업그레이드 후 SEG AsyncOS 15.0에 대한 이전 Exchange Server 연결 문제 해결

목차

소개

이 문서에서는 버전 15.0으로 업그레이드한 후 SEG(Secure Email Gateway)로 인한 Exchange 2013(또는 이전) 연결 문제를 해결하는 단계를 설명합니다.

사용되는 구성 요소

Exchange 2013 이상

SEG 버전 15.0.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

문제

SEG를 버전 15.0으로 업그레이드한 후에는 2013년 이전 버전의 Exchange 서버 간 연결이 설정되지 않습니다. CLI에서 tophosts를 선택하면 도메인이 down (*)으로 표시된 것을 볼 수 있습니다

```
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_logs에서 네트워크 오류의 이유로 도메인에 대한 연결 오류를 볼 수 있습니다.

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

패킷 캡처에서는 TLS 협상 직후에 Exchange 서버가 FIN 패킷과의 연결을 닫는 것을 볼 수 있습니다.

솔루션

Exchange 서버가 2013 이전 버전인지 확인한 다음 이 암호 문자열을 해결 방법으로 사용하여 SEG가 이전 서버에 연결하도록 허용할 수 있습니다. 이렇게 하면 exchange를 현재 지원되는 버전으로 업그레이드할 수 있을 때까지 메일을 배달할 수 있습니다.

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

CLI(Command Line Interface) 또는 웹 GUI(Graphical User Interface)를 통해 입력할 수 있습니다.
CLI에서:

```
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
```

GUI에서 다음을 수행합니다.
1단계. System Administration(시스템 관리) 탭에서 선택합니다.
2단계. SSL Configuration(SSL 컨피그레이션)을 선택합니다.
3단계. Edit Settings(설정 편집) 버튼을 선택합니다.
4단계. 이 문서에서 제공한 문자열을 사용하도록 아웃바운드 SMTP SSL 암호를 변경합니다.
5단계. 변경 사항을 제출하고 커밋합니다.

관련 정보

AsyncOS 15.0용 사용 설명서: 시스템 관리

ESA에서 SSL/TLS와 함께 사용되는 방법 및 암호 변경

Cisco 버그 ID CSCwh48138 - ESA 15.0 Email delivery failure over TLS with Exchange 2013

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.