

Tests et dépannage

Ce chapitre décrit comment dépanner l'ASA et tester la connectivité de base.

- Récupérer les mots de passe d'activation et Telnet, à la page 1
- Configurer et exécuter des captures à l'aide de l'Assistant de capture de paquets, à la page 5
- Utilisation et rapport d'utilisation du processeur (CPU), à la page 12
- Tester votre configuration, à la page 17
- Supervision des performances et des ressources du système, à la page 26
- Supervision des connexions, à la page 28
- Historique des tests et du dépannage , à la page 29

Récupérer les mots de passe d'activation et Telnet

Si vous oubliez les mots de passe d'activation ou Telnet, vous pouvez les récupérer pour les modèles ASA virtuel et ISA 3000. Vous devez effectuer la tâche à l'aide de l'interface de ligne de commande.

Remarque Pour les autres plateformes, vous ne pouvez pas récupérer les mots de passe perdus. Vous pouvez uniquement restaurer la configuration d'usine par défaut et réinitialiser les mots de passe par défaut. Pour Firepower 4100/9300, consultez le Guide de configuration de FXOS. Pour les autres modèles, consultez le Guide de dépannage de FXOS.

Récupérer les mots de passe sur l'ISA 3000

Pour récupérer les mots de passe des ISA 3000, procédez comme suit :

Procédure

Étape 1 Connectez-vous au port de console de l'ASA.

Étape 2 Mettez l'ASA hors tension, puis rallumez-le.

Étape 3 Après le démarrage, appuyez sur la touche **Échap** lorsque vous êtes invité à passer en mode ROMMON.

Étape 4 Pour mettre à jour la valeur du registre de configuration, entrez la commande suivante :

```
rommon #1> confreg 0x41

You must reset or power cycle for new config to take effect
```

L'ASA affiche la valeur actuelle du registre de configuration et une liste d'options de configuration. Enregistrez la valeur actuelle du registre de configuration afin de pouvoir la restaurer ultérieurement.

```
Configuration Register: 0x00000041

Configuration Summary
 [ 0 ] password recovery
 [ 1 ] display break prompt
 [ 2 ] ignore system configuration
 [ 3 ] auto-boot image in disks
 [ 4 ] console baud: 9600
 boot: ...... auto-boot index 1 image in disks
```

Étape 5 Rechargez l'ASA en saisissant la commande suivante :

```
rommon #2> boot
Launching BootLoader...
Boot configuration file contains 1 entry.

Loading disk0:/asa932-226-k8.bin... Booting...Loading...
```

L'ASA charge la configuration par défaut au lieu de la configuration de démarrage.

Étape 6 Accédez au mode d'exécution privilégié en saisissant la commande suivante :

```
ciscoasa# enable
```

Étape 7 Lorsque le mot de passe vous est demandé, appuyez sur **Entrée**.

Le mot de passe est une valeur vide.

Étape 8 Chargez la configuration de démarrage en saisissant la commande suivante :

```
ciscoasa# copy startup-config running-config
```

Étape 9 Accédez au mode de configuration globale en saisissant la commande suivante :

```
ciscoasa# configure terminal
```

Étape 10 Modifiez les mots de passe, au besoin, dans la configuration par défaut en saisissant les commandes suivantes :

```
ciscoasa(config)# password password
ciscoasa(config)# enable password password
ciscoasa(config)# username name password password
```

Étape 11 Chargez la configuration par défaut en saisissant la commande suivante :

```
ciscoasa(config)# no config-register
```

La valeur par défaut du registre de configuration est 0x1. Voir la référence des commandes pour en savoir plus sur le registre de configuration.

Étape 12 Enregistrez les nouveaux mots de passe dans la configuration de démarrage en saisissant la commande suivante :

```
ciscoasa(config)# copy running-config startup-config
```

Récupérer les mots de passe ou les images sur l'ASA virtuel

Pour récupérer les mots de passe ou les images sur l'ASA virtuel, procédez comme suit :

Procédure

Étape 1 Copiez la configuration en cours d'exécution dans un fichier de sauvegarde sur l'ASA virtuel :

copy running-config *nom de fichier*

Exemple :

```
ciscoasa# copy running-config backup.cfg
```

Étape 2 Redémarrez l'ASA virtuel :

reload

Étape 3 Dans le menu GNU GRUB, appuyez sur la flèche vers le bas, choisissez <**filename**> **sans option de chargement de configuration**, puis appuyez sur **Enter** (Entrée). Le nom de fichier est le nom de fichier d'image de démarrage par défaut sur l'ASA virtuel. L'image de démarrage par défaut n'est jamais démarrée automatiquement par la commande **fallback**. Chargez ensuite l'image de démarrage sélectionnée.

```
GNU GRUB version 2.0(12)4
bootflash:/asa100123-20-smp-k8.bin
bootflash: /asa100123-20-smp-k8.bin with no configuration load
```

Exemple :

```
GNU GRUB version 2.0(12)4
bootflash: /asa100123-20-smp-k8.bin with no configuration load
```

Étape 4 Copiez le fichier de configuration de sauvegarde vers la configuration en cours d'exécution.

copy *nom_de_fichier* **running-config**

Exemple :

```
ciscoasa (config)# copy backup.cfg running-config
```

Étape 5 Réinitialisez le mot de passe.

enable password *password*

Exemple :

```
ciscoasa(config)# enable password cisco123
```

Étape 6 Enregistrez la nouvelle configuration.

write memory

Exemple :

```
ciscoasa(config)# write memory
```

Désactiver la récupération du mot de passe pour le matériel ISA 3000

Remarque Vous ne pouvez pas désactiver la récupération du mot de passe sur les modèles ASA virtuel, Secure Firewall.

Pour désactiver la récupération du mot de passe et vous assurer que les utilisateurs non autorisés ne peuvent pas utiliser le mécanisme de récupération du mot de passe pour compromettre l'ASA, procédez comme suit.

Avant de commencer

Sur l'ASA, la commande **no service password-recovery** vous empêche de passer en mode ROMMON avec la configuration intacte. Lorsque vous passez en mode ROMMON, l'ASA vous invite à effacer tous les systèmes de fichiers flash. Vous ne pouvez pas passer en mode ROMMON sans effectuer au préalable cet effacement. Si vous choisissez de ne pas effacer le système de fichiers flash, l'ASA se recharge. Étant donné que la récupération du mot de passe dépend de l'utilisation du mode ROMMON et du maintien de la configuration existante, cet effacement vous empêche de récupérer un mot de passe. Cependant, la désactivation de la récupération du mot de passe empêche les utilisateurs non autorisés d'afficher la configuration ou d'insérer des mots de passe différents. Dans ce cas, pour restaurer le système à un état de fonctionnement, chargez une nouvelle image et un fichier de configuration de sauvegarde, le cas échéant.

La commande **service password-recovery** apparaît dans le fichier de configuration pour information uniquement. Lorsque vous saisissez la commande à l'invite de l'interface de ligne de commande, le paramètre est enregistré dans la NVRAM. La seule façon de modifier le paramètre est d'entrer la commande à l'invite de l'interface de ligne de commande. Le chargement d'une nouvelle configuration avec une version différente de la commande ne modifie pas le paramètre. Si vous désactivez la récupération du mot de passe lorsque l'ASA est configuré pour ignorer la configuration de démarrage au démarrage (en préparation de la récupération du mot de passe), l'ASA modifie le paramètre pour charger la configuration de démarrage comme d'habitude. Si vous utilisez le basculement et que l'unité de secours est configurée pour ignorer la configuration de

démarrage, la même modification est apportée au registre de configuration lorsque la commande **no service password- recovery** est dupliquée sur l'unité de secours.

Procédure

Désactivez la récupération du mot de passe.

no service password-recovery

Exemple :

```
ciscoasa (config)# no service password-recovery
```

Configurer et exécuter des captures à l'aide de l'Assistant de capture de paquets

Vous pouvez utiliser l'assistant de capture de paquets pour configurer et exécuter des captures pour le dépannage des erreurs. Les captures peuvent utiliser des ACL pour limiter le type de trafic capturé, les adresses et les ports source et de destination, et une ou plusieurs interfaces. L'assistant exécute une capture sur chacune des interfaces d'entrée et de sortie. Vous pouvez enregistrer les captures sur votre PC pour les examiner dans un analyseur de paquets.



Remarque Cet outil ne prend pas en charge la capture de SSL VPN sans client.

Pour configurer et exécuter des captures, procédez comme suit.

Procédure

Étape 1 Choisissez **Wizards (Assistants)** > **Packet Capture Wizard (Assistant de capture de paquets)**.

L'écran **Overview of Packet Capture** (Aperçu de la capture de paquets) apparaît, avec une liste des tâches que l'assistant vous guidera pour accomplir. Ces tâches comprennent les éléments suivants :

- Sélection d'une interface d'entrée.
- Sélection d'une interface de sortie.
- Définition des paramètres du tampon.
- Exécution des captures.
- Enregistrement des captures sur votre PC (facultatif).

Étape 2 Cliquez sur **Next** (suivant).

Dans un environnement de grappe, l'écran **Cluster Option** (Option de grappe) s'affiche. Passez à l'étape 3.

Dans un environnement sans grappe, l'écran **Ingress Traffic Selector** (Sélecteur de trafic d'entrée) s'affiche. Passez à l'étape 4.

Étape 3 Choisissez l'une des options suivantes dans l'écran **Cluster Option** (Pption de grappe) pour exécuter une capture : **This device only** (Ce périphérique uniquement) ou **The whole cluster** (L'ensemble de la grappe), puis cliquez sur **Next** (Suivant) pour afficher l'écran **Ingress Selector** (Sélecteur d'entrée).

Étape 4 Cliquez sur le bouton radio **Select Interface** (Sélectionner l'interface) pour capturer des paquets sur une interface.

Dans un environnement de mise en grappe, pour capturer uniquement les paquets du plan de commande de grappe, cochez la case **CP-Cluster** (Grappe CP).

Étape 5 Cliquez sur le bouton radio **Use backplane channel** (Utiliser le canal de fond de panier) pour capturer des paquets dans le plan de données ASA CX.

Étape 6 Effectuez l'une des opérations suivantes dans la zone **Packet Match Criteria** (Critères de correspondance des paquets) :

- Cliquez sur le bouton radio **Select access list (Sélectionner la liste d'accès)** pour spécifier l'ACL à utiliser pour les paquets correspondants, puis choisissez l'ACL dans la liste déroulante **Select ACL** (Sélectionner une ACL). Cliquez sur **Manage** (Gérer) pour afficher le volet **ACL Manager** (Gestionnaire ACL) afin d'ajouter une ACL précédemment configurée à la liste déroulante actuelle. Choisissez une ACL, puis cliquez sur **OK**.

  L'option de liste d'accès est désactivée lorsque vous activez la capture de paquet de commutateurs. Pour de plus amples renseignements, consultez la section Sélecteur de trafic d'entrée, à la page 9.

- Cliquez sur le bouton radio **Specify Packet Parameters** pour spécifier les paramètres des paquets.

a) Effectuez l'une des opérations suivantes dans la liste déroulante **ICMP Capture** (Capture ICMP) :



Remarque Le champ **ICMP Capture** (Capture ICMP) est rempli uniquement lorsque vous sélectionnez **The whole cluster** (L'ensemble de la grappe) comme option de grappe dans la fenêtre précédente.

- Sélectionnez **include-decrypted** pour capturer les paquets IPsec déchiffrés qui contiennent du trafic normal et déchiffré une fois qu'ils pénètrent dans le périphérique de pare-feu.
- Sélectionnez **persist** pour capturer les paquets persistants sur les unités de grappe.

Étape 7 Pour continuer, consultez Sélecteur de trafic d'entrée, à la page 9.

Étape 8 Cliquez sur **Next** (Suivant) pour afficher l'écran **Egress Traffic Selector** (Sélecteur de trafic de sortie).

Étape 9 Cliquez sur le bouton radio **Select Interface** (Sélectionner l'interface) pour capturer des paquets sur une interface.

Dans un environnement de mise en grappe, pour capturer les paquets du plan de commande de grappe, cochez la case **CP-Cluster** (Grappe CP).

Remarque Pour en savoir plus sur les champs Egress Traffic Selector (Sélecteur de trafic de sortie), consultez Sélecteur de trafic de sortie, à la page 10.

Pour en savoir plus sur les champs Egress Traffic Selector (Sélecteur de trafic de sortie), consultez Sélecteur de trafic de sortie, à la page 10.

Étape 10 Cliquez sur **Next** (Suivant) pour afficher l'écran **Buffers & Captures** (Tampons et captures). Pour continuer, consultez Buffers (Tampons).

Étape 11 Cochez la case **Get capture every 10 seconds** (Obtenir une capture toutes les 10 secondes) dans la zone **Capture Parameters** (Paramètres de capture) pour obtenir automatiquement la dernière capture toutes les 10 secondes. Par défaut, cette capture utilise le tampon circulaire.

Étape 12 Vous spécifiez la taille du tampon et la taille des paquets dans la zone **Buffer Parameters** (Paramètres du tampon). La taille de tampon est la quantité maximale de mémoire que la capture peut utiliser pour stocker les paquets. La taille de paquet est le paquet le plus long que la capture peut contenir. Nous vous conseillons d'utiliser la taille de paquet la plus longue pour capturer le plus de renseignements possible.

a) (Facultatif. Applicable uniquement aux périphériques Secure Firewall 3100) Cochez la case **Switch** (Commutateur) pour stocker les paquets de commutation capturés.
b) Saisissez la taille de paquet. La taille valide varie de 14 à 1522 octets. Pour la capture de paquets de commutateurs, la taille valide varie de 64 à 9006 octets.
c) Saisissez la taille de tampon. La taille valide varie de 1534 et 33554432 octets. Pour la capture de paquets de commutateurs, la taille valide varie de 256 à 2048 octets.
d) Cochez la case **Use circular buffer** (Utiliser le tampon circulaire) pour stocker les paquets capturés.

Remarque Lorsque vous choisissez ce paramètre, si toute la mémoire tampon est utilisée, la capture commence à remplacer les paquets les plus anciens.

Étape 13 Cliquez sur **Next** (Suivant) pour afficher l'écran **Summary** (Résumé), qui affiche les options de grappe pour toutes les unités de la grappe (si vous utilisez la mise en grappe), les sélecteurs de trafic et les paramètres de tampon que vous avez saisis. Pour continuer, consultez Summary (Résumé).

Étape 14 Cliquez sur **Next** (Suivant) pour afficher l'écran **Run Captures** (Exécuter les captures), puis sur **Start** (Démarrer) pour commencer à capturer les paquets. Cliquez sur **Stop** (Arrêter) pour mettre fin à la capture. Pour continuer, consultez Exécuter des captures, à la page 11. Si vous utilisez la mise en grappe, passez à l'étape 16.

Étape 15 Cliquez sur **Get Capture Buffer** (Obtenir le tampon de capture) pour déterminer l'espace tampon restant. Cliquez sur **Clear Buffer on Device** (Effacer le tampon de l'appareil) pour supprimer le contenu actuel et faire de la place dans le tampon pour capturer plus de paquets.

Étape 16 Dans un environnement de mise en grappe, sur l'écran **Run Captures** (Exécuter les captures), effectuez une ou plusieurs des étapes suivantes :

- Cliquez sur **Get Cluster Capture Summary** (Obtenir le résumé de la capture de la grappe) pour afficher un résumé des renseignements sur la capture de paquets pour toutes les unités de la grappe, suivis des renseignements sur la capture de paquets pour chaque unité.

- Cliquez sur **Get Capture Buffer** (Obtenir le tampon de capture) pour déterminer l'espace tampon restant dans chaque unité de la grappe. La boîte de dialogue **Capture Buffer from Device** (Capturer le tampon de l'appareil) s'affiche.
- Cliquez sur **Clear Capture Buffer** (Effacer le tampon de capture) pour supprimer le contenu actuel d'une ou de toutes les unités d'une grappe et faire de la place dans le tampon pour capturer plus de paquets.

Étape 17 Cliquez sur **Save captures** (Enregistrer les captures) pour afficher la boîte de dialogue **Save Capture** (Enregistrer la capture). Vous avez la possibilité d'enregistrer la capture d'entrée, la capture de sortie ou les deux. Pour continuer, consultez Save Captures (Enregistrer les captures).

Étape 18 Cliquez sur **Save Ingress Capture** (Enregistrer la capture d'entrée) pour afficher la boîte de dialogue **Save capture file** (Enregistrer le fichier de capture). Spécifiez l'emplacement de stockage sur votre PC, puis cliquez sur **Save** (Enregistrer).

Étape 19 Cliquez sur **Launch Network Sniffer Application** (Lancer l'application de l'analyseur de réseau) pour démarrer l'application d'analyse de paquet spécifiée dans **Tools (Outils)** > **Preferences (Préférences)** pour l'analyse de la capture d'entrée.

Étape 20 Cliquez sur **Save Egress Capture** (Enregistrer la capture de sortie) pour afficher la boîte de dialogue **Save capture file** (Enregistrer le fichier de capture). Spécifiez l'emplacement de stockage sur votre PC, puis cliquez sur **Save** (Enregistrer).

Étape 21 Cliquez sur **Launch Network Sniffer Application** (Lancer l'application de l'analyseur de réseau) pour démarrer l'application d'analyse de paquet spécifiée dans **Tools (Outils)** > **Preferences (Préférences)** pour l'analyse de la capture de sortie.

Étape 22 Cliquez sur **Close** (Fermer), puis **Finish** (Terminer) pour quitter l'assistant.

Lignes directrices pour la capture des paquets

Mode contextuel

- Vous pouvez configurer les captures sur la liaison de commande de grappe dans un contexte; seul le paquet associé au contexte envoyé dans la liaison de commande de grappe est capturé.
- Vous ne pouvez configurer qu'une seule capture pour un VLAN partagé; si vous configurez une capture dans plusieurs contextes sur le VLAN partagé, seule la dernière capture configurée est utilisée.
- Si vous supprimez la dernière capture configurée (active), aucune capture ne devient active, même si vous avez déjà configuré une capture dans un autre contexte; vous devez supprimer la capture et l'ajouter à nouveau pour la rendre active.
- Tout le trafic qui entre dans l'interface à laquelle la capture est connectée est capturé, y compris le trafic vers d'autres contextes sur le VLAN partagé. Par conséquent, si vous activez une capture dans le contexte A pour un VLAN qui est également utilisé par le contexte B, le trafic entrant du contexte A et du contexte B est capturé.
- Pour le trafic de sortie, seul le trafic du contexte avec la capture active est capturé. La seule exception est lorsque vous n'activez pas l'inspection ICMP (par conséquent, le trafic ICMP n'a pas de session dans le chemin accéléré). Dans ce cas, le trafic ICMP d'entrée et de sortie pour tous les contextes sur le VLAN partagé est capturé.

Directives supplémentaires

- Si l'ASA reçoit des paquets avec un en-tête TCP mal formaté et les abandonne du fait de la raison d'abandon ASP *invalid-tcp-hdr-length*, la sortie de la commande **show capture** sur l'interface où ces paquets sont reçus n'affiche pas ces paquets.
- Vous pouvez uniquement capturer le trafic IP; vous ne pouvez pas capturer des paquets non IP tels que les ARP.
- Pour les paquets marqués SGT en ligne, les paquets capturés contiennent un en-tête CMD supplémentaire que votre visualiseur PCAP pourrait ne pas comprendre.
- Les captures de paquets comprennent les paquets que le système modifie ou injecte dans la connexion en raison de l'inspection, de la normalisation de la NAT, du TCP ou d'autres fonctionnalités qui ajustent le contenu d'un paquet.
- La trace de la durée de vie d'un paquet virtuel injecté dans un chemin de données ne reflète pas exactement la façon dont le chemin de données gère les paquets physiques. Cette différence dépend de la version du logiciel, de la configuration et du type de paquets virtuels injectés. Voici les paramètres de configuration qui pourraient entraîner cette disparité :
  - Il existe au moins 2 instructions NAT pour le même hôte.
  - Les flux avant et arrière d'une connexion ont des protocoles différents. Par exemple, le flux avant est UDP ou TCP, le flux arrière est ICMP.
  - L'inspection d'erreurs ICMP est activée.

Sélecteur de trafic d'entrée

Pour configurer l'interface d'entrée, les hôtes ou réseaux source et de destination, ainsi que le protocole de capture de paquets, procédez comme suit :

Procédure

Étape 1 Choisissez le nom de l'interface d'entrée dans la liste déroulante.

Étape 2 Saisissez l'hôte et le réseau de la source d'entrée. Cliquez sur le bouton radio **Use backplane channel** (Utiliser le canal de fond de panier) pour capturer des paquets dans le plan de données ASA CX.

Étape 3 Saisissez l'hôte et le réseau de destination d'entrée.

Étape 4 Saisissez le type de protocole à capturer. Les protocoles disponibles sont ah, eigrp, esp, gre, icmp, icmp6, igmp, igrp, ip, ipinip, nos, ospf, pcp, pim, snp, tcp ou udp.

a) Saisissez le type ICMP pour ICMP uniquement. Les types disponibles sont les suivants : all, alternate address, conversion-error, echo, echo-reply, information-reply, information-request, mask-reply, mask-request, mobile-redirect, parameter-problem, redirect, router-advertisement, router-solicitation, source-quench, time-exceeded, timestamp-reply, timestamp-request, traceroute ou unreachable.

b) Spécifiez les services de port source et destination pour les protocoles TCP et UDP uniquement. Les options disponibles sont les suivantes :
   - Choisissez **All Services** (Tous les services) pour inclure tous les services.
   - Choisissez **Service Groups** (Groupes de services) pour inclure un groupe de service.

Pour inclure un service spécifique, choisissez l'une des options suivantes : aol, bgp, chargen, cifx, citrix-ica, ctiqbe, daytime, discard, domain, echo, exec, finger, ftp, ftp-data, gopher, h323, hostname, http, https, ident, imap4, irc, kerberos, klogin, kshell, ldap, ldaps, login, lotusnotes, lpd, netbios-ssn, nntp, pcanywhere-data, pim-auto-rp, pop2, pop3, pptp, rsh, rtsp, sip, smtp, sqlnet, ssh, sunrpc, tacacs, talk, telnet, uucp, or whois.

Étape 5 Pour activer la capture de paquets pour le service Cisco TrustSec, dans la zone **Security Group Tagging** (Balisation du groupe de sécurité), cochez la case **SGT number** (Numéro SGT) et saisissez le numéro de balise du groupe de sécurité. Les numéros de balise de groupe de sécurité valides sont compris entre 2 et 65519.

Étape 6 (Facultatif. Applicable uniquement aux périphériques Secure Firewall 3100) Pour activer la capture de paquets du commutateur, dans la zone **Switch Control** (Contrôle du commutateur), cochez la case **Switch** (Commutateur) et spécifiez les plages de VLAN interne et de VLAN externe (de 1 à 4096).

Remarque Lorsque vous activez la capture de paquets de commutateurs, l'option de liste d'accès est désactivée.

Sélecteur de trafic de sortie

Pour configurer l'interface de sortie, les hôtes/réseaux source et de destination, ainsi que les services de port source et de destination pour la capture de paquets, procédez comme suit :

Procédure

Étape 1 Cliquez sur le bouton radio **Select Interface** (Sélectionner l'interface) pour capturer des paquets sur une interface. Cliquez sur le bouton radio **Use backplane channel** (Utiliser le canal de fond de panier) pour capturer des paquets dans le plan de données ASA CX.

Étape 2 Choisissez le nom de l'interface de sortie dans la liste déroulante.

Étape 3 Saisissez l'hôte et le réseau source de sortie.

Étape 4 Saisissez l'hôte et le réseau de destination de sortie.

Le type de protocole sélectionné lors de la configuration d'entrée est déjà répertorié.

Étape 5 (Facultatif. Applicable uniquement aux périphériques Secure Firewall 3100) Si vous avez activé la capture de paquets du commutateur, précisez les plages de VLAN interne et de VLAN externe (de 1 à 4096). Pour activer la capture de paquets du commutateur, consultez Sélecteur de trafic d'entrée, à la page 9.

Tampons

Pour configurer la taille des paquets, la taille du tampon et l'utilisation du tampon circulaire pour la capture de paquets, procédez comme suit :

Procédure

Étape 1 Saisissez le paquet le plus long que la capture peut contenir. Utilisez la plus longue taille disponible pour capturer le plus de renseignements possible.

Étape 2 Saisissez la quantité maximale de mémoire que la capture peut utiliser pour stocker les paquets.

Étape 3 Utilisez le tampon circulaire pour stocker les paquets. Lorsque le tampon circulaire a utilisé toute la mémoire tampon, la capture écrase d'abord les paquets les plus anciens.

Résumé

L'écran **Summary** (Résumé) affiche les options de grappe (si vous utilisez la mise en grappe), les sélecteurs de trafic et les paramètres de tampon pour la capture de paquets sélectionnée dans les écrans précédents de l'assistant.

Exécuter des captures

Pour démarrer et arrêter la session de capture, afficher le tampon de capture, lancer une application d'analyse de réseau, enregistrer les captures de paquets et effacer le tampon, procédez comme suit :

Procédure

Étape 1 Cliquez sur **Start** (Démarrer) pour commencer la session de capture de paquets sur une interface sélectionnée.

Étape 2 Cliquez sur **Stop** (Arrêter) pour arrêter la session de capture de paquets sur une interface sélectionnée.

Étape 3 Cliquez sur **Get Capture Buffer** (Obtenir le tampon de capture) pour obtenir un instantané des paquets capturés sur l'interface.

Étape 4 Cliquez sur **Ingress** (Entrée) pour afficher le tampon de capture sur l'interface d'entrée.

Étape 5 Cliquez sur **Egress** (Sortie) pour afficher le tampon de capture sur l'interface de sortie.

Étape 6 Cliquez sur **Clear Buffer on Device** (Effacer le tampon sur le périphérique) pour effacer le tampon du périphérique.

Étape 7 Cliquez sur **Launch Network Sniffer Application** (Lancer l'application de l'analyseur de réseau) pour démarrer l'application d'analyse de paquet afin d'analyser la capture d'entrée ou la capture de sortie spécifiée dans **Tools (Outils)** > **Preferences (Préférences)**.

Étape 8 Cliquez sur **Save Captures** (Enregistrer les captures) pour enregistrer les captures d'entrée et de sortie au format ASCII ou PCAP.

Enregistrer des captures

Pour enregistrer les captures de paquets d'entrée et de sortie dans le format de fichier ASCII ou PCAP pour une analyse plus approfondie des paquets, procédez comme suit :

Procédure

Étape 1 Cliquez sur **ASCII** pour enregistrer le tampon de capture au format ASCII.

Étape 2 Cliquez sur **PCAP** pour enregistrer le tampon de capture au format PCAP.

Étape 3 Cliquez sur **Save ingress capture** (Enregistrer la capture d'entrée) pour spécifier un fichier dans lequel enregistrer la capture de paquets d'entrée.

Étape 4 Cliquez sur **Save egress capture** (Enregistrer la capture de sortie) pour spécifier un fichier dans lequel enregistrer la capture de paquets de sortie.

Utilisation et rapport d'utilisation du processeur (CPU)

Le rapport d'utilisation du processeur résume le pourcentage du processeur utilisé pendant la période précisée. En règle générale, le cœur fonctionne à environ 30 à 40 % de la capacité totale du processeur en dehors des heures de pointe et à environ 60 à 70 % de capacité pendant les heures de pointe.

Utilisation de vCPU dans l'ASA virtuel

Utilisez la commande **show cpu usage** sur l'ASA virtuel pour afficher les statistiques d'utilisation du processeur. L'utilisation de vCPU dans ASA virtuel affiche la quantité de vCPU utilisée pour le chemin de données, le point de contrôle et les processus externes.

L'utilisation de vCPU signalée par le fournisseur de services en nuage (comme VMware, Azure, OCI, etc.) comprend l'utilisation de l'ASA virtuel comme décrit plus :

- Temps d'inactivité d'ASA virtuel
- %SYS surdébit utilisé pour la VM ASA virtuel
- Surdébit du déplacement des paquets entre les vSwitches, les vNIC et les pNIC. Ce surdébit peut être assez important.

Exemple d'utilisation du processeur

Voici un exemple dans lequel l'utilisation de vCPU signalée est sensiblement différente :

- Rapports ASA virtuel : 40 %
- DP : 35 %
- Processus externes : 5 %
- Rapports vSphere : 95 %
- ASA (comme les rapports ASA virtuel) : 40 %
- Interrogation ASA inactive : 10 %
- Frais généraux : 45 %

Le surdébit est utilisé pour effectuer des fonctions d'hyperviseur et pour déplacer des paquets entre les NIC et les vNIC à l'aide du vSwitch.

L'utilisation peut dépasser 100 %, car le serveur ESXi peut utiliser des ressources de traitement supplémentaires pour le surdébit au nom de l'ASA virtuel.

Rapport d'utilisation du CPU VMware

Dans vSphere, cliquez sur l'onglet **VM Performance** (Performances de la VM), puis sur **Advanced** (Avancé) pour afficher la liste déroulante **Chart Options** (Options du graphique), qui indique l'utilisation de vCPU pour chaque état (%Utilisateur, %Inactif, %Sys, etc.) de la VM. Ces renseignements sont utiles pour comprendre le point de vue de VMware sur l'utilisation des ressources de CPU.

Sur l'interface shell du serveur ESXi (vous accédez à l'interface shell en utilisant SSH pour vous connecter à l'hôte), esxtop est disponible. Esxtop a une apparence similaire à la commande **top** de Linux et fournit des renseignements sur l'état de la VM pour les performances de vSphere, notamment les suivantes :

- Détails sur l'utilisation du vCPU, de la mémoire et du réseau
- Utilisation du vCPU pour chaque état de chaque VM.
- Mémoire (type M pendant l'exécution) et réseau (type N pendant l'exécution), ainsi que les statistiques et le nombre d'abandons RX

ASA virtuel et graphiques vCenter

Il existe des différences dans les numéros de % du CPU entre l'ASA virtuel et vCenter :

- Les numéros de graphique vCenter sont toujours supérieurs aux numéros d'ASA virtuel.
- vCenter l'appelle « %CPU usage » (% d'usage du CPU); l'ASA virtuel l'appelle « %CPU utilization » (% d'utilisation du CPU).

Les termes « %CPU utilization » et « %CPU usage » ont des significations différentes :

- CPU utilization fournit des statistiques sur les CPU physiques.
- CPU usage fournit des statistiques sur les CPU logiques, qui sont basées sur l'hyperthreading du processeur. Mais, comme un seul vCPU est utilisé, l'hyperthreading n'est pas activé.

vCenter calcule le pourcentage d'usage du CPU comme suit :

Nombre de processeur (CPU) virtuels utilisés activement, spécifié en pourcentage du nombre total de CPU disponibles

Ce calcul est la vue de l'hôte de l'utilisation du CPU, et non la vue du système d'exploitation invité, et est l'utilisation moyenne du CPU sur tous les CPU virtuels disponibles dans la machine virtuelle.

Par exemple, si une machine virtuelle avec un CPU virtuel fonctionne sur un hôte qui a quatre CPU physiques et que l'usage des CPU est de 100 %, la machine virtuelle utilise complètement un CPU physique. Le calcul de l'usage du CPU virtuel est l'usage en MHz/nombre de CPU virtuels x fréquence du cœur.

Lorsque vous comparez l'utilisation en MHz, les chiffres de vCenter et d'ASA virtuel correspondent. Selon le graphique vCenter, l'utilisation du CPU en % MHz est calculée comme suit : 60/(2499 x 1 vCPU) = 2,4

Rapports d'utilisation du CPU Amazon CloudWatch

Vous pouvez afficher l'explorateur de mesures pour surveiller les ressources en fonction de leurs balises et de leurs propriétés. Procédez comme suit pour afficher les statistiques d'utilisation du processeur pour une instance en particulier :

Procédure

Étape 1 Ouvrez la console **CloudWatch** et choisissez **Metrics** (Mesures) dans le volet de navigation.

Étape 2 Sélectionnez l'espace de noms de la mesure **EC2** et sélectionnez la dimension **Per-instance Metrics** (Mesures par instance).

Étape 3 Saisissez **CPU Utilization** (Utilisation du CPU) dans le champ de recherche et appuyez sur Entrée. Sélectionnez la ligne de l'instance requise pour afficher un graphique de la mesure **CPU Utilization** (Utilisation du CPU) pour cette instance.

Pour en savoir plus, consultez la documentation relative à Amazon CloudWatch.

ASA virtuel et graphiques Amazon CloudWatch

Les chiffres du graphique Amazon CloudWatch sont supérieurs aux chiffres réels en raison des différentes façons de calculer l'utilisation du CPU sur l'ASA virtuel et le CloudWatch.

Lorsque l'ASA virtuel fonctionne en mode d'interrogation, chaque CPU exécute une boucle de commandes allégées au lieu d'entrer en mode d'économie d'alimentation ou dans tout autre état inactif. Cela améliore les performances en maintenant chaque cœur actif en tout temps au lieu de devoir l'activer/le désactiver ou que leurs horloges soient ajustées en fonction des états d'alimentation Intel.

À l'intérieur de l'ASA virtuel, cette activité est comprise comme un comportement inactif et l'utilisation du CPU est correctement calculée. Cependant, sur Amazon CloudWatch, le comportement inactif ressemble à une activité normale du CPU, car tous les cycles du CPU ont des instructions à exécuter, ce qui conduit le CloudWatch à afficher un pourcentage d'utilisation du CPU élevé (85 à 90 %).

Rapport d'utilisation du CPU Azure

Effectuez les étapes suivantes pour afficher le % d'utilisation du CPU sur toutes les VM surveillées à l'aide des observations de VM du moniteur Azure :

Procédure

Étape 1 Accédez au portail Azure, sélectionnez **Monitor** (Superviser) et choisissez **Virtual Machines** (Machines virtuelles) dans la section **Solutions**.

Étape 2 Sélectionnez l'onglet **Performance** pour afficher le tableau **CPU Utilization %** (% d'utilisation du CPU). Ce tableau affiche les cinq machines ayant la plus forte utilisation moyenne du processeur.

Effectuez les étapes suivantes pour afficher le tableau du % d'utilisation du CPU directement à partir d'une machine virtuelle Azure spécifique :

Procédure

Étape 1 Accédez au portail Azure et sélectionnez **Virtual Machines** (Machines virtuelles).

Étape 2 Dans la liste des VM, choisissez une VM.

Étape 3 Dans la section **Monitoring** (Supervision), sélectionnez **Insights** (Observations).

Étape 4 Sélectionnez l'onglet **Performance**.

Consultez la section Comment représenter graphiquement les performances avec les observations de VM pour en savoir plus.

Graphiques ASA virtuel et Azure

Il existe des différences dans les numéros de % du CPU entre l'ASA virtuel et Azure. Les numéros du graphique Azure sont toujours supérieurs aux numéros de l'ASA virtuel, car Azure calcule l'utilisation en % du CPU comme la quantité de CPU virtuels utilisés activement, spécifié en pourcentage du total des CPU disponibles.

Ce calcul est la vue de l'hôte de l'utilisation du CPU, et non la vue du système d'exploitation invité, et est l'utilisation moyenne du CPU sur tous les CPU virtuels disponibles dans la machine virtuelle.

Par exemple, si une machine virtuelle avec un CPU virtuel fonctionne sur un hôte qui a quatre CPU physiques et que l'usage des CPU est de 100 %, la machine virtuelle utilise complètement un CPU physique. Le calcul de l'utilisation du CPU virtuel est l'utilisation en MHz/nombre de CPU virtuels x fréquence du cœur.

Azure limite également la quantité de CPU demandée par le système d'exploitation invité. Imaginez un scénario dans lequel l'ASA virtuel signale une utilisation du CPU à 40 % et l'hyperviseur signale une utilisation du CPU à 90 %. Maintenant, si l'ASA virtuel a besoin de plus de puissance de traitement, l'utilisation du CPU peut dépasser 80 % et l'hyperviseur peut alors signaler l'utilisation du CPU à plus de 95 %. Cela conduit l'hyperviseur à limiter le CPU de l'ASA virtuel même si l'ASA virtuel n'exécute qu'une boucle de commandes légères en mode d'interrogation et présente un comportement inactif.

Rapport d'utilisation du CPU Hyper-V

En plus d'afficher les renseignements de configuration du CPU, de la RAM et de l'espace disque pour les serveurs en nuage disponibles, vous pouvez également afficher les renseignements sur le disque, les E/S et le réseau. Utilisez ces renseignements pour vous aider à décider quel serveur en nuage correspond à vos besoins. Vous pouvez afficher les serveurs disponibles par le biais du client nova de ligne de commande ou de l'interface du **panneau de commande en nuage**.

Dans la ligne de commande, exécutez la commande suivante :

```
nova flavor-list
```

Toutes les configurations de serveur disponibles sont affichées. La liste contient les renseignements suivants :

- ID – ID de configuration du serveur
- Name – nom de la configuration, étiqueté par taille de RAM et type de performance

- Mémoire_Mo – la quantité de RAM pour la configuration
- Disque – la taille du disque en Go (pour les serveurs en nuage à usage général, la taille du disque système)
- Éphémère – la taille du disque de données
- Permutation – la taille de l'espace de permutation
- VCPU – le nombre de CPU virtuels associés à la configuration
- Facteur_RXTX – la quantité de bande passante, en Mbit/s, allouée aux ports PublicNet, aux ports ServiceNet et aux réseaux isolés (réseaux en nuage) reliés à un serveur.
- Est_Public – non utilisé

Graphiques ASA virtuel et Hyper-V

Il existe des différences dans les numéros de % du CPU entre l'ASA virtuel et Hyper-V :

- Les numéros de graphique Hyper-V sont toujours supérieurs aux numéros d'ASA virtuel.
- Hyper-V l'appelle « %CPU usage » (% d'usage du CPU); l'ASA virtuel l'appelle « %CPU utilization » (% d'utilisation du CPU).

Les termes « %CPU utilization » et « %CPU usage » ont des significations différentes :

- CPU utilization fournit des statistiques sur les CPU physiques.
- CPU usage fournit des statistiques sur les CPU logiques, qui sont basées sur l'hyperthreading du processeur. Mais, comme un seul vCPU est utilisé, l'hyperthreading n'est pas activé.

Hyper-V calcule le pourcentage d'usage du CPU comme suit :

Nombre de processeur (CPU) virtuels utilisés activement, spécifié en pourcentage du nombre total de CPU disponibles

Ce calcul est la vue de l'hôte de l'utilisation du CPU, et non la vue du système d'exploitation invité, et est l'utilisation moyenne du CPU sur tous les CPU virtuels disponibles dans la machine virtuelle.

Par exemple, si une machine virtuelle avec un CPU virtuel fonctionne sur un hôte qui a quatre CPU physiques et que l'usage des CPU est de 100 %, la machine virtuelle utilise complètement un CPU physique. Le calcul de l'usage du CPU virtuel est l'usage en MHz/nombre de CPU virtuels x fréquence du cœur.

Remarque Il est conseillé de consulter les rapports d'ASA virtuel pour obtenir un pourcentage d'usage précis du processeur.

Rapport d'utilisation du CPU OCI

Vous pouvez afficher le % d'utilisation du processeur dans le protocole OCI à l'aide de la mesure d'instance de calcul : **oci_computeagent**. La mesure d'utilisation du CPU affiche le niveau d'activité du CPU et est exprimée en pourcentage de temps total. Effectuez les étapes suivantes pour afficher les tableaux de mesures pour une seule instance de calcul :

Procédure

Étape 1 Ouvrez le menu de navigation et cliquez sur **Instances** sous **Compute** (Calcul).

Étape 2 Cliquez sur une instance, puis sur **Metrics** (Mesures) sous **Resources** (Ressources).

Étape 3 Sélectionnez **oci_computeagent** dans la liste Metric namespace (Espace de noms de mesures).

Consultez la section Mesures des instances de calcul pour en savoir plus.

ASA virtuel et graphiques OCI

Les numéros du graphique OCI sont toujours supérieurs aux numéros de l'ASA virtuel, car l'OCI calcule l'utilisation en % du CPU comme la quantité de CPU virtuels utilisés activement, spécifié en pourcentage du total des CPU disponibles.

Ce calcul est la vue de l'hôte de l'utilisation du CPU, et non la vue du système d'exploitation invité, et est l'utilisation moyenne du CPU sur tous les CPU virtuels disponibles dans la machine virtuelle.

Par exemple, si une machine virtuelle avec un CPU virtuel fonctionne sur un hôte qui a quatre CPU physiques et que l'usage des CPU est de 100 %, la machine virtuelle utilise complètement un CPU physique. Le calcul de l'utilisation du CPU virtuel est l'utilisation en MHz/nombre de CPU virtuels x fréquence du cœur.

Tester votre configuration

Cette section décrit comment tester la connectivité pour l'ASA en mode unique ou pour chaque contexte de sécurité, comment envoyer un message Ping aux interfaces ASA et comment autoriser les hôtes d'une interface à envoyer un message Ping aux hôtes sur une autre interface.

Tester la connectivité de base : envoi d'un ping à des adresses

Ping est une commande simple qui vous permet de déterminer si une adresse particulière est active et réactive. Les rubriques suivantes fournissent des renseignements supplémentaires sur la commande et les types de tests que vous pouvez effectuer avec celle-ci.

Ce que vous pouvez tester en utilisant le ping

Lorsque vous envoyez un message Ping à un périphérique, un paquet est envoyé à ce dernier, qui renvoie une réponse. Ce processus permet aux périphériques réseau de se détecter, de s'identifier et de se tester mutuellement.

Vous pouvez utiliser les messages Ping pour effectuer les tests suivants :

- Test de boucle avec retour de deux interfaces : vous pouvez initier l'envoi d'un message Ping d'une interface à une autre sur le même ASA, en tant que test de boucle avec retour externe pour vérifier l'état « opérationnel » de base et le fonctionnement de chaque interface.
- Envoyer un message Ping à un ASA : vous pouvez envoyer un message Ping à une interface sur un autre ASA pour vérifier qu'il est opérationnel et qu'il répond.

- Envoyer un message Ping via un ASA : vous pouvez envoyer un message Ping via un ASA intermédiaire en effectuant un Ping vers un périphérique situé de l'autre côté de l'ASA. Les paquets traverseront deux interfaces ASA intermédiaires dans chaque direction. Cette action effectue un test de base des interfaces, du fonctionnement et du temps de réponse de l'unité intermédiaire.
- Envoyer un message Ping pour tester le fonctionnement suspect d'un appareil réseau : vous pouvez envoyer un message Ping d'une interface ASA vers un appareil réseau que vous soupçonnez de fonctionner de manière incorrecte. Si l'interface est configurée correctement et qu'aucun écho n'est reçu, il pourrait y avoir des problèmes avec l'appareil.
- Envoyer un message Ping pour tester les communications intermédiaires : vous pouvez envoyer un message Ping à partir d'une interface ASA vers un appareil réseau connu pour fonctionner correctement. Si l'écho est reçu, le bon fonctionnement de tous les appareils intermédiaires et la connectivité physique sont confirmés.

Choisir entre le ping ICMP et TCP

L'ASA comprend le Ping traditionnel, qui envoie des paquets de requête d'écho ICMP et reçoit les paquets de réponse d'écho en retour. Il s'agit d'un outil standard qui fonctionne bien si tous les périphériques du réseau autorisent le trafic ICMP. Avec le Ping ICMP, vous pouvez envoyer un message Ping aux adresses IPv4 ou IPv6, ou aux noms d'hôte.

Cependant, certains réseaux interdisent le protocole ICMP. Si cela est le cas pour votre réseau, vous pouvez plutôt utiliser le Ping TCP pour tester la connectivité du réseau. Avec le Ping TCP, le Ping envoie des paquets TCP SYN et considère le Ping comme réussi s'il reçoit un SYN-ACK en réponse. Avec le Ping TCP, vous pouvez envoyer un message Ping à des adresses IPv4 ou à des noms d'hôte, mais vous ne pouvez pas envoyer un message Ping à des adresses IPv6.

Gardez à l'esprit qu'un message Ping ICMP ou TCP réussi signifie simplement que l'adresse que vous utilisez est active et répond à ce type de trafic. Cela signifie que la connectivité de base fonctionne. D'autres politiques exécutées sur un périphérique peuvent empêcher des types de trafic de passer avec succès par un périphérique.

Activer le protocole ICMP

Par défaut, vous pouvez envoyer un message Ping d'une interface à haute sécurité vers une interface à faible sécurité. Il vous suffit d'activer l'inspection ICMP pour permettre le trafic de retour. Si vous souhaitez effectuer un message Ping depuis une interface moins sécurisée vers une interface hautement sécurisée, vous devez appliquer une ACL pour autoriser le trafic.

Lors de l'envoi d'un message Ping à une interface ASA, toutes les règles ICMP appliquées à l'interface doivent autoriser les paquets de requête d'écho et de réponse d'écho. Les règles ICMP sont facultatives : si vous ne les configurez pas, tout le trafic ICMP vers une interface est autorisé.

Cette procédure explique toute la configuration ICMP que vous pourriez devoir effectuer pour activer l'envoi d'un message Ping ICMP des interfaces ASA ou pour l'envoi d'un message Ping par l'intermédiaire d'un ASA.

Procédure

Étape 1 Assurez-vous que les règles ICMP autorisent la requête d'écho/la réponse d'écho.

Les règles ICMP sont facultatives et s'appliquent aux paquets ICMP envoyés directement à une interface. Si vous n'appliquez pas de règles ICMP, tous les accès ICMP sont autorisés. Dans ce cas, aucune action n'est requise.

Cependant, si vous mettez en œuvre des règles ICMP, assurez-vous d'inclure des règles qui autorisent n'importe quelle adresse pour les messages d'écho et la réponse d'écho sur chaque interface. Configurez les règles ICMP dans le volet **Configuration > Device Management (Gestion des périphériques) > Management Access (Accès de gestion) > ICMP**.

Étape 2 Assurez-vous que les critères d'accès autorisent le protocole ICMP.

Lors de l'envoi d'un message Ping à un hôte via un ASA, les critères d'accès doivent autoriser le trafic ICMP à sortir et à revenir. Le critère d'accès doit autoriser au moins les paquets ICMP de requête d'écho/réponse d'écho. Vous pouvez ajouter ces règles en tant que règles globales.

Si vous n'avez pas de critères d'accès, vous devrez également autoriser l'autre type de trafic souhaité, car l'application de critères d'accès à une interface ajoute un refus implicite, de sorte que tout autre trafic sera abandonné.

Configurez les critères d'accès dans le volet **Configuration > Firewall (Pare-feu) > Access Rules (Critères d'accès)**. Si vous ajoutez simplement les règles à des fins de test, vous pouvez les supprimer après avoir terminé les tests.

Étape 3 Activez l'inspection ICMP.

L'inspection ICMP est nécessaire lors de l'envoi d'un message Ping à l'ASA, par opposition à l'envoi d'un message Ping à une interface. L'inspection permet de renvoyer le trafic (c'est-à-dire le paquet de réponse d'écho) à l'hôte qui a initié le message Ping et garantit également qu'il y a une réponse par paquet, ce qui empêche certains types d'attaques.

Vous pouvez simplement activer l'inspection ICMP dans la politique d'inspection globale par défaut.

a) Choisissez **Configuration > Firewall (Pare-feu) > Service Policy Rules (Règles de politique de service)**.
b) Modifiez la règle globale **inspection_default**.
c) Dans l'onglet **Rule Actions (Actions de règles) > Protocol Inspection (Inspection de protocole)**, sélectionnez ICMP.
d) Cliquez sur **OK**, puis sur **Apply** (Appliquer).

Envoyer un message ping à des hôtes

Pour envoyer un message Ping à n'importe quel appareil, choisissez simplement **Tools (Outils) > Ping**, saisissez l'adresse IP ou le nom d'hôte de la destination à laquelle vous envoyez un message Ping, puis cliquez sur **Ping**. Pour le ping TCP, sélectionnez **TCP** et incluez également le port de destination. C'est généralement tout ce que vous avez à faire pour effectuer un test.

Exemple de sortie pour un envoyer un message Ping réussi :

```
Sending 5, 100-byte ICMP Echos to out-pc, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Si l'envoi d'un message Ping échoue, la sortie indique ? pour chaque tentative en échec, et le taux de réussite est inférieur à 100 % (un échec complet correspond à 0 %) :

```
Sending 5, 100-byte ICMP Echos to 10.132.80.101, timeout is 2 seconds:
?????
Success rate is 0 percent (0/5)
```

Cependant, vous pouvez également ajouter des paramètres pour contrôler certains aspects du message Ping. Voici vos options de base :

- Ping ICMP : vous pouvez sélectionner l'interface utilisée pour l'adresse IP source; cependant, l'interface de sortie est déterminée par une recherche de routage à l'aide de la table de routage des données. Vous pouvez envoyer un message Ping aux adresses IPv4 ou IPv6 ou aux noms d'hôte.
- Ping TCP : vous devez également sélectionner le port TCP pour la destination à laquelle vous envoyez un ping. Par exemple, **www.example.com 80** pour envoyer un message Ping au port HTTP. Vous pouvez envoyer un message Ping à des adresses IPv4 ou à des noms d'hôte, mais pas aux adresses IPv6.

  Vous avez également la possibilité de spécifier l'interface utilisée pour l'adresse IP source; cependant, l'interface de sortie est déterminée par une recherche de routage à l'aide de la table de routage des données.

  Enfin, vous pouvez spécifier la fréquence de répétition du message Ping (la valeur par défaut est de 5 fois) ou le délai d'expiration pour chaque tentative (la valeur par défaut est de 2 secondes).

Tester la connectivité ASA de manière systématique

Si vous souhaitez effectuer un test plus systématique de la connectivité ASA, vous pouvez utiliser la procédure générale suivante.

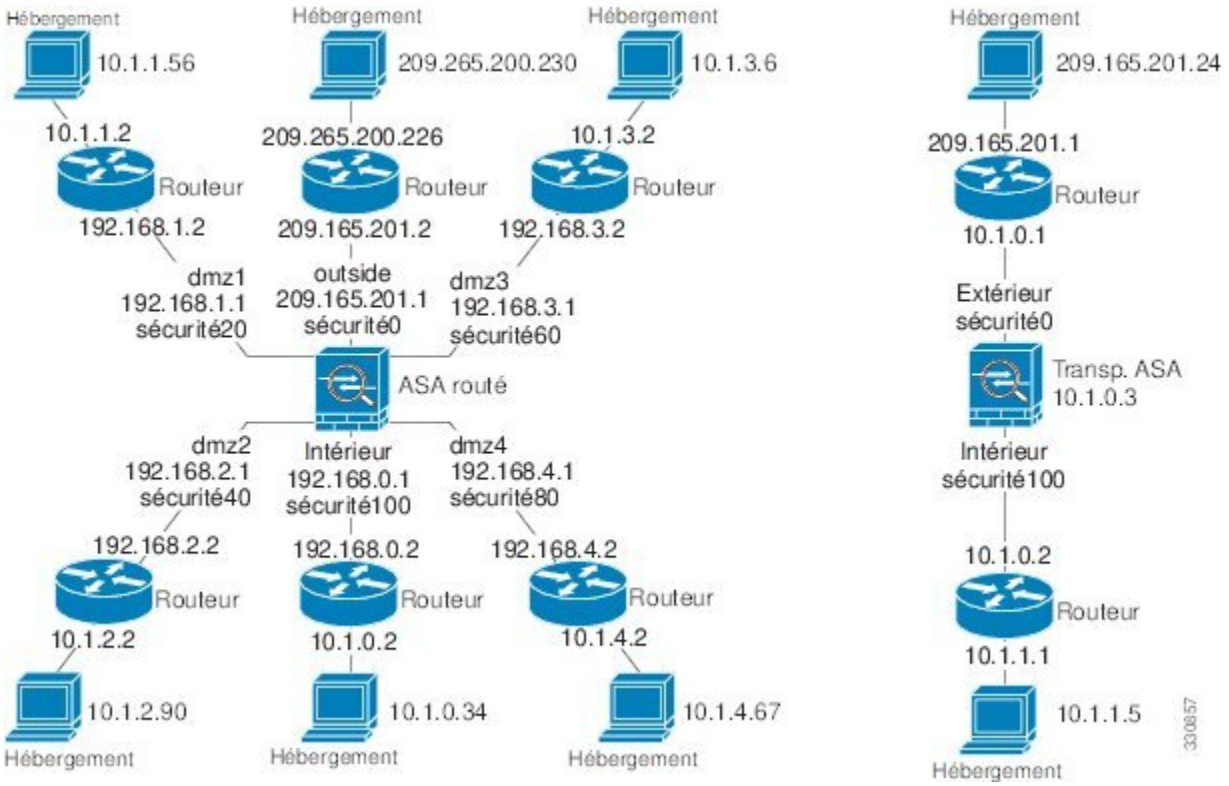
Avant de commencer

Si vous souhaitez voir les messages de journal système mentionnés dans la procédure, activez la journalisation (la commande **logging enable**, ou **Configuration > Device Management (Gestion des périphériques) > Logging (Journalisation) > Logging Setup (Configuration de la journalisation)** dans ASDM).

Procédure

Étape 1 Tracez un diagramme de votre ASA ou de votre contexte de sécurité en mode unique qui affiche les noms d'interface, les niveaux de sécurité et les adresses IP. Le diagramme doit également inclure tous les routeurs directement connectés et un hôte de l'autre côté du routeur à partir duquel vous allez envoyer un message Ping à l'ASA.

Illustration 1 : Diagramme de réseau avec interfaces, routeurs et hôtes



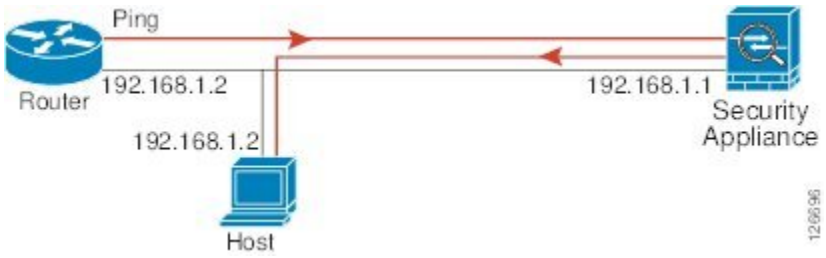
Étape 2 Envoyez un ping à chaque interface ASA à partir des routeurs directement connectés. Pour le mode transparent, envoyez un message Ping à l'adresse IP des BVI. Ce test garantit que les interfaces ASA sont actives et que la configuration d'interface est correcte.

Un message Ping peut échouer si l'interface ASA n'est pas active, si la configuration d'interface est incorrecte ou si un commutateur entre l'ASA et un routeur est en panne (voir la figure suivante). Dans ce cas, aucun message de débogage ni message de journal système ne s'affiche, car le paquet n'atteint jamais l'ASA.

Illustration 2 : Échec de ping à l'interface ASA



Illustration 3 : Échec de ping en raison de problèmes d'adressage IP



Si la réponse Ping ne revient pas au routeur, une boucle de commutation ou des adresses IP redondantes peuvent exister (voir la figure suivante).

Étape 3 Envoyez un ping à chaque interface ASA à partir d'un hôte distant. Pour le mode transparent, envoyez un message Ping à l'adresse IP des BVI. Ce test vérifie si le routeur connecté directement peut acheminer le paquet entre l'hôte et l'ASA et si l'ASA peut correctement acheminer le paquet vers l'hôte.

Un message Ping peut échouer si l'ASA n'a pas de route de retour vers l'hôte par le routeur intermédiaire (voir la figure suivante). Dans ce cas, les messages de débogage indiquent que l'envoi du message Ping a réussi, mais le message de journal système 110001 s'affiche, indiquant qu'une défaillance de routage s'est produite.

Illustration 4 : Échec de ping, car l'ASA n'a pas de route de retour



Étape 4 Envoyez un ping d'une interface ASA vers un périphérique réseau qui fonctionne correctement.

- Si le ping n'est pas reçu, il peut y avoir un problème avec le matériel de transmission ou la configuration de l'interface.
- Si l'interface ASA est configurée correctement et ne reçoit pas de réponse d'écho de l'appareil « connu pour être en bon état de fonctionnement », des problèmes avec la fonction de réception matérielle de l'interface peuvent exister. Si une interface différente ayant une capacité de réception « connue pour être bonne » peut recevoir un écho après avoir envoyé un message ping au même appareil « connu pour être bon », le problème de réception matérielle de la première interface est confirmé.

Étape 5 Envoyez un ping de l'hôte ou du routeur par l'interface source vers un autre hôte ou routeur sur une autre interface. Répétez cette étape pour autant de paires d'interfaces que vous souhaitez vérifier. Si vous utilisez la NAT, ce test montre que la NAT fonctionne correctement.

Si l'envoi d'un message Ping réussit, un message de journal système s'affiche pour confirmer la traduction d'adresses pour le mode routé (305009 ou 305011) et qu'une connexion ICMP a été établie (302020). Vous pouvez également saisir la commande **show xlate** ou **show conns** pour afficher ces renseignements.

L'envoi d'un message Ping peut échouer parce que la NAT n'est pas configurée correctement. Dans ce cas, un message de journal système s'affiche, indiquant que la NAT a échoué (305005 ou 305006). Si l'envoi d'un message Ping provient d'un hôte externe vers un hôte interne et que vous n'avez pas de traduction statique, vous recevez le message 106010.

Illustration 5 : Échec de ping parce que l'ASA ne traduit pas les adresses



Tracer les routes vers les hôtes

Si vous rencontrez des difficultés pour envoyer du trafic vers une adresse IP, vous pouvez tracer la route vers l'hôte pour déterminer s'il y a un problème sur le chemin réseau.

Procédure

Étape 1 Rendre l'ASA visible sur les routes de trace, à la page 23.

Étape 2 Déterminer les routes de paquets, à la page 23.

Rendre l'ASA visible sur les routes de trace

Par défaut, l'ASA n'apparaît pas sur les routes de trace en tant que saut. Pour l'afficher, vous devez décrémenter la durée de vie des paquets qui passent par l'ASA et augmenter la limite de débit pour les messages ICMP inaccessibles.

Procédure

Étape 1 Décrémentez la TTL à l'aide d'une politique de service.

a) Choisissez **Configuration > Firewall (Pare-feu) > Service Policy Rules (Règles de politique de service)**.
b) Ajoutez ou modifiez une règle. Par exemple, si vous avez déjà une règle à laquelle vous pouvez ajouter l'option de décrémentation de la TTL, vous n'avez pas besoin d'en créer une nouvelle.
c) Parcourez l'assistant jusqu'à la page Rule Actions (Actions découlant d'une règle), appliquez la règle globalement ou à une interface et spécifiez la correspondance de trafic. Par exemple, vous pouvez créer une règle de correspondance globale.
d) Sur la page Rule Actions (Actions découlant d'une règle), cliquez sur l'onglet **Connection Settings** (Paramètres de connexion) et sélectionnez **Decrement time to live for a connection** (Décrémenter la durée de vie d'une connexion).
e) Cliquez sur **OK** ou **Finish** (Terminer), puis **Apply** (Appliquer).

Étape 2 Augmentez la limite de débit pour les messages ICMP inaccessibles.

a) Choisissez **Configuration > Device Management (Gestion des périphériques) > Management Access (Accès de gestion) > ICMP**.
b) Augmentez la valeur **IPv4 ICMP Unreachable Message Limits > Rate Limit** (Limites de messages ICMP inaccessibles IPv4 > Limite de débit) au bas de la page. Par exemple, augmentez-la à 50.
c) Cliquez sur **Apply** (Appliquer).

Déterminer les routes de paquets

Utilisez la route de trace pour vous aider à déterminer la route que les paquets emprunteront pour atteindre leur destination. Une route de trace fonctionne en envoyant des paquets UDP ou des échos ICMPv6 à une destination sur un port non valide. Comme le port n'est pas valide, les routeurs situés sur le chemin vers la

destination répondent par un message de dépassement de temps ICMP ou ICMPv6 et signalent cette erreur à l'ASA.

La route de trace affiche le résultat de chaque sonde envoyée. Chaque ligne de sortie correspond à une valeur TTL par ordre croissant. Le tableau suivant explique les symboles de sortie.

Symbole de sortie	Description
*	Aucune réponse n'a été reçue pour la sonde dans le délai d'expiration.
U	Aucune route vers la destination.
nn msec	Pour chaque nœud, le temps d'aller-retour (en millisecondes) pour le nombre spécifié de sondes.
!N.	Réseau ICMP inaccessible. Pour ICMPv6, l'adresse est hors du champ d'application.
!H	Hôte ICMP inaccessible.
!P	ICMP inaccessible. Pour ICMPv6, port inaccessible.
!A	ICMP administrativement interdit.
?	Erreur ICMP inconnue.

Procédure

Étape 1 Choisissez **Tools (Outils)** > **Traceroute (Route de trace)**.

Étape 2 Saisissez le nom d'hôte ou l'adresse IP de destination vers lesquels vous tracez la route. Configurez un serveur DNS pour utiliser un nom d'hôte.

Étape 3 (Facultatif) Configurez les caractéristiques de la trace. Les valeurs par défaut conviennent dans la plupart des cas.

- **Timeout** (Délai d'expiration) : durée d'attente d'une réponse avant expiration du délai. La valeur par défaut est de 3 secondes.
- **Port** : le port UDP à utiliser. La valeur par défaut est 33434.
- **Probe** (Sonde) : nombre de sondes à envoyer à chaque niveau TTL. La valeur par défaut est de 3.
- **TTL** : valeurs de durée de vie minimum et maximum pour les sondes. La valeur minimum par défaut est de 1, mais vous pouvez la définir à une valeur plus élevée pour supprimer l'affichage des sauts connus. La valeur par défaut est 30. La route de trace se termine lorsque le paquet atteint sa destination ou lorsque la valeur maximum est atteinte.
- **Specify source interface or IP address** (Spécifier l'interface source ou l'adresse IP) : l'interface à utiliser comme source de la trace. Vous pouvez définir l'interface par son nom ou par son adresse IP. Pour IPv6, vous ne pouvez pas spécifier l'interface source; vous pouvez uniquement spécifier l'adresse IP source. Une adresse IPv6 n'est valide que si vous avez activé IPv6 sur une interface ASA.En mode transparent, vous devez utiliser l'adresse de gestion.

- **Reverse Resolve** (Résolution inverse) : si vous souhaitez que la sortie affiche les noms des sauts rencontrés si la résolution de nom DNS est configurée. Désélectionnez l'option pour afficher uniquement les adresses IP.
- **Use ICMP** (Utiliser ICMP) : si vous souhaitez envoyer des paquets de sonde ICMP au lieu de paquets de sonde UDP.

Étape 4 Cliquez sur **Trace Route** (Route de trace) pour démarrer la route de trace.

La zone **Traceroute Output** (Sortie de la route de trace) affiche des messages détaillés sur les résultats de la route de trace.

Utiliser l'outil Packet Tracer pour tester la configuration de la politique

Vous pouvez tester la configuration de votre politique en modélisant un paquet basé sur des adresses source et de destination, et des caractéristiques de protocole. La trace effectue des recherches de politiques pour tester les critères d'accès, la NAT, le routage, etc., pour voir si le paquet est autorisé ou refusé.

En testant les paquets de cette manière, vous pouvez voir les résultats de vos politiques et vérifier si les types de trafic que vous souhaitez autoriser ou refuser sont gérés comme vous le souhaitez. En plus de vérifier votre configuration, vous pouvez utiliser le traceur pour déboguer un comportement inattendu, tel que le refus de paquets alors qu'ils devraient être autorisés.

Procédure

Étape 1 Choisissez **Tools (Outils)** > **Packet Tracer (Outil de trace de paquets)**.

Étape 2 Choisissez l'**Interface** source pour la trace de paquet.

Étape 3 Spécifiez le **Packet Type** (Type de paquet) pour la trace de paquet. Les types de protocole disponibles sont ICMP, IP, TCP, UDP, SCTP.

Étape 4 (Facultatif) Si vous souhaitez suivre un paquet dont la valeur de balise de groupe de sécurité est intégrée dans l'en-tête CMD de couche 2 (Trustsec), cochez la case **SGT number** (Numéro SGT) et saisissez le numéro de balise de groupe de sécurité, de 0 à 65 533.

Étape 5 (Mode transparent) Si vous souhaitez que le traceur de paquets entre dans une interface parent, qui est ensuite redirigée vers une sous-interface, cochez **VLAN ID** (ID de VLAN) et entrez l'ID, de 1 à 4 096. L'ID de VLAN est disponible uniquement lorsque l'interface d'entrée n'est pas une sous-interface.

Étape 6 (Mode transparent) Spécifiez la **Destination MAC Address** (Adresse MAC de destination).

Étape 7 Spécifiez la source et la destination des paquets.

Vous pouvez spécifier des adresses IPv4 ou IPv6, des noms de domaine complets (FQDN), des noms de groupes de sécurité ou des balises si vous utilisez Cisco Trustsec. Pour l'adresse source, vous pouvez également spécifier un nom d'utilisateur au format Domaine\nom d'utilisateur.

Étape 8 Spécifiez les caractéristiques du protocole :

- ICMP : saisissez le type ICMP, le code ICMP (0 à 255) et éventuellement l'identifiant ICMP.
- TCP/UDP/SCTP : saisissez les numéros de port source et de destination.

- Adresse IP brute : saisissez le numéro de protocole, de 0 à 255.

Étape 9 Utilisez le traceur de paquets pour déboguer les paquets sur les unités de grappe. Dans la liste déroulante **Cluster Capture** (Capture de grappe), sélectionnez :

a) **decrypted** : injecte un paquet déchiffré dans un tunnel VPN et simule également un paquet qui traverse un tunnel VPN.
b) **persist** : injecte le paquet dont vous souhaitez suivre les unités de grappe.
c) **bypass-checks** : ignore les vérifications de sécurité comme les ACL, les filtres VPN, l'usurpation d'adresse IPsec et uRPF.
d) **transmit** : autorise des paquets simulés à quitter l'ASA.

Étape 10 Cliquer sur **Start** (Démarrer) pour suivre le paquet.

Information Display Area (Zone d'affichage des renseignements) affiche des messages détaillés sur les résultats de la trace de paquet.

Supervision des performances et des ressources du système

Vous pouvez surveiller diverses ressources système pour déterminer les performances ou d'autres problèmes potentiels.

Supervision des performances

Vous pouvez afficher les informations sur les performances de l'ASA dans un format graphique ou tableau.

Procédure

Étape 1 Choisissez **Monitoring (Supervision)** > **Properties (Propriétés)** > **Connection Graphs (Graphiques de connexion)** > **Perfmon**.

Étape 2 Vous pouvez attribuer un titre à la fenêtre de graphique en le saisissant dans **Graph Window Title** (Titre de fenêtre de graphique), ou vous pouvez choisir un titre existant.

Étape 3 Sélectionnez jusqu'à quatre entrées dans la liste des graphiques disponibles, puis cliquez sur **Add** (Ajouter) pour les déplacer vers la liste des graphiques sélectionnés. Les options disponibles sont les suivantes :

- AAA Perfmon : demandes par seconde pour les demandes authentification, d'autorisation et de gestion de comptes.
- Inspection Perfmon : paquets par seconde pour l'inspection HTTP, FTP et TCP.
- Web Perfmon : demandes par seconde pour les demandes d'accès URL et de serveur d'URL.
- Connexions Perfmon : connexions par seconde pour toutes les connexions, les connexions UDP, les connexions TCP et l'interception TCP.
- Xlate Perfmon : xlates NAT par seconde.

Étape 4 Cliquez sur **Show Graphs** (Afficher les graphiques).

Vous pouvez faire basculer chaque graphique entre les affichages de graphique et de tableau. Vous pouvez également modifier la fréquence d'actualisation des données et exporter ou imprimer les données.

Supervision des blocs de mémoire

Vous pouvez afficher les renseignements sur les blocs de mémoire disponibles et utilisés dans un format graphique ou tableau.

Procédure

Étape 1 Choisissez **Monitoring (Supervision)** > **Properties (Propriétés)** > **System Resources Graphs (Graphiques des ressources du système)** > **Blocks (Blocs)**.

Étape 2 Vous pouvez attribuer un titre à la fenêtre de graphique en le saisissant dans **Graph Window Title** (Titre de fenêtre de graphique), ou vous pouvez choisir un titre existant.

Étape 3 Sélectionnez des entrées dans la liste des graphiques disponibles, puis cliquez sur **Add** (Ajouter) pour les déplacer dans la liste des graphiques sélectionnés. Les options disponibles sont les suivantes :

- Blocs utilisés : affiche les blocs de mémoire utilisés de l'ASA.
- Blocs libres : affiche les blocs de mémoire libres de l'ASA.

Étape 4 Cliquez sur **Show Graphs** (Afficher les graphiques).

Vous pouvez faire basculer chaque graphique entre les affichages de graphique et de tableau. Vous pouvez également modifier la fréquence d'actualisation des données et exporter ou imprimer les données.

Supervision du CPU

Vous pouvez afficher l'utilisation du processeur.

Procédure

Étape 1 Choisissez **Monitoring (Supervision)** > **Properties (Propriétés)** > **System Resources Graphs (Graphiques des ressources du système)** > **CPU**.

Étape 2 Vous pouvez attribuer un titre à la fenêtre de graphique en le saisissant dans **Graph Window Title** (Titre de fenêtre de graphique), ou vous pouvez choisir un titre existant.

Étape 3 Ajoutez l'utilisation du CPU à la liste des graphiques sélectionnés.

Étape 4 Cliquez sur **Show Graphs** (Afficher les graphiques).

Vous pouvez faire basculer le graphique entre les affichages de graphique et de tableau. Vous pouvez également modifier la fréquence d'actualisation des données et exporter ou imprimer les données.

Supervision de la mémoire

Vous pouvez afficher les renseignements d'utilisation de la mémoire dans un format graphique ou tableau.

Procédure

Étape 1 Choisissez **Monitoring (Supervision)** > **Properties (Propriétés)** > **System Resources Graphs (Graphiques des ressources du système)** > **Memory (Mémoire)**.

Étape 2 Vous pouvez attribuer un titre à la fenêtre de graphique en le saisissant dans **Graph Window Title** (Titre de fenêtre de graphique), ou vous pouvez choisir un titre existant.

Étape 3 Sélectionnez des entrées dans la liste des graphiques disponibles, puis cliquez sur **Add** (Ajouter) pour les déplacer dans la liste des graphiques sélectionnés. Les options disponibles sont les suivantes :

- Mémoire libre : affiche la mémoire libre de l'ASA.
- Mémoire utilisée : affiche la mémoire utilisée de l'ASA.

Étape 4 Cliquez sur **Show Graphs** (Afficher les graphiques).

Vous pouvez faire basculer chaque graphique entre les affichages de graphique et de tableau. Vous pouvez également modifier la fréquence d'actualisation des données et exporter ou imprimer les données.

Supervision de l'utilisation du CPU par processus

Vous pouvez superviser les processus qui s'exécutent sur le CPU. Vous pouvez obtenir des renseignements sur le pourcentage de CPU utilisé par un processus donné. Les statistiques d'utilisation du CPU sont triées par ordre décroissant pour afficher le consommateur le plus élevé en haut. Des renseignements concernant la charge sur le CPU par processus sont également inclus, 5 secondes, 1 minute et 5 minutes avant l'heure du journal. Ces renseignements sont mis à jour automatiquement toutes les 5 secondes pour fournir des statistiques en temps réel. Dans ASDM, ils sont mis à jour toutes les 30 secondes.

Pour afficher l'utilisation du CPU par processus, choisissez **Monitoring (Supervision)** > **Properties (Propriétés)** > **Per-Process CPU Usage (Utilisation du CPU par processus)**.

Vous pouvez arrêter l'actualisation automatique, actualiser manuellement les renseignements ou les enregistrer dans un fichier. Vous pouvez également cliquer sur **Configure CPU Usage Colors** (Configurer les couleurs d'utilisation du CPU) pour choisir des couleurs d'arrière-plan et de premier plan en fonction des pourcentages d'utilisation, afin de faciliter l'analyse des processus à utilisation élevée.

Supervision des connexions

Pour afficher les connexions actuelles sous forme de tableau, dans la fenêtre principale d'ASDM, choisissez **Monitoring (Supervision) > Properties (Propriétés) > Connections (Connexions)**. Les renseignements relatifs à chaque connexion comprennent les caractéristiques du protocole, des adresses source et de destination, le temps d'inactivité depuis l'envoi ou la réception du dernier paquet, ainsi que le volume de trafic dans la connexion.

Historique des tests et du dépannage

Nom de la caractéristique	Versions de plateforme	Description
Prise en charge IPv6 pour les routes de trace	9.7(1)	La commande **traceroute** a été modifiée pour accepter une adresse IPv6. Nous avons modifié l'écran suivant : **Tools (Outils)** > **Traceroute (Route de trace)**
Prise en charge de l'outil de trace de paquets pour les interfaces membres du groupe de ponts	9.7(1)	Vous pouvez désormais utiliser l'outil de trace de paquets pour les interfaces membres d'un groupe de ponts. Nous avons ajouté les champs **VLAN ID** (ID de VLAN) et **Destination MAC Address** (Adresse MAC de destination) dans l'écran de l'outil de trace de paquets :**Tools (Outils)** > **Packet Tracer (Outil de trace de paquets)**
Démarrer et arrêter manuellement les captures de paquets	9.7(1)	Vous pouvez maintenant arrêter et démarrer manuellement la capture. Écrans ajoutés ou modifiés : **Wizards (Assistants)** > **Packet Capture Wizard (Assistant de capture de paquets)** > **Run Captures (Exécuter des captures)** Options ajoutées ou modifiées : bouton **Start** (Démarrer), bouton **Stop** (Arrêter)

Nom de la caractéristique	Versions de plateforme	Description
Capacités améliorées de l'outil de trace de paquets et de la capture de paquets	9.9(1)	L'outil de trace de paquets a été amélioré avec les fonctionnalités suivantes : • Tracer un paquet lorsqu'il passe entre les unités de grappe. • Autoriser des paquets simulés à quitter l'ASA. • Contourner les contrôles de sécurité pour un paquet simulé. • Considérer un paquet simulé comme un paquet IPsec/SSL déchiffré. La capture de paquets a été améliorée avec les fonctionnalités suivantes : • Capturer les paquets après leur déchiffrement. • Capturer les traces et les conserver dans la liste persistante. Écrans nouveaux ou modifiés : **Tools (Outils)** > **Packet Tracer (Outil de trace de paquets)** Nous avons ajouté le champ **Cluster Capture** (Capture de grappe) pour prendre en charge les options suivantes : **decrypted**, **persist**, **bypass-checks**, **transmit** Nous avons ajouté deux nouvelles options dans la vue **Filter By** (Filtrer par) dans la liste déroulante **All Sessions** (Toutes les sessions) : **Origin** et **Origin-ID** **Monitoring (Supervision)** > **VPN** > **VPN Statistics (Statistiques de VPN)** > **Packet Tracer and Capture (Outil de trace et capture de paquets)** Nous avons ajouté le champ **ICMP Capture** (Capture ICMP) dans l'écran Packet Capture Wizard (Assistant de capture de paquets) :**Wizards (Assistants)** > **Packet Capture Wizard (Assistant de capture de paquets)** Nous avons ajouté deux options : **include-decrypted** et **persist** pour prendre en charge la capture ICMP.

Nom de la caractéristique	Versions de plateforme	Description
Prise en charge de la capture de paquets pour le trafic IPv6 correspondant sans l'utilisation d'une ACL	9.10(1)	Si vous utilisez le mot clé **match** pour la commande **capture**, le mot clé **any** ne correspond qu'au trafic IPv4. Vous pouvez désormais spécifier les mots clés **any4** et **any6** pour capturer le trafic IPv4 ou IPv6. Le mot clé **any** continue de correspondre uniquement au trafic IPv4. Commandes nouvelles ou modifiées : **capture match** ASDM n'est pas pris en charge.
Nouvelle commande **debug telemetry** pour Forepower 9300/4100.	9.14(1)	Si vous utilisez la commande **debug telemetry**, les messages de débogage liés à la télémétrie s'affichent. Les débogages aident à identifier la cause des erreurs lors de la génération du rapport de télémétrie. Aucun écran modifié.
Modifications de la commande **ping**	9.18(2)	Pour prendre en charge l'envoi d'un message ping à une interface de boucle avec retour, la commande **ping** a maintenant changé de comportement. Si vous spécifiez l'interface dans la commande, l'adresse IP source correspond à l'adresse IP de l'interface spécifiée, mais l'interface de sortie réelle est déterminée par une recherche de route à l'aide de la table de routage des données. Commandes nouvelles ou modifiées : **ping**

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.