Solução de problemas de proxy no Cisco Secure Firewall Management Center (FMC)

Contents

Introdução

Este documento descreve a configuração de um proxy no FMC para permitir que os usuários se conectem à Internet através de um servidor intermediário, aumentando a segurança e, às vezes, melhorando o desempenho. Este artigo orienta você durante as etapas de configuração de um proxy no FMC e fornece dicas de solução de problemas comuns.

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Secure Firewall Management Center (FMC)
- Proxy

Componentes Utilizados

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

- FMC 7.4.x

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.

Configuração

Configure o proxy http da rede na GUI do FMC:

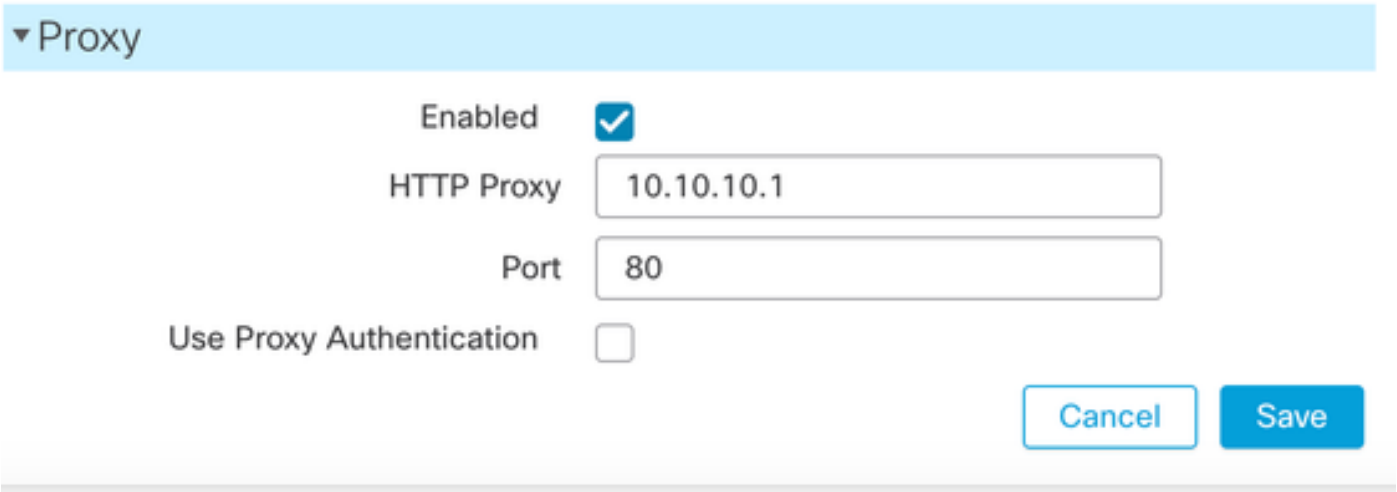
Faça login na GUI do FMC > Escolha System > Configuration e escolha Management Interfaces.

 Note: Não há suporte para proxies que usam a autenticação NT LAN Manager (NTLM). Se você usar o Smart Licensing, o FQDN do proxy não poderá ter mais de 64 caracteres.

Na área Proxy, defina as configurações do proxy HTTP.

O centro de gerenciamento é configurado para se conectar diretamente à Internet nas portas TCP/443 (HTTPS) e TCP/80 (HTTP). Você pode usar um servidor proxy, para o qual você pode se autenticar via HTTP Digest.

- Marque a caixa de seleçãoHabilitado.
- No campo HTTP Proxyfield, insira o endereço IP ou o nome de domínio totalmente qualificado do servidor proxy.
- No campoPorta, insira um número de porta.
- Forneça credenciais de autenticação escolhendo Usar autenticação de proxy e forneça um Nome de usuário e uma Senha.
- Click Save.



Nota: Para a senha proxy, você pode usar A-Z, a-z e 0-9 e caracteres especiais.

Troubleshooting

Obtenha acesso ao FMC CLI e ao modo especialista e verifique iprep_proxy.conf para garantir que as configurações de proxy estejam corretas:

<#root>

```
admin@fmc:~$
cat /etc/sf/iprep_proxy.conf

iprep_proxy {
PROXY_HOST 10.10.10.1;
PROXY_PORT 80;
}
```

Verifique as conexões ativas para verificar a conexão proxy ativa:

<#root>

```
admin@fmc:~$
netstat -na | grep 10.10.10.1

tcp 0 0 10.40.40.1:40220 10.10.10.1:80
ESTABLISHED
```

Usando o comando curl, verifique os detalhes da solicitação e a resposta do proxy. Se você receber a resposta: HTTP/1.1 200 Connection established, isso indica que o FMC está enviando e recebendo tráfego com êxito através do proxy.

<#root>

admin@fmc:~$

curl -x http://10.10.10.1:80 -I https://tools.cisco.com

HTTP/1.1 200 Connection established

Se você configurou o nome de usuário e a senha para o proxy, verifique a autenticação e a resposta do proxy:

```
curl -u proxyuser:proxypass --proxy http://proxy.example.com:80 https://example.com
```

Verificação

Estabelecimento de Conexão Bem-sucedido via Proxy

Ao executar um comando curl com um proxy, tal como curl -x http://proxy:80 -I https://tools.cisco.com, uma série de interações de rede esperadas ocorrem, que podem ser observadas através da captura de pacotes (tcpdump). Esta é uma visão geral de alto nível do processo, enriquecida com saídas reais de tcpdump:

Início do handshake TCP:
O cliente (FMC) inicia uma conexão TCP com o servidor proxy na porta 80, enviando um pacote SYN. O proxy responde com um SYN-ACK e o cliente conclui o handshake com um ACK. Isso estabelece a sessão TCP sobre a qual a comunicação HTTP prossegue.

Exemplo de saída de tcpdump:

```
10:20:58.987654 IP client.54321 > proxy.80: Flags [S], seq 0, win 64240, options [mss 1460], length 0
10:20:58.987700 IP proxy.80 > client.54321: Flags [S.], seq 0, ack 1, win 65160, options [mss 1460], le
10:20:58.987734 IP client.54321 > proxy.80: Flags [.], ack 1, win 64240, length 0
```

Solicitação HTTP CONNECT:
Uma vez estabelecida a conexão TCP, o cliente envia uma solicitação HTTP CONNECT ao

proxy, instruindo-o a criar um túnel para o servidor HTTPS de destino (tools.cisco.com:443). Essa solicitação permite que o cliente negocie uma sessão TLS fim-a-fim por meio do proxy.

Exemplo de tcpdump (HTTP decodificado):

```
CONNECT tools.cisco.com:443 HTTP/1.1
Host: tools.cisco.com:443
User-Agent: curl/8.5.0
Proxy-Connection: Keep-Alive
```

Confirmação de estabelecimento de conexão:
O proxy responde com uma resposta HTTP/1.1 200 Connection estabelecida, indicando que o túnel para o servidor de destino foi criado com êxito. Isso significa que o proxy está agora agindo como um relé, encaminhando tráfego criptografado entre o cliente e tools.cisco.com.

Exemplo de tcpdump:

<#root>

```
HTTP/1.1
```

200

```
 Connection established
```

Comunicação HTTPS via túnel:
Após a resposta CONNECT bem-sucedida, o cliente inicia o handshake SSL/TLS diretamente com tools.cisco.com pelo túnel estabelecido. Como esse tráfego é criptografado, o conteúdo não fica visível no tcpdump, mas os comprimentos e os tempos dos pacotes são observáveis, incluindo os pacotes Hello do cliente TLS e Hello do servidor.

Exemplo de tcpdump:

```
10:20:59.123456 IP client.54321 > proxy.80: Flags [P.], length 517 (Client Hello)
10:20:59.123789 IP proxy.80 > client.54321: Flags [P.], length 1514 (Server Hello)
```

Tratamento do redirecionamento HTTP (302 encontrados):
Como parte da comunicação HTTPS, o cliente solicita o recurso de tools.cisco.com. O servidor responde com um redirecionamento HTTP/1.1 302 Encontrado para outro URL (https://tools.cisco.com/healthcheck), que o cliente pode seguir dependendo dos parâmetros curl

e da finalidade da solicitação. Embora esse redirecionamento ocorra dentro da sessão TLS criptografada e não seja diretamente visível, é esperado comportamento e pode ser observado se o tráfego TLS for descriptografado.

O tráfego de redirecionamento criptografado seria semelhante a este:

```
10:21:00.123000 IP client.54321 > proxy.80: Flags [P.], length 517 (Encrypted Application Data)
10:21:00.123045 IP proxy.80 > client.54321: Flags [P.], length 317 (Encrypted Application Data)
```

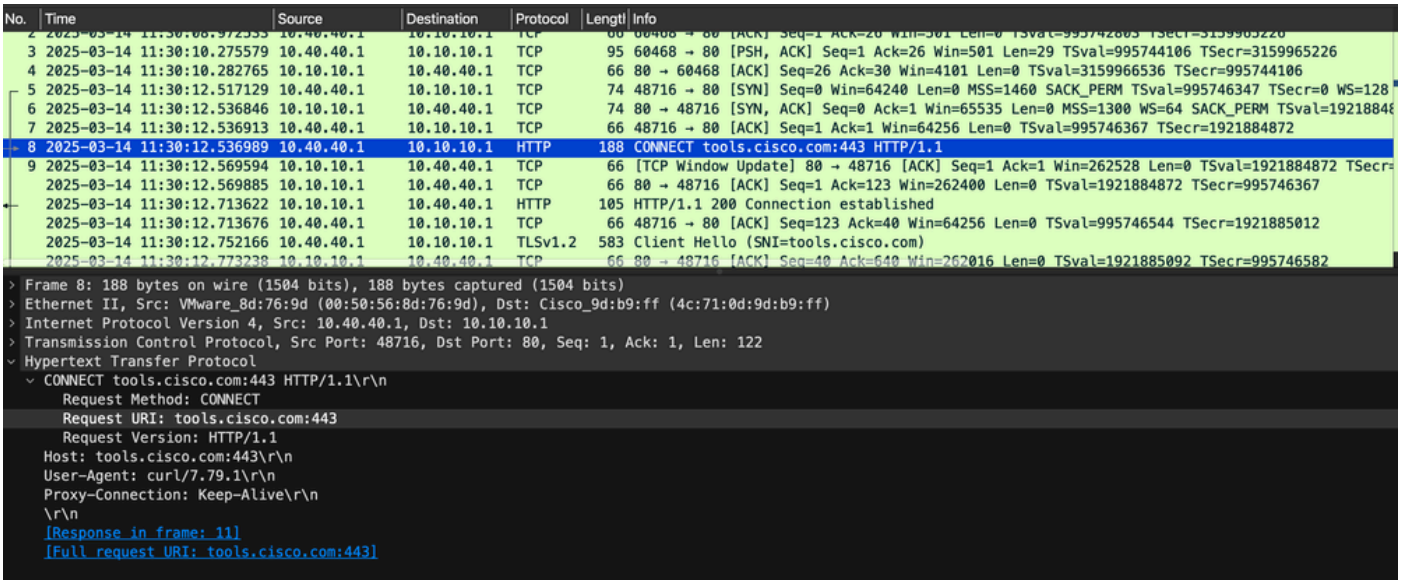
Desmontagem da conexão:
Quando a troca estiver concluída, o cliente e o proxy fecham normalmente a conexão TCP trocando pacotes FIN e ACK, garantindo o término adequado da sessão.

Exemplo de saída de tcpdump:

```
10:21:05.000111 IP client.54321 > proxy.80: Flags [F.], seq 1234, ack 5678, length 0
10:21:05.000120 IP proxy.80 > client.54321: Flags [F.], seq 5678, ack 1235, length 0
10:21:05.000125 IP client.54321 > proxy.80: Flags [.], ack 5679, length 0
```

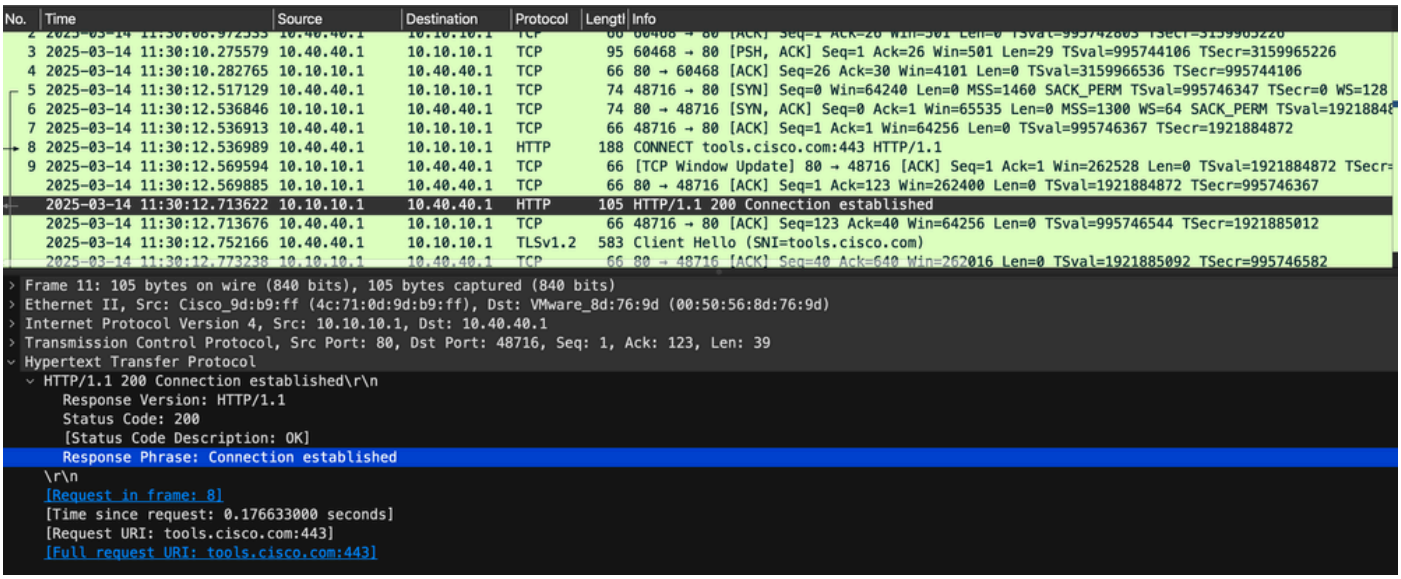
Tip: Analisando a saída tcpdump, você pode verificar se a solicitação HTTPS através do proxy explícito segue o fluxo esperado: Handshake TCP, solicitação CONNECT, estabelecimento de túnel, handshake TLS, comunicação criptografada (incluindo possíveis redirecionamentos) e fechamento de conexão grátis. Isso confirma que a interação do proxy e do cliente está funcionando conforme projetado e ajuda a identificar quaisquer problemas no fluxo, como falhas no tunelamento ou na negociação SSL.

O FMC (10.40.40.1) estabelece um handshake TCP bem-sucedido com o Proxy (10.10.10.1) na porta 80, seguido por um HTTP CONNECT para o servidor (72.163.4.161) na porta 443. O servidor responde com uma mensagem HTTP 200 Connection established. O handshake TLS é concluído e os dados fluem corretamente. Finalmente, a conexão TCP termina normalmente (FIN).



```
No.  Time                    Source        Destination   Protocol  Lengt  Info
   3 2025-03-14 11:30:10.275579 10.40.40.1  10.10.10.1    TCP         95 60468 → 80 [PSH, ACK] Seq=1 Ack=26 Win=501 Len=29 TSval=995744106 TSecr=3159965226
   4 2025-03-14 11:30:10.282765 10.10.10.1  10.40.40.1    TCP         66 80 → 60468 [ACK] Seq=26 Ack=30 Win=4101 Len=0 TSval=3159966536 TSecr=995744106
   5 2025-03-14 11:30:12.517129 10.40.40.1  10.10.10.1    TCP         74 48716 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=995746347 TSecr=0 WS=128
   6 2025-03-14 11:30:12.536846 10.10.10.1  10.40.40.1    TCP         74 80 → 48716 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1300 WS=64 SACK_PERM TSval=1921884
   7 2025-03-14 11:30:12.536913 10.40.40.1  10.10.10.1    TCP         66 48716 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=995746367 TSecr=1921884872
   8 2025-03-14 11:30:12.536989 10.40.40.1  10.10.10.1    HTTP       188 CONNECT tools.cisco.com:443 HTTP/1.1
   9 2025-03-14 11:30:12.569594 10.10.10.1  10.40.40.1    TCP         66 [TCP Window Update] 80 → 48716 [ACK] Seq=1 Ack=1 Win=262528 Len=0 TSval=1921884872 TSecr=
     2025-03-14 11:30:12.569885 10.10.10.1  10.40.40.1    TCP         66 80 → 48716 [ACK] Seq=1 Ack=123 Win=262400 Len=0 TSval=1921884872 TSecr=995746367
     2025-03-14 11:30:12.713622 10.10.10.1  10.40.40.1    HTTP       105 HTTP/1.1 200 Connection established
     2025-03-14 11:30:12.713676 10.40.40.1  10.10.10.1    TCP         66 48716 → 80 [ACK] Seq=123 Ack=40 Win=64256 Len=0 TSval=995746544 TSecr=1921885012
     2025-03-14 11:30:12.752166 10.40.40.1  10.10.10.1    TLSv1.2    583 Client Hello (SNI=tools.cisco.com)
     2025-03-14 11:30:12.773238 10.10.10.1  10.40.40.1    TCP         66 80 → 48716 [ACK] Seq=40 Ack=640 Win=262016 Len=0 TSval=1921885092 TSecr=995746582

> Frame 8: 188 bytes on wire (1504 bits), 188 bytes captured (1504 bits)
> Ethernet II, Src: VMware_8d:76:9d (00:50:56:8d:76:9d), Dst: Cisco_9d:b9:ff (4c:71:0d:9d:b9:ff)
> Internet Protocol Version 4, Src: 10.40.40.1, Dst: 10.10.10.1
> Transmission Control Protocol, Src Port: 48716, Dst Port: 80, Seq: 1, Ack: 1, Len: 122
v Hypertext Transfer Protocol
  v CONNECT tools.cisco.com:443 HTTP/1.1\r\n
      Request Method: CONNECT
      Request URI: tools.cisco.com:443
      Request Version: HTTP/1.1
    Host: tools.cisco.com:443\r\n
    User-Agent: curl/7.79.1\r\n
    Proxy-Connection: Keep-Alive\r\n
    \r\n
    [Response in frame: 11]
    [Full request URI: tools.cisco.com:443]
```



```
No.  Time                    Source        Destination   Protocol  Lengt  Info
   3 2025-03-14 11:30:10.275579 10.40.40.1  10.10.10.1    TCP         95 60468 → 80 [PSH, ACK] Seq=1 Ack=26 Win=501 Len=29 TSval=995744106 TSecr=3159965226
   4 2025-03-14 11:30:10.282765 10.10.10.1  10.40.40.1    TCP         66 80 → 60468 [ACK] Seq=26 Ack=30 Win=4101 Len=0 TSval=3159966536 TSecr=995744106
   5 2025-03-14 11:30:12.517129 10.40.40.1  10.10.10.1    TCP         74 48716 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=995746347 TSecr=0 WS=128
   6 2025-03-14 11:30:12.536846 10.10.10.1  10.40.40.1    TCP         74 80 → 48716 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1300 WS=64 SACK_PERM TSval=1921884
   7 2025-03-14 11:30:12.536913 10.40.40.1  10.10.10.1    TCP         66 48716 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=995746367 TSecr=1921884872
   8 2025-03-14 11:30:12.536989 10.40.40.1  10.10.10.1    HTTP       188 CONNECT tools.cisco.com:443 HTTP/1.1
   9 2025-03-14 11:30:12.569594 10.10.10.1  10.40.40.1    TCP         66 [TCP Window Update] 80 → 48716 [ACK] Seq=1 Ack=1 Win=262528 Len=0 TSval=1921884872 TSecr=
     2025-03-14 11:30:12.569885 10.10.10.1  10.40.40.1    TCP         66 80 → 48716 [ACK] Seq=1 Ack=123 Win=262400 Len=0 TSval=1921884872 TSecr=995746367
     2025-03-14 11:30:12.713622 10.10.10.1  10.40.40.1    HTTP       105 HTTP/1.1 200 Connection established
     2025-03-14 11:30:12.713676 10.40.40.1  10.10.10.1    TCP         66 48716 → 80 [ACK] Seq=123 Ack=40 Win=64256 Len=0 TSval=995746544 TSecr=1921885012
     2025-03-14 11:30:12.752166 10.40.40.1  10.10.10.1    TLSv1.2    583 Client Hello (SNI=tools.cisco.com)
     2025-03-14 11:30:12.773238 10.10.10.1  10.40.40.1    TCP         66 80 → 48716 [ACK] Seq=40 Ack=640 Win=262016 Len=0 TSval=1921885092 TSecr=995746582

> Frame 11: 105 bytes on wire (840 bits), 105 bytes captured (840 bits)
> Ethernet II, Src: Cisco_9d:b9:ff (4c:71:0d:9d:b9:ff), Dst: VMware_8d:76:9d (00:50:56:8d:76:9d)
> Internet Protocol Version 4, Src: 10.10.10.1, Dst: 10.40.40.1
> Transmission Control Protocol, Src Port: 80, Dst Port: 48716, Seq: 1, Ack: 123, Len: 39
v Hypertext Transfer Protocol
  v HTTP/1.1 200 Connection established\r\n
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: Connection established
    \r\n
    [Request in frame: 8]
    [Time since request: 0.176633000 seconds]
    [Request URI: tools.cisco.com:443]
    [Full request URI: tools.cisco.com:443]
```

Problemas conhecidos

Restrições de ACL de proxy

Se houver um problema de permissão (como uma lista de acesso no proxy), você poderá observar isso por meio da captura de pacotes (tcpdump). Esta é uma explicação de alto nível do cenário de falha, juntamente com saídas de exemplo tcpdump:

Início do handshake TCP:
O cliente (Firepower) começa estabelecendo uma conexão TCP com o proxy na porta 80. O handshake TCP (SYN, SYN-ACK, ACK) é concluído com êxito, o que significa que o proxy está acessível.

Exemplo de saída de tcpdump:

```
10:20:58.987654 IP client.54321 > proxy.80: Flags [S], seq 0, win 64240, options [mss 1460], length 0
10:20:58.987700 IP proxy.80 > client.54321: Flags [S.], seq 0, ack 1, win 65160, options [mss 1460], le
10:20:58.987734 IP client.54321 > proxy.80: Flags [.], ack 1, win 64240, length 0
```

Solicitação HTTP CONNECT:
Uma vez conectado, o cliente envia uma solicitação HTTP CONNECT ao proxy, solicitando que ele crie um túnel para tools.cisco.com:443.

Exemplo de tcpdump (HTTP decodificado):

```
CONNECT tools.cisco.com:443 HTTP/1.1
Host: tools.cisco.com:443
User-Agent: curl/8.5.0
Proxy-Connection: Keep-Alive
```

Resposta de erro do proxy:

Em vez de permitir o túnel, o proxy nega a solicitação, provavelmente devido a uma lista de acesso (ACL) que não permite esse tráfego. O proxy responde com um erro como 403 Forbidden ou 502 Bad Gateway.

Exemplo de saída tcpdump mostrando erro:

<#root>

```
HTTP/1.1
```

403

```
 Forbidden
Content-Type: text/html
Content-Length: 123
Connection: close
```

Desmontagem da conexão:
Após enviar a mensagem de erro, o proxy fecha a conexão e ambos os lados trocam pacotes FIN/ACK.

Exemplo de saída de tcpdump:

```
10:21:05.000111 IP client.54321 > proxy.80: Flags [F.], seq 1234, ack 5678, length 0
10:21:05.000120 IP proxy.80 > client.54321: Flags [F.], seq 5678, ack 1235, length 0
10:21:05.000125 IP client.54321 > proxy.80: Flags [.], ack 5679, length 0
```

Tip: No tcpdump, você pode ver que, embora a conexão TCP e a solicitação HTTP CONNECT tenham sido bem-sucedidas, o proxy negou a configuração do túnel. Isso geralmente indica que o proxy tem uma ACL ou restrição de permissão impedindo a passagem do tráfego.

Falha no download do proxy (Tempo limite/Transferência incompleta)

Nesse cenário, o FMC se conecta com êxito ao proxy e inicia o download do arquivo, mas a transferência expira ou não é concluída. Isso geralmente ocorre devido à inspeção de proxy, tempos limite ou limites de tamanho de arquivo no proxy.

Iniciação de handshake TCP
O FMC inicia uma conexão TCP com o proxy na porta 80 e o handshake é concluído com êxito.
Exemplo de saída de tcpdump:

```
10:20:58.987654 IP fmc.54321 > proxy.80: Flags [S], seq 0, win 64240, options [mss 1460], length 0
10:20:58.987700 IP proxy.80 > fmc.54321: Flags [S.], seq 0, ack 1, win 65160, options [mss 1460], lengt
10:20:58.987734 IP fmc.54321 > proxy.80: Flags [.], ack 1, win 64240, length 0
```

Solicitação HTTP CONNECT
O FMC envia uma solicitação HTTP CONNECT ao proxy para alcançar o destino externo.
Exemplo de tcpdump (HTTP decodificado):

```
CONNECT tools.cisco.com:443 HTTP/1.1
Host: tools.cisco.com:443
User-Agent: FMC-Agent
Proxy-Connection: Keep-Alive
```

Estabelecimento de túnel e handshake TLS
O proxy responde com a conexão HTTP/1.1 200 estabelecida, permitindo que o handshake TLS comece.

Exemplo de saída de tcpdump:

<#root>

```
HTTP/1.1
```

```
200

 Connection established
10:20:59.123456 IP fmc.54321 > proxy.80: Flags [P.], length 517 (Client Hello)
10:20:59.123789 IP proxy.80 > fmc.54321: Flags [P.], length 1514 (Server Hello)
```

Tempo limite ou download incompleto
Após iniciar a transferência de arquivo, o download é interrompido ou não é concluído, levando a um tempo limite. A conexão permanece ociosa.
As possíveis razões incluem:

- Atrasos ou filtragem na inspeção de proxy.
- Tempos limite de proxy para transferências longas.
- Limites de tamanho de arquivo impostos pelo proxy.

Exemplo de tcpdump mostrando inatividade:

<#root>

```
10:21:00.456000 IP fmc.54321 > proxy.80: Flags [P.], length 1440

# FMC sending data


# No response from proxy, connection goes idle...


# After a while, FMC may close the connection or retry.
```


Tip: O FMC inicia o download, mas não é concluído devido a tempos limite ou transferências incompletas, geralmente causadas por filtragem de proxy ou restrições de tamanho de arquivo.

O proxy falha no download do arquivo (problema de MTU)

Nesse caso, o FMC se conecta ao proxy e inicia o download dos arquivos, mas a sessão falha devido a problemas de MTU. Esses problemas causam fragmentação de pacotes ou perda de pacotes, especialmente com arquivos grandes ou handshakes SSL/TLS.

Iniciação de handshake TCP
O FMC inicia o handshake TCP com o proxy, que é bem-sucedido.
Exemplo de saída de tcpdump:

```
10:20:58.987654 IP fmc.54321 > proxy.80: Flags [S], seq 0, win 64240, options [mss 1460], length 0
10:20:58.987700 IP proxy.80 > fmc.54321: Flags [S.], seq 0, ack 1, win 65160, options [mss 1460], lengt
10:20:58.987734 IP fmc.54321 > proxy.80: Flags [.], ack 1, win 64240, length 0
```

Solicitação HTTP CONNECT e estabelecimento de túnel
O FMC envia uma solicitação HTTP CONNECT e o proxy responde, permitindo que o túnel seja estabelecido.
Exemplo de tcpdump (HTTP decodificado):

```
CONNECT tools.cisco.com:443 HTTP/1.1
Host: tools.cisco.com:443
User-Agent: FMC-Agent
Proxy-Connection: Keep-Alive
```

O handshake TLS começa
O FMC e o tools.cisco.com começam a negociar SSL/TLS e os pacotes iniciais são trocados.
Exemplo de saída de tcpdump:

<#root>

```
HTTP/1.1
```

200

```
 Connection established
10:20:59.123456 IP fmc.54321 > proxy.80: Flags [P.], length 517 (Client Hello)
10:20:59.123789 IP proxy.80 > fmc.54321: Flags [P.], length 1514 (Server Hello)
```

Fragmentação ou queda de pacote devido à MTU
Quando o FMC ou o servidor tenta enviar pacotes grandes, problemas de MTU causam fragmentação de pacote ou quedas de pacote, resultando em falhas de transferência de arquivo ou negociação de TLS.
Isso geralmente ocorre quando a MTU entre o FMC e o proxy (ou entre o proxy e a Internet) está definida incorretamente ou é muito pequena.
Exemplo de tcpdump mostrando a tentativa de fragmentação:

<#root>

```
10:21:00.456000 IP fmc.54321 > proxy.80: Flags [P.], length 1440
```

 # Large packet

```
10:21:00.456123 IP proxy.80 > fmc.54321: Flags [R], seq X, win 0, length 0
# Proxy resets connection due to MTU issue
```

Tip: O problema de MTU resulta em pacotes descartados ou fragmentados, que interrompem o handshake TLS ou fazem com que os downloads de arquivos falhem. Isso é comumente visto quando a inspeção SSL ou a fragmentação de pacote ocorre devido a configurações incorretas de MTU.

Em um cenário de falha, o FMC obtém o CONNECT sem HTTP 200, com retransmissões e FINs confirmando que não há troca de TLS/dados, possivelmente devido a problemas de MTU ou um problema de proxy/upstream.

Ao usar curl, você pode encontrar vários códigos de resposta HTTP indicando problemas no servidor ou erros de autenticação. Esta é uma lista dos códigos de erro mais comuns e seus significados:

Código HTTP	Significado	Causa
400	Solicitação Incorreta	Sintaxe de solicitação incorreta
401	Não autorizado	Credenciais ausentes ou incorretas
403	Proibido	Acesso negado
404	Not found	Recurso não encontrado
500	Internal Error	Erro do servidor
502	Gateway incorreto	Erro de comunicação do servidor
503	Serviço indisponível	Sobrecarga ou manutenção do servidor
504	Tempo limite do gateway	Tempo limite entre servidores

Referências

Notas de versão do Cisco Secure Firewall Threat Defense, versão 7.4.x

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.