升級後Exchange Server與SEG AsyncOS 15.0的舊連線故障排除

目錄

[簡介](#)
[採用元件](#)
[問題](#)
[解決方案](#)
[在CLI中：](#)
[在GUI中：](#)
[相關資訊](#)

簡介

本文檔介紹在升級到15.0版後通過安全電子郵件網關(SEG)修復Exchange 2013（或更舊）連線問題的步驟。

採用元件

Exchange 2013或更高版本。

SEG版本15.0。

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。

問題

將SEG升級到版本15.0後，未在2013年以前的Exchange伺服器之間建立連線。如果從CLI檢查tophosts，可以看到該域被標籤為down(*)

```
mx1.cisco.com > tophosts

Sort results by:

1. Active Recipients
2. Connections Out
3. Delivered Recipients
4. Hard Bounced Recipients
5. Soft Bounced Events
[1]> 1

Status as of:                  Sun Sep 03 11:44:11 2023 -03
```

```
Hosts marked with '*' were down as of the last delivery attempt.

                          Active  Conn.     Deliv.       Soft       Hard
#   Recipient Host        Recip.    Out     Recip.    Bounced    Bounced
1*  cisco.com         118      0          0          0     507
2*  alt.cisco.com     94       0        226          0     64
3*  prod.cisco.com    89       0          0          0     546
```

在Mail_logs中，您可以看到由於網路錯誤而導致的域連接失敗。

```
Thu Aug 29 08:16:21 2023 Info: Connection Error: DCID 4664840 domain: cisco.com IP: 10.0.0.1 port: 25 d
```

在資料包捕獲中，可以看到Exchange伺服器在TLS協商後立即關閉與FIN資料包的連線。

解決方案

確認Exchange Server的版本是2013或更舊版本，然後可以使用此密碼字串作為解決方法，以允許SEG連線到那些較舊版本的伺服器。這允許郵件在可以將exchange升級到當前支援的版本之前傳遞。

```
ECDH+aRSA:ECDH+ECDSA:DHE+DSS+AES:AES128:AES256:!SRP:!AESGCM+DH+aRSA:!AESGCM+RSA:!aNULL:!eNULL:!DES:!3DE
```

您可以通過命令列介面(CLI)或Web圖形使用者介面(GUI)輸入此資訊。
在CLI中：

```
mx1.cisco.com> sslconfig

Choose the operation you want to perform:
- GUI - Edit GUI HTTPS ssl settings.
- INBOUND - Edit Inbound SMTP ssl settings.
- OUTBOUND - Edit Outbound SMTP ssl settings.
- VERIFY - Verify and show ssl cipher list.
- OTHER_CLIENT_TLSV10 - Edit TLS v1.0 for other client services.
- PEER_CERT_FQDN - Validate peer certificate FQDN compliance for Alert Over TLS, Outbound SMTP, updater
- PEER_CERT_X509 - Validate peer certificate X509 compliance for Alert Over TLS, Outbound SMTP, updater
[]> outbound

Enter the outbound SMTP ssl method you want to use.
1. TLS v1.1
2. TLS v1.2
3. TLS v1.0
[2]>

Enter the outbound SMTP ssl cipher you want to use.
[!aNULL:!eNULL]> ECDH+aRSA:ECDH+ECDSA:DHE+DSS+AES:AES128:AES256:!SRP:!AESGCM+DH+aRSA:!AESGCM+RSA:!aNULL

.....
Hit enter until you are back to the default command line.
```

```
mx1.cisco.com> commit
```

在GUI中：
步驟1.在System Administration索引標籤上選擇。
步驟2.選擇SSL Configuration。
步驟3.選擇Edit Settings按鈕。
步驟4.更改出站SMTP SSL密碼以使用本文章中提供的字串。
步驟5. 提交並提交更改。

相關資訊

AsyncOS 15.0使用手冊：系統管理

更改在ESA上與SSL/TLS一起使用的方法和密碼

思科錯誤ID CSCwh48138 - ESA 15.0 Exchange 2013使用TLS時電子郵件傳遞失敗

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）。