Cisco Email Security의 CSN(Cisco Success Network)

목차

소개

이 문서에서는 Cisco ESA(Email Security Appliance)용 AsyncOS 13.5.1 릴리스의 일부로 제공되는 Cisco Success Network 기능에 대한 정보를 제공합니다. CSN(Cisco Success Network)은 사용자 지원 클라우드 서비스입니다.CSN이 활성화되면 ESA와 Cisco 클라우드(CTR 연결 사용) 간에 보안 연결을 설정하여 기능 상태 정보를 스트리밍합니다.스트리밍 CSN 데이터는 ESA에서 원하는 데이터를 선택하고 정형 형식으로 원격 관리 스테이션으로 전송하는 메커니즘을 제공합니다.

혜택

- 제품의 효율성을 높일 수 있는 사용 가능한 미사용 기능에 대해 고객에게 알립니다.
- 고객에게 제품에 대해 제공될 수 있는 추가 기술 지원 서비스 및 모니터링에 대한 정보를 제공합니다.
- Cisco가 제품을 개선할 수 있도록 지원합니다.

수집된 정보

다음은 ESA 디바이스에서 구성한 이 기능의 일부로 수집되는 기능 정보 목록입니다.

- 장치 모델(x90, x95, 000v,100v, 300v, 600v)
- 장치 일련 번호(UDI)
- UserAccountID(VLAN ID 번호 또는 SLPIID)
- 소프트웨어 버전
- 설치 날짜
- slVAN(Smart Licensing의 가상 어카운트 이름)
- 구축 모드

- IronPort 안티스팸
- 그레이메일 안전 수신 거부
- Sophos
- McAfee
- 파일 평판
- 파일 분석
- 데이터 유출 방지
- 외부 위협 피드
- Ironport 이미지 분석
- 신종 바이러스 필터
- Cisco IronPort 이메일 암호화 설정(봉투 암호화)
- PXE 암호화
- 도메인 평판
- URL 필터링
- 페이지 사용자 지정 차단
- 메시지 추적
- 정책, 바이러스 및 Outbreak 격리
- 스팸 쿼런틴

사전 요구 사항

요구 사항

이 기능을 구성하려면 다음 요구 사항을 충족해야 합니다.

- CTR(Cisco Threat Response) 어카운트

방화벽 관련 컨피그레이션

CSN 기능을 얻기 위해 필요한 방화벽 컨피그레이션은 현재 CTR 통신에 의존하며, 자세한 내용은 이 문서를 참조하십시오. ESA와 CTR 통합

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- ESA(Email Security Appliance) AsyncOS 버전 13.5.1.x 이상

구성

ESA UI 또는 CLI를 모두 사용하여 이 기능을 구성할 수 있습니다.두 단계에 대한 자세한 내용은 아래에 나와 있습니다.

CSN 및 CTR 종속성

CSN 기능은 성공적인 작동을 위해 CTR 기능 연결에 따라 달라지며 이 표에서는 이 두 프로세스 간의 관계에 대한 자세한 내용을 제공합니다.

위협 대응	CSN	SSE 커넥터	CSN 프로세스
사용 안 함	사용 안 함	아래로	사용 안 함
사용 안 함 (등록 취소)	사용	아래로	아래로
사용 안 함 (등록됨)	사용	위로	위로
사용	수동으로 사용 안 함	위로	아래로
사용	사용	위로	위로

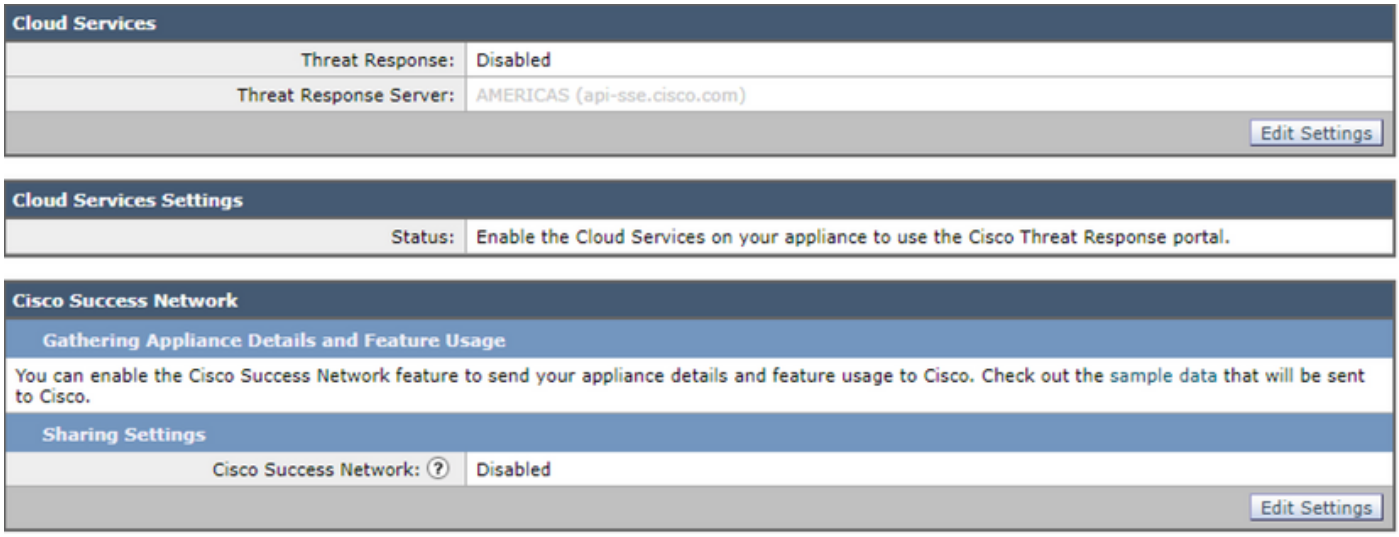
UI를 사용하는 CSN 구성

1) ESA UI에 로그인합니다.

2) Network(**네트워크) >> Cloud Service Settings(클라우드 서비스 설정**)로 이동합니다(13.5.1.x로 업그레이드를 시작하기 전에 CTR이 비활성화된 것으로 가정). 업그레이드 전에 CTR이 활성화된 경우 CSN도 기본적으로 활성화됩니다.CTR이 비활성화된 경우 CSN도 비활성화됩니다.

> **참고:**CTR은 SMA에서 보고 정보를 CTR로 전송하기 위해 활성화되었기 때문에 중앙 집중식 구축의 CTR은 업그레이드 전에 비활성화된 것으로 가정합니다.

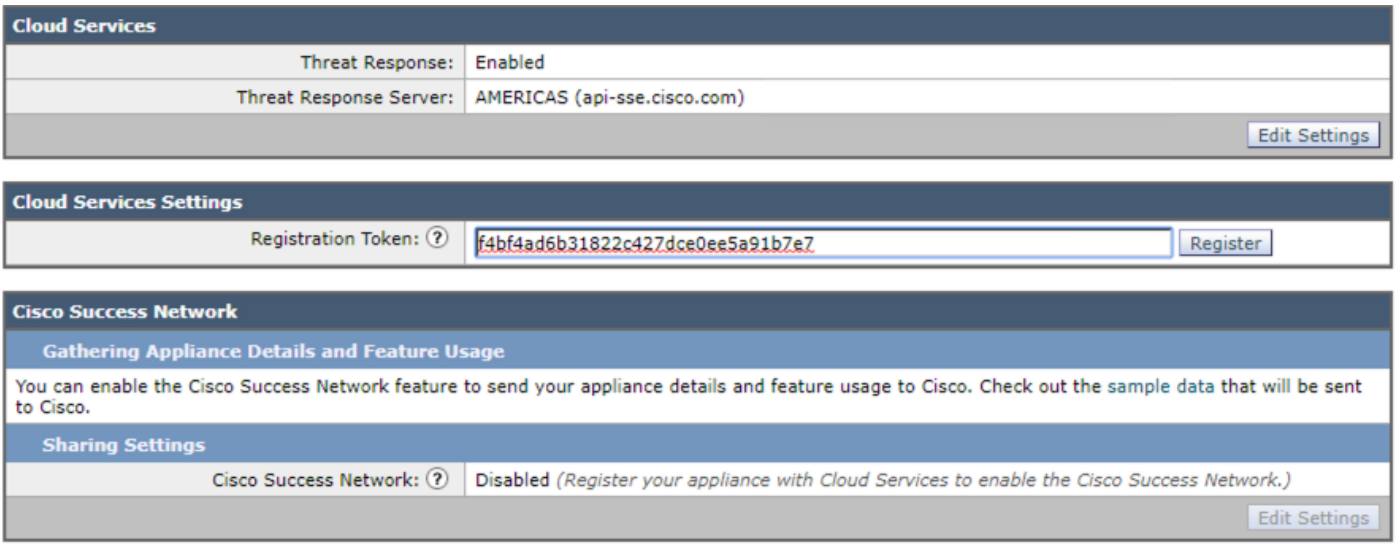
3) ESA 디바이스에서 기본값으로 관찰되는 내용은 다음과 같습니다.-



4) 이제 먼저 ESA에서 CTR 서비스를 활성화하고 변경 사항을 "제출"하여 이 ESA를 등록합니다.

5) CTR 페이지에 "The Cisco Cloud Service is busy(Cisco 클라우드 서비스가 사용 중입니다.) 이 상태가 표시됩니다.잠시 후 이 페이지로 이동하여 어플라이언스 상태를 확인합니다." 디바이스에 변경 사항을 커밋합니다.

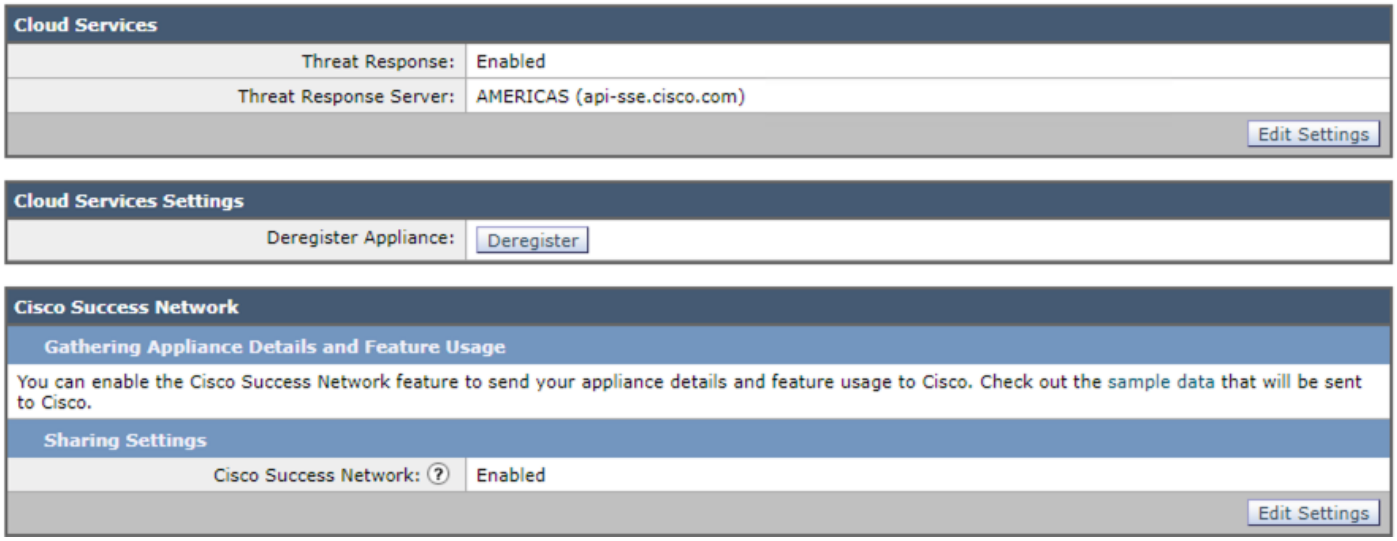
6) CTR 토큰을 가져와 CTR에 디바이스를 등록합니다.



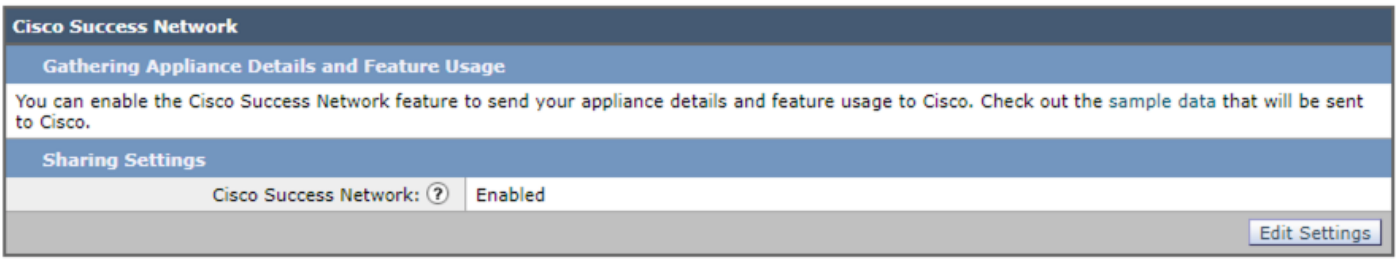
7) 등록이 완료되면 이 상태를 확인해야 합니다.

성공 — Cisco Threat Response 포털에 어플라이언스를 등록하라는 요청이 시작됩니다.잠시 후에 이 페이지로 이동하여 어플라이언스 상태를 확인합니다.

8) 페이지를 새로 고치면 CTR Registered 및 CSN Enabled(CTR 등록 및 CSN 활성화)가 표시됩니다.



9) 앞서 설명한 대로 이 ESA가 중앙 집중화되어 있으므로 이 시나리오에서 CTR을 비활성화해야 하며 CSN이 예상대로 활성화된 것으로 표시됩니다.이 ESA는 SMA(Non-Centralized)에서 관리하지 않는 경우 CTR을 계속 활성화할 수 있습니다.



이는 컨피그레이션의 최종 상태여야 합니다.**이 설정이 Machine Level이므로 모든 ESA에 대해 이 단계를 수행해야 합니다.**

CLI를 사용하는 CSN 컨피그레이션

```
(Machine esa )> csnconfig

You can enable the Cisco Success Network feature to send your appliance details and feature
usage to Cisco.

Choose the operation you want to perform:
- ENABLE - To enable the Cisco Success Network feature on your appliance.
[]> enable

The Cisco Success Network feature is currently enabled on your appliance.
```

CLI를 사용하여 이를 활성화하는 과정에서 변경 사항을 커밋해야 합니다.

문제 해결

이 기능을 트러블슈팅하려면 이 기능에 대한 정보를 가지고 있는 PUB(**/data/pub/csn_logs**) 로그를 사용할 수 있습니다.아래 샘플은 디바이스에서 등록이 완료된 당시의 로그입니다.

```
(Machine ESA) (SERVICE)> tail

Currently configured logs:
    Log Name            Log Type                                Retrieval           Interval
 ---------------------------------------------------------------------------------------
 1. API                 API Logs                                Manual Download     None
 2. amp                 AMP Engine Logs                         Manual Download     None
 3. amparchive          AMP Archive                             Manual Download     None
 4. antispam            Anti-Spam Logs                          Manual Download     None
 5. antivirus           Anti-Virus Logs                         Manual Download     None
 6. asarchive           Anti-Spam Archive                       Manual Download     None
 7. authentication      Authentication Logs                     Manual Download     None
 8. avarchive           Anti-Virus Archive                      Manual Download     None
 9. bounces             Bounce Logs                             Manual Download     None
10. cli_logs            CLI Audit Logs                          Manual Download     None
11. csn_logs            CSN Logs                                Manual Download     None
```

```
12. ctr_logs            CTR Logs                            Manual Download     None
13. dlp                 DLP Logs                            Manual Download     None
14. eaas                Advanced Phishing Protection Logs   Manual Download     None
15. encryption          Encryption Logs                     Manual Download     None
16. error_logs          IronPort Text Mail Logs             Manual Download     None
17. euq_logs            Spam Quarantine Logs                Manual Download     None
18. euqgui_logs         Spam Quarantine GUI Logs            Manual Download     None
19. ftpd_logs           FTP Server Logs                     Manual Download     None
20. gmarchive           Graymail Archive                    Manual Download     None
21. graymail            Graymail Engine Logs                Manual Download     None
22. gui_logs            HTTP Logs                           Manual Download     None
23. ipr_client          IP Reputation Logs                  Manual Download     None
24. mail_logs           IronPort Text Mail Logs             Manual Download     None
25. remediation         Remediation Logs                    Manual Download     None
26. reportd_logs        Reporting Logs                      Manual Download     None
27. reportqueryd_logs   Reporting Query Logs                Manual Download     None
28. s3_client           S3 Client Logs                      Manual Download     None
29. scanning            Scanning Logs                       Manual Download     None
30. sdr_client          Sender Domain Reputation Logs       Manual Download     None
31. service_logs        Service Logs                        Manual Download     None
32. smartlicense        Smartlicense Logs                   Manual Download     None
33. sntpd_logs          NTP logs                            Manual Download     None
34. status              Status Logs                         Manual Download     None
35. system_logs         System Logs                         Manual Download     None
36. threatfeeds         Threat Feeds Logs                   Manual Download     None
37. trackerd_logs       Tracking Logs                       Manual Download     None
38. unified-2           Consolidated Event Logs             Manual Download     None
39. updater_logs        Updater Logs                        Manual Download     None
40. upgrade_logs        Upgrade Logs                        Manual Download     None
41. url_rep_client      URL Reputation Logs                 Manual Download     None
Enter the number of the log you wish to tail.
[]> 11

Press Ctrl-C to stop.
Sun Apr 26 18:16:13 2020 Info: Begin Logfile
Sun Apr 26 18:16:13 2020 Info: Version: 13.5.1-177 SN: 564D2E7007BA223114B8-786BB6AB7179
Sun Apr 26 18:16:13 2020 Info: Time offset from UTC: -18000 seconds
Sun Apr 26 18:16:13 2020 Info: System is coming up.
Sun Apr 26 18:16:13 2020 Info: DAEMON: Watchdog thread started
Sun Apr 26 18:16:16 2020 Info: The appliance is uploading CSN data
Sun Apr 26 18:16:16 2020 Info: The appliance has successfully uploaded CSN data
```