تكوين التقاط حزمة ASA باستخدام CLI و ASDM

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين جدار حماية Cisco ASA لالتقاط الحزم المطلوبة باستخدام ASDM أو CLI (واجهة سطر الأوامر).

المتطلبات الأساسية

المتطلبات

يفترض هذا الإجراء أن ASA يعمل بالكامل وتم تكوينه للسماح لـ Cisco ASDM أو CLI بإجراء تغييرات التكوين.

المكونات المستخدمة

لا يقيد هذا المستند إلى أجهزة أو برمجيات معينة.

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 قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

المنتجات ذات الصلة

يتم إستخدام هذا التكوين أيضا مع منتجات Cisco التالية:

- ASA الإصدارات 9.1(5) من Cisco والإصدارات الأحدث
- Cisco ASDM، الإصدار 7.2.1

معلومات أساسية

يصف هذا وثيقة كيف أن يشكل **Cisco Adaptive Security Appliance (ASA) Next-Generation Firewall** in order to على قبض الربط ب مرغوب مع إما **Cisco Adaptive Security Device Manager (ASDM)** أو **Command Line Interface (CLI) (ASDM)**.

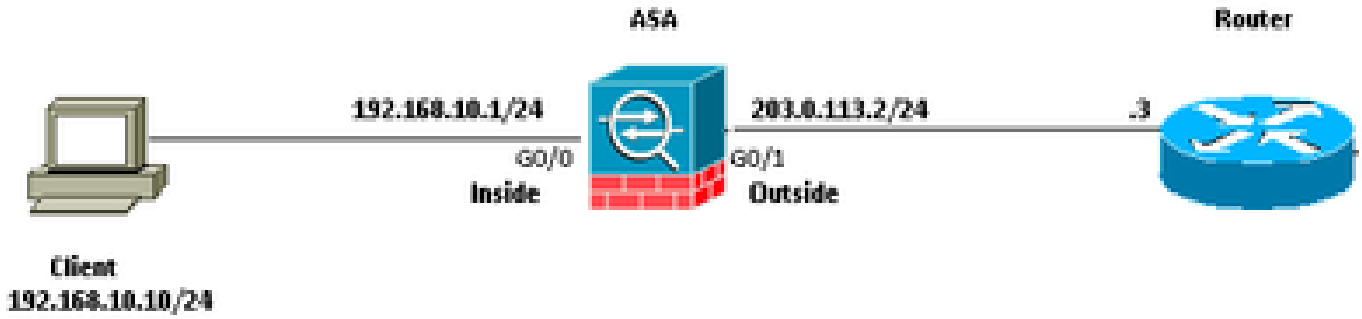
تكون عملية التقاط الحزمة مفيدة لاستكشاف أخطاء الاتصال وإصلاحها أو مراقبة الأنشطة المشبوهة. بالإضافة إلى ذلك، من المه

التكوين

يوفر هذا القسم المعلومات المستخدمة لتكوين ميزات التقاط الحزمة الموضحة في هذا المستند.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



التكوينات

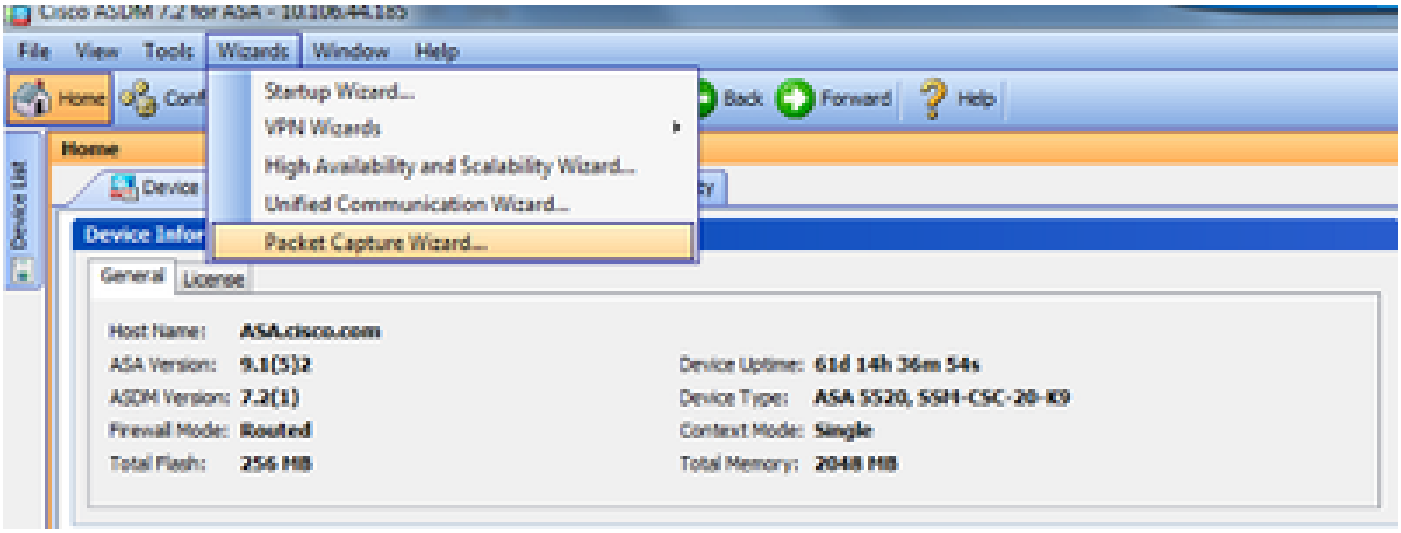
ال ip ليس عنوان خطة يستعمل في هذا تشكيل قانونيا routable على الإنترنت. هم rfc 1918 عنوان أن يكون استعملت في مختبر بيئ

تكوين التقاط الحزم باستخدام ASDM

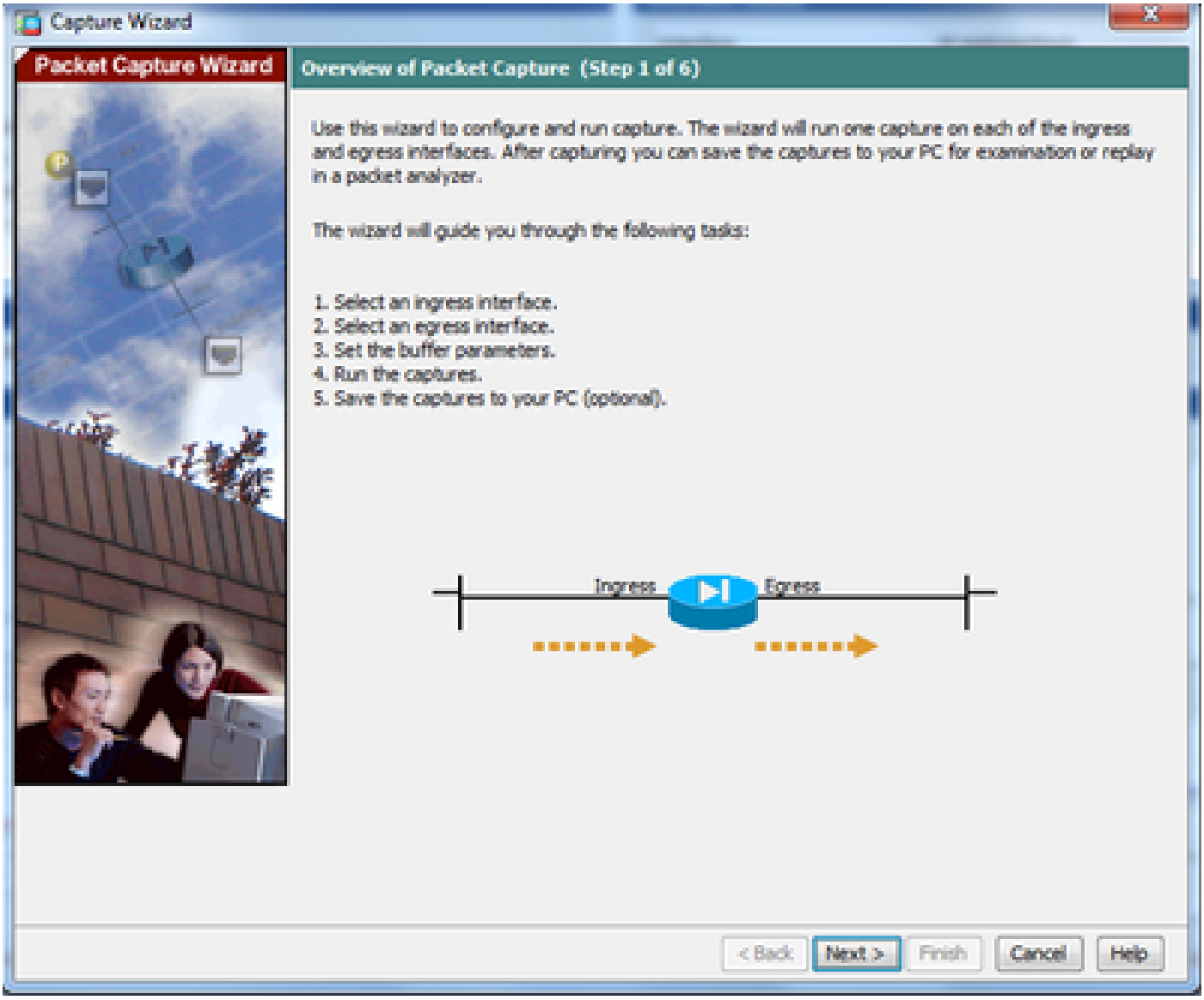
يتم استخدام مثال التكوين هذا في التقاط الحزم التي يتم إرسالها أثناء إختبار الاتصال من المستخدم1 (داخل الشبكة) إلى الموج

أكمل هذه الخطوات لتكوين ميزة التقاط الحزمة على ASA باستخدام ASDM:

1. انتقل **Wizards** > **Packet Capture Wizard** لبدء تكوين التقاط الحزمة، كما هو موضح:



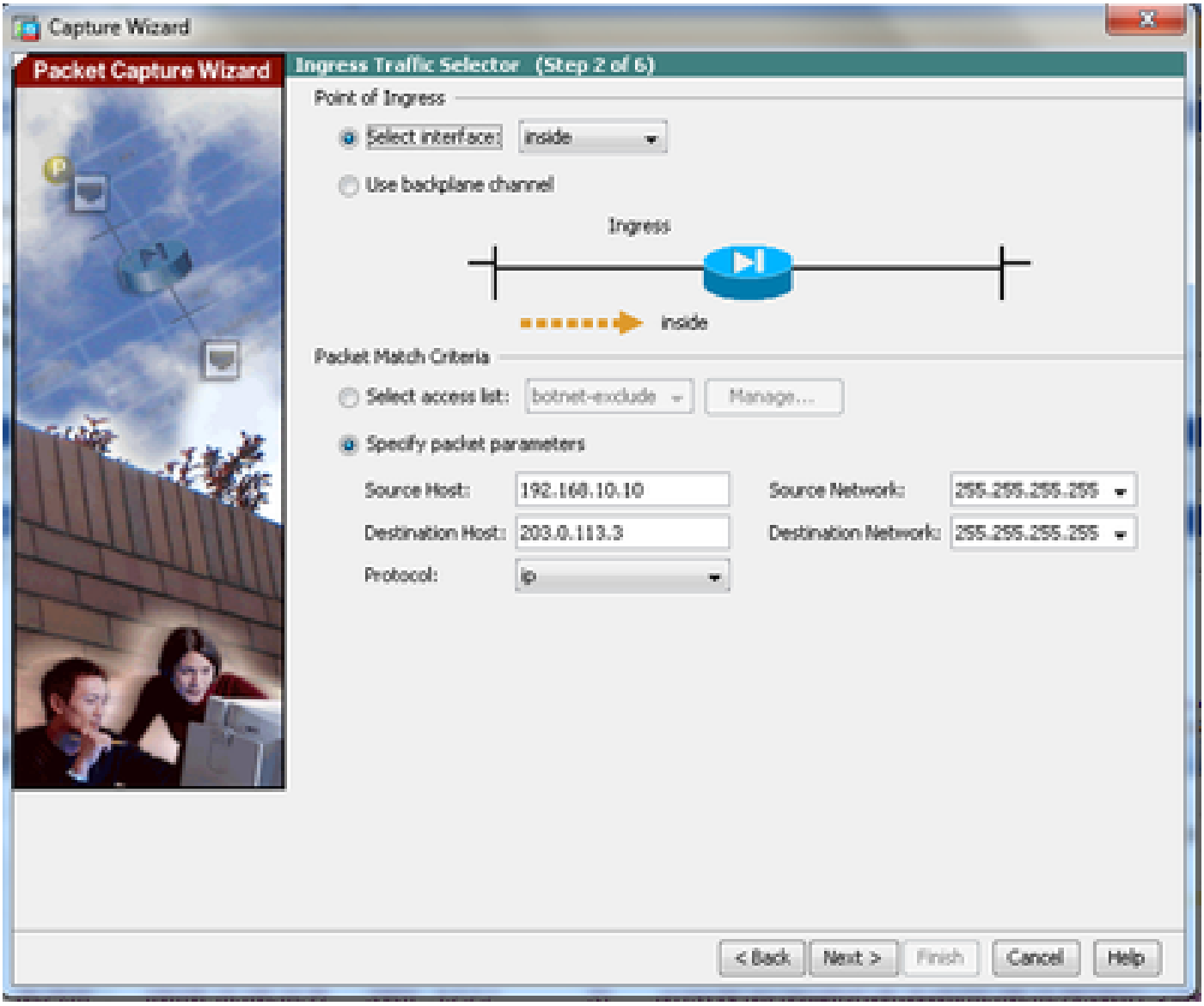
2. **Capture Wizard** تفتح. انقر.**Next**



3.0 في النافذة الجديدة، قم بتوفير المعلمات التي يتم إستخدامها في التقاط حركة مرور المدخل.

3.1 حدد **inside** لعناوين IP المصدر والوجهة **Ingress Interface** للحزم التي سيتم التقاطها مع قناع الشبكة الفرعية الخاص بها في الم

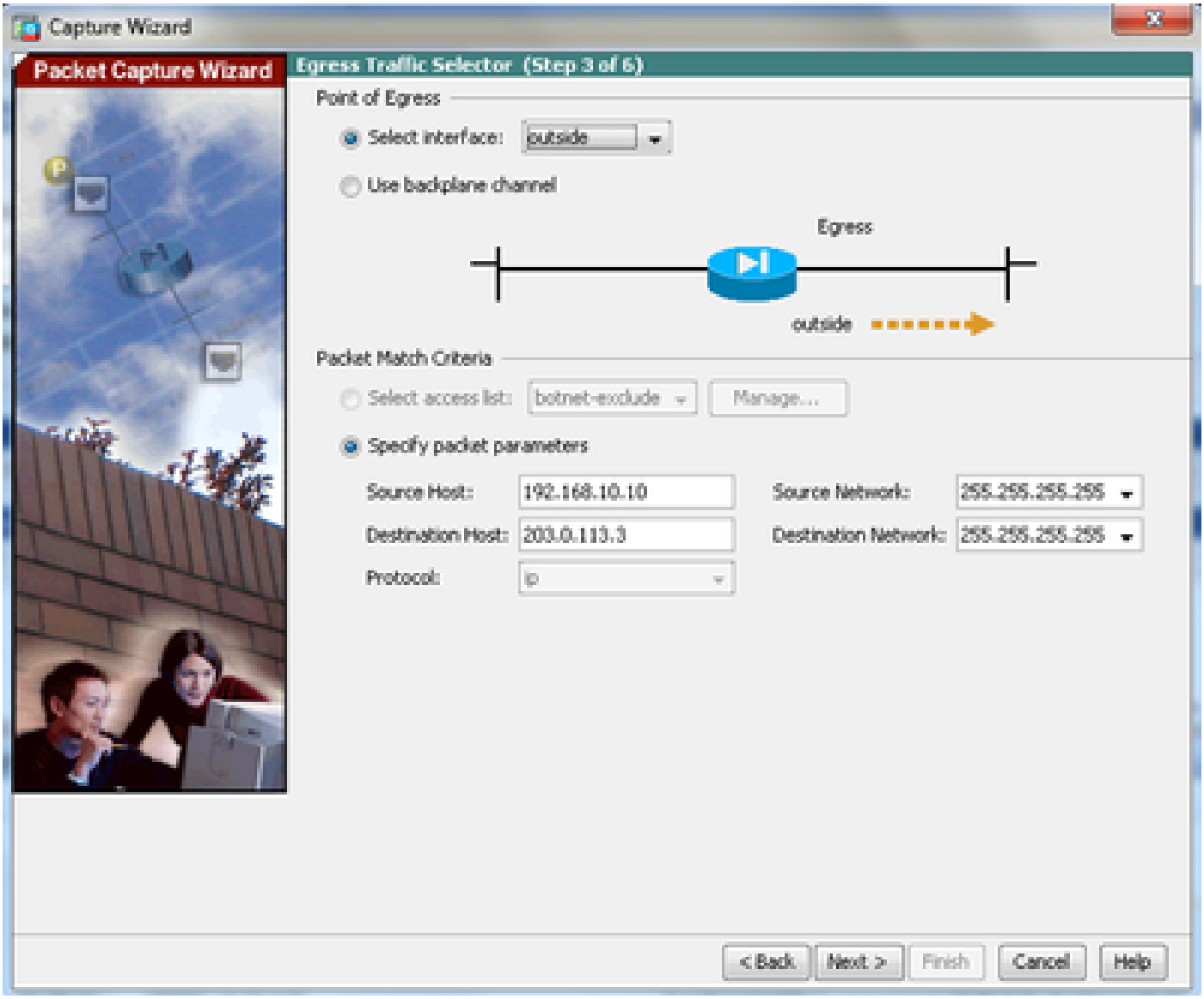
3.2 أختر نوع الحزمة التي سيتم الاستيلاء عليها بواسطة ASA (IP وه نوع الحزمة المختارة هنا)، كما وه موضح:



3. 3 انقر **Next**.

4.1 حدد **outside** لعناوين IP المصدر والوجهة **Egress Interface** ووفرها، بالإضافة إلى قناع الشبكة الفرعية الخاص بها، في الفراغات ذات

If Network Address Translation (NAT) على "جدار الحماية" و خذ ذلك بعين الاعتبار أيضا.



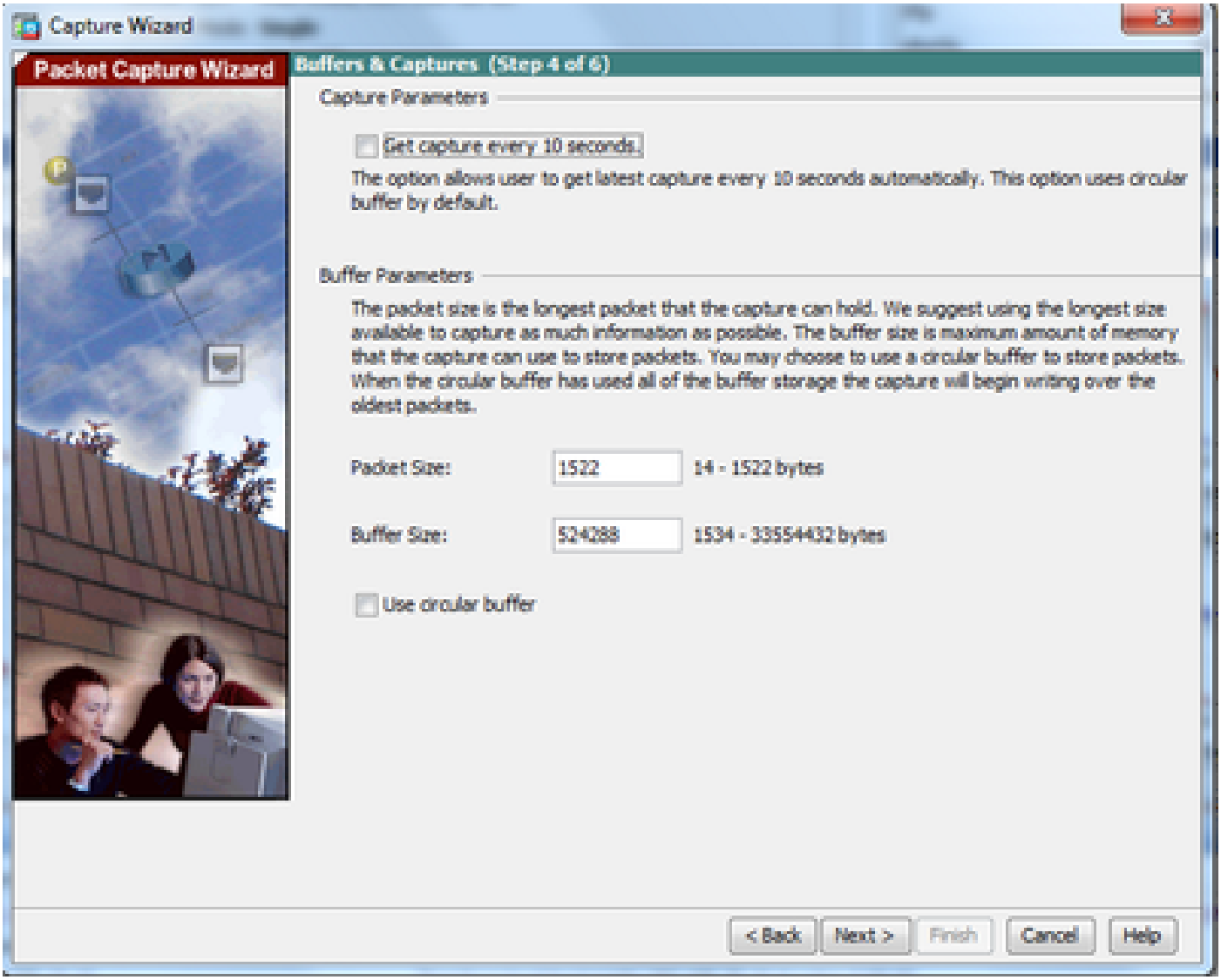
4. 2 انقر **Next**.

5.1 أدخل المكان المناسب **Packet Size** والمساحة **Buffer Size** المخصصة المتوفرة. هذه البيانات مطلوبة حتى يحدث الالتقاط.

5.2 حدد **Use circular buffer** المربع لاستخدام خيار المخزن المؤقت الدائري. المخازن المؤقتة الدائرية لا يتم ملؤها أبدا.

مع وصول المخزن المؤقت إلى أقصى حجم له، يتم تجاهل البيانات الأقدم ويستمر الالتقاط.

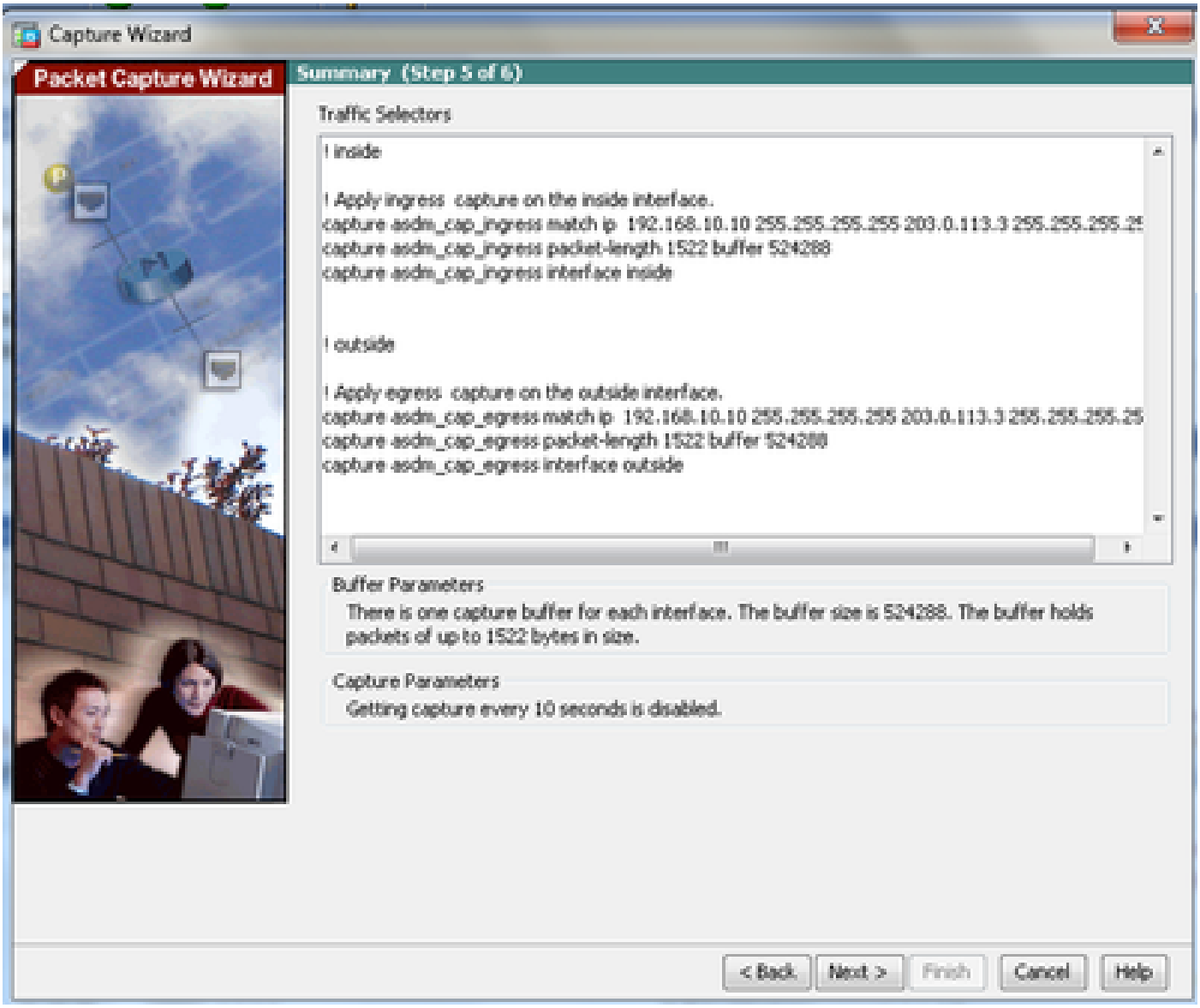
في هذا المثال، لا يتم إستخدام مخزن مؤقت دائري، لذلك لم يتم تحديد خانة الاختيار.



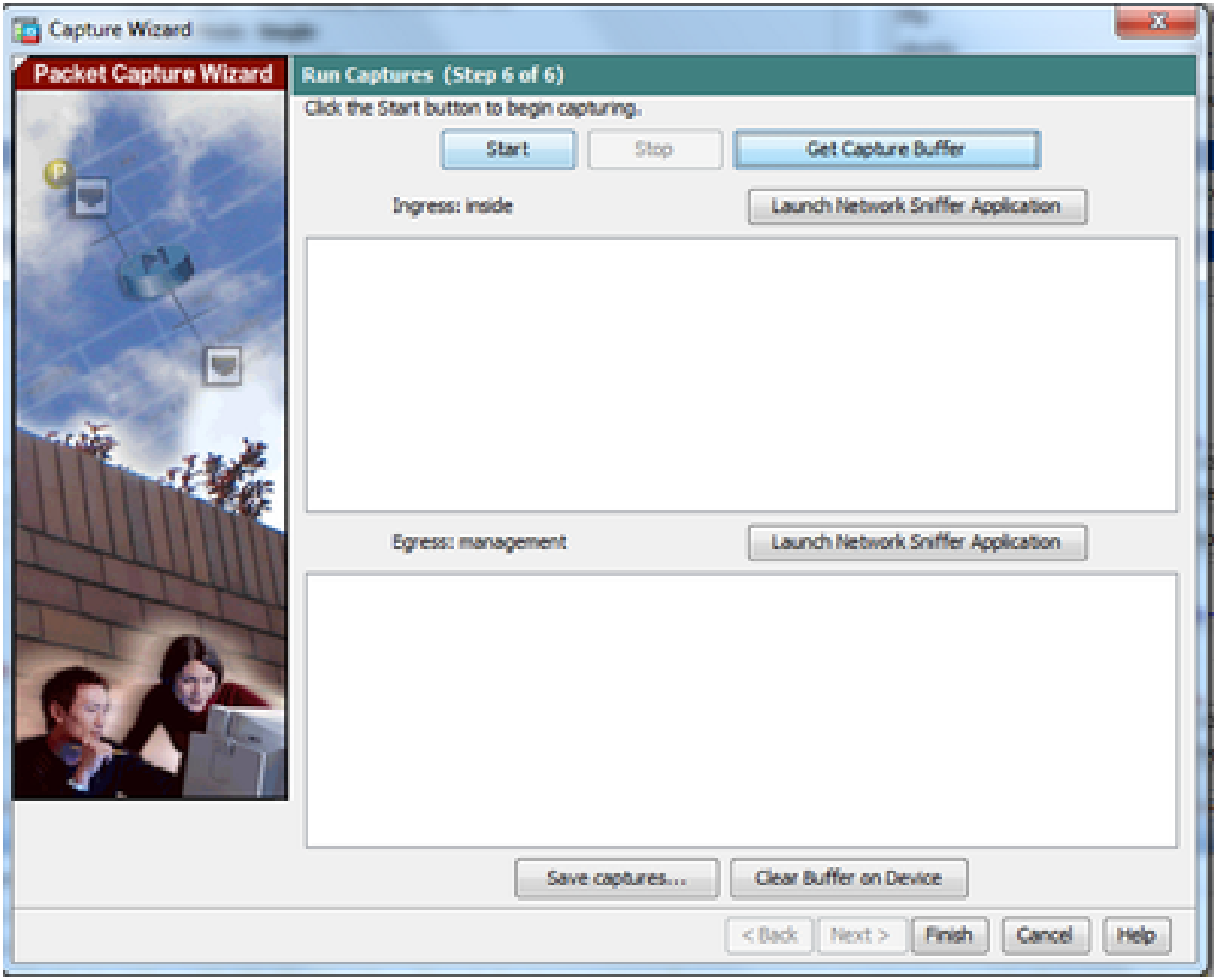
5. 3 انقر **Next**.

6.0 يدي اذه انافذة ال **Access-lists** أن ينبغي كنت شكلت علي ال ASA (so that that الربط ب رغب يكون قبض) ونوع الربط أن يكون قبض

6. 1 انقر **Next**.

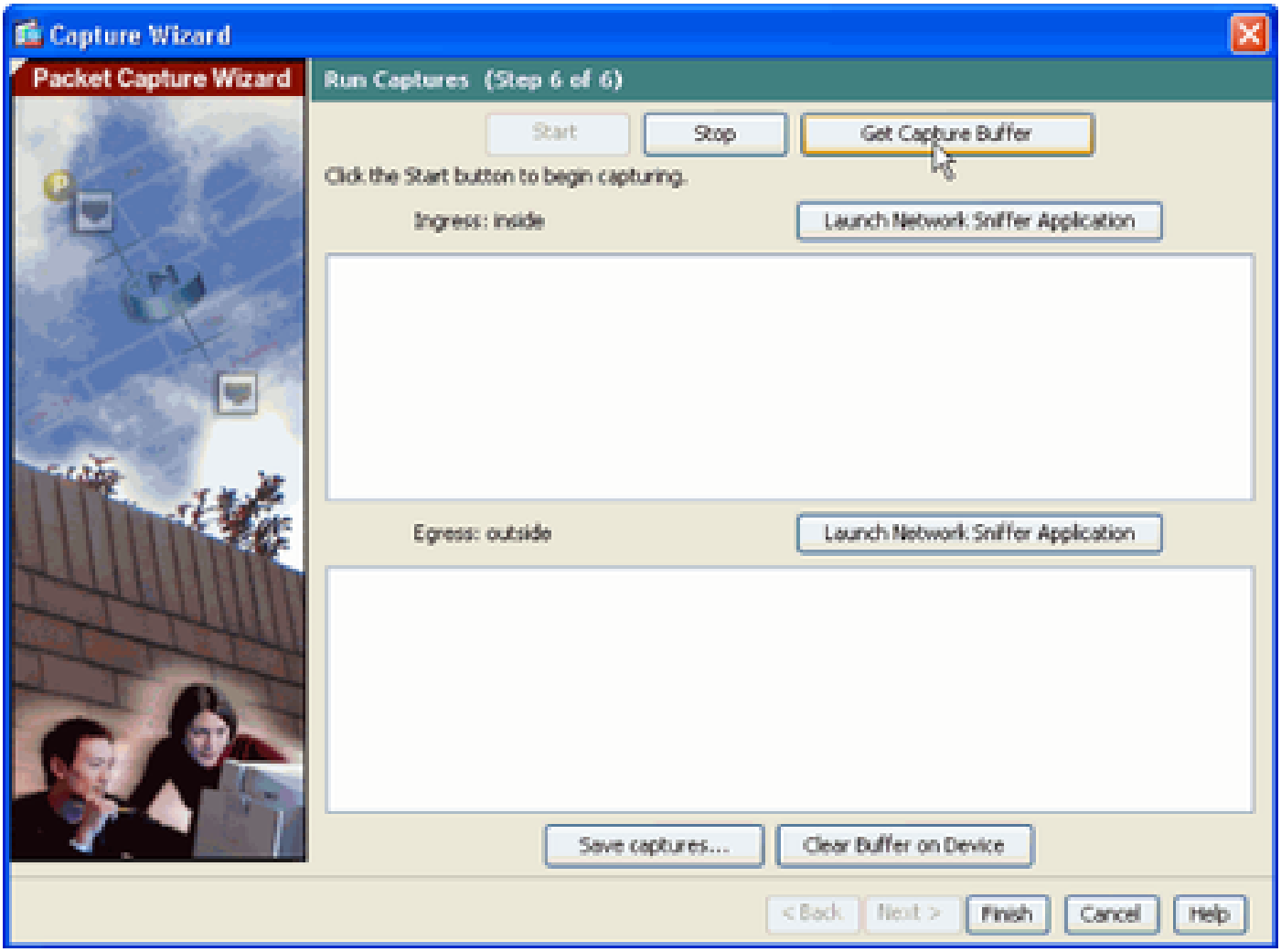


7. انقر **Start** لبدء التقاط الحزمة، كما هو موضح:



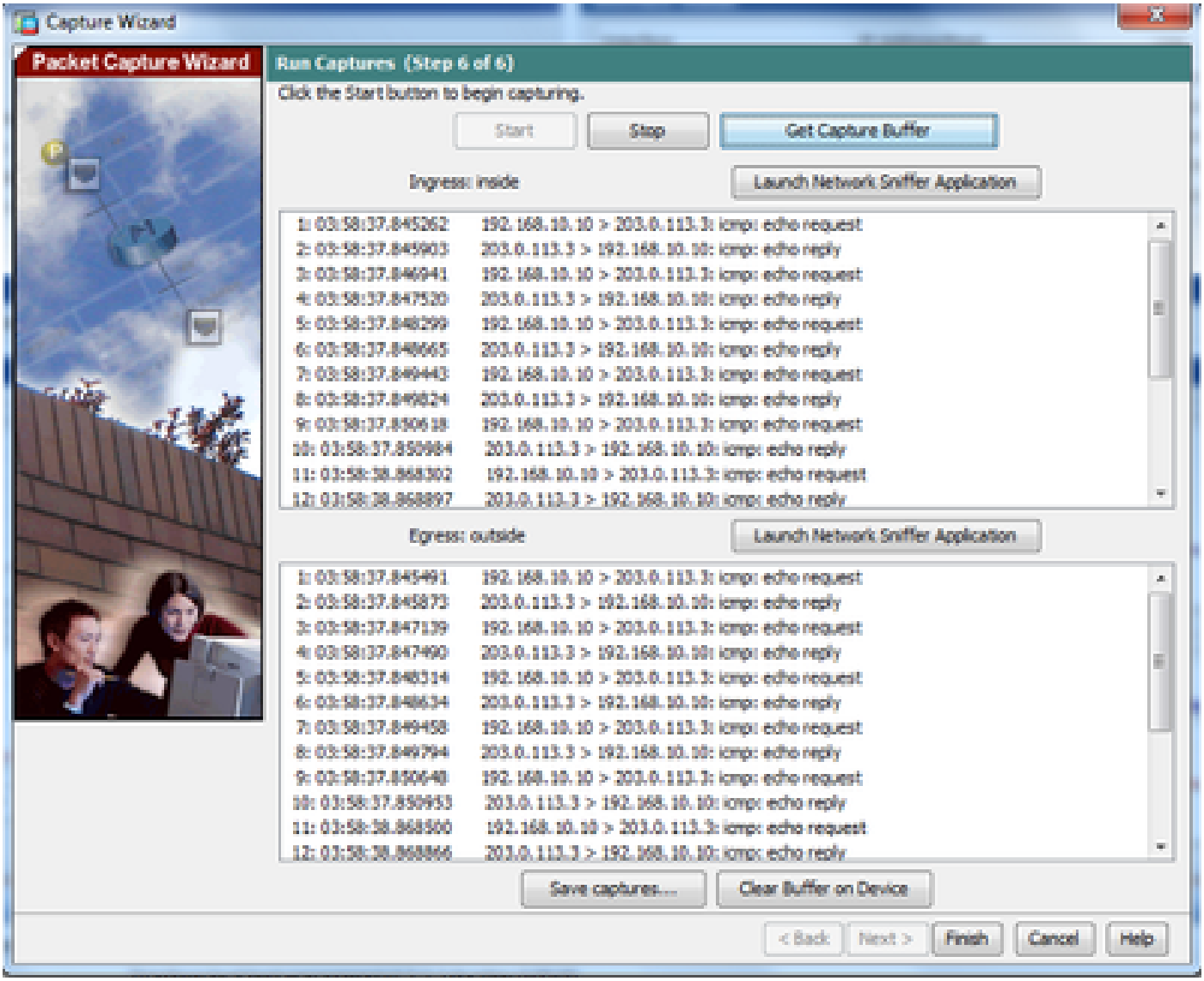
مع بدء التقاط الحزمة، حاول إختبار اتصال الشبكة الخارجية من الشبكة الداخلية حتى يتم التقاط الحزم التي تتدفق بين المص

8. انقر **Get Capture Buffer** لعرض الحزم التي يتم التقاطها بواسطة المخزن المؤقت للالتقاط ASA.



تظهر الحزم الملتقطة في هذه النافذة لكل من حركة مرور الدخول والخروج.

9. انقر **Save captures** لحفظ معلومات الالتقاط.

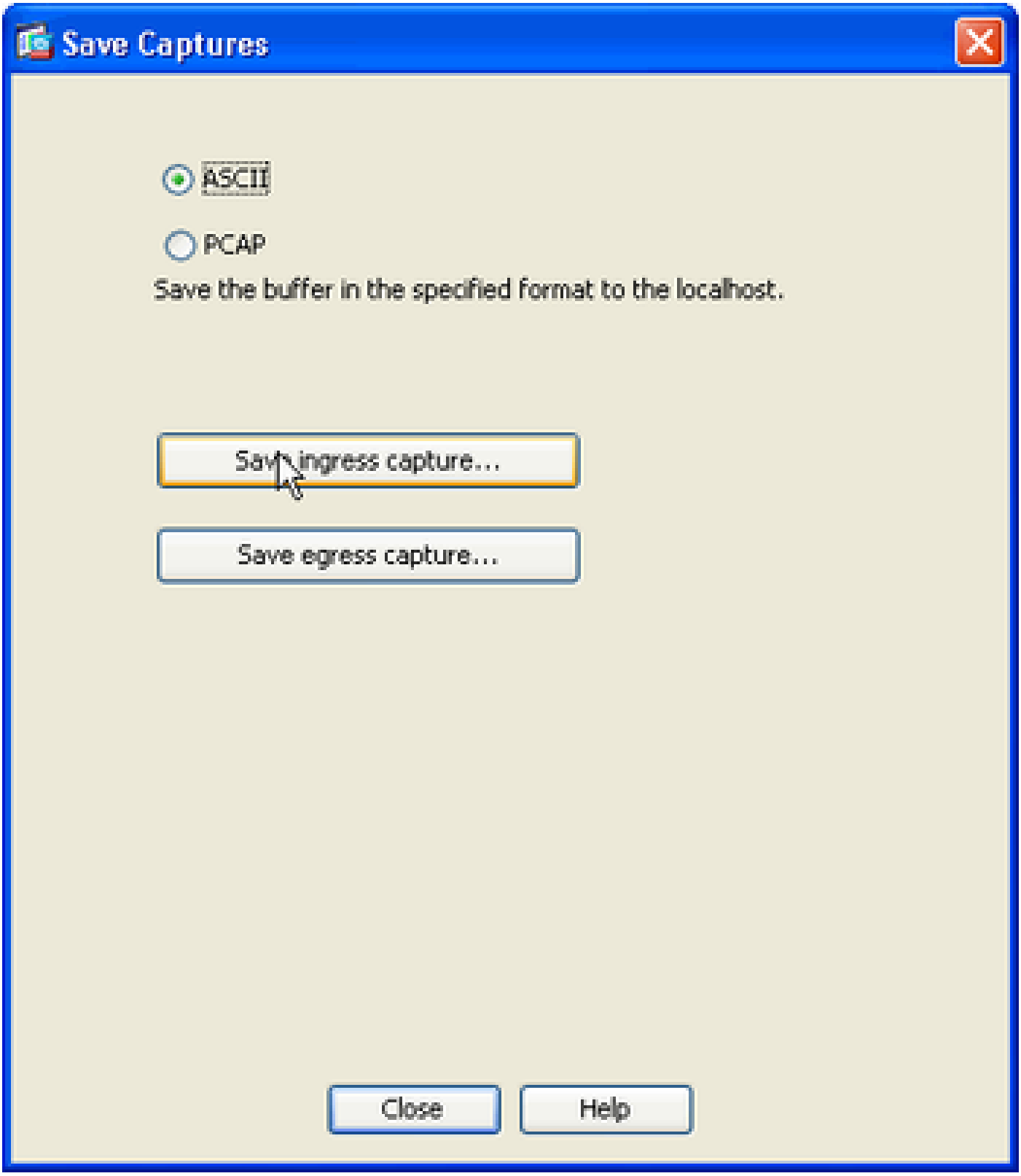


10.1 من **Save captures** النافذة، أختر التنسيق المطلوب الذي سيتم حفظ مخزن الالتقاط المؤقت به.

10.2 هذه إما **ASCII** أو **PCAP**. انقر زر الخيار الموجود بجوار أسماء التنسيق.

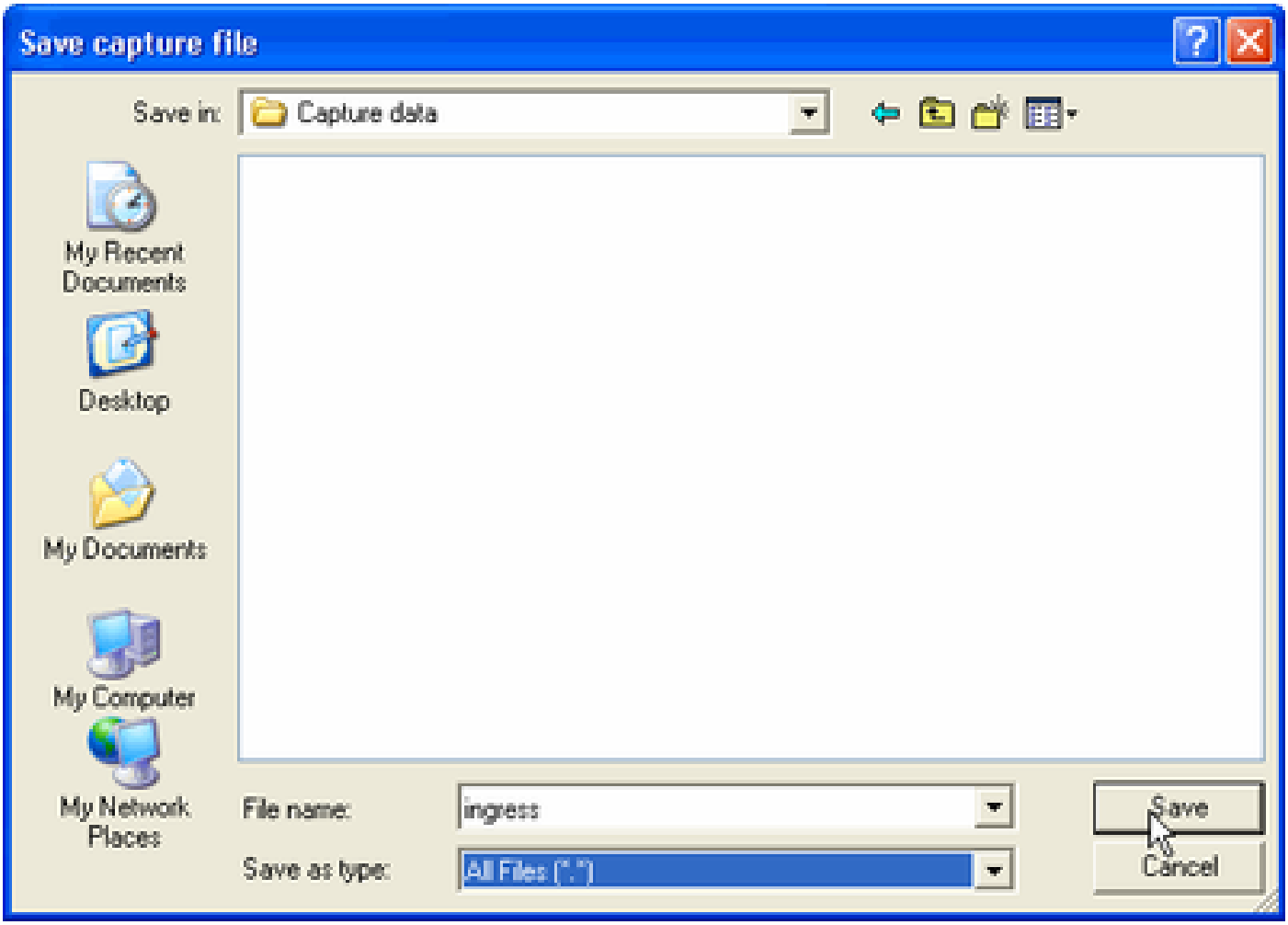
10.3 ثم انقر **Save ingress capture** أو **Save egress capture** حسب المطلوب.

يمكن فتح ملفات PCAP باستخدام محلل الالتقاط، مثل **Wireshark**، وهي الطريقة المفضلة.

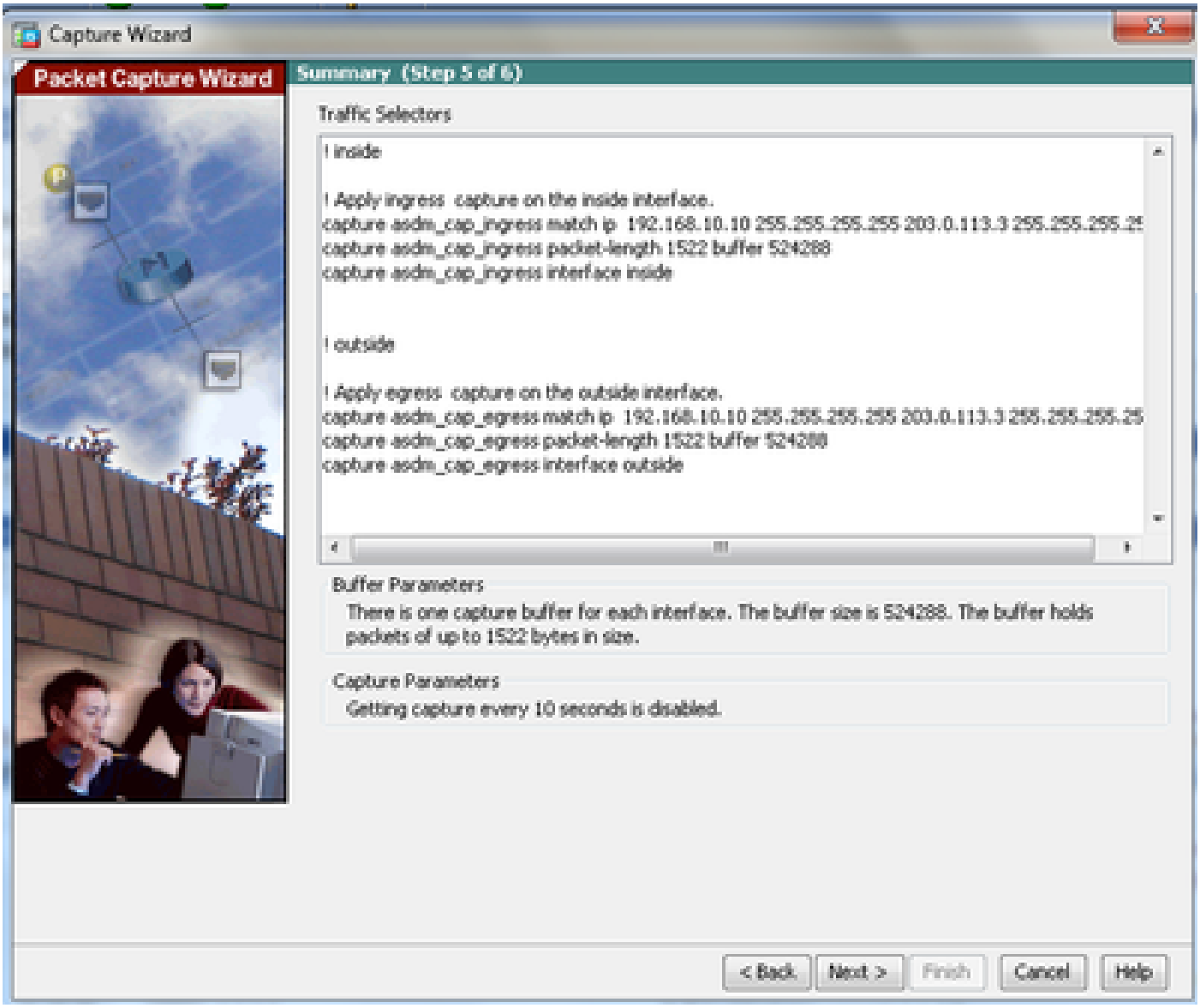


11.1 من **Save capture file** النافذة، قم بتوفير اسم الملف والمكان حيث يجب حفظ ملف الالتقاط.

11. 2 انقر **Save**.



12. انقر **Finish**.



يؤدي هذا إلى اكتمال إجراء التقاط حزمة GUI.

تكوين التقاط الحزم باستخدام CLI (واجهة سطر الأوامر)

أتمت هذا steps in order to شكلت الربط التقاط سمة على ال ASA مع ال CLI:

1. قم بتكوين الواجهات الداخلية والخارجية كما هو موضح في الرسم التخطيطي للشبكة باستخدام عنوان IP الصحيح ومستوي

2. ابدأ عملية التقاط الحزمة باستخدام الأمر capture في وضع EXEC ذي الامتيازات. في مثال التكوين هذا، يتم تعريف الالتقاط

<#root>

ASA#

```
capture capin interface inside match ip 192.168.10.10 255.255.255.255
 203.0.113.3 255.255.255.255
```

3. وعلى نحو مماثل، يتم تعريف الالتقاط المسمى **capout**. ربطه إلى القارن خارجي، وعينت مع ال **match** الكلمة المفتاح أن فقط ا

<#root>

ASA#

```
 capture capout interface outside match ip 192.168.10.10 255.255.255.255
 203.0.113.3 255.255.255.255
```

يبدأ ASA الآن في التقاط تدفق حركة المرور بين الواجهات. لإيقاف الالتقاط في أي وقت، أدخل الأمر no capture متبوعا باسم ا

فيما يلي مثال:

<#root>

```
no capture capin interface inside
no capture capout interface outside
```

أنواع الالتقاط المتاحة على ASA

يصف هذا القسم مختلف نوع الالتقاط أن يكون يتوفر على ال ASA.

- **asa_dataplane** - على قبض ربط على للولحة الخلفية ASA التي تمر بين ASA ووحدة تستخدم للولحة الخلفية، مثل وحدة ASA

<#root>

ASA#

cap asa_dataplace interface asa_dataplane

ASA#

show capture

capture asa_dataplace type raw-data interface asa_dataplane [Capturing - 0 bytes]

- **asp-drop** كود drop - يلتقط الحزم التي يتم إسقاطها من مسار الأمان السريع. يعين الشفرة الإسقاط نوع حركة المرور ا

<#root>

ASA#

capture asp-drop type asp-drop acl-drop

```
ASA#
```

show cap

```
ASA#
```

show capture asp-drop

```
 2 packets captured

 1: 04:12:10.428093       192.168.10.10.34327 > 10.94.0.51.15868: S
    2669456341:2669456341(0) win 4128 <mss 536> Drop-reason: (acl-drop)
    Flow is denied by configured rule
 2: 04:12:12.427330       192.168.10.10.34327 > 10.94.0.51.15868: S
    2669456341:2669456341(0) win 4128 <mss 536> Drop-reason: (acl-drop)
    Flow is denied by configured rule
 2 packets shown

ASA#
```

show capture asp-drop

```
 2 packets captured

 1: 04:12:10.428093       192.168.10.10.34327 > 10.94.0.51.15868: S
    2669456341:2669456341(0) win 4128 <mss 536> Drop-reason: (acl-drop)
    Flow is denied by configured rule
 2: 04:12:12.427330       192.168.10.10.34327 > 10.94.0.51.15868: S
    2669456341:2669456341(0) win 4128 <mss 536> Drop-reason: (acl-drop)
    Flow is denied by configured rule
 2 packets shown
```

- **ethernet-type** النوع - يحدد نوع Ethernet للالتقاط. تتضمن أنواع الإيثرنت المدعومة 8021Q، و ARP، و IP، و IP6، و LACP، و PPI

يوضح هذه المثال كيفية التقاط حركة مرور ARP:

<#root>

ASA#

cap arp ethernet-type ?

exec mode commands/options:
  802.1Q
  <0-65535> Ethernet type
  arp
  ip
  ip6
  pppoed
  pppoes
  rarp
  vlan

cap arp ethernet-type arp interface inside

ASA#

show cap arp

22 packets captured

   1: 05:32:52.119485   arp who-has 10.10.3.13 tell 10.10.3.12

2: 05:32:52.481862   arp who-has 192.168.10.123 tell 192.168.100.100
3: 05:32:52.481878   arp who-has 192.168.10.50 tell 192.168.100.10

   4: 05:32:53.409723   arp who-has 10.106.44.135 tell 10.106.44.244
   5: 05:32:53.772085   arp who-has 10.106.44.108 tell 10.106.44.248
   6: 05:32:54.782429   arp who-has 10.106.44.135 tell 10.106.44.244
   7: 05:32:54.784695   arp who-has 10.106.44.1 tell xx.xx.xx.xxx:

- **real-time** - يعرض الحزم الملتقطة باستمرار في الوقت الفعلي. لإنهاء التقاط حزمة في الوقت الفعلي، اضغط على

- هذا الخيار غير مدعوم عندما تستخدم **cluster exec capture** الأمر.

<#root>

ASA#

cap capin interface inside real-time

Warning: using this option with a slow console connection may
result in an excessive amount of non-displayed packets
due to performance limitations.

Use ctrl-c to terminate real-time capture

- **Trace** - يتتبع الحزم التي تم الاستيلاء عليها بطريقة مماثلة لميزة متعقب حزمة ASA.

<#root>

ASA#

cap in interface Webserver trace match tcp any any eq 80

// Initiate Traffic

1: 07:11:54.670299 192.168.10.10.49498 > 198.51.100.88.80: S
2322784363:2322784363(0) win 8192
<mss 1460,nop,wscale 2,nop,nop,sackOK>

Phase: 1

```
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in   0.0.0.0         0.0.0.0         outside

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group any in interface inside
access-list any extended permit ip any4 any4 log
Additional Information:

Phase: 5
Type: NAT
Subtype:
Result: ALLOW
Config:
object network obj-10.0.0.0
nat (inside,outside) dynamic interface
Additional Information:
Dynamic translate 192.168.10.10/49498 to 203.0.113.2/49498

Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type:
Subtype:
Result: ALLOW
Config:
```

```
Additional Information:

Phase: 9
Type: ESTABLISHED
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 10
Type:
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 11
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 12
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 13
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 41134, packet dispatched to next module

Phase: 14
Type: ROUTE-LOOKUP
Subtype: output and adjacency
Result: ALLOW
Config:
Additional Information:
found next-hop 203.0.113.1 using egress ifc outside
adjacency Active
next-hop mac address 0007.7d54.1300 hits 3170

Result:
output-interface: outside
output-status: up
output-line-status: up
Action: allow
```

ملاحظة: في ASA 9.10+، تلتقط أي كلمة أساسية الحزم بعناوين IPv4 فقط. تلتقط الكلمة الأساسية any6 حركة مرور IPv6 فقط.

هذه إعدادات متقدمة يمكن تكوينها باستخدام التقاط الحزم.

الرجاء مراجعة الدليل المرجعي للأوامر حول كيفية تعيينها.

- **ikev1/ikev2** - يلتقط معلومات بروتوكول Internet Key Exchange الإصدار 1 (IKEv1) أو IKEv2 فقط.
  - **isakmp** - على التقاط حركة مرور اقتران أمان الإنترنت وبروتوكول إدارة المفاتيح (ISAKMP) اتصالات VPN. ال يمتلك نظا
  - **lacp** - التقاط حركة مرور بروتوكول التحكم في تجميع الارتباطات (LACP). إذا تم تكوينها، فإن اسم الواجهة هو اسم الواجهة
  - **tls-proxy** - التقاط البيانات الواردة والصادرة التي تم فك تشفيرها من وكيل أمان طبقة النقل (TLS) على واجهة واحدة أو أ
  - **webvpn** - التقاط بيانات WebVPN لاتصال WebVPN معين.

تحذير: عند تمكين التقاط WebVPN، يؤثر ذلك على أداء جهاز الأمان. تأكد من تعطيل التقاط بعد أن تقوم بإنشاء م

الافتراضيات

هذه هي القيم الافتراضية لنظام ASA:

- النوع الافتراضي هو بيانات خام.
- حجم المخزن المؤقت الافتراضي هو 512 كيلوبايت.
- نوع إيثرنت الافتراضي هو حزم IP.
- طول الحزمة الافتراضي هو 1،518 بايت.

عرض الحزم الملتقطة

على ال ASA

دخلت in order to شاهدت الربط على قبض، العرض التقاط أمر يتبعه ال capture إسم. يوفر هذه القسم مخرجات الأمر **show** لمحتويات المخ

<#root>

ASA#

show cap capin

```
 8 packets captured

 1: 03:24:35.526812       192.168.10.10 > 203.0.113.3: icmp: echo request
 2: 03:24:35.527224       203.0.113.3 > 192.168.10.10: icmp: echo reply
 3: 03:24:35.528247       192.168.10.10 > 203.0.113.3: icmp: echo request
 4: 03:24:35.528582       203.0.113.3 > 192.168.10.10: icmp: echo reply
 5: 03:24:35.529345       192.168.10.10 > 203.0.113.3: icmp: echo request
 6: 03:24:35.529681       203.0.113.3 > 192.168.10.10: icmp: echo reply
 7: 03:24:57.440162       192.168.10.10 > 203.0.113.3: icmp: echo request
 8: 03:24:57.440757       203.0.113.3 > 192.168.10.10: icmp: echo reply
```

يعرض **show capture capout** الأمر محتويات المخزن المؤقت للالتقاط المسمى **capout**:

<#root>

ASA#

show cap capout

```
 8 packets captured

 1: 03:24:35.526843       192.168.10.10 > 203.0.113.3: icmp: echo request
 2: 03:24:35.527179       203.0.113.3 > 192.168.10.10: icmp: echo reply
 3: 03:24:35.528262       192.168.10.10 > 203.0.113.3: icmp: echo request
 4: 03:24:35.528567       203.0.113.3 > 192.168.10.10: icmp: echo reply
 5: 03:24:35.529361       192.168.10.10 > 203.0.113.3: icmp: echo request
 6: 03:24:35.529666       203.0.113.3 > 192.168.10.10: icmp: echo reply
 7: 03:24:47.014098       203.0.113.3 > 203.0.113.2: icmp: echo request
 8: 03:24:47.014510       203.0.113.2 > 203.0.113.3: icmp: echo reply
```

التنزيل من ASA للتحليل دون اتصال

هناك طريقتان لتنزيل التقاط الحزمة للتحليل دون اتصال:

1. انتقل إلى

   https://<ip_of_asa>/admin/capture/<capture_name>/pcap

   على أي متصفح.

تلميح: إذا تركت **pcap** الكلمة الأساسية، حينئذ يتم توفير ما يعادل مخرجات **show capture <cap_name>** الأمر فقط.

---

1. أدخل الأمر copy capture وبروتوكول نقل الملفات المفضل لديك لتنزيل الالتقاط:

```
copy /pcap capture:<capture-name> tftp://<server-ip-address>
```

تلميح: عند أستكشاف أخطاء ام وإصلاحها باستخدام التقاط الحزم، توصي Cisco بتنزيل عمليات الالتقاط للتحليل د

مسح التقاط

دخلت in order to أمسحت الالتقاط مصد، **clear capture** <**capture-name**> الأمر:

```
<#root>

ASA#
```

show capture

```
 capture capin type raw-data interface inside [Capturing - 8190 bytes]
 match icmp any any
 capture capout type raw-data interface outside [Capturing - 11440 bytes]
 match icmp any any

 ASA#
```

clear cap capin

```
 ASA#
```

clear cap capout

```
ASA#
```

```
show capture
```

```
capture capin type raw-data interface inside [Capturing - 0 bytes]
match icmp any any
capture capout type raw-data interface outside [Capturing - 0 bytes]
match icmp any any
```

أدخل **clear capture /all** الأمر لمسح المخزن المؤقت لجميع عمليات الالتقاط:

<#root>

```
ASA#
```

```
clear capture /all
```

إيقاف التقاط

الطريقة الوحيدة لإيقاف التقاط على ASA هي تعطيله بالكامل باستخدام هذا الأمر:

```
no capture <capture-name>
```

التحقق من الصحة

ال يوجد حالياً إجراء للتحقق من صحة هذه التكوين.

استكشاف الأخطاء وإصلاحها

هناك حالياً ما من خاص أستكشاف الأخطاء وإصلاحها معلومة يتوفر ل هذه تشكيل.

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).