Solucione problemas de falhas de atualização de feeds de inteligência de segurança no Firepower Management Center

Contents

Introduction

Este documento descreve como solucionar problemas com atualizações do Security Intelligence Feed.

Background

O Security Intelligence Feed é composto de várias listas atualizadas regularmente de endereços IP com reputação ruim, conforme determinado pelo Cisco Talos Security Intelligence and Research Group (Talos). É importante manter o feed de inteligência atualizado regularmente para que um Cisco Firepower System possa usar informações atualizadas para filtrar o tráfego de rede.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Firepower Management Center
- Feed de inteligência de segurança

Componentes Utilizados

As informações neste documento são baseadas em um Cisco Firepower Management Center que executa o software versão 5.2 ou posterior.

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.

Problema

Ocorre uma falha de atualização do Security Intelligence Feed. Você pode verificar a falha pela GUI da Web ou pela CLI (explicada mais adiante nas seções a seguir).

Verifique o problema na GUI da Web

Quando ocorre uma falha de atualização do Security Intelligence Feed, o Firepower Management Center exibe alertas de integridade.

Verifique o problema na CLI

Para determinar a causa raiz de uma falha de atualização com o Security Intelligence Feed, insira este comando na CLI do Firepower Management Center:

```
admin@Sourcefire3D:~$ cat /var/log/messages
```

Procure um destes avisos nas mensagens:

```
Sourcefire3D SF-IMS[2004]: [2011] CloudAgent:IPReputation [WARN] Cannot download
Sourcefire_Intelligence_Feed

Sourcefire3D SF-IMS[24085]: [24090] CloudAgent:IPReputation [WARN] Download
unsucessful: Failure when receiving data from the peer
```

Solução

Conclua estes passos para fazer o troubleshooting do problema:

1. Verifique se o comando **intelligence.sourcefire.com** o site está ativo. Navegue até https://intelligence.sourcefire.comem um navegador.

2. Acesse o CLI do Firepower Management Center pelo Secure Shell (SSH).

3. Ping intelligence.sourcefire.com no Firepower Management Center:

   ```
   admin@Sourcefire3D:~$ sudo ping intelligence.sourcefire.verifyyou receive an output similar
   to this:

   64 bytes from x (xxx.xxx.xx.x): icmp_req=1 ttl=244 time=4.05 ifyou do not receive a
   response similar to that shown, then you can have an outbound connectivity issue, or you do
   not have a route to intelligence.sourcefire.com.
   ```

4. Resolver o nome de host para intelligence.sourcefire.com:

```
admin@Firepower:~$ sudo nslookup intelligence.sourcefire.com
```

Verifique se você recebeu uma resposta semelhante a esta:

```
Server: 8.8.8.8
Address: 8.8.8.8#53

Name: intelligence.sourcefire.com
Address: xxx.xxx.xx.x
```

Observação: a saída mencionada acima usa o servidor do sistema de nome de domínio público (DNS) do Google como exemplo. A saída depende das configurações de DNS definidas em **System > Local > Configuration**, no **Network** seção. Se você não receber uma resposta semelhante à exibida, verifique se as configurações DNS estão corretas.**Cuidado**: o servidor usa um esquema de endereço IP de rodízio para balanceamento de carga, tolerância a falhas e tempo de atividade. Portanto, os endereços IP podem mudar e a Cisco recomenda que o firewall seja configurado com um **CNAME** em vez de um endereço IP.

5. Verificar a conectividade com intelligence.sourcefire.com com o uso do Telnet:

```
admin@Firepower:~$ sudo telnet intelligence.sourcefire.com 443
```

Verifique se você recebeu uma saída semelhante a esta:

```
Trying xxx.xxx.xx.x...
Connected to intelligence.sourcefire.com.
Escape character is '^]'.
```

Observação: se você conseguir concluir a segunda etapa com êxito, mas não conseguir executar telnet para i**ntelligence.sourcefire.com** pela porta 443, você pode ter uma regra de firewall que bloqueia a porta 443 de saída para intelligence.sourcefire.com.

6. Navegue até **System > Local > Configuration** e verifique as configurações de proxy do **Manual Proxy** configuração sob o comando **Network** seção.

Observação: se este proxy fizer uma inspeção SSL, você deverá colocar em vigor uma regra de desvio que ignore o proxy para **intelligence.sourcefire.com**.

7. Teste se você pode executar um HTTP GET solicitação contra intelligence.sourcefire.com:

```
admin@Firepower:~sudo curl -vvk https://intelligence.sourcefire.com
* About to connect() to intelligence.sourcefire.com port 443 (#0)
* Trying 198.148.79.58...
* Adding handle: conn: 0xec5630
* Adding handle: send: 0
* Adding handle: recv: 0
* Curl_addHandleToPipeline: length: 1
* - Conn 0 (0xec5630) send_pipe: 1, recv_pipe: 0
* Connected to intelligence.sourcefire.com (198.148.79.58) port 443 (#0)
* SSLv3, TLS handshake, Client hello (1):
* SSLv3, TLS handshake, Server hello (2):
* SSLv3, TLS handshake, CERT (11):
* SSLv3, TLS handshake, Server key exchange (12):
* SSLv3, TLS handshake, Server finished (14):
* SSLv3, TLS handshake, Client key exchange (16):
* SSLv3, TLS change cipher, Client hello (1):
* SSLv3, TLS handshake, Finished (20):
* SSLv3, TLS change cipher, Client hello (1):
```

```
* SSLv3, TLS handshake, Finished (20):
* SSL connection using DHE-RSA-AES256-SHA
* Server certificate:
* subject: O=Sourcefire Inc.; OU=VRT Department of Intelligence;
emailAddress=vrt-systems@sourcefire.com; L=Columbia; ST=MD; C=US;
CN=intelligence.sourcefire.com
* start date: 2016-02-29 22:50:29 GMT
* expire date: 2019-02-28 22:50:29 GMT
* issuer: O=Sourcefire Inc.; OU=VRT Department of Intelligence;
emailAddress=vrt-systems@sourcefire.com; L=Columbia; ST=MD; C=US;
CN=intelligence.sourcefire.com; nsCaRevocationUrl=
https://intelligence.sourcefire.com/vrtca.crl
* SSL certificate verify result: unable to get local issuer certificate
(20), continuing anyway.
>GET / HTTP/1.1
>User-Agent: curl/7.31.0
>Host: intelligence.sourcefire.com
>Accept: */*
>
<HTTP/1.1 200 OK
<Date: Tue, 01 Mar 2016 13:06:16 GMT
* Server Apache is not blacklisted
<Server: Apache
<Last-Modified: Tue, 09 Dec 2014 20:08:06 GMT
<ETag: "9da27-3-509ce19e67580"
<Accept-Ranges: bytes
<Content-Length: 3
<Content-Type: text/html
<
:)
* Connection #0 to host intelligence.sourcefire.com left intact
```

Observação: o rosto sorridente no final do curl indica uma conexão bem-sucedida.**Observação**: se você usar um proxy, o curl requer um nome de usuário. O comando é **curl -U <user> -vk** https://intelligence.sourcefire.com. Além disso, depois de inserir o comando, você será solicitado a inserir a senha do proxy.

8. Verifique se o tráfego HTTPS usado para baixar o feed Security Intelligence não passa por um descriptografador SSL. Para verificar se não ocorre descriptografia SSL, valide as informações do certificado do servidor na saída da etapa 6. Se o certificado do servidor não corresponder ao que é exibido no exemplo a seguir, você poderá ter um descriptografador SSL que renuncia ao certificado. Se o tráfego passar por um descriptografador SSL, você deverá ignorar todo o tráfego que vai para o intelligence.sourcefire.com.

```
admin@Firepower:~$ sudo curl -vvk https://intelligence.sourcefire.com
* About to connect() to intelligence.sourcefire.com port 443 (#0)
* Trying 198.148.79.58...
* Adding handle: conn: 0xec5630
* Adding handle: send: 0
* Adding handle: recv: 0
* Curl_addHandleToPipeline: length: 1
* - Conn 0 (0xec5630) send_pipe: 1, recv_pipe: 0
* Connected to intelligence.sourcefire.com (198.148.79.58) port 443 (#0)
* SSLv3, TLS handshake, Client hello (1):
* SSLv3, TLS handshake, Server hello (2):
* SSLv3, TLS handshake, CERT (11):
* SSLv3, TLS handshake, Server key exchange (12):
* SSLv3, TLS handshake, Server finished (14):
* SSLv3, TLS handshake, Client key exchange (16):
* SSLv3, TLS change cipher, Client hello (1):
* SSLv3, TLS handshake, Finished (20):
```

```
* SSLv3, TLS change cipher, Client hello (1):
* SSLv3, TLS handshake, Finished (20):
* SSL connection using DHE-RSA-AES256-SHA
* Server certificate:
* subject: O=Sourcefire Inc.; OU=VRT Department of Intelligence;
emailAddress=vrt-systems@sourcefire.com; L=Columbia; ST=MD; C=US;
CN=intelligence.sourcefire.com
* start date: 2016-02-29 22:50:29 GMT
* expire date: 2019-02-28 22:50:29 GMT
* issuer: O=Sourcefire Inc.; OU=VRT Department of Intelligence;
emailAddress=vrt-systems@sourcefire.com; L=Columbia; ST=MD; C=US;
CN=intelligence.sourcefire.com; nsCaRevocationUrl=
https://intelligence.sourcefire.com/vrtca.crl
*  SSL certificate verify result: unable to get local issuer certificate
(20), continuing anyway.
>GET / HTTP/1.1
>User-Agent: curl/7.31.0
>Host: intelligence.sourcefire.com
>Accept: */*
>
<HTTP/1.1 200 OK
<Date: Tue, 01 Mar 2016 13:06:16 GMT
* Server Apache is not blacklisted
<Server: Apache
<Last-Modified: Tue, 09 Dec 2014 20:08:06 GMT
<ETag: "9da27-3-509ce19e67580"
<Accept-Ranges: bytes
<Content-Length: 3
<Content-Type: text/html
<
:)
* Connection #0 to host intelligence.sourcefire.com left intact
```

Observação: a descriptografia SSL deve ser ignorada para o Security Intelligence Feed porque o descriptografador SSL envia ao Firepower Management Center um certificado desconhecido no handshake SSL. O certificado enviado ao Firepower Management Center não está assinado por uma CA confiável da Sourcefire, portanto, a conexão não é confiável.

Informações Relacionadas

- Automatic Falha de atualização de download em um Firepower Management Center
- Endereços de servidor necessários para operações de proteção avançada contra malware (AMP)
- Portas de comunicação necessárias para a operação do sistema Firepower
- Suporte Técnico e Documentação - Cisco Systems

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.