思科郵件安全上的思科成功網路(CSN)

目錄

簡介

本檔案提供有關思科成功網路功能的資訊，該功能可作為思科電子郵件安全裝置(ESA)的AsyncOS 13.5.1版本的一部分。 Cisco Success Network(CSN)是一種使用者支援的雲服務。啟用CSN後，在ESA和思科雲之間建立安全連線（使用CTR連線），以流傳輸功能狀態資訊。流式CSN資料提供了一種機制，從ESA中選擇感興趣的資料，並以結構化格式將其傳送到遠端管理站。

優勢

- 通知客戶有關可提高產品有效性的可用未使用功能。
- 通知客戶產品可能提供的其他技術支援服務和監控。
- 以幫助思科改進產品。

收集的資訊

以下是在ESA裝置上配置後，作為此功能的一部分收集的功能資訊清單：

- 裝置型號(x90、x95、000v、100v、300v、600v)
- 裝置序列號(UDI)
- 使用者帳戶ID（VLN ID號或SLPIID）
- 軟體版本
- 安裝日期
- slVAN（智慧許可中的虛擬帳戶名稱）
- 部署模式
- IronPort反垃圾郵件
- 灰色郵件安全取消訂閱
- 索福斯
- McAfee

- 檔案信譽
- 檔案分析
- 防止資料丟失
- 外部威脅源
- Ironport影像分析
- 爆發過濾器
- Cisco IronPort電子郵件加密設定（信封加密）
- PXE加密
- 域信譽
- URL篩選
- 阻止頁面自定義
- 郵件跟蹤
- 策略、病毒和爆發隔離區
- 垃圾郵件隔離區

必要條件

需求

要配置此功能，必須滿足以下一些要求：

- CTR（思科威脅響應）帳戶

防火牆相關設定

CSN正常工作所需的防火牆配置當前取決於CTR通訊，有關詳細資訊，請參閱本文檔：將ESA與CTR整合

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Email Security Appliance(ESA)AsyncOS版本13.5.1.x及更高版本。

設定

可以使用ESA UI或CLI配置此功能。兩個步驟的詳細資訊如下所示。

CSN和CTR相關性

CSN功能取決於成功操作的CTR功能連線，下表提供了有關這兩個進程之間關係的詳細資訊。

威脅響應	CSN	SSE聯結器	CSN流程
已禁用	已禁用	關閉	已禁用
已禁用（取消註冊）	已啟用	關閉	關閉
已禁用（已	已啟用	UP	UP

註冊）
已啟用　　手動禁用　UP　　關閉
已啟用　　已啟用　　UP　　UP

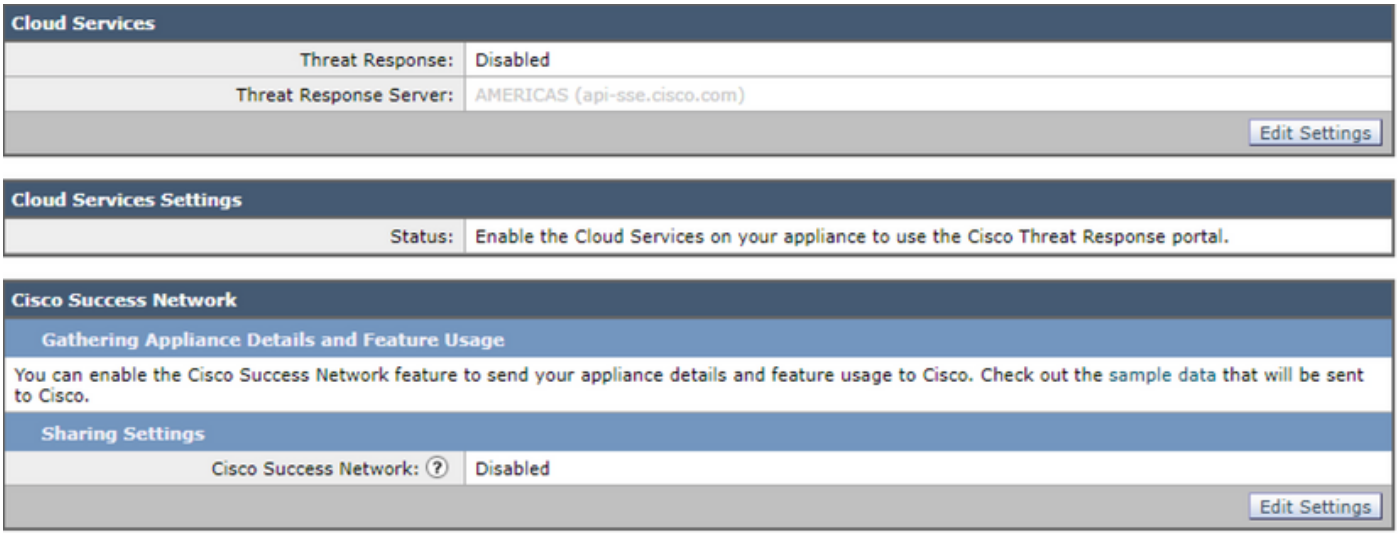
使用UI配置CSN

1)登入ESA UI。

2)瀏覽到**Network >> Cloud Service Settings**（在升級到13.5.1.x之前，我假定已禁用CTR）。 升級之前，如果啟用CTR，則預設情況下也會啟用CSN。如果禁用CTR，則CSN也將禁用。

> **附註**：我們假定在升級之前已禁用CTR，因為集中部署中的CTR應該被禁用，因為它僅在SMA上啟用，用於向CTR傳送報告資訊。

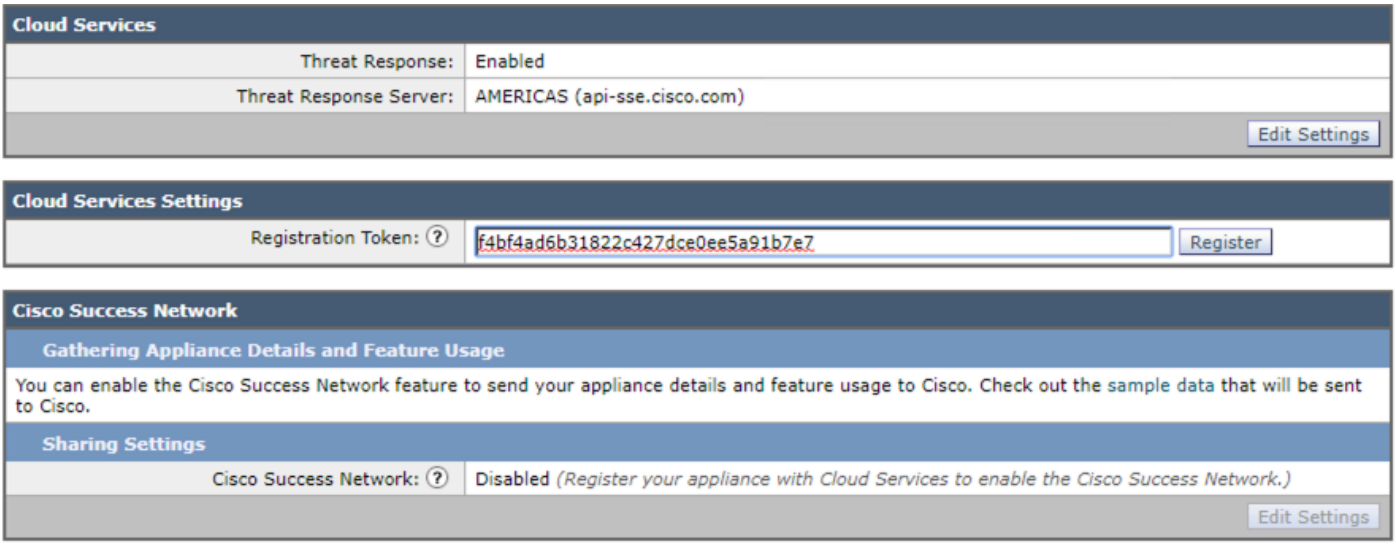
3)這是您在ESA裝置上看到的預設配置：-



4)現在，我們將通過在ESA上啟用CTR服務並「提交」更改來註冊此ESA。

5)在CTR頁面「The Cisco Cloud Service is busy」上顯示此狀態。過一段時間後導航回此頁面，檢查裝置狀態。」 將更改提交到裝置。

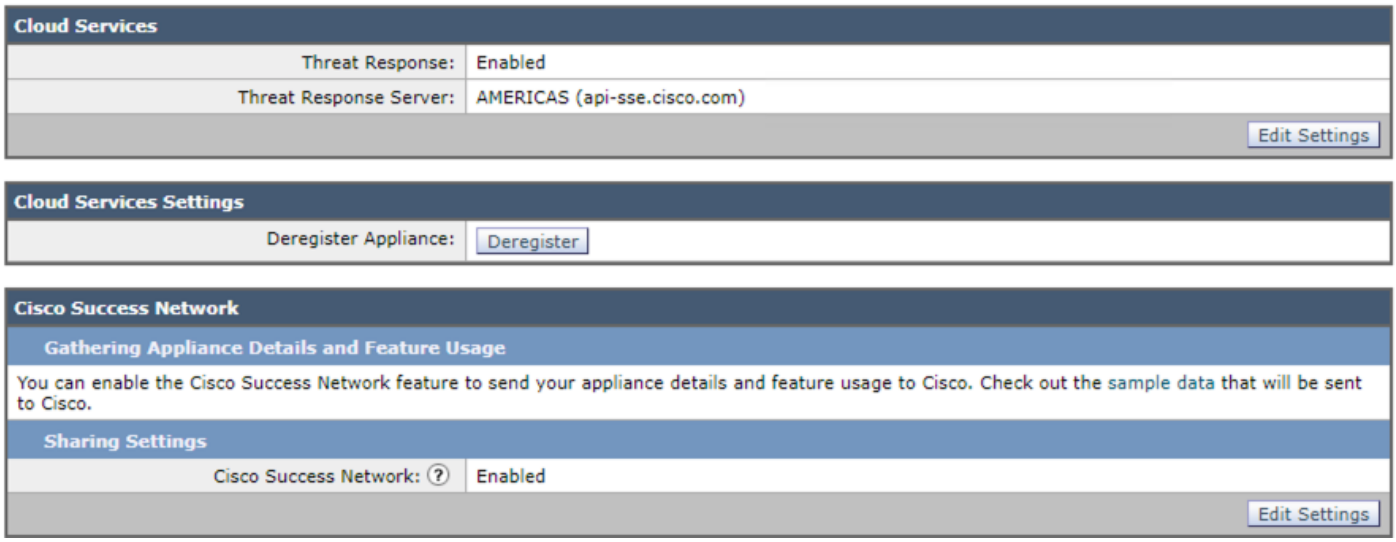
6)然後繼續操作，獲取CTR令牌並將裝置註冊到CTR:



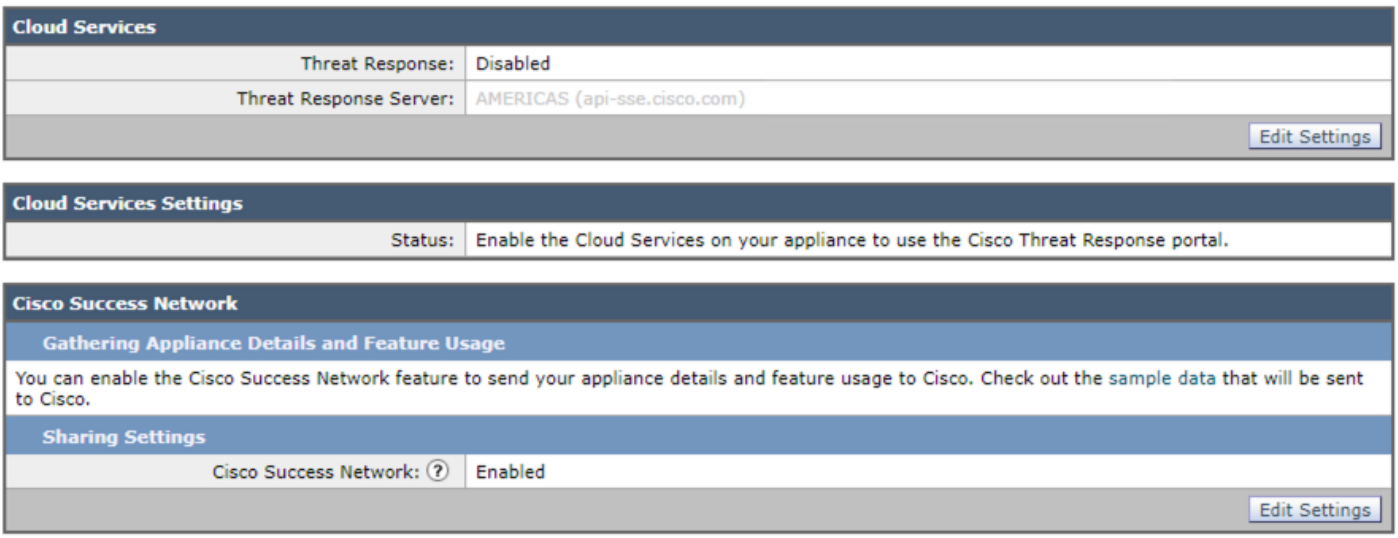
7)註冊成功後應看到此狀態：

成功 — 啟動向思科威脅響應門戶註冊裝置的請求。一段時間後導航回此頁面以檢查裝置狀態。

8)刷新頁面後，您會看到CTR已註冊和CSN已啟用：



9)如前所述，此場景中的CTR需要禁用，因為此ESA是集中式的，並且您仍會看到按預期啟用了CSN。如果此ESA不是由SMA（非集中式）管理，您可以保持啟用CTR。



這應該是組態的最終狀態。**每個ESA都應該執行此步驟，因為該設定為「電腦級別」。**

使用CLI配置CSN

```
(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.
```

使用CLI啟用時，需要提交更改。

疑難排解

要對此功能進行故障排除，有一個PUB(/data/pub/csn_logs)日誌可用，該日誌包含有關此功能的資訊。以下示例是在裝置上完成註冊時的日誌：

```
(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
```