Fehlerbehebung für Proxy auf Cisco Secure Firewall Management Center (FMC)

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration eines Proxys auf dem FMC beschrieben, damit Benutzer sich über einen zwischengeschalteten Server mit dem Internet verbinden können. Dadurch wird die Sicherheit erhöht und in manchen Fällen die Leistung verbessert. Dieser Artikel führt Sie durch die Schritte zum Konfigurieren eines Proxys auf dem FMC und enthält Tipps zur Fehlerbehebung für häufige Probleme.

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Secure Firewall Management Center (FMC)
- Proxy

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- FMC 7.4.x

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfiguration

Netzwerk-HTTP-Proxy auf der FMC-GUI konfigurieren:

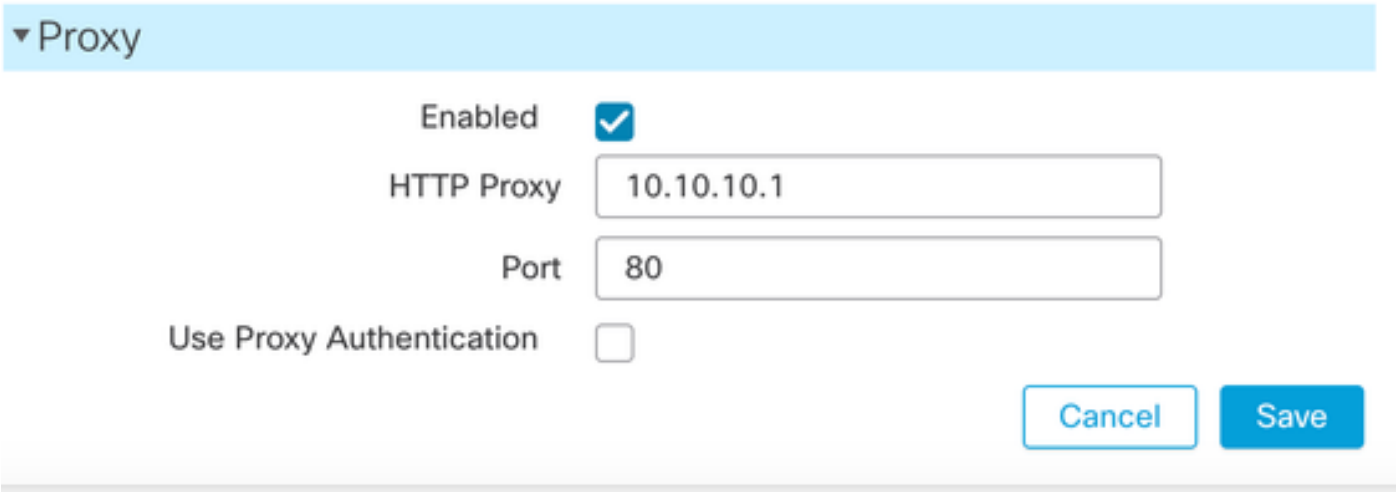
Login FMC GUI > Choose System > Configuration (Anmeldung über FMC-GUI > System > Konfiguration auswählen) und wählen Sie Management Interfaces (Verwaltungsschnittstellen) aus.

Anmerkung: Proxys mit NT LAN Manager (NTLM)-Authentifizierung werden nicht unterstützt. Wenn Sie Smart Licensing verwenden, darf der FQDN des Proxys nicht mehr als 64 Zeichen enthalten.

Konfigurieren Sie im Bereich Proxy die HTTP-Proxyeinstellungen.

Das Management Center ist so konfiguriert, dass es über die Ports TCP/443 (HTTPS) und TCP/80 (HTTP) eine direkte Verbindung mit dem Internet herstellt. Sie können einen Proxyserver verwenden, bei dem Sie sich über HTTP Digest authentifizieren können.

- Aktivieren Sie das Kontrollkästchen Aktiviert.
- Geben Sie im Feld HTTP Proxy (HTTP-Proxy) die IP-Adresse oder den vollqualifizierten Domänennamen des Proxyservers ein.
- Geben Sie im Portfeld eine Portnummer ein.
- Geben Sie Anmeldeinformationen für die Authentifizierung ein, indem SieProxy-Authentifizierung verwenden und dann einen Benutzernamen und ein Kennwort angeben.
- Klicken Sie auf Speichern.



Hinweis: Als Proxy-Passwort können Sie A-Z, a-z und 0-9 sowie Sonderzeichen verwenden.

Fehlerbehebung

Rufen Sie die FMC-CLI und den Expertenmodus auf, und überprüfen Sie dann iprep_proxy.conf, um sicherzustellen, dass die Proxyeinstellungen korrekt sind:

<#root>

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

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

Überprüfen Sie die aktiven Verbindungen, um die aktive Proxy-Verbindung zu überprüfen:

<#root>

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

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

Überprüfen Sie mit dem Befehl curl sowohl die Anforderungsdetails als auch die Antwort vom Proxy. Wenn Sie die Antwort HTTP/1.1 200 Connection established erhalten, bedeutet dies, dass das FMC erfolgreich Datenverkehr über den Proxy sendet und empfängt.

<#root>

admin@fmc:~$

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

HTTP/1.1 200 Connection established

Wenn Sie den Benutzernamen und das Kennwort für den Proxy konfiguriert haben, überprüfen Sie die Authentifizierung und die Proxy-Antwort:

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

Verifizierung

Erfolgreiche Herstellung der Verbindung über Proxy

Wenn Sie einen curl-Befehl mit einem Proxy wie curl -x http://proxy:80 -I https://tools.cisco.com ausführen, treten eine Reihe erwarteter Netzwerkinteraktionen auf, die über die Paketerfassung (tcpdump) beobachtet werden können. Dies ist ein grober Überblick über den Prozess, angereichert mit echten tcpdump-Ergebnissen:

TCP-Handshake-Initiierung:
Der Client (FMC) initiiert eine TCP-Verbindung zum Proxyserver an Port 80, indem er ein SYN-Paket sendet. Der Proxy antwortet mit SYN-ACK, und der Client schließt den Handshake mit ACK ab. Hierdurch wird die TCP-Sitzung eingerichtet, über die die HTTP-Kommunikation stattfindet.

Beispiel für tcpdump-Ausgabe:

```
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
```

HTTP CONNECT-Anforderung:
Sobald die TCP-Verbindung hergestellt ist, sendet der Client eine HTTP CONNECT-Anforderung

an den Proxy und weist diesen an, einen Tunnel zum Ziel-HTTPS-Server (tools.cisco.com:443) zu erstellen. Diese Anforderung ermöglicht es dem Client, eine End-to-End-TLS-Sitzung über den Proxy auszuhandeln.

Beispiel für tcpdump (decodiertes HTTP):

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

Bestätigung des Verbindungsaufbaus:
Der Proxy antwortet mit einer Antwort vom Typ "HTTP/1.1 200-Verbindung hergestellt", die angibt, dass der Tunnel zum Zielserver erfolgreich erstellt wurde. Das bedeutet, dass der Proxy jetzt als Relay fungiert und verschlüsselten Datenverkehr zwischen dem Client und tools.cisco.com weiterleitet.

Beispiel für tcpdump:

<#root>

```
HTTP/1.1
```

200

```
 Connection established
```

HTTPS-Kommunikation über Tunnel:
Nach der erfolgreichen CONNECT-Antwort initiiert der Client den SSL/TLS-Handshake über den eingerichteten Tunnel direkt mit tools.cisco.com. Da dieser Datenverkehr verschlüsselt ist, ist der Inhalt im tcpdump nicht sichtbar, es können jedoch Paketlängen und -zeitpunkte beobachtet werden, einschließlich TLS-Client-Hello- und Server-Hello-Pakete.

Beispiel für 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)
```

Verarbeitung der HTTP-Umleitung (302 gefunden):
Im Rahmen der HTTPS-Kommunikation fordert der Client die Ressource von tools.cisco.com an.

Der Server antwortet mit einer HTTP/1.1 302 Found-Umleitung zu einer anderen URL (https://tools.cisco.com/healthcheck), die der Client abhängig von den Curl-Parametern und dem Zweck der Anfrage verfolgen kann. Obwohl diese Umleitung innerhalb der verschlüsselten TLS-Sitzung erfolgt und nicht direkt sichtbar ist, wird ein Verhalten erwartet, das beobachtet werden kann, wenn TLS-Datenverkehr entschlüsselt wird.

Der verschlüsselte Umleitungsverkehr sieht wie folgt aus:

```
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)
```

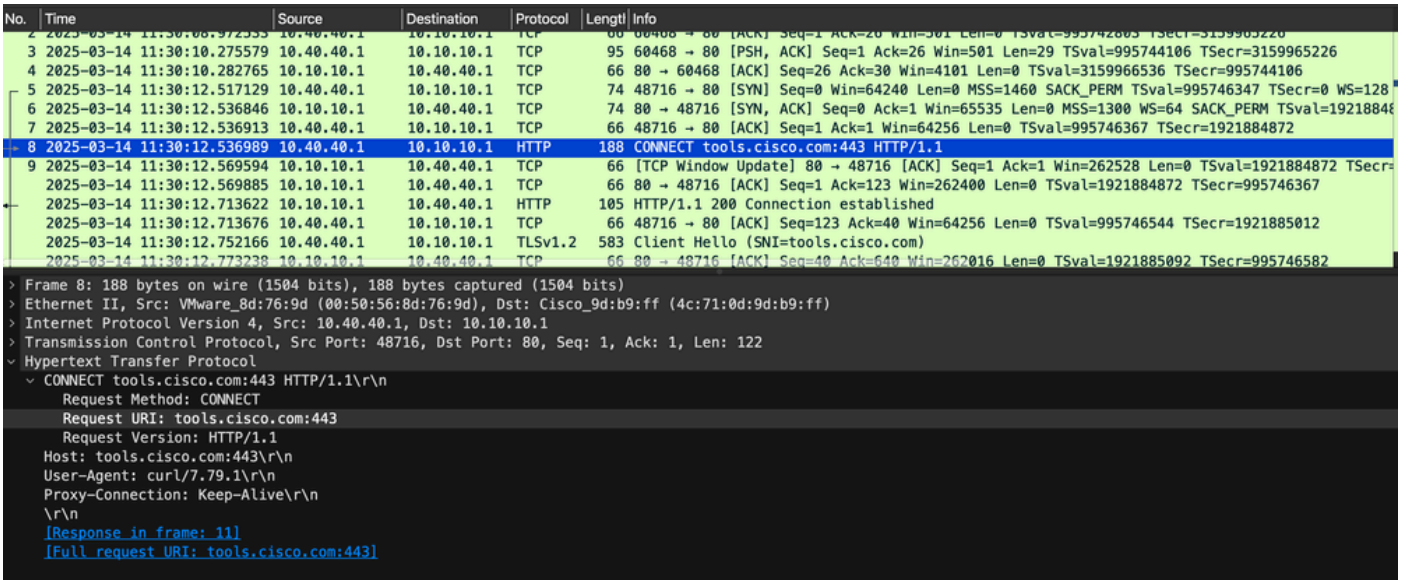
Verbindungsabbruch:
Sobald der Austausch abgeschlossen ist, schließen sowohl der Client als auch der Proxy die TCP-Verbindung ordnungsgemäß, indem sie FIN- und ACK-Pakete austauschen und so eine ordnungsgemäße Sitzungsbeendigung sicherstellen.

Beispiel für tcpdump-Ausgabe:

```
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
```

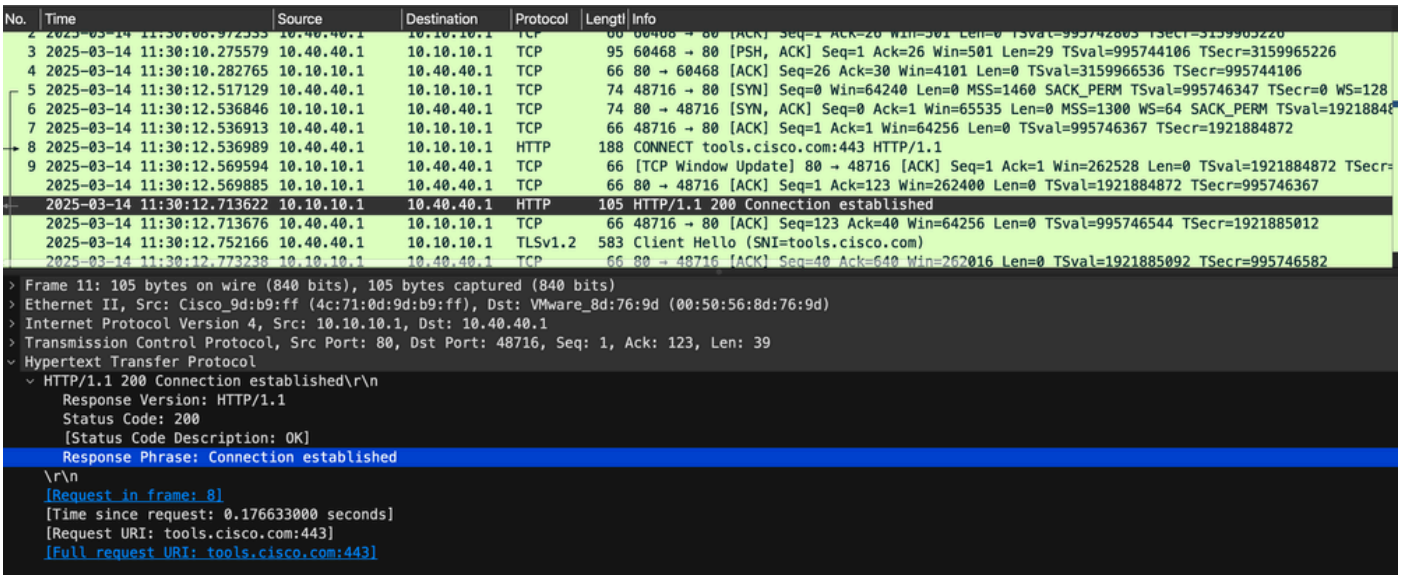
Tipp: Durch Analyse der tcpdump-Ausgabe können Sie überprüfen, ob die HTTPS-Anforderung über den expliziten Proxy dem erwarteten Fluss folgt: TCP-Handshake, CONNECT-Anfrage, Tunnelaufbau, TLS-Handshake, verschlüsselte Kommunikation (einschließlich möglicher Umleitungen) und ordnungsgemäßes Schließen der Verbindung. Dies bestätigt, dass der Proxy und die Client-Interaktion wie vorgesehen funktionieren, und hilft bei der Identifizierung von Problemen im Datenfluss, wie z. B. bei Tunneling oder SSL-Aushandlung.

Das FMC (10.40.40.1) richtet einen erfolgreichen TCP-Handshake mit dem Proxy (10.10.10.1) an Port 80 ein, gefolgt von einer HTTP CONNECT an den Server (72.163.4.161) an Port 443. Der Server antwortet mit einem HTTP 20 0 Nachricht Verbindung hergestellt. Der TLS-Handshake wird beendet, und die Daten werden ordnungsgemäß übertragen. Schließlich wird die TCP-Verbindung ordnungsgemäß beendet (FIN).



```
No.  Time                    Source        Destination   Protocol  Lengtl 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  Lengtl 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]
```

Bekannte Probleme

Proxy-ACL-Einschränkungen

Wenn ein Berechtigungsproblem vorliegt (wie bei einer Zugriffsliste auf dem Proxy), können Sie dies durch Paketerfassung (tcpdump) beobachten. Dies ist eine allgemeine Erklärung des Fehlerszenarios mit Beispielen für tcpdump-Ausgaben:

TCP-Handshake-Initiierung:
Der Client (FirePOWER) startet mit dem Aufbau einer TCP-Verbindung zum Proxy an Port 80. Der TCP-Handshake (SYN, SYN-ACK, ACK) wird erfolgreich abgeschlossen, d.h. der Proxy ist erreichbar.

Beispiel für tcpdump-Ausgabe:

```
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
```

HTTP CONNECT-Anforderung:
Sobald die Verbindung hergestellt ist, sendet der Client eine HTTP CONNECT-Anfrage an den Proxy und fordert diesen auf, einen Tunnel zu tools.cisco.com:443 zu erstellen.

Beispiel für tcpdump (decodiertes HTTP):

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

Fehlerantwort vom Proxy:

Anstatt den Tunnel zu erlauben, verweigert der Proxy die Anforderung, wahrscheinlich aufgrund einer Zugriffsliste (ACL), die diesen Verkehr nicht zulässt. Der Proxy antwortet mit einem Fehler wie 403 Forbidden oder 502 Bad Gateway.

Beispiel einer tcpdump-Ausgabe mit einem Fehler:

<#root>

```
HTTP/1.1
```

403

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

Verbindungsabbruch:
Nach dem Senden der Fehlermeldung schließt der Proxy die Verbindung und tauscht FIN-/ACK-Pakete auf beiden Seiten aus.

Beispiel für tcpdump-Ausgabe:

```
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
```

Tipp: Aus dem tcpdump können Sie sehen, dass der Proxy die Tunneleinrichtung verweigert hat, obwohl die TCP-Verbindung und die HTTP CONNECT-Anforderung erfolgreich waren. Dies weist in der Regel darauf hin, dass der Proxy über eine ACL oder eine Berechtigungsbeschränkung verfügt, die den Datenverkehr am Weiterleiten hindert.

Download des Proxys fehlgeschlagen (Timeout/unvollständige Übertragung)

In diesem Szenario stellt FMC erfolgreich eine Verbindung mit dem Proxy her und startet den Dateidownload, aber die Übertragung läuft zeitlich ab oder kann nicht abgeschlossen werden. Dies liegt in der Regel an der Proxy-Überprüfung, Zeitüberschreitungen oder Größenbeschränkungen für die Datei auf dem Proxy.

TCP-Handshake-Initiierung
FMC initiiert eine TCP-Verbindung zum Proxy an Port 80, und der Handshake wird erfolgreich abgeschlossen.
Beispiel für tcpdump-Ausgabe:

```
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
```

HTTP CONNECT-Anforderung
FMC sendet eine HTTP CONNECT-Anforderung an den Proxy, um das externe Ziel zu erreichen.
Beispiel für tcpdump (decodiertes HTTP):

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

Tunnelaufbau und TLS-Handshake
Der Proxy antwortet mit eingerichteter HTTP/1.1/200-Verbindung, sodass der TLS-Handshake beginnen kann.

Beispiel für tcpdump-Ausgabe:

<#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)
```

Timeout oder unvollständiger Download
Nachdem die Dateiübertragung gestartet wurde, wird der Download beendet oder nicht abgeschlossen, was zu einer Zeitüberschreitung führt. Die Verbindung bleibt inaktiv.
Mögliche Gründe:

- Verzögerungen bei der Proxyüberprüfung oder Filterung.
- Proxy-Timeouts für lange Übertragungen.
- Vom Proxy auferlegte Dateigrößenbeschränkungen.

Beispiel für TCP-Dump mit Inaktivität:

<#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.
```

Tipp: FMC initiiert den Download, schließt jedoch aufgrund von Zeitüberschreitungen oder unvollständigen Übertragungen nicht ab, die häufig durch Proxy-Filterung oder Größenbeschränkungen verursacht werden.

Download der Proxy-Datei schlägt fehl (MTU-Problem)

In diesem Fall stellt FMC eine Verbindung zum Proxy her und beginnt mit dem Herunterladen von Dateien. Die Sitzung schlägt jedoch aufgrund von MTU-Problemen fehl. Diese Probleme verursachen eine Paketfragmentierung oder verlorene Pakete, insbesondere bei großen Dateien oder SSL/TLS-Handshakes.

TCP-Handshake-Initiierung
FMC initiiert einen TCP-Handshake mit dem Proxy, der erfolgreich ist.

Beispiel für tcpdump-Ausgabe:

```
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
```

HTTP CONNECT-Anforderung und Tunnelaufbau
FMC sendet eine HTTP CONNECT-Anfrage, und der Proxy antwortet, sodass der Tunnel eingerichtet werden kann.
Beispiel für tcpdump (decodiertes HTTP):

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

TLS-Handshake beginnt
FMC und tools.cisco.com handeln SSL/TLS aus, und die ersten Pakete werden ausgetauscht.
Beispiel für tcpdump-Ausgabe:

<#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)
```

Paketfragmentierung oder Paketverlust aufgrund von MTU
Wenn FMC oder der Server versucht, große Pakete zu senden, verursachen MTU-Probleme eine Paketfragmentierung oder Paketverluste, was zu Fehlern bei der Dateiübertragung oder TLS-Aushandlung führt.
Dies tritt in der Regel dann auf, wenn die MTU zwischen FMC und Proxy (oder zwischen Proxy und Internet) falsch eingestellt oder zu gering ist.
Beispiel für tcpdump mit einem Fragmentierungsversuch:

<#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
```

Tipp: Das MTU-Problem führt zu verworfenen oder fragmentierten Paketen, die den TLS-Handshake unterbrechen oder dazu führen, dass das Herunterladen von Dateien fehlschlägt. Dies tritt häufig auf, wenn eine SSL-Überprüfung oder Paketfragmentierung aufgrund falscher MTU-Einstellungen erfolgt.

Bei einem Fehlerszenario erhält FMC CONNECT ohne HTTP 200, wobei Neuübertragungen und FINs keinen TLS-/Datenaustausch bestätigen, möglicherweise aufgrund von MTU-Problemen oder eines Proxy-/Upstream-Problems.

Wenn Sie curl verwenden, können verschiedene HTTP-Antwortcodes auftreten, die serverseitige Probleme oder Authentifizierungsfehler anzeigen. Dies ist eine Liste der häufigsten Fehlercodes und ihrer Bedeutung:

HTTP-Code	Bedeutung	Ursache
400	Ungültige Anforderung	Falsche Anforderungssyntax
401	Nicht autorisiert	Fehlende oder falsche Anmeldeinformationen
403	Verboten	Zugriff verweigert
404	Nicht gefunden	Ressource nicht gefunden
500	Internal error	Serverfehler
502	Ungültiges Gateway	Serverfehlkommunikation
503	Dienst nicht verfügbar	Server-Überlastung oder -Wartung
504	Gateway-Zeitüberschreitung	Timeout zwischen Servern

Referenzen

Cisco Secure Firewall Threat Defense - Versionshinweise, Version 7.4.x

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.