Solucione problemas "Falha na configuração da nuvem" em dispositivos Firepower

Contents

Introdução

Este documento descreve cenários comuns em que o sistema Firepower aciona o alerta de integridade: atualizações de dados de ameaças - configuração de nuvem da Cisco - falha.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Firepower Management Center
- Firepower Threat Defense
- Módulo de sensor Firepower
- Integração com a nuvem
- Resolução DNS e conectividade proxy
- Integração com Cisco Threat Response (CTR)

Componentes Utilizados

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

- Firepower Management Center (FMC) versão 6.4.0 ou posterior

- Firepower Threat Defense (FTD) ou Firepower Sensor Module (SFR) versão 6.4.0 ou posterior
- Cisco Secure Services Exchange (SSE)
- Portal Cisco Smart Account

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

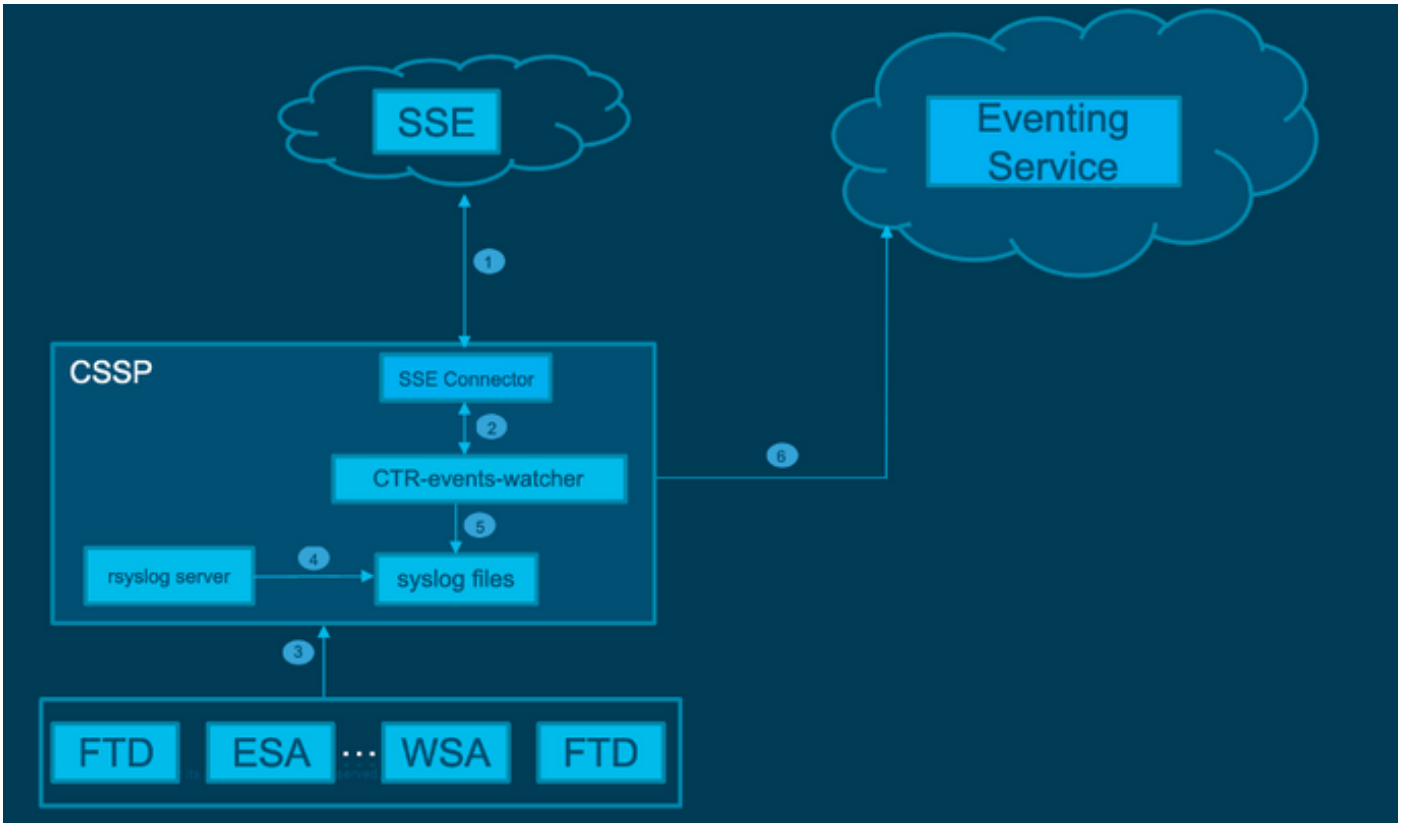
O erro Cloud Configuration é observado porque o FTD não consegue se comunicar com api-sse.cisco.com.

Este é o site que os dispositivos Firepower precisam alcançar para se integrarem aos serviços SecureX e de nuvem.

Este alerta faz parte do recurso Contenção rápida de ameaças (RTC). Esse recurso é habilitado por padrão nas novas versões do Firepower, nas quais o FTD precisa poder se comunicar com api-sse.cisco.com na Internet.

Se essa comunicação não estiver disponível, o módulo do monitor de integridade do FTD exibirá esta mensagem de erro: Atualizações de dados de ameaças - Configuração de nuvem da Cisco - Falha

Diagrama de Rede



Problema

O bug da Cisco ID CSCvr46845 explica que quando o Sistema Firepower aciona o Alerta de Integridade Configuração de Nuvem da Cisco - Falha, o problema está frequentemente relacionado à conectividade entre o FTD e api-sse.cisco.com.

No entanto, o alerta é muito genérico e pode apontar vários problemas, mesmo que ainda relacionados à conectividade, mas em um contexto diferente.

Existem dois cenários principais possíveis:

Cenário 1. No caso em que a integração de nuvem não está habilitada, esse alerta é esperado porque a conectividade com o portal de nuvem não é permitida.

Cenário 2. No caso em que a integração de nuvem está habilitada, é necessário realizar uma análise mais detalhada para eliminar as circunstâncias que envolvem uma falha de conectividade.

O Exemplo de Alerta de Falha de Integridade é mostrado na próxima imagem:

Exemplo de alerta de falha de integridade

Troubleshooting

Solução para o cenário 1. O erro de configuração de nuvem é observado porque o FTD não consegue se comunicar com https://api-sse.cisco.com/

Para desativar o alerta Cisco Cloud Configuration-Failure, navegue para System > Health > Policy > Edit policy > Threat Data Updates on Devices. Escolha Enabled (Off) (Habilitado), Save Policy (Salvar política) e Exit.

Aqui estão as diretrizes de referência para a configuração em linha.

Solução para o cenário 2. Quando a integração com a nuvem deve ser habilitada.

Comandos úteis para a solução de problemas:

<#root>

```
curl -v -k https://api-sse.cisco.com
```

```
 <-- To verify connection with the external site
```

```
nslookup api-sse.cisco.com
```

```
 <-- To dicard any DNS error

/ngfw/etc/sf/connector.properties

 <-- To verify is configure properly the FQDN settings

lsof -i | grep conn

 <-- To verify the outbound connection to the cloud on port 8989/tcp is ESTABLISHED
```

Opção 1. Configuração DNS ausente

Etapa 1. Verifique se os DNS estão configurados no FTD. Se não houver configurações de DNS, proceda da seguinte forma:

```
> show network
```

Etapa 2. Adicione o DNS com o comando:

```
> configure network dns servers dns_ip_addresses
```

Depois de configurar o DNS, o alerta de integridade é corrigido e o dispositivo é mostrado como íntegro. O é um breve intervalo de tempo antes que a alteração seja refletida, pois os servidores DNS apropriados estão configurados.

Opção 2. O DNS do cliente não pôde resolver https://api-sse.cisco.com

Teste com o comando curl. Se o dispositivo não puder alcançar o local da nuvem, há uma saída semelhante a este exemplo.

```
<#root>

FTD01:/home/ldap/abbac#

curl -v -k

https://api-sse.cisco.com
* Rebuilt URL to: https://api-sse.cisco.com/
* getaddrinfo(3) failed for api-sse.cisco.com:443
* Couldn't resolve host 'api-sse.cisco.com'
* Closing connection 0
curl: (6)

Couldn't resolve host 'api-sse.cisco.com'
```

Dica: comece com o mesmo método de solução de problemas da Opção 1. Verifique primeiro se a configuração DNS está definida corretamente. Você pode observar um problema de DNS depois que ele executa o comando curl.

Uma saída de curl correta deve ser a seguinte:

<#root>

```
root@fp:/home/admin# curl -v -k https://api-sse.cisco.com
* Rebuilt URL to: https://api-sse.cisco.com/
* Trying 10.6.187.110...
* Connected to api-sse.cisco.com (10.6.187.110) port 443 (#0)
* ALPN, offering http/1.1
* Cipher selection: ALL:!EXPORT:!EXPORT40:!EXPORT56:!aNULL:!LOW:!RC4:@STRENGTH
* successfully set certificate verify locations:
* CAfile: none
CApath: /etc/ssl/certs
* TLSv1.2 (OUT), TLS header, Certificate Status (22):
* TLSv1.2 (OUT), TLS handshake, Client hello (1):
* TLSv1.2 (IN), TLS handshake, Server hello (2):
* TLSv1.2 (IN), TLS handshake, Certificate (11):
* TLSv1.2 (IN), TLS handshake, Server key exchange (12):
* TLSv1.2 (IN), TLS handshake, Server finished (14):
* TLSv1.2 (OUT), TLS handshake, Client key exchange (16):
* TLSv1.2 (OUT), TLS change cipher, Client hello (1):
* TLSv1.2 (OUT), TLS handshake, Finished (20):
* TLSv1.2 (IN), TLS change cipher, Client hello (1):
* TLSv1.2 (IN), TLS handshake, Finished (20):
* SSL connection using TLSv1.2 / ECDHE-RSA-AES128-GCM-SHA256
* ALPN, server accepted to use http/1.1
* Server certificate:
* subject: C=US; ST=California; L=San Jose; O=Cisco Systems, Inc.; CN=api-sse.cisco.com
* start date: 2019-12-03 20:57:56 GMT
* expire date: 2021-12-03 21:07:00 GMT
* issuer: C=US; O=HydrantID (Avalanche Cloud Corporation); CN=HydrantID SSL ICA G2
* SSL certificate verify result: self signed certificate in certificate chain (19), continuing anyway.
> GET / HTTP/1.1
> Host: api-sse.cisco.com
> User-Agent: curl/7.44.0
> Accept: */*
>
< HTTP/1.1 403 Forbidden
< Date: Wed, 30 Dec 2020 21:41:15 GMT
< Content-Type: text/plain; charset=utf-8
< Content-Length: 9
< Connection: keep-alive
< Keep-Alive: timeout=5
< ETag: "5fb40950-9"
< Cache-Control: no-store
< Pragma: no-cache
< Content-Security-Policy: default-src https: ;
< X-Content-Type-Options: nosniff
< X-XSS-Protection: 1; mode=block
< X-Frame-Options: SAMEORIGIN
< Strict-Transport-Security: max-age=31536000; includeSubDomains
<

* Connection #0 to host api-sse.cisco.com left intact
```

```
Forbidden
```

Vá para o nome do host do servidor.

<#root>

```
#
```

curl -v -k

```
https://cloud-sa.amp.cisco.com
*   Trying 10.21.117.50...
* TCP_NODELAY set
* Connected to cloud-sa.amp.cisco.com (10.21.117.50) port 443 (#0)
* ALPN, offering http/1.1
* Cipher selection: ALL:!EXPORT:!EXPORT40:!EXPORT56:!aNULL:!LOW:!RC4:@STRENGTH
* successfully set certificate verify locations:
*   CAfile: /etc/ssl/certs/ca-certificates.crt
  CApath: none
* TLSv1.2 (OUT), TLS header, Certificate Status (22):
* TLSv1.2 (OUT), TLS handshake, Client hello (1):
```

Use as ferramentas básicas de conectividade, como os comandos nslookup, telnet e ping, para verificar, bem como a resolução DNS correta para o site Cisco Cloud.

Observação: o Firepower Cloud Services deve ter uma conexão de saída com a nuvem na porta 8989/tcp.

Aplique nslookup aos nomes de host do servidor.

```
# nslookup cloud-sa.amp.sourcefire.com
# nslookup cloud-sa.amp.cisco.com
# nslookup api.amp.sourcefire.com
# nslookup panacea.threatgrid.com
```

<#root>

```
root@fp:/home/admin#
```

nslookup api-sse.cisco.com

```
Server: 10.25.0.1
Address: 10.25.0.1#53

Non-authoritative answer:
api-sse.cisco.com canonical name = api-sse.cisco.com.akadns.net.
Name: api-sse.cisco.com.akadns.net
Address: 10.6.187.110
Name: api-sse.cisco.com.akadns.net
```

```
Address: 10.234.20.16
```

Os problemas de conexão com a AMP Cloud possivelmente se devem à resolução de DNS. Verifique as configurações de DNS ou faça nslookup no FMC.

```
nslookup api.amp.sourcefire.com
```

Telnet

<#root>

```
root@fp:/home/admin#
telnet api-sse.cisco.com 8989

root@fp:/home/admin#
telnet api-sse.cisco.com 443
root@fp:/home/admin#
telnet cloud-sa.amp.cisco.com 443
```

Ping

<#root>

```
root@fp:/home/admin#
ping api-sse.cisco.com
```

Mais Opções de Solução de Problemas

Verifique as propriedades do conector em /ngfw/etc/sf/connector.properties. Você deve ver essa saída com a porta de conector correta (8989) e o connector_fqdn com a URL correta.

<#root>

```
root@Firepower-module1:sf#
cat /ngfw/etc/sf/connector.properties

registration_interval=180
connector_port=8989
```

```
region_discovery_endpoint=https://api-sse.cisco.com/providers/sse/api/v1/regions
connector_fqdn=api-sse.cisco.com
```

Para obter mais informações, consulte o Guia de configuração do Firepower.

Problemas conhecidos

ID de bug da Cisco CSCvs05084 FTD Cisco Falha de configuração de nuvem devido a proxy

ID de bug da Cisco CSCvp56922 Use a API do conector sse do contexto de atualização para atualizar o nome de host e a versão do dispositivo

Bug DOC do ID de bug Cisco CSCvu02123: URL de atualização acessível de dispositivos Firepower para SSE no guia de configuração do CTR

O bug da Cisco ID CSCvr46845 ENH: Health message Cisco Cloud Configuration - Failure precisa de melhoria

[Vídeo]Firepower - Registre o FMC no SSE

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.