垃圾郵件

- 啟用，閾值保留為預設閾值。（對計分的修改可能會增加誤報。）

防病毒

- 郵件掃描：**僅掃描病毒** 確保「包括X報頭」覈取方塊已啟用
- 對於**無法掃描的郵件**和**感染病毒的郵件**，請將Archive Original Message設定為No

AMP

- 對於**無法掃描的消息錯誤操作**，請使用Advanced和Add Custom Header to Message,X-TG-MSGERROR，值：沒錯。
- 對於**速率限制上的不可掃描操作**，請使用Advanced和Add Custom Header to Message,X-TG-RATERLIMIT，值：沒錯。
- 對於**檔案分析處於掛起狀態**的郵件，請使用**對郵件應用的**操作：「隔離」。

灰色郵件

- 對每個判定結果(Marketing、Social、Bulk)啟用掃描，並為**Add Text to Subject**預置，**操作為Deliver**。
- 有關**批次郵件操作**，請使用**Advanced**和**Add Custom Header（可選）**:X-Bulk，值：沒錯。

內容過濾器

- 已選擇ENABLED和URL_QUARANTINE_MALICIOUS、URL_REWRITE_SUSPICIOUS、URL_INSIGHT、DKIM_FAILURE、SPF_HARDFAIL、EXECUTIVE_SPOOF、DOMAIN_SPOOF、SDR和TG_RATE_LIMIT
- 本指南稍後將介紹這些內容過濾器

爆發過濾器

- 預設威脅級別為3;請根據您的安全要求進行調整。 如果郵件的威脅級別等於或超過此閾值，該郵件將移至爆發隔離區。（1=最低威脅，5=最高威脅）
- 啟用消息修改

- 為「為所有郵件啟用」設定的URL重寫。
- 將主題更改為： [可能的$threat_category欺詐]

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	

策略名稱（顯示）

- **阻止清單郵件策略**
  BLOCKLIST郵件策略配置為禁用除高級惡意軟體防護以外的所有服務，並使用QUARANTINE操作連結到內容過濾器。

- **ALLOWLIST郵件策略**
  ALLOWLIST郵件策略已禁用Antispam、Graymail以及為URL_QUARANTINE_MALICIOUS、URL_REWRITE_SUSPICIOUS、URL_INSIBLE、DKIM_FAILURE、SPF_HARDFAIL、EXECUTIVE SPOOF、DOMAIN_SPOOF、SDR、TG_RATE_LIMIT或您選擇和配置的內容過濾器啟用的內容過濾器。

- **ALLOW_SPOOF郵件策略**
  ALLOW_SPOOF郵件策略啟用所有預設服務，並為URL_QUARANTINE_MALICIOUS、URL_REWRITE_SUSPICIOUS、URL_INSIBLE、SDR或您選擇和配置的內容過濾器啟用內容過濾器。

傳出郵件策略

預設策略配置如下：

反垃圾郵件

- 已禁用

防病毒

- 郵件掃描：**僅掃描病毒** 取消選中「包括X報頭」覈取方塊。
- （可選）對於所有消息：**Advanced > Other Notification**，啟用「Others」並包含您的管理員/SOC聯絡人電子郵件地址

高級惡意軟體防護

- 僅啟用檔案信譽
- **對速率限制的不可掃描操**作：使用**Advanced**和**Add Custom Header to Message**:X-TG-

RATERLIMIT，值：「沒錯。」
- **包含惡意軟體附件的郵**件：使用**Advanced**和**Add Custom Header to Message**:X-TG-OUTBOUND，值："檢測到惡意軟體。"

灰色郵件

- 已禁用

內容過濾器

- 選擇啟用和TG_OUTBOUND_MALICIOUS、Strip_Secret_Header、EXTERNAL_SENDER_REMOVE、ACCOUNT_TAKEOVER或內容過濾器。

爆發過濾器

- 已禁用

DLP

- 根據您的DLP許可和DLP配置啟用。

其他設定

詞典（郵件策略>詞典）

- 啟用並審閱**Profanity**和**Sexual_Content**字典
- 使用所有執行名稱建立**Executive_FED**詞典，用於偽造電子郵件檢測
- 根據您的策略、環境、安全控制需要，為受限關鍵字或其他關鍵字建立附加詞典

目標控制（郵件策略>目標控制）

- 對於預設域，將**TLS支援**配置為**首選**
- 您可以為Web郵件域新增目標並設定較低的閾值
- 如需詳細資訊，請參閱我們的使用目的地控制設定限制您的傳出郵件速率指南。

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.

內容過濾器

附註：有關內容過濾器的其他資訊，請參閱使用手冊中的「內容過濾器」，獲取您已部署的思科安全郵件網關的相應版本的AsyncOS。

傳入內容過濾器

URL_QUARANTINE_MALICIOUS

條件：URL信譽；url-reputation(-10.00, -6.00, "bypass_urls", 1, 1)

Action:隔離：隔離("URL_MALIOUS")

URL_REWRITE_SUSPICIOUS

條件：URL信譽；url-reputation(-5.90, -5.60, "bypass_urls", 0, 1)

Action:URL信譽；url-reputation-proxy-redirect(-5.90, -5.60,"",0)

URL_INADEQUATE

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

Action:Quarantine;duplicate-quarantine("UNITABLE_CONTENT")

DKIM_FAILURE

條件：DKIM身份驗證;dkim身份驗證==硬失敗

Action:隔離；duplicate-quarantine("DKIM_FAIL")

SPF_HARDFAIL

條件：SPF驗證；spf-status驗==失敗

Action:Quarantine;duplicate-quarantine("SPF_HARDFAIL")

EXECUTIVE_SPOOF

條件：偽造的電子郵件檢測；偽造的電子郵件檢測("Executive_FED", 90, "")

條件：Other Header; header("X-IronPort-SenderGroup")!= "(?i)allowspoof"

* set **Apply rule:僅當所有條件都匹配時**

Action:新增/編輯標題；edit-header-text("Subject", "(.*)", "[EXTERNAL]\\1")

Action:Quarantine; duplicate-quarantine("FORGED_EMAIL")

域_欺騙

條件：其他標題；header("X-spoof")

Action:Quarantine;duplicate-quarantine("ANTI_SPOOF")

特別提款權

條件：域信譽;sdr-reputation(['bad'], "")

條件：域信譽;sdr-age （「天」、<、5、「」 ）

* set **Apply rule:如果一個或多個條件匹配**

Action:Quarantine;duplicate-quarantine("SDR_DATA")

TG_RATE_LIMIT

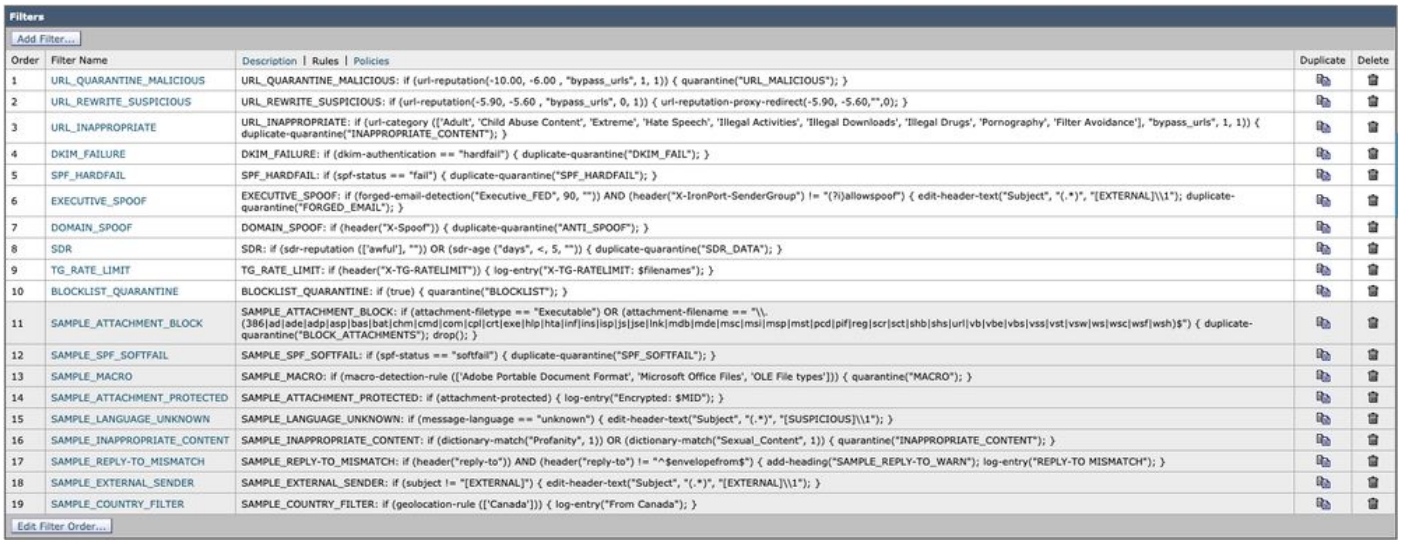
條件：其他標頭；標頭("X-TG-RATERLIMIT")

Action:新增日誌條目；log-entry("X-TG-RATERLIMIT:$filenames")

BLOCKLIST_QUARANTINE

條件：(無)

Action:隔離；隔離（「阻止清單」 ）



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...

傳出內容過濾器

TG_OUTBOUND_MALICIOUS

條件：惡意軟體的其他標頭；標頭("X-TG-OUTBOUND")==

Action:隔離；隔離("TG_OUTBOUND_MALWARE")

Strip_Secret_Header

條件：其他標題；標題("PLACEHOLDER")==PLACEHOLDER

Action:剝離報頭；剝離報頭("X-IronPort-Tenant")

EXTERNAL_SENDER_REMOVE

條件：(無)

Action:新增/編輯標題；edit-header-text("Subject", "\\[EXTERNAL\\]\\s?", "")

ACCOUNT_TAKEOVER

條件：其他報頭；報頭("X-AMP-Result")==(?i)惡意

條件：URL信譽；url-reputation(-10.00, -6.00, "", 1, 1)

*設定**應用規則：如果一個或多個條件匹配**

Action:Notify;notify (""<插入管理員或通訊電子郵件地址>", "POSSIBLE ACCOUNT TAKEOVER", "", "ACCOUNT_TAKEOVER_WARNING")

Action: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...

對於思科安全電子郵件雲客戶，我們的金牌配置和最佳實踐建議中確實包含示例內容過濾器。此外，請檢視「SAMPLE_」過濾器，瞭解對您的配置有幫助的條件和操作的詳細資訊。

Cisco Live

Cisco Live在全球託管許多會話，並提供涵蓋思科安全電郵最佳實踐的現場會話和技術分會。對於過去的會話和訪問許可權，請訪問Cisco Live（需要CCO登入）：

- Cisco Email Security:最佳實踐和微調 — BRKSEC-2131
- DMARC制定您的電子郵件周界 — BRKSEC-2131
- 正在修復電子郵件！ — 思科電子郵件安全高級故障排除 — BRKSEC-3265
- 適用於思科電子郵件安全的API整合 — DEVNET-2326
- 利用思科的雲郵件安全保護SaaS郵箱服務 — BRKSEC-1025
- 電子郵件安全：最佳實踐和微調 — TECSEC-2345
- 250 not OK — 使用思科電子郵件安全進行防禦 — TECSEC-2345
- 思科域保護和思科高級網路釣魚防護：充分利用郵件安全領域的下一層！- BRKSEC-1243
- SPF不是「Spoof」的縮寫！讓我們充分利用電子郵件安全領域的下一層！- DGTL-BRKSEC-2327

其他資訊

思科安全電子郵件閘道檔案

- 發佈通知

- 使用手冊
- CLI參考指南
- 思科安全電子郵件網關API程式設計指南
- 思科安全電子郵件網關中使用的開源
- 思科內容安全虛擬裝置安裝指南（包括vESA）

安全電子郵件雲網關文檔

- 發佈通知
- 使用手冊

Cisco Secure Email and Web Manager文檔

- 發行說明和相容表
- 使用手冊
- Cisco Secure Email and Web Manager的API程式設計指南
- 思科內容安全虛擬裝置安裝指南（包括vSMA）

思科安全產品檔案

- 思科安全產品組合命名架構

相關資訊

- 思科安全電子郵件安全合規性
- 產品說明：安全電子郵件
- 思科通用雲術語
- 思科支援與下載
- [外部] OpenSPF:SPF基本資訊和高級資訊

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。