FXP نيوكت لاثم عم ASA تافلم لقن

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين بروتوكول تغيير الملف (FXP) على جهاز الأمان القابل للتكيف (ASA) من Cisco عبر واجهة سطر الأوامر (CLI).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة أساسية ببروتوكول نقل الملفات (FTP) (الأوضاع النشطة/الخاملة).

المكونات المستخدمة

أسست المعلومة في هذا وثيقة على ال cisco ASA أن يركض برمجية صيغة 8.0 ومتأخر.

ملاحظة: يستخدم مثال التكوين هذا محطتي عمل Microsoft Windows تعملان كخادمين ل FXP وتشغيلان خدمات FTP (برنامج مساعدة 3C). لديهم أيضا FXP ممكن. كما يتم إستخدام محطة عمل أخرى من Microsoft Windows تشغل برنامج عميل FTP Rush) FXP).

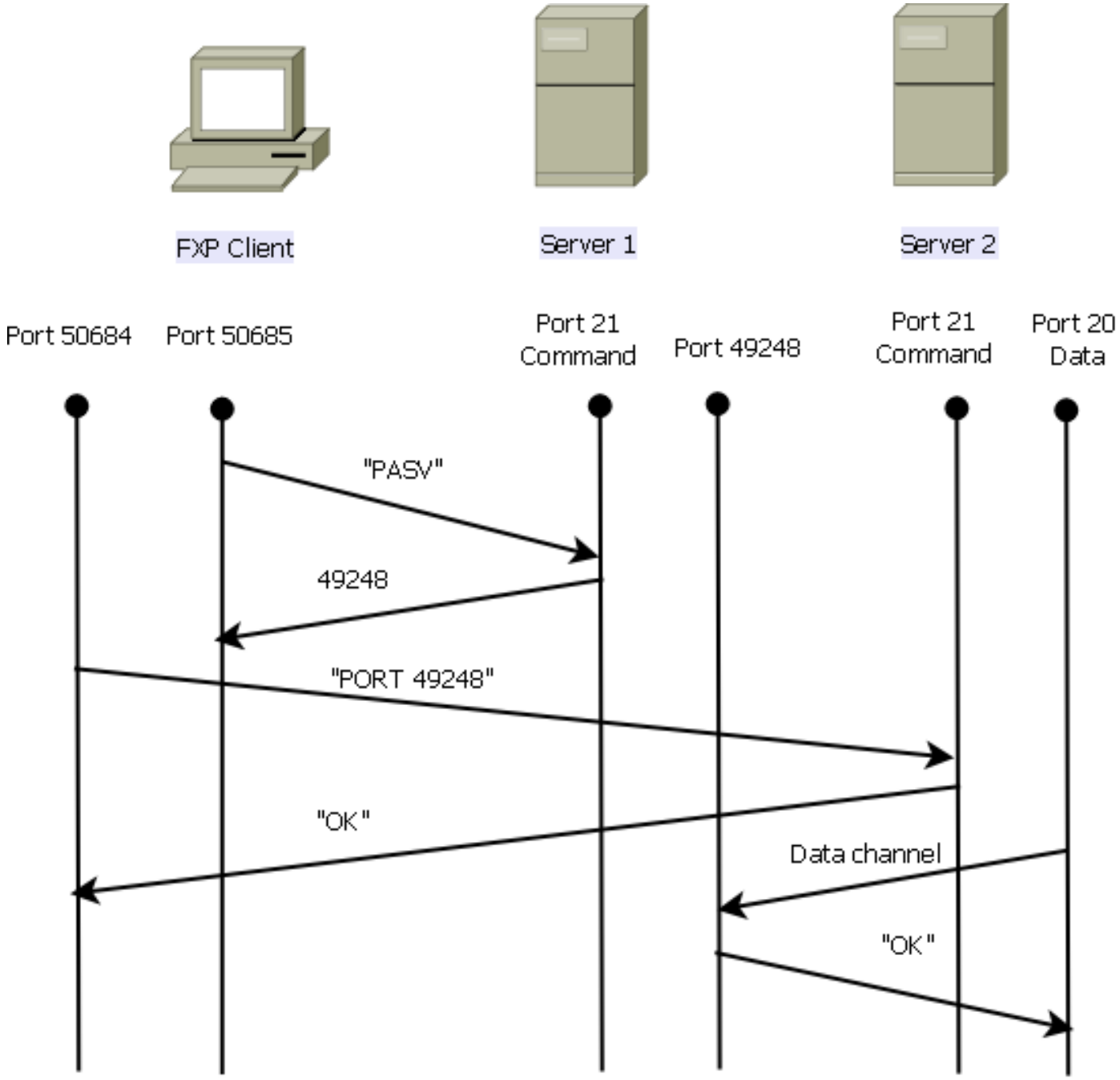
تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

يتيح لك بروتوكول FXP نقل الملفات من خادم FTP إلى خادم FTP آخر عبر عميل FXP دون الحاجة إلى الاعتماد على سرعة اتصال العميل بالإنترنت. مع FXP، تعتمد سرعة النقل القصوى فقط على الاتصال بين الخادمين، والذي يكون عادة أسرع بكثير من اتصال العميل. يمكنك تطبيق بروتوكول FXP في السيناريوهات التي يتطلب فيها الخادم ذو النطاق الترددي العريض الفائق موارد من خادم آخر ذي نطاق ترددي عريض فائق، ولكن يتمتع العميل ذو النطاق الترددي العريض المنخفض فقط، مثل مسؤول الشبكة الذي يعمل عن بعد، بسلطة الوصول إلى الموارد الموجودة على كلا الخادمين.

يعمل بروتوكول FXP كامتداد لبروتوكول FTP، والآلية مذكورة في القسم 5.2 من بروتوكول FTP RFC 959. في الأساس، يقوم عميل FXP ببدء اتصال تحكم بخادم FTP1، ويفتح اتصال تحكم آخر بخادم FTP2، ثم يقوم بتعديل سمات الاتصال الخاصة بالخوادم بحيث تشير إلى بعضها البعض بحيث تتم عملية النقل مباشرة بين الخادمين.

آلية نقل الملفات عبر FXP



فيما يلي نظرة عامة على العملية:

1. يفتح العميل اتصال التحكم مع الخادم1 على منفذ TCP 21.

يرسل العميل الأمر **PASV** إلى الخادم 1.

يستجيب Server1 بعنوان IP الخاص به والمنفذ الذي يستمع إليه.

2. يفتح العميل اتصال تحكم مع الخادم 2 على منفذ TCP 21.

يمرر العميل العنوان/المنفذ الذي يتم إستقباله من الخادم1 إلى الخادم2 في أمر **منفذ**.

يستجيب Server2 لإعلام العميل بنجاح **الأمر** الخاص **بالمنفذ**. يعرف Server2 الآن أين سيتم إرسال البيانات.

3. لبدء عملية الإرسال من الخادم 1 إلى الخادم 2:

يرسل العميل الأمر **STOR** إلى الخادم 2 ويوجهه لتخزين التاريخ الذي يستلمه.

يرسل العميل الأمر **RETR** إلى الخادم 1 ويوجهه لاسترداد الملف أو إرساله.

4. تنتقل جميع البيانات الآن مباشرة من المصدر إلى خادم FTP الوجهة. يقوم كلا الخادمين فقط بالإبلاغ عن رسائل الحالة عند الفشل/النجاح إلى العميل.

هكذا يظهر جدول الاتصال:

```
,TCP server2 192.168.1.10:21 client 172.16.1.10:50684, idle 0:00:04, bytes 694
                                                                    flags UIOB
  ,TCP client 172.16.1.10:50685 server1 10.1.1.10:21, idle 0:00:04, bytes 1208
                                                                    flags UIOB
```

فحص FTP و FXP

يكون نقل الملفات عبر ASA عبر FXP ناجحا فقط عندما يتم **تعطيل** فحص FTP على ASA.

عندما يحدد عميل FXP عنوان IP ومنفذ TCP الذي يختلف عن ذاك الخاص بالعميل في الأمر **FTP port**، يتم إنشاء حالة غير آمنة حيث يكون المهاجم قادرا على تنفيذ مسح المنفذ مقابل مضيف على الإنترنت من خادم FTP للجهة الخارجية. وذلك لأنه قد تم توجيه خادم FTP لفتح اتصال بمنفذ على جهاز قد لا يكون العميل الذي تم إنشاؤه. يسمى هذا **هجوم إرتطام FTP**، ويغلق فحص FTP الاتصال لأنه يعتبر هذا انتهاكا للأمان.

فيما يلي مثال:

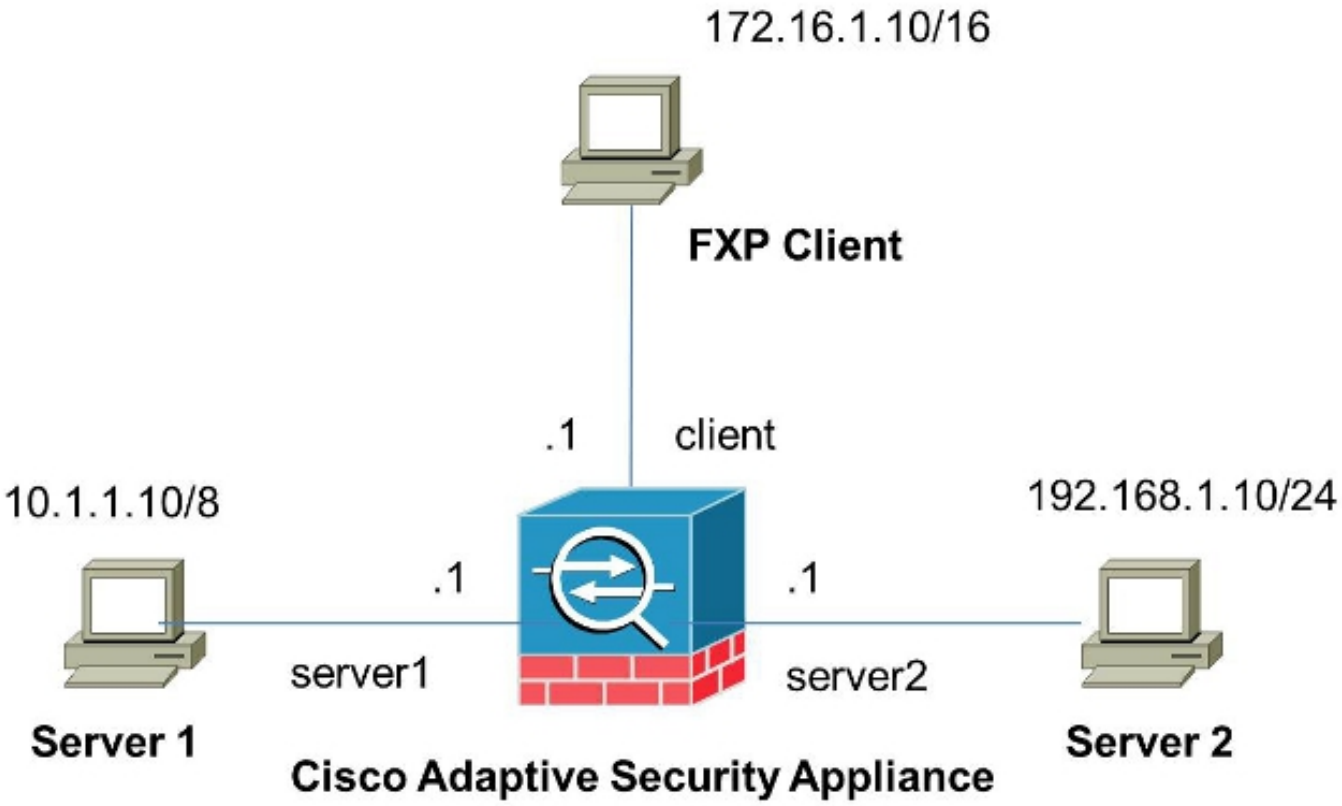
```
ASA-6-302013: Built inbound TCP connection 24886 for client:172.16.1.10/49187%
              (to server2:192.168.1.10/21 (192.168.1.10/21 (172.16.1.10/49187)
ASA-6-302013: Built inbound TCP connection 24889 for client:172.16.1.10/49190%
        (to server2:192.168.1.10/49159 (192.168.1.10/49159 (172.16.1.10/49190)
  ASA-6-302014: Teardown TCP connection 24889 for client:172.16.1.10/49190 to%
               server2:192.168.1.10/49159 duration 0:00:00 bytes 1078 TCP FINs
  ASA-4-406002: FTP port command different address: 172.16.1.10(10.1.1.10) to%
                                                  on interface client 192.168.1.10
  ASA-6-302014: Teardown TCP connection 24886 for client:172.16.1.10/49187 to%
  server2:192.168.1.10/21 duration 0:00:00 bytes 649 Flow closed by inspection
```

التكوين

أستخدم المعلومات الموضحة في هذا القسم لتكوين FXP على ASA.

ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

الرسم التخطيطي للشبكة



تكوين ASA عبر CLI

أتمت هذا steps in order to شكلت ال ASA:

1. تعطيل فحص FTP:

```
FXP-ASA(config)# policy-map global_policy
FXP-ASA(config-pmap)#  class inspection_default
FXP-ASA(config-pmap-c)# no inspect ftp
```

2. قم بتكوين قوائم الوصول للسماح بالاتصال بين عميل FXP وخوادم FTP:

```
FXP-ASA(config)#access-list serv1 extended permit ip host 10.1.1.10 any
FXP-ASA(config)#access-list serv1 extended permit ip any host 10.1.1.10
FXP-ASA(config)#access-list serv2 extended permit ip host 192.168.1.10 any
FXP-ASA(config)#access-list serv2 extended permit ip any host 192.168.1.10
FXP-ASA(config)#access-list client extended permit ip host 172.16.1.10 any
FXP-ASA(config)#access-list client extended permit ip any host 172.16.1.10
```

3. تطبيق قوائم الوصول على الواجهات المقابلة:

```
FXP-ASA(config)#access-group serv1 in interface server1
FXP-ASA(config)#access-group client in interface client
FXP-ASA(config)#access-group serv2 in interface server2
```

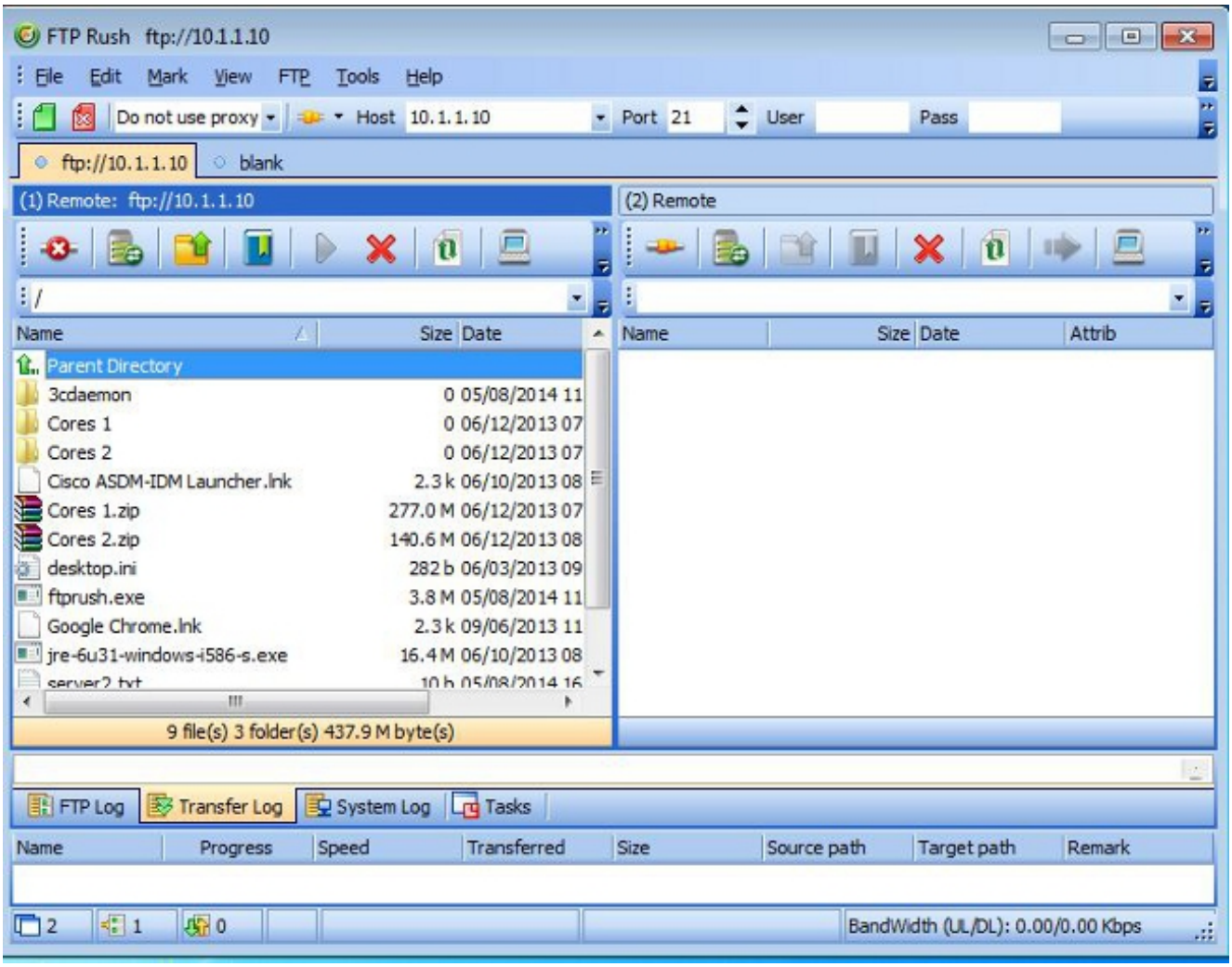
التحقق من الصحة

أستخدم المعلومات الموضحة في هذا القسم للتحقق من أن التكوين لديك يعمل بشكل صحيح.

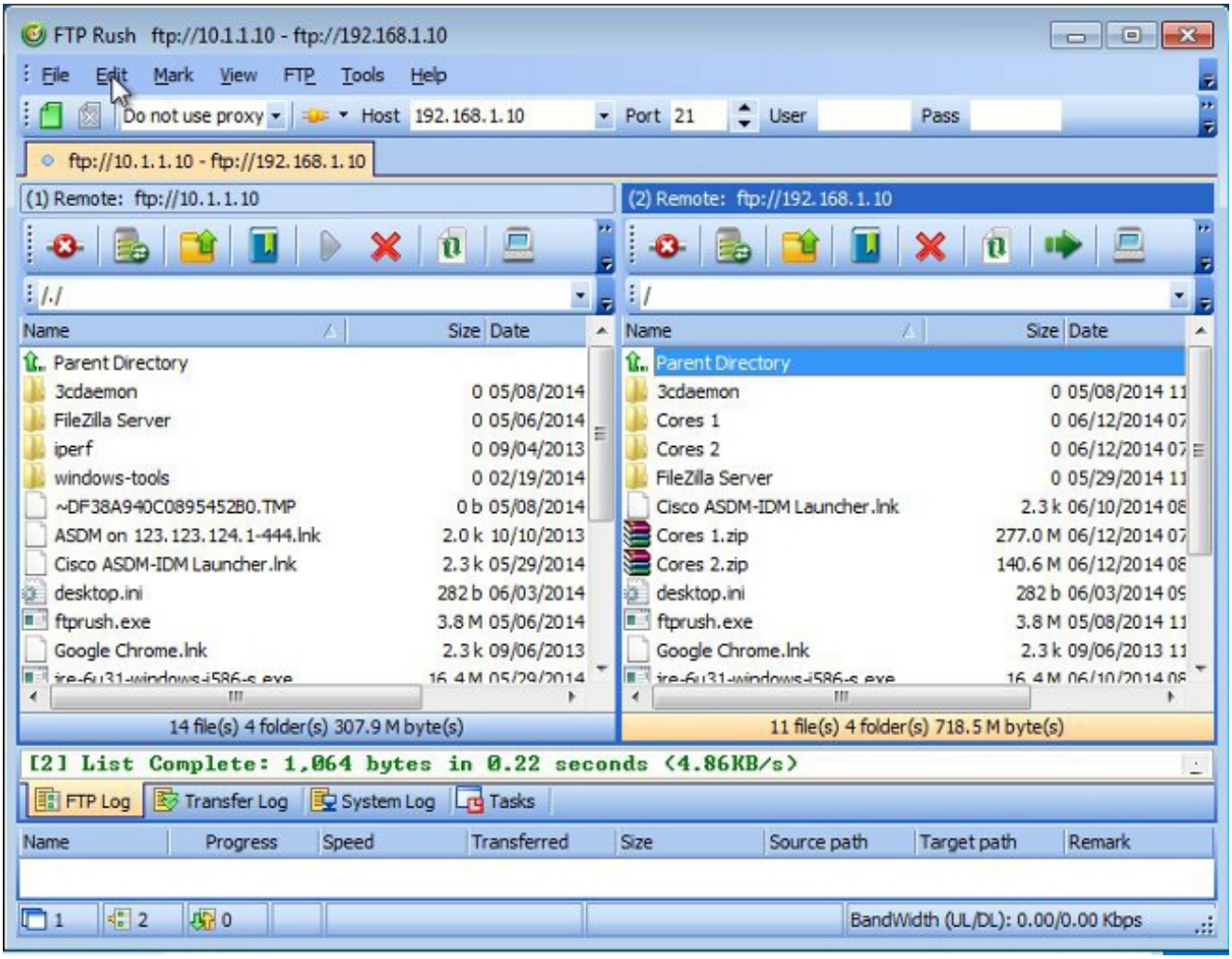
عملية نقل الملفات

أتمت هذا steps in order to دققت بنجاح مبرد نقل بين الإثنان FTP نادل:

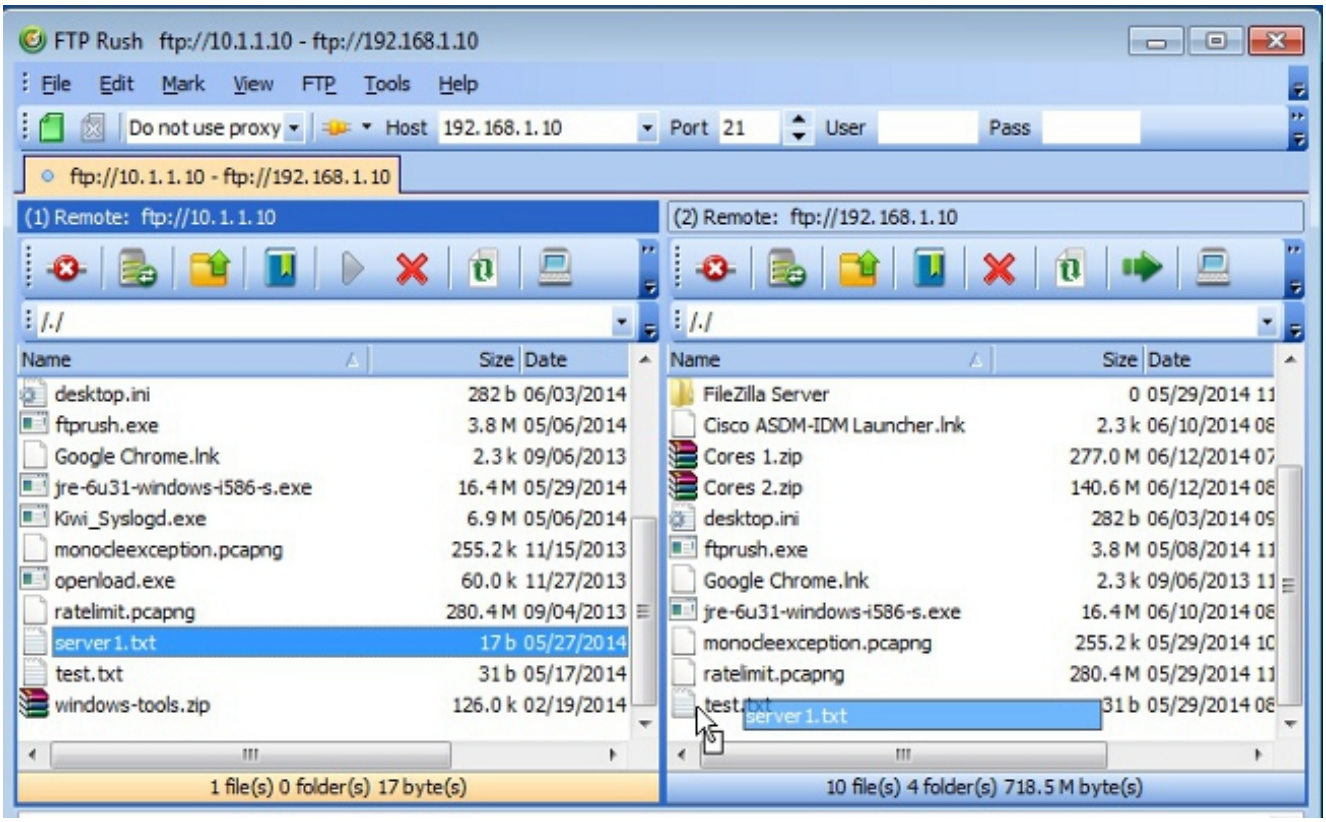
1. الاتصال بالخادم 1 من جهاز عميل FXP:



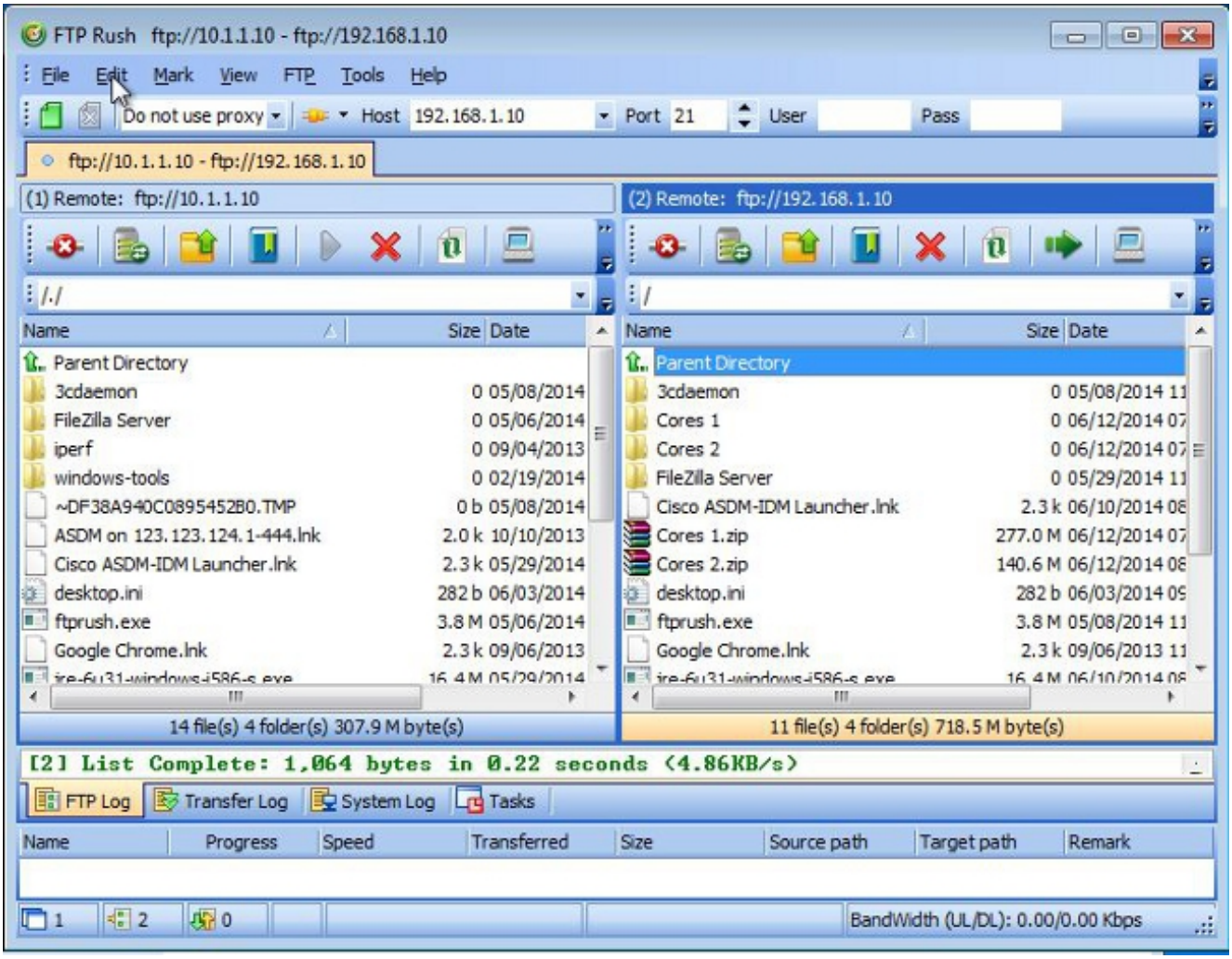
2. الاتصال بالخادم 2 من جهاز عميل FXP:



قم بسحب الملف وإفلاته ليتم نقله من نافذة الخادم 1 إلى نافذة الخادم 2: .3



4. تحقق من نجاح نقل الملفات:



استكشاف الأخطاء وإصلاحها

يوفر هذا القسم لقطات لسيناريوهين مختلفين يمكنك إستخدامهما لاستكشاف أخطاء التكوين وإصلاحها.

سيناريو تعطيل فحص FTP

عندما يتم تعطيل فحص FTP، كما هو موضح في قسم فحص FTP و FXP في هذا المستند، تظهر هذه البيانات على واجهة عميل ASA:

```
2006-12-12 02:56:17.199376  172.16.1.10   10.1.1.10     FTP    60 Request: PASV
2006-12-12 02:56:17.200902  10.1.1.10     172.16.1.10   FTP   100 Response: 227 Entering passive mode (10,1,1,10,192,96)
2006-12-12 02:56:17.201481  172.16.1.10   192.168.1.10  FTP    77 Request: PORT 10,1,1,10,192,96
2006-12-12 02:56:17.203297  192.168.1.10  172.16.1.10   FTP    84 Response: 200 PORT command successful.
2006-12-12 02:56:17.203953  172.16.1.10   192.168.1.10  FTP    77 Request: STOR Kiwi_Syslogd.exe
2006-12-12 02:56:17.206272  192.168.1.10  172.16.1.10   FTP   106 Response: 150 File status OK ; about to open data connection
2006-12-12 02:56:17.206852  172.16.1.10   10.1.1.10     FTP    77 Request: RETR Kiwi_Syslogd.exe
2006-12-12 02:56:17.208698  10.1.1.10     172.16.1.10   FTP    90 Response: 125 Using existing data connection
2006-12-12 02:56:17.420617  172.16.1.10   192.168.1.10  TCP    54 50684 > ftp [ACK] Seq=159 Ack=459 Win=130560 Len=0
2006-12-12 02:56:17.420724  172.16.1.10   10.1.1.10     TCP    54 50685 > ftp [ACK] Seq=119 Ack=433 Win=130668 Len=0
2006-12-12 02:56:18.340741  10.1.1.10     172.16.1.10   FTP   110 Response: 226 Closing data connection; File transfer successful.
2006-12-12 02:56:18.341382  192.168.1.10  172.16.1.10   FTP   110 Response: 226 Closing data connection; File transfer successful.
```

فيما يلي بعض الملاحظات حول هذه البيانات:

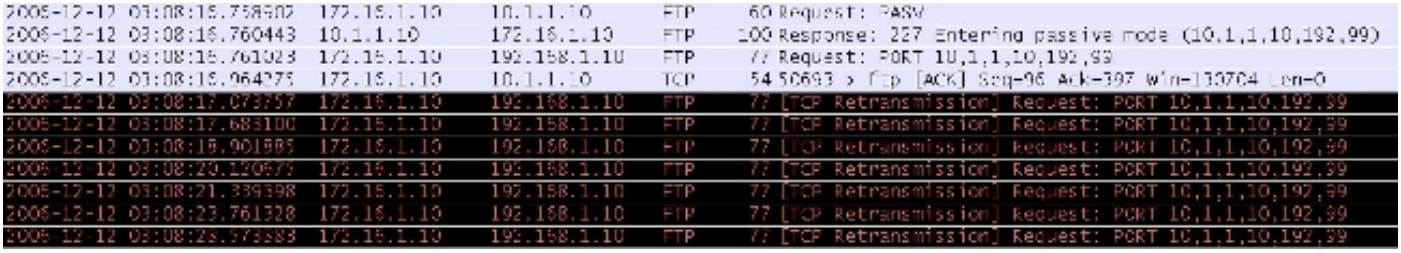
- عنوان IP للعميل هو **172.16.1.10**.

- عنوان IP للخادم 1 هو **10.1.1.10**.
- عنوان IP للخادم 2 هو **192.168.1.10**.

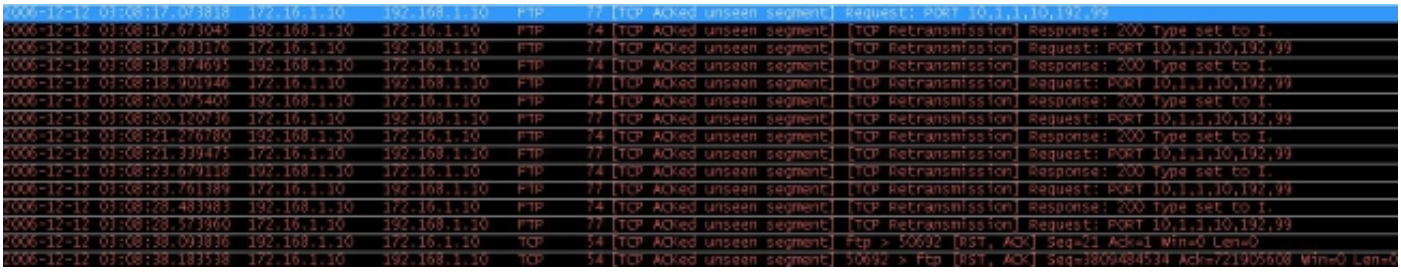
في هذا المثال، يتم نقل الملف المسمى **Kiwi_Syslod.exe** من الخادم 1 إلى الخادم 2.

تمكين فحص FTP

عند تمكين فحص FTP، تظهر هذه البيانات على واجهة عميل ASA:



هنا التقاط إسقاط ASA:



يتم إسقاط طلب **المنفذ** من خلال فحص FTP لأنه يحتوي على عنوان IP ومنفذ يختلف عن عنوان IP الخاص بالعميل والمنفذ. وبعد ذلك، يتم إنهاء اتصال عنصر التحكم بالخادم بواسطة الفحص.

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).