アップグレード後のSEG AsyncOS 15.0への古いExchange Server接続のトラブルシューティング

内容

[概要](#)
[使用するコンポーネント](#)
[問題](#)
[解決方法](#)
[CLIで次のコマンドを実行します。](#)
[GUIで次の操作を行います。](#)
[関連情報](#)

概要

このドキュメントでは、バージョン15.0へのアップグレード後にSecure Email Gateway(SEG)でExchange 2013（またはそれ以前の）接続の問題を修正する手順について説明します。

使用するコンポーネント

Exchange 2013またはそれ以前。

SEGバージョン15.0。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

問題

SEGをバージョン15.0にアップグレードした後、2013より前のExchangeサーバ間の接続が確立されません。CLIからtophostsをチェックすると、ドメインがダウン(*)としてマークされていることが確認できます

```
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
```

Mail_logsから、ネットワークエラーの原因によるドメインへの接続障害を確認できます。

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

パケットキャプチャでは、TLSネゴシエーションの直後に、ExchangeサーバがFINパケットとの接続を閉じることが確認できます。

解決方法

Exchangeサーバのバージョンが2013以前であることを確認します。この暗号文字列を回避策として使用し、SEGがそれらの古いサーバに接続できるようにします。これにより、exchangeを現在サポートされているバージョンにアップグレードするまで、メールを配信できます。

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

この情報は、コマンドラインインターフェイス(CLI)またはWebグラフィカルユーザインターフェイス(GUI)を使用して入力できます。
CLIで次のコマンドを実行します。

```
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
```

GUIで次の操作を行います。
ステップ 1：System Administrationタブでを選択します。
ステップ 2：SSL Configurationでを選択します。
ステップ 3：Edit Settingsボタンを選択します。
ステップ 4：この記事で提供されている文字列を使用するように、発信SMTP SSL暗号を変更します。
ステップ 5： 変更を送信し、保存します。

関連情報

AsyncOS 15.0ユーザガイド：システム管理

ESA の SSL/TLS で使用される方式と暗号の変更

Cisco Bug ID CSCwh48138 - Exchange 2013を使用したESA 15.0のTLS経由の電子メール配信の失敗

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。