Red del éxito de Cisco (CSN) en la Seguridad del correo electrónico de Cisco

Contenido

Introducción

Este documento proporcionó a la información en la función de red del éxito de Cisco que estaría disponible como parte de la versión de AsyncOS 13.5.1 para el dispositivo de seguridad del correo electrónico de Cisco (ESA). La red del éxito de Cisco (CSN) es un servicio usuario-habilitado de la nube. Cuando se habilita CSN, una conexión segura se establece entre el ESA y la nube de Cisco (usando CTR la conexión), para fluir la información de estatus de la característica. Fluir los datos CSN proporciona un mecanismo para seleccionar los datos del interés del ESA y para transmitirlos en un formato estructurado a las estaciones de la administración remota.

Beneficios

- Para informar al cliente con respecto a las características inusitadas disponibles que pueden mejorar la eficacia del producto.
- Para informar al cliente con respecto los Servicios de soporte técnico y a la supervisión adicionales que pudieron estar disponibles para el producto.
- Para ayudar a Cisco para mejorar el producto.

Información recopilada

Éstas son la lista de información de la característica que se recoja como parte de esta característica configurada una vez en el dispositivo ESA:

- Modelo del dispositivo (x90, x95, 000v,100v, 300v, 600v)
- Número de serie del dispositivo (UDI)

- UserAccountID (número de ID VLN o SLPIID)
- Versión de software
- Instale la fecha
- slVAN (nombre de la cuenta virtual en la autorización de Smart)
- Modo del despliegue
- Anti-Spam de IronPort
- La caja fuerte de Graymail desinscribe
- Sophos
- McAfee
- Reputación del archivo
- Análisis del archivo
- Data Loss Prevention
- Alimentaciones de la amenaza exterior
- Análisis de imagen de Ironport
- Filtros del brote
- Configuraciones de encripción del correo electrónico de Cisco IronPort (cifrado del sobre)
- Cifrado PXE
- Reputación del dominio
- Filtrado de URL
- Arreglo para requisitos particulares de la página del bloque
- Seguimiento de mensajes
- Cuarentenas de la directiva, del virus y del brote
- Cuarentena del Spam

Prerrequisitos

Requisitos

Para configurar esta característica, éstos son algunos de los requisitos que deben ser satisfechos:

- CTR cuenta (de la Respuesta de Cisco ante amenazas)

Configuración relacionada del Firewall

La configuración de escudo de protección necesaria para conseguir CSN funcional es actualmente dependiente en CTR la comunicación y para referir por favor a este documento para más información: ESA de integración con CTR

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Versión 13.5.1.x y posterior de AsyncOS del dispositivo de seguridad del correo electrónico (ESA).

Configurar

Usted puede configurar esta característica usando el ESA UI o el CLI. Los detalles en ambos los pasos se muestran abajo.

CSN y CTR dependencias

La característica CSN depende CTR de la Conectividad de la característica para su funcionamiento exitoso y esta tabla proporciona más información sobre la relación entre estos dos procesos.

Respuesta de la amenaza	CSN	Conector de SSE	Proceso CSN
Discapacitado	Discapacitado	Abajo	Discapacitado
Discapacitado (cancele)	Habilitado	Abajo	Abajo
Discapacitado (registrado)	Habilitado	Encima de	Encima de
Habilitado	Inhabilitado manualmente	Encima de	Abajo
Habilitado	Habilitado	Encima de	Encima de

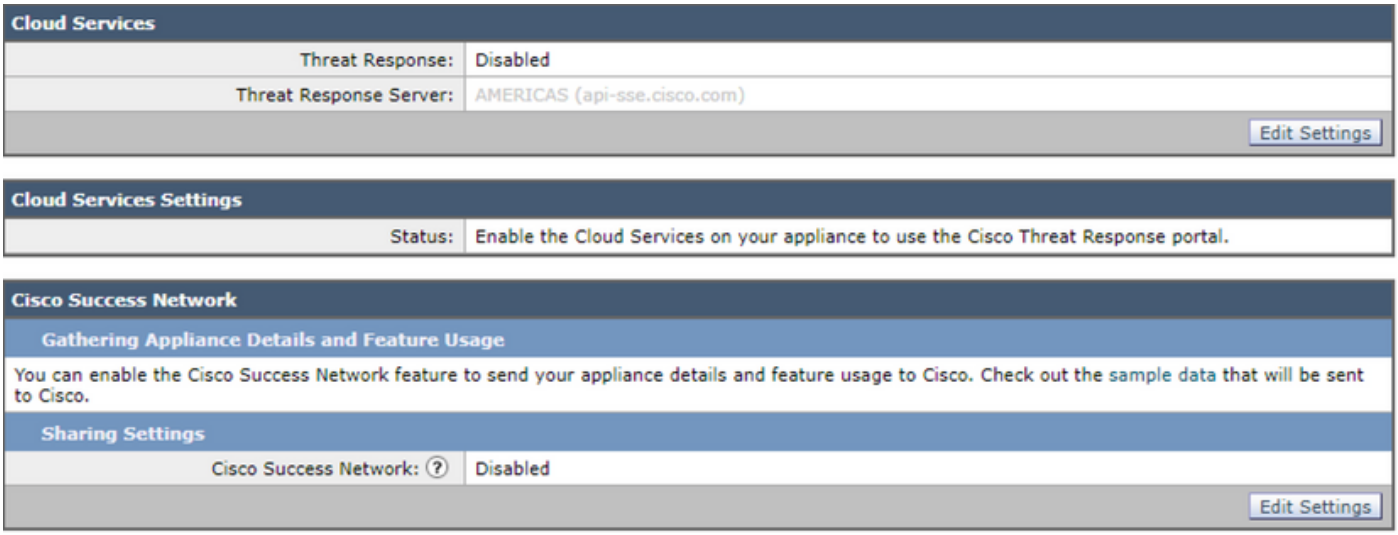
Configuración CSN usando el UI

1) Inicie sesión en el ESA UI.

2) Hojee a las **configuraciones del servicio de la red >>** de la **nube** (asumiré que CTR fue inhabilitado antes de que comenzáramos con la actualización a 13.5.1.x). Antes de que la actualización, si CTR fue habilitado, después CSN también sea habilitada por abandono. Si CTR fue inhabilitado, después CSN también será inhabilitado.

> Nota: Asumiremos CTR fuimos inhabilitados antes de que la actualización tan CTR en un despliegue centralizado se suponga ser inhabilitada como se habilita solamente en el S A para enviar la información de la información a CTR.

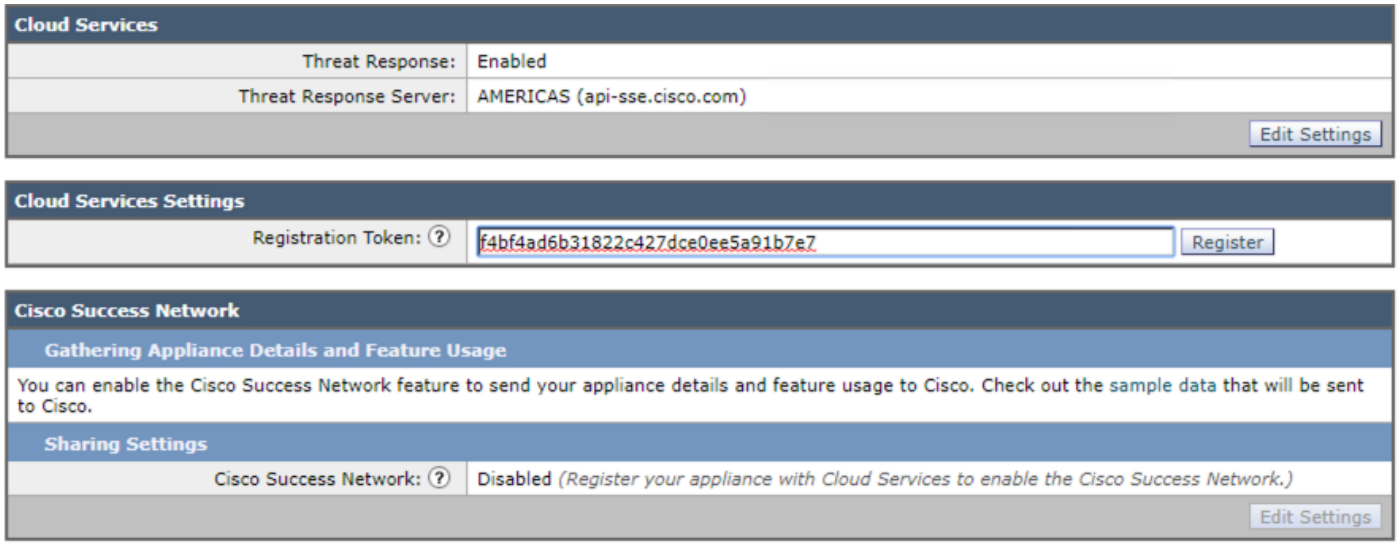
3) Esto es lo que usted observaría como valor por defecto en el dispositivo ESA: -



4) Ahora registraremos este ESA primero habilitando CTR los servicios en el ESA y "someta" los cambios.

5) mostraría que este estatus en CTR la página "el servicio de la nube de Cisco está ocupado. Navegue de nuevo a esta página después de un cierto tiempo para marcar el estatus del dispositivo." Confíe los cambios al dispositivo.

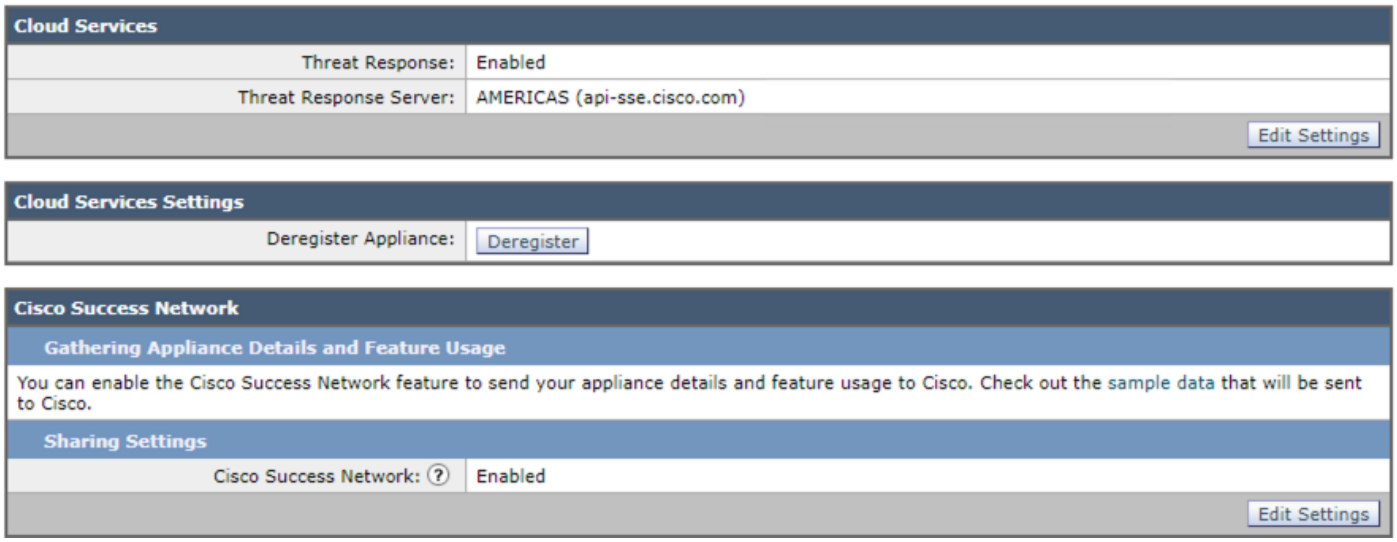
6) Usted entonces se movería a continuación y conseguiría CTR el token y registraría el dispositivo a CTR:



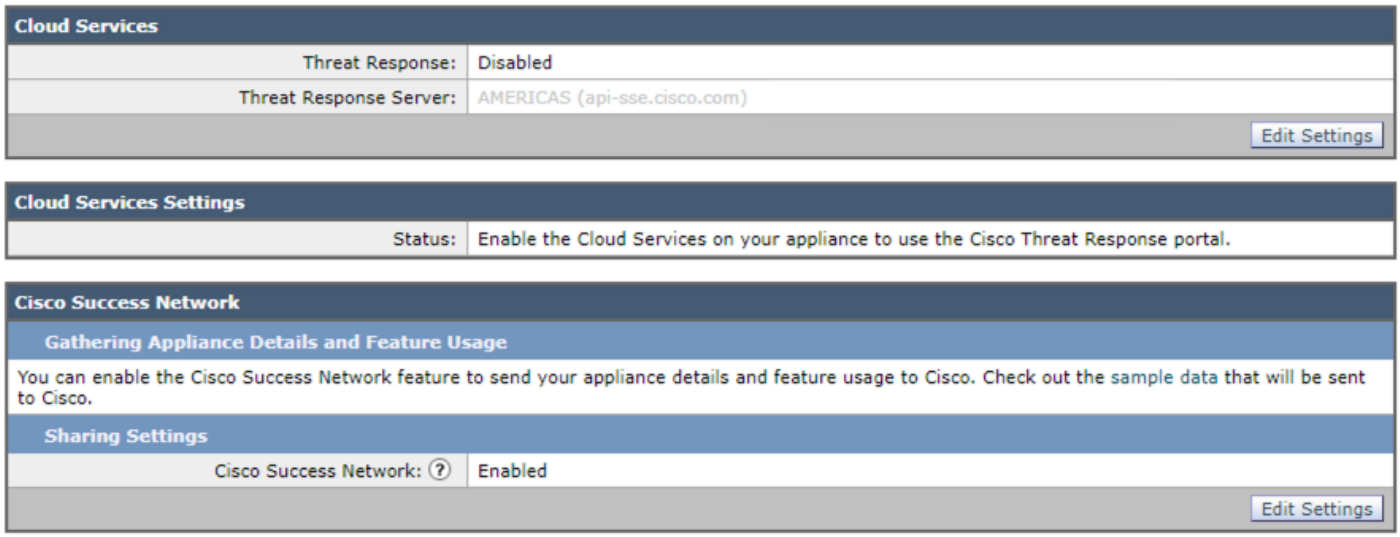
7) Usted debe ver este estatus una vez que el registro es acertado:

Éxito — Se inicia una petición de registrar su dispositivo con el portal de la Respuesta de Cisco ante amenazas. Navegue de nuevo a esta página después de un cierto tiempo para marcar el estatus del dispositivo.

8) Una vez que usted restaura la página, usted vería CTR haber registrado y el CSN habilitados:



9) Según lo discutido, CTR en este escenario necesita ser inhabilitado como este ESA se centraliza y usted todavía vería CSN habilitado como se esperaba. En caso de que, este ESA no sea manejado por el S A (NON-centralizado), usted puede guardar el CTR habilitado.



Éste debe ser el Estado final de la configuración. **Este paso se debe seguir para cada ESA pues esta configuración es nivel de equipo.**

Configuración CSN usando el CLI

```
(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.
```

Los cambios necesitarían ser confiados como parte de habilitar esto usando el CLI.

Troubleshooting

Para resolver problemas esta característica, hay un registro publicación (**/data/pub/csn_logs**) disponible que tendría la información sobre esta característica. La muestra abajo es el registro cuando el registro fue completado en el dispositivo:

```
(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
```