Rede do sucesso de Cisco (CSN) na Segurança do email de Cisco

Índice

Introdução

Este documento forneceu a informação nos recursos de rede do sucesso de Cisco que estariam disponíveis como parte da liberação de AsyncOS 13.5.1 para a ferramenta de segurança do email de Cisco (ESA). A rede do sucesso de Cisco (CSN) é um serviço USER-permitido da nuvem. Quando CSN é permitido, uma conexão segura está estabelecida entre o ESA e a nuvem de Cisco (que usam a conexão CTR), para fluir a informação de status da característica. Fluir dados CSN fornece um mecanismo para selecionar dados do interesse do ESA e para transmiti-los em um formato estruturado às estações de gerenciamento remotas.

Benefícios

- Para informar o cliente em relação às características não utilizadas disponíveis que podem melhorar a eficácia do produto.
- Para informar o cliente em relação aos Serviços de suporte técnico e à monitoração adicionais que puderam estar disponíveis para o produto.
- Para ajudar Cisco a melhorar o produto.

Informações recolhidas

Estas são a lista de informação da característica que é recolhida como parte desta característica configurada uma vez no dispositivo ESA:

- Modelo do dispositivo (x90, x95, 000v,100v, 300v, 600v)
- Número de série do dispositivo (UDI)
- UserAccountID (número de ID VLN ou SLPIID)

- Versão de software
- Instale a data
- slVAN (nome da conta virtual em licenciar de Smart)
- Modo do desenvolvimento
- Anti-Spam de IronPort
- Cancelar assinatura do cofre forte de Graymail
- Sophos
- McAfee
- Reputação do arquivo
- Análise do arquivo
- Prevenção de perda de dados
- Alimentações da ameaça externo
- Análise de imagem de Ironport
- Filtros da manifestação
- Configurações de criptografia do email de Cisco IronPort (criptografia do envelope)
- Criptografia PXE
- Reputação do domínio
- Filtragem URL
- Personalização da página do bloco
- Rastreamento de mensagem
- Quarentena da política, do vírus e da manifestação
- Quarentena do Spam

Pré-requisitos

Requisitos

Para configurar esta característica, estes são algumas das exigências que devem ser cumpridas:

- Conta CTR (Cisco Threat Response)

Configuração relacionada do Firewall

A configuração de firewall necessária obter CSN funcional é atualmente dependente da comunicação CTR e referir por favor este documento para mais informação: ESA de integração com CTR

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Versão 13.5.1.x e mais recente de AsyncOS da ferramenta de segurança do email (ESA).

Configurar

Você pode configurar esta característica usando o ESA UI ou o CLI. Os detalhes em ambas as etapas são mostrados abaixo.

Dependências CSN e CTR

A característica CSN depende da Conectividade da característica CTR para sua operação bem-sucedida e esta tabela fornece mais informação no relacionamento entre estes dois processos.

Resposta da ameaça	CSN	Conector SSE	Processo CSN
Deficiente	Deficiente	Para baixo	Deficiente
Deficiente (cancele a matrícula)	Permitido	Para baixo	Para baixo
Deficiente (registrado)	Permitido	Acima de	Acima de
Permitido	Desabilitado manualmente	Acima de	Para baixo
Permitido	Permitido	Acima de	Acima de

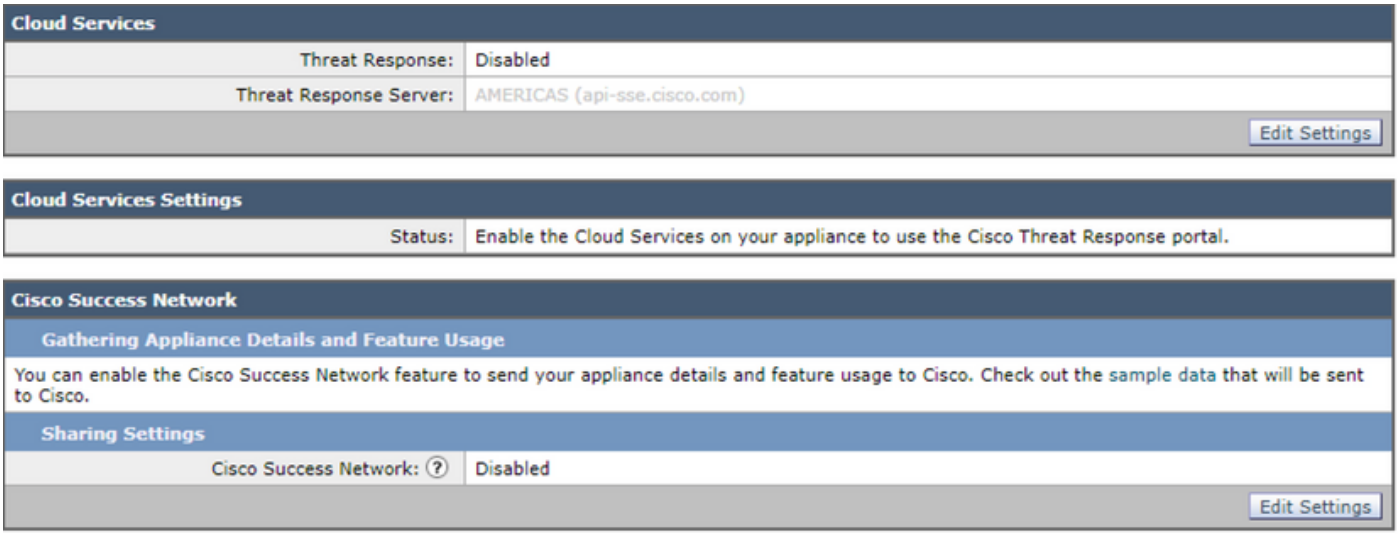
Configuração CSN usando o UI

1) Entre no ESA UI.

2) Consulte aos **ajustes do serviço da rede >>** da **nuvem** (eu suporei que o CTR esteve desabilitado antes que nós começamos com a elevação a 13.5.1.x). Antes que a elevação, se o CTR foi permitido, a seguir CSN estará permitida igualmente à revelia. Se o CTR foi desabilitado, a seguir CSN será desabilitado igualmente.

> Nota: Nós suporemos que o CTR esteve desabilitado antes que a elevação como o CTR em um desenvolvimento centralizado esteja suposta para ser desabilitada como ela for permitida somente no S A para mandar a informação do relatório ao CTR.

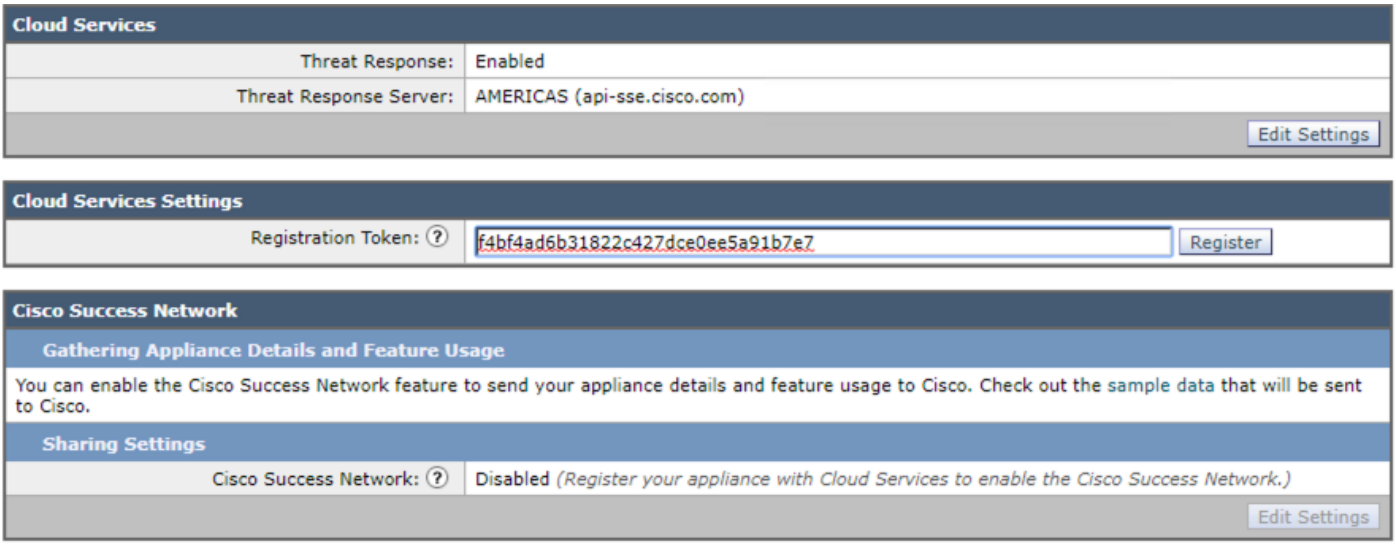
3) Este é o que você observaria como o padrão no dispositivo ESA: -



4) Nós registraremos agora este ESA primeiramente permitindo os serviços CTR no ESA e "submeta" as mudanças.

5) Mostraria que este estado na página CTR "que Cisco se nubla o serviço é ocupado. Navegue de volta a esta página após algum tempo para verificar o estado do dispositivo." Comprometa as mudanças ao dispositivo.

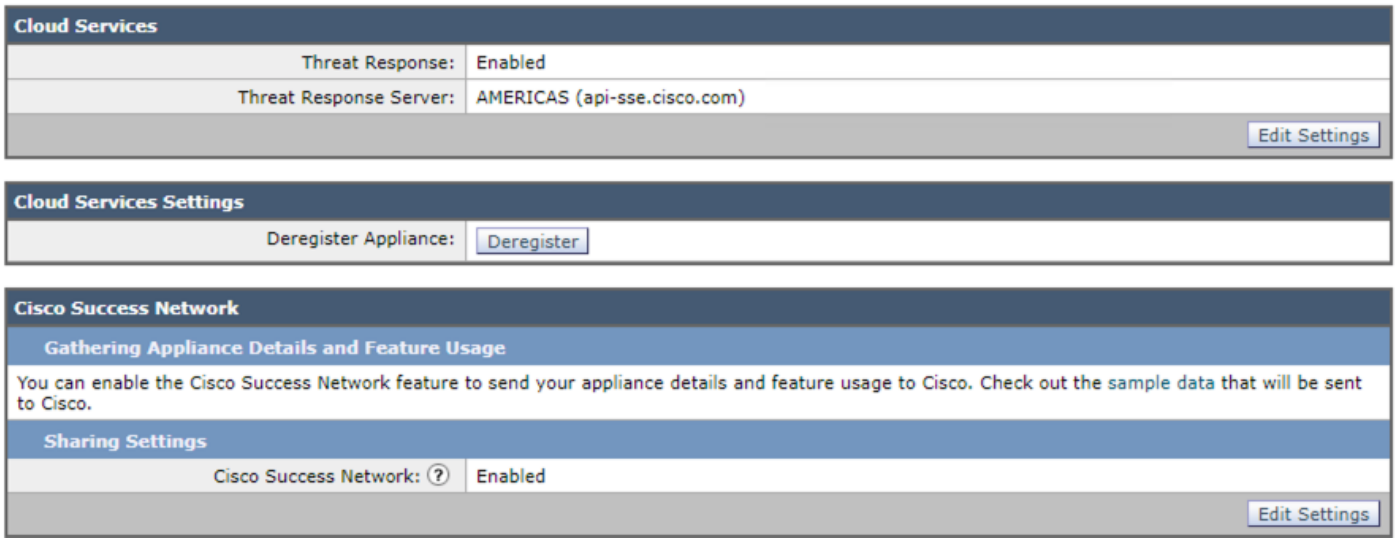
6) Você mover-se-ia então adiante e obter-se-ia o token CTR e registrar-se-&z o dispositivo ao CTR:



7) Você deve ver este estado uma vez que o registro é bem sucedido:

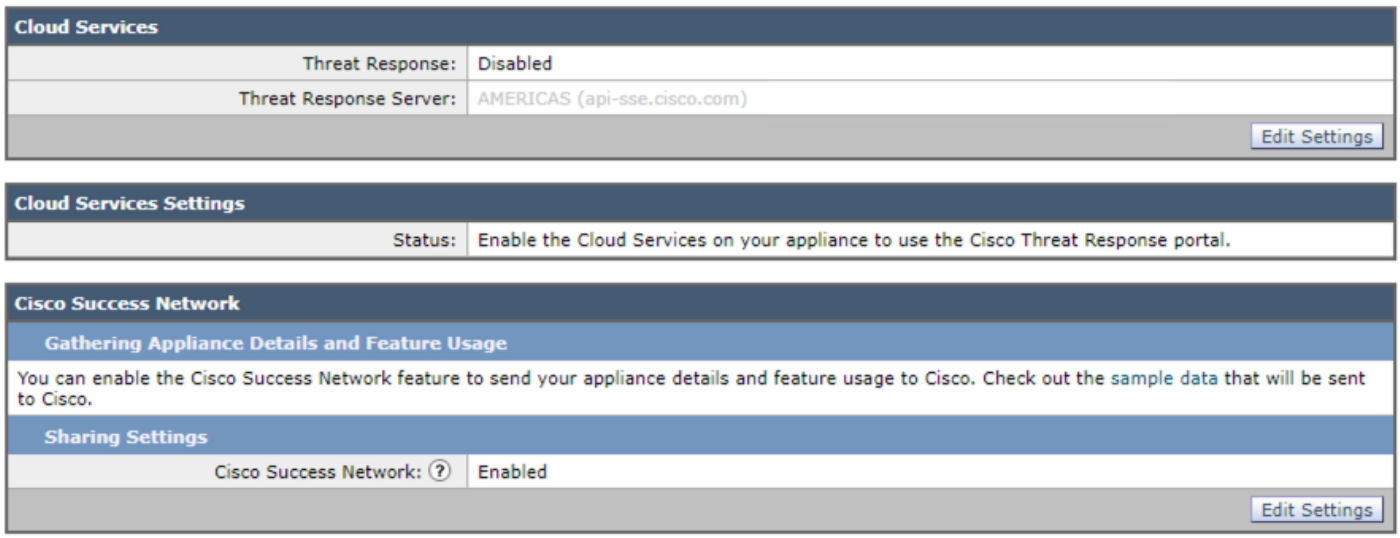
Sucesso — Um pedido registrar seu dispositivo com o portal do Cisco Threat Response é iniciado. Navegue de volta a esta página após algum tempo para verificar o estado do dispositivo.

8) Uma vez que você refresca a página, você veria o CTR registrado e CSN permitido:



9) Como discutido, o CTR nesta encenação precisa de ser desabilitado como este ESA é

centralizado e você ainda veria CSN permitido como esperado. Caso que, este ESA não está controlado pelo S A (NON-centralizado), você pode manter o CTR permitido.



Este deve ser o estado final da configuração. **Esta etapa deve ser seguida para cada ESA porque este ajuste é nível da máquina.**

Configuração CSN usando o 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.
```

As mudanças precisariam de ser comprometidas como parte de permitir isto que usa o CLI.

Troubleshooting

Para pesquisar defeitos esta característica, há um log do BAR (**/data/pub/csn_logs**) disponível que tenha a informação nesta característica. A amostra abaixo é o log no momento em que o registro foi terminado no 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
```