أستكشاف أخطاء الوكيل وإصلاحها على مركز إدارة جدار الحماية الآمن (FMC) من Cisco

المحتويات

المقدمة

يوضح هذا المستند تكوين وكيل على FMC للسماح للمستخدمين بالاتصال بالإنترنت من خلال خادم وسيط، مما يحسن الأمان ويحسن الأداء في بعض الأحيان. ترشدك هذه المقالة خلال خطوات تكوين وكيل على FMC وتوفير تلميحات أستكشاف المشكلات وإصلاحها الخاصة بالمشكلات الشائعة.

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- مركز إدارة جدار الحماية الآمن (FMC) من Cisco
- وكيل

المكونات المستخدمة

تستند المعلومات الواردة في هذه المستند إلى إصدارات البرامج والمكونات المادية التالية:

- FMC 7.4.x

تم إنشاء المعلومات الواردة في هذه المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذه المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

تكوين وكيل شبكة http على واجهة المستخدم الرسومية (GUI) ل FMC:

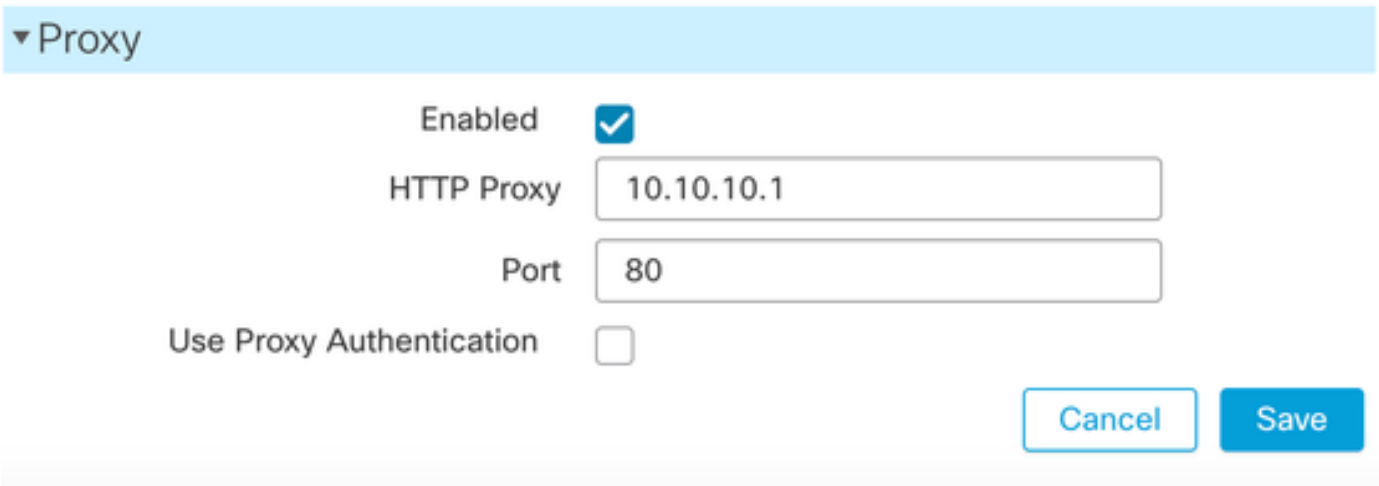
login FMC GUI>يختار نظام>تشكيل، وبعد ذلك يختار إدارة قارن.

ملاحظة: الوكلاء الذين يستخدمون مصادقة مدير شبكة LAN (NTLM) ل NT غير مدعومين. إذا كنت تستخدم "الترخيص الذكي"، فلا يمكن أن يحتوي FQDN للوكيل على أكثر من 64 حرفا.

في منطقة الوكيل، قم بتكوين إعدادات وكيل HTTP.

تم تكوين مركز الإدارة للاتصال مباشرة بالإنترنت على المنافذ TCP/443 (HTTPS) و TCP/80 (HTTP). قد تستخدم خادم وكيل، قد تقوم بالمصادقة عليه عبر ملخص HTTP.

- حدد خانة الاختيار تمكين.
- في HTTP ProxyField، أدخل عنوان IP أو اسم مجال مؤهل بالكامل للخادم الوكيل.
- دخلت في ال portfield، رقم أيسر.
- قم بتوفير بيانات اعتماد المصادقة عن طريق إختيار إستخدام مصادقة الوكيل، ثم قم بتوفير اسم وكلمة مرور مستخدم.
- انقر فوق حفظ.



ملاحظة: لكل مهمة مرور الوكيل يمكنك إستخدام a-z و a-z و 0-9 والحرف الخاصة.

استكشاف الأخطاء وإصلاحها

احصل على الوصول إلى واجهة سطر الأوامر (CLI) من FMC ووضع الخبراء، ثم تحقق من إعدادات الوكيل للتأكد من صحة iprep_proxy.conf:

```
<#root>

admin@fmc:~$

cat /etc/sf/iprep_proxy.conf


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

تحقق من الاتصالات النشطة للتحقق من اتصال الوكيل النشط:

```
<#root>

admin@fmc:~$

netstat -na | grep 10.10.10.1


tcp 0 0 10.40.40.1:40220 10.10.10.1:80

ESTABLISHED
```

باستخدام الأمر curl، تحقق من كل من تفاصيل الطلب والاستجابة من الوكيل. إذا كنت تتلقى الاستجابة: تم إنشاء اتصال HTTP/1.1 200 ، فإن هذا يشير إلى أن FMC قوم بإرسال حركة مرور البيانات واستقبالها بنجاح من خلال الوكيل.

```
<#root>

admin@fmc:~$

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


HTTP/1.1 200 Connection established
```

إذا كنت قد انتهيت من تكوين اسم المستخدم وكلمة المرور للوكيل، فتحقق من المصادقة ورد الوكيل:

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

التحقق

إنشاء اتصال ناجح عبر الوكيل

عند تشغيل أمر curl مع وكيل، مثل curl -x http://proxy:80 -i https://tools.cisco.com، تحدث سلسلة من تفاعلات الشبكة المتوقعة، والتي يمكن مالحظتها من خالل التقاط الحزم (tcpdump). هذه نظرة عامة عالية المستوى على العملية، يتم إثرائها بنواتج تفريغ TCPDUMP الحقيقية:

بدء مصافحة TCP:
يقوم العميل (FMC) بفتح اتصال TCP بالخادم الوكيل على المنفذ 80 عن طريق إرسال حزمة SYN. يستجيب الوكيل باستخدام SYN-ACK، ويقوم العميل بإكمال المصافحة باستخدام ACK. وهذا يؤسس جلسة عمل TCP التي يتم عليها اتصال HTTP.

مثال على إخراج 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
```

طلب اتصال HTTP:
بمجرد إنشاء اتصال TCP، يرسل العميل طلب اتصال HTTP إلى الوكيل، موصيا إياه بإنشاء نفق إلى خادم HTTPS الهدف (tools.cisco.com:443). يسمح هذا الطلب للعميل بالتفاوض على جلسة TLS من نهاية إلى نهاية من خالل الوكيل.

مثال tcpdump (Decoded HTTP):

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

إقرار إنشاء االتصال:

ردود الوكيل مع إستجابة محددة لاتصال HTTP/1.1 200، تشير إلى أنه تم إنشاء النفق إلى الخادم الهدف بنجاح. وهذا يعني أن الوكيل يعمل الآن كترحيل، حيث يقوم بإعادة توجيه حركة مرور البيانات المشفرة بين العميل و tools.cisco.com.

مثال tcpdump:

```
<#root>

HTTP/1.1

200

 Connection established
```

اتصال HTTPS عبر النفق:
بعد إستجابة الاتصال الناجحة، يبدأ العميل مصافحة SSL/TLS مباشرة مع tools.cisco.com عبر النفق الذي تم إنشاؤه. بما أن حركة المرور هذه مشفرة، فإن المحتويات لا تظهر في ذلك الوقت. يمكن ملاحظة أطوال الحزم وتوقيتاتها، بما في ذلك حزم TLS Client Hello و Server Hello.

مثال 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)
```

معالجة إعادة توجيه HTTP (تم العثور على 302):
كجزء من اتصال HTTPS، يطلب العميل المرور من tools.cisco.com. يستجيب الخادم باستخدام HTTP/1.1 302 الذي تم العثور عليه لإعادة التوجيه إلى URL آخر (https://tools.cisco.com/healthcheck)، والذي يمكن للعميل متابعته استنادا إلى المعلمات المتاحة والغرض من الطلب. على الرغم من أن عملية إعادة التوجيه هذه تحدث ضمن جلسة TLS المشفرة وغير مرئية مباشرة، إلا أنها توقع سلوكا ويمكن ملاحظتها إذا تم فك تشفير حركة مرور TLS.

سوف تظهر حركة مرور إعادة التوجيه المشفرة كما يلي:

```
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)
```

تقسيم الاتصال إلى أسفل:
بمجرد اكتمال عملية الاستبدال، يقوم كل من العميل والوكيل بإغلاق اتصال TCP بشكل

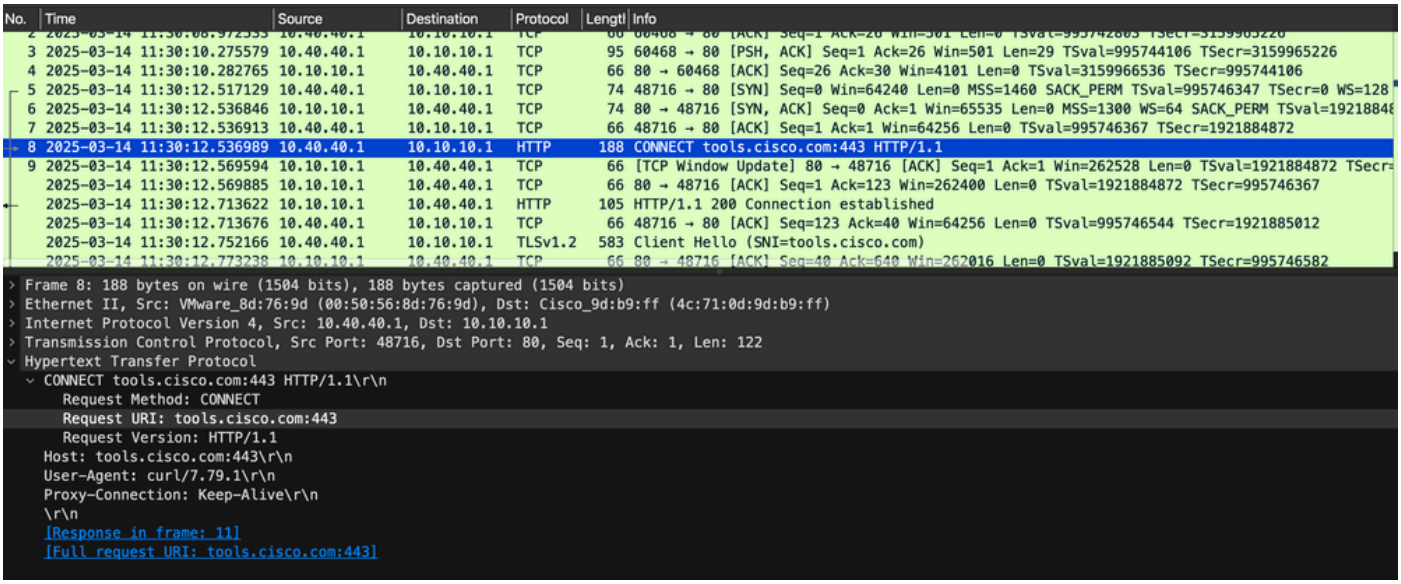
سلس من خلال تبادل حزم FIN و ACK، مما يضمن إنهاء الجلسة بشكل صحيح.

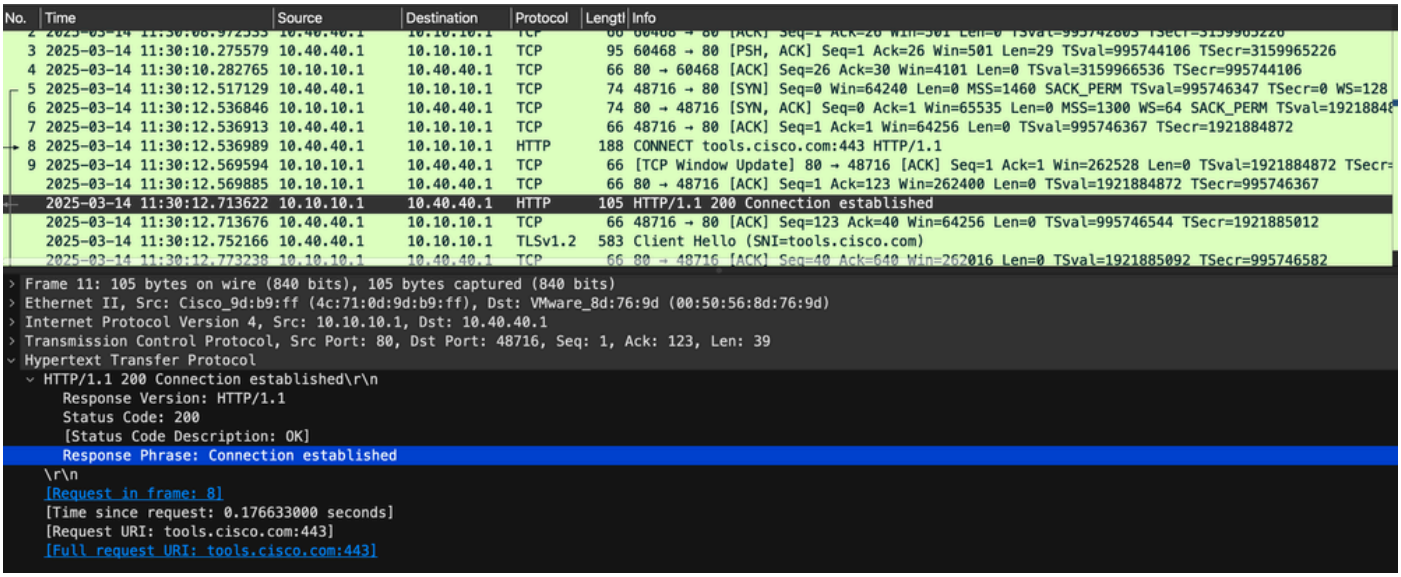
مثال على إخراج tcpdump:

```
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
```

تلميح: عن طريق تحليل إخراج tcpdump، يمكنك التحقق من أن طلب HTTPS من خلال الوكيل الصريح يتبع التدفق المتوقع: مصافحة TCP، طلب اتصال، إنشاء نفق، مصافحة TLS، الاتصال المشفر (بما في ذلك عمليات إعادة التوجيه المحتملة)، وإغلاق الاتصال بشكل رائع. وهذا يؤكد أن تفاعل الوكيل والعميل يعمل كما هو مصمم، ويساعد على تحديد أي مشاكل في التدفق، مثل حالات الفشل في تفاوض إنشاء قنوات الاتصال النفقي أو تفاوض SSL.

تقوم FMC (10.40.40.1) بإنشاء مصافحة TCP ناجحة مع الوكيل (10.10.10.1) على المنفذ 80، يتبعها اتصال HTTP بالخادم (72.163.4.161) على المنفذ 443. يستجيب الخادم برسالة تم تأسيس اتصال HTTP 200. يتم إكمال تأكيد اتصال TLS، وتدفق البيانات بشكل صحيح. أخيرا، ينتهي اتصال TCP بشكل جميل (FIN).





مشكلات معروفة

قيود قائمة التحكم في الوصول (ACL) للوكيل

إذا كانت هناك مشكلة في الأذونات (مثل قائمة الوصول على الوكيل)، فيمكنك ملاحظة ذلك من خلال التقاط الحزمة (tcpdump). هذا شرح عالي المستوى لسيناريو الفشل، مع مثال مخرجات tcpdump:

بدء مصافحة TCP:
يبدأ العميل (FirePOWER) بإنشاء اتصال TCP للوكيل على المنفذ 80. يتم إكمال مصافحة TCP (SYN، SYN-ACK، ACK) بنجاح، مما يعني أنه يمكن الوصول إلى الوكيل.

مثال على إخراج 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
```

طلب اتصال HTTP:
وبمجرد الاتصال، يرسل العميل طلب اتصال HTTP إلى الوكيل، طالبا منه إنشاء نفق إلى tools.cisco.com:443.

مثال tcpdump (Decoded HTTP):

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

```
Proxy-Connection: Keep-Alive
```

إستجابة الخطأ من الوكيل:

بدلا من السماح بالنفق، يرفض الوكيل الطلب، ربما بسبب قائمة الوصول (ACL) التي لا تسمح بهذه حركة المرور. يستجيب الوكيل بخطأ مثل عبارة 403 Forbidden أو عبارة 502 Bad.

مثال على إخراج tcpdump الذي يظهر الخطأ:

```
<#root>

HTTP/1.1

403

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

تقسيم الاتصال إلى أسفل:
بعد إرسال رسالة الخطأ، يقوم الوكيل بإغلاق الاتصال، ويتبادل كلا الجانبين حزم FIN/ACK.

مثال على إخراج 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
```

تلميح: من Tcpdump، يمكنك أن ترى أنه على الرغم من نجاح اتصال TCP وطلب اتصال HTTP، إلا أن الوكيل رفض إعداد النفق. يشير ذلك عادة إلى أن الوكيل لديه قائمة تحكم في الوصول (ACL) أو قيد الأذونات يمنع حركة المرور من المرور.

فشل الوكيل في التنزيل (المهلة/النقل غير المكتمل)

في هذا السيناريو، تتصل FMC بنجاح بالوكيل وتبدأ تنزيل الملف، ولكن ينتهي وقت النقل وأ يفشل في الإكمال. وعادة ما يكون ذلك نتيجة للتفتيش الوكيل وأ فترات المهلة الزمنية أو حدود حجم الملف على الوكيل.

بدء مصافحة TCP
تقوم FMC بتهيئة اتصال TCP للوكيل على المنفذ 80، ويتم المصافحة بنجاح.

مثال على إخراج 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
```

طلب اتصال HTTP
ترسل FMC طلب اتصال HTTP إلى الوكيل للوصول إلى الهدف الخارجي.
مثال tcpdump (Decoded HTTP):

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

إنشاء النفق ومصافحة TLS
يستجيب الوكيل باستخدام اتصال HTTP/1.1 200 الذي تم إنشاؤه، مما يتيح بدء مصافحة TLS.

مثال على إخراج 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)
```

المهلة أو التنزيل غير المكتمل
بعد بدء نقل الملف، يتوقف التنزيل أو ال يكتمل، مما يؤدي إلى مهلة. يبقى الاتصال خامل.
الأسباب المحتملة تشمل:

- تأخر فحص الوكيل أو التصفية.
- فترات الانتظار للوكيل لعمليات النقل الطويلة.
- حدود حجم الملف التي يفرضها الوكيل.

مثال TCPDUMP الذي يظهر عدم النشاط:

<#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.
```

تلميح: تقوم FMC بتهيئة التنزيل ولكنها تفشل في الإكمال بسبب حالات انتهاء المهلة الزمنية أو النقل غير الكامل، غالبا ما يكون ذلك بسبب تصفية الوكيل أو قيود حجم الملف.

فشل الوكيل في تنزيل الملف (مشكلة MTU)

في هذه الحالة، يتصل FMC بالوكيل ويبدأ في تنزيل الملفات، ولكن تفشل الجلسة بسبب مشاكل MTU. تتسبب هذه المشاكل في تجزئة الحزمة أو الحزم المسقطة، وخاصة مع الملفات الكبيرة أو مصافحة SSL/TLS.

بدء مصافحة TCP
تقوم FMC بتهيئة مصافحة TCP باستخدام الوكيل، والذي ينجح.
مثال على إخراج 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
```

طلب اتصال HTTP وإنشاء النفق
ترسل FMC طلب اتصال HTTP، ويستجيب الوكيل، مما يسمح بإنشاء النفق.
مثال tcpdump (Decoded HTTP):

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

بدء مصافحة TLS
تبدأ FMC و tools.cisco.com التفاوض على SSL/TLS، ويتم تبادل الحزم الأولية.
مثال على إخراج 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)
```

تجزئة الحزمة أو إسقاطها بسبب MTU
عندما تحاول FMC أو الخادم إرسال حزم كبيرة، تتسبب مشكلة MTU في تجزئة الحزمة أو TLS. فوض عمليات إسقاط الحزم، مما ينتج عنه نقل المخالفات أو حالات فشل
وهذا يحدث عادة عندما يتم تعيين وحدة الحد الأقصى للنقل (MTU) بشكل غير صحيح بين وحدة التحكم في إدارة الهيكل (FMC) والوكيل (أو بين الوكيل والإنترنت) أو عندما تكون صغيرة جدا.
مثال tcpdump الذي يظهر محاولة التجزئة:

```
<#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
```

تلميح: ينتج عن إصدار MTU حزم مسقطة أو مجزأة، مما يؤدي إلى تعطيل مصافحة TLS أو التسبب في فشل عمليات تنزيل المخالفات. يظهر هذا بشكل عام عندما يحدث فحص SSL أو تجزئة الحزمة بسبب إعدادات MTU غير الصحيحة.

في سيناريو الفشل، تحصل FMC على الاتصال دون بروتوكول HTTP 200، مع عمليات إعادة المحاولة ونظام FIN التي تؤدي إلى تبادل TLS/البيانات، ربما بسبب مشكلة في وحدة الحد الأقصى للنقل (MTU) أو بسبب مشكلة في الوكيل/الخادم.

عند إستخدام curl، يمكنك مواجهة مختلف رموز إستجابة HTTP التي تشير إلى مشاكل من جانب الخادم أو أخطاء في المصادقة. هذه قائمة أشهر رموز الأخطاء و معانيها:

رمز HTTP	المعنى	السبب
400	طلب غير صحيح	بناء جملة طلب غير صحيح

رمز HTTP	المعنى	السبب
401	غير مصرح به	بيانات الاعتماد مفقودة أو غير صحيحة
403	ممنوع	تم رفض الوصول
404	لم يتم العثور	لم يتم العثور على المورد
500	خطأ داخلي	خطأ في الخادم
502	Bad Gateway	سوء اتصال الخادم
503	الخدمة غير متوفرة	تحميل الخادم الزائد أو الصيانة
504	مهلة البوابة	المهلة بين الخوادم

المراجع

ملاحظات إصدار الدفاع ضد تهديد جدار الحماية الآمن من Cisco، الإصدار 7.4.x

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).