Proxy-oplossing op Cisco Secure Firewall Management Center (FMC)

Inhoud

Inleiding

In dit document wordt beschreven hoe een proxy op FMC moet worden geconfigureerd zodat gebruikers via een intermediaire server verbinding met internet kunnen maken, waardoor de beveiliging wordt verbeterd en de prestaties soms worden verbeterd. Dit artikel begeleidt u door de stappen om een proxy op FMC te configureren en tips te geven voor probleemoplossing bij veelvoorkomende problemen.

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Secure Firewall Management Center (FMC)
- Proxy

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- VCC 7.4.x

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configuratie

Netwerk http-proxy configureren op FMC GUI:

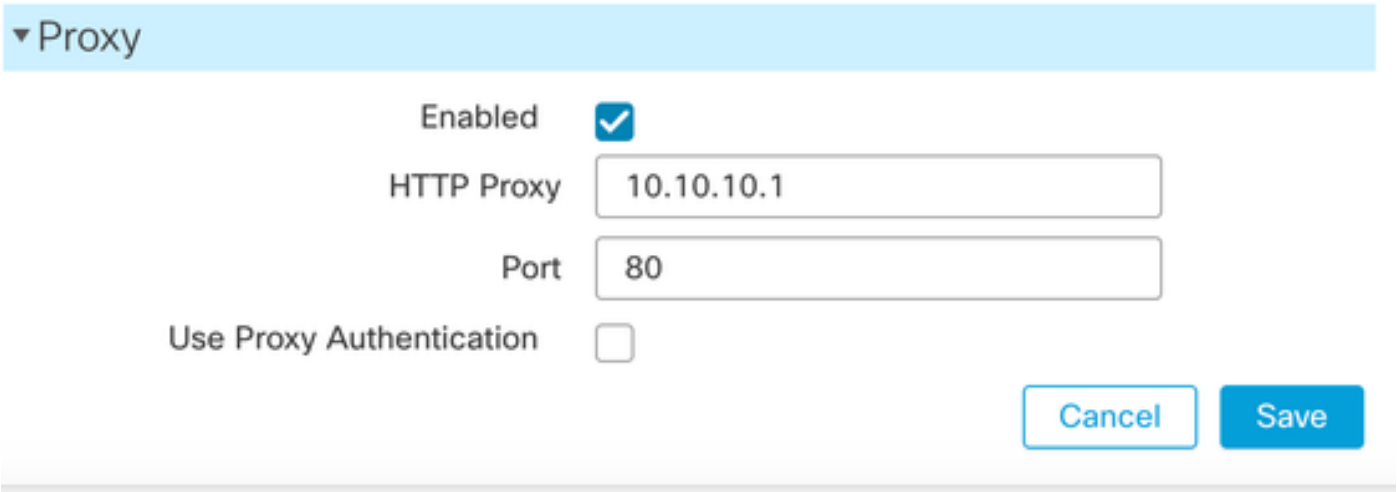
Login FMC GUI > Kies systeem > configuratie, en kies vervolgens Beheerinterfaces.

Opmerking: Proxy's die NAT LAN Manager (NTLM)-verificatie gebruiken, worden niet ondersteund. Als u Smart Licensing gebruikt, kan de proxy-FQDN niet meer dan 64 tekens bevatten.

In het gebied Proxy configureer HTTP-proxyinstellingen.

Het beheercentrum is ingesteld om rechtstreeks verbinding te maken met internet via de poorten TCP/443 (HTTPS) en TCP/80 (HTTP). U zou een proxyserver kunnen gebruiken, waarop u via HTTP Digest zou kunnen authenticeren.

- Schakel het selectievakje Inschakelen in.
- Voer in het HTTP-veld het IP-adres of de volledig gekwalificeerde domeinnaam van uw proxyserver in.
- Geef in het Portfield een poortnummer op.
- Voer verificatiereferenties in door te kiezenProxy-verificatie gebruiken en geef vervolgens een gebruikersnaam en wachtwoord op.
- Klik op Save (Opslaan).



Opmerking: Voor het proxy wachtwoord kunt u A-Z, a-z, en 0-9 en speciale tekens gebruiken.

Problemen oplossen

Krijg toegang tot FMC CLI en expert-modus, en controleer vervolgens iprep_proxy.conf om er zeker van te zijn dat de proxy-instellingen correct zijn:

```
<#root>

admin@fmc:~$

cat /etc/sf/iprep_proxy.conf


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

Controleer de actieve verbindingen om de actieve proxyverbinding te verifiëren:

```
<#root>

admin@fmc:~$

netstat -na | grep 10.10.10.1


tcp 0 0 10.40.40.1:40220 10.10.10.1:80

ESTABLISHED
```

Met de curl opdracht verifieert u zowel de aanvraagdetails als de reactie van de proxy. Als u het antwoord ontvangt: HTTP/1.1 200 Connection ingesteld, geeft dit aan dat het VCC met succes verkeer verstuurt en ontvangt via de proxy.

<#root>

admin@fmc:~$

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

HTTP/1.1 200 Connection established

Als u de gebruikersnaam en het wachtwoord voor de proxy hebt ingesteld, verifieert u de verificatie en de proxyrespons:

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

Verificatie

Succesvolle verbinding via proxy

Wanneer een curl-opdracht met een proxy wordt uitgevoerd, zoals curl -x http://proxy:80 - I https://tools.cisco.com, vindt er een reeks verwachte netwerkinteracties plaats, die via packet capture (tcpdump) kan worden geobserveerd. Dit is een overzicht op hoog niveau van het proces, verrijkt met echte tcpdump output:

Initiatie TCP-handdruk:
De client (FMC) initieert een TCP-verbinding naar de proxyserver op poort 80 door een SYN-pakket te verzenden. De proxy reageert met een SYN-ACK, en de client voltooit de handdruk met een ACK. Hiermee wordt de TCP-sessie ingesteld waarover HTTP-communicatie verloopt.

Voorbeeld cpdump-uitvoer:

```
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-aanvraag:
Zodra de TCP-verbinding tot stand is gebracht, stuurt de client een HTTP CONNECT-verzoek

naar de proxy met de instructie een tunnel te maken naar de doel-HTTPS-server (tools.cisco.com:443). Met dit verzoek kan de client via de proxy onderhandelen over een end-to-end TLS-sessie.

Voorbeeld cpdump (gedecodeerd HTTP):

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

Erkenning van verbindingsinrichting:
De proxy antwoordt met een HTTP/1.1 200 Connection vastgestelde reactie, erop wijzend dat de tunnel naar de doelserver met succes is gecreëerd. Dit betekent dat de proxy nu fungeert als een relay, het doorsturen van versleuteld verkeer tussen de client en tools.cisco.com.

Voorbeeld tcpdump:

<#root>

```
HTTP/1.1
```

200

```
 Connection established
```

HTTPS-communicatie via tunnels:
Na de succesvolle CONNECT-respons start de client de SSL/TLS-handshake direct met tools.cisco.com via de ingestelde tunnel. Aangezien dit verkeer versleuteld is, is de inhoud niet zichtbaar in de tcpdump, maar pakketlengtes en -tijden zijn waarneembaar, waaronder TLS-client-Hello en -server-Hello-pakketten.

Voorbeeld 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)
```

Behandeling van HTTP Redirect (302 gevonden):
Als onderdeel van de HTTPS-communicatie vraagt de client de bron via tools.cisco.com. De server reageert met een HTTP/1.1 302 Found omleiden naar een andere URL

(https://tools.cisco.com/healthcheck), die de client kan volgen, afhankelijk van de curl parameters en het doel van het verzoek. Hoewel deze omleiding binnen de versleutelde TLS-sessie plaatsvindt en niet direct zichtbaar is, is het verwacht gedrag en kan worden waargenomen als TLS-verkeer wordt ontsleuteld.

Het versleutelde omleidingsverkeer ziet er zo uit:

```
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)
```

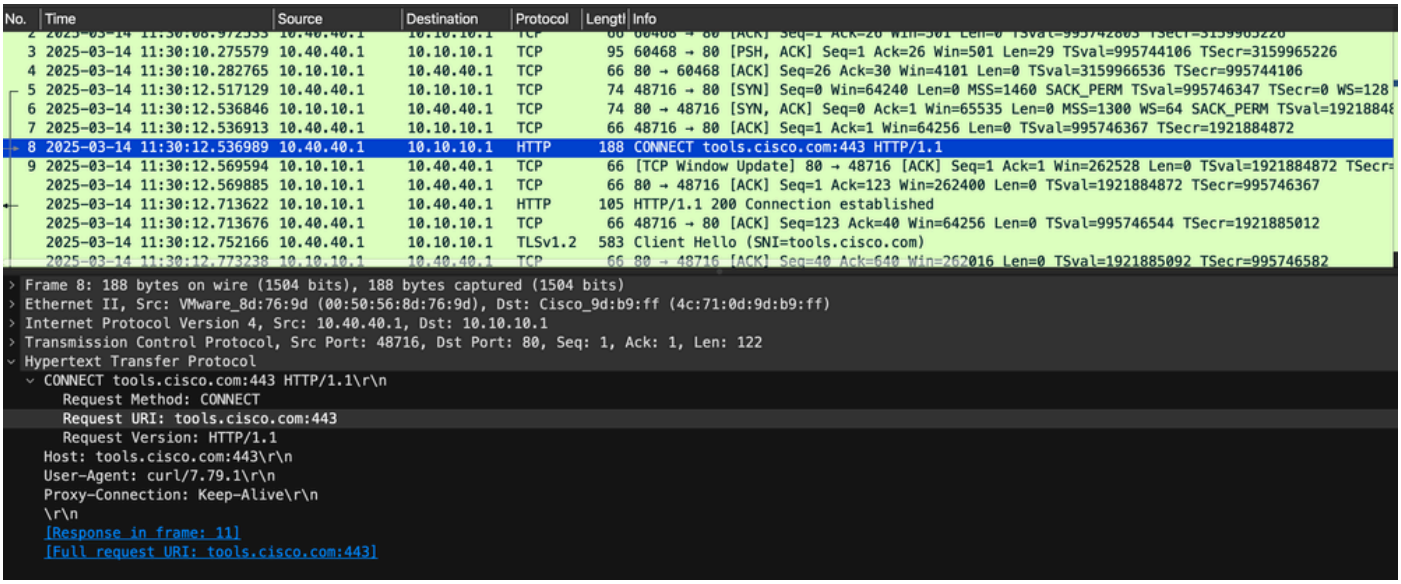
Uitval verbinding:
Zodra de uitwisseling is voltooid, sluiten zowel client als proxy de TCP-verbinding op elegante wijze door FIN- en ACK-pakketten uit te wisselen, waarbij een goede sessiebeëindiging wordt gegarandeerd.

Voorbeeld cpdump-uitvoer:

```
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
```

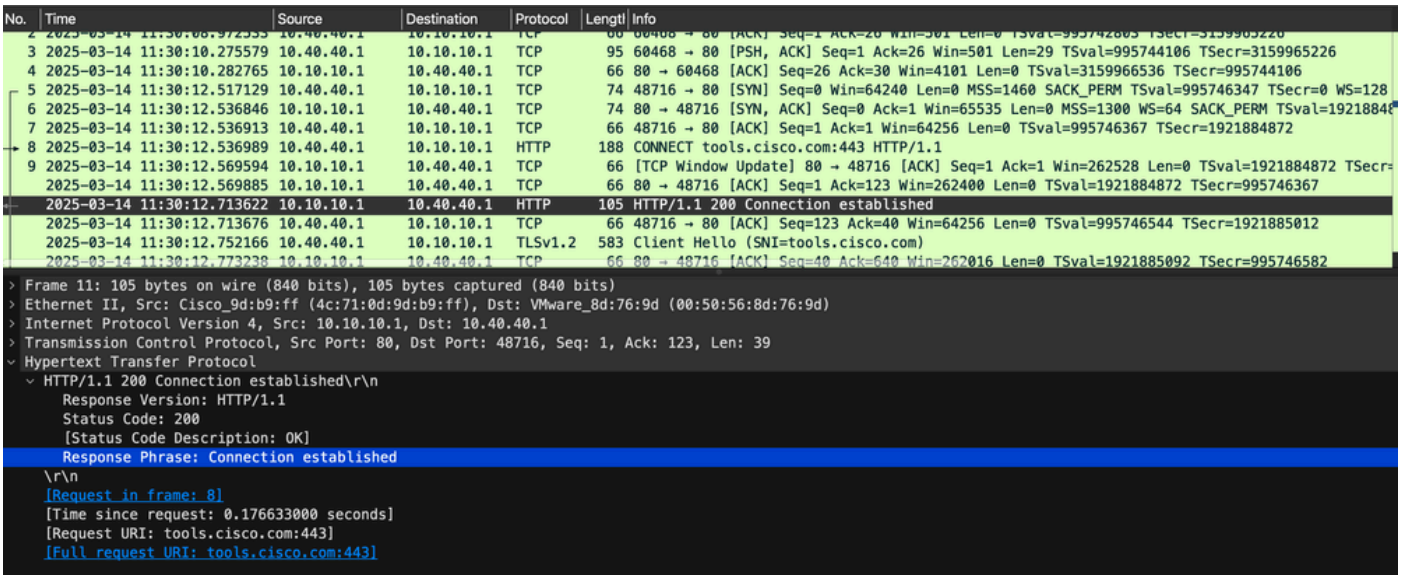
Tip: Door de tcpdump-uitvoer te analyseren, kunt u verifiëren dat het HTTPS-verzoek via de expliciete proxy de verwachte stroom volgt: TCP-handdruk, CONNECT-verzoek, tunnelinstelling, TLS-handdruk, versleutelde communicatie (inclusief mogelijke omleidingen) en graceful connection close. Dit bevestigt dat de proxy en client interactie werkt zoals ontworpen en helpt bij het identificeren van problemen in de stroom, zoals fouten in tunneling of SSL onderhandeling.

Het FMC (10.40.40.1) vormt een succesvolle TCP-handdruk met de proxy (10.10.10.1) op poort 80, gevolgd door een HTTP CONNECT met de server (72.163.4.161) op poort 443. De server reageert met een HTTP 200 Connection-bericht. De TLS-handdruk is voltooid en de gegevensstromen zijn correct. Tot slot eindigt de TCP-verbinding netjes (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]
```

Bekende problemen

Beperkingen van proxy-ACL

Als er een toestemmingskwestie is (zoals een toegangslijst op de proxy), kunt u dat waarnemen via packet capture (tcpdump). Dit is een verklaring op hoog niveau van het mislukkingsscenario, samen met voorbeeldoutput tcpdump:

Initiatie TCP-handdruk:
De client (Firepower) begint met het opzetten van een TCP verbinding met de proxy op poort 80. De TCP handshake (SYN, SYN-ACK, ACK) voltooit met succes, wat betekent dat de proxy bereikbaar is.

Voorbeeld cpdump-uitvoer:

```
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-aanvraag:
Na verbinding stuurt de client een HTTP CONNECT-aanvraag naar de proxy, met het verzoek een tunnel te maken naar tools.cisco.com:443.

Voorbeeld cpdump (gedecodeerd HTTP):

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

Fout Reactie van proxy:

In plaats van de tunnel toe te staan, ontkent de volmacht het verzoek, waarschijnlijk wegens een toegangslijst (ACL) die dit verkeer niet toestaat. De proxy reageert met een fout zoals 403 Verboden of 502 Bad Gateway.

Voorbeeld output cpdump die fout toont:

<#root>

```
HTTP/1.1
```

403

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

Uitval verbinding:
Na het verzenden van de foutmelding sluit de proxy de verbinding en wisselen beide kanten FIN/ACK-pakketten uit.

Voorbeeld cpdump-uitvoer:

```
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: Van tcpdump, kunt u zien dat hoewel de TCP verbinding en HTTP CONNECT verzoek succesvol waren, de proxy ontkende de tunnelopstelling. Dit wijst gewoonlijk erop dat de volmacht een ACL of toestemmingsbeperking heeft die het verkeer verhindert over te gaan.

Proxy faalt download (time-out/onvolledige overdracht)

In dit scenario verbindt FMC met succes met de proxy en start de bestandsdownload, maar de overdrachttijden verlopen of worden niet voltooid. Dit is typisch toe te schrijven aan volmachtsinspectie, onderbrekingen, of de grenzen van de dossiergrootte op de volmacht.

Initiatie van TCP-handdruk
FMC start op poort 80 een TCP-verbinding met de proxy en de handdruk wordt met succes voltooid.
Voorbeeld cpdump-uitvoer:

```
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-aanvraag
FMC stuurt een HTTP CONNECT-verzoek naar de proxy om het externe doel te bereiken.
Voorbeeld cpdump (gedecodeerd HTTP):

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

Tunneloprichting en TLS-handdruk
Proxy reageert met HTTP/1.1 200 Connection ingesteld, waardoor de TLS handshake kan beginnen.

Voorbeeld cpdump-uitvoer:

```
<#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)
```

Time-out of onvolledige download
Na het initiëren van de bestandsoverdracht, de download stallen of niet voltooid, wat leidt tot een timeout. De verbinding blijft leeg.
Mogelijke redenen zijn onder meer:

- Proxy-inspectievertragingen of filtering.
- Proxy timeouts voor lange overdrachten.
- Beperkingen van bestandsgrootte opgelegd door de proxy.

Voorbeeld van tcpdump met inactiviteit:

<#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: FMC initieert de download maar slaagt er niet in te voltooien vanwege onderbrekingen of onvolledige overdrachten, vaak veroorzaakt door proxyfiltering of beperkingen van de bestandsgrootte.

Proxy faalt File Download (MTU-probleem)

In dit geval verbindt FMC zich met de proxy en begint het downloaden van bestanden, maar de sessie mislukt vanwege MTU-problemen. Deze problemen veroorzaken pakketfragmentatie of verloren pakketten, vooral met grote bestanden of SSL/TLS handshakes.

Initiatie van TCP-handdruk
FMC initieert TCP handshake met de proxy, die slaagt.
Voorbeeld cpdump-uitvoer:

```
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-aanvraag en -tunnelinstelling
FMC stuurt een HTTP CONNECT-verzoek en de proxy reageert, waardoor de tunnel kan worden opgezet.
Voorbeeld cpdump (gedecodeerd HTTP):

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

TLS-handdruk start
FMC en tools.cisco.com beginnen te onderhandelen over SSL/TLS en de eerste pakketten worden uitgewisseld.
Voorbeeld cpdump-uitvoer:

<#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)
```

Packet Fragmentation of Drop als gevolg van MTU
Wanneer FMC of de server probeert grote pakketten te verzenden, veroorzaken MTU problemen pakketfragmentatie of pakketdalingen, wat resulteert in bestandsoverdracht of TLS-onderhandeling mislukkingen.
Dit gebeurt meestal wanneer de MTU tussen FMC en de proxy (of tussen de proxy en het internet) onjuist is ingesteld of te klein is.
Voorbeeld van tcpdump die fragmentatiepoging toont:

<#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: MTU-probleem resulteert in gevallen of gefragmenteerde pakketten, die de TLS-handdruk onderbreken of ervoor zorgen dat het downloaden van bestanden mislukt. Dit wordt vaak gezien bij SSL-inspectie of pakketfragmentatie als gevolg van onjuiste MTU-instellingen.

In een faalscenario krijgt FMC CONNECT zonder HTTP 200, waarbij heruitzendingen en FIN's bevestigen dat er geen TLS/data-uitwisseling is, mogelijk door MTU-problemen of een proxy/upstream-probleem.

Wanneer u curl gebruikt, kunt u verschillende HTTP-responscodes tegenkomen die wijzen op serverproblemen of verificatiefouten. Dit is een lijst van de meest voorkomende foutcodes en hun betekenissen:

HTTP-code	Betekenis	Oorzaak
400	Slecht verzoek	Onjuiste aanvraagsyntaxis
401	Onbevoegd	Ontbrekende of onjuiste referenties
403	Verboden	Toegang geweigerd
404	Niet gevonden	Resource niet gevonden
500	Interne fout	Serverfout
502	Slechte gateway	Servermiscommunicatie
503	Service niet beschikbaar	Serveroverbelasting of -onderhoud
504	Time-out gateway	Time-out tussen servers

Referenties

Cisco Secure Firewall Threat Defense release Notes, versie 7.4.x

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.