

# Surveillance et dépannage des problèmes de performances ASA

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Conventions](#)

[Dépannage des problèmes de performances](#)

[Paramètres de vitesse et de duplex](#)

[Utilisation du processeur](#)

[Utilisation élevée de la mémoire](#)

[PortFast, transmission et liaison de jonction](#)

[Traduction d'adresses réseau \(NAT\)](#)

[SYSLOG](#)

[SNMP](#)

[Recherches DNS inversées](#)

[Commandes show](#)

[show cpu usage](#)

[show traffic](#)

[show perfmon](#)

[show blocks](#)

[show memory](#)

[show xlate](#)

[show conn count](#)

[show interface](#)

[show processes](#)

[Résumé des commandes](#)

[Informations connexes](#)

---

## Introduction

Ce document décrit les commandes à utiliser pour surveiller et dépanner les performances d'un dispositif de sécurité adaptatif Cisco (ASA).

# Conditions préalables

## Exigences

Aucune exigence spécifique n'est associée à ce document.

## Composants utilisés

Les informations contenues dans ce document sont basées sur un dispositif de sécurité adaptatif Cisco (ASA) qui exécute la version 8.3 et les versions ultérieures.

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.


## Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

## Dépannage des problèmes de performances

Pour le dépannage des problèmes de performance, vérifiez les domaines de base décrits dans cette section.

---

 **Remarque** : si vous disposez de la sortie de la `show` commande de votre périphérique Cisco, vous pouvez utiliser l'[analyseur CLI Cisco](#) afin d'afficher les problèmes potentiels et les correctifs. Cisco CLI Analyzer prend en charge certaines show commandes. Si vous utilisez Cisco CLI Analyzer, vous devez être un utilisateur Cisco enregistré, vous devez être connecté à votre compte Cisco et JavaScript doit être activé dans votre navigateur.

---

## Paramètres de vitesse et de duplex

Le dispositif de sécurité est préconfiguré pour détecter automatiquement les paramètres de vitesse et de duplex sur une interface. Cependant, il existe plusieurs situations qui peuvent entraîner l'échec du processus de négociation automatique, ce qui entraîne des incohérences de vitesse ou de duplex (et des problèmes de performances). Pour une infrastructure réseau à fonction critique, Cisco va manuellement coder en dur la vitesse et le duplex sur chaque interface afin d'éviter tout risque d'erreur. Ces périphériques ne se déplacent généralement pas. Par conséquent, si vous les configurez correctement, vous n'avez pas besoin de les modifier.

Quel que soit le périphérique réseau, la vitesse peut être détectée, mais le duplex doit être négocié. Si deux périphériques réseau sont configurés pour négocier automatiquement la vitesse et le mode duplex, ils échangent des trames (appelées impulsions de liaison rapide ou FLP) qui annoncent leurs capacités de vitesse et de mode duplex. Au regard d'un partenaire de liaison incompatible, ces impulsions sont similaires à des trames habituelles de 10 Mbps. Au regard d'un partenaire de liaison capable de décoder les impulsions, les FLP contiennent tous les paramètres de vitesse et de duplex que le partenaire de liaison peut fournir. La station qui reçoit les FLP va reconnaître les trames et les périphériques vont s'accorder mutuellement sur les paramètres de vitesse et de duplex les plus élevés qu'ils peuvent atteindre. Si un périphérique ne prend pas en charge la négociation automatique, l'autre périphérique reçoit les FLP et passe en mode de détection parallèle. Afin de détecter la vitesse du partenaire, le périphérique écoute la longueur des impulsions, puis définit la vitesse en fonction de la longueur. Le problème surgit lors de la configuration du duplex. Étant donné que le mode bidirectionnel doit être négocié, le périphérique configuré pour la négociation automatique ne peut pas déterminer les paramètres de l'autre périphérique. Il utilise donc par défaut le mode bidirectionnel non simultané, comme indiqué dans la norme IEEE 802.3u.

Par exemple, si vous configurez l'interface ASA pour la négociation automatique et que vous la connectez à un commutateur codé en dur pour 100 Mbits/s et le mode bidirectionnel simultané, l'ASA envoie des FLP. Cependant, le commutateur ne répond pas car il est codé en dur pour la vitesse et le duplex et ne participe pas à la négociation automatique. Comme il ne reçoit aucune réponse du commutateur, l'ASA passe en mode de détection parallèle et détecte la longueur des impulsions dans les trames envoyées par le commutateur. En d'autres termes, l'ASA détecte que le commutateur est défini sur 100 Mbits/s, il définit donc la vitesse de l'interface en fonction de cela. Cependant, comme le commutateur n'échange pas de FLP, l'ASA ne peut pas détecter si le commutateur peut fonctionner en mode bidirectionnel simultané, de sorte que l'ASA définit le mode bidirectionnel non simultané sur l'interface, comme indiqué dans la norme IEEE 803.2u. Étant donné que le commutateur est codé en dur à 100 Mbits/s et en mode bidirectionnel simultané, et que l'ASA vient juste de négocier automatiquement à 100 Mbits/s et en mode bidirectionnel non simultané (comme c'est le cas), le résultat est une non-correspondance de mode bidirectionnel qui peut entraîner de graves problèmes de performances.

Une vitesse ou une erreur de correspondance de duplex est le plus souvent indiquée quand les compteurs d'erreur sur les interfaces en question augmentent. Les erreurs les plus communes concernent la trame, les contrôles de redondance cyclique (crc) et les trames trop courtes. Si ces valeurs augmentent sur votre interface, une vitesse/erreur de correspondance de duplex ou un problème de câblage se produit. Vous devez résoudre ce problème avant de continuer.

## Exemple

<#root>

Interface GigabitEthernet0/0 "outside", is up, line protocol is up Hardware is i82546GB rev03, BW 1000 Mbps, DLY 10 usec Auto-Duplex(Full-duplex), A

157 runts

, 0 giants

379 input errors, 107 CRC, 273 frame

, 0 overrun, 0 ignored, 0 abort 0 pause input, 0 resume input 0 L2 decode drops 121 packets output, 774

Utilisation du processeur

Si vous avez remarqué que l'utilisation du CPU est élevée, effectuez ces étapes afin de dépanner :

- Vérifiez que le nombre de connexions dans show xlate count est faible.
- Vérifiez que le bloc mémoire est normal.
- Vérifiez que le nombre d'ACL est plus élevé.
- Exécutez la commande show memory detail et vérifiez que la mémoire utilisée par l'ASA est une utilisation normale.
- Vérifiez que les nombres dans show processes cpu-hog et show processes memory sont normaux.
- Tout hôte se trouvant à l'intérieur ou à l'extérieur de l'apppliance de sécurité peut générer le trafic malveillant ou de masse qui peut être un trafic de diffusion/de multidiffusion et entraîner l'utilisation élevée du CPU. Afin de résoudre ce problème, configurez une liste d'accès pour refuser le trafic entre les hôtes (de bout en bout) et pour vérifier l'utilisation.
- Vérifiez les paramètres de bidirectionnalité et de vitesse dans les interfaces ASA. Le paramètre de non-correspondance avec les interfaces distantes peut augmenter l'utilisation du processeur.

Cet exemple montre le nombre plus élevé d'erreur en entrée et de dépassements dus à la non-correspondance de la vitesse. Utilisez la commande show interface afin de vérifier les erreurs :

<#root>

Ciscoasa#

```
sh int GigabitEthernet0/1
```

```
Interface GigabitEthernet0/1 "inside", is up, line protocol is up
Hardware is i82546GB rev03, BW 1000 Mbps, DLY 10 usec
  Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
  Input flow control is unsupported, output flow control is unsupported
  MAC address 0013.c480.b2b8, MTU 1500
  IP address 192.168.17.4, subnet mask 255.255.255.0
  311981 packets input, 20497296 bytes, 0 no buffer
  Received 311981 broadcasts, 157 runts, 0 giants
```

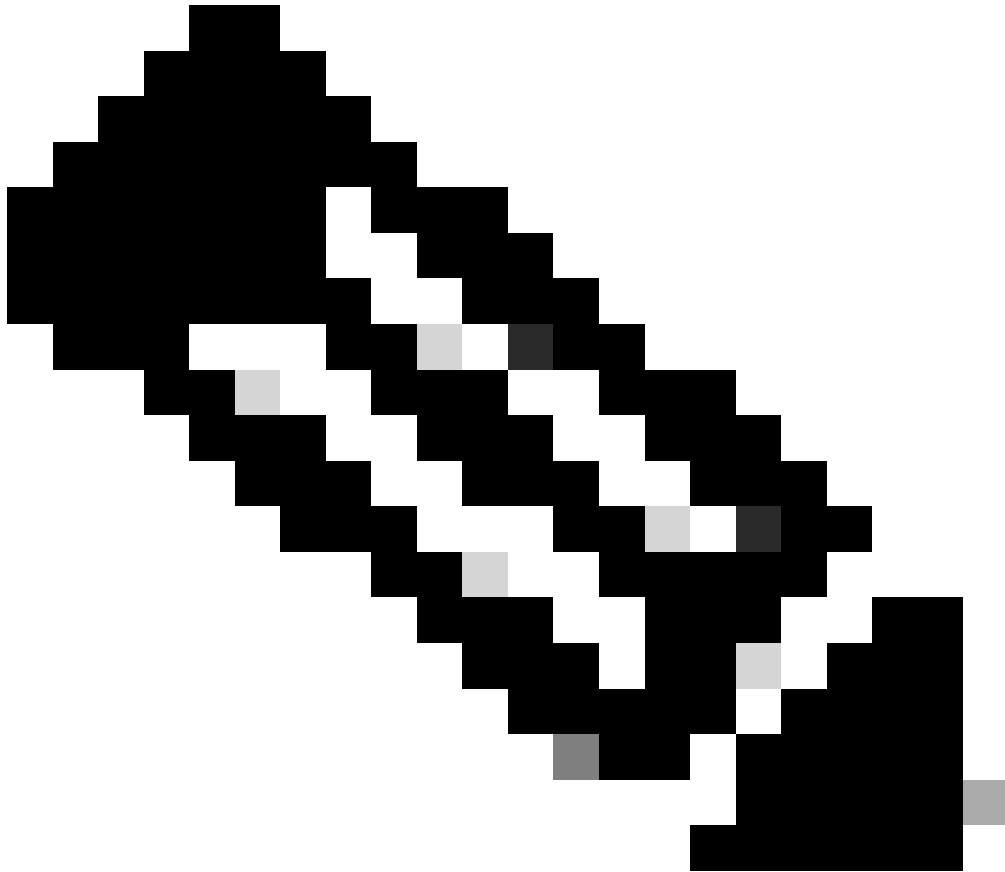
```
7186 input errors, 0 CRC, 0 frame, 7186 overrun
```

```
, 0 ignored, 0 abort
  0 pause input, 0 resume input
  0 L2 decode drops
  121 packets output, 7744 bytes, 0 underruns
  0 pause output, 0 resume output
  0 output errors, 0 collisions, 1 interface resets
  0 late collisions, 0 deferred
  0 input reset drops, 0 output reset drops, 0 tx hangs
  input queue (blocks free curr/low): hardware (255/249)
  output queue (blocks free curr/low): hardware (255/254)
```

Afin de résoudre ce problème, définissez la vitesse sur *auto* sur l'interface correspondante.

---

---

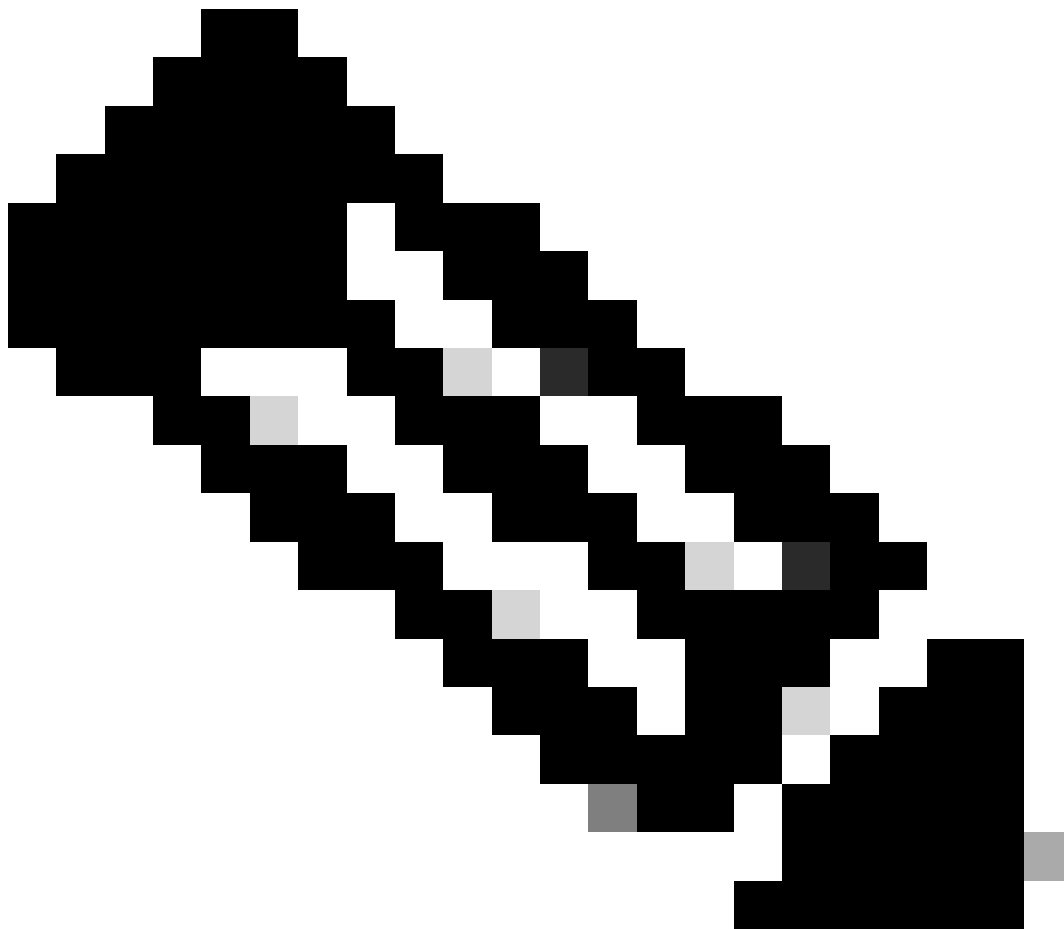


**Remarque** : Cisco recommande d'activer la commande sur toutes les interfaces `verify reverse-path interface`. Cela entraîne l'abandon des paquets qui n'ont pas d'adresse source valide et entraîne une moindre utilisation de l'UC. Cela s'applique au FWSM lorsqu'il rencontre des problèmes de CPU élevés.

- 
- Une autre raison pour l'utilisation élevée du CPU peut être due à un trop grand nombre d'itinéraires de multidiffusion. Émettez la commande `show mroute` afin de vérifier si ASA reçoit trop de routes de multidiffusion.
  - Utilisez la `show local-host` commande afin de voir si le réseau subit une attaque par déni de service, ce qui peut indiquer une attaque de virus dans le réseau.
  - Un CPU élevé peut se produire en raison de l'ID de bogue Cisco [CSCsq48636](#) . Référez-vous à l'ID de bogue Cisco [CSCsq48636](#)


pour plus d'informations.

---



**Remarque :** seuls les utilisateurs Cisco enregistrés peuvent accéder aux outils Cisco internes et aux informations de bogue.

---

 **Remarque :** si la solution fournie précédemment ne résout pas le problème, mettez à niveau la plate-forme ASA en fonction de la configuration requise. Référez-vous à [Modules de sécurité Cisco pour les dispositifs de sécurité](#) pour plus d'informations sur les capacités et les capacités de la plate-forme d'appareil de sécurité adaptatif. Contactez le TAC ([support technique Cisco](#)) pour plus d'informations.

---

Voici quelques causes possibles et résolutions pour l'utilisation élevée de la mémoire :

- **Journalisation des événements** : la journalisation des événements peut consommer de grandes quantités de mémoire. Afin de résoudre ce problème, installez et consignez tous les événements vers un serveur externe, tel qu'un serveur syslog.
- **Fuite de mémoire** : un problème connu dans le logiciel du dispositif de sécurité peut entraîner une consommation de mémoire élevée. Afin de résoudre ce problème, mettez à niveau le logiciel d'appliance de sécurité.
- **Débogage activé** : le débogage peut consommer de grandes quantités de mémoire. Afin de résoudre ce problème, désactivez le débogage à l'aide de la commande `undebug all`.
- **Blocage des ports** : le blocage des ports sur l'interface externe d'un dispositif de sécurité entraîne la consommation de grandes quantités de mémoire par le dispositif de sécurité pour bloquer les paquets via les ports spécifiés. Afin de résoudre ce problème, bloquez le trafic de routage offensant du côté de l'ISP.
- **Détection des menaces** : la fonctionnalité de détection des menaces se compose de différents niveaux de statistiques collectées pour diverses menaces et de la détection des menaces analysées, qui détermine le moment où un hôte effectue une analyse. **Désactivez cette fonctionnalité pour consommer moins de mémoire.**


PortFast, transmission et liaison de jonction

Par défaut, beaucoup de commutateurs, tels que les commutateurs Cisco qui exécutent le système d'exploitation (SE) de Catalyst, sont conçus pour être des périphériques prêts à l'emploi. Par conséquent, de nombreux paramètres de port par défaut ne sont pas souhaitables lorsqu'un ASA est connecté au commutateur. Par exemple, sur un commutateur qui exécute le système d'exploitation de Catalyst, la transmission par défaut et la liaison de jonction sont définies sur Auto et PortFast est désactivé. Si vous connectez un ASA à un commutateur qui exécute le système d'exploitation Catalyst, désactivez la canalisation, désactivez l'agrégation et activez PortFast.

La transmission, également connue sous le nom de Fast EtherChannel ou Giga EtherChannel, est utilisée pour relier deux ports physiques ou plus dans un groupe logique afin d'augmenter le débit global à travers la liaison. Quand un port est configuré pour la transmission automatique, il envoie des trames de Protocole d'agrégation de ports (PAgP) pendant que la liaison devient active afin de déterminer s'il fait partie d'un canal. Ces trames peuvent causer des problèmes si l'autre périphérique tente de négocier automatiquement la vitesse et le mode bidirectionnel de la liaison. Si la transmission sur le port est définie sur Auto, elle entraîne également un retard supplémentaire d'environ 3 secondes avant que le port commence à transférer le trafic de routage après que la liaison est établie.



---


 **Remarque** : sur les commutateurs de la gamme Catalyst XL, la transmission n'est pas définie sur Auto par défaut. Pour cette raison, vous devez désactiver la transmission sur tout port de commutateur qui se connecte à un ASA.

---

La liaison de jonction, également connue par les protocoles classiques de jonction Inter-Switch Link (ISL) ou Dot1q, combine plusieurs LAN virtuels (VLAN) sur un port (ou une liaison) unique. La liaison de jonction est typiquement utilisée entre deux commutateurs lorsque les deux ont plus d'un VLAN défini sur eux. Quand un port est configuré pour la liaison de jonction automatique, il envoie des trames Dynamic Trunking Protocol (DTP) pendant que la liaison s'établit afin de déterminer si le port auquel elle se connecte veut effectuer une jonction. Ces trames DTP peuvent entraîner des problèmes de négociation automatique de la liaison. Si la liaison de jonction est définie sur Auto sur un port de commutation, elle ajoute un retard supplémentaire d'environ 15 secondes avant que le port commence à transférer le trafic de routage après que la liaison est établie.

PortFast, également connu sous le nom de Fast Start, est une option qui informe le commutateur qu'un périphérique de la couche 3 est connecté hors d'un port de commutation. Le port n'attend pas les 30 secondes par défaut (15 secondes pour écouter et 15 secondes pour apprendre) ; au lieu de cela, cette action amène le commutateur à mettre le port en état de transmission immédiatement après l'établissement de la liaison. Il est important de comprendre que, quand vous activez PortFast, le spanning-tree n'est pas désactivé. Le spanning-tree est encore en activité sur ce port. Quand vous activez PortFast, le commutateur est seulement informé qu'il n'y a pas un autre commutateur ou routeur (périphérique de couche 2 uniquement) connecté à l'autre bout de la liaison. Le commutateur contourne le retard habituel de 30 secondes pendant qu'il essaie de déterminer si une boucle de routage de la couche 2 donne des résultats si elle apporte ce port. Après que la liaison soit évoquée, elle continue de participer au spanning-tree. Le port envoie les unités BPDU (bridge packet data units) et le commutateur écoute toujours les BPDU sur ce port. Pour ces raisons, il est recommandé d'activer PortFast sur n'importe quel port de commutateur qui se connecte à un ASA.

---


 **Remarque** : Catalyst OS versions 5.4 et ultérieures incluent la commande qui vous permet d'utiliser une seule commande pour désactiver la transmission, désactiver l'agrégation et activer PortFast. Cette set port host <mod>/<port> commande permet de désactiver la transmission, de désactiver l'agrégation et d'activer PortFast.

---

Traduction d'adresses réseau (NAT)

À chaque session NAT ou de surcharge NAT (PAT) est attribuée un emplacement de routage de traduction connu sous le nom de *xlate*. Ces *xlate* peuvent persister même après des modifications apportées aux règles NAT qui les affectent. Ceci peut entraîner une pénurie en matière d'emplacements ou de comportement inhabituel de routage de traduction ou à chacun des deux par le trafic qui subit le routage de traduction. Cette section explique comment afficher et effacer des *xlate* sur l'appliance de sécurité.

---

 **Attention** : une interruption momentanée du flux de tout le trafic à travers le périphérique peut se produire lorsque vous effacez globalement les *xlate* sur l'appliance de sécurité.

---

Exemple de configuration ASA pour PAT qui utilise l'adresse IP de l'interface externe :

```
object network OBJ_GENERIC_ALL subnet 0.0.0.0 0.0.0.0 nat (inside,outside) source dynamic OBJ_GENERIC_ALL interface
```

Le trafic qui traverse l'appliance de sécurité passe très probablement par un NAT. Afin d'afficher les traductions qui sont en cours d'utilisation sur l'appliance de sécurité, émettez la commande `show xlate` :

```
<#root>
```

```
Ciscoasa#
```

```
show xlate
```

```
5 in use, 5 most used Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T - twice NAT
```

Les emplacements de routage de traduction peuvent persister après avoir effectué des modifications majeures. Afin d'effacer les emplacements de traduction actuels sur l'appliance de sécurité, émettez la commande `clear xlate` :

```
<#root>
```

```
Ciscoasa#
```

```
clear xlate
```

```
<#root>
```

```
Ciscoasa#
```

```
show xlate
```

0 in use, 1 most used

La commande `clear xlate` efface toute la traduction dynamique actuelle de la table `xlate`. Afin d'effacer une traduction IP particulière, vous pouvez utiliser la commande `clear xlate` avec le mot global `[ip address]` clé.

Voici un exemple de configuration ASA pour NAT :

```
object network inside-net subnet 0.0.0.0 0.0.0.0 object network outside-pat-pool range 10.10.10.10 10.10.10.100 nat (inside,outside) source dynamic inside
```

Observez le résultat `show xlate` de la traduction de l'intérieur 10.2.2.2 vers l'extérieur global 10.10.10.10 :

```
<#root>
```

```
Ciscoasa#
```

```
show xlate
```

2 in use, 2 most used

Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T - twice

```
TCP PAT from inside:10.2.2.2/1429 to any:10.10.10.10/64768 flags ri idle 62:33:57 timeout 0:00:30
```

```
TCP PAT from inside:10.5.5.5/1429 to any:10.10.10.11/64768 flags ri idle 62:33:57 timeout 0:00:30
```

Effacez le routage de traduction pour l'adresse IP globale 10.10.10.10 :

<#root>

```
Ciscoasa# clear xlate global 10.10.10.10
```

Dans cet exemple, le routage de traduction de 10.2.2.2 interne à 10.10.10.10 globale externe a disparu :

<#root>

```
Ciscoasa#
```

```
show xlate
```

```
1 in use, 2 most used
```

```
Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T - twice
```

```
TCP PAT from inside:10.5.5.5/1429 to any:10.10.10.11/64768 flags ri idle 62:33:57 timeout 0:00:30
```

## SYSLOG

Les Syslogs vous permettent de dépanner les problèmes sur l'ASA. Cisco propose un serveur syslog gratuit pour Windows NT appelé ASA Firewall Syslog Server (PFSS). Vous pouvez télécharger PFSS à partir de [Cisco Technical Support & Downloads](#).

Plusieurs autres fournisseurs proposent des serveurs syslog pour diverses plates-formes Windows, telles que Windows 2000 et Windows XP. La plupart des machines UNIX et Linux ont des serveurs syslog installés par défaut.


Lorsque vous configurez le serveur syslog, configurez l'ASA afin de lui envoyer des journaux.

Exemple :

<#root>

```
logging on logging host <ip_address_of_syslog_server> logging trap debugging
```

---

 **Remarque** : cet exemple configure l'ASA pour envoyer des syslogs de débogage (niveau 7) et plus critiques au serveur syslog. Ces journaux ASA étant les plus détaillés, utilisez-les uniquement lorsque vous dépannez un problème. Pour une opération normale, configurez le niveau de journalisation sur Warning (niveau 4) ou Error (niveau 3).

---

Si vous éprouvez un problème de ralentissement des performances, ouvrez Syslog dans un fichier texte et recherchez l'adresse IP source liée au problème de performances. (Si vous utilisez UNIX, vous pouvez utiliser le programme `grep` par Syslog pour l'adresse IP de la source.) Recherchez les messages indiquant que le serveur externe a tenté d'accéder à l'adresse IP interne sur le port TCP 113 (pour le protocole d'identification ou Ident), mais que l'ASA a refusé le paquet. Le message doit être similaire à l'exemple suivant :

```
%ASA-2-106001: Inbound TCP connection denied from 10.64.10.2/35969 to 192.168.110.179/113 flags SYN
```

Si vous recevez ce message, émettez la commande `reset inbound` à l'ASA. L'ASA ne supprime pas les paquets en silence ; au lieu de cela, cette commande amène l'ASA à réinitialiser immédiatement toute connexion entrante qui est refusée par la stratégie de sécurité. Le serveur n'attend pas que le paquet Ident expire sa connexion TCP ; au lieu de cela, il reçoit immédiatement un paquet de réinitialisation.

## SNMP

Une méthode recommandée pour les déploiements d'entreprise consiste à surveiller les performances de Cisco ASA avec SNMP. Cisco ASA prend en charge cette fonctionnalité avec les versions SNMP 1, 2c et 3.

Vous pouvez configurer l'appliance de sécurité pour envoyer des dérouterements à un serveur de gestion de réseau (NMS) ou vous pouvez utiliser

le NMS pour parcourir les MIB sur l'appliance de sécurité. Les MIB sont un ensemble de définitions et le dispositif de sécurité tient à jour une base de données de valeurs pour chaque définition. Pour plus d'informations à ce sujet, référez-vous au [Guide de configuration de la gamme Cisco ASA 5500 avec l'interface de ligne de commande, 8.4 et 8.6.](#)

Toutes les bases MIB prises en charge pour Cisco ASA sont disponibles sur la liste de support MIB ASA. Dans cette liste, ces MIB sont utiles lorsque vous surveillez les performances :

- CISCO-FIREWALL-MIB ---- Contient des objets utiles pour le basculement.
- CISCO-PROCESS-MIB ---- Contient des objets utiles pour l'utilisation du processeur.
- CISCO-MEMORY-POOL-MIB ---- Contient des objets utiles pour les objets mémoire.

#### Recherches DNS inversées

Si les performances de l'ASA sont faibles, vérifiez que vous disposez d'enregistrements DNS PTR (Domain Name System Pointer), également appelés enregistrements de recherche DNS inverse, dans le serveur DNS faisant autorité pour les adresses externes que l'ASA utilise. Cela inclut toutes les adresses de votre pool global de traduction d'adresses de réseau (NAT) (ou l'interface externe ASA si vous surchargez l'interface), toutes les adresses statiques et les adresses internes (si vous n'utilisez pas NAT avec elles). Certaines applications, telles que les serveurs FTP (File Transfer Protocol) et Telnet, peuvent utiliser des recherches DNS inversées afin de déterminer d'où vient l'utilisateur et s'il s'agit d'un hôte valide. Si la recherche DNS inversée ne la résout pas, alors des performances se sont dégradées pendant que la requête de routage s'arrête.

Afin de s'assurer qu'un enregistrement PTR existe pour ces hôtes, émettez la commande à partir de votre PC ou de votre machine UNIX ; incluez l'adresse IP globale que vous utilisez pour vous connecter à Internet. nslookup

#### Exemple

```
<#root>
```

```
% nslookup 192.168.219.25
```

```
10.219.133.198.in-addr.arpa name = www.cisco.com.
```

Vous devez recevoir une réponse avec le nom DNS du périphérique affecté à cette adresse IP. Si vous ne recevez pas de réponse, contactez la personne qui contrôle votre DNS afin de demander l'ajout des enregistrements PTR pour chacune de vos adresses IP globales.

### Dépassements sur l'interface

Si vous avez une salve de trafic, des paquets abandonnés peuvent se produire si la salve dépasse la capacité de mise en mémoire tampon de la mémoire tampon FIFO sur la carte réseau et les mémoires tampons de l'anneau de réception. Si vous activez les trames de pause pour le contrôle de flux peut atténuer ce problème. Les trames Pause (XOFF) et XON sont générées automatiquement par la carte réseau en fonction de l'utilisation de la mémoire tampon FIFO. Une trame de pause est envoyée lorsque l'utilisation de la mémoire tampon dépasse la limite supérieure. Afin d'activer les trames de pause (XOFF) pour le contrôle de flux, utilisez cette commande :

```
<#root>
```

```
hostname(config)#
```

```
interface tengigabitethernet 1/0
```

```
hostname(config-if)#
```

```
flowcontrol send on
```

Commandes show

```
show cpu usage
```

La commande `show cpu usage` est utilisée pour déterminer la charge de trafic placée sur le processeur ASA. Aux moments où le trafic est maximal, le réseau connaît des poussées d'activités ou des attaques et l'utilisation du CPU peut atteindre des pics.

L'ASA dispose d'un processeur unique pour traiter diverses tâches ; par exemple, il traite les paquets et imprime les messages de débogage sur la console. Chaque processus a sa propre raison de routage, et certains processus requièrent plus de temps du CPU que d'autres. Le cryptage est

probablement le processus le plus exigeant en termes de CPU. Par conséquent, si votre ASA achemine beaucoup de trafic à travers des tunnels cryptés, vous devez envisager un ASA plus rapide, un concentrateur VPN dédié, tel que le VPN 3000. Le VAC décharge le cryptage et le décryptage du processeur ASA et l'exécute dans le matériel de la carte. Cela permet à l'ASA de chiffrer et de déchiffrer 100 Mbits/s de trafic avec 3DES (chiffrement 168 bits).

La journalisation est un autre processus qui peut consommer une grande quantité de ressources système. Pour cette raison, il est recommandé de désactiver la journalisation de la console, de la surveillance et de la mémoire tampon sur l'ASA. Vous pouvez activer ces processus quand vous dépannez un problème de routage, mais désactivez-les pour les opérations quotidiennes, particulièrement si vous manquez de capacité de CPU. Il est également conseillé de définir la journalisation syslog ou SNMP (Simple Network Management Protocol) (historique de journalisation) sur le niveau 5 (Notification) ou inférieur. `no logging message <syslog_id>` En outre, vous pouvez désactiver des ID de message Syslog spécifiques à l'aide de la commande .

Cisco Adaptive Security Device Manager (ASDM) fournit également un graphique sur l'Monitoring onglet qui vous permet de visualiser l'utilisation du CPU de l'ASA au fil du temps. Vous pouvez utiliser ce graphique afin de déterminer la charge sur votre ASA.

La **show cpu usage** commande peut être utilisée pour afficher les statistiques d'utilisation du CPU.

### Exemple

```
<#root>
```

```
Ciscoasa#
```

```
show cpu usage
```

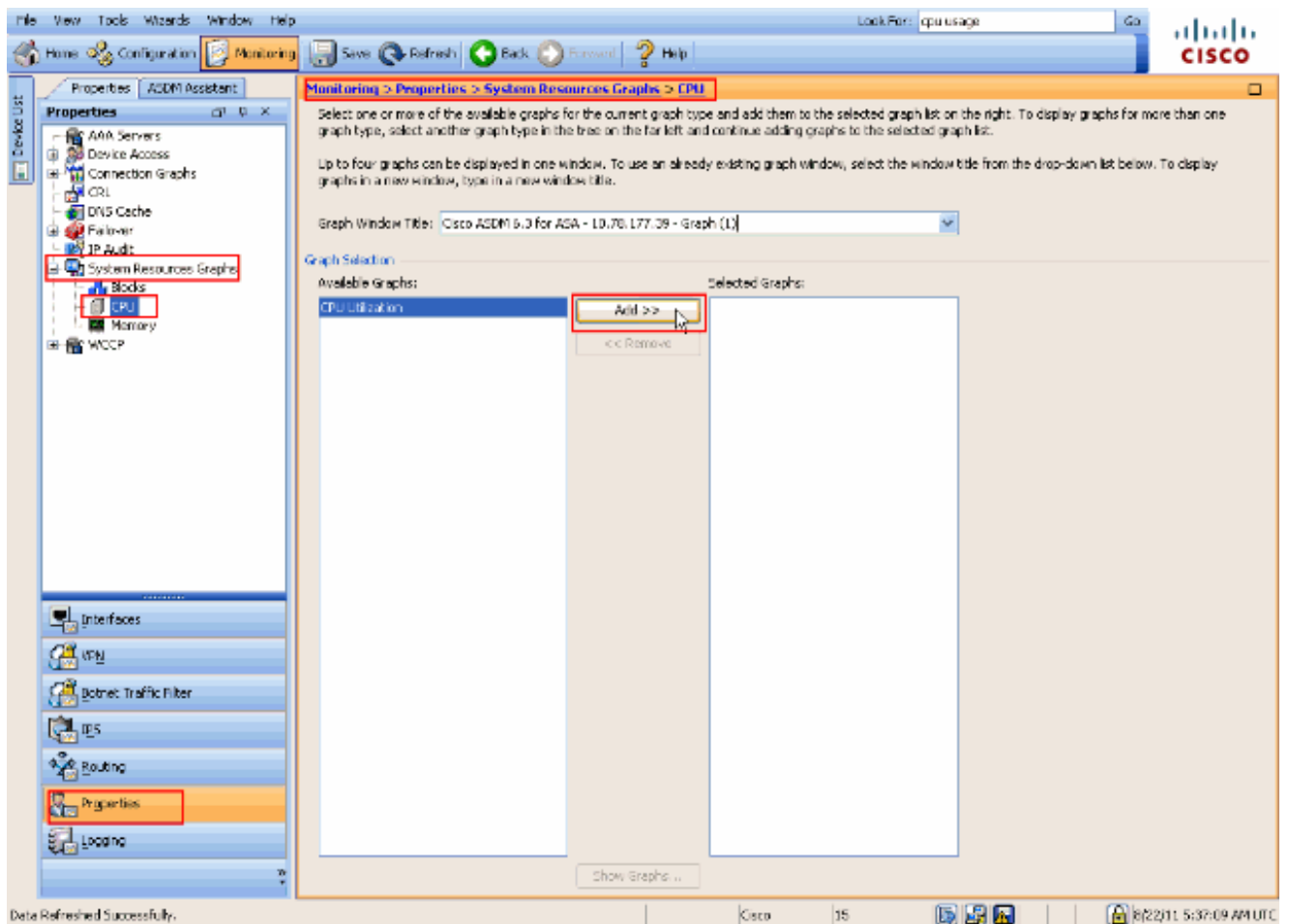
```
CPU utilization for 5 seconds = 1%; 1 minute: 2%; 5 minutes: 1%
```

### Afficher l'utilisation du processeur sur ASDM

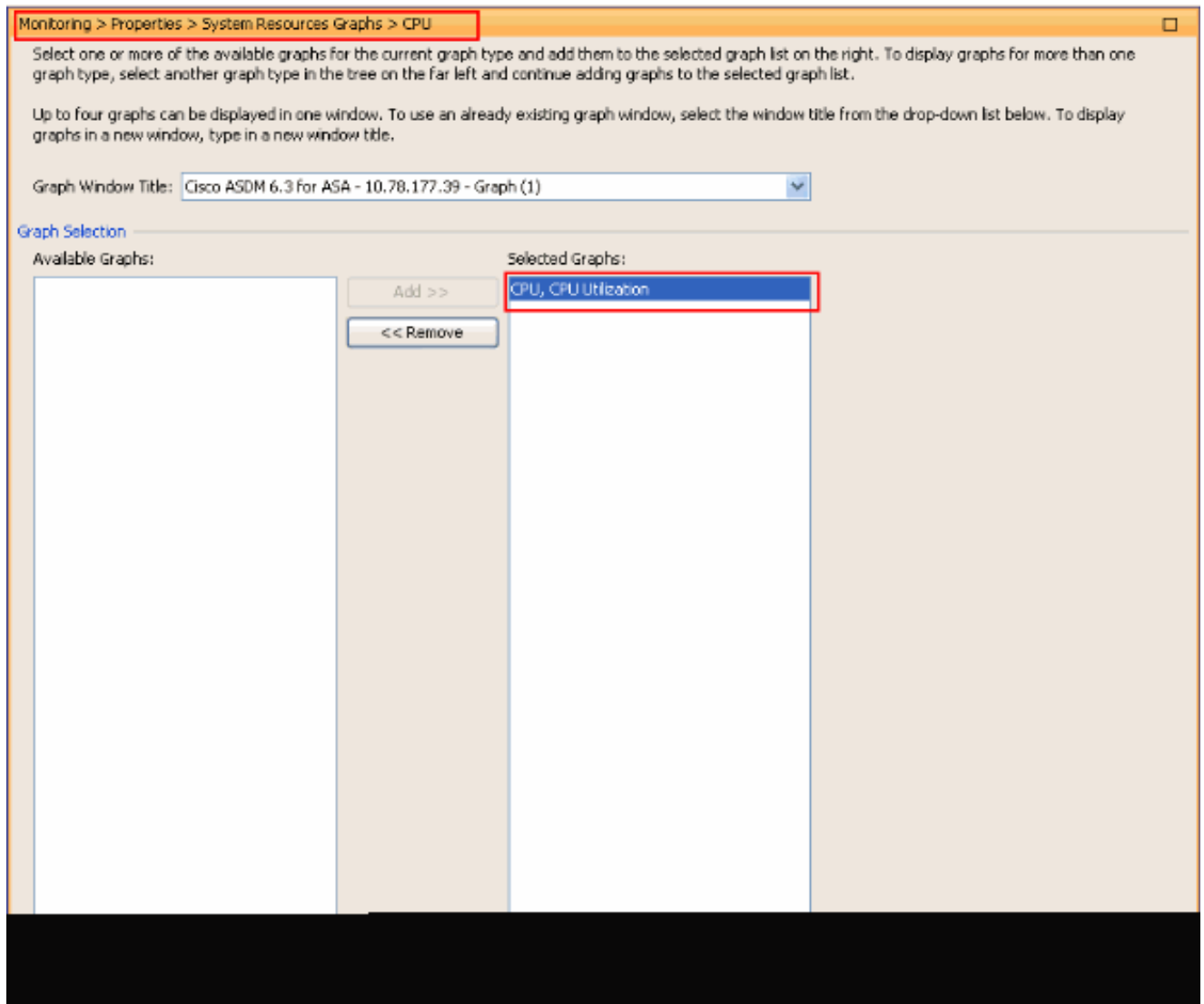
Complétez ces étapes afin d'afficher l'utilisation du CPU sur l'ASDM :

- Accédez à Monitoring > Properties > System Resources Graphics > CPU dans ASDM et sélectionnez le **titre** de la **fenêtre de graphique**. Choisissez ensuite les graphes requis dans la liste des **graphes disponibles** et cliquez sur **Ajouter** comme indiqué.

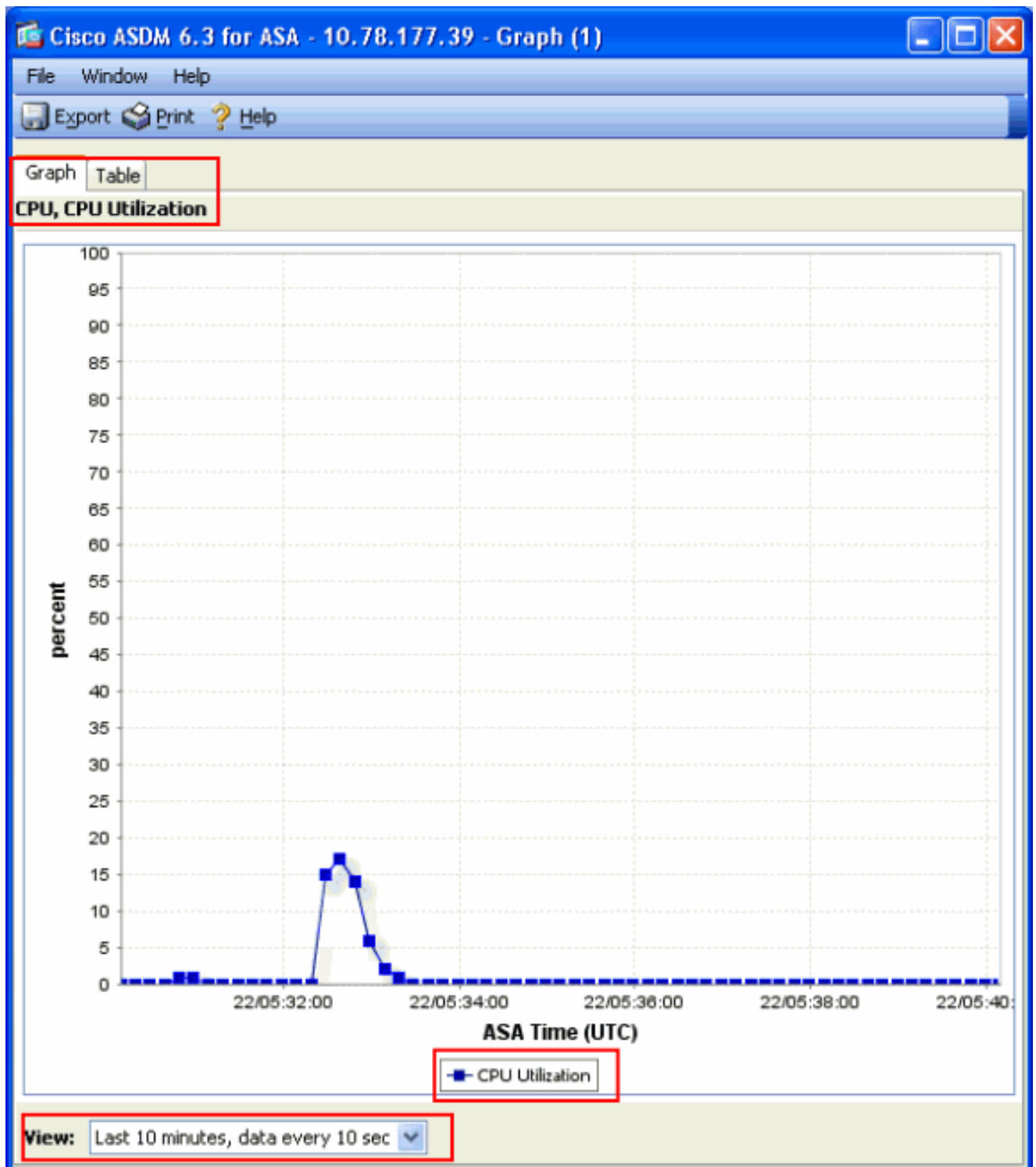




- Une fois le nom de graphique requis ajouté sous la section **Graphiques sélectionnés**, cliquez sur **Afficher les graphiques**.



L'image suivante présente le graphique **Utilisation du CPU** sur l'ASDM. Différentes vues de ce graphique sont disponibles et peuvent être modifiées lorsque la vue de la liste déroulante Vue est sélectionnée. Ce résultat peut être imprimé ou enregistré sur l'ordinateur, selon les besoins.



#### Description du résultat

Ce tableau décrit les champs du `show cpu usage` résultat.

Champ	Description
Utilisation du CPU pendant 5 secondes	Utilisation du CPU pendant les cinq dernières secondes.
1 minute	Moyenne d'exemples d'utilisation sur 5 secondes du CPU au cours de la dernière minute
5 minutes	Moyenne d'exemples d'utilisation sur 5 secondes du CPU au cours des cinq dernières minutes

show traffic

La commande `show traffic` montre la quantité de trafic qui passe par l'ASA sur une période de temps donnée. Les résultats sont basés sur le délai depuis que la commande a été lancée pour la dernière fois. Pour obtenir des résultats précis, émettez d'abord **clear traffic** la commande, puis attendez 1 à 10 minutes avant d'émettre la `show traffic` commande. Vous pouvez également émettre la `show traffic` commande et attendre 1 à 10 minutes avant de l'émettre à nouveau, mais seul le résultat de la deuxième instance est valide.

Vous pouvez utiliser la commande `show traffic` afin de déterminer combien de trafic passe par votre ASA. Si vous avez plusieurs interfaces, la commande peut vous aider à déterminer les interfaces qui envoient et qui reçoivent la plupart des données. Pour les appliances ASA avec deux interfaces, la somme du trafic entrant et sortant sur l'interface externe doit être égale à la somme du trafic entrant et sortant sur l'interface interne.

### Exemple

```
<#root>
```

```
Ciscoasa#
```

```
show traffic
```

```
outside: received (in 124.650 secs): 295468 packets 167218253 bytes 2370 pkts/sec 1341502 bytes/sec tr
```

Si vous vous rapprochez du débit évalué ou si vous l'atteignez sur une de vos interfaces, vous devez mettre à niveau vers une interface plus

rapide ou limiter le niveau de trafic entrant ou sortant de cette interface. Si vous ne le faites pas, des paquets risquent d'être abandonnés. Comme expliqué dans la **show interfaces** section, vous pouvez examiner les compteurs d'interface afin de découvrir le débit.

show perfmom

La commande `show perfmom` est utilisée pour surveiller la quantité et les types de trafic que l'ASA inspecte. Cette commande est la seule façon de déterminer le nombre de routages de traduction (xlate) et de connexions (conn) par seconde. Les connexions sont encore décomposées en connexions TCP et connexions de Protocole de datagramme utilisateur (UDP). Voir la section **description du résultat pour des descriptions du résultat que cette commande génère**.

### Exemple

```
PERFMON STATS Current Average Xlates 18/s 19/s Connections 75/s 79/s TCP Conns 44/s 49/s UDP Conns 31/s 30/s URL Access 27/s 30/s URL Serve
```

### Description du résultat

Ce tableau décrit les champs du résultat `show perfmom`.

Champ	Description
Xlates	Routages de traduction accumulés par seconde
Connexions	Connexions établies par seconde
Conn. TCP	Connexions TCP par seconde
Conn. UDP	Connexions UDP par seconde
Accès URL	Nombre d'URL (sites Web) accédés par seconde

Dem. au serveur URL	Demandes envoyées à Websense et N2H2 par seconde (filter commande requise)
Correction de TCP	Nombre de paquets TCP transmis par l'ASA par seconde
InterceptionTCPI	Nombre de paquets SYN par seconde qui ont dépassé la limite embryonnaire fixée sur un routage statique
Correction de HTTP	Nombre de paquets destinés au port 80 par seconde (commande requise <code>fixup protocol http</code> )
Correction de FTP	Commandes FTP inspectées par seconde
Authen AAA	Demandes d'authentification par seconde
Auteur AAA	Demandes d'autorisation par seconde
Compte AAA	Demandes de compte par seconde

show blocks

Avec la show cpu usage commande, vous pouvez utiliser la show blockscommande afin de déterminer si l'ASA est surchargé.

#### Blocs de paquets (1 550 et 16384 octets)

Lorsqu'il arrive dans l'interface ASA, un paquet est placé dans la file d'attente de l'interface d'entrée, transmis au système d'exploitation et placé dans un bloc. Pour les paquets Ethernet, les blocs de 1 550 octets sont utilisés ; si le paquet arrive sur une carte Gigabit Ethernet 66 MHz, les blocs de 16384 octets sont utilisés. L'ASA détermine si le paquet est autorisé ou refusé en fonction de l'algorithme ASA (Adaptive Security Algorithm) et traite le paquet jusqu'à la file d'attente de sortie sur l'interface de sortie. Si l'ASA ne peut pas prendre en charge la charge de trafic, le nombre de blocs de 1 550 octets disponibles (ou de blocs de 16384 octets pour GE à 66 MHz) passe près de 0 (comme indiqué dans la colonne CNT du résultat de la commande). Lorsque la colonne CNT atteint zéro, l'ASA tente d'allouer plus de blocs, jusqu'à un maximum de 8192. Si aucun autre bloc n'est disponible, l'ASA abandonne le paquet.

## Basculement et blocs Syslog (256 octets)

Les blocs de 256 octets sont principalement utilisés pour des messages de basculement dynamique. L'ASA actif génère et envoie des paquets à l'ASA en veille afin de mettre à jour la table de traduction et de connexion. Pendant les périodes de trafic par salves où des taux élevés de connexions sont créés ou interrompus, le nombre de blocs de 256 octets disponibles peut tomber à 0. Cette suppression indique qu'une ou plusieurs connexions ne sont pas mises à jour vers l'ASA de secours. C'est généralement acceptable parce que la prochaine fois autour du protocole de basculement dynamique rattrape le xlate ou la connexion qui sont perdus. Cependant, si la colonne CNT pour les blocs de 256 octets reste à ou près de 0 pendant des périodes prolongées, l'ASA ne peut pas suivre les tables de traduction et de connexion qui sont synchronisées en raison du nombre de connexions par seconde que l'ASA traite. Si cela se produit régulièrement, mettez à niveau l'ASA vers un modèle plus rapide.

Les messages Syslog envoyés depuis l'ASA utilisent également les blocs de 256 octets, mais ils ne sont généralement pas libérés dans une quantité telle qu'ils entraînent une diminution du pool de blocs de 256 octets. Si la colonne CNT montre que le nombre de blocs de 256 octets est près de 0, assurez-vous que vous n'effectuez la journalisation en étant sur Debugging (niveau 7) sur le serveur syslog. Ceci est indiqué par la ligne de déroutement de journalisation dans la configuration ASA. Il est recommandé de définir la journalisation sur Notification (niveau 5) ou inférieur, sauf si vous avez besoin d'informations supplémentaires à des fins de débogage.

### Exemple

```
<#root>
```

```
Ciscoasa#
```

```
show blocks
```

```
SIZE MAX LOW CNT 4 1600 1597 1600 80 400 399 400 256 500 495 499 1550 1444 1170 1188 16384 2048 1532 1
```

### Description du résultat

Ce tableau décrit les colonnes du résultat `show blocks`.

Colonne	Description
---------	-------------

ENCOLLER	E Taille, en octets, du pool de blocs. Chaque taille représente un type particulier
MAXIMUM	Nombre maximal de blocs disponibles pour le pool de blocs d'octets spécifié. Le nombre maximal de blocs sont retirés de la mémoire au démarrage. Généralement, le nombre maximal de blocs ne change pas. L'exception concerne les blocs de 256 et de 1 550 octets, où l'appliance de sécurité adaptative peut créer dynamiquement davantage de données si nécessaire, jusqu'à un maximum de 8 192.
FAIBLE	Repère de basse mer. Ce nombre indique le nombre le plus faible de blocs de cette taille disponibles depuis la mise sous tension de l'appliance de sécurité adaptative ou depuis la dernière suppression des blocs (avec la commande clear blocks). Un zéro dans la colonne LOW indique un événement précédent où la mémoire était pleine.
CNT	Nombre actuel de blocs disponibles pour ce pool de blocs de taille spécifique. Un zéro dans la colonne CNT signifie que la mémoire est pleine maintenant.

Ce tableau décrit les valeurs de ligne SIZE dans le résultat de lashow blocks commande.

Valeur de SIZE	Description
0	Utilisé par les blocs dupb.
4	Duplique les blocs existants dans les applications telles que DNS, ISAKMP, le filtrage des URL, uauth, TFTP et les modules TCP. En outre, ce bloc de taille peut être utilisé normalement par le code pour envoyer des paquets aux pilotes, et ainsi de suite.
80	Utilisé dans l'interception TCP pour générer des paquets d'accusé de réception et pour les messages Hello de basculement.
256	Utilisé pour les mises à jour de basculement dynamique, la journalisation Syslog et d'autres fonctions TCP. Ces blocs sont principalement utilisés pour les messages de basculement avec état. L'appareil de sécurité adaptatif actif génère et envoie des paquets à l'appareil de sécurité adaptatif en veille pour mettre à jour la table de traduction et de connexion. Dans le cas d'un trafic par salves, où des taux élevés de connexions sont créés ou interrompus, le nombre de blocs disponibles peut descendre à 0. Cette situation



	<p>indique qu'une ou plusieurs connexions n'ont pas été mises à jour vers l'appliance de sécurité adaptative de secours. Le protocole de basculement dynamique intercepte la traduction ou la connexion perdue la prochaine fois. Si la colonne CNT pour les blocs de 256 octets reste à 0 ou proche de 0 pendant de longues périodes, l'appliance de sécurité adaptative peine à maintenir les tables de traduction et de connexion synchronisées en raison du nombre de connexions par seconde qu'elle traite. Les messages Syslog envoyés à partir de l'appliance de sécurité adaptative utilisent également les blocs de 256 octets, mais ils ne sont généralement pas libérés dans une quantité telle qu'ils provoquent un épuisement du pool de blocs de 256 octets. Si la colonne CNT indique que le nombre de blocs de 256 octets est proche de 0, assurez-vous que vous ne vous connectez pas au niveau du débogage (niveau 7) sur le serveur syslog. Ceci est indiqué par la ligne de déroutement de journalisation dans la configuration du dispositif de sécurité adaptatif. Nous vous recommandons de définir la journalisation sur Notification (niveau 5) ou inférieur, sauf si vous avez besoin d'informations supplémentaires à des fins de débogage.</p>
1550	<p>Utilisé pour stocker des paquets Ethernet à traiter via l'appliance de sécurité adaptative. Lorsqu'un paquet entre dans une interface d'appliance de sécurité adaptative, il est placé dans la file d'attente de l'interface d'entrée, transmis au système d'exploitation et placé dans un bloc. L'appliance de sécurité adaptative détermine si le paquet doit être autorisé ou refusé en fonction de la stratégie de sécurité et traite le paquet jusqu'à la file d'attente de sortie sur l'interface de sortie. Si l'appliance de sécurité adaptative éprouve des difficultés à suivre la charge de trafic, le nombre de blocs disponibles peut être proche de 0 (comme indiqué dans la colonne CNT du résultat de la commande). Lorsque la colonne CNT est égale à zéro, le dispositif de sécurité adaptatif tente d'allouer plus de blocs, jusqu'à un maximum de 8192. Si aucun autre bloc n'est disponible, l'appliance de sécurité adaptative abandonne le paquet.</p>
16384	<p>Utilisé uniquement pour les cartes Gigabit Ethernet 64 bits 66 MHz (i82543). Reportez-vous à la description du routeur 1550 pour plus d'informations sur les paquets Ethernet.</p>
2048	<p>Trames de contrôle ou guidées utilisées pour les mises à jour de contrôle.</p>

show memory

La commande `show memory` affiche la mémoire physique totale (ou RAM) de l'ASA, ainsi que le nombre d'octets actuellement disponibles. Pour utiliser ces informations, vous devez d'abord comprendre comment l'ASA utilise la mémoire. Lorsque l'ASA démarre, il copie le système d'exploitation de la mémoire Flash dans la mémoire vive et l'exécute à partir de la mémoire vive (comme les routeurs). Ensuite, l'ASA copie la configuration de démarrage à partir de la mémoire Flash et la place dans la mémoire vive. Enfin, l'ASA alloue de la mémoire vive afin de créer les pools de blocs décrits dans la section `show blocks`. Une fois cette allocation terminée, l'ASA a besoin de mémoire vive supplémentaire uniquement si la taille de la configuration augmente. En outre, l'ASA stocke les entrées de traduction et de connexion dans la mémoire vive.

En fonctionnement normal, la mémoire libre sur l'ASA doit changer très peu, voire pas du tout. En général, la seule fois où vous devez manquer de mémoire est lorsque vous êtes attaqué et que des centaines de milliers de connexions passent par l'ASA. Afin de vérifier les connexions, émettez la commande `show conn count` qui affiche le nombre actuel et maximal de connexions via l'ASA. Si l'ASA manque de mémoire, il finit par tomber en panne. Avant le crash, vous pouvez remarquer des messages d'échec d'allocation de mémoire dans le syslog (%ASA-3-211001).

Si vous manquez de mémoire en raison d'une attaque, contactez l'équipe [d'assistance technique Cisco](#).

## Exemple

```
<#root>
```

```
Ciscoasa#
```


```
show memory
```

```
Free memory: 845044716 bytes (79%) Used memory: 228697108 bytes (21%) ----- T
```

```
show xlate
```


La commande `show xlate count` affiche le nombre actuel et maximal de traductions via l'ASA. Une traduction est un mappage d'une adresse interne à une adresse externe et peut être un mappage un-à-un, tel que Traduction d'adresses de réseau (NAT), ou un mappage plusieurs-à-un tel que Traduction d'adresses de port (PAT). Cette commande est un sous-ensemble de la `show xlate` commande, qui produit chaque traduction via l'ASA. Le résultat de la commande montre les traductions « en cours d'utilisation », qui se réfère au nombre de traductions actives dans l'ASA lorsque la commande est émise ; « le plus utilisé » se réfère au nombre maximal de traductions jamais vues sur l'ASA depuis sa mise sous tension.

---

 **Remarque** : un hôte unique peut avoir plusieurs connexions vers différentes destinations, mais une seule traduction. Si le nombre de `xlate` est nettement supérieur au nombre d'hôtes sur votre réseau interne, il est possible qu'un de vos hôtes internes ait été compromis. Si votre hôte interne a été compromis, il usurpe l'adresse source et envoie des paquets à l'ASA.

---

---

 **Remarque** : lorsque la configuration `vpnclient` est activée et que l'hôte interne envoie des requêtes DNS, la commande peut répertorier plusieurs `show xlate xlate` pour une traduction statique.

---

## Exemple

```
<#root>
```

```
Ciscoasa#
```

```
show xlate count
```

```
84 in use, 218 most used
```

```
<#root>
```

```
Ciscoasa(config)#
```

```
show xlate
```

```
3 in use, 3 most used Flags: D - DNS, d - dump, I - identity, i - inside, n - no random, o - outside,  
TCP PAT from inside:10.1.1.15/1026 to outside:192.168.49.1/1024 flags ri idle 62:33:57 timeout 0:00:30  
  
UDP PAT from 10.1.1.15/1028 to outside:192.168.49.1/1024 flags ri idle 62:33:57 timeout 0:00:30  
  
ICMP PAT from inside:10.1.1.15/21505 to outside:192.168.49.1/0 flags ri idle 62:33:57 timeout 0:00:30
```

La première entrée est une traduction d'adresses de port TCP pour le port hôte (10.1.1.15, 1026) sur le réseau interne au port hôte (192.168.49.1, 1024) sur le réseau externe. L'indicateur « r » dénote que la traduction est une traduction d'adresse de port. L'indicateur « i » dénote que la traduction s'applique au port interne de l'adresse.

La deuxième entrée est une traduction d'adresses de port UDP pour le port hôte (10.1.1.15, 1028) sur le réseau interne au port hôte (192.168.49.1, 1024) sur le réseau externe. L'indicateur « r » dénote que la traduction est une traduction d'adresse de port. L'indicateur « i » dénote que la traduction s'applique au port interne de l'adresse.

La troisième entrée est une traduction d'adresse de port ICMP pour l'id de l'hôte ICMP (10.1.1.15, 21505) sur le réseau interne à l'id de l'hôte ICMP (192.168.49.1, 0) sur le réseau externe. L'indicateur « r » dénote que la traduction est une traduction d'adresse de port. L'indicateur « i »

dénote que la traduction s'applique au port interne de l'adresse.

Les champs internes d'adresse apparaissent comme adresses sources sur les paquets qui passent de l'interface plus sécurisée à l'interface moins sécurisée. Réciproquement, ils apparaissent comme adresses de destination sur les paquets qui passent de l'interface moins sécurisée à l'interface plus sécurisée.

```
show conn count
```

La commande `show conn count` affiche le nombre actuel et maximal de connexions via l'ASA. Une connexion est un mappage des informations de la couche 4 d'une adresse interne à une adresse externe. Les connexions sont établies lorsque l'ASA reçoit un paquet SYN pour les sessions TCP ou lorsque le premier paquet d'une session UDP arrive. Les connexions sont interrompues lorsque l'ASA reçoit le paquet ACK final, ce qui se produit lorsque la connexion de session TCP se ferme ou lorsque le délai d'attente expire dans la session UDP.

Un nombre de connexions extrêmement élevé (50 à 100 fois la normale) peut indiquer que vous êtes attaqué. Émettez la commande `show memory` afin de vous assurer que le nombre élevé de connexions n'entraîne pas le manque de mémoire de l'ASA. Si vous êtes soumis à des attaques, vous pouvez limiter le nombre maximal de connexions par entrée statique et également limiter le nombre maximal de connexions embryonnaires. Cette action protège vos serveurs internes et évite leur surcharge. Référez-vous au [Guide de configuration de la gamme Cisco ASA 5500 avec l'interface de ligne de commande, 8.4 et 8.6](#) pour plus d'informations.

### Exemple

```
<#root>
```

```
Ciscoasa#
```

```
show conn count
```

```
2289 in use, 44729 most used
```

```
show interface
```

La commande [show interface](#) peut aider à déterminer les problèmes de non-correspondance de mode duplex et les problèmes de câble. Elle peut également fournir un meilleur aperçu si l'interface est dépassée. Si la capacité du processeur de l'ASA est insuffisante, le nombre de blocs de 1

550 octets est proche de 0. (Observez les blocs de 16384 octets sur les cartes Gig 66 MHz.) Un autre indicateur est l'augmentation de « l'absence de mémoires tampon » sur l'interface. Le message no buffers indique que l'interface ne peut pas envoyer le paquet au système d'exploitation ASA car il n'y a aucun bloc disponible pour le paquet et le paquet est abandonné. Si aucune augmentation des niveaux de mémoire tampon ne se produit régulièrement, émettez la show proc cpu commande afin de vérifier l'utilisation du CPU sur l'ASA. Si l'utilisation du CPU est élevée en raison d'une charge de trafic élevée, mettez à niveau vers un ASA plus puissant qui peut gérer la charge.

Quand un paquet arrive dans une interface, il est d'abord placé dans la file d'attente matérielle d'entrée. Si la file d'attente matérielle d'entrée est pleine, le paquet est placé dans la file d'attente logicielle d'entrée. Le paquet est passé de sa file d'attente d'entrée et placé dans un bloc de 1 550 octets (ou dans un bloc de 16384 octets sur des interfaces Gigabit Ethernet 66 MHz). L'ASA détermine ensuite l'interface de sortie pour le paquet et place le paquet dans la file d'attente matérielle appropriée. Si la file d'attente matérielle est pleine, le paquet est placé dans la file d'attente logicielle de sortie. Si les blocs maximaux dans l'une ou l'autre des files d'attente de logiciel sont grands, alors l'interface est débordée. Par exemple, si 200 Mbits/s entrent dans l'ASA et sortent tous sur une seule interface de 100 Mbits/s, la file d'attente du logiciel de sortie indique des nombres élevés sur l'interface sortante, ce qui indique que l'interface ne peut pas gérer le volume de trafic. Si vous vous trouvez face à cette situation, mettez à niveau vers une interface plus rapide.

### Exemple

```
<#root>
```

```
Ciscoasa#
```

```
show interface
```

```
Interface GigabitEthernet0/1 "inside", is up, line protocol is up Hardware is i82546GB rev03, BW 1000
```

Vous devez également vérifier si l'interface comporte des erreurs. Si vous recevez des runts, des erreurs en entrée, des CRC, ou des erreurs de trame, il est probable que vous ayez une erreur de correspondance de duplex. Le câble peut également être défectueux. Voir la section [Paramètres de vitesse et de duplex pour plus d'informations sur les problèmes de duplex](#). Souvenez-vous que chaque compteur d'erreur représente le nombre de paquets qui sont abandonnés en raison de cette erreur particulière. Si vous voyez un compteur spécifique qui s'incrémente régulièrement, les performances de votre ASA en pâtissent très probablement, et vous devez trouver la cause première du problème.


Pendant que vous examinez les compteurs d'interface, notez que si l'interface est définie en mode bidirectionnel simultané, vous ne devez pas rencontrer de collisions, de collisions tardives ou de paquets différés. Inversement, si l'interface est définie sur le mode bidirectionnel non simultané, vous devez recevoir des collisions, certaines collisions tardives et peut-être certains paquets différés. Le nombre total de collisions, de collisions tardives et de paquets différés ne doit pas dépasser 10 % de la somme des compteurs de paquets d'entrée et de sortie. Si vos collisions dépassent 10 % de votre trafic total, alors la liaison est surchargée, et vous devez effectuer une mise à niveau en duplex intégral ou à une vitesse plus rapide (de 10 à 100 Mbps). Rappelez-vous que des collisions de 10 % signifient que l'ASA abandonne 10 % des paquets qui passent par cette interface ; chacun de ces paquets doit être retransmis.

Référez-vous à la interface commande dans les [Références des commandes des appareils de sécurité adaptatifs de la gamme Cisco ASA 5500](#) pour des informations détaillées sur les compteurs d'interface.

show processes

La commande **show processes** sur l'ASA affiche tous les processus actifs qui s'exécutent sur l'ASA au moment où la commande est exécutée. Ces informations de routage sont utiles pour déterminer les processus qui reçoivent trop de temps du CPU et ceux qui n'en reçoivent aucun. Afin d'obtenir ces informations, émettez la **show processes** commande deux fois ; attendez environ 1 minute entre chaque instance. Pour le processus en question, soustrayez la valeur d'exécution affichée dans le deuxième résultat de la valeur d'exécution affichée dans le premier résultat. Ce résultat indique le temps processeur (en millisecondes) que le processus a reçu au cours de cet intervalle. Notez que certains processus sont planifiés pour fonctionner à des intervalles particuliers, et une partie traite seulement le passage quand elles ont les informations à traiter. Le processus 577poll a très probablement la plus grande valeur d'exécution de tous vos processus. C'est normal parce que le processus 577poll interroge les interfaces Ethernet afin de déterminer si elles ont des données qui doivent être traitées.

---

 **Remarque** : l'examen de chaque processus ASA n'est pas traité dans ce document, mais il est brièvement mentionné pour en vérifier l'exhaustivité. Référez-vous à [ASA 8.3 et versions ultérieures : Surveiller et dépanner les problèmes de performances](#) pour plus d'informations sur les processus ASA.

---

## Résumé des commandes

En résumé, utilisez la commande **show cpu usage** afin d'identifier la charge sous laquelle l'ASA est. Souvenez-vous que le résultat est une moyenne en cours d'exécution ; l'ASA peut avoir des pics plus élevés d'utilisation du processeur qui sont masqués par la moyenne en cours d'exécution. Une fois que l'ASA atteint 80 % d'utilisation du CPU, la latence via l'ASA augmente lentement jusqu'à environ 90 % de CPU. Lorsque l'utilisation du CPU est supérieure à 90 %, l'ASA commence à abandonner des paquets.

Si l'utilisation du CPU est élevée, utilisez la **show processes** commande afin d'identifier les processus qui utilisent le plus de temps CPU. Utilisez ces informations afin de réduire une partie du temps consommé par les processus intensifs (tels que la journalisation).

Si le CPU ne fonctionne pas à chaud, mais que vous pensez que les paquets sont toujours abandonnés, utilisez la commande afin de vérifier l'interface ASA pour l'absence de tampons et de collisions, peut-être causée par une non-correspondance de duplex, **show interface** pour vérifier l'interface ASA. Si le nombre d'absences de mémoire tampon augmente par incrément, et que l'utilisation du CPU n'est pas faible, l'interface ne peut pas prendre en charge le trafic qui la traverse.

Si les mémoires tampon n'ont aucun problème, vérifiez les blocs. `show blocks` Si la colonne CNT actuelle dans la sortie est proche de 0 sur les blocs de 1550 octets (blocs de 16384 octets pour les cartes Gig 66 MHz), l'ASA abandonne très probablement les paquets Ethernet parce qu'il est trop occupé. Dans ce cas, le processeur atteint un pic.

Si vous rencontrez des problèmes lorsque vous établissez de nouvelles connexions par le biais de l'ASA, utilisez la `show conn count` commande afin de vérifier le nombre actuel de connexions par le biais de l'ASA.

Si le nombre actuel est élevé, vérifiez le résultat `show memory` afin de vous assurer que l'ASA ne manque pas de mémoire. Si la mémoire est faible, recherchez la source des connexions à l'aide de la commande `show conn` ou `show local-host` afin de vérifier que votre réseau n'a pas subi d'attaque par déni de service.

Vous pouvez utiliser d'autres commandes afin de mesurer la quantité de trafic qui passe par l'ASA. La **`show traffic`** commande affiche l'ensemble des paquets et octets par interface, et la `show perfmon` divise le trafic en différents types que l'ASA inspecte.

#### Informations connexes

- [Pare-feu Cisco ASA 5500-X](#)
- [Assistance technique de Cisco et téléchargements](#)

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.