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

ال يقيد هذا وثيقة إلى خاص جهاز أو برمجية صيغة.

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

يوضح هذا المستند كيفية تكوين **Cisco Adaptive Security Appliance (ASA) Next-Generation Firewall** من أجل التقاط الحزم المطلوبة باستخدام 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 الممكن إنشاء لقطات متعددة لتحليل أنواع مختلفة من حركة المرور على واجهات متعددة.

التكوين

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

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:

التكوينات

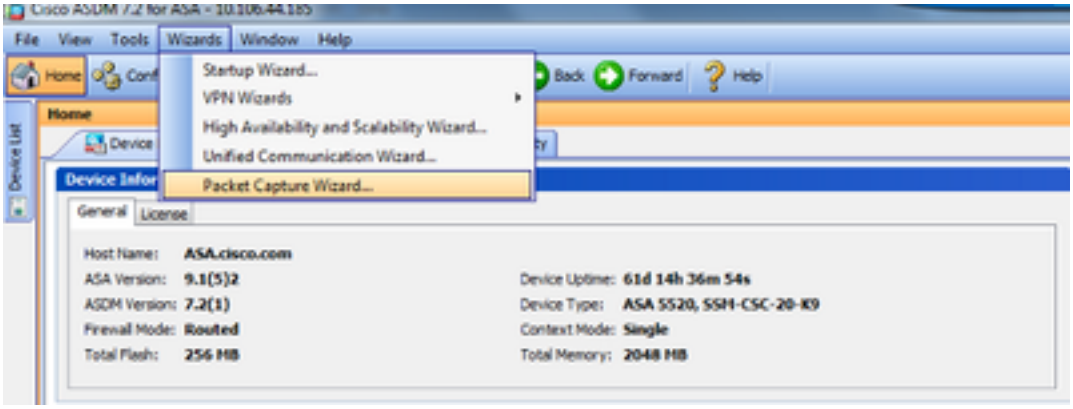
ال ip ليس عنوان خطة يستعمل في هذا تشكيل قانونيا routable على الإنترنت. هم rfc 1918 عنوان أن يكون استعملت في مختبر بيئة.

تكوين التقاط الحزم باستخدام ASDM

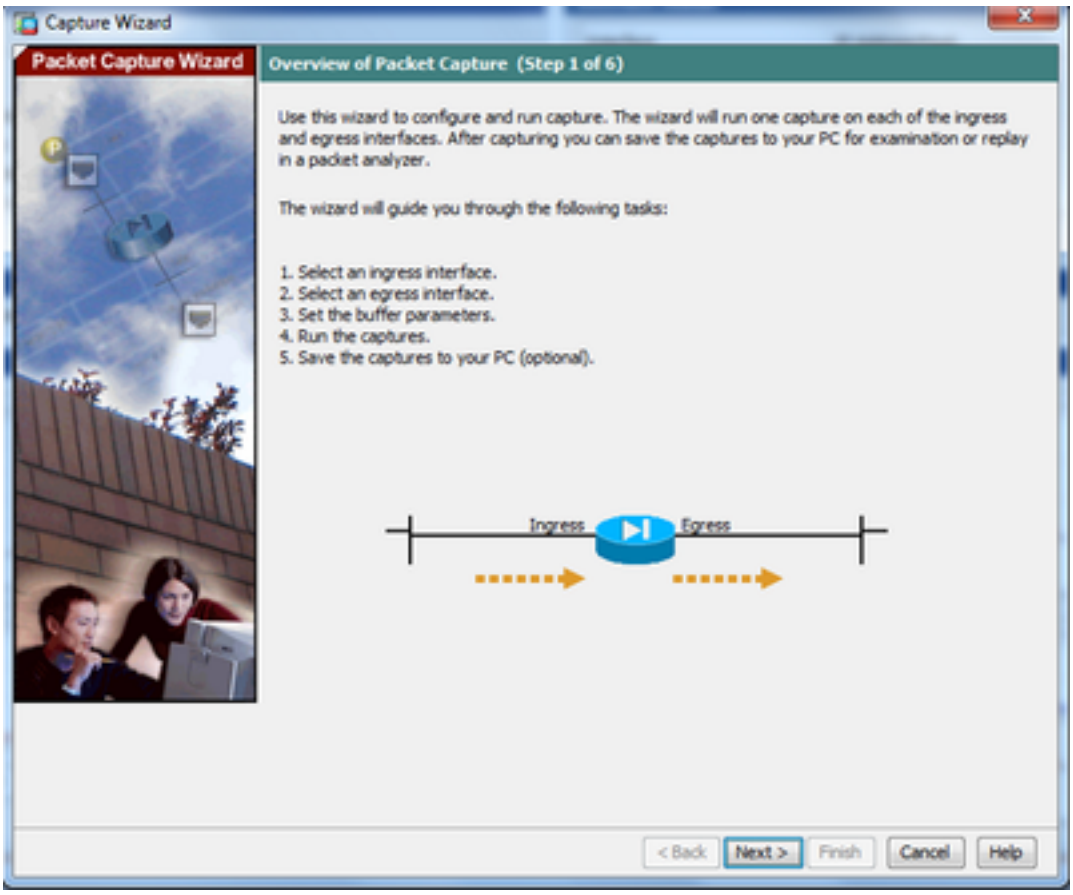
يتم إستخدام مثال التكوين هذا في التقاط الحزم التي يتم إرسالها أثناء إختبار الاتصال من المستخدم1 (داخل الشبكة) إلى الموجه1 (خارج الشبكة).

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

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



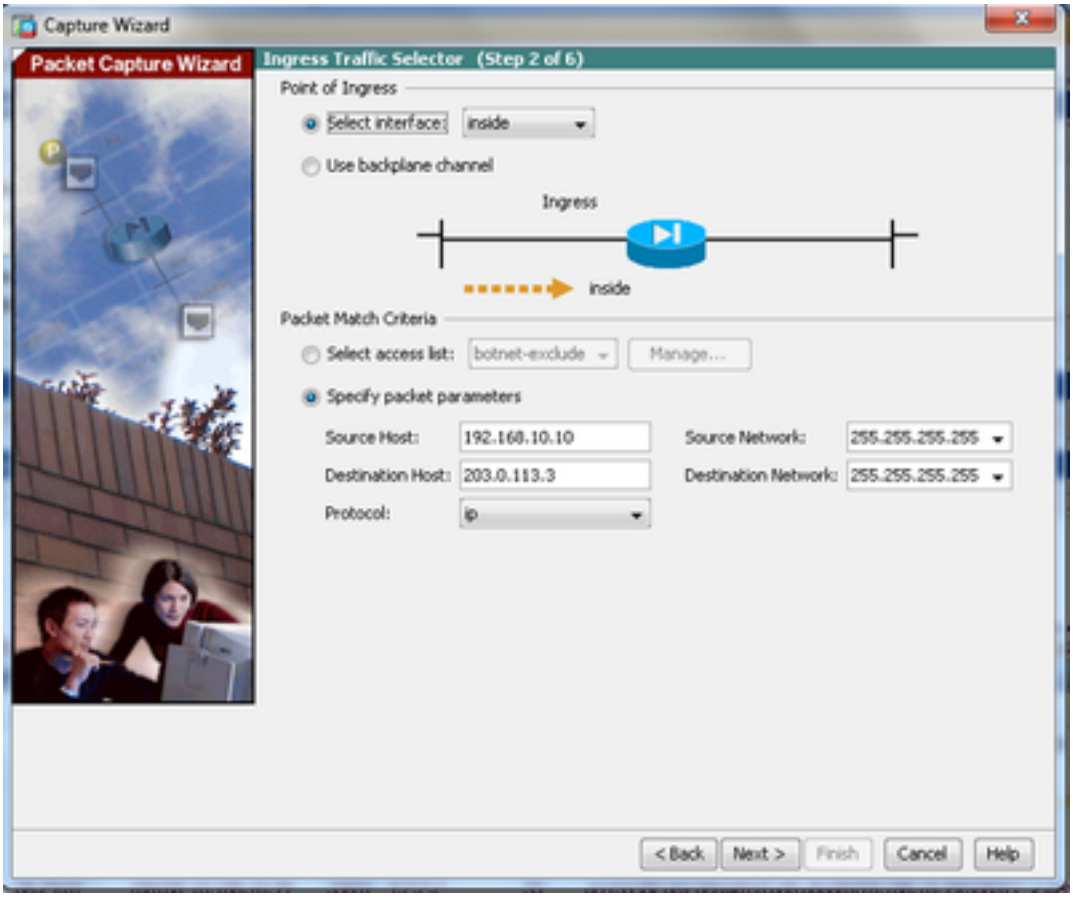
2 - **Capture Wizard** يفتح. انقر **Next**.



3.0 في النافذة الجديدة، قم بتوفير المعلومات التي يتم إستخدامها في التقاط حركة مرور الدخل.

3.1 تحديد **inside** من أجل **Ingress Interface** وتوفر عناوين IP للمصدر والوجهة للحزم التي سيتم التقاطها، مع قناع الشبكة الفرعية الخاص بها، في المساحة المقابلة المقدمة.

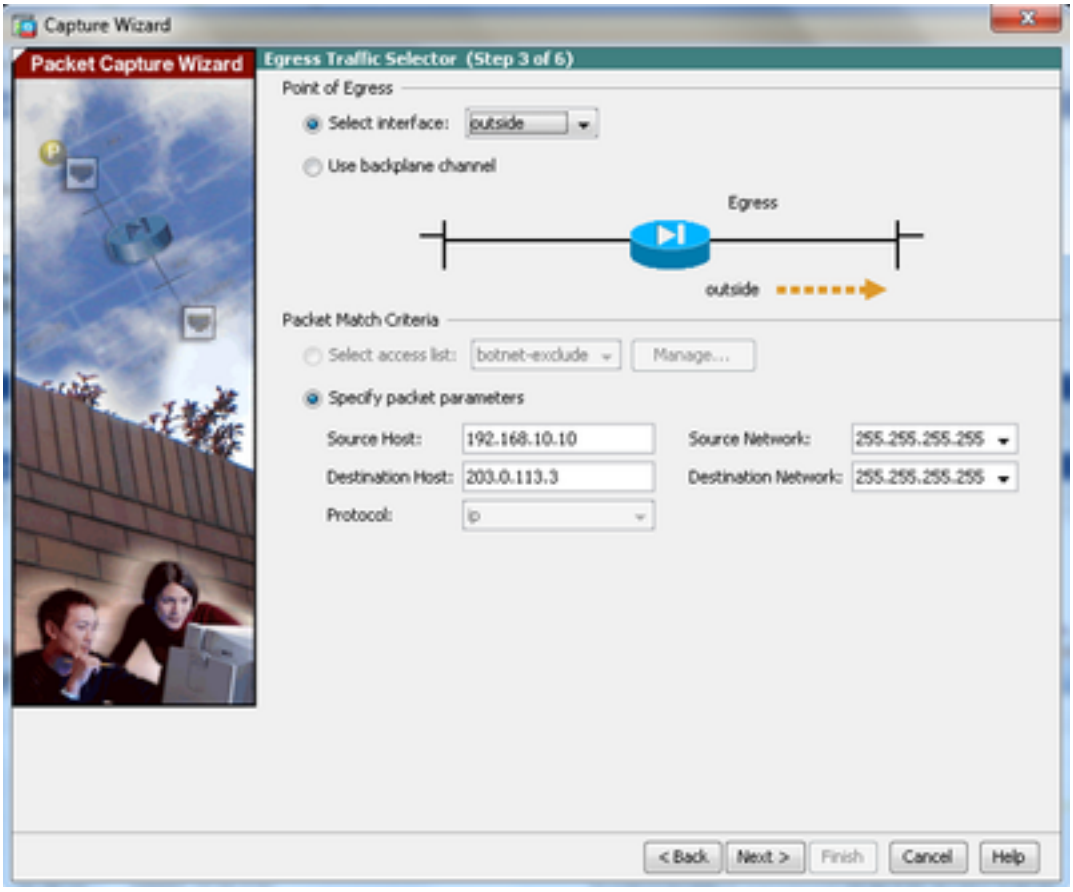
3.2 أختر نوع الحزمة التي سيتم الاستيلاء عليها بواسطة ASA (IP هو نوع الحزمة المختارة هنا)، كما هو موضح:



3.3 انقر **Next.**

4.1 تحديد **outside** من أجل **Egress Interface** وتوفر عناويني IP المصدر والوجهة، مع قناع الشبكة الفرعية الخاص بها، في الفراغات ذات الصلة المقدمة.

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



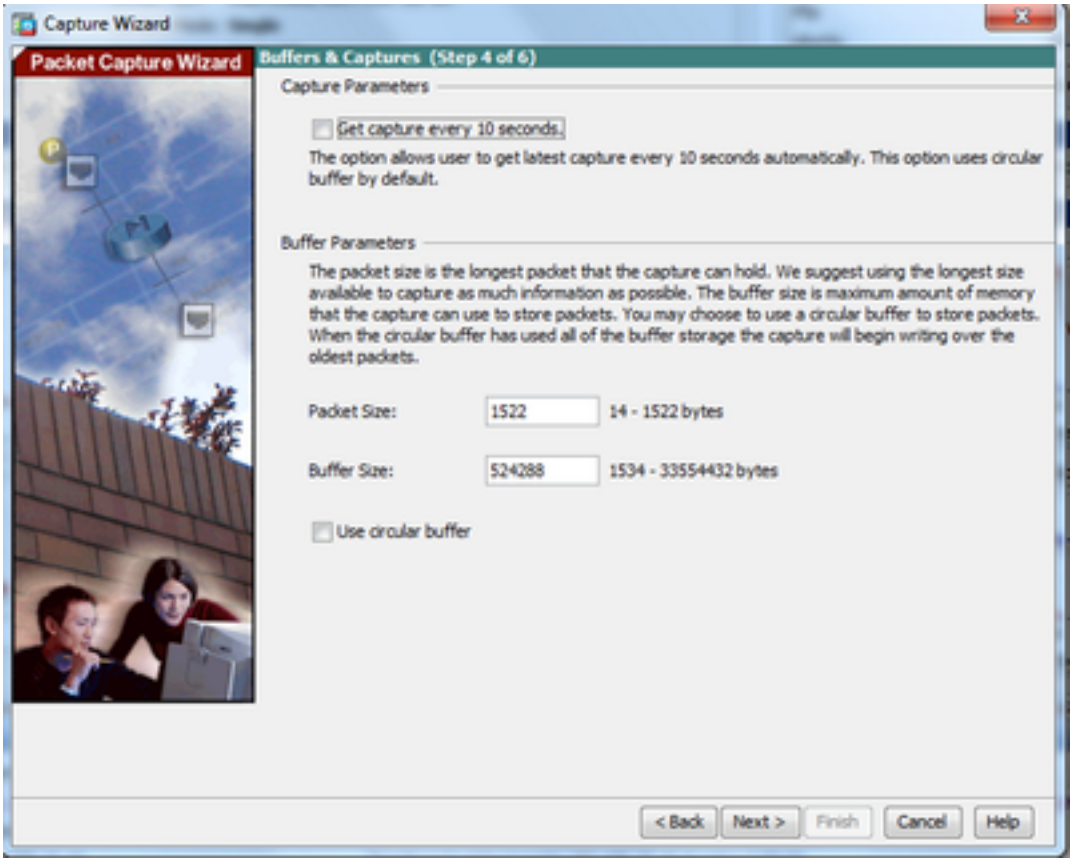
4.2 انقر **Next**.

5.1 أدخل الرقم المناسب **Packet Size** و **Buffer Size** في الحيز المخصص لكل منها. هذه البيانات مطلوبة حتى يحدث االلتقاط.

5.2 تحقق من **Use circular buffer** مربع االستخدام خيار مخزن مؤقت دائري. المخازن المؤقتة الدائرية ال يتم ملؤها أبدا.

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

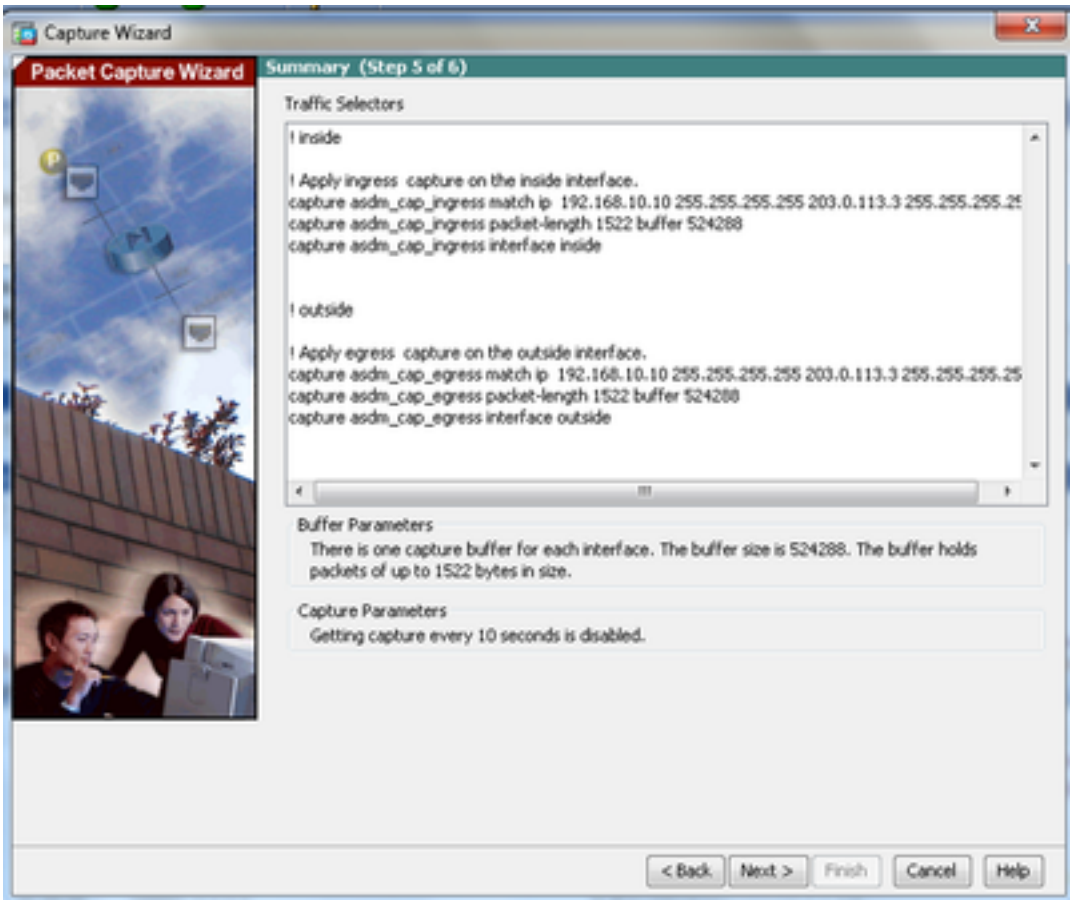
في هذا المثال، ال يتم إستخدام مخزن مؤقت دائري، لذلك لم يتم تحديد خانة الاختيار.



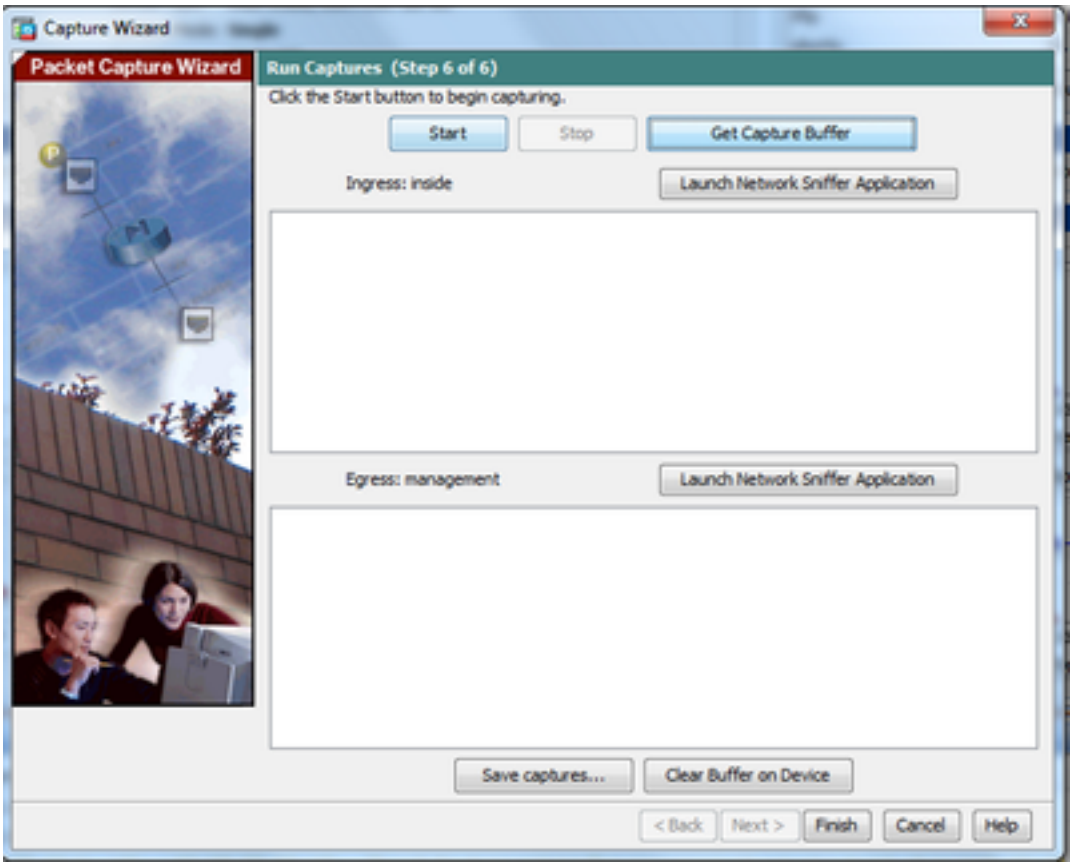
5.3 انقر **Next**.

6. 0 تعرض هذه النافذة **Access-lists** أن ينبغي كنت شكلت على ال ASA (so that the رغب ربط يكون التقطت) ونوع الربط أن يكون قبض (ip ربط يكون التقطت في هذا مثال).

6.1 انقر **Next**.

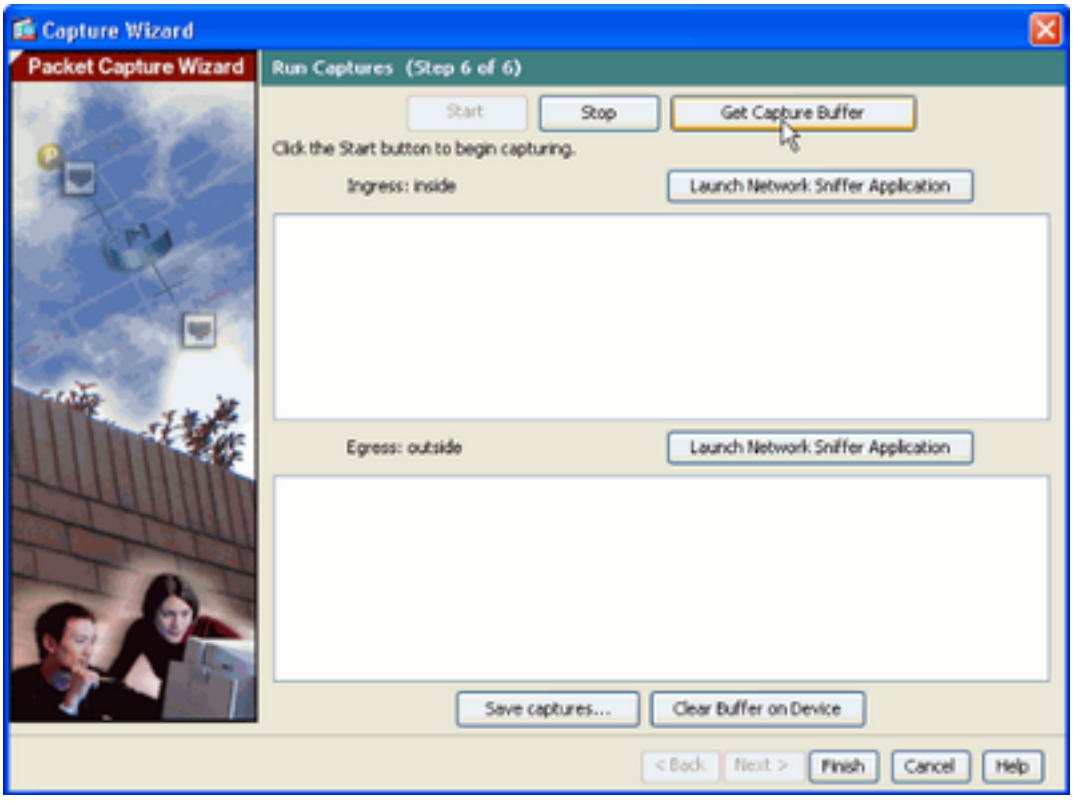


7. انقر فوق **Start** لبدء التقاط الحزمة، كما هو موضح:



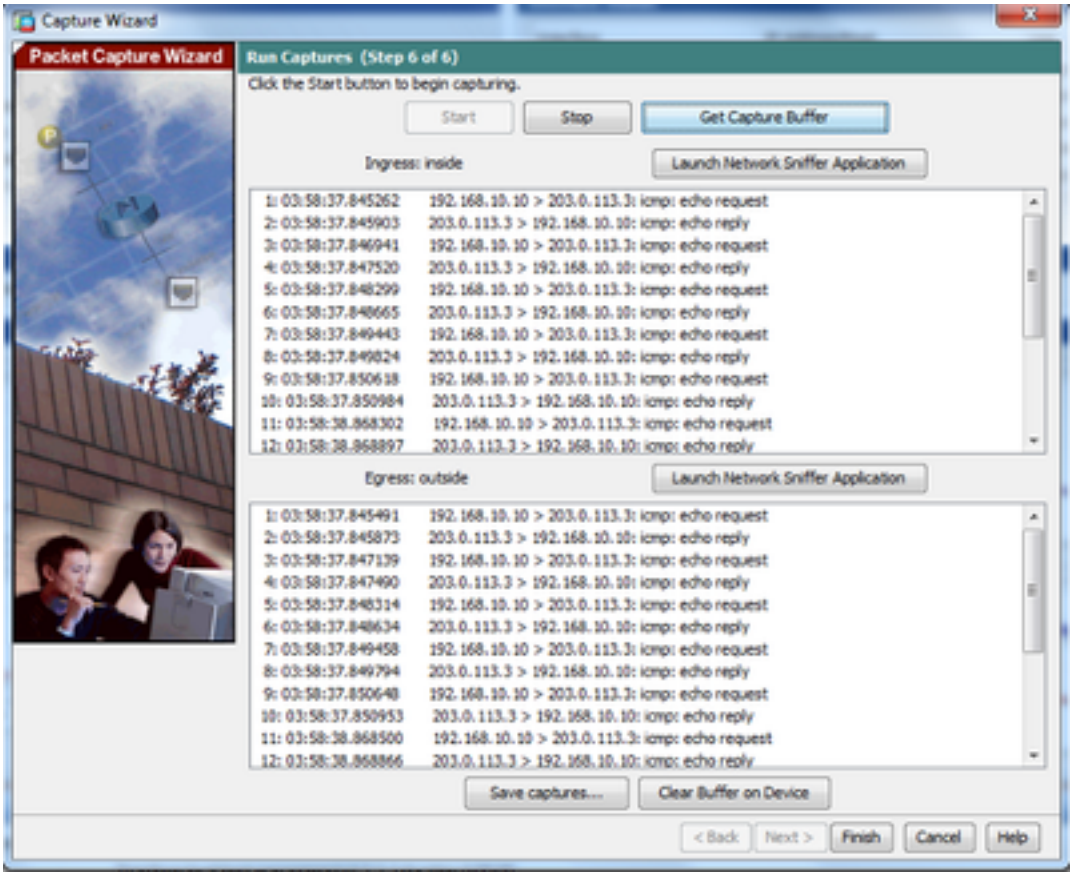
مع بدء التقاط الحزمة، حاول إختبار اتصال الشبكة الخارجية من الشبكة الداخلية حتى يتم التقاط الحزم التي تتدفق بين المصدر والوجهة عناوين IP بواسطة المخزن المؤقت للالتقاط ASA.

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



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

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

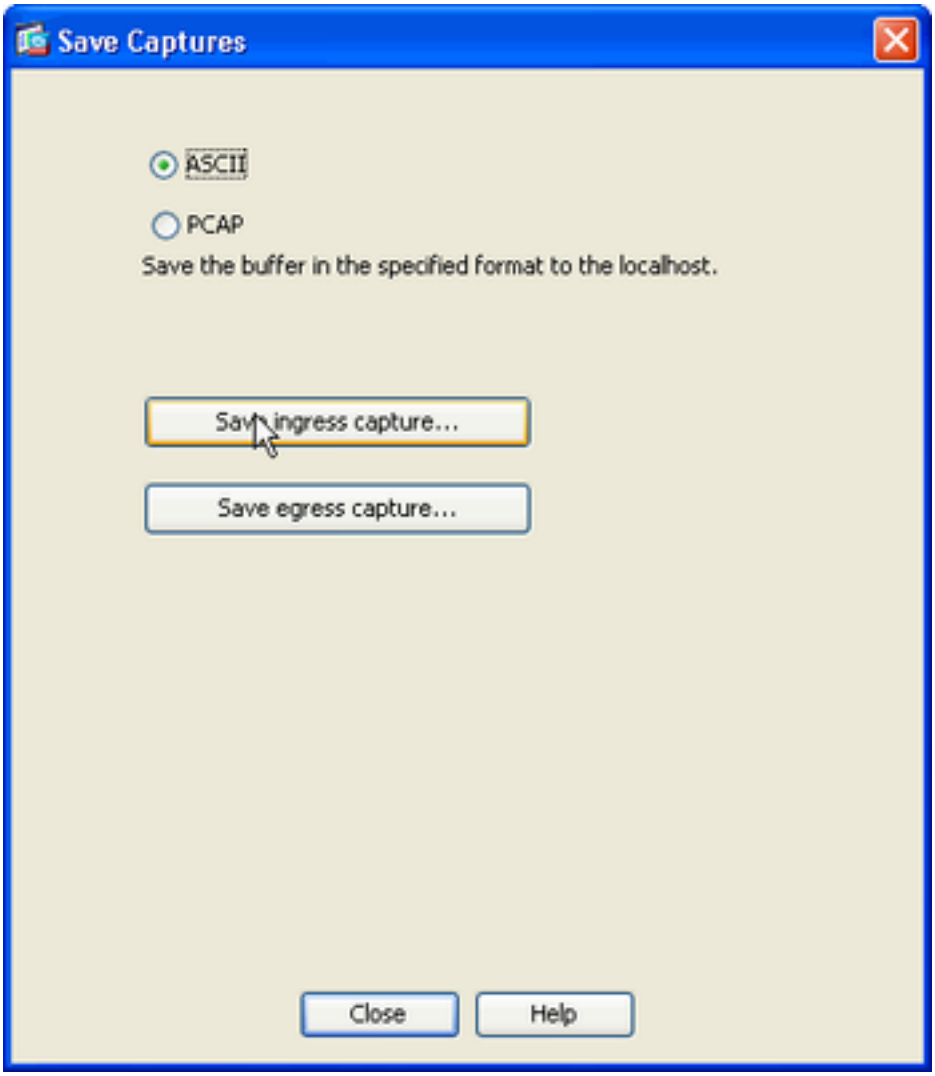


10. 1 من موقع **Save captures** أختر التنسيق المطلوب الذي سيتم حفظ مخزن الالتقاط المؤقت به.

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

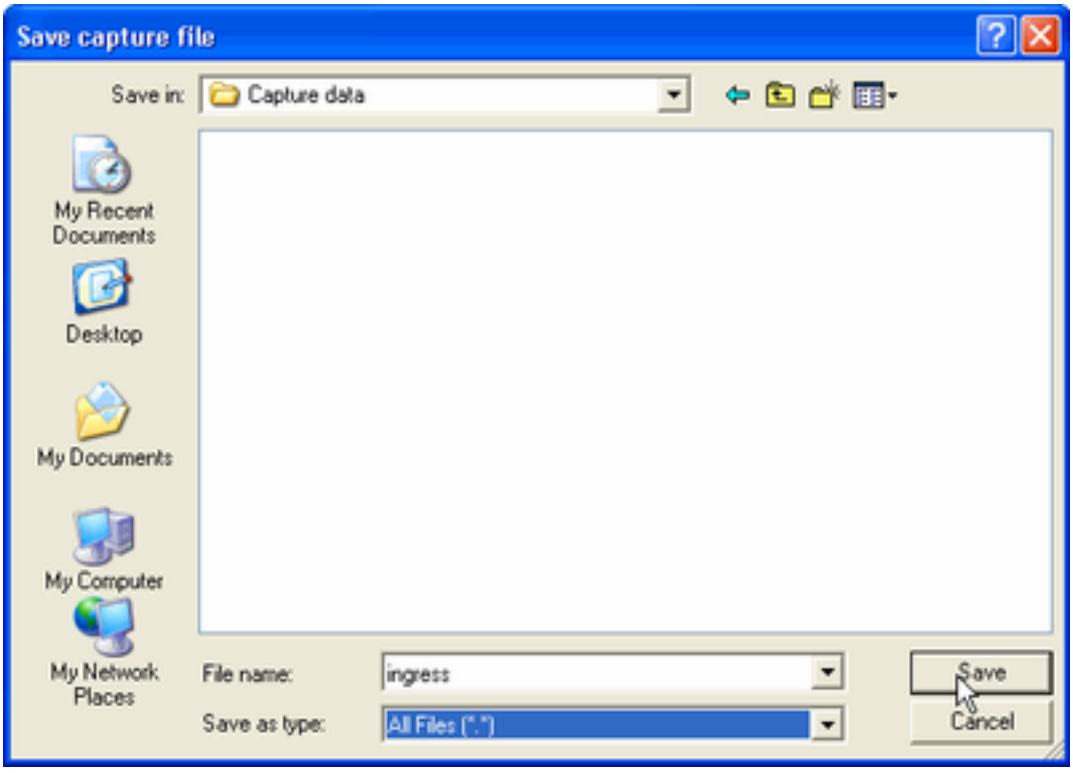
10.3 ثم انقر **Save ingress capture** أو **Save egress capture** كما هو مطلوب.

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

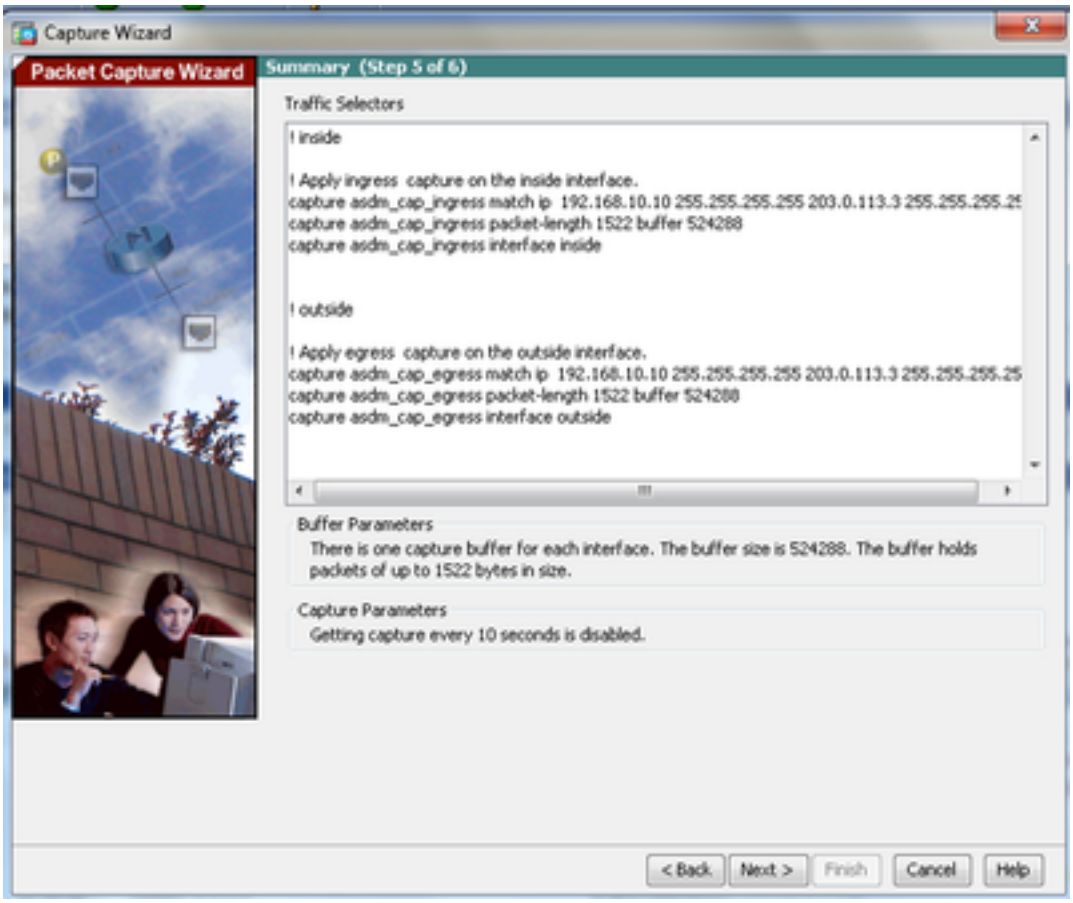


11.1 من موقع **Save capture file** نافذة، قم بتوفير اسم الملف والمكان حيث يتم حفظ ملف الالتقاط.

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 الـ ASA مع الـ CLI:

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

2. ابدأ عملية التقاط الحزمة باستخدام الأمر capture في وضع EXEC ذي الامتيازات. في هذا المثال التكوين، يتم تعريف الالتقاط المسمى **capin**. ربطه إلى القارن **الداخلي**، وعينت مع **الـ match** الكلمة المفتاح أن فقط الربط أن يطابق الحركة مرور الفائدة التقطت:

```
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 **الخارجي**، وعينت مع **الـ match** الكلمة المفتاح أن فقط الربط أن يطابق الحركة مرور الفائدة التقطت:

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

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

فيما يلي مثال:

```
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 الـ ASA.

- **asa_dataplane** - على قبض ربط على الوحة الخلفية ASA التي تمر بين ASA ووحدة ASA CX أو IPS النمطية، مثل وحدة تستخدم الوحة الخلفية.

```
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 - التقاط الحزم التي تم إسقاطها من مسار الأمان السريع. تعيين الشفرة الإسقاط نوع حركة المرور التي تم إسقاطها من خلال مسار الأمان السريع.

```
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 VLAN، و RARP، و PPPoS، و PPPoED، و LACP، و IP6، و IP، و ARP، و 8021Q.

يوضح هذا المثال كيفية التقاط حركة مرور ARP:

```
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 المطقطة باستمرار في الوقت الفعلي. إنهاء التقاط حزمة في الوقت الفعلي، اضغط على Ctrl-C. إزالة الالتقاط بشكل دائم، أستخدم الصيغة no من الأمر هذا.
- ال يتم دعم هذا الخيار عند إستخدام **cluster exec capture** erasecat4000_flash:.

```
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.

```
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 البيانات التي يتم معالجتها عبر بروتوكول IPv6.

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) لاتصالات VPN. لا يمتلك نظام ISAKMP الفرعي حق الوصول إلى بروتوكولات الطبقة العليا. الالتقاط هو التقاط زائف، مع الطبقات المادية، IP، و UDP مجمعة للحصول على رأس PCAP. يتم الحصول على عناوين النظير من تبادل SA ويتم تخزينها في طبقة IP.
- **lacp** - التقاط حركة مرور بروتوكول التحكم في تجميع الارتباطات (LACP). إذا تم تكوينها، فإن اسم الواجهة هو اسم الواجهة الفعلي. وهذا مفيد عندما تعمل مع EtherChannels in order to تعيين السلوك الحالي لـ LACP.
- **tls-proxy** - التقاط البيانات الواردة والصادرة التي تم فك تشفيرها من وكيل أمان طبقة النقل (TLS) على واجهة واحدة أو أكثر.
- **webvpn** - التقاط بيانات WebVPN لاتصال WebVPN معين.

تحذير: عند تمكين التقاط WebVPN، يؤثر ذلك على أداء جهاز الأمان. تأكد من تعطيل الالتقاط بعد أن يتم إنشاء ملفات الالتقاط المطلوبة لاستكشاف الأخطاء وإصلاحها.

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 الـ ASA

in order to تشاهد الربط على قبض، العرض التقاط أمر يتبعه الـ capture إسم. يوفر هذا القسم مخرجات الأمر **show** لمحتويات المخزن المؤقت للالتقاط. يعرض الأمر **show capture capin** محتويات المخزن المؤقت للالتقاط المسمى **capin**:

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

```
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>/pcapعلى أي متصفح.

   تلميح: إذا تركت **pcap** الكلمة الأساسية، ثم المكافئ فقط من **show capture** يتم توفير إخراج الأمر.

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 دون اتصال.

مسح التقاط

لمسح مخزن الالتقاط المؤقت، أدخل **clear capture** :

```
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** أمر in order to مسح المخزن المؤقت لكل االلتقاط:

```
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 هذا التكوين.

استكشاف الأخطاء وإصالحها

هناك حاليا ما من خاص أستكشاف الأخطاء وإصالحها معلومة يتوفر ل هذا 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).