思科安全防火墙管理中心(FMC)上的代理故障排除

目录

简介

本文档介绍在FMC上配置代理，以允许用户通过中间服务器连接到Internet，从而增强安全性，有时还能提高性能。这篇文章将指导您完成在FMC上配置代理的步骤，并提供常见问题的故障排除提示。

要求

Cisco 建议您了解以下主题：

- 思科安全防火墙管理中心(FMC)
- 代理

使用的组件

本文档中的信息基于以下软件和硬件版本：

- FMC 7.4.x

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

在FMC GUI上配置网络http-proxy:

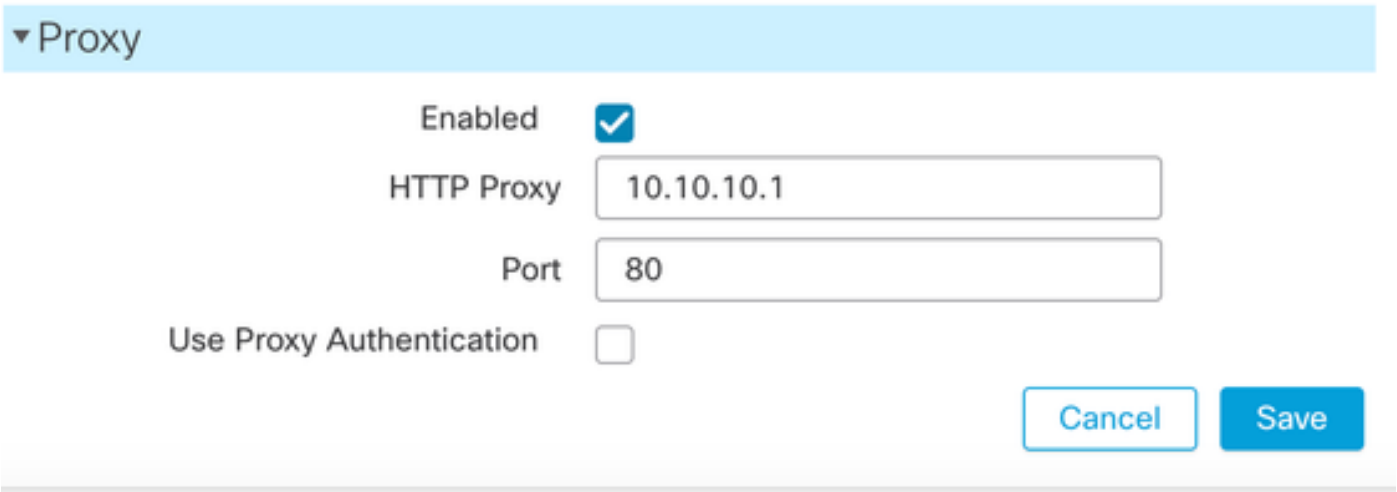
登录FMC GUI > 选择System > Configuration，然后选择Management Interfaces。

注意：不支持使用NT LAN Manager(NTLM)身份验证的代理。如果使用智能许可，代理FQDN不能超过64个字符。

在Proxy区域中，配置HTTP代理设置。

管理中心配置为通过端口TCP/443(HTTPS)和TCP/80(HTTP)直接连接到Internet。 您可以使用代理服务器，您可以通过HTTP摘要对代理服务器进行身份验证。

- 选中Enabled复选框。
- 在HTTP代理字段中，输入代理服务器的IP地址或完全限定域名。
- 在端口字段中，输入端口号。
- 选择Use Proxy Authentication，然后提供User Name和Password，从而提供身份验证凭证。
- Click Save.



注意：对于代理密码，可以使用A-Z、a-z和0-9以及特殊字符。

故障排除

访问FMC CLI和专家模式，然后验证iprep_proxy.conf以确保代理设置正确：

<#root>

admin@fmc:~$

cat /etc/sf/iprep_proxy.conf

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

检查活动连接以验证活动代理连接：

<#root>

admin@fmc:~$

netstat -na | grep 10.10.10.1

tcp 0 0 10.40.40.1:40220 10.10.10.1:80

ESTABLISHED

使用curl命令验证请求详细信息和来自代理的响应。如果收到响应：HTTP/1.1 200 Connection established，则表示FMC通过代理成功发送和接收流量。

<#root>

admin@fmc:~$

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

HTTP/1.1 200 Connection established

如果已配置代理的用户名和密码，请验证身份验证和代理响应：

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

确认

通过代理成功建立连接

当使用代理(例如curl -x http://proxy:80 -I https://tools.cisco.com)运行curl命令时，将会出现一系列预期的网络交互，可通过数据包捕获(tcpdump)观察这些网络交互。 这是该过程的高级概述，并提供了实际tcpdump输出：

TCP握手启动：
客户端(FMC)通过发送SYN数据包启动到端口80上代理服务器的TCP连接。代理用SYN-ACK响应，客户端用ACK完成握手。这将建立HTTP通信所经过的TCP会话。

tcpdump输出示例：

```
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请求：
建立TCP连接后，客户端向代理发送HTTP CONNECT请求，指示其创建通往目标HTTPS服务器(tools.cisco.com:443)的隧道。 此请求允许客户端通过代理协商端到端TLS会话。

示例tcpdump（解码的HTTP）：

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

连接建立确认：
代理以HTTP/1.1 200 Connection established响应进行回复，表示已成功创建到目标服务器的隧道。这意味着代理现在充当中继，在客户端和tools.cisco.com之间转发加密流量。

示例tcpdump:

<#root>

```
HTTP/1.1
```

200

```
 Connection established
```

通过隧道的HTTPS通信：
成功执行CONNECT响应后，客户端通过已建立的隧道直接与tools.cisco.com发起SSL/TLS握手。由于此流量是加密的，因此内容在tcpdump中不可见，但数据包长度和计时是可观察的，包括TLS客户端Hello数据包和服务器Hello数据包。

示例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)
```

HTTP重定向处理（找到302个）：
作为HTTPS通信的一部分，客户端从tools.cisco.com请求资源。服务器以HTTP/1.1 302 Found重定向到另一个URL(https://tools.cisco.com/healthcheck)进行响应，客户端可以根据卷曲参数和请求的用途进行响应。虽然此重定向在加密TLS会话中发生并且不直接可见，但它是预期行为，并且如果解密了TLS流量，则可以观察到此重定向。

加密的重定向流量将如下所示：

```
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)
```

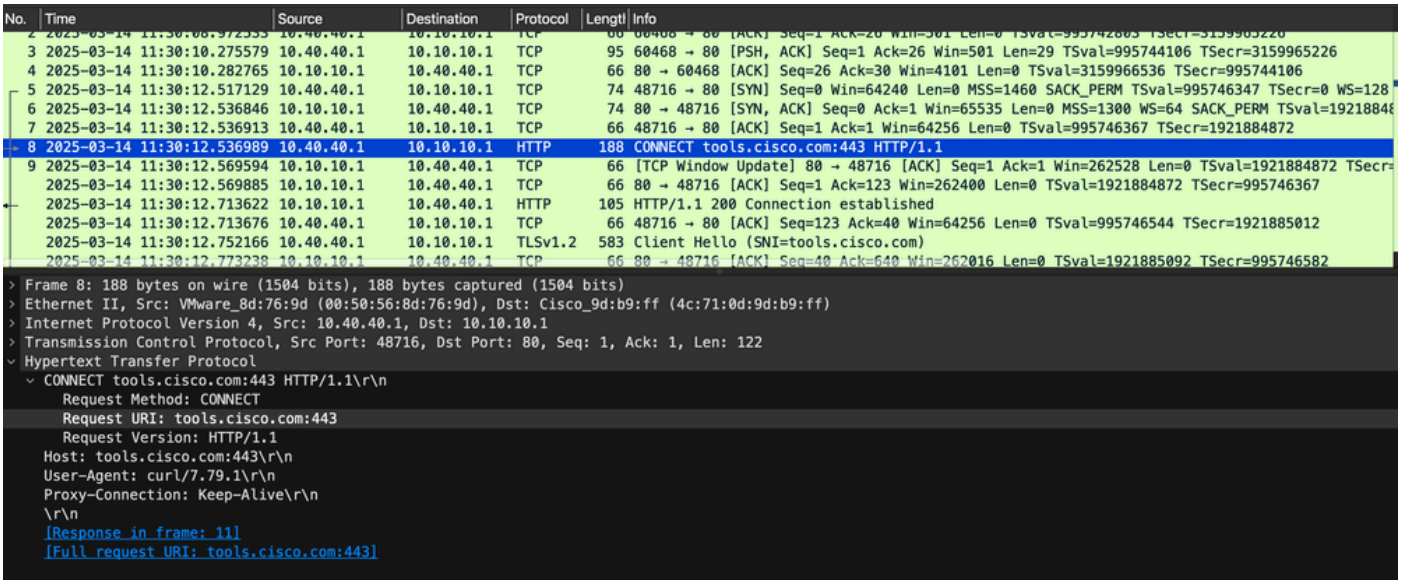
连接断开：
交换完成后，客户端和代理通过交换FIN和ACK数据包来正常关闭TCP连接，从而确保正确的会话终止。

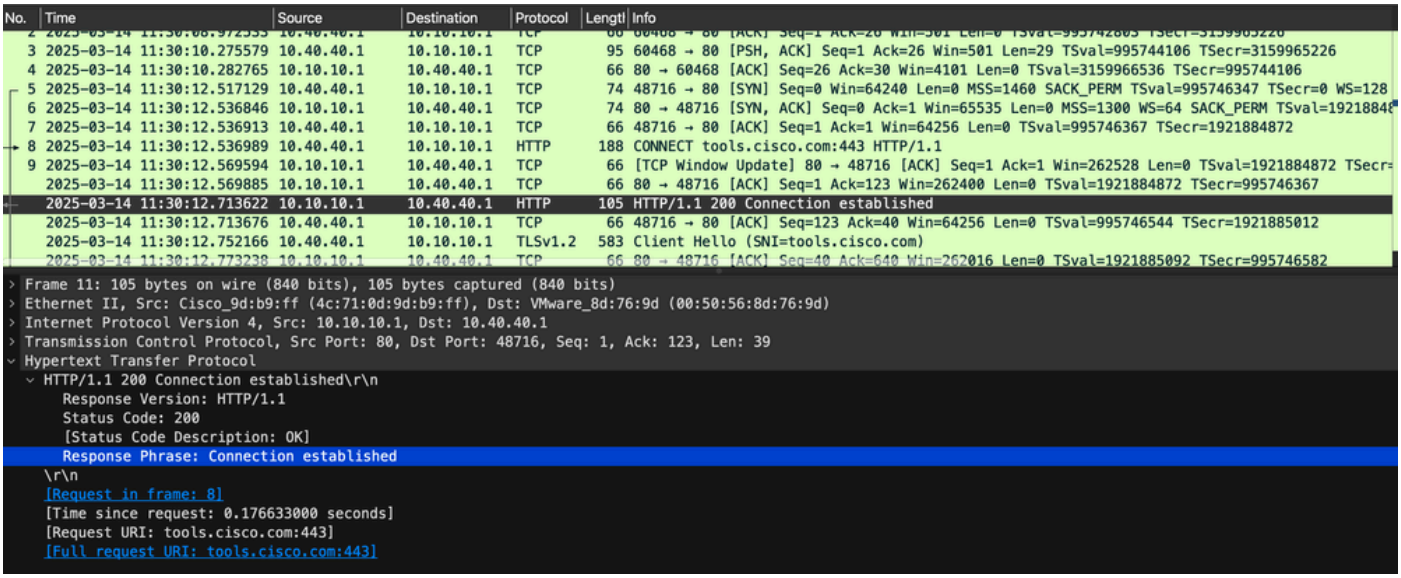
tcpdump输出示例：

```
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
```

提示：通过分析tcpdump输出，您可以验证通过显式代理的HTTPS请求是否遵循预期流：TCP握手、CONNECT请求、隧道建立、TLS握手、加密通信（包括可能的重定向）和流畅的连接关闭。这可以确认代理和客户端交互是否按设计运行，并帮助识别流中的任何问题，例如隧道或SSL协商失败。

FMC(10.40.40.1)在端口80上与代理(10.10.10.1)成功建立TCP握手，随后在端口443上建立到服务器(72.163.4.161)的HTTP连接。服务器回复HTTP 200 Connection established消息。TLS握手完成，数据正确流动。最后，TCP连接正常终止(FIN)。





已知问题

代理ACL限制

如果存在权限问题（例如代理上的访问列表），可以通过数据包捕获(tcpdump)进行观察。 以下是有关故障场景的简要说明，以及tcpdump输出示例：

TCP握手启动：
客户端(Firepower)首先在端口80上建立与代理的TCP连接。TCP握手(SYN、SYN-ACK、ACK)成功

完成，这意味着代理可访问。

tcpdump输出示例：

```
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请求：
连接后，客户端向代理发送HTTP CONNECT请求，要求其创建通向tools.cisco.com:443的隧道。

示例tcpdump（解码的HTTP）：

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

来自代理的错误响应：

代理拒绝该请求，而不是允许隧道，原因很可能是访问列表(ACL)不允许此流量。代理响应错误，如403 Forbidden或502 Bad Gateway。

显示错误的tcpdump输出示例：

```
<#root>

HTTP/1.1

403

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

连接断开：
发送错误消息后，代理关闭连接，两端交换FIN/ACK数据包。

tcpdump输出示例：

```
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
```

提示：从tcpdump中可以看到，尽管TCP连接和HTTP CONNECT请求成功，但代理拒绝隧道设置。这通常表示代理具有ACL或权限限制来阻止流量通过。

代理下载失败（超时/传输不完整）

在这种情况下，FMC成功连接到代理并开始下载文件，但传输超时或无法完成。这通常是由于代理检测、超时或代理的文件大小限制。

TCP握手启动
FMC发起到端口80上代理的TCP连接，握手成功完成。
tcpdump输出示例：

```
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请求
FMC向代理发送HTTP CONNECT请求以到达外部目标。
示例tcpdump（解码的HTTP）：

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

隧道建立和TLS握手
代理响应HTTP/1.1 200 Connection established，从而允许TLS握手开始。

tcpdump输出示例：

```
<#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)
```

超时或未完成下载
启动文件传输后，下载停止或不完成，导致超时。连接保持空闲。
可能的原因包括：

- 代理检查延迟或过滤。
- 长传输的代理超时。
- 代理施加的文件大小限制。

显示非活动的tcpdump示例：

<#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.

提示：FMC启动下载，但由于超时或传输不完整（通常由代理过滤或文件大小限制导致）而无法完成。

代理文件下载失败（MTU问题）

在这种情况下，FMC连接到代理并开始下载文件，但会话因MTU问题而失败。这些问题会导致数据包分段或丢弃数据包，尤其是对于大型文件或SSL/TLS握手。

TCP握手启动
FMC发起与代理的TCP握手，成功完成。
tcpdump输出示例：

```
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请求和隧道建立
FMC发送HTTP CONNECT请求，代理响应，允许建立隧道。
示例tcpdump（解码的HTTP）：

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

TLS握手开始
FMC和tools.cisco.com开始协商SSL/TLS，并交换初始数据包。
tcpdump输出示例：

```
<#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)
```

由于MTU导致的数据包分段或丢弃
当FMC或服务器尝试发送大数据包时，MTU问题会导致数据包分段或丢包，从而导致文件传输或TLS协商失败。
当FMC和代理（或代理和互联网）之间的MTU设置不正确或太小时，通常会发生这种情况。
显示分段尝试的tcpdump示例：

```
<#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
```


提示：MTU问题导致数据包丢弃或分段，从而中断TLS握手或导致文件下载失败。当MTU设置不正确导致SSL检查或数据包分段时，通常会出现这种情况。

在故障场景中，FMC获取不带HTTP 200的CONNECT，重新传输和FIN确认没有TLS/数据交换，可能是由于MTU问题或代理/上游问题。

使用curl时，可能会遇到指示服务器端问题或身份验证错误的各种HTTP响应代码。下面列出了最常见的错误代码及其含义：

HTTP代码	含义	原因
400	错误的请求	请求语法不正确
401	未授权	凭据缺失或不正确
403	已禁止	拒绝进入。
404	找不到	找不到资源
500	Internal Error	服务器错误
502	错误的网关	服务器通信错误
503	服务不可用	服务器过载或维护
504	网关超时	服务器之间的超时

参考

[思科安全防火墙威胁防御版本说明，版本7.4.x]

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。