Solucionar problemas da integração do FMC com o CTR

Contents

Introduction

Este documento descreve as etapas para solucionar problemas do processo do Conector do Security Services Exchange (SSE) quando ele se torna desabilitado nos dispositivos Firepower Management Center (FMC) ou Firepower Threat Defense (FTD) para integração com o Cisco Threat Response (CTR).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- FMC
- FTD
- integração de CTR

Componentes Utilizados

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

- FMC no software versão 6.4.0 ou superior
- FTD no software versão 6.4.0 ou superior
- Cisco Security Services Exchange
- Conta CTR

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

SSEConnector

O SSEConnector é um processo nos dispositivos Firepower após a 6.4.0 que registra os dispositivos no portal SSE. O FMC envia broadcasts para todos os FTDs gerenciados quando a configuração de nuvem da Cisco está definida como On (Ativado) ou Off (Desativado). Quando o Cisco Cloud é ativado, o serviço SSEConnector inicia a comunicação entre o portal SSE e os dispositivos Firepower. Cada FTD solicita ao FMC um token de registro que permite que os dispositivos sejam integrados ao portal SSE. Após essa integração, o contexto SSE é ativado nos dispositivos e o EventHandler é reconfigurado para enviar Eventos de intrusão para a nuvem da Cisco.

CTR

A Threat Response é um hub de orquestração de resposta a incidentes de ameaças, que oferece suporte e automatiza integrações em vários produtos de segurança da Cisco. A resposta a ameaças acelera as principais tarefas de segurança: detecção, investigação e remediação, e é a pedra angular da nossa arquitetura de segurança integrada.

O objetivo do Threat Response é ajudar as equipes de operações de rede e os respondedores a incidentes a entender as ameaças em sua rede por toda a inteligência de ameaças coletada e combinada da Cisco e de terceiros.

Mas, mais do que tudo, a resposta a ameaças foi projetada para reduzir a complexidade das ferramentas de segurança, ajudar a identificar ameaças e acelerar a resposta a incidentes.

A Threat Response é uma plataforma de integração (https://visibility.amp.cisco.com/). O sistema funciona por meio de "módulos", que são partes independentes de código que lidam com comunicações com diferentes sistemas integrados (por exemplo, Threat Grid ou AMP). Esses módulos lidam com todas as três funções que um sistema integrado pode fornecer (enriquecimento, contexto local e resposta).

Para que o CTR pode ser usado?

- Resposta a incidentes
- Exames complementares de diagnóstico
- Busca de ameaças
- Gerenciamento de incidentes

Quando você procura um observável, todos os módulos configurados perguntam aos sistemas pelos quais eles são responsáveis por procurar qualquer registro desses observáveis. Em seguida, eles pegam as respostas fornecidas e as transmitem de volta para a resposta a

ameaças, depois recebem os resultados coletados de todos os módulos (neste caso, o módulo Stealthwatch), organizam e organizam os dados e os exibem em um gráfico.

Para integrar o CTR a produtos diferentes, há mais dois portais "https://castle.amp.cisco.com/" (Castle) e "https://admin.sse.itd.cisco.com/app/devices" (Security Services Exchange)

Portal do Castelo

Aqui você pode gerenciar as contas de segurança da Cisco:

Uma conta do Cisco Security permite que você gerencie vários aplicativos no portfólio do Cisco Security. De acordo com seus direitos de licenciamento, isso pode incluir:

- AMP para endpoints
- Threat Grid
- Resposta a ameaças

Portal de troca de serviços de segurança

Este portal é uma extensão do portal CTR, onde você pode gerenciar os dispositivos que foram registrados no portal CTR, para que aqui você possa criar os tokens necessários para integrar os produtos.

O Security Services Exchange oferece gerenciamento de dispositivos, serviços e eventos quando você integra determinados produtos de segurança da Cisco com o Cisco Threat Response, incluindo estes produtos e recursos:

- Gerencie a lista de dispositivos de gerenciamento de segurança que se integram ao Cisco Threat Response.
- Colete dados de eventos de dispositivos integrados do Cisco Firepower, em preparação para encaminhá-los (automática ou manualmente) para o Cisco Threat Response.

Troubleshoot

Verificar se os serviços de nuvem estão ativados

No FMC, primeiro, verifique em **System > Licenses > Smart Licenses** se você não está no modo de avaliação.

Verifique agora, em **System > Integration** na guia **Smart Software Satellite**, se a opção selecionada é **Conectar diretamente ao Cisco Smart Software Manager**, já que esse recurso não é suportado em um ambiente com conexão aérea.

Navegue até **System > Integration** na guia **Cloud Services** e verifique se a opção **Cisco Cloud Event Configuration** está ativada.

Verificar a conectividade entre o FMC/FTD e o portal SSE

Esses próximos URLs precisam ser permitidos, pois os IPs podem mudar:

Região dos EUA

- api-sse.cisco.com
- est.sco.cisco.com (comum em todas as regiões)
- mx*.sse.itd.cisco.com (atualmente apenas mx01.sse.itd.cisco.com)
- dex.sse.itd.cisco.com (para o sucesso do cliente)
- eventing-ingest.sse.itd.cisco.com (para CTR e CDO)

Região da UE

- api.eu.sse.itd.cisco.com
- est.sco.cisco.com (comum em todas as regiões)
- mx*.eu.sse.itd.cisco.com (atualmente apenas mx01.eu.sse.itd.cisco.com)
- dex.eu.sse.itd.cisco.com (para o sucesso do cliente)
- eventing-ingest.eu.sse.itd.cisco.com (para CTR e CDO)

Região APJ

- api.apj.sse.itd.cisco.com
- est.sco.cisco.com (comum em todas as regiões)
- mx*.apj.sse.itd.cisco.com (atualmente apenas mx01.apj.sse.itd.cisco.com)
- dex.apj.sse.itd.cisco.com (para o sucesso do cliente)
- eventing-ingest.apj.sse.itd.cisco.com (para CTR e CDO)

O FMC e o FTD precisam de uma conexão com os URLs SSE em sua interface de gerenciamento, para testar a conexão, insira estes comandos na CLI do Firepower com acesso raiz:

```
curl -v https://api-sse.cisco.com/providers/sse/services/registration/api/v2/clients --cacert
/ngfw/etc/ssl/connectorCA.pem
curl -v https://est.sco.cisco.com --cacert /ngfw/etc/ssl/connectorCA.pem

curl -v https://eventing-ingest.sse.itd.cisco.com --cacert /ngfw/etc/ssl/connectorCA.pem
curl -v https://mx01.sse.itd.cisco.com --cacert /ngfw/etc/ssl/connectorCA.pem
```

Depois que cada comando é executado, você deve ver esta linha ao redor do fim da conexão: **Conexão #0 para o host "URL" deixado intacto**.

Se a conexão expirar ou você não receber essa linha na saída, verifique se as interfaces de gerenciamento têm acesso permitido a esses URLs e se não há nenhum dispositivo upstream que bloqueie ou modifique a conexão entre os dispositivos e esses URLs.

A verificação de certificado pode ser ignorada com este comando:

```
root@ftd01:~# curl -v -k https://api-sse.cisco.com
* Rebuilt URL to: https://api-sse.cisco.com/
* Trying 52.4.85.66...
* Connected to api-sse.cisco.com (52.4.85.66) 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, Request CERT (13):
* TLSv1.2 (IN), TLS handshake, Server finished (14):
* TLSv1.2 (OUT), TLS handshake, Certificate (11):
* 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 S SL ICA G2
* SSL certificate verify result: self signed certificate in certificate c hain (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, 08 Apr 2020 01:27:55 GMT
<Content-Type: text/plain; charset=utf-8
<Content-Length: 9
<Connection: keep-alive
<Keep-Alive: timeout=5
<ETag: "5e17b3f8-9"
<Cache-Control: no-store
<Pragma: no-cache
<Content-Security-Policy: default-src 'self'
<X-Content-Type-Options: nosniff
<X-XSS-Protection: 1; mode=block
<Strict-Transport-Security: max-age=31536000; includeSubdomains;
```

> **Note**: Você recebe a mensagem 403 proibido, pois os parâmetros enviados do teste não são o que o SSE espera, mas isso prova o suficiente para validar a conectividade.

Verificar o estado do SSEConnector

Você pode verificar as propriedades do conector como abaixo.

```
# more /ngfw/etc/sf/connector.properties
registration_interval=180
connector_port=8989
connector_fqdn=api-sse.cisco.com
```

Para verificar a conectividade entre o SSConnector e o EventHandler, você pode usar este comando, este é um exemplo de uma conexão incorreta:

```
root@firepower:/etc/sf# netstat -anlp | grep EventHandler_SSEConnector.sock
unix 2 [ ACC ] STREAM LISTENING 3022791165 11204/EventHandler
```

```
/ngfw/var/sf/run/EventHandler_SSEConnector.sock
```

No exemplo de uma conexão estabelecida, você pode ver que o status do fluxo está conectado:

```
root@firepower:/etc/sf# netstat -anlp | grep EventHandler_SSEConnector.sock
unix 2 [ ACC ] STREAM LISTENING 382276 7741/EventHandler
/ngfw/var/sf/run/EventHandler_SSEConnector.sock
unix 3 [ ] STREAM CONNECTED 378537 7741/EventHandler
/ngfw/var/sf/run/EventHandler_SSEConnector.soc
```

Verificar os dados enviados ao portal SSE e CTR

Para enviar eventos do dispositivo FTD para VER, uma conexão TCP precisa ser estabelecida com https://eventing-ingest.sse.itd.cisco.com Este é um exemplo de uma conexão não estabelecida entre o portal SSE e o FTD:

```
root@firepower:/ngfw/var/log/connector# lsof -i | grep conn
connector 60815 www 10u IPv4 3022789647 0t0 TCP localhost:8989 (LISTEN)
connector 60815 www 12u IPv4 110237499 0t0 TCP firepower.cisco.com:53426->ec2-100-25-93-
234.compute-1.amazonaws.com:https (SYN_SENT)
```

Nos registros connector.log:

```
time="2020-04-13T14:34:02.88472046-05:00" level=error msg="[firepower.cisco.com][events.go:90
events:connectWebSocket] dial tcp 18.205.49.246:443: getsockopt: connection timed out"
time="2020-04-13T14:38:18.244707779-05:00" level=error msg="[firepower.cisco.com][events.go:90
events:connectWebSocket] dial tcp 100.25.93.234:443: getsockopt: connection timed out"
time="2020-04-13T14:42:42.564695622-05:00" level=error msg="[firepower.cisco.com][events.go:90
events:connectWebSocket] dial tcp 18.205.49.246:443: getsockopt: connection timed out"
time="2020-04-13T14:47:48.484762429-05:00" level=error msg="[firepower.cisco.com][events.go:90
events:connectWebSocket] dial tcp 100.25.93.234:443: getsockopt: connection timed out"
time="2020-04-13T14:52:38.404700083-05:00" level=error msg="[firepower.cisco.com][events.go:90
events:connectWebSocket] dial tcp 100.25.93.234:443: getsockopt: connection timed out"
```

> **Note**: Observado que os endereços IP exibidos em 18.205.49.246 e 18.205.49.246 pertencem a https://eventing-ingest.sse.itd.cisco.com podem mudar, é por isso que a recomendação é permitir o tráfego para o portal SSE com base em URL em vez de endereços IP.

Se essa conexão não for estabelecida, os eventos não serão enviados ao portal SSE, este é um exemplo de uma conexão estabelecida entre o FTD e o portal SSE:

```
root@firepower:# lsof -i | grep conn
connector 13277   www   10u  IPv4 26077573      0t0  TCP localhost:8989 (LISTEN)
connector 13277   www   19u  IPv4 26077679      0t0  TCP 192.168.1.200:56495->ec2-35-172-147-
246.compute-1.amazonaws.com:https (ESTABLISHED)
```

Problemas comuns

Após a atualização para a versão 6.4, o conector SSE não se comunica com o portal SSE. Connector.log fornece erros semelhantes aos eventos:(*Service).Start] Não foi possível conectar ao ponto de extremidade ZeroMQ PUSH: não foi possível discar para \"ipc:///ngfw/var/sf/run/EventHandler_SSEConnector.sock\": dial unix /ngfw/var/sf/run/EventHandler_SSEConnector.sock: connect: nenhum arquivo ou diretório desse tipo\n"

Reinicie o SSEConnector Service:

1) desabilitado por ferramenta sudo SSEConnector

2) sudo pmtool enablebyid SSEConnector

3) Reinicie o dispositivo. Após o reinício, o dispositivo se comunica com a nuvem.

Locais importantes do arquivo de log

Logs de depuração - Mostra mensagens de conexão ou falha bem-sucedidas

```
/ngfw/var/log/connector/connector.log
```

Configurações

```
/ngfw/etc/sf/connector.properties
```

Configurações

```
curl localhost:8989/v1/contexts/default
```

Informações Relacionadas

- https://docs.castle.amp.cisco.com/CiscoSecurityAccountUserGuide.pdf
- Suporte Técnico e Documentação - Cisco Systems