Paramètres de base

Ce chapitre décrit comment configurer les paramètres de base sur l'ASA qui sont généralement requis pour une configuration fonctionnelle.

Définir le nom d'hôte, le nom de domaine ainsi que les mots de passe d'activation et pour Telnet

Pour définir le nom d'hôte, le nom de domaine et les mots de passe d'activation et pour Telnet, procédez comme suit.

Avant de commencer

Avant de définir le nom d'hôte, le nom de domaine et les mots de passe d'activation et pour Telnet, assurez-vous les conditions préalables suivantes sont réunies :

- En mode contexte multiple, vous pouvez configurer le nom d'hôte et le nom de domaine dans les espaces d'exécution du système et du contexte.
- Les mots de passe d'activation et pour Telnet doivent être définis dans chaque contexte. Ils ne sont pas disponibles dans le système.
- Pour passer du système à une configuration de contexte, entrez la commande **changeto context** *name*.

Procédure

Étape 1 Précisez le nom d'hôte de l'ASA ou d'un contexte. Le nom d'hôte par défaut est « asa ».

nom d'hôte*nom*

Exemple :

```
ciscoasa(config)# hostname myhostnamexample12345
```

Ce nom peut comporter jusqu'à 63 caractères. Le nom d'hôte doit commencer et se terminer par une lettre ou un chiffre et ne comporter que des lettres, des chiffres ou un tiret.

Lorsque vous définissez un nom d'hôte pour l'ASA, ce nom apparaît dans l'invite de ligne de commande. Si vous établissez des sessions avec plusieurs appareils, le nom d'hôte facilite le suivi de l'emplacement où vous entrez des commandes.

En mode contexte multiple, le nom d'hôte que vous avez défini dans l'espace d'exécution du système apparaît dans l'invite de ligne de commande de tous les contextes. Le nom d'hôte que vous définissez dans un contexte n'apparaît pas sur la ligne de commande, mais il peut être utilisé par le jeton **$(hostname)** de la commande **banner**.

Étape 2 Précisez le nom de domaine de l'ASA. Le nom de domaine par défaut est default.domain.invalid.

domain-name *name*

Exemple :

```
ciscoasa(config)# domain-name example.com
```

L'ASA ajoute le nom de domaine sous forme de suffixe aux noms non qualifiés. Par exemple, si vous définissez le nom de domaine « example.com » et indiquez un serveur syslog sous le nom non qualifié de « jupiter », l'ASA remplace ce nom par « jupiter.example.com ».

Étape 3 Changez le mot de passe d'activation. Par défaut, le mot de passe d'activation est une valeur vide, mais vous êtes invité à la modifier la première fois que vous entrez la commande **enable**.

enable password *password*

Exemple :

```
ciscoasa(config)# enable password Pa$$w0rd
```

Le mot de passe d'activation vous permet de passer en mode d'exécution privilégié si vous ne configurez pas l'authentification d'activation. Le mot de passe d'activation vous permet également de vous connecter à ASDM avec un nom d'utilisateur vide si vous ne configurez pas l'authentification HTTP.

L'argument *password* est un mot de passe sensible à la casse, composé de 8 à 127 caractères. Il peut s'agir de n'importe quelle combinaison de caractères imprimables ASCII (codes 32 à 126), avec les exceptions suivantes :

- Aucun espace
- Aucun point d'interrogation

- Il est interdit d'utiliser trois caractères ASCII (ou plus) qui se suivent ou qui se répètent. Par exemple, les mots de passe suivants seront refusés :
  - **abc**utilisateur1
  - utilisateur**543**
  - utilisateur**aaaa**
  - utilisateur2**666**

Cette commande modifie le mot de passe pour le niveau de privilège le plus élevé (15). Si vous configurez l'autorisation de commande « local », vous pouvez définir des mots de passe d'activation pour chaque niveau de privilège, de 0 à 15, en utilisant la syntaxe suivante :

enable password *password* **level** *number*

Le mot clé **encrypted** (pour les mots de passe de 32 caractères ou moins dans les versions 9.6 et antérieures) ou le mot clé **pbkdf2** (pour les mots de passe de plus de 32 caractères dans les versions 9.6 et ultérieures, et les mots de passe de toutes les longueurs dans les versions 9.7 et ultérieures) indique que le mot de passe est chiffré (à l'aide d'un hachage basé sur MD5 ou d'un hachage PBCDF2 (Password-Based Key Derivation Function 2) utilisant SHA-512). Notez que les mots de passe existants continuent d'utiliser le hachage basé sur MD5, sauf si vous entrez un nouveau mot de passe. Lorsque vous définissez un mot de passe dans la commande **enable password**, l'ASA le chiffre avant de l'enregistrer dans la configuration à des fins de sécurité. Lorsque vous entrez la commande **show running-config**, la commande **enable password** n'affiche pas le mot de passe réel. Elle affiche le mot de passe chiffré suivi du mot clé **encrypted** ou **pbkdf2**. Par exemple, si vous entrez le mot de passe « test », la sortie de la commande **show running-config** se présentera comme suit :

```
username user1 password DLaUiAX3l78qgoB5c7iVNw== encrypted
```

Vous ne saisirez le mot clé **encrypted** ou **pbkdf2** dans l'interface de ligne de commande que si vous coupez-collez un fichier de configuration pour l'utiliser dans un autre ASA et que vous utilisez le même mot de passe.

Vous ne pouvez pas réinitialiser le mot de passe à une valeur vide.

Étape 4 Définissez le mot de passe de connexion pour l'accès Telnet. Il n'y a pas de mot de passe par défaut.

Le mot de passe de connexion est utilisé pour l'accès Telnet si vous ne configurez pas l'authentification Telnet.

passwd *password* [**encrypted**]

Exemple :

```
ciscoasa(config)# passwd cisco12345
```

Le *mot de passe* est sensible à la casse et peut comporter jusqu'à 16 caractères alphanumériques et spéciaux. Vous pouvez utiliser n'importe quel caractère dans le mot de passe, à l'exception d'un point d'interrogation ou d'un espace.

Le mot de passe est enregistré dans la configuration sous une forme chiffrée, ce qui vous empêche de voir le mot de passe d'origine après l'avoir saisi. Si, pour une raison quelconque, vous devez copier le mot de passe dans un autre ASA, mais que vous ne connaissez pas le mot de passe d'origine, vous pouvez saisir la commande

passwd avec le mot de passe chiffré et le mot clé **encrypted**. Normalement, vous ne voyez ce mot clé que lorsque vous entrez la commande **show running-config passwd**.

Régler la date et l'heure

Remarque Ne définissez pas la date et l'heure de de Firepower 2100 en mode plateforme, 4100/9300; l'ASA reçoit ces paramètres du châssis.

Définir les dates des fuseaux horaires et de l'heure avancée

Pour définir le fuseau horaire et la plage de dates de l'heure avancée, procédez comme suit.

Procédure

Étape 1 Définissez le fuseau horaire. Par défaut, le fuseau horaire est UTC.

- Modèles Firepower et Secure Firewall :

  clock timezone *zone*

  - *zone* : saisissez la commande **clock timezone ?** pour afficher une liste de noms de fuseau horaire acceptables.

  Exemple :

```
ciscoasa(config)# clock timezone ?
Available timezones:
CET
CST6CDT
Cuba
EET
Egypt
Eire
EST
EST5EDT
Factory
GB
GB-Eire
GMT
GMT0
GMT-0
GMT+0
Greenwich
Hongkong
HST
Iceland
Iran
Israel
Jamaica
```

```
Japan
[...]

ciscoasa(config)# clock timezone US/?

configure mode commands/options:
  US/Alaska          US/Aleutian    US/Arizona    US/Central
  US/East-Indiana    US/Eastern     US/Hawaii     US/Indiana-Starke
  US/Michigan        US/Mountain    US/Pacific

ciscoasa(config)# clock timezone US/Mountain
```

- Tous les autres modèles :

  clock timezone *zone* [-]*hours* [*minutes*]

  - *zone* : spécifie le fuseau horaire en tant que chaîne, par exemple, PST pour l'heure standard du Pacifique.
  - [-]*hours* : définit le nombre d'heures de décalage par rapport à l'heure UTC. Par exemple, PST est de -8 heures.
  - *minutes* : définit le nombre de minutes de décalage par rapport à l'heure UTC.

  Exemple :

```
ciscoasa(config)# clock timezone PST -8
```

Étape 2 (ASA virtuel et ISA 3000) Saisissez l'une des commandes suivantes pour modifier la plage de dates pour l'heure avancée à partir de la valeur par défaut. La plage de dates récurrentes par défaut va de 2 h le deuxième dimanche de mars à 2 h le premier dimanche de novembre.

- Définissez les dates de début et de fin de l'heure avancée comme date précise dans une année donnée. Si vous utilisez cette commande, vous devez réinitialiser les dates chaque année.

  clock summer-time *zone* **date** {*day month* | *month day*} *year hh***:***mm* {*day month* | *month day*} *year hh***:***mm* [*offset*]

  - *zone* : spécifie le fuseau horaire sous forme de chaîne, par exemple, PDT pour l'heure avancée du centre.
  - *day* : définit le jour du mois, de 1 à 31. Vous pouvez saisir le jour et le mois comme **a**vril 1er ou 1er avril, par exemple, selon votre format de date standard.
  - *month* : définit le mois sous la forme d'une chaîne de caractères. Vous pouvez saisir le jour et le mois comme avril 1er ou 1er avril, selon votre format de date standard.
  - *year* : définit l'année en utilisant quatre chiffres, par exemple, 2004. La plage d'années va de 1993 à 2035.
  - *hh:mm* : définit l'heure et les minutes sur 24 heures.
  - *offset* : définit le nombre de minutes pour modifier l'heure pour l'heure avancée. Par défaut, la valeur est de 60 minutes.

  Exemple :

```
ciscoasa(config)# clock summer-time PDT 1 April 2010 2:00 60
```

- Spécifiez les dates de début et de fin de l'heure avancée, sous la forme d'un jour et d'une heure du mois, et non d'une date précise dans une année. Cette commande vous permet de définir une plage de dates récurrentes que vous n'avez pas besoin de modifier chaque année.

  clock summer-time *zone* **recurring** [*week weekday month hh*:*mm week weekday month hh*:*mm*] [*offset*]

  - *zone* : spécifie le fuseau horaire sous forme de chaîne, par exemple, PDT pour l'heure avancée du centre.
  - *week* : spécifie la semaine du mois sous la forme d'un nombre entier compris entre 1 et 4 ou avec les mots « première » ou « dernière ». Par exemple, si le jour peut tomber sur la cinquième semaine, précisez « dernière ».
  - *weekday* : spécifie le jour de la semaine : lundi, mardi, mercredi, etc.
  - *month* : définit le mois sous la forme d'une chaîne de caractères.
  - *hh:mm* : définit l'heure et les minutes sur 24 heures.
  - *offset* : définit le nombre de minutes pour modifier l'heure pour l'heure avancée. Par défaut, la valeur est de 60 minutes.

  Exemple :

```
ciscoasa(config)# clock summer-time PDT recurring first Monday April 2:00 60
```

Définir la date et l'heure à l'aide du serveur NTP

Le protocole NTP est utilisé pour mettre en œuvre un système hiérarchique de serveurs qui fournissent une heure synchronisée avec précision entre les systèmes du réseau. Ce type de précision est requis pour les opérations urgentes, telles que la validation de listes de révocation de certificats, qui comprennent un horodatage précis. Vous pouvez configurer plusieurs serveurs NTP. L'ASA choisit le serveur avec la strate la plus basse, qui est une mesure de la fiabilité des données.

L'heure dérivée d'un serveur NTP remplace toute heure définie manuellement.

L'ASA prend en charge NTPv4.

Avant de commencer

En mode de contexte multiple, vous pouvez définir l'heure dans la configuration système uniquement.

Procédure

Étape 1 (Facultatif) Activez l'authentification avec un serveur NTP.

a) Activez l'authentification.

ntp authenticate

Exemple :

```
ciscoasa(config)# ntp authenticate
```

Lorsque vous activez l'authentification NTP, vous devez également spécifier un ID de clé dans la commande **ntp trusted-key** et associer cette clé au serveur à l'aide de la commande **ntp server key**. Configurez la clé réelle pour l'ID à l'aide de la commande **ntp authentication-key**. Si vous avez plusieurs serveurs, configurez un ID distinct pour chaque serveur.

b) Spécifiez un ID de clé d'authentification comme clé de confiance, qui est nécessaire pour l'authentification auprès d'un serveur NTP.

ntp trusted-key *key_id*

Exemple :

```
ciscoasa(config)# ntp trusted-key 1
ciscoasa(config)# ntp trusted-key 2
ciscoasa(config)# ntp trusted-key 3
ciscoasa(config)# ntp trusted-key 4
```

L'argument *key_id* est une valeur comprise entre 1 et 4294967295. Vous pouvez saisir plusieurs clés de confiance à utiliser avec plusieurs serveurs.

c) Définissez une clé pour vous authentifier auprès d'un serveur NTP.

ntp authentication-key *key_id* {**md5** | **sha1** | **sha256** | **sha512** | **cmac**} *key*

Exemple :

```
ciscoasa(config)# ntp authentication-key 1 md5 aNiceKey1
ciscoasa(config)# ntp authentication-key 2 md5 aNiceKey2
ciscoasa(config)# ntp authentication-key 3 md5 aNiceKey3
ciscoasa(config)# ntp authentication-key 4 md5 aNiceKey4
```

- *key_id* : définit l'ID que vous avez défini à l'aide de la commande **ntp trusted-key**.
- {**md5** | **sha1** | **sha256** | **sha512** | **cmac**} : définit l'algorithme.
- *key* : définit la clé sous la forme d'une chaîne pouvant comporter jusqu'à 32 caractères.

Étape 2 Identifiez un serveur NTP.

ntp server {*ipv4_address* | *ipv6_address* }[**key** *key_id*] [**source** *interface_name*] [**prefer**]

Exemple :

```
ciscoasa(config)# ntp server 10.1.1.1 key 1 prefer
ciscoasa(config)# ntp server 10.2.1.1 key 2
ciscoasa(config)# ntp server 2001:DB8::178 key 3
ciscoasa(config)# ntp server 2001:DB8::8945:ABCD key 4
```

Si vous avez activé l'authentification NTP (**ntp authenticate**), vous devez spécifier l'argument **key** *key_id* à l'aide de l'ID que vous avez défini à l'aide de la commande **ntp trusted-key**.

La paire mot clé-argument **source** *interface_name* identifie l'interface sortante pour les paquets NTP si vous ne souhaitez pas utiliser l'interface par défaut dans la table de routage. Étant donné que le système n'inclut aucune interface en mode de contexte multiple, spécifiez un nom d'interface défini dans le contexte d'administration.

Le mot clé **prefer** définit ce serveur NTP comme le serveur préféré si plusieurs serveurs ont une précision similaire. Le NTP utilise un algorithme pour déterminer quel serveur est le plus précis et se synchronise avec celui-ci. Si les serveurs sont de précision similaire, le mot clé **prefer** spécifie lequel de ces serveurs utiliser. Cependant, si un serveur est nettement plus précis que le serveur préféré, l'ASA utilise le plus précis. Par exemple, l'ASA utilise un serveur de strate 2 plutôt qu'un serveur de strate 3 qui est préféré.

Vous pouvez identifier plusieurs serveurs; l'ASA utilise le serveur le plus précis.

Régler la date et l'heure manuellement

Pour définir la date et l'heure manuellement, procédez comme suit :

Avant de commencer

En mode de contexte multiple, vous pouvez définir l'heure dans la configuration système uniquement.

Procédure

Réglez la date et l'heure manuellement.

clock set *hh*:*mm*:*ss* {*month day* | *day month*} *year*

Exemple :

```
ciscoasa# clock set 20:54:00 april 1 2004
```

L'argument *hh*:*mm*:*ss* définit l'heure, les minutes et les secondes sur 24 heures. Par exemple, saisissez 20:54:00 pour 20:54.

La valeur du jour définit le jour du mois, de 1 à 31. Vous pouvez saisir le jour et le mois comme avril 1er ou 1er avril, par exemple, selon votre format de date standard.

La valeur du mois définit le mois. Selon votre format de date standard, vous pouvez saisir le jour et le mois comme avril 1er ou 1er avril.

La valeur de l'année définit l'année en utilisant quatre chiffres, par exemple, 2004. La fourchette d'années va de 1993 à 2035.

Le fuseau horaire par défaut est UTC. Si vous modifiez le fuseau horaire après avoir saisi la commande **clock set** à l'aide de la commande **clock timezone**, l'heure s'ajuste automatiquement au nouveau fuseau horaire.

Cette commande règle l'heure dans la puce matérielle et n'enregistre pas l'heure dans le fichier de configuration. Cette heure résiste aux redémarrages. Contrairement aux autres commandes **clock**, celle-ci est une commande

EXEC privilégée. Pour réinitialiser l'horloge, vous devez régler une nouvelle heure avec la commande clock set.

Configurer le protocole PTP (Precision Time Protocol) (ISA 3000)

Le protocole PTP (Precision Time Protocol) est un protocole de synchronisation horaire développé pour synchroniser les horloges de divers périphériques au sein d'un réseau par paquets. Ces horloges sont généralement de précision et de stabilité variables. Le protocole est spécialement conçu pour les systèmes de mesure et de contrôle industriels en réseau. Il est idéal pour une utilisation dans les systèmes distribués, car il nécessite une bande passante et un surdébit de traitement minimaux.

Un système PTP est un système en réseau distribué, composé d'une combinaison de périphériques PTP et non-PTP. Les périphériques PTP comprennent les horloges normales, les horloges périphériques et les horloges transparentes. Les périphériques non PTP comprennent les commutateurs réseau, les routeurs et les autres périphériques de l'infrastructure.

Vous pouvez configurer l'ASA pour qu'il soit une horloge transparente. L'ASA ne synchronise pas son horloge avec les horloges PTP. L'ASA utilisera le profil PTP par défaut, comme défini sur les horloges PTP.

Lorsque vous configurez les périphériques PTP, vous définissez un numéro de domaine pour les périphériques qui sont destinés à fonctionner ensemble. Ainsi, vous pouvez configurer plusieurs domaines PTP, puis configurer chaque périphérique non PTP pour qu'il utilise les horloges PTP d'un domaine spécifique.

Avant de commencer

- Cette fonctionnalité est uniquement disponible sur l'ISA 3000.
- L'utilisation du PTP n'est prise en charge qu'en mode de contexte unique.
- Cisco PTP prend uniquement en charge les messages PTP en multidiffusion.
- Le PTP est activé sur toutes les interfaces ISA 3000 en mode transparent par défaut. En mode routé, vous devez ajouter la configuration nécessaire pour vous assurer que les paquets PTP sont autorisés à transiter par le périphérique.
- Le PTP est disponible uniquement pour les réseaux IPv4, et non pour les réseaux IPv6.
- La configuration PTP est prise en charge sur les interfaces Ethernet physiques, qu'elles soient autonomes ou membres d'un groupe de ponts. Elle n'est pas prise en charge sur :
    - Interface de gestion.
    - Sous-interfaces, EtherChannels, BVI ou toute autre interface virtuelle.
- Les flux PTP sur les sous-interfaces VLAN sont pris en charge, en supposant que la configuration PTP appropriée est présente sur l'interface parente.
- Vous devez vous assurer que les paquets PTP sont autorisés à circuler dans le périphérique. En mode de pare-feu transparent, la configuration de la liste d'accès permettant le trafic PTP est configurée par défaut. Le trafic PTP est identifié par les ports UDP 319 et 320 et par l'adresse IP de destination 224.0.1.129. Ainsi, en mode de pare-feu routé, toute liste ACL autorisant ce trafic devrait être acceptable.
- En mode de pare-feu routé, vous devez également activer le routage de multidiffusion pour les groupes de multidiffusion PTP :

- Entrez la commande du mode de configuration globale **multicast-routing**.
- Et pour chaque interface qui n'est pas membre d'un groupe de ponts et sur laquelle le protocole PTP est activé, saisissez la commande de configuration d'interface **igmp join-group 224.0.1.129** pour activer statiquement l'appartenance au groupe de multidiffusion PTP. Cette commande n'est pas prise en charge ni nécessaire pour les membres du groupe de ponts.

Procédure

Étape 1 Spécifiez le numéro de domaine de tous les ports du périphérique :

ptp domain *domain_num*

Exemple :

```
ciscoasa(config)# ptp domain 54
```

L'argument *domain_num* est le numéro de domaine de tous les ports du périphérique. Les paquets reçus dans un domaine différent sont traités comme des paquets de multidiffusion ordinaires et ne subissent aucun traitement PTP. Cette valeur peut aller de zéro à 255; la valeur par défaut est zéro. Saisissez le numéro de domaine configuré sur les périphériques PTP de votre réseau.

Étape 2 (Facultatif) Configurez le mode d'horloge PTP sur le périphérique :

ptp mode e2etransparent

Exemple :

```
ciscoasa(config)# ptp mode e2etransparent
```

Cette commande active le mode transparent de bout en bout sur toutes les interfaces compatibles avec PTP.

Étape 3 Activez PTP sur une interface :

ptp enable

Activez PTP sur chaque interface par laquelle le système peut communiquer avec une horloge PTP dans le domaine configuré.

Exemple :

```
ciscoasa(config)# interface gigabitethernet1/2
ciscoasa(config-if)# ptp enable
```

Configurer la phrase secrète principale

La phrase secrète principale vous permet de stocker en toute sécurité les mots de passe en texte brut dans un format chiffré et fournit une clé utilisée pour chiffrer ou masquer tous les mots de passe de manière universelle, sans modifier aucune fonctionnalité. Voici les fonctionnalités qui utilisent la phrase secrète principale :

- OSPF
- EIGRP

- Équilibrage de la charge VPN
- VPN (accès à distance et de site à site)
- Basculement
- Serveurs AAA
- Logging (journalisation)
- Licences partagées

Ajouter ou modifier la phrase secrète principale

Pour ajouter ou modifier la phrase secrète principale, procédez comme suit.

Avant de commencer

- Cette procédure ne sera acceptée que dans une session sécurisée, par exemple par la console, SSH ou ASDM via HTTPS.
- Si le basculement est activé, mais qu'aucune clé partagée de basculement n'est définie, un message d'erreur s'affiche si vous modifiez la phrase secrète principale, vous informant que vous devez saisir une clé partagée de basculement pour protéger les modifications de phrase secrète principale contre l'envoi en texte brut.
- L'activation ou la modification du chiffrement par mot de passe dans le basculement actif/veille entraîne un **write standby**, qui réplique la configuration active sur l'unité de secours. Sans cette réplication, les mots de passe chiffrés sur l'unité de secours seront différents, même s'ils utilisent la même phrase secrète; la réplication de la configuration garantit que les configurations sont identiques. Pour le basculement actif/actif, vous devez saisir manuellement **write standby**. Un **write standby** peut entraîner une interruption du trafic en mode actif/actif, car la configuration est effacée sur l'unité secondaire avant que la nouvelle configuration ne soit synchronisée. Vous devez activer tous les contextes sur l'ASA principal à l'aide des commandes **failover active group 1** et **failover active group 2**, saisir **write standby**, puis restaurer les contextes du groupe 2 sur l'unité secondaire à l'aide de la commande **no failover active group 2**.

Procédure

Étape 1 Définissez la phrase secrète utilisée pour générer la clé de chiffrement. La phrase secrète doit comporter de 8 à 128 caractères. Tous les caractères, à l'exception de la touche retour arrière et des guillemets doubles, sont acceptés pour la phrase secrète. Si vous ne saisissez pas la nouvelle phrase secrète dans la commande, vous serez invité à la saisir. Pour modifier la phrase secrète, vous devez saisir l'ancienne phrase secrète.

key config-key password-encryption [*new_passphrase* [*old_passphrase*]]

Exemple :

```
ciscoasa(config)# key config-key password-encryption
Old key: bumblebee
New key: haverford
Confirm key: haverford
```

Remarque
Utilisez les invites interactives pour saisir les mots de passe afin d'éviter que les mots de passe soient enregistrés dans le tampon de l'historique des commandes.

Utilisez la commande **no key config-key password-encrypt** avec prudence, car elle change les mots de passe chiffrés en mots de passe en texte brut. Vous pouvez utiliser la forme **no** de cette commande lors de la rétrogradation à une version logicielle qui ne prend pas en charge le chiffrement des mots de passe.

Étape 2 Activez le chiffrement des mots de passe.

password encryption aes

Exemple :

```
ciscoasa(config)# password encryption aes
```

Dès que le chiffrement des mots de passe est activé et que la phrase secrète principale est disponible, tous les mots de passe des utilisateurs seront chiffrés. La configuration en cours d'exécution affichera les mots de passe dans le format chiffré.

Si la phrase secrète n'est pas configurée au moment où le chiffrement du mot de passe est activé, la commande réussira en prévision de la disponibilité future de la phrase secrète.

Si vous désactivez ultérieurement le chiffrement des mots de passe à l'aide de la commande **no password encryption aes**, tous les mots de passe chiffrés existants resteront inchangés et, tant que la phrase secrète principale existe, les mots de passe chiffrés seront déchiffrés, comme l'exige l'application.

Étape 3 Enregistrez la valeur d'exécution de la phrase secrète principale et la configuration résultante.

write memory

Exemple :

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

Si vous ne saisissez pas cette commande, les mots de passe de la configuration de démarrage peuvent toujours être visibles s'ils n'ont pas été enregistrés pour le chiffrement précédemment. De plus, en mode de contexte multiple, le mot de passe principal est modifié dans la configuration du contexte système. Par conséquent, les mots de passe de tous les contextes seront affectés. Si la commande write memory n'est pas saisie en mode de contexte système, mais pas dans tous les contextes d'utilisateur, les mots de passe chiffrés dans les contextes d'utilisateur peuvent être obsolètes. Vous pouvez également utiliser la commande write memory all dans le contexte système pour enregistrer toutes les configurations.

Exemples

L'exemple suivant montre qu'aucune clé n'existait auparavant :

```
ciscoasa(config)# key config-key password-encryption 12345678
```

L'exemple suivant montre qu'une clé existe déjà :

```
ciscoasa(config)# key config-key password-encryption 23456789
Old key: 12345678
```

Dans l'exemple suivant, vous saisissez la commande sans paramètres afin que le système vous demande les clés. Comme une clé existe déjà, vous êtes invité à l'utiliser.

```
ciscoasa(config)# key config-key password-encryption
Old key: 12345678
New key: 23456789
Confirm key: 23456789
```

Dans l'exemple suivant, il n'y a pas de clé existante, vous n'êtes donc pas invité à la fournir.

```
ciscoasa(config)# key config-key password-encryption
New key: 12345678
Confirm key: 12345678
```

Désactiver la phrase secrète principale

La désactivation de la phrase secrète principale rétablit les mots de passe chiffrés en mots de passe en texte brut. Supprimer la phrase secrète peut être utile si vous rétrogradez à une version précédente du logiciel qui ne prend pas en charge les mots de passe chiffrés.

Avant de commencer

- Vous devez connaître la phrase secrète principale actuelle pour la désactiver. Consultez Supprimer la phrase secrète principale, à la page 14 si vous ne connaissez pas la phrase secrète.
- Cette procédure fonctionne uniquement dans une session sécurisée; c'est-à-dire par Telnet, SSH ou ASDM via HTTPS.

  Pour désactiver la phrase secrète principale, procédez comme suit :

Procédure

Étape 1 Supprimez la phrase secrète principale. Si vous ne saisissez pas la phrase secrète dans la commande, vous serez invité à la saisir.

no key config-key password-encryption [*old_passphrase*]]

Exemple :

```
ciscoasa(config)# no key config-key password-encryption

Warning! You have chosen to revert the encrypted passwords to plain text.
This operation will expose passwords in the configuration and therefore
exercise caution while viewing, storing, and copying configuration.

Old key: bumblebee
```

Étape 2 Enregistrez la valeur d'exécution de la phrase secrète principale et la configuration résultante.

write memory

Exemple :

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

La mémoire non volatile contenant la phrase secrète sera effacée et remplacée par le modèle 0xFF.

En mode multiple, la phrase secrète principale est modifiée dans la configuration du contexte système. Par conséquent, les mots de passe de tous les contextes seront affectés. Si la commande write memory est saisie en mode de contexte système, mais pas dans tous les contextes d'utilisateur, les mots de passe chiffrés dans les contextes d'utilisateur peuvent être obsolètes. Vous pouvez également utiliser la commande write memory all dans le contexte système pour enregistrer toutes les configurations.

Supprimer la phrase secrète principale

Vous ne pouvez pas récupérer la phrase secrète principale. Si la phrase secrète principale est perdue ou inconnue, vous pouvez la supprimer.

Pour supprimer la phrase secrète principale, procédez comme suit :

Procédure

Étape 1 Supprimez la clé principale et la configuration qui comprend les mots de passe chiffrés.

write erase

Exemple :

```
ciscoasa(config)# write erase
```

Étape 2 Rechargez l'ASA avec la configuration de démarrage, sans clé principale ni mot de passe chiffré.

reload

Exemple :

```
ciscoasa(config)# reload
```

Configurer des serveurs DNS

Vous devez configurer un serveur DNS pour que l'ASA puisse résoudre les noms d'hôte en adresses IP. Vous devez également configurer un serveur DNS pour utiliser des objets réseau de noms de domaine complets (FQDN) dans les critères d'accès.

Certaines fonctionnalités de l'ASA nécessitent l'utilisation d'un serveur DNS pour accéder aux serveurs externes par nom de domaine. D'autres fonctionnalités, telles que la commande **ping** ou **traceroute**, vous permettent de saisir un nom que vous souhaitez envoyer par message Ping ou par route de trace. L'ASA peut résoudre le nom en communiquant avec un serveur DNS. De nombreuses commandes SSL VPN et de certificat prennent également en charge les noms.

Par défaut, il existe un groupe de serveurs DNS par défaut appelé DefaultDNS. Vous pouvez créer plusieurs groupes de serveurs DNS : un groupe est le groupe par défaut, tandis que les autres groupes peuvent être associés à des domaines spécifiques. Une requête DNS qui correspond à un domaine associé à un groupe de serveurs DNS utilisera ce groupe. Par exemple, si vous souhaitez que le trafic destiné aux serveurs internes eng.cisco.com utilise un serveur DNS interne, vous pouvez mapper eng.cisco.com à un groupe DNS interne. Toutes les requêtes DNS qui ne correspondent pas à un mappage de domaine utiliseront le groupe de serveurs DNS par défaut, qui n'a pas de domaine associé. Par exemple, le groupe DefaultDNS peut inclure un serveur DNS public disponible sur l'interface externe. D'autres groupes de serveurs DNS peuvent être configurés pour les groupes de tunnels VPN. Consultez la commande **tunnel-group** dans la référence de commande pour en savoir plus.

Remarque L'ASA a une prise en charge limitée pour l'utilisation du serveur DNS, en fonction de la fonctionnalité. Par exemple, la plupart des commandes nécessitent que vous saisissiez une adresse IP et ne peuvent utiliser un nom que lorsque vous configurez manuellement la commande **name** pour associer un nom à une adresse IP et permettre l'utilisation des noms à l'aide de la commande names.

Avant de commencer

Assurez-vous de configurer les règles de routage et d'accès appropriées pour toute interface sur laquelle vous activez la recherche de domaine DNS afin de pouvoir atteindre le serveur DNS.

Procédure

Étape 1 Permettez à l'ASA d'envoyer des requêtes DNS à un serveur DNS afin d'effectuer une recherche de nom pour les commandes prises en charge.

dns domain-lookup *interface_name*

Si vous n'activez pas la recherche DNS sur une interface, l'ASA ne communiquera pas avec le serveur DNS sur cette interface. Assurez-vous d'activer la recherche DNS sur toutes les interfaces qui seront utilisées pour accéder aux serveurs DNS.

Exemple :

```
ciscoasa(config)# dns domain-lookup inside
ciscoasa(config)# dns domain-lookup outside
```

Étape 2 Créez un ou plusieurs groupes de serveurs DNS et ajoutez des serveurs aux groupes.

a) Nommez le groupe de serveurs DNS.

dns server-group *name*

Pour configurer le groupe de serveurs DefaultDNS par défaut, spécifiez DefaultDNS comme nom.

Exemple :

```
ciscoasa(config)# dns server-group DefaultDNS
```

b) Spécifiez un ou plusieurs serveurs DNS pour le groupe.

name-server *ip_address* [*ip_address2*] [...] [*ip_address6*] *[interface_name]*

Vous pouvez saisir les six adresses IP dans la même commande, séparées par des espaces, ou vous pouvez saisir chaque commande séparément.

(Facultatif) Spécifiez le *nom de l'interface* par lequel l'ASA communique avec le serveur. Si vous ne spécifiez pas d'interface, l'ASA vérifie la table de routage des données; s'il n'y a aucune correspondance, il vérifie la table de routage de gestion uniquement.

L'ASA essaie chaque serveur DNS dans l'ordre jusqu'à ce qu'il reçoive une réponse.

Exemple :

```
ciscoasa(config-dns-server-group)# name-server 10.1.1.5 192.168.1.67 209.165.201.6 outside
```

c) (Pour le groupe par défaut uniquement) Configurez le nom de domaine ajouté au nom d'hôte s'il n'est pas entièrement qualifié.

domain-name *name*

Exemple :

```
ciscoasa(config-dns-server-group)# domain-name example.com
```

d) (Facultatif) Configurez les propriétés supplémentaires du groupe de serveurs DNS.

Utilisez les commandes suivantes pour modifier les caractéristiques du groupe, si les paramètres par défaut ne conviennent pas à votre réseau.

- **timeout** *seconds* : le nombre de secondes, de 1 à 30, à attendre avant d'essayer le serveur DNS suivant. La valeur par défaut est de 2 secondes. Chaque fois que l'ASA réessaie la liste des serveurs, ce délai est doublé.
- **retries** *number* : le nombre de tentatives, de 0 à 10, pour retenter d'accéder à la liste des serveurs DNS lorsque l'ASA ne reçoit pas de réponse.
- **expire-entry-timer minutes** *number* : la TTL minimum pour l'entrée DNS, en minutes. Si le délai d'expiration est plus long que la durée de vie de l'entrée, cette dernière est augmentée jusqu'à la valeur du délai d'expiration de l'entrée. Si la durée de vie est plus longue que le délai d'expiration, la valeur du délai d'expiration est ignorée : dans ce cas, aucun délai supplémentaire n'est ajouté à la durée de vie. À l'expiration, l'entrée est supprimée de la table de consultation du DNS. La suppression d'une entrée nécessite la recompilation de la table, de sorte que des suppressions fréquentes peuvent augmenter la charge de traitement du périphérique. Comme certaines entrées DNS peuvent avoir une durée de vie très courte (jusqu'à trois secondes), vous pouvez utiliser ce paramètre pour prolonger virtuellement cette dernière. La valeur par défaut est 1 minute (c'est-à-dire que la durée de vie minimale pour toutes les résolutions est de 1 minute). La plage est comprise entre 1 et 65535 minutes. Cette option est utilisée uniquement pour la résolution d'objets réseau FQDN.

- **poll-timer minutes** *number* : la durée, en minutes, du cycle d'interrogation utilisé pour résoudre les objets réseau/hôte FQDN en adresses IP. Les objets FQDN ne sont résolus que s'ils sont utilisés dans une politique de pare-feu. La minuterie détermine le temps maximum entre les résolutions; la valeur de durée de vie (TTL) de l'entrée DNS est également utilisée pour déterminer quand mettre à jour la résolution d'adresse IP, de sorte que les FQDN individuels puissent être résolus plus fréquemment que le cycle d'interrogation. La valeur par défaut est 240 (quatre heures). La plage est comprise entre 1 et 65535 minutes.

e) Répétez les étapes ci-dessus pour ajouter des groupes de serveurs DNS supplémentaires.

Étape 3 (Facultatif) Mappez les domaines à des groupes de serveurs DNS spécifiques.

dns-group-map

dns-to-domain *dns_group_name domain*

Vous pouvez mapper jusqu'à 30 domaines. Vous ne pouvez pas mapper le même domaine à plusieurs groupes de serveurs DNS, mais vous pouvez mapper plusieurs domaines au même groupe de serveurs. Ne mappez aucun domaine au groupe que vous souhaitez utiliser par défaut (par exemple, DefaultDNS).

Exemple :

```
ciscoasa(config)# dns-group-map
ciscoasa(config-dns-group-map)# dns-to-domain group1 eng.cisco.com
ciscoasa(config-dns-group-map)# dns-to-domain group1 hr.cisco.com
ciscoasa(config-dns-group-map)# dns-to-domain group2 example.com
```

Étape 4 Spécifiez le groupe DNS par défaut.

dns-group *name*

Par défaut, DefaultDNS est spécifié. Si vous avez configuré d'autres groupes, vous pouvez définir un groupe par défaut différent à l'aide de cette commande. Le groupe par défaut ne peut avoir aucun domaine associé dans la carte des groupes DNS.

Exemple :

```
ciscoasa(config)# dns-group new_default_group
```

Configurer le contournement matériel et l'alimentation double (Cisco ISA 3000)

Le contournement matériel garantit que le trafic continue de circuler entre une paire d'interfaces en ligne pendant une panne de courant. Les paires d'interfaces prises en charge sont les interfaces en cuivre GigabitEthernet 1/1 et 1/2; et GigabitEthernet 1/3 et 1/4. Lorsque le contournement matériel est actif, aucune fonction de pare-feu n'est en place. Veuillez donc vous assurer de bien comprendre les risques liés à l'autorisation du trafic de transit. Consultez les lignes directrices suivantes relatives au contournement matériel :

- Cette fonctionnalité est uniquement disponible sur le périphérique Cisco ISA 3000.
- Si vous avez un modèle Ethernet à fibre optique, seule la paire Ethernet en cuivre (GigabitEthernet 1/1 et 1/2) prend en charge le contournement matériel.

- Lorsque l'ISA 3000 perd de l'alimentation et passe en mode de contournement matériel, seules les paires d'interfaces prises en charge peuvent communiquer; avec la configuration par défaut, inside1 <---> inside2 et outside1 <---> outside2 ne peuvent plus communiquer. Toutes les connexions existantes entre ces interfaces seront perdues.
- Nous vous suggérons de désactiver la répartition aléatoire des séquences TCP (comme le décrit cette procédure). Si la répartition aléatoire est activée (par défaut), lorsque le contournement matériel sera activé, les sessions TCP devront être rétablies. Par défaut, l'ISA 3000 réécrit le numéro de séquence initial (ISN) des connexions TCP qui le traversent en nombre aléatoire. Lorsque le contournement matériel est activé, l'ISA 3000 ne se trouve plus dans le chemin de données et ne traduit pas les numéros de séquence; le client destinataire reçoit un numéro de séquence inattendu et interrompt la connexion. Même lorsque la répartition aléatoire de la séquence TCP est désactivée, certaines connexions TCP devront être rétablies car la liaison a été temporairement interrompue pendant le basculement.
- Les connexions Cisco TrustSec sur les interfaces de contournement matériel sont abandonnées lorsque le contournement matériel est activé. Lorsque l'ISA 3000 démarre et que le contournement matériel est désactivé, les connexions sont renégociées.
- Lorsque le contournement matériel est désactivé et que le trafic reprend par le chemin de données de l'ISA 3000, certaines sessions TCP existantes doivent être rétablies en raison de la liaison qui est temporairement inactive pendant le basculement.
- Lorsque le contournement matériel est actif, les PHY Ethernet sont déconnectés, de sorte que l'ASA ne peut pas déterminer l'état de l'interface. Les interfaces peuvent sembler être en panne.

Pour les alimentations doubles dans l'ISA 3000, vous pouvez établir des alimentations doubles comme la configuration attendue dans le système d'exploitation ASA. En cas de défaillance d'une alimentation, l'ASA émet une alarme. Par défaut, l'ASA s'attend à une seule alimentation et n'émettra pas d'alarme tant qu'il dispose d'une alimentation opérationnelle.

Avant de commencer

- Vous devez connecter les interfaces de contournement matériel pour accéder aux ports du commutateur. Ne les connectez pas aux ports de ligne principale.

Procédure

Étape 1 Configurez le contournement matériel pour qu'il s'active en cas de panne de courant :

hardware-bypass GigabitEthernet {**1/1-1/2** | **1/3-1/4**} [**sticky**]

Exemple :

```
ciscoasa(config)# hardware-bypass GigabitEthernet 1/1-1/2
ciscoasa(config)# hardware-bypass GigabitEthernet 1/3-1/4
```

Le mot clé **sticky** maintient l'appareil en mode de contournement matériel après le rétablissement du courant et le démarrage de l'appareil. Dans ce cas, vous devez désactiver manuellement le contournement matériel lorsque vous êtes prêt; cette option vous permet de contrôler le moment où une brève interruption du trafic se produit.

Étape 2 Activez ou désactivez manuellement le contournement matériel :

[**no**] **hardware-bypass manual GigabitEthernet** {**1/1-1/2** | **1/3-1/4**}

Exemple :

```
ciscoasa# hardware-bypass manual GigabitEthernet 1/1-1/2
ciscoasa# no hardware-bypass manual GigabitEthernet 1/1-1/2
```

Étape 3 (Facultatif) Configurez le contournement matériel pour qu'il reste actif jusqu'après le démarrage du module ASA FirePOWER :

hardware-bypass boot-delay module-up sfr

Vous devez activer le contournement matériel sans l'option **sticky** (rémanence) pour que le délai de démarrage fonctionne. Sans la commande **hardware-bypass boot-delay**, le contournement matériel risque de devenir inactif avant la fin du démarrage du module ASA FirePOWER. Ce scénario peut entraîner l'abandon du trafic si vous avez configuré le module en cas de non-conformité, par exemple.

Étape 4 Désactivez la gestion aléatoire de la séquence TCP. Cet exemple montre comment désactiver la répartition aléatoire pour tout le trafic en ajoutant le paramètre à la configuration par défaut.

policy-map global_policy

class sfrclass

set connection random-sequence-number disable

Si vous décidez de le réactiver ultérieurement, remplacez « disable » par **enable**.

Étape 5 Établissez les alimentations doubles comme configuration attendue :

power-supply dual

Étape 6 Enregistrez la configuration.

write memory

Le comportement du contournement matériel après la mise en ligne du système est déterminé par les paramètres de configuration dans la configuration de démarrage. Vous devez donc enregistrer votre configuration en cours d'exécution.

Modifier les performances et le comportement ASP (Accelerated Security Path)

L'ASP est une couche d'implémentation qui met en œuvre vos politiques et vos configurations. Elle ne présente pas d'intérêt direct, sauf lors de la résolution de problèmes avec le centre d'assistance technique Cisco. Cependant, il existe certains comportements liés aux performances et à la fiabilité que vous pouvez ajuster.

Choisir un modèle de validation transactionnelle de moteur de règles

Par défaut, lorsque vous modifiez une politique basée sur des règles (comme des critères d'accès), les modifications prennent effet immédiatement. Cependant, cette immédiateté s'accompagne d'une légère perte de performances. Cette perte de performances est plus notable pour les très grandes listes de règles dans un

environnement à haut débit de connexions par seconde, par exemple lorsque vous modifiez une stratégie comportant 25 000 règles alors que l'ASA traite 18 000 connexions par seconde.

Les performances sont affectées, car le moteur de règles compile des règles pour accélérer la recherche de règles. Par défaut, le système recherche également les règles non compilées lors de l'évaluation d'une tentative de connexion afin que de nouvelles règles puissent être appliquée; comme les règles ne sont pas compilées, la recherche prend plus de temps.

Vous pouvez modifier ce comportement pour que le moteur de règles utilise un modèle transactionnel lors de la mise en œuvre des modifications de règles, en continuant à utiliser les anciennes règles jusqu'à ce que les nouvelles règles soient compilées et prêtes à l'emploi. Avec le modèle transactionnel, les performances ne devraient pas baisser pendant la compilation des règles. Le tableau suivant clarifie la différence de comportement.

Modèle	Avant la compilation	Pendant la compilation	Après la compilation
Par défaut	Correspond aux anciennes règles.	Correspondance avec les nouvelles règles. (Le débit de connexions par seconde diminue.)	Correspond aux nouvelles règles.
Transactionnel	Correspond aux anciennes règles.	Correspondance avec les anciennes règles. (Le débit de connexions par seconde n'est pas affecté.)	Correspond aux nouvelles règles.

Un avantage supplémentaire du modèle transactionnel est que, lors du remplacement d'une ACL sur une interface, il n'y a aucun intervalle entre la suppression de l'ancienne ACL et l'application de la nouvelle. Cette fonctionnalité réduit le risque que des connexions acceptables soient abandonnées pendant l'opération.

Avant de commencer

- La validation transactionnelle n'est pas conseillée pour les règles de contrôle d'accès si vous utilisez des objets FQDN pour des noms d'hôte dont la résolution peut changer fréquemment, car la compilation du groupe d'accès pourrait ne jamais aboutir complètement en raison des fluctuations DNS. Si vous souhaitez tout de même utiliser la validation transactionnelle, envisagez d'allonger le délai d'expiration du DNS.
- Si vous activez le modèle transactionnel pour un type de règle, des journaux système marquant le début et la fin de la compilation sont générés. Ces journaux système sont numérotés de 780 001 à 780 004.

Procédure

Activez le modèle de validation transactionnelle pour le moteur de règles :

asp rule-engine transactional-commit *option*

Où les options sont les suivantes :

- **access-group** : critères d'accès appliqués globalement ou aux interfaces.
- **nat** : règles de traduction des adresses réseau.

Exemple :

```
ciscoasa(config)# asp rule-engine transactional-commit access-group
```

Activer l'équilibrage de charges ASP

Le mécanisme d'équilibrage de charges ASP permet d'éviter les problèmes suivants :

- Dépassements causés par des pics de trafic imprévus sur les flux
- Dépassements causés par des flux volumineux surchargeant les anneaux de réception d'interfaces spécifiques
- Dépassements causés par des anneaux de réception d'interfaces relativement surchargés, dans lesquels un seul cœur ne peut pas supporter la charge.

L'équilibrage de charges ASP permet à plusieurs cœurs de travailler simultanément sur les paquets qui ont été reçus d'un seul anneau de réception d'interface. Si le système abandonne des paquets et que la sortie de la commande **show cpu** est bien inférieure à 100 %, cette fonctionnalité peut améliorer votre débit si les paquets appartiennent à de nombreuses connexions non liées.

Remarque L'équilibrage de charges ASP est désactivé sur l'ASA virtuel. Avec l'intégration de DPDK (Dataplane Development Kit) dans le chemin de sécurité accéléré (ASP) de l'ASA virtuel, l'ASA virtuel affiche de meilleures performances avec cette fonctionnalité désactivée.

Procédure

Étape 1 Activez et désactivez la commutation automatique de l'équilibrage de charges ASP :

asp load-balance per-packet auto

Étape 2 Activez manuellement l'équilibrage de charges ASP :

asp load-balance per-packet

L'équilibrage de charges ASP est activé jusqu'à ce que vous le désactiviez manuellement, même si vous avez également activé la commande **auto**.

Étape 3 Désactivez manuellement l'équilibrage de charges ASP :

no asp load-balance per-packet

Cette commande s'applique uniquement si vous avez activé manuellement l'équilibrage de charges ASP. Si vous avez également activé la commande **auto**, le système revient à l'activation ou à la désactivation automatique de l'équilibrage de charges ASP.

Supervision du cache DNS

L'ASA fournit un cache local des renseignements DNS à partir des demandes DNS externes qui sont envoyées pour certaines commandes de VPN et de certificat SSL VPN sans client. Chaque demande de traduction DNS est d'abord recherchée dans le cache local. Si la mémoire cache locale contient les informations, l'adresse IP qui en résulte est renvoyée. Si la mémoire cache locale ne peut pas résoudre la demande, une requête DNS est envoyée aux différents serveurs DNS qui ont été configurés. Si un serveur DNS externe résout la demande, l'adresse IP qui en résulte est stockée dans la mémoire cache locale avec son nom d'hôte correspondant.

Consultez la commande suivante pour superviser le cache DNS :

- **show dns-hosts**

  Cette commande affiche le cache DNS, qui comprend les entrées apprises dynamiquement à partir d'un serveur DNS ainsi que le nom et les adresses IP saisis manuellement à l'aide de la commande name.

Historique des paramètres de base

Nom de la caractéristique	Versions de plateforme	Description
Plusieurs groupes de serveurs DNS	9.18(1)	Vous pouvez désormais utiliser plusieurs groupes de serveurs DNS : un groupe est le groupe par défaut, tandis que les autres groupes peuvent être associés à des domaines spécifiques. Une requête DNS qui correspond à un domaine associé à un groupe de serveurs DNS utilisera ce groupe. Par exemple, si vous souhaitez que le trafic destiné aux serveurs internes eng.cisco.com utilise un serveur DNS interne, vous pouvez mapper eng.cisco.com à un groupe DNS interne. Toutes les requêtes DNS qui ne correspondent pas à un mappage de domaine utiliseront le groupe de serveurs DNS par défaut, qui n'a pas de domaine associé. Par exemple, le groupe DefaultDNS peut inclure un serveur DNS public disponible sur l'interface externe. Commandes nouvelles/modifiées : **dns-group-map**, **dns-to-domain**
Serveurs DNS de confiance pour la résolution du domaine d'objet de service réseau.	9.17(1)	Vous pouvez spécifier les serveurs DNS auxquels le système doit faire confiance lors de la résolution des noms de domaine dans les objets de service de réseau. Cette fonctionnalité garantit que toutes les résolutions de noms de domaine DNS acquièrent des adresses IP auprès de sources de confiance. Commandes nouvelles/modifiées : **dns trusted-source**, **show dns trusted-source**
Modification du comportement de la TTL de l'entrée DNS	9.17(1)	Auparavant, la valeur configurée était ajoutée à la TTL existante de chaque entrée (la valeur par défaut était de 1 minute). Désormais, si le délai d'expiration est plus long que la TTL de l'entrée, cette dernière est augmentée jusqu'à la valeur du délai d'expiration de l'entrée. Si la TTL est plus longue que le délai d'expiration, la valeur du délai d'expiration est ignorée; dans ce cas, aucun délai supplémentaire n'est ajouté à la TTL. Commandes nouvelles ou modifiées : **expire-entry-timer minutes**

Nom de la caractéristique	Versions de plateforme	Description
Exigences relatives à l'utilisateur local et au mot de passe d'activation	9.17(1)	Pour les utilisateurs locaux et le mot de passe d'activation, les exigences de mot de passe suivantes ont été ajoutées : • Longueur du mot de passe : au moins 8 caractères. Auparavant, le minimum était de 3 caractères. • Caractères répétitifs et séquentiels : trois caractères ASCII ou plus consécutifs ne sont pas autorisés. Par exemple, les mots de passe suivants seront refusés : • **abc**utilisateur1 • utilisateur**543** • utilisateur**aaaa** • utilisateur2**666** Commandes nouvelles/modifiées : **enable password**, **username**
Prise en charge NTPv4	9.14(1)	L'ASA prend désormais en charge NTPv4. Aucune commande modifiée.
Algorithmes d'authentification NTP supplémentaires	9.13(1)	Auparavant, seul MD5 était pris en charge pour l'authentification NTP. L'ASA prend désormais en charge les algorithmes suivants : • MD5 • SHA-1 • SHA-256 • SHA-512 • AES-CMAC Commandes nouvelles ou modifiées : **ntp authentication-key**
Prise en charge de NTP sur IPv6	9.12(1)	Vous pouvez maintenant spécifier une adresse IPv6 pour le serveur NTP. Commandes nouvelles ou modifiées : **ntp server**

Nom de la caractéristique	Versions de plateforme	Description
Le changement de mot de passe **enable** est maintenant requis lors de la connexion	9.12(1)	Le mot de passe par défaut **enable** est vide. Lorsque vous essayez d'accéder en mode d'exécution privilégié sur l'ASA, vous devez désormais modifier le mot de passe pour une valeur de 3 à 127 caractères. Vous ne pouvez pas le garder vide. La commande **no enable password** n'est plus prise en charge. Au niveau de l'interface de ligne de commande, vous pouvez accéder au mode d'exécution privilégié à l'aide des commandes **enable**, **login** (avec un utilisateur de niveau de privilège 2+), ou d'une session SSH ou Telnet lorsque vous activez **aaa authorization exec auto-enable**. Toutes ces méthodes nécessitent que vous définissiez le mot de passe d'activation. Cette exigence de changement de mot de passe n'est pas appliquée pour les connexions ASDM. Dans ASDM, par défaut, vous pouvez vous connecter sans nom d'utilisateur et avec le mot de passe **enable**. Commandes nouvelles ou modifiées : **enable password**
L'équilibrage de charges ASP est désactivé sur l'ASA virtuel	9.10(1)	Avec la récente intégration de DPDK (Dataplane Development Kit) dans le chemin de sécurité accéléré (ASP) de l'ASA virtuel, l'ASA virtuel affiche de meilleures performances avec cette fonctionnalité désactivée.
L'équilibrage automatique de la charge ASP est désormais pris en charge pour l'ASA virtuel.	9.8(1)	Auparavant, vous pouviez uniquement activer et désactiver manuellement l'équilibrage de charges ASP. Nous avons modifié la commande suivante : **asp load-balance per-packet auto**
Hachage PBKDF2 pour tous les mots de passe locaux **username** et **enable**	9.7(1)	Les mots de passe locaux **username** et **enable** de toutes les longueurs sont stockés dans la configuration à l'aide du hachage PBKDF2 (Password-Based Key Derivation Function 2) à l'aide de SHA-512. Auparavant, les mots de passe de 32 caractères et moins utilisaient la méthode de hachage basée sur MD5. Les mots de passe existants continuent d'utiliser le hachage basé sur MD5, sauf si vous entrez un nouveau mot de passe. Consultez le chapitre « Logiciels et configurations » du Guide de configuration des opérations générales pour connaître les lignes directrices relatives à la rétrogradation. Nous avons modifié les commandes suivantes : **enable, username**
Prise en charge des alimentations doubles pour l'ISA 3000	9.6(1)	Pour les alimentations doubles dans l'ISA 3000, vous pouvez établir des alimentations doubles comme la configuration attendue dans le système d'exploitation ASA. En cas de défaillance d'une alimentation, l'ASA émet une alarme. Par défaut, l'ASA s'attend à une seule alimentation et n'émettra pas d'alarme tant qu'il dispose d'une alimentation opérationnelle. Nous avons introduit la commande suivante : **power-supply dual**
Prise en charge de mots de passe plus longs pour les mots de passe locaux **username** et **enable** (jusqu'à 127 caractères)	9.6(1)	Vous pouvez désormais créer des mots de passe **username** et **enable** locaux jusqu'à 127 caractères (l'ancienne limite était de 32). Lorsque vous créez un mot de passe de plus de 32 caractères, il est stocké dans la configuration à l'aide d'un hachage PBCDF2 (Password-Based Key Derivation Function 2). Les mots de passe plus courts continuent d'utiliser la méthode de hachage basée sur MD5. Nous avons modifié les commandes suivantes : **enable, username**

Nom de la caractéristique	Versions de plateforme	Description
contournement matériel ISA 3000	9.4(1.225)	L'ISA 3000 prend en charge une fonction de contournement matériel pour permettre au trafic de continuer à circuler dans l'appareil en cas de perte d'alimentation. Nous avons introduit les commandes suivantes : **hardware-bypass, hardware-bypass manual, hardware-bypass boot-delay, show hardware-bypass** *Cette fonctionnalité n'est pas disponible dans la version 9.5(1).*
Équilibrage de charges ASP automatique	9.3(2)	Vous pouvez maintenant activer le basculement automatique vers la fonction d'équilibrage de charges ASP. **Remarque** La fonction automatique n'est pas prise en charge sur l'ASA virtuel; seules l'activation et la désactivation manuelles sont prises en charge. Nous avons introduit la commande suivante : **asp load-balance per-packet auto**.
Suppression du mot de passe Telnet par défaut	9.0(2)/9.1(2)	Pour améliorer la sécurité de l'accès de gestion à l'ASA, le mot de passe de connexion par défaut pour Telnet a été supprimé; vous devez définir manuellement le mot de passe avant de pouvoir vous connecter en utilisant Telnet. **Remarque** Le mot de passe de connexion n'est utilisé pour Telnet que si vous ne configurez pas l'authentification de l'utilisateur Telnet (la commande **aaa authentication telnet console**). Auparavant, lorsque vous effaciez le mot de passe, l'ASA rétablissait le mot de passe par défaut « cisco ». Maintenant, lorsque vous effacez le mot de passe, le mot de passe est supprimé. Le mot de passe de connexion est également utilisé pour les sessions Telnet, du commutateur à l'ASASM (voir la commande **session**). Pour l'accès initial à l'ASASM, vous devez utiliser la commande **service-module session**, jusqu'à ce que vous définissiez un mot de passe de connexion. Nous avons modifié la commande suivante : **password**
Visibilité du chiffrement des mots de passe	v 8.4(1)	Nous avons modifié la commande **show password encryption**.
Phrase secrète principale	8.3(1)	Nous avons introduit cette fonctionnalité. La phrase secrète principale vous permet de stocker en toute sécurité les mots de passe en texte brut dans un format chiffré et fournit une clé utilisée pour chiffrer ou masquer tous les mots de passe de manière universelle, sans modifier aucune fonctionnalité. Nous avons introduit les commandes suivantes : **key config-key password-encryption**, **password encryption aes**, **clear configure password encryption aes**, **show running-config password encryption aes, show password encryption**

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.