對接收和傳送郵件期間的間歇問題和中斷連線進行故障排除

目錄

簡介

本文檔介紹如何對接收和傳送郵件期間的間歇性問題和中斷連線進行故障排除。

必要條件

思科建議您瞭解以下主題：

- Cisco Private Internet Exchange(PIX)或Adaptive Security Appliance(ASA)版本7.x及更高版本
- 思科電子郵件安全裝置(ESA)

背景資訊

Cisco ESA電子郵件網關本身就是電子郵件防火牆。這樣就不需要上游防火牆（例如Cisco PIX或ASA）來檢查進出某個ESA的郵件流量。建議為任何安全裝置主機地址禁用防火牆上的擴展簡單郵件傳輸協定(ESMTP)應用檢查功能。預設情況下，對通過思科防火牆的所有連線啟用ESMTP協定檢查。這表示透過TCP連線埠25在郵件閘道之間發出的所有命令，以及個別訊息標頭都會進行分析，以嚴格遵守要求建議(RFC)規範，包括RFC的821、1123和1870。已定義最大收件人數和郵件大小預設值，這些值可能導致與您的ESA之間的傳送出現問題。此處列出了這些特定配置預設值（取自思科命令查詢工具）。

inspect esmtp命令包括**fixup smtp**命令以前提供的功能，並為某些ESMTP命令提供附加支援。ESMTP應用檢查增加了對8個ESMTP命令的支援，包括AUTH、EHLO、ETRN、HELP、SAML、SEND、SOML和VRFY等。除了支援七個RFC 821命令(DATA、HELO、MAIL、NOOP、QUIT、**RCPT**、**RSET**)外，安全裝置總共支援15個SMTP命令。不支援其他ESMTP命令，如ATRN、**STARTLS**、**ONEX**、**VERB**、**CHUNKING和專用擴展。**不支援的命令被轉換為X，但被內部伺服器

拒絕。這會導致出現消息，例如500 Command unknown:XXX。不完整的命令將被丟棄。

inspect esmtp命令將伺服器SMTP標語中的字元更改為星號，但「2」、「0」、「0」字元除外。回車(CR)和換行符(LF)被忽略。啟用SMTP檢測後，用於互動SMTP的會話將等待有效的命令，並且如果以下規則未遵守，防火牆esmtp狀態機將保持會話的正確狀態：

- SMTP命令的長度必須至少為四個字元。
- SMTP命令必須以回車符和換行符終止。
- SMTP命令必須等待響應才能發出下一個回覆。

SMTP伺服器使用數字回覆代碼和可選的可讀字串來響應客戶端請求。SMTP應用程式檢查控制並減少了使用者可以使用的命令以及伺服器返回的消息。SMTP檢測執行三項主要任務：

- 將SMTP請求限製為七個基本SMTP命令和八個擴展命令。
- 監視SMTP命令響應序列。
- 生成審計追蹤。替換郵108002地址中嵌入的無效字元時，將生成稽核記錄屬性。如需詳細資訊，請參閱RFC 821。

SMTP檢查監視以下異常簽名的命令和響應順序：

- 截斷的命令。
- 命令終止不正確（未以<CR><LR>終止）。
- 如果發現用於PCI Express(PIPE)簽名的PHY介面作為MAIL from或RCPT命令的引數，會話將關閉。使用者無法設定。
- SMTP伺服器進行意外轉換。
- 對於未知命令，安全裝置會將資料包中的所有字元更改為X。在這種情況下，伺服器將向客戶端生成錯誤代碼。由於資料包發生變化，必須重新計算或調整TCP校驗和。
- TCP資料流編輯。

show service-policy inspect ESMTP的輸出提供了預設檢查值及其相應的操作。

```
Global policy:
Service-policy: global_policy
Class-map: inspection_default
Inspect: esmtp _default_esmtp_map, packet 104468, drop 0, reset-drop 0
mask-banner, count 639 obfuscate the SMTP banner greeting
match cmd line length gt 512 deny all SMTP commands (and close connection)
drop-connection log, packet 0
match cmd RCPT count gt 100 drop all messages (and connection) with more
than 100 recipients
drop-connection log, packet 0
match body line length gt 998 log all messages with lines > 998 chars
log, packet 0
match header line length gt 998 drop all messages (and connection)
with headers > 998 chars
drop-connection log, packet 41
match sender-address length gt 320 drop all messages (and connection) with
envelope sender > 320 bytes
drop-connection log, packet 0
match MIME filename length gt 255 drop all messages (and connection) with
MIME attachment filenames > 255 bytes
drop-connection log, packet 0
match ehlo-reply-parameter others obfuscate extended commands not explicitly
noted in the RFCs (such as STARTTLS)
mask, packet 2555
```

問題

有時，思科ESA可能無法正確傳送或接收消息。以下一個或多個消息可在Cisco ESA裝置mail_logs中看到：

- 消息中止MID XXX
- 接收中止的21916丟失
- ICID 21916 close
- 連線錯誤：DCID:XXX域：example.com IP:10.1.2.3埠：25個詳細資訊：[錯誤60] 介面操作超時：10.10.10.1原因：網路錯誤

解決方案

其中一些預設設定可能會影響傳輸層安全(TLS)加密郵件的傳送、郵件清單活動和故障排除。更好的策略可能會讓您利用防火牆檢查未首先通過安全裝置的所有剩餘電子郵件流量，同時免除所有具有此功能的流量。此示例說明如何調整預設配置（如前所述），以免除單個安全主機地址的ESMTP應用檢測。

您可以定義進出思科ESA內部地址的所有流量，以便在模組化策略框架(MPF)類對映中參考：

```
access-list ironport_esa_internal extended permit ip any 192.168.1.1
access-list ironport_esa_internal extended permit ip 192.168.1.1 any
```

這將建立一個新的類對映以專門匹配或選擇要以不同方式處理的流量：

```
class-map ironport_esa
match address ironport_esa_internal
```

本節連結新的思科類對映並禁用ESMTP協定檢測功能：

```
policy-map global_policy
class ironport_esa
no inspect esmtp
```

另請注意address translation語句，該語句可幫助控制到地址的傳入和半開放（初始）連線的數量。這可用於對抗拒絕服務攻擊(DoS)，但可能會干擾傳送速率。

用於跟蹤**NAT**和**STATIC**命令的引數的格式…… [tcp(max_conns)] [max_embryonic]。
此示例指定總共50個TCP連線和100個半開啟或半開連線嘗試的限制：

```
static (inside,outside) 1.1.1.1 192.168.1.1 netmask 255.255.255.255 tcp 50 100
```