Solución de problemas de proxy en Cisco Secure Firewall Management Center (FMC)

Contenido

Introducción

En este documento se describe la configuración de un proxy en FMC para permitir que los usuarios se conecten a Internet a través de un servidor intermediario, lo que mejora la seguridad y, en ocasiones, el rendimiento. En este artículo se explican los pasos necesarios para configurar un proxy en FMC y se ofrecen consejos para la resolución de problemas habituales.

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Secure Firewall Management Center (FMC)
- Proxy

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- FMC 7.4.x

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configuración

Configuración del proxy http de red en la GUI de FMC:

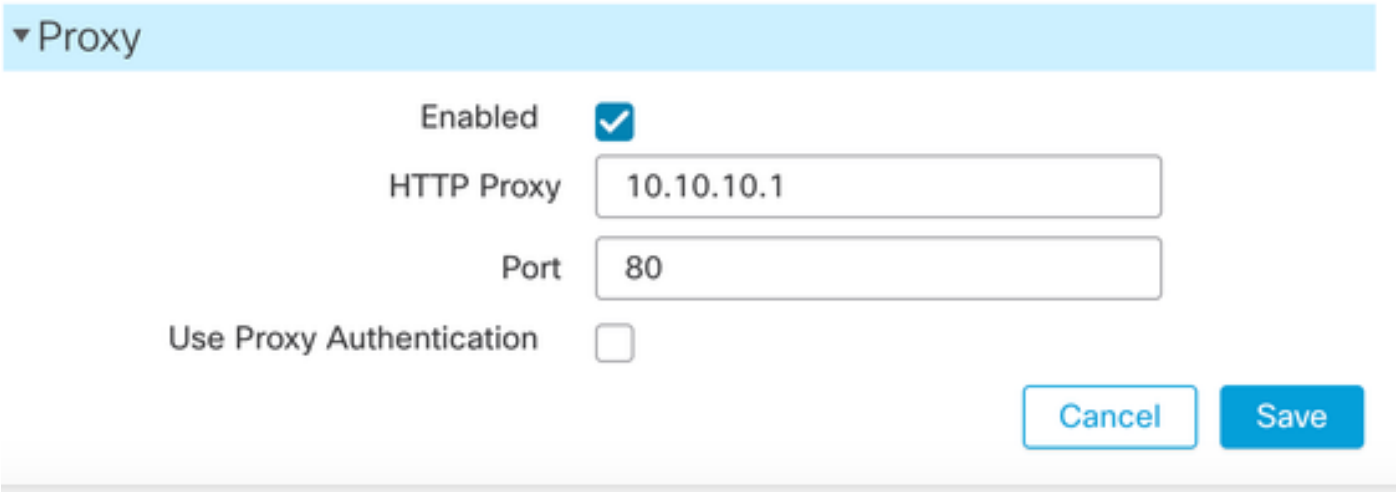
Inicie sesión en FMC GUI > Elija System > Configuration y luego elija Management Interfaces.

Nota: No se admiten los proxies que utilizan la autenticación NT LAN Manager (NTLM). Si utiliza Smart Licensing, el FQDN del proxy no puede tener más de 64 caracteres.

En el área Proxy, configure los valores de proxy HTTP.

El centro de administración se configura para conectarse directamente a Internet en los puertos TCP/443 (HTTPS) y TCP/80 (HTTP). Puede utilizar un servidor proxy, al que se puede autenticar a través de HTTP Digest.

- Marque la casilla de verificación Habilitado.
- En el campoHTTP Proxy, introduzca la dirección IP o el nombre de dominio completo del servidor proxy.
- En el campo Puerto, introduzca un número de puerto.
- Suministre las credenciales de autenticación eligiendoUsar autenticación de proxy y, a continuación, proporcione unNombre de usuario y unaContraseña.
- Click Save.



Nota: Para la contraseña de proxy puede utilizar caracteres A-Z, a-z y 0-9 y caracteres especiales.

Troubleshoot

Obtenga acceso a FMC CLI y al modo experto, y luego verifique iprep_proxy.conf para asegurarse de que la configuración del proxy sea correcta:

<#root>

```
admin@fmc:~$
```

cat /etc/sf/iprep_proxy.conf

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

Verifique las conexiones activas para verificar la conexión de proxy activa:

<#root>

```
admin@fmc:~$
```

netstat -na | grep 10.10.10.1

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

ESTABLISHED

Con el comando curl, verifique tanto los detalles de la solicitud como la respuesta del proxy. Si recibe la respuesta: HTTP/1.1 200 Connection establecido, esto indica que el FMC está enviando y recibiendo tráfico con éxito a través del proxy.

<#root>

```
admin@fmc:~$
```

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

HTTP/1.1 200 Connection established

Si ha configurado el nombre de usuario y la contraseña para el proxy, verifique la autenticación y la respuesta del proxy:

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

Verificación

Establecimiento correcto de la conexión mediante proxy

Al ejecutar un comando curl con un proxy, como curl -x http://proxy:80 -I https://tools.cisco.com, se producen una serie de interacciones de red esperadas, que se pueden observar a través de la captura de paquetes (tcpdump). Esta es una descripción general de alto nivel del proceso, enriquecida con salidas tcpdump reales:

Inicio de intercambio de señales TCP:
El cliente (FMC) inicia una conexión TCP con el servidor proxy en el puerto 80 enviando un paquete SYN. El proxy responde con un SYN-ACK, y el cliente completa el intercambio de señales con un ACK. Esto establece la sesión TCP sobre la que se produce la comunicación HTTP.

Ejemplo de salida 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
```

Solicitud HTTP CONNECT:

Una vez establecida la conexión TCP, el cliente envía una solicitud HTTP CONNECT al proxy, indicándole que cree un túnel al servidor HTTPS de destino (tools.cisco.com:443). Esta solicitud permite al cliente negociar una sesión TLS de extremo a extremo a través del proxy.

Ejemplo tcpdump (HTTP descodificado):

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

Reconocimiento de establecimiento de conexión:
El proxy responde con una respuesta establecida de HTTP/1.1 200 Connection, que indica que el túnel al servidor de destino se ha creado correctamente. Esto significa que el proxy actúa ahora como un relay, reenviando el tráfico cifrado entre el cliente y tools.cisco.com.

Ejemplo de tcpdump:

<#root>

```
HTTP/1.1
```

200

```
 Connection established
```

Comunicación HTTPS a través del túnel:
Después de la respuesta CONNECT exitosa, el cliente inicia el intercambio de señales SSL/TLS directamente con tools.cisco.com a través del túnel establecido. Dado que este tráfico está cifrado, el contenido no es visible en tcpdump, pero se pueden observar las longitudes y los intervalos de paquetes, incluidos los paquetes Hello de cliente TLS y Hello de servidor.

Ejemplo 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)
```

Gestión de redirección HTTP (302 encontrados):
Como parte de la comunicación HTTPS, el cliente solicita el recurso de tools.cisco.com. El servidor responde con un HTTP/1.1 302 Found redireccionado a otra URL

(https://tools.cisco.com/healthcheck), que el cliente puede seguir dependiendo de los parámetros curl y propósito de la solicitud. Aunque esta redirección ocurre dentro de la sesión TLS cifrada y no es visible directamente, se espera un comportamiento y se puede observar si el tráfico TLS se descifra.

El tráfico de redirección cifrado tendría este aspecto:

```
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)
```

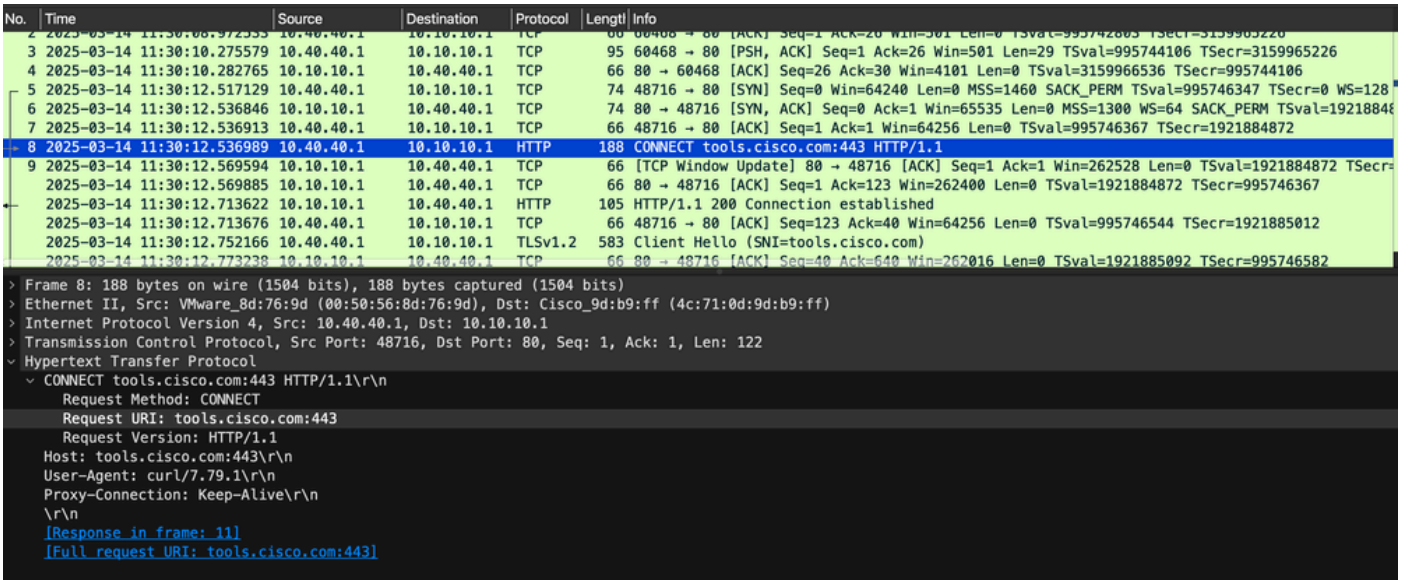
Desconexión de la conexión:
Una vez finalizado el intercambio, tanto el cliente como el proxy cierran correctamente la conexión TCP intercambiando los paquetes FIN y ACK, lo que garantiza la terminación correcta de la sesión.

Ejemplo de salida 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
```

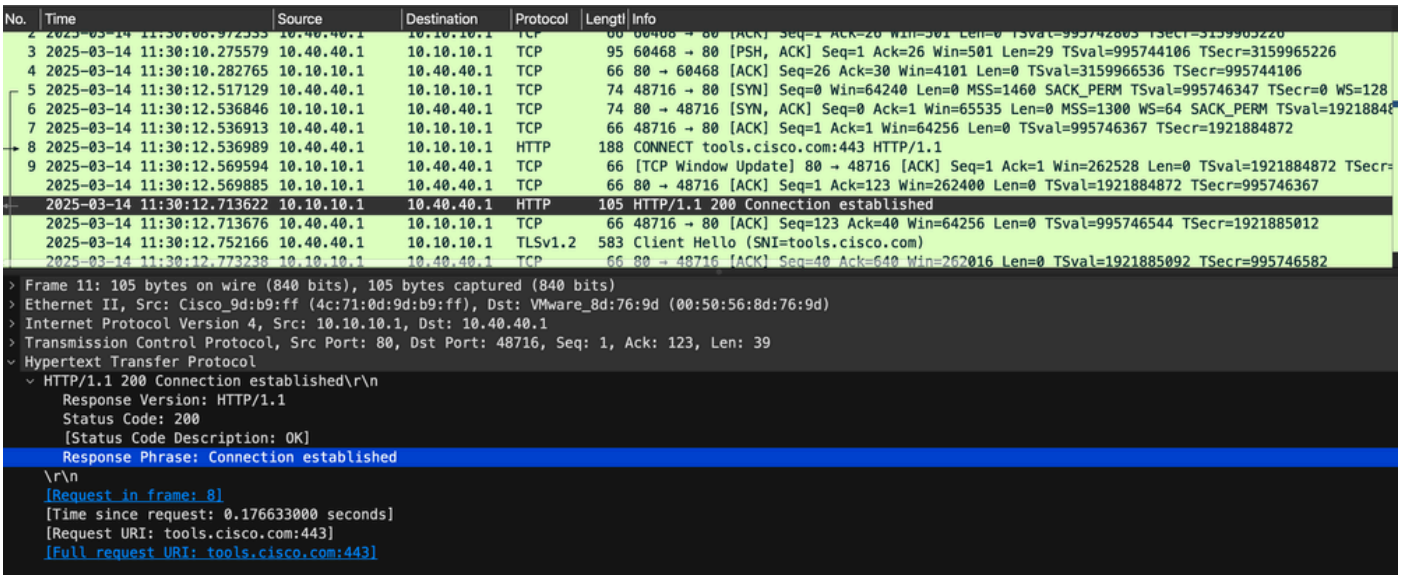
Consejo: Al analizar la salida tcpdump, puede verificar que la solicitud HTTPS a través del proxy explícito siga el flujo esperado: protocolo de enlace TCP, solicitud CONNECT, establecimiento de túnel, protocolo de enlace TLS, comunicación cifrada (incluidos posibles redireccionamientos) y cierre de conexión correcto. Esto confirma que la interacción del proxy y el cliente funciona correctamente y ayuda a identificar cualquier problema en el flujo, como fallos en la tunelización o la negociación SSL.

El FMC (10.40.40.1) establece un protocolo de enlace TCP correcto con el proxy (10.10.10.1) en el puerto 80, seguido de una conexión HTTP al servidor (72.163.4.161) en el puerto 443. El servidor responde con un mensaje HTTP 200 Connection establecido. El intercambio de señales TLS se completa y los datos fluyen correctamente. Por último, la conexión TCP finaliza correctamente (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)

```
> 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)

```
> 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 conocidos

Restricciones de ACL de Proxy

Si hay un problema de permisos (como una lista de acceso en el proxy), puede observarlo a través de la captura de paquetes (tcpdump). Esta es una explicación de alto nivel del escenario de falla, junto con ejemplos de salidas tcpdump:

Inicio de intercambio de señales TCP:
El cliente (Firepower) comienza estableciendo una conexión TCP con el proxy en el puerto 80. El protocolo de enlace TCP (SYN, SYN-ACK, ACK) se completa correctamente, lo que significa que el proxy es accesible.

Ejemplo de salida 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
```

Solicitud HTTP CONNECT:
Una vez conectado, el cliente envía una solicitud HTTP CONNECT al proxy, pidiéndole que cree un túnel a tools.cisco.com:443.

Ejemplo tcpdump (HTTP descodificado):

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

Respuesta de error del proxy:

En lugar de permitir el túnel, el proxy deniega la solicitud, probablemente debido a una lista de acceso (ACL) que no permite este tráfico. El proxy responde con un error como 403 Forbidden o 502 Bad Gateway.

Ejemplo de salida tcpdump que muestra el error:

<#root>

```
HTTP/1.1
```

403

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

Desconexión de la conexión:
Después de enviar el mensaje de error, el proxy cierra la conexión y ambos lados intercambian paquetes FIN/ACK.

Ejemplo de salida 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
```

Consejo: Desde tcpdump, puede ver que aunque la conexión TCP y la solicitud HTTP CONNECT se realizaron correctamente, el proxy denegó la configuración del túnel. Esto normalmente indica que el proxy tiene una ACL o restricción de permisos que impide el paso del tráfico.

Descarga fallida del proxy (tiempo de espera/transferencia incompleta)

En esta situación, FMC se conecta correctamente al proxy e inicia la descarga del archivo, pero la transferencia se agota o no puede completarse. Esto se debe normalmente a la inspección de proxy, tiempos de espera o límites de tamaño de archivo en el proxy.

Inicio de intercambio de señales TCP
FMC inicia una conexión TCP con el proxy en el puerto 80 y el protocolo de enlace se completa correctamente.
Ejemplo de salida 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
```

Solicitud HTTP CONNECT
FMC envía una solicitud HTTP CONNECT al proxy para alcanzar el destino externo.
Ejemplo tcpdump (HTTP descodificado):

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

Establecimiento de túnel y protocolo de enlace TLS
El proxy responde con HTTP/1.1.200 Connection establecido, lo que permite que comience el intercambio de señales TLS.

Ejemplo de salida 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)
```

Tiempo de espera o descarga incompleta
Después de iniciar la transferencia de archivos, la descarga se detiene o no se completa, lo que provoca un tiempo de espera. La conexión permanece inactiva.
Entre las posibles razones se incluyen:

- Filtrado o retrasos de inspección de proxy.
- Tiempos de espera de proxy para transferencias largas.
- Límites de tamaño de archivo impuestos por el proxy.

Ejemplo de tcpdump mostrando inactividad:

<#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.
```

 Consejo: FMC inicia la descarga pero no puede completarse debido a tiempos de espera o transferencias incompletas, a menudo provocados por el filtrado proxy o restricciones de tamaño de archivo.

El proxy falla la descarga del archivo (problema de MTU)

En este caso, FMC se conecta al proxy y comienza a descargar archivos, pero la sesión falla debido a problemas de MTU. Estos problemas provocan la fragmentación de paquetes o la pérdida de paquetes, especialmente con archivos grandes o protocolos de enlace SSL/TLS.

Inicio de intercambio de señales TCP
FMC inicia el protocolo de enlace TCP con el proxy, lo que se realiza correctamente.
Ejemplo de salida 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
```

Solicitud HTTP CONNECT y establecimiento de túnel
FMC envía una solicitud HTTP CONNECT y el proxy responde, lo que permite establecer el túnel.
Ejemplo tcpdump (HTTP descodificado):

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

Comienza el intercambio de señales TLS
FMC y tools.cisco.com comienzan a negociar SSL/TLS, y se intercambian los paquetes iniciales.
Ejemplo de salida 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)
```

Fragmentación o eliminación de paquetes debido a MTU
Cuando FMC o el servidor intentan enviar paquetes de gran tamaño, los problemas de MTU provocan la fragmentación de paquetes o la pérdida de paquetes, lo que da como resultado la transferencia de archivos o los errores de negociación de TLS.
Esto suele ocurrir cuando la MTU entre FMC y el proxy (o entre el proxy e Internet) está configurada incorrectamente o es demasiado pequeña.
Ejemplo de tcpdump que muestra el intento de fragmentación:

<#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
```

Consejo: El problema de MTU produce paquetes perdidos o fragmentados, que interrumpen el intercambio de señales de TLS o hacen que falle la descarga de archivos. Esto se observa comúnmente cuando ocurre la inspección SSL o la fragmentación de paquetes debido a configuraciones de MTU incorrectas.

En caso de fallo, FMC obtiene CONNECT sin HTTP 200, con retransmisiones y FIN que confirman que no hay intercambio de datos/TLS, posiblemente debido a problemas de MTU o a un problema de proxy/flujo ascendente.

Al utilizar curl, puede encontrar varios códigos de respuesta HTTP que indican problemas en el servidor o errores de autenticación. Esta es una lista de los códigos de error más comunes y sus significados:

Código HTTP	Significado	Causa
400	Solicitud incorrecta	Sintaxis de solicitud incorrecta
401	No autorizado	Faltan credenciales o son incorrectas
403	Prohibido	Access Denied
404	Not found	Recurso no encontrado
500	Internal Error	Error del servidor
502	Gateway incorrecto	Mala comunicación del servidor
503	Servicio no disponible	Sobrecarga o mantenimiento del servidor
504	Tiempo de espera de gateway	Tiempo de espera entre servidores

Referencias

Notas de la versión de Cisco Secure Firewall Threat Defence, versión 7.4.x

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).