ASA 8.3 et plus tard : Surveiller et dépanner les problèmes de performance

Contenu

Introduction

Ce document fournit des informations au sujet d'ASA commande que vous pouvez utiliser pour surveiller et dépanner la représentation d'une appliance de sécurité adaptable Cisco (ASA).

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur une appliance de sécurité adaptable Cisco (ASA) cette version 8.3 et ultérieures de passages.

Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si vous travaillez dans un réseau opérationnel, assurez-vous de bien comprendre l'impact potentiel de toute commande avant de l'utiliser.

Conventions

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

Dépannez

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

> Remarque: Si vous avez la sortie de la **commande show de** votre périphérique de Cisco, vous pouvez employer l'analyseur de Cisco CLI (clients enregistrés seulement) afin d'afficher des éventuels problèmes et des difficultés. L'analyseur de Cisco CLI prend en charge certaines **commandes show**. Si vous utilisez l'analyseur de Cisco CLI, vous devez être un client enregistré, vous devez être ouvert une session à votre compte Cisco, et vous devez avoir le Javascript activé chez 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 certaines situations qui peuvent faire échouer le processus de négociation automatique et qui peuvent provoquer une disparité dans la vitesse ou le duplex (et créer 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 sont en général assez fixes, donc si vous les configurez correctement, vous ne devriez pas avoir à les changer.

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 duplex, ils vont s'échanger des trames (appelées Fast Link Pulses, ou FLP) qui vont annoncer leurs capacités de vitesse et de 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, ce sera l'autre périphérique qui se chargera de recevoir les FLP et de passer en mode de détection parallèle. Afin de détecter la vitesse du partenaire, le périphérique se met à l'écoute des longueurs d'impulsions pour définir ensuite la vitesse en conséquence. Le problème surgit lors de la configuration du duplex. Puisque le duplex doit être négocié, le périphérique qui est placé pour autonégocier ne peut pas déterminer les configurations sur l'autre périphérique, ainsi il se transfère sur bidirectionnel-alterné, comme stipulé dans la norme d'IEEE 802.3u.

Par exemple, si vous configurez l'interface ASA pour la négociation automatique et la connectez à un commutateur qui est codé en dur pour des 100 Mbits/s et bidirectionnel simultané, l'ASA envoie FLPs. Cependant, le commutateur ne réagira pas, car il est codé en dur pour la vitesse et le duplex et ne participe pas à la négociation automatique. Puisqu'il ne reçoit aucune réponse du commutateur, les transitions ASA dans le mode parallèle de détection et sent la longueur des impulsions dans les trames que le commutateur envoie. C'est-à-dire, l'ASA sent que le commutateur est placé aux 100 Mbits/s, ainsi il place la vitesse d'interface en conséquence.

Cependant, parce que le commutateur ne permute pas FLPs, l'ASA ne peut pas la détecter si le commutateur peut exécuter bidirectionnel simultané, ainsi l'ASA place le duplex d'interface à bidirectionnel-alterné, comme stipulé dans la norme d'IEEE 803.2u. Puisque le commutateur est codé en dur aux 100 Mbits/s et bidirectionnel simultané, et l'ASA a juste autonégocié aux 100 Mbits/s et bidirectionnel-alterné (comme elle devrait), le résultat est un conflit du mode bidirectionnel qui peut poser des 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 incrémentent 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

```
Interface GigabitEthernet0/0 "outside", 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
       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, 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)
```

Utilisation du CPU

Si vous notiez l'utilisation du processeur est élevée, se terminent ces étapes afin de dépanner :

1. Vérifiez que le nombre de connexions dans la commande **show xlate count** est bas.
2. Vérifiez que le bloc mémoire est normal.
3. Vérifiez que le nombre d'ACL est plus élevé.

4. Émettez la commande de **détail de show memory**, et la vérifiez que la mémoire utilisée par l'ASA est utilisation normale.

5. Vérifiez que les nombres dans les commandes **show processes cpu-hog** et **show processes memory** sont normaux.

6. Tout hôte se trouvant à l'intérieur ou à l'extérieur de l'appliance 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.

7. Vérifiez le duplex et les configurations de débit dans des interfaces ASA. Le paramètre de non-correspondance avec les interfaces distants peut augmenter l'utilisation du CPU.

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

   ```
   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: Le routage Cisco recommande que vous activiez la commande d'interface ip verify reverse-path sur toutes les interfaces, car elle abandonnera les paquets qui n'ont pas une source adresse valide, ce qui entraîne une utilisation moins intensive du CPU. Ceci s'applique à FWSM faisant face aux questions élevées CPU.
8. Une autre raison pour l'utilisation élevée du CPU peut être due à un trop grand nombre d'itinéraires de multidiffusion. Émettez la commande de mroute d'exposition afin de vérifier si l'ASA reçoit trop de routes multicasts.

9. Utilisez la commande show local-host afin de vérifier si le réseau rencontre une attaque de déni de service, qui peut signaler une attaque virale dans le réseau.

10. La CPU de haute pourrait se produire en raison de l'ID de bogue Cisco CSCsq48636. Référez-vous au pour en savoir plus de l'ID de bogue Cisco CSCsq48636 (clients

enregistrés seulement).

Remarque: Si la solution fournissait en haut ne résout pas le problème, améliorent la plate-forme ASA selon les conditions requises. Référez-vous à la fiche technique de Dispositifs de sécurité adaptatifs dédiés de la gamme Cisco ASA 5500 pour plus d'informations sur des capacités et des capacités de plate-forme d'appliance de sécurité adaptable. Entrez en contact avec TAC (clients enregistrés seulement) pour de plus amples informations.

Utilisation élevée de la mémoire

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

- **Journalisation des événements :** La journalisation des événements peut consommer une grande quantité 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 identifié dans le logiciel d'appliance de sécurité peut mener à une consommation élevée de mémoire. Afin de résoudre ce problème, mettez à niveau le logiciel d'appliance de sécurité.
- **Débogage activé :** Le débogage peut consommer une grande quantité 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'une appliance de sécurité entraîne une très grande consommation de mémoire au niveau de l'appliance de sécurité afin de bloquer les paquets à travers les ports spécifiés. Afin de résoudre ce problème, bloquez le trafic de routage offensant du côté de l'ISP.
- **Menace-détection :** La fonctionnalité de détection de menace se compose de différents niveaux de collecte de statistiques pour différentes menaces, aussi bien que de la détection de menaces d'analyse, qui détermine quand 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. En soi, plusieurs des paramètres de port par défaut ne sont pas desirables quand une ASA est

branchée 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 une ASA à un commutateur qui exécute le SYSTÈME D'EXPLOITATION de Catalyst, désactivez l'acheminement, désactivez la jonction, et l'enable 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 poser des problèmes de routage si un autre périphérique tente de négocier automatiquement la vitesse et le duplex 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 Catalyst de la série XL, la transmission n'est pas définie par défaut sur Auto. Pour cette raison, vous devriez désactiver l'acheminement sur n'importe quel port de commutateur qui se connecte à une 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 poser des problèmes de routage avec la négociation automatique de 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 le routage par défaut de 30 secondes (15 secondes à écouter et 15 secondes à apprendre) ; au lieu de cela, cette action pousse le commutateur à mettre le port en état de transmission juste après que la liaison est établie. 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 que vous activez PortFast sur n'importe quel port de commutateur qui

se connecte à une ASA.

> Remarque: Les versions du système d'exploitation pour Catalyst 5.4 et ultérieures incluent la commande **set port host <mod>/<port>** qui permet d'utiliser une commande simple pour désactiver la transmission et la liaison de jonction, et activer PortFast.

Traduction d'adresses réseau (NAT)

Àchaque 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 de l'écoulement de tout le trafic par le périphérique peut se produire quand vous globalement des clears xlate sur les dispositifs de sécurité.

Échantillonnez la configuration ASA pour PAT qui utilise l'adresse IP extérieure d'interface :

```
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)
```

Le trafic qui traverse l'appliance de sécurité passe très probablement par un NAT. Afin d'afficher les routages de traduction qui sont en service sur l'appliance de sécurité, lancez la commande **show xlate** :

```
Ciscoasa#show xlate

5 in use, 5 most used

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

NAT from any:192.168.1.10 to any:172.16.1.1/24

    flags s idle 277:05:26 timeout 0:00:00
```

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

```
Ciscoasa#clear xlate

Ciscoasa#show xlate
0 in use, 1 most used
```

La commande **clear xlate** efface toute la traduction dynamique actuelle de la table de routage de xlate. Afin d'effacer un routage de traduction particulier d'IP, vous pouvez utiliser la commande **clear xlate** avec le mot clé **de l'[adresse ip]** global.

Voici une configuration de l'échantillon ASA pour NAT :

```
Ciscoasa#show xlate
0 in use, 1 most used
```

Observez le résultat de **show xlate** pour le routage de traduction de 10.2.2.2 interne à 10.10.10.10 globale externe :

```
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 :

```
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 :

```
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 Syslog te permettent pour dépanner des questions sur l'ASA. Cisco offre un serveur libre de Syslog pour Windows NT a appelé le serveur de Syslog de Pare-feu ASA (PFSS). Vous pouvez télécharger PFSS de la page de téléchargements de logiciels (clients enregistrés seulement).

Plusieurs autres fournisseurs, tels que Kiwi Enterprises , offrent des serveurs syslog pour différentes plates-formes Windows, telles que Windows 2000 et Windows XP. La plupart des machines UNIX et Linux ont des serveurs syslog installés par défaut.

Quand vous installez le serveur de Syslog, configurez l'ASA afin de lui envoyer des logs.

Exemple :

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

Remarque: Cet exemple configure l'ASA pour envoyer l'élimination des imperfections

(niveau des Syslog 7) et plus essentiels au serveur de Syslog. Puisque ces logs ASA sont les plus bavards, utilisez-les seulement quand vous dépannez une question. 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.) Vérifiez les messages qui indiquent le serveur externe jugé pour accéder à l'adresse IP interne sur le port TCP 113 (pour le protocole d'identification, ou l'ident), mais l'ASA a refusé le paquet. Le message devrait être semblable à l'exemple suivant :

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

Si vous recevez ce message, fournissez la commande de resetinbound de service à l'ASA. L'ASA ne relâche pas silencieusement des paquets ; au lieu de cela, cette commande fait remettre à l'état initial immédiatement l'ASA n'importe quelle connexion entrante qui est refusée par la stratégie de sécurité. Le serveur n'attend pas le paquet Ident pour arrêter sa connexion TCP ; au lieu de cela, elle reçoit immédiatement un paquet de réinitialisation.

SNMP

La surveillance de la représentation de Cisco ASA utilisant le SNMP est la méthode recommandée pour les déploiements en entreprise. Cisco ASA prend en charge la Surveillance de réseau avec des versions 1 SNMP, 2c et 3.

Vous pouvez configurer les dispositifs de sécurité pour envoyer des déroutements à un serveur de Gestion de réseau (NMS), ou vous pouvez employer les NMS pour parcourir le MIB sur les dispositifs de sécurité. Le MIB est une collection de définitions, et les dispositifs de sécurité mettent à jour une base de données des valeurs pour chaque définition. Pour plus d'informations sur ceci, référez-vous à configurer le SNMP sur Cisco ASA.

Tout le MIB pris en charge pour Cisco ASA peut être trouvé à la liste de support MIB ASA. De cette liste, ce MIB est utile pour la supervision des 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 des objets de mémoire.

Recherches DNS inversées

Si vous éprouvez la représentation lente avec l'ASA, vérifiez que vous avez des enregistrements du pointeur de système de noms de domaine (PTR de DN), également connus sous le nom d'enregistrements inverses de consultation de DN, dans le serveur DNS bien fondé pour les adresses externes que l'ASA utilise. Ceci inclut n'importe quelle adresse dans votre groupe global de Traduction d'adresses de réseau (NAT) (ou l'ASA en dehors de l'interface si vous surchargez sur l'interface), n'importe quelle adresse statique, et adresse interne (si vous n'utilisez pas NAT avec elles). Quelques applications, telles que le Protocole de transfert de fichiers (FTP) et les serveurs Telnet, peuvent employer des recherches DNS inversées afin de déterminer l'origine de 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, lancez la **commande nslookup** de votre PC ou de votre ordinateur UNIX ; incluez l'adresse IP globale que vous utilisez pour vous connecter au routage Internet.

Exemple

```
% nslookup 198.133.219.25
25.219.133.198.in-addr.arpa     name = www.cisco.com.
```

Vous devez recevoir une réponse en retour avec le nom de DNS du périphérique attribué 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 de capacité sur l'interface

Si vous avez une rafale du trafic, les paquets lâchés peuvent se produire si la rafale dépasse la capacité tampon du tampon FIFO sur le NIC et les mémoires tampons de sonnerie de réception. L'activation des trames de pause pour le contrôle de flux peut alléger cette question. La pause (XOFF) et les trames XON sont générées automatiquement par le NIC réalisé par matériel sur

l'utilisation de tampon FIFO. Une trame de pause est envoyée quand l'utilisation de mémoire tampon dépasse la marque des grandes marées. Afin d'activer des trames de la pause (XOFF) pour le contrôle de flux, utilisez cette commande :

```
hostname(config)#interface tengigabitethernet 1/0

hostname(config-if)#
flowcontrol send on
```

Référez-vous à activer l'interface physique et à configurer le pour en savoir plus de paramètres d'Ethernets.

Commandes show

show cpu usage

La commande d'**utilisation de show cpu** est utilisée de déterminer la charge de la circulation placée sur la CPU 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 a une CPU simple pour traiter un grand choix de tâches ; par exemple, il traite des paquets et imprime des messages de débogage à 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 CPU-le plus intensif, ainsi si votre ASA passe beaucoup de trafic par des tunnels chiffrés, vous devriez considérer une ASA plus rapide, un concentrateur dédié VPN, tel que le VPN 3000. Le VCA débarque le cryptage et le déchiffrement de la CPU ASA et l'exécute dans le matériel sur la carte. Ceci permet à l'ASA pour chiffrer et déchiffrer des 100 Mbits/s du trafic avec 3DES (cryptage 168-bit).

La journalisation est un autre processus qui peut consommer une grande quantité de ressources système. Pour cette raison, il est recommandé que vous désactivez la console, moniteur, et mettez en mémoire tampon ouvrir une session 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 que l'utilisation de Syslog ou la journalisation par Protocole de gestion de réseau simple (SNMP) (historique de journalisation) soit définie au niveau 5 (Notification) ou inférieur. En outre, vous pouvez désactiver des ID spécifiques de messages syslog avec la commande **no logging message <id_syslog>**.

Le Cisco Adaptive Security Device Manager (ASDM) fournit également un graphique sur l'onglet de surveillance qui te permet pour visualiser l'utilisation du CPU de l'ASA au fil du temps. Vous pouvez employer ce graphique afin de déterminer le chargement sur votre ASA.

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

Exemple

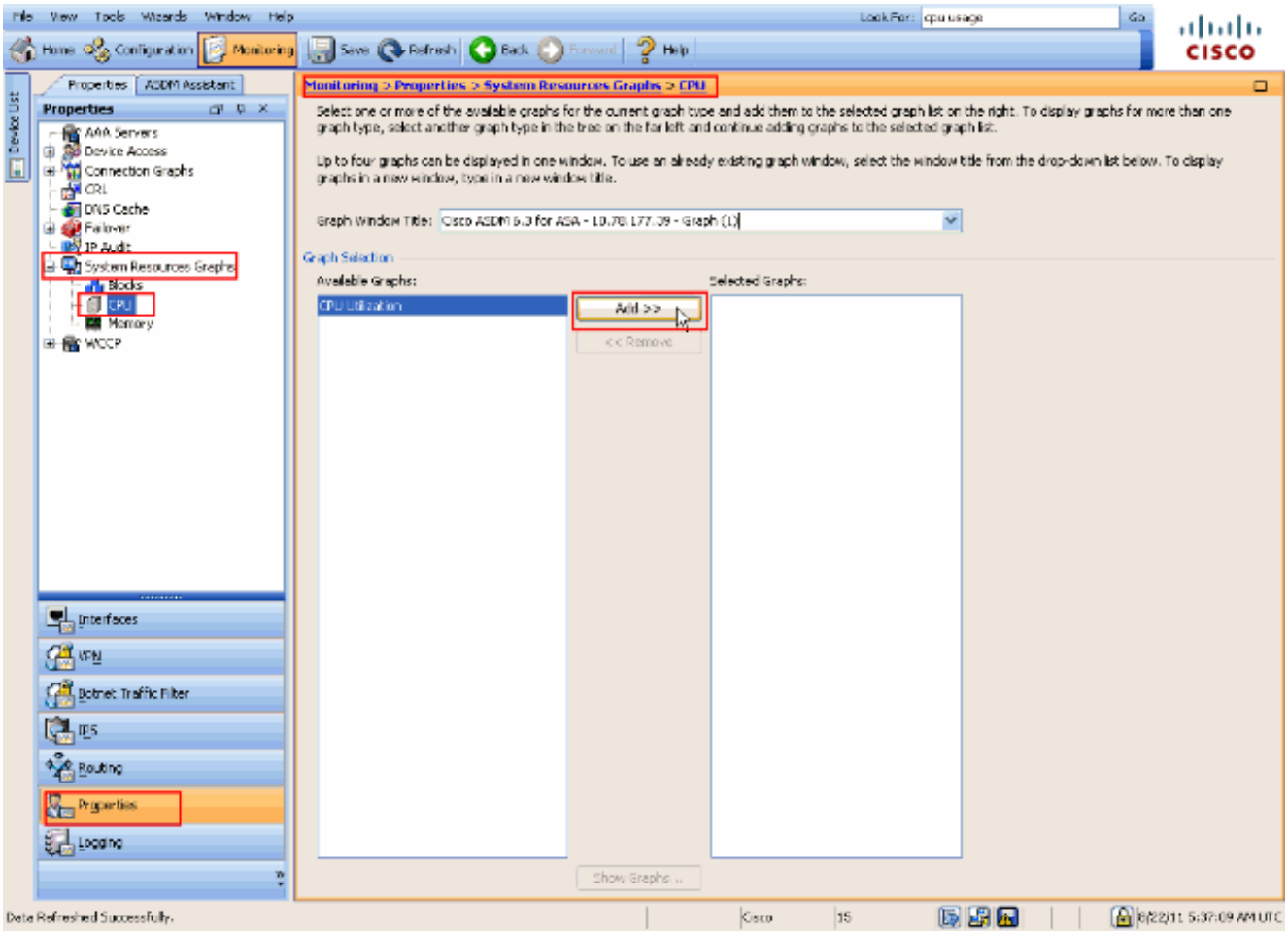
```
Ciscoasa#show cpu usage

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

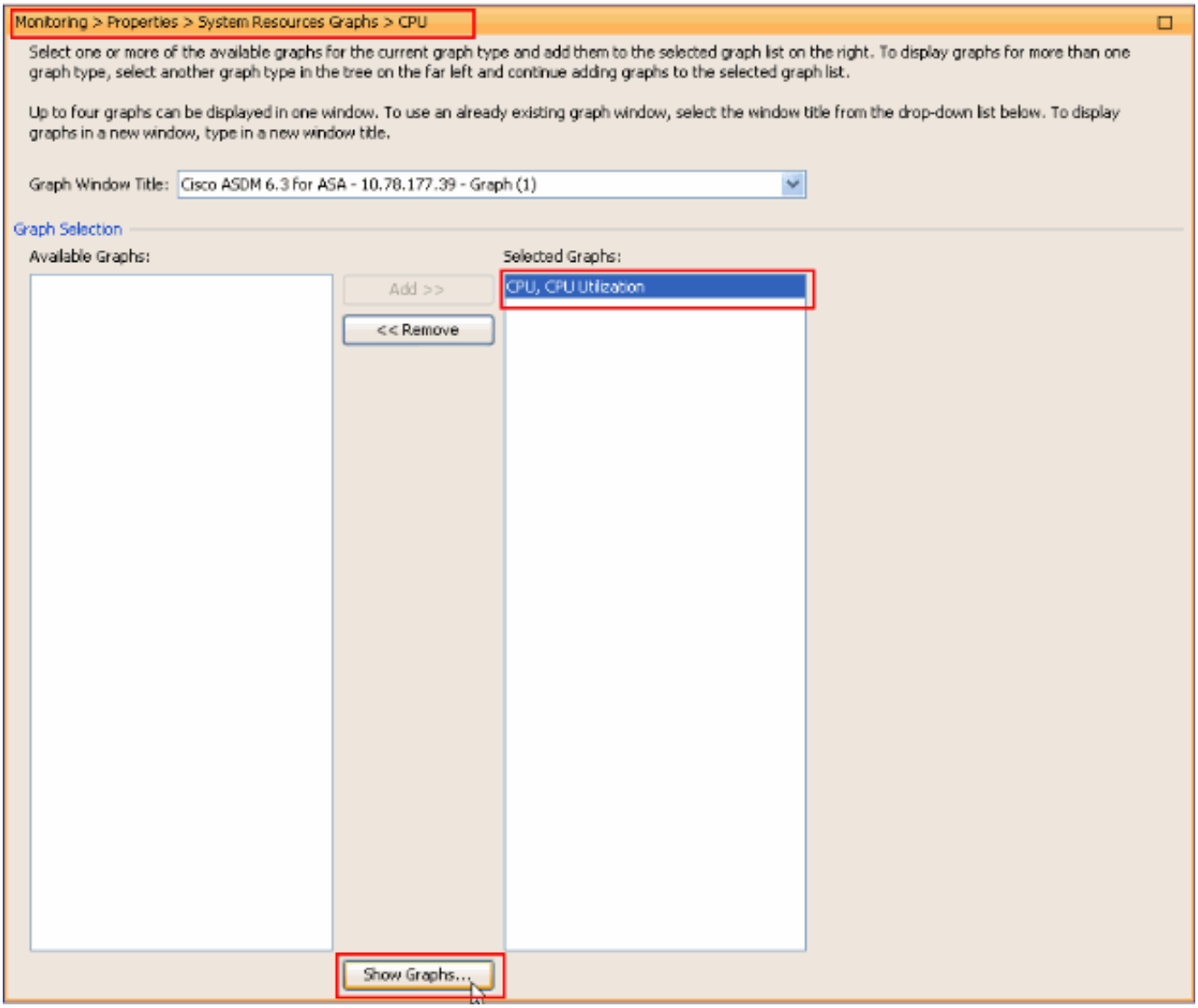
Visionnement de l'utilisation du CPU sur l'ASDM

Terminez-vous ces étapes afin de visualiser l'utilisation du CPU sur l'ASDM :

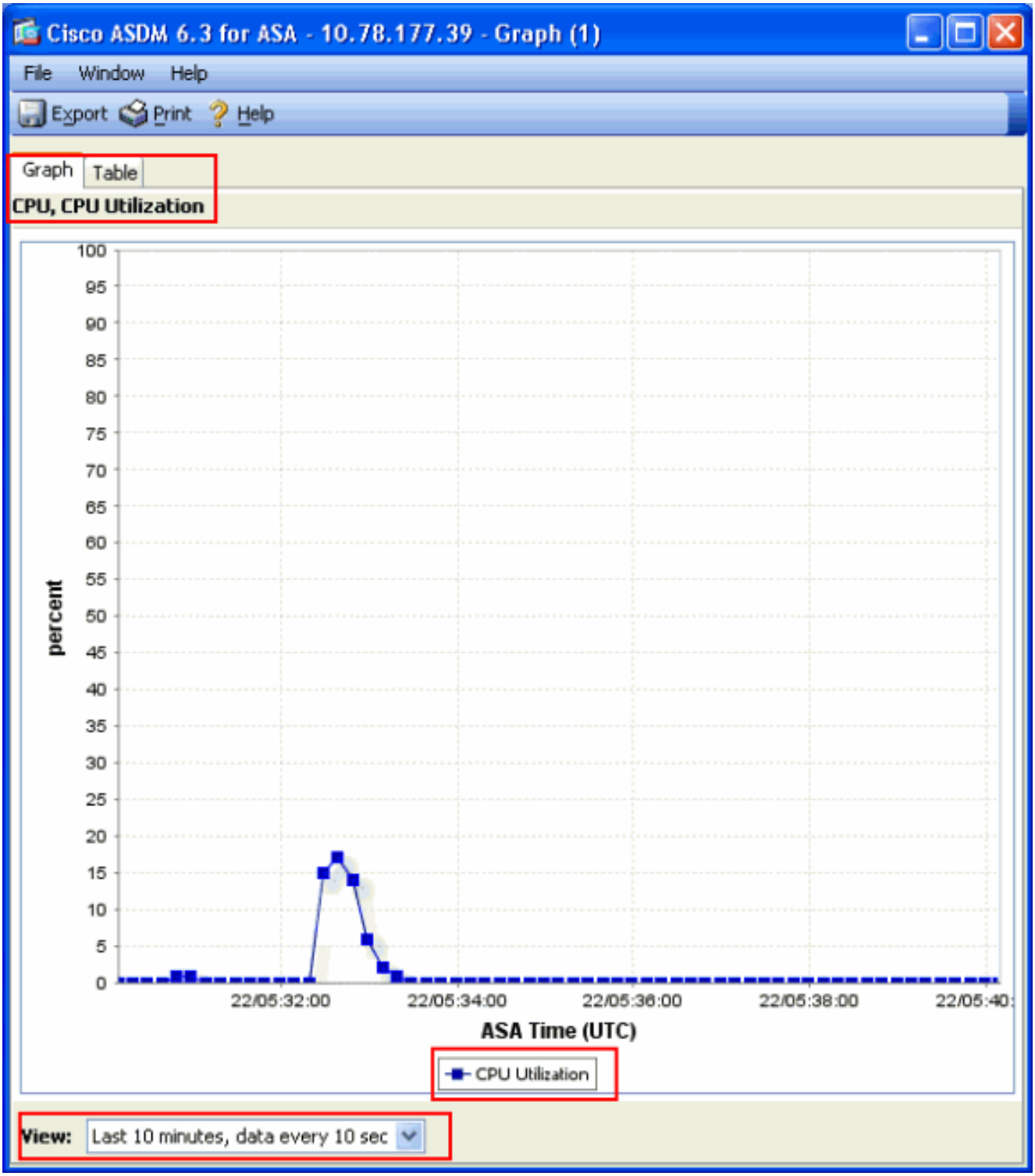
1. Allez à la **surveillance > Properties > les graphiques de ressources système > la CPU** dans l'ASDM et choisissez le **titre de fenêtre de graphique**. Puis, choisissez les graphiques requis de la liste de **graphiques disponibles** et cliquez sur Add comme affiché.



2. Une fois que le nom exigé de graphique est ajouté sous les **graphiques sélectionnés** sectionnez, cliquez sur les **graphiques d'exposition**.



La prochaine image affiche le graphique d'**utilisation du CPU** sur l'ASDM. Les différentes vues de ce graphique sont disponibles et peuvent être changées en sélectionnant la vue de la liste déroulante de vue. Cette sortie peut être imprimée ou enregistrée à l'ordinateur au besoin.



[Description du résultat]

Ce tableau décrit les champs dans le résultat de **show cpu usage** .

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 dernières minutes

show traffic

La commande de **show traffic** affiche combien de trafic qui traverse l'ASA sur une période donnée. Les résultats sont basés sur le délai depuis que la commande a été lancée pour la dernière fois. Pour des résultats exacts, lancez d'abord la commande **clear traffic**, puis attendez 1 à 10 minutes avant de lancer la commande **show traffic**. Vous pouvez également lancer la commande **show traffic** et attendre 1 à 10 minutes avant de lancer la commande de nouveau, mais seul le résultat de la deuxième instance est valide.

Vous pouvez employer la commande de **show traffic** afin de déterminer combien de trafic traverse 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 des appliances ASA avec deux interfaces, la somme du trafic en entrée et en sortie sur l'interface extérieure devrait égaler la somme du trafic en entrée et en sortie sur l'interface interne.

Exemple

```
Ciscoasa#show traffic
outside:
        received (in 124.650 secs):
                295468 packets  167218253 bytes
                2370 pkts/sec   1341502 bytes/sec
        transmitted (in 124.650 secs):
                260901 packets  120467981 bytes
                2093 pkts/sec   966449 bytes/sec
inside:
        received (in 124.650 secs):
                261478 packets  120145678 bytes
                2097 pkts/sec   963864 bytes/sec
        transmitted (in 124.650 secs):
                294649 packets  167380042 bytes
                2363 pkts/sec   1342800 bytes/sec
```

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 section show interface, vous pouvez examiner les compteurs de l'interface afin de découvrir les détails concernant le débit.

show perfmon

La commande de perfmon d'exposition est utilisée de surveiller la quantité et les types de trafic que l'ASA examine. 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

```
Ciscoasa#show traffic
outside:
        received (in 124.650 secs):
                295468 packets  167218253 bytes
                2370 pkts/sec   1341502 bytes/sec
        transmitted (in 124.650 secs):
                260901 packets  120467981 bytes
                2093 pkts/sec   966449 bytes/sec
inside:
        received (in 124.650 secs):
                261478 packets  120145678 bytes
                2097 pkts/sec   963864 bytes/sec
        transmitted (in 124.650 secs):
                294649 packets  167380042 bytes
                2363 pkts/sec   1342800 bytes/sec
```

Description du résultat

Ce tableau décrit les champs dans le résultat de **show perfmon**.

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 à N2H2 par seconde (requiert la commande **filte**
Correction de TCP	Nombre de paquets TCP qui l'ASA en avant par seconde
TCPIntercept	Nombre de paquets SYN par seconde qui ont dépassé la limite embryonnaire fixée su routage statique
Correction de HTTP	Nombre de paquets destinés au port 80 par seconde (requiert la commande **fixup prot http**)

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 commande d'utilisation de show cpu, vous pouvez utiliser les blocs d'exposition commandez afin de déterminer si l'ASA est surchargée.

Blocs de traitement de paquet (1 550 et 16 384 octets)

Quand il entre dans l'interface ASA, un paquet est placé sur la file d'attente d'interface d'entrée, passé jusqu'au SYSTÈME D'EXPLOITATION, et placé dans un bloc. Pour des paquets Ethernet, les blocs de 1 550 octets sont utilisés ; si le paquet arrive sur une carte Gigabit Ethernet de 66 MHz, les blocs 16 384 octets sont utilisés. L'ASA détermine si le paquet est permis ou refusé basé sur Adaptive Security Algorithm (ASA) et traite le paquet à la file d'attente de sortie sur l'interface sortante. Si l'ASA ne peut pas prendre en charge la charge de la circulation, le nombre de 1550-byte disponible bloque (ou blocs 16384-byte pour 66 MHZ GE) des vols planés de près de 0 (suivant les indications de la colonne CNT de la sortie de commande). Quand la colonne CNT frappe zéro, les tentatives ASA d'allouer plus de blocs, jusqu'à un maximum de 8192. Si plus de blocs ne sont disponibles, l'ASA relâche le paquet.

Basculement et blocs Syslog (256 octets)

Les blocs de 256 octets sont principalement utilisés pour des messages de basculement dynamique. L'ASA active génère et envoie des paquets au standby ASA afin de mettre à jour la traduction et la table de connexion. Pendant les périodes de salve de trafic où des haut débits de connexions sont créés ou interrompus, le nombre de blocs de 256 octets disponibles peut chuter à 0. Cette baisse indique qu'un ou plusieurs connexions ne sont pas mises à jour au standby ASA. 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 256-byte bloque des séjours à ou près de 0 pendant des longues périodes, l'ASA ne peut pas suivre les tables de traduction et de connexion qui sont synchronisées en raison du nombre de connexions par seconde ce les processus ASA. Si ceci se produit uniformément, améliorez l'ASA à un modèle plus rapide.

Les messages de Syslog envoyés de l'ASA utilisent également les blocs 256-byte, mais ils ne sont pas généralement libérés dans une telle quantité qui entraîne un épuisement du groupe du bloc 256-byte. 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 logging trap dans la configuration ASA. Il est recommandé de définir la journalisation au maximum sur Notification (niveau 5), à moins que vous ayez besoin d'informations supplémentaires pour le débogage.

Exemple

```
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   1538
```

Description du résultat

Ce tableau décrit les colonnes dans le résultat de **show blocs**.

Colonne	Description
TAILLE	E classent, dans les octets, du groupe de bloc. Chaque taille représente un type particulier
Max	Nombre maximal de blocs disponibles pour le groupe spécifié de bloc d'octet. Le nombre maxim blocs sont découpés hors de la mémoire au démarrage. Généralement, le nombre maximal de b ne change pas. L'exception est pour le 256- et les blocs 1550-byte, où l'appliance de sécurité adaptable peut dynamiquement créer plus une fois nécessaire, jusqu'à un maximum de 8192.
BAS	Seuil inférieur. Ce nombre indique le nombre le plus peu élevé de blocs de cette taille disponible puisque l'appliance de sécurité adaptable a été mise sous tension, ou puisque le dernier dédouanement des blocs (avec la commande claire de blocs). Un zéro dedans la BASSE colonn indique un événement précédent où la mémoire était pleine.
CNT	Nombre en cours de blocs disponibles pour ce groupe spécifique de bloc de taille. Un zéro deda que la colonne CNT signifie que la mémoire est pleine maintenant.

Ce tableau décrit les valeurs de la ligne SIZE dans le résultat de la commande **show blocks**.

Valeur de SIZE	Description
0	Utilisé par des blocs de dupb.

4	Blocs existants de doublons dans les applications telles que des DN, l'ISAKMP, le Filtrage URL, l'uauth, des modules TFTP, et de TCP. En outre, ce bloc classé peut être utilisé normalement par pour envoyer des paquets aux gestionnaires, etc.
80	Utilisé dans l'Interception TCP pour générer des paquets d'accusé de réception et pour des messa Hello de Basculement.
256	Utilisé pour fonctions de mises à jour de basculement dynamique, syslogging, et autre de TCP. Ce blocs sont principalement utilisés pour des messages de basculement dynamique. L'appliance de sécurité adaptable active génère et envoie des paquets à l'appliance de sécurité adaptable de rés pour mettre à jour la traduction et la table de connexion. Dans le trafic bursty, où des hauts débits connexions sont créés ou démolis, le nombre de blocs disponibles pourrait chuter à 0. Cette situat indique qu'un ou plusieurs connexions n'ont pas été mises à jour à l'appliance de sécurité adaptab réserve. Le protocole de basculement dynamique attrape la traduction ou la connexion manquante prochaine fois. Si la colonne CNT pour 256-byte bloque des séjours à ou près de 0 pendant des longues périodes, alors l'appliance de sécurité adaptable a le problème gardant les tables de tradu et de connexion synchronisées en raison du nombre de connexions par seconde que l'appliance d sécurité adaptable traite. Les messages de Syslog envoyés de l'appliance de sécurité adaptable utilisent également les blocs 256-byte, mais ils ne sont pas généralement libérés dans une telle quantité pour entraîner un épuisement du groupe du bloc 256-byte. Si la colonne CNT prouve que nombre de blocs 256-byte est près de 0, assurez-vous que vous ne vous connectez pas à l'élimina des imperfections (niveau 7) au serveur de Syslog. Ceci est indiqué par la ligne de logging trap da configuration d'appliance de sécurité adaptable. Nous recommandons que vous placiez se connec la notification (le niveau 5) ou diminuent, à moins que vous ayez besoin des informations complémentaires pour l'élimination des imperfections.
1550	Utilisé pour enregistrer des paquets Ethernet pour traiter par l'appliance de sécurité adaptable. Qu un paquet écrit une interface d'appliance de sécurité adaptable, il est placé sur la file d'attente d'interface d'entrée, passé jusqu'au système d'exploitation, et placé dans un bloc. L'appliance de sécurité adaptable détermine si le paquet devrait être permis ou refusé basé sur la stratégie de sécurité et traite le paquet à la file d'attente de sortie sur l'interface sortante. Si l'appliance de sécu adaptable a le problème suivant la charge de la circulation, le nombre de blocs disponibles planera près de 0 (suivant les indications de la colonne CNT de la sortie de commande). Quand la colonne CNT est zéro, les tentatives d'appliance de sécurité adaptable d'allouer plus de blocs, jusqu'à un maximum de 8192. Si plus de blocs ne sont disponibles, l'appliance de sécurité adaptable relâche paquet.
16384	Seulement utilisé pour le 64-bit, cartes Gigabit Ethernet 66-MHz (i82543). Voyez la description pou 1550 pour plus d'informations sur des paquets Ethernet.
2048	Contrôlez ou avez guidé les trames utilisées pour des mises à jour de contrôle.

show memory

La commande de **show memory** affiche toute la mémoire physique (ou la RAM) pour l'ASA, avec le nombre d'octets actuellement disponibles. Afin d'utiliser ces informations, vous devez d'abord comprendre comment l'ASA utilise la mémoire. Quand l'ASA démarre, elle copie le SYSTÈME D'EXPLOITATION de l'éclair dans la RAM et exécute le SYSTÈME D'EXPLOITATION de la RAM (juste comme des Routeurs). Ensuite, l'ASA copie la configuration de démarrage de l'éclair et la place dans la RAM. En conclusion, l'ASA alloue la RAM afin de créer les groupes de bloc discutés dans la section de blocs d'exposition. Une fois que cette allocation est complète, l'ASA a besoin de RAM supplémentaire seulement si la configuration augmente dans la taille. En outre, l'ASA enregistre les entrées de traduction et de connexion dans la RAM.

Pendant le fonctionnement normal, la mémoire disponible sur l'ASA devrait changer très peu, le cas échéant. Typiquement, le seul cas où vous devriez s'exécuter le bas sur la mémoire est si vous êtes soumise aux attaques et les centaines de milliers de connexions passent par l'ASA. Afin de vérifier les connexions, émettez la commande de **compte de show conn**, qui affiche le courant et le nombre maximal de connexions par l'ASA. Si l'ASA manque de mémoire, elle tombe en panne par la suite. Avant le crash, vous pourriez noter des messages de défaillance d'allocation de mémoire dans le Syslog (%ASA-3-211001). Si vous manquez de mémoire parce que vous êtes soumis à des attaques, entrez en contact avec le Centre d'assistance technique Cisco (TAC).

Exemple

```
Ciscoasa#
show memory
Free memory:       845044716 bytes (79%)

Used memory:       228697108 bytes (21%)

-------------     ----------------

Total memory:     1073741824 bytes (100%)
```

show xlate

La commande de **compte de show xlate** affiche le courant et le nombre maximal de traductions par 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 commande de **show xlate**, qui sort chaque traduction par l'ASA. La sortie de commande affiche des traductions « en service, » ce qui se rapporte au nombre de traductions actives dans l'ASA quand la commande est émise ; « le plus utilisé » se rapporte aux traductions maximum qui ont été jamais vues sur l'ASA depuis qu'elle a été mise sous tension.

> Remarque: Un hôte unique peut avoir plusieurs connexions vers différentes destinations, mais seulement une 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 charrie l'adresse source et envoie à des paquets l'ASA.

> Remarque: Quand la configuration vpnclient est activée et l'hôte interne envoie des

demandes DNS, la commande **show xlate** peut répertorier plusieurs xlate pour une traduction statique.

Exemple

```
Ciscoasa#
show xlate count
84 in use, 218 most used
```

```
Ciscoasa(config)#show xlate

3 in use, 3 most used

Flags: D - DNS, d - dump, I - identity, i - inside, n - no random,

       o - outside, r - portmap, s - static

TCP PAT from inside:10.1.1.15/1026 to outside:192.150.49.1/1024 flags ri
idle 62:33:57 timeout 0:00:30
UDP PAT from 10.1.1.15/1028 to outside:192.150.49.1/1024 flags ri
idle 62:33:57 timeout 0:00:30
ICMP PAT from inside:10.1.1.15/21505 to outside:192.150.49.1/0 flags ri
idle 62:33:57 timeout 0:00:30
```

La première entrée est une traduction d'adresses de port TCP pour le port de hôte (10.1.1.15, 1026) sur le réseau intérieur au port de hôte (192.150.49.1, 1024) sur le réseau extérieur. 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 (192.150.49.1, 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 (192.150.49.1, 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 de compte de show conn affiche le courant et le nombre maximal de connexions par l'ASA. Une connexion est un mappage des informations de la couche 4 d'une adresse interne à une adresse externe. Des connexions sont accumulées quand l'ASA reçoit un paquet de synchronisation pour des sessions TCP ou quand le premier paquet en session d'UDP arrive. Des connexions sont déchirées en bas de quand l'ASA reçoit le paquet de la finale ACK, qui se produit quand la prise de contact de session TCP se ferme ou quand le délai d'attente expire en session d'UDP.

Les comptes extrêmement élevés de connexion (normale de périodes 50-100) pourraient indiquer que vous êtes soumise aux attaques. Émettez la commande de **show memory** afin de s'assurer que le compte élevé de connexion ne fait pas manquer l'ASA de mémoire. 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 pour en savoir plus de références de commandes de Dispositifs de sécurité adaptatifs dédiés de la gamme Cisco ASA 5500.

Exemple

```
Ciscoasa#show conn count
2289 in use, 44729 most used
```

show interface

La commande d'interface d'exposition peut aider à déterminer des problèmes de non-correspondance de mode duplex et à câbler des questions. Elle peut également fournir un meilleur aperçu si l'interface est dépassée. Si l'ASA manque de capacité CPU, le nombre de blocs 1550-byte plane de près de 0. (regardez les blocs 16384-byte sur les cartes de yole de 66 MHZ.) Un autre indicateur est l'augmentation de « l'absence de mémoires tampon » sur l'interface. L'aucun message de mémoires tampons n'indique que l'interface ne peut pas envoyer le paquet au SYSTÈME D'EXPLOITATION ASA parce qu'il n'y a aucun bloc disponible pour le paquet, et le paquet est lâché. Si une augmentation d'aucun niveaux de mémoire tampon se produit régulièrement, émettez la commande **CPU de show proc** afin de vérifier l'utilisation du CPU sur l'ASA. Si l'utilisation du CPU est élevée en raison d'une charge de trafic intense, améliorez à une ASA plus puissante qui peut manipuler le chargement.

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 1550-byte (ou dans un bloc 16384-byte sur des interfaces de Gigabit Ethernet de 66 MHZ). L'ASA alors détermine l'interface de sortie pour le paquet et place le paquet dans la file d'attente appropriée de matériel. 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 tout sort des 100 Mbits/s simples relie, la file d'attente de logiciel de sortie indique des nombres élevés sur l'interface sortante, qui indique que l'interface ne peut pas manipuler le volume de trafic. Si vous vous trouvez face à cette situation, mettez à niveau vers une interface plus rapide.

Exemple

```
Ciscoasa#show interface
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
       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, 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)
```

Vous devez également vérifier l'interface pour 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 pourrait être défectueux aussi bien. 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 que les incréments régulièrement, la représentation sur votre ASA souffre très probablement, et vous devez trouver l'origine du problème.

Pendant que vous examinez les compteurs d'interface, notez que si l'interface est définie en duplex intégral, vous ne devriez constater de collisions, de collisions tardives ou de paquets reportés. Réciproquement, si l'interface est définie en semi-duplex, vous devriez recevoir des collisions, quelques collisions tardives et probablement quelques paquets reportés. Le nombre total de collisions, de collisions tardives et de paquets reportés ne devrait pas être supérieur à 10 % de la somme de compteurs de paquet en entrée et en 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). Souvenez-vous que les collisions du moyen de 10% que l'ASA relâche 10% des paquets qui passent par cette interface ; chacun de ces paquets doit être retransmis.

Référez-vous à la **commande d'interface** dans des références de commandes de Dispositifs de sécurité adaptatifs dédiés de la gamme Cisco ASA 5500 pour des informations détaillées sur les compteurs d'interface.

show processes

Le show processes commande sur l'ASA affiche tous les processus actifs qui fonctionnent sur l'ASA alors que 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, lancez la commande **show processes** 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 t'affiche combien de temps- CPU (en quelques millisecondes) le processus reçu dans cet intervalle de temps. 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: Un examen de chaque processus ASA est hors de portée de ce document, mais est mentionné brièvement pour l'exhaustivité. Référez-vous au show processes ASA commandent pour plus d'informations sur les processus ASA.

Résumé des commandes

En résumé, employez la commande d'**utilisation de show cpu** afin d'identifier le chargement que l'ASA est dessous. Souvenez-vous que le résultat est une moyenne d'exécution ; l'ASA peut avoir des pics plus élevés de l'utilisation du CPU qui sont masqués par la moyenne d'exécution. Une fois que l'ASA atteint l'utilisation du CPU de 80%, la latence par l'ASA grimpe lentement jusqu'à la CPU environ de 90%. Quand l'utilisation du CPU est plus de 90%, les débuts ASA pour relâcher des paquets.

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

Si la CPU n'exécute pas chaud, mais vous croyez que des paquets sont encore lâchés, employez la **commande d'interface d'exposition** afin de vérifier l'interface ASA pour aucune mémoires tampons et collisions, probablement provoquée par un conflit du mode bidirectionnel. 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. Si la colonne du courant CNT dans la sortie de **blocs d'exposition** est proche de 0 sur les blocs 1550-byte (blocs 16384-byte pour des cartes de yole de 66 MHZ), l'ASA relâche très probablement des paquets Ethernet parce qu'elle est trop occupée. Dans ce cas, le processeur atteint un pic.

Si vous éprouvez le problème quand vous établissez de nouveaux rapports par l'ASA, employez la commande de **compte de show conn** afin de vérifier le compte en cours de connexions par l'ASA.

Si le compte en cours est élevé, vérifiez le **show memory** sorti afin de s'assurer que l'ASA ne manque pas de mémoire. Si la capacité de mémoire est faible, étudiez la source des connexions avec la commande **show conn** ou **show local-host** pour vérifier que votre réseau n'a pas fait l'objet d'une attaque de déni de service.

Vous pouvez employer d'autres commandes afin de mesurer le niveau de trafic qui traverse l'ASA. La commande de **show traffic** affiche les paquets et les octets d'agrégat par interface, et le **perfmon d'exposition** divise le trafic vers le bas en différents types que l'ASA examine.

Informations connexes

- Dispositifs de sécurité adaptatifs de la gamme Cisco ASA 5500
- Support technique - Cisco Systems