

Configuration des captures de paquets ASA avec CLI et ASDM

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Produits connexes](#)

[Informations générales](#)

[Configurer](#)

[Diagramme du réseau](#)

[Configurations](#)

[Configuration de la capture de paquets avec l'ASDM](#)

[Configuration de la capture de paquets avec la CLI](#)

[Types de capture disponibles sur l'ASA](#)

[Valeurs par défaut](#)

[Afficher les paquets capturés](#)

[Sur l'ASA](#)

[Téléchargement à partir de l'ASA for Offline Analysis](#)

[Effacer une capture](#)

[Arrêter une capture](#)

[Vérifier](#)

[Dépannage](#)

Introduction

Ce document décrit comment configurer le pare-feu Cisco ASA pour capturer les paquets souhaités avec l'ASDM ou l'interface de ligne de commande.

Conditions préalables

Exigences

Cette procédure suppose que l'ASA est entièrement opérationnel et qu'il est configuré afin de permettre à Cisco ASDM ou à l'interface de ligne de commande d'apporter des modifications à la configuration.

Composants utilisés

Ce document n'est pas limité à des versions matérielles ou logicielles spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Produits connexes

Cette configuration est également utilisée avec les produits Cisco suivants :

- Cisco ASA versions 9.1(5) et ultérieures
- Cisco ASDM version 7.2.1

Informations générales

Ce document décrit comment configurer le pare-feu de nouvelle génération Cisco Adaptive Security Appliance (ASA) afin de capturer les paquets souhaités avec Cisco Adaptive Security Device Manager (ASDM) ou l'interface de ligne de commande (CLI) (ASDM).

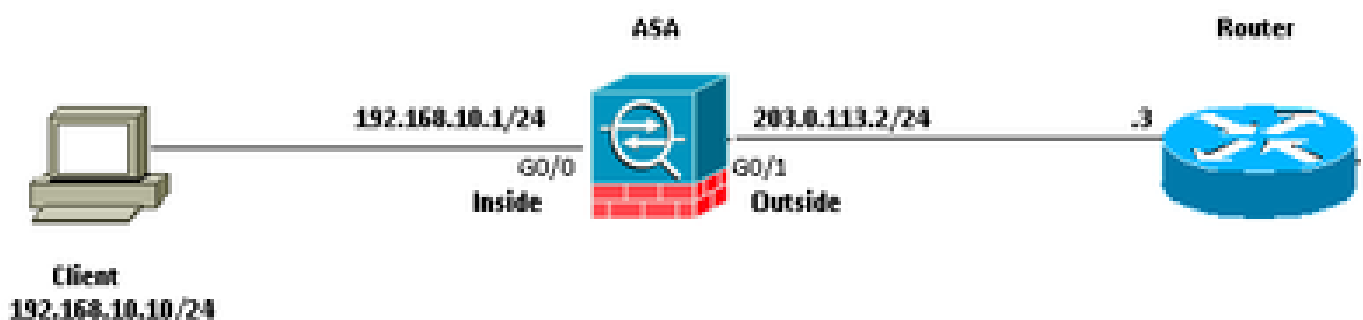
Le processus de capture de paquets est utile pour dépanner les problèmes de connectivité ou surveiller les activités suspectes. En outre, il est possible de créer plusieurs captures afin d'analyser différents types de trafic sur plusieurs interfaces.

Configurer

Cette section fournit des informations permettant de configurer les fonctionnalités de capture de paquets décrites dans ce document.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Configurations

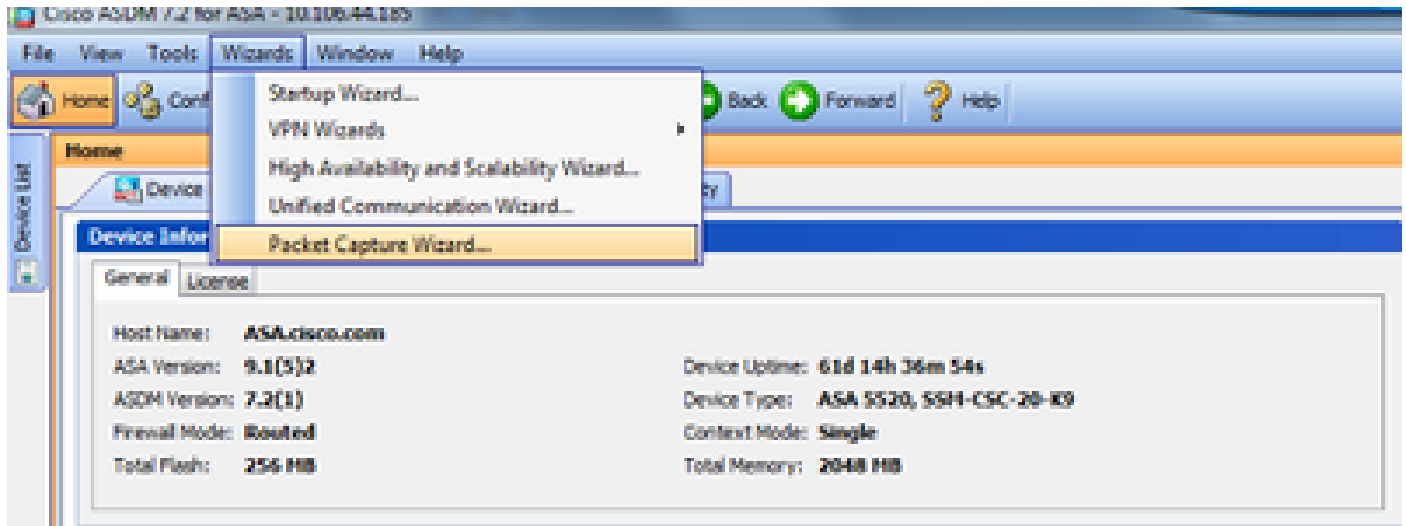
Les systèmes d'adresse IP utilisés dans cette configuration ne sont pas légalement routables sur Internet. Ce sont des adresses RFC 1918 qui sont utilisées dans un environnement de laboratoire.

Configuration de la capture de paquets avec l'ASDM

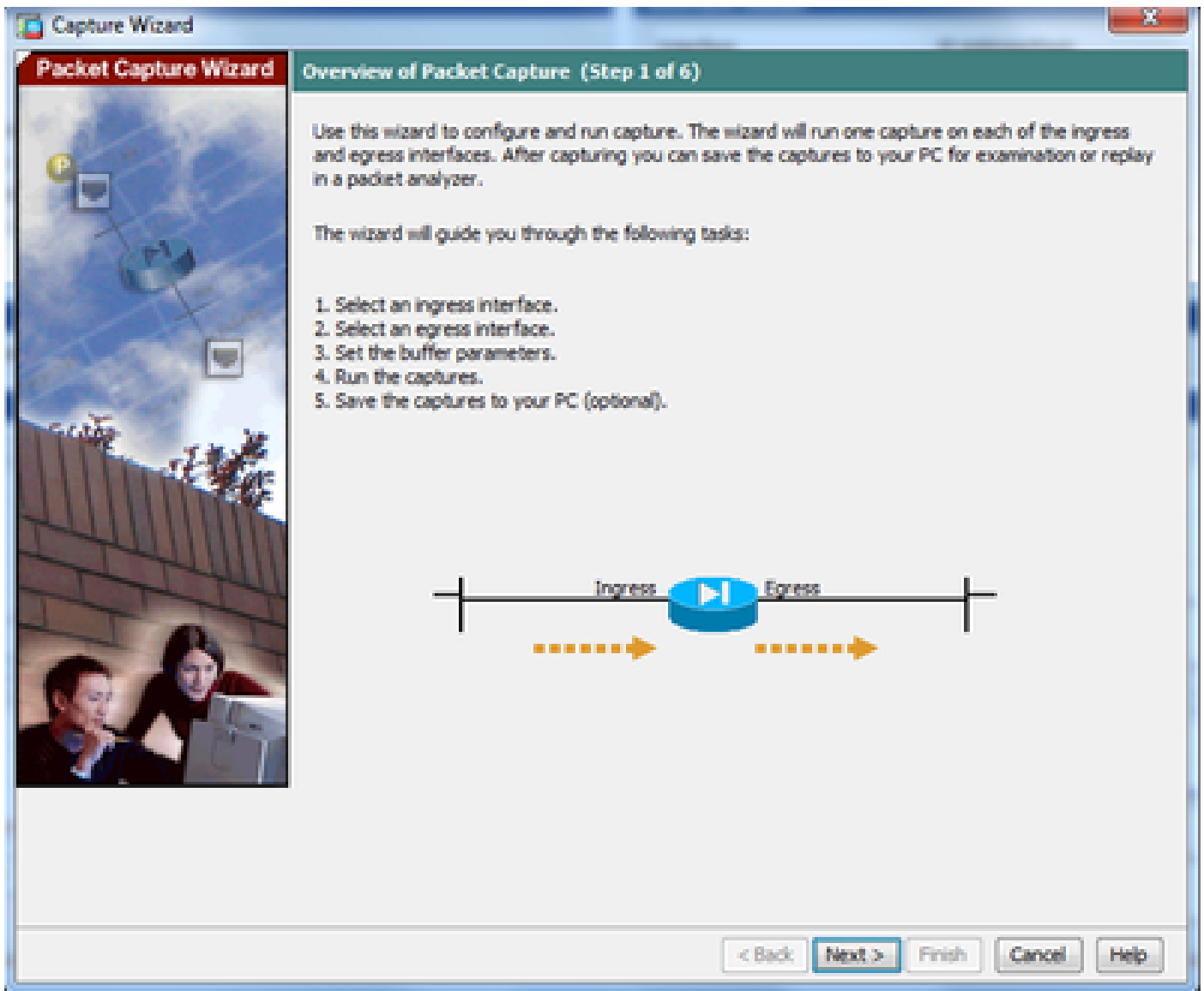
Cet exemple de configuration est utilisé pour capturer les paquets qui sont transmis pendant une requête ping de l'utilisateur 1 (réseau interne) vers le routeur 1 (réseau externe).

Complétez ces étapes afin de configurer la fonctionnalité de capture de paquets sur l'ASA avec l'ASDM :

1. Accédez à Wizards > Packet Capture Wizard pour démarrer la configuration de capture de paquets, comme indiqué :



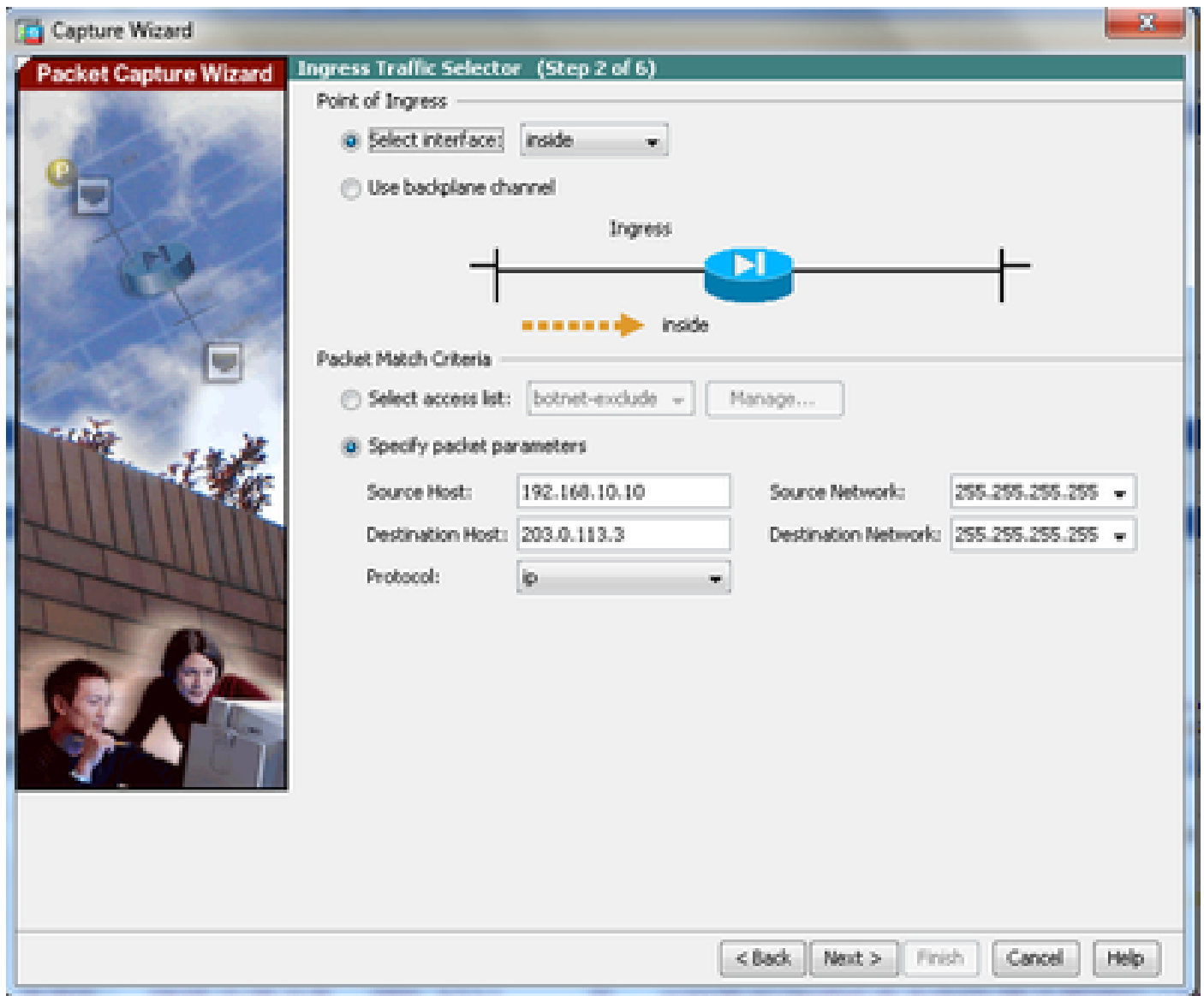
2. L'Assistant Capture s'ouvre. Cliquez sur Next (Suivant).



3.0 Dans la nouvelle fenêtre, indiquez les paramètres utilisés dans pour capturer le trafic entrant.

3.1 Sélectionnez inside pour l'interface d'entrée et fournissez les adresses IP source et de destination des paquets à capturer, ainsi que leur masque de sous-réseau, dans l'espace prévu à cet effet.

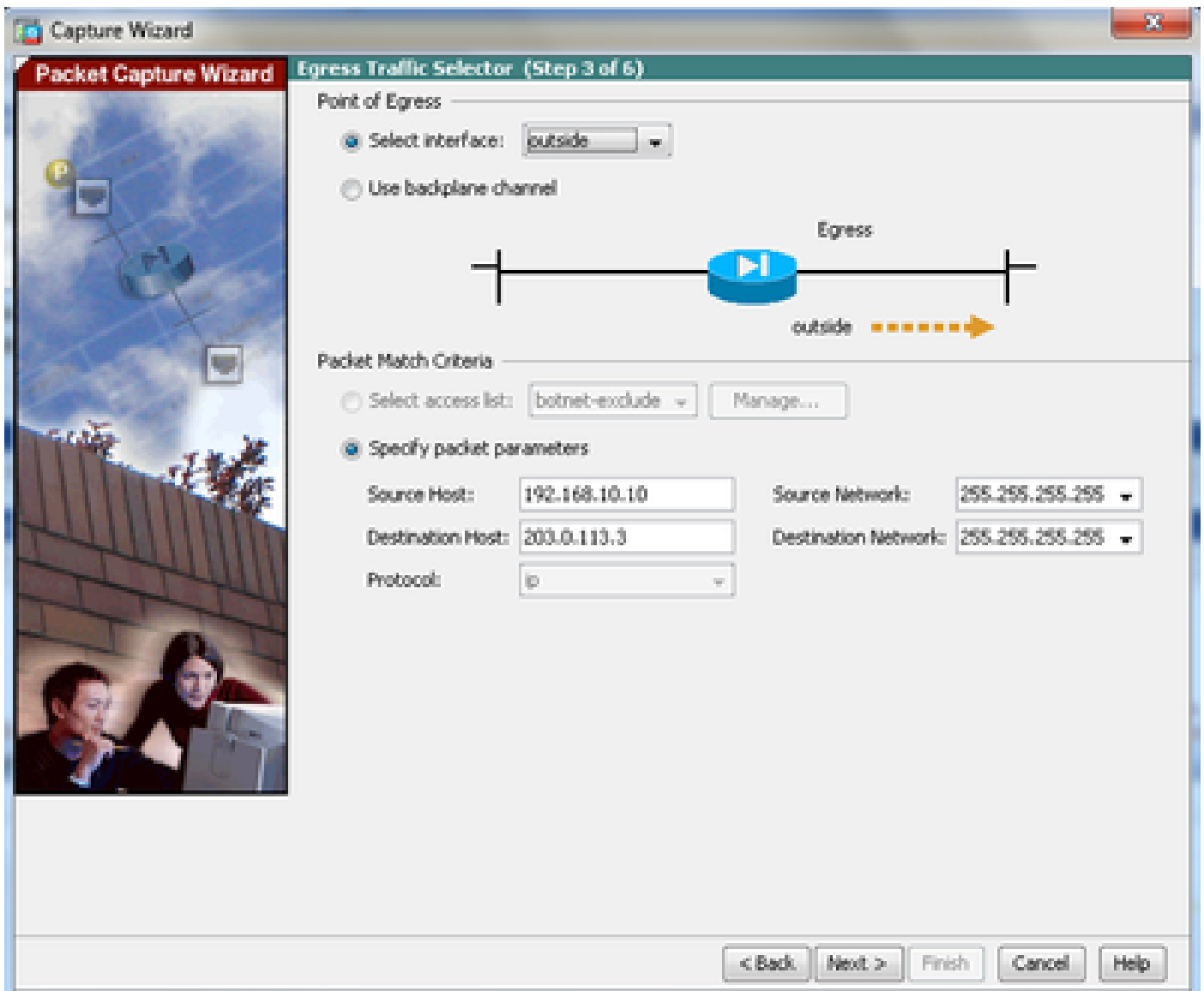
3.2 Choisissez le type de paquet à capturer par l'ASA (IP est le type de paquet choisi ici), comme indiqué :



3.3 Cliquez sur Next.

4.1 Sélectionnez outside pour l'interface de sortie et fournissez les adresses IP source et de destination, ainsi que leur masque de sous-réseau, dans les espaces respectifs prévus.

Si la traduction d'adresses de réseau (NAT) est effectuée sur le pare-feu, prenez également cela en considération.



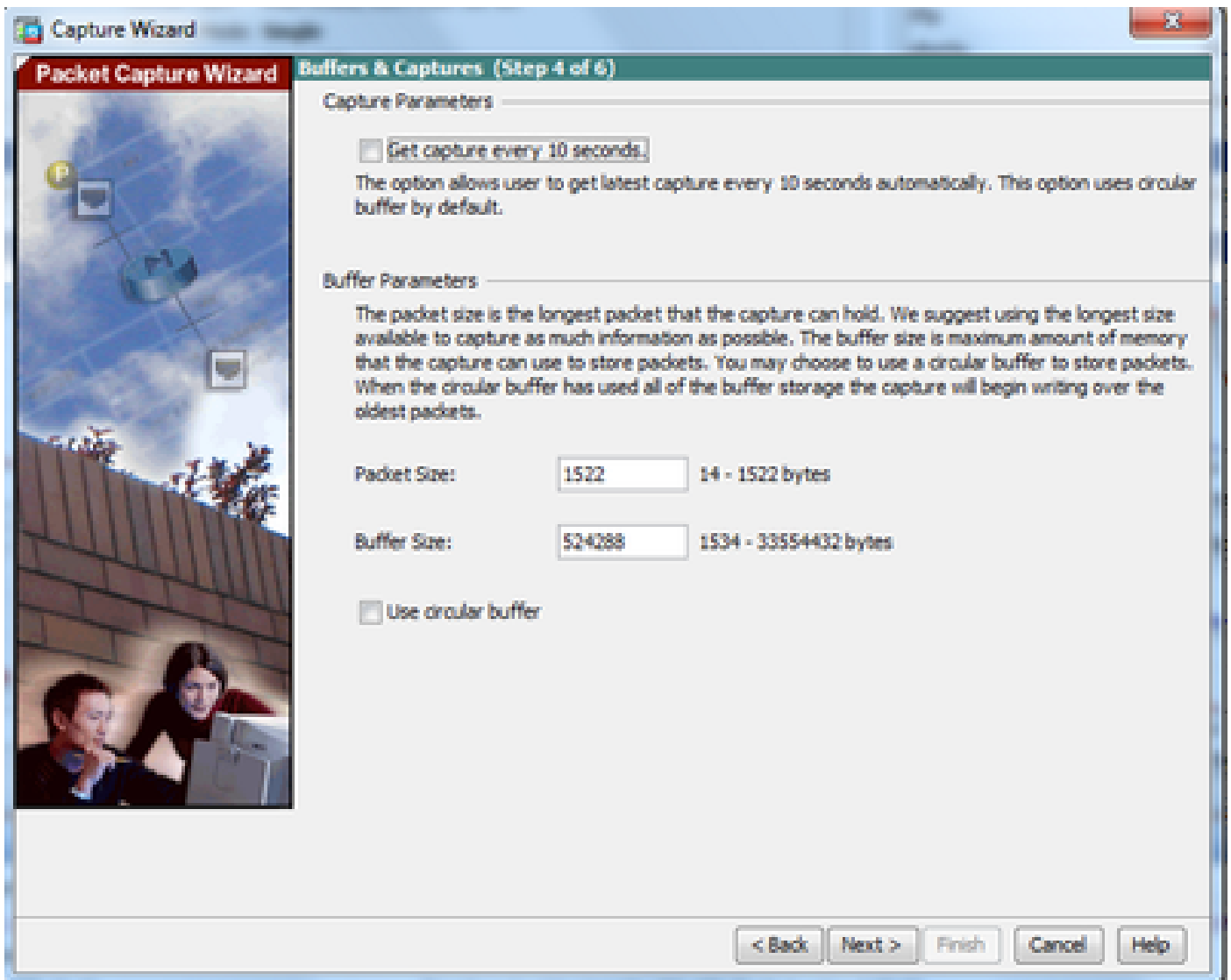
4.2 Cliquez sur Next.

5.1 Entrez la taille de paquet appropriée et la taille de tampon dans l'espace prévu à cet effet. Ces données sont nécessaires pour que la capture ait lieu.

5.2 Cochez la case Utiliser la mémoire tampon circulaire pour utiliser l'option Mémoire tampon circulaire. Les tampons circulaires ne se remplissent jamais.

Lorsque la mémoire tampon atteint sa taille maximale, les données plus anciennes sont ignorées et la capture se poursuit.

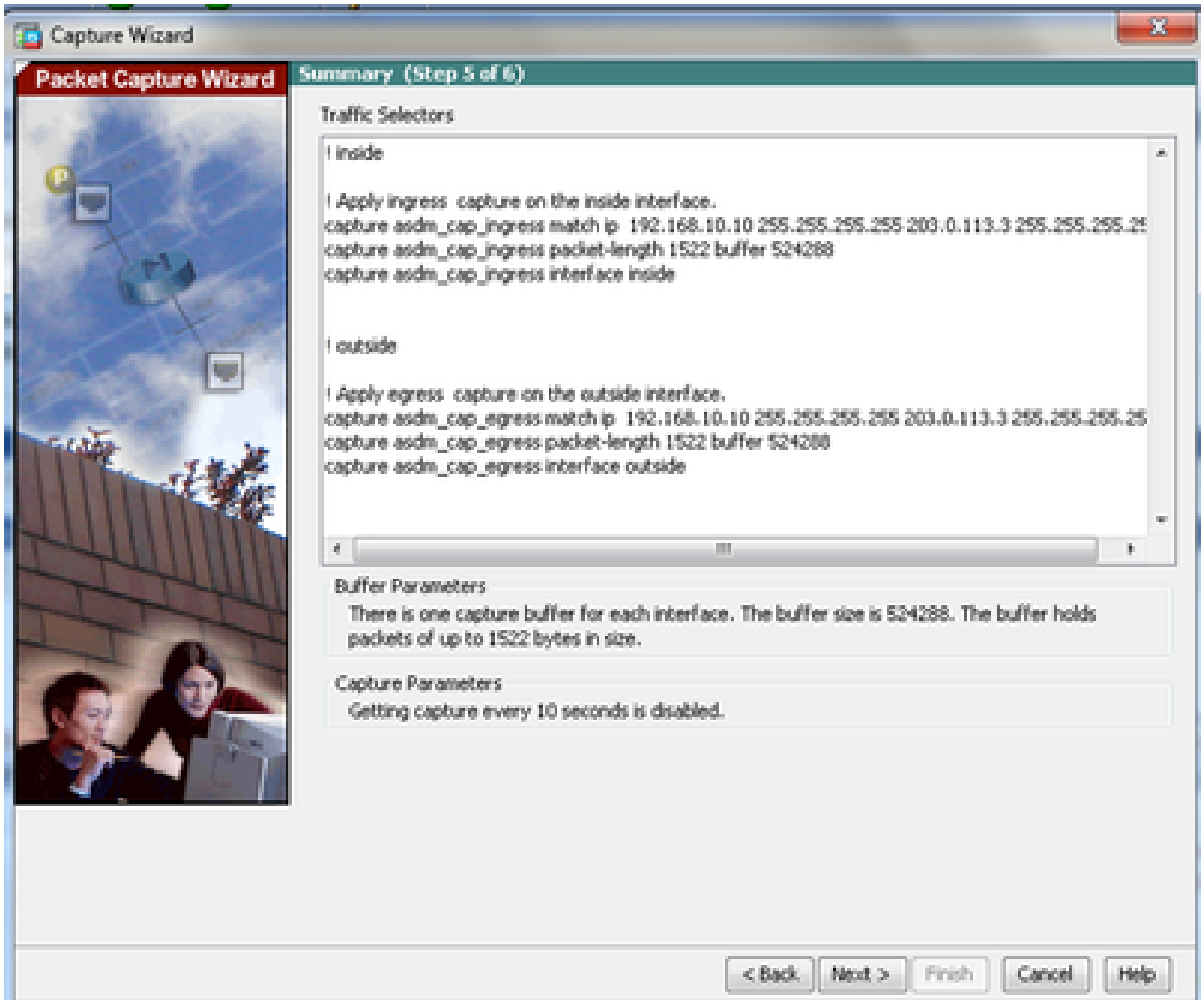
Dans cet exemple, la mémoire tampon circulaire n'est pas utilisée et la case n'est donc pas cochée.



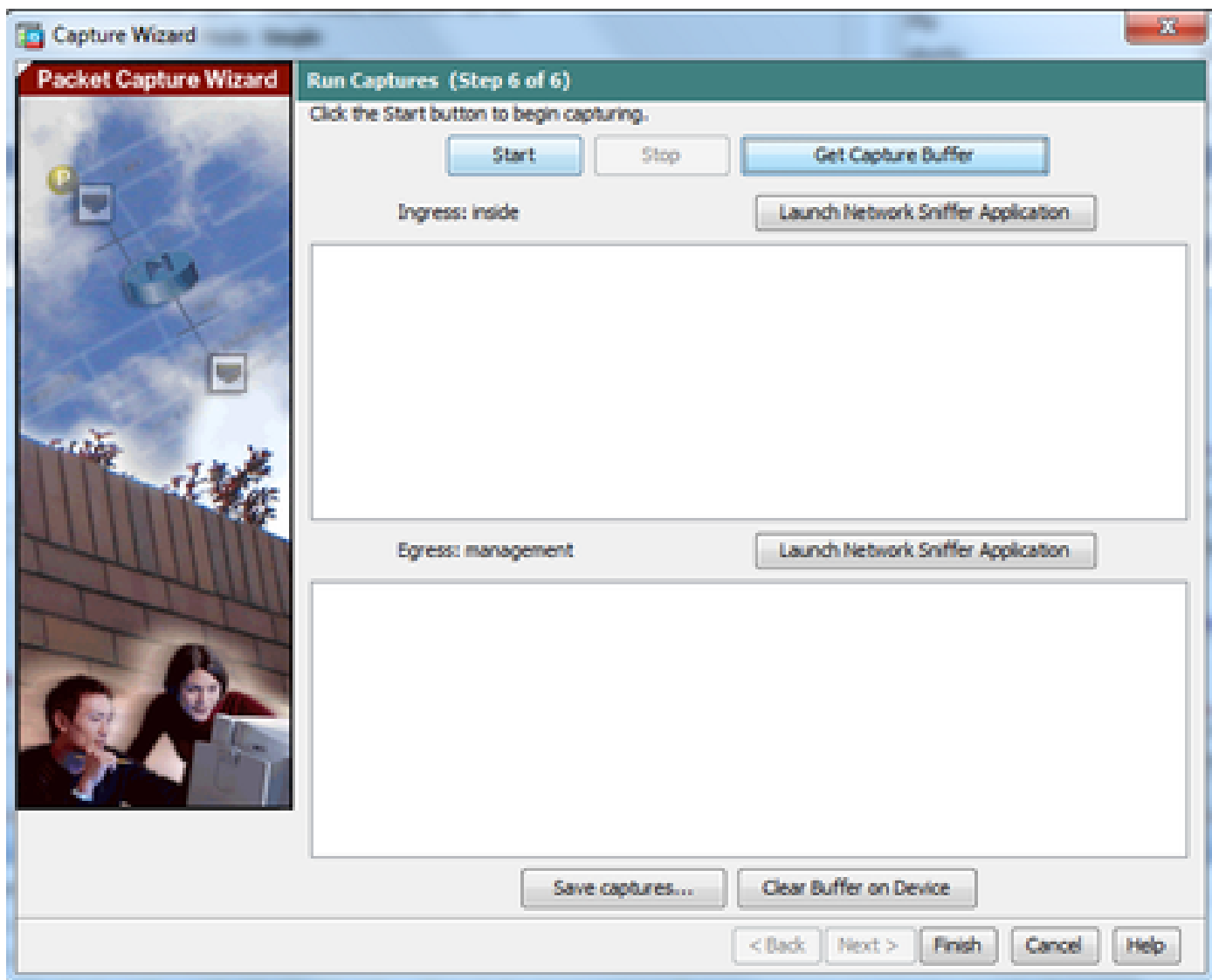
5.3 Cliquez sur Next.

6.0 Cette fenêtre montre les listes d'accès qui doivent être configurées sur l'ASA (afin que les paquets souhaités soient capturés) et le type de paquets à capturer (les paquets IP sont capturés dans cet exemple).

6.1 Cliquez sur Next.

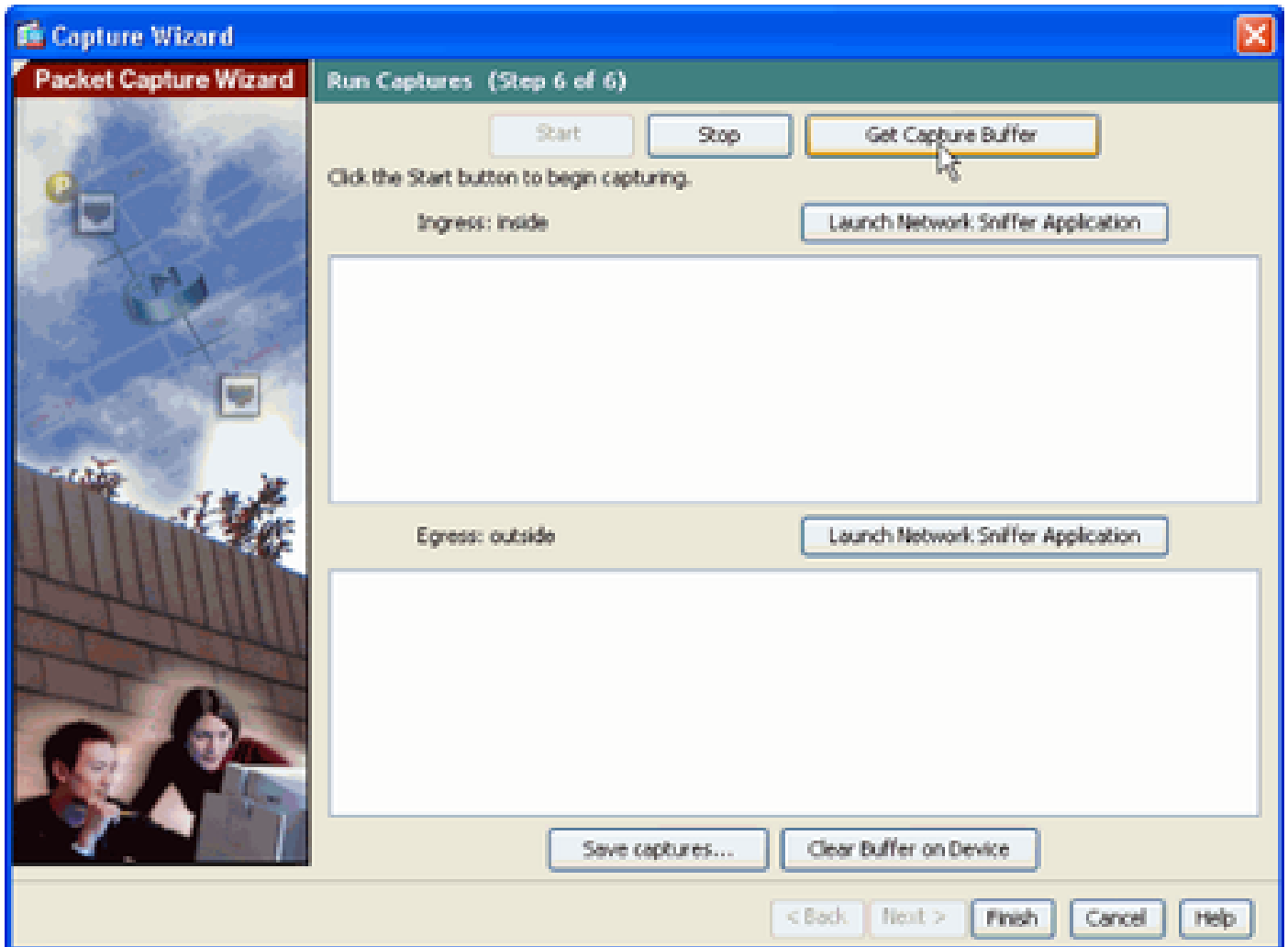


7. Cliquez sur Start afin de démarrer la capture de paquets, comme indiqué :



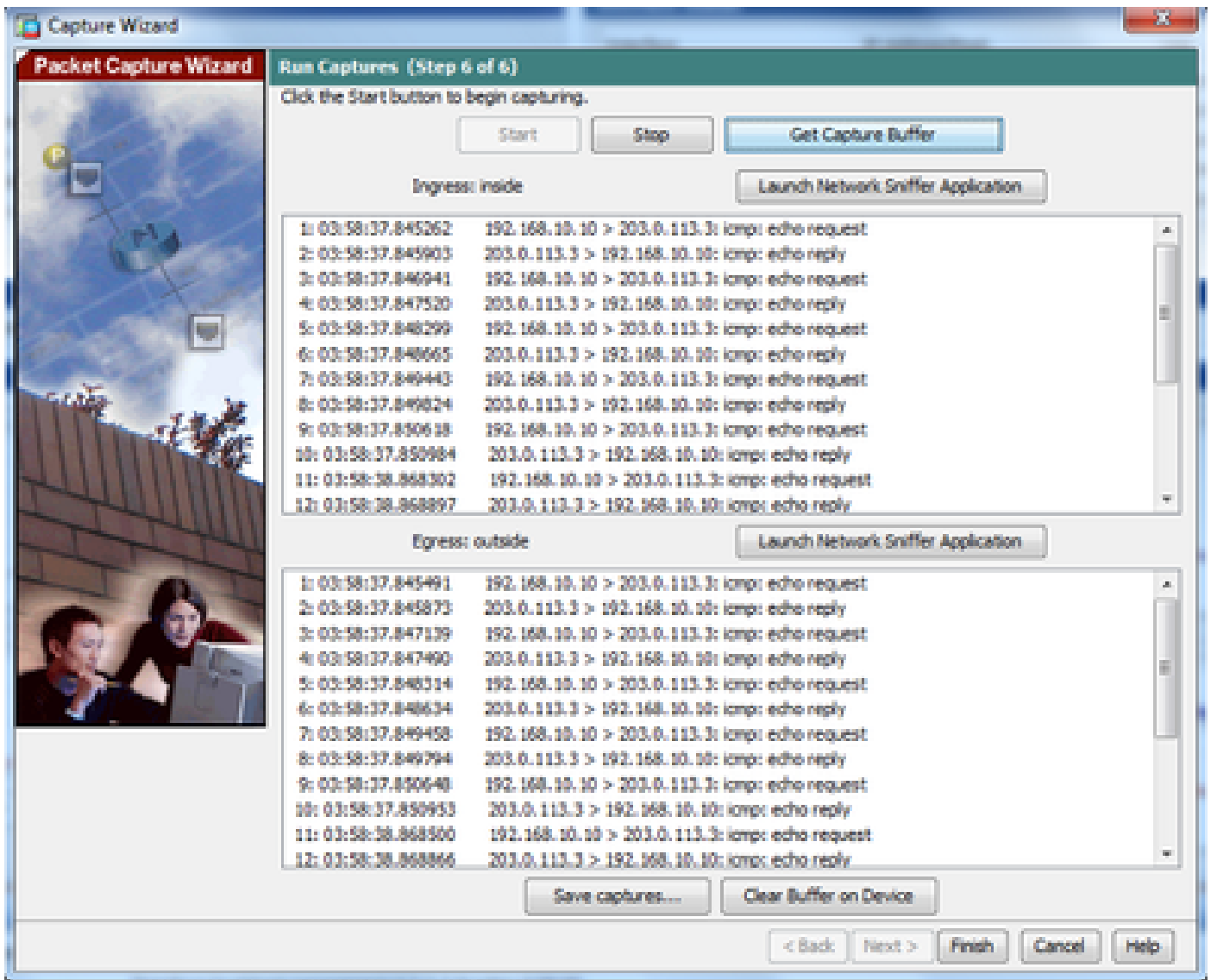
Après le démarrage de la capture de paquets, essayez d'envoyer une requête ping au réseau externe à partir du réseau interne afin que les paquets qui circulent entre les adresses IP source et de destination soient capturés par la mémoire tampon de capture ASA.

8. Cliquez sur Get Capture Buffer afin de visualiser les paquets qui sont capturés par le tampon de capture ASA.



Les paquets capturés sont affichés dans cette fenêtre pour le trafic entrant et sortant.

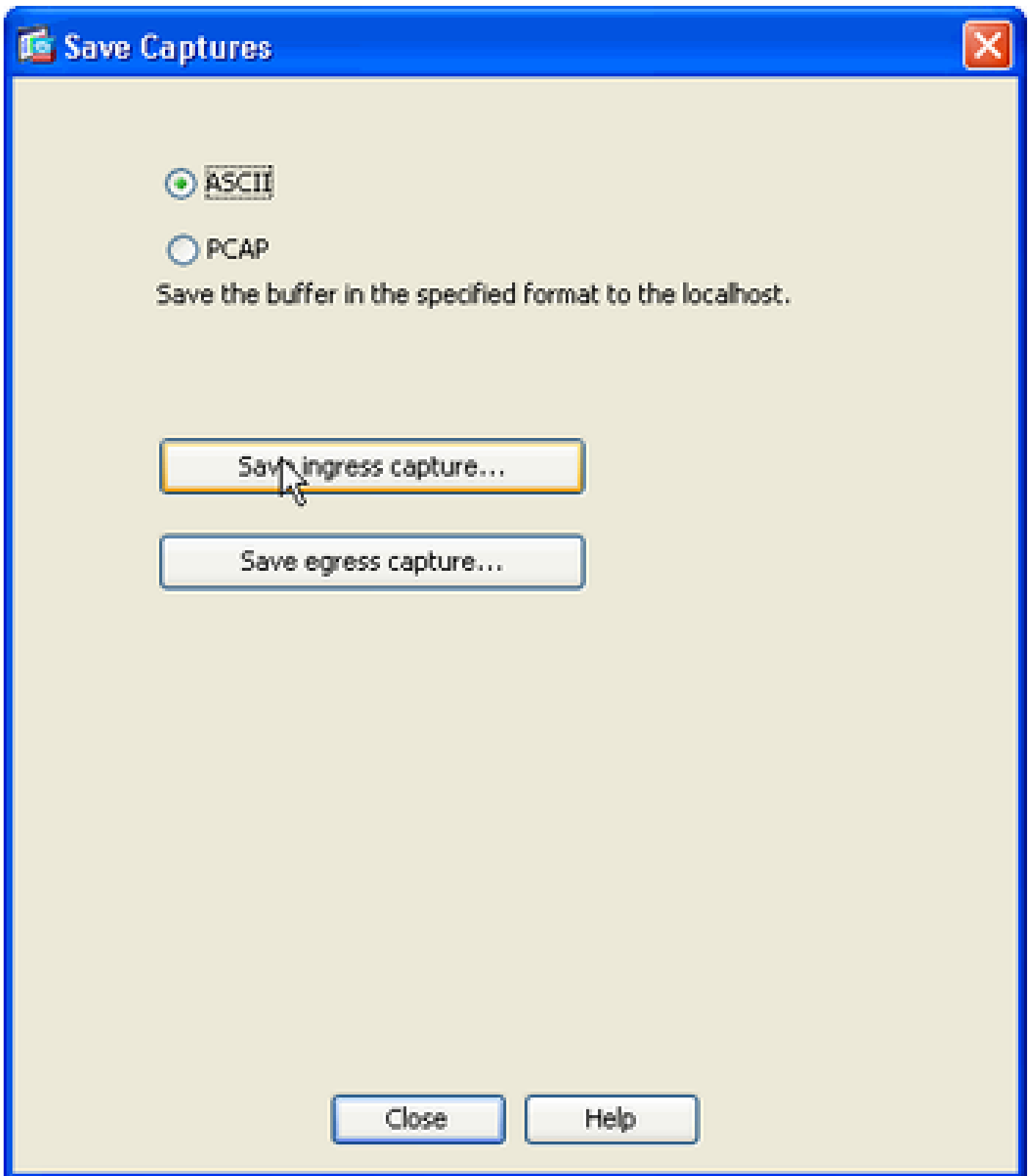
9. Cliquez sur Enregistrer les captures pour enregistrer les informations de capture.



10.1 Dans la fenêtre Save captures, choisissez le format requis dans lequel la mémoire tampon de capture doit être enregistrée. Il s'agit d'ASCII ou PCAP.

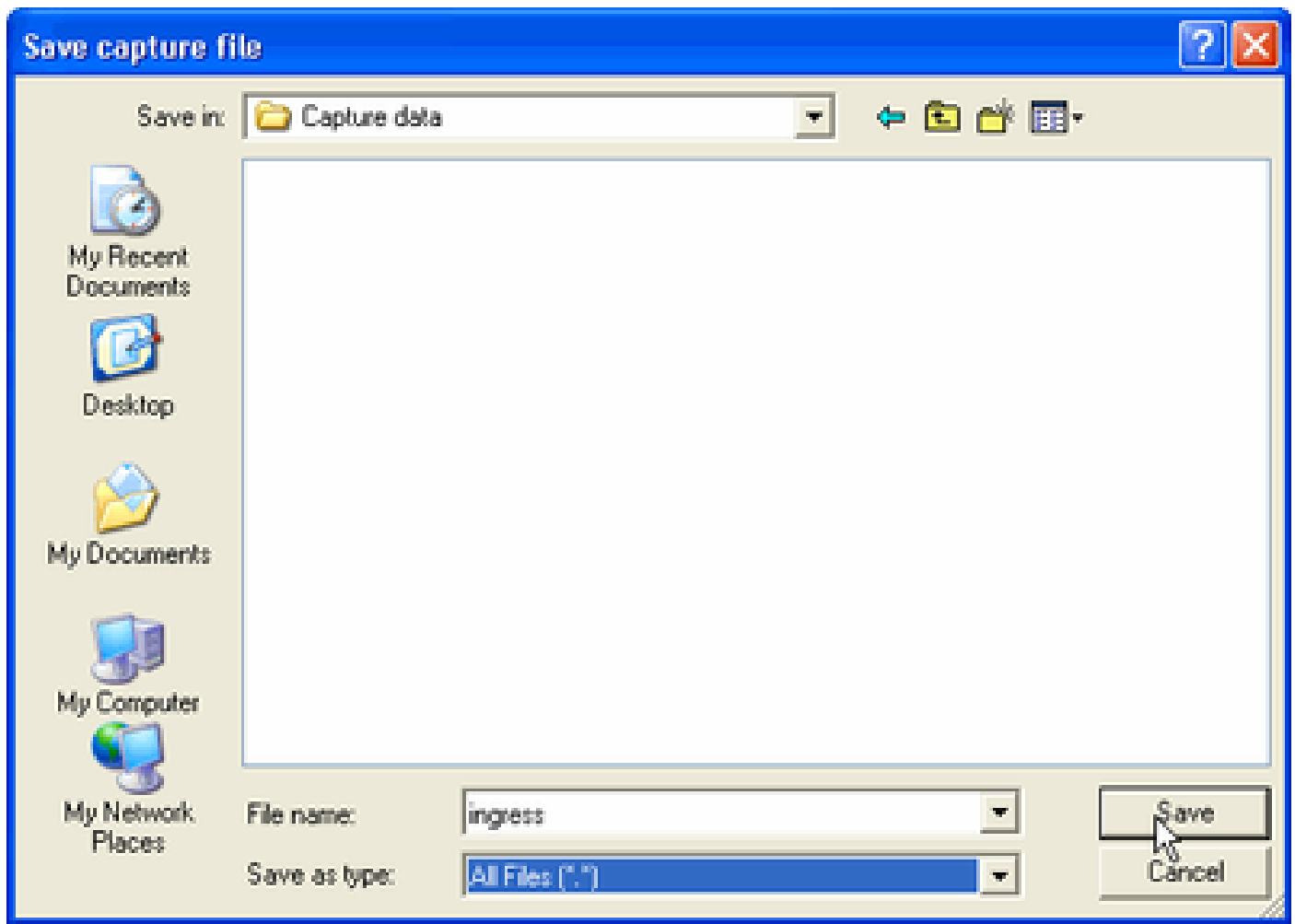
10.2 Cliquez sur la case d'option en regard des noms de format.

10.3 Cliquez sur Save ingress capture ou sur Save egress capture, si nécessaire. Les fichiers PCAP peuvent alors être ouverts avec des analyseurs de capture, tels que Wireshark, et c'est la méthode préférée.

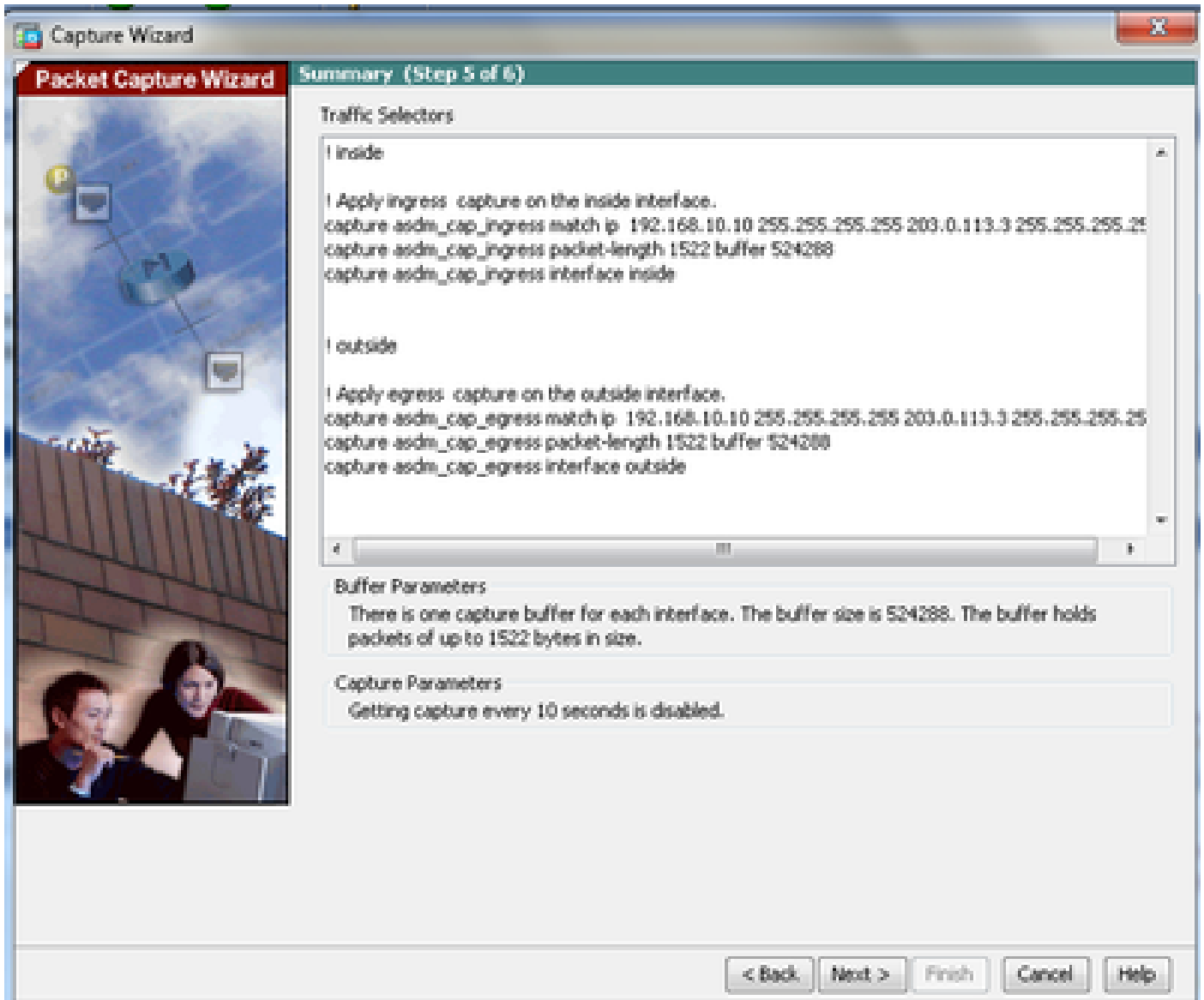


11.1 Dans la fenêtre Save capture file, indiquez le nom du fichier et l'emplacement où le fichier de capture doit être enregistré.

11.2 Cliquez sur Save.



12. Cliquez sur Terminer.



La procédure de capture des paquets de l'interface utilisateur graphique est terminée.

Configuration de la capture de paquets avec la CLI

Complétez ces étapes afin de configurer la fonctionnalité de capture de paquets sur l'ASA avec l'interface de ligne de commande :

1. Configurez les interfaces internes et externes comme illustré dans le schéma du réseau avec les niveaux d'adresse IP et de sécurité corrects.
2. Lancez le processus de capture de paquets à l'aide de la commande capture en mode d'exécution privilégié. Dans cet exemple de configuration, la capture nommée capin est définie. Liez-le à l'interface interne, et spécifiez avec le mot clé match que seuls les paquets qui correspondent au trafic d'intérêt sont capturés :

```
<#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. De même, la capture nommée capout est définie. Liez-le à l'interface externe, et spécifiez avec le mot clé match que seuls les paquets qui correspondent au trafic d'intérêt sont capturés :

```
<#root>
```

```
ASA#
```

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

L'ASA commence maintenant à capturer le flux de trafic entre les interfaces. Afin d'arrêter la capture à tout moment, entrez la commande no capture suivie du nom de la capture.

Voici un exemple :

```
<#root>
```

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

Types de capture disponibles sur l'ASA

Cette section décrit les différents types de capture disponibles sur l'ASA.

- `asa_dataplane` : capture les paquets sur le fond de panier ASA qui passent entre l'ASA et un module qui utilise le fond de panier, tel que le module ASA CX ou IPS.

```
<#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 drop-code` : capture les paquets abandonnés par le chemin de sécurité accéléré.

Le drop-code spécifie le type de trafic abandonné par le chemin de sécurité accéléré.

```
<#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 type : sélectionne un type Ethernet à capturer. Les types Ethernet pris en charge sont les suivants : 8021Q, ARP, IP, IP6, LACP, PPPOED, PPPOES, RARP et VLAN.

Cet exemple montre comment capturer le trafic 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 - Affiche les paquets capturés en continu en temps réel. Pour terminer une capture de paquets en temps réel, appuyez sur Ctrl-C. Afin de supprimer définitivement la capture, utilisez la forme no de cette commande.
- Cette option n'est pas prise en charge lorsque vous utilisez la commande cluster exec capture.

```
<#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 - Trace les paquets capturés d'une manière similaire à la fonctionnalité Packet Tracer 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
```

 Remarque : sur ASA 9.10+, le mot clé any capture uniquement les paquets avec des adresses ipv4. Le mot clé any6 capture tout le trafic adressé à ipv6.

Il s'agit de paramètres avancés qui peuvent être configurés avec des captures de paquets.

Consultez le guide de référence des commandes pour savoir comment les définir.

- ikev1/ikev2 : capture uniquement les informations de protocole IKEv1 (Internet Key Exchange Version 1) ou IKEv2.
- isakmp : capture le trafic ISAKMP (Internet Security Association and Key Management Protocol) pour les connexions VPN. Le sous-système ISAKMP n'a pas accès aux protocoles de couche supérieure. La capture est une pseudo-capture, avec les couches physique, IP et UDP combinées afin de satisfaire un analyseur PCAP. Les adresses homologues sont obtenues à partir de l'échange SA et sont stockées dans la couche IP.
- lacp - Capture le trafic LACP (Link Aggregation Control Protocol). S'il est configuré, le nom de l'interface est le nom de l'interface physique. Ceci est utile lorsque vous travaillez avec des Etherchannels afin d'identifier le comportement actuel de LACP.
- tls-proxy : capture les données entrantes et sortantes décryptées à partir du proxy TLS (Transport Layer Security) sur une ou plusieurs interfaces.
- webvpn - Capture les données WebVPN pour une connexion WebVPN spécifique.

 Attention : lorsque vous activez la capture WebVPN, cela affecte les performances de l'apppliance de sécurité. Assurez-vous de désactiver la capture après avoir généré les fichiers de capture nécessaires au dépannage.

Valeurs par défaut

Voici les valeurs par défaut du système ASA :

- Le type par défaut est raw-data.
- La taille de la mémoire tampon par défaut est de 512 Ko.

- Le type Ethernet par défaut est paquets IP.
- La longueur de paquet par défaut est de 1 518 octets.

Afficher les paquets capturés

Sur l'ASA

Pour afficher les paquets capturés, entrez la commande `show capture` suivie du nom de la capture. Cette section fournit les résultats de la commande `show` du contenu de la mémoire tampon de capture. La commande `show capture capin` affiche le contenu de la mémoire tampon de capture nommée `capin` :

```
<#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
```

La commande `show capture capout` affiche le contenu de la mémoire tampon de capture nommée `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
```


Téléchargement à partir de l'ASA for Offline Analysis

Il existe plusieurs façons de télécharger les captures de paquets pour analyse hors ligne :

1. Naviguez jusqu'à


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

sur n'importe quel navigateur.

 Conseil : si vous omettez le mot clé pcap, seul l'équivalent de la sortie de commande show capture <cap_name> est fourni.

1. Entrez la commande copy capture et votre protocole de transfert de fichiers préféré afin de télécharger la capture :

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

 Conseil : lorsque vous résolvez un problème lié à l'utilisation des captures de paquets, Cisco vous recommande de télécharger les captures pour une analyse hors ligne.

Effacer une capture

Afin d'effacer la mémoire tampon de capture, entrez la commande clear capture <capture-name> :

```
<#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
```

Entrez la commande `clear capture /all` afin d'effacer la mémoire tampon pour toutes les captures :

```
<#root>
```

```
ASA#
```

```
clear capture /all
```

Arrêter une capture

La seule façon d'arrêter une capture sur l'ASA est de la désactiver complètement avec cette commande :

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

Vérifier

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Aucune information de dépannage spécifique n'est actuellement disponible pour cette configuration.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.