

# 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, à la page 1
- Régler la date et l'heure, à la page 3
- Configurer la phrase secrète principale, à la page 7
- Configurer des serveurs DNS, à la page 10
- Configurer le contournement matériel et l'alimentation double (Cisco ISA 3000), à la page 13
- Modifier les performances et le comportement ASP (Accelerated Security Path), à la page 15
- Supervision du cache DNS, à la page 17
- Historique des paramètres de base, à la page 18


# 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, dans le volet **Configuration > Device List**, double-cliquez sur le nom du contexte sous l'adresse IP de l'appareil actif.

### Procédure

**Étape 1** Choisissez **Configuration** > **Device Setup** > **Device Name/Password**.

**Étape 2** Entrez le nom d'hôte. Le nom d'hôte par défaut est « ciscoasa ».

Le nom d'hôte apparaît dans l'invite de ligne de commande, et si vous établissez des sessions avec plusieurs appareils, celui-ci facilite le suivi de l'emplacement où vous entrez des commandes. Le nom d'hôte est également utilisé dans les messages syslog.

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. Il peut être utilisé pour une bannière.

**Étape 3** Entrez le nom de domaine. Le nom de domaine par défaut est default.domain.invalid.

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 4** Changez le mot de passe (d'activation) du mode privilégié. 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** dans l'interface de ligne de commande.

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. Contrairement à l'accès par l'interface de ligne de commande, ASDM n'oblige pas à modifier le mot de passe d'activation.

a) Cochez la case **Change the private mode password** pour modifier le mot de passe du mode privilégié.
b) Entrez puis entrez le nouveau mot de passe et confirmez-le. Définissez un mot de passe sensible à la casse 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**

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

**Étape 5** 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.

a) Cochez la case **Change the password to access the console of the security appliance** pour changer le mot de passe pour accéder à la console de l'appareil de sécurité.
b) Entrez l'ancien mot de passe (pour un nouvel ASA, laissez ce champ vide), puis entrez le nouveau mot de passe et confirmez-le. Le mot de passe peut comporter jusqu'à 16 caractères. Il peut s'agir de n'importe quelle combinaison de caractères imprimables ASCII (codes 32 à 126), à l'exception des espaces et du point d'interrogation.

**Étape 6** Cliquez sur **Apply** pour enregistrer vos modifications.

# 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 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.

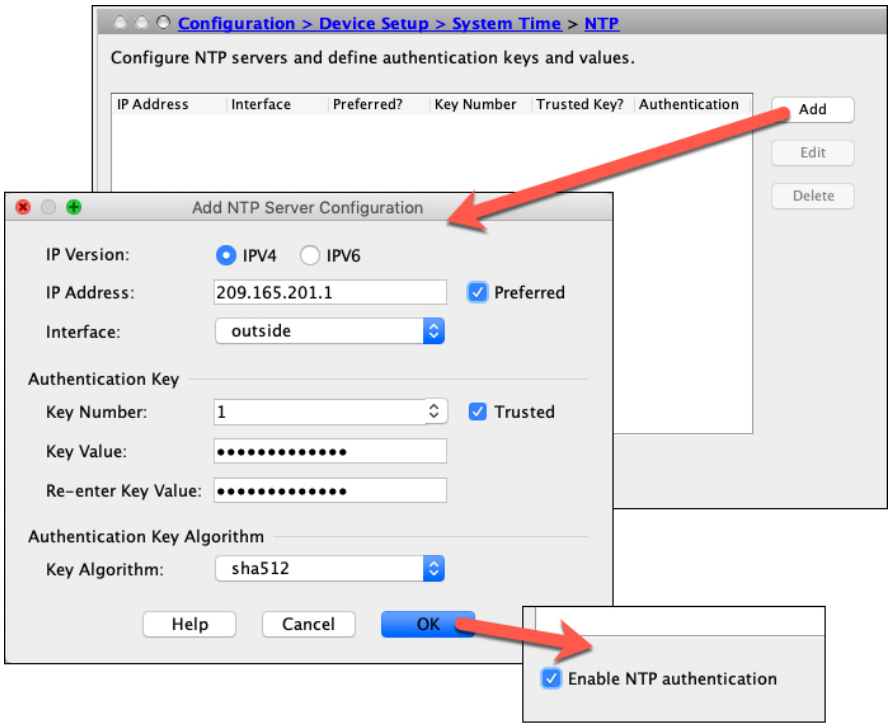
L'ASA prend en charge NTPv4.

### Avant de commencer

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

### Procédure

**Étape 1** Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **System Time (Heure du système)** > **NTP**.




**Étape 2** Cliquez sur **Add** (Ajouter) pour afficher la boîte de dialogue **Add NTP Server Configuration** (Ajouter une configuration de serveur NTP).

**Étape 3** Saisissez l'**IPv4** ou **IPv6 IP Address** (Adresse IP IPv4 ou IPv6) du serveur NTP.

Vous ne pouvez pas saisir de nom d'hôte pour le serveur; l'ASA ne prend pas en charge la recherche DNS pour le serveur NTP.

**Étape 4** (Facultatif) Cochez la case **Preferred** (Préféré) pour définir ce serveur comme serveur préféré.

Le NTP utilise un algorithme pour déterminer quel serveur est le plus précis et se synchronise avec lui. Si les serveurs ont la même précision, le serveur préféré est utilisé. Cependant, si un serveur est nettement plus précis que le serveur préféré, l'ASA utilise le plus précis.

**Étape 5** (Facultatif) Choisissez **l'interface** dans la liste déroulante.

Ce paramètre spécifie l'interface sortante pour les paquets NTP. Si l'interface est vide, l'ASA utilise l'interface de contexte d'administration par défaut conformément à la table de routage de gestion.

**Étape 6** (Facultatif) Configurez l'authentification NTP

a) Saisissez un **Key Number** (Numéro de clé) compris entre 1 et 4294967295, ou choisissez un numéro de clé existant dans la liste déroulante si vous avez précédemment créé une clé pour un autre serveur NTP que vous souhaitez réutiliser.

Ce paramètre spécifie l'ID de clé pour cette clé d'authentification, qui vous permet d'utiliser l'authentification pour communiquer avec le serveur NTP. Les paquets du serveur NTP doivent également utiliser cet ID de clé.

b) Cochez la case **Trusted** (Approuvé).

c) Saisissez la **Key Value** (Valeur de clé), qui est une chaîne de 32 caractères maximum, puis saisissez à nouveau la valeur de clé.

d) Sélectionnez un **Key Algorithm** (Algorithme de clé) dans la liste déroulante.
e) Cliquez sur **OK**.

**Étape 7** Cochez la case **Enable NTP authentication** (Activer l'authentification NTP) pour activer l'authentification NTP.

**Étape 8** Cliquez sur **Apply** pour enregistrer vos modifications.

# 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

**Étape 1** Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **System Time (Heure du système)** > **Clock (Horloge)**.

**Étape 2** Choisissez le fuseau horaire dans la liste déroulante. Ce paramètre spécifie le fuseau horaire comme GMT plus ou moins le nombre d'heures approprié. Si vous sélectionnez le fuseau horaire de l'Est, de l'Heure Centrale, de l'Heure de montage ou de l'Heure du Pacifique, l'heure s'ajuste automatiquement pour l'heure avancée, de 2 h le deuxième dimanche de mars à 2 h le premier dimanche de novembre.

**Remarque** La modification du fuseau horaire de l'ASA peut interrompre la connexion aux SSM intelligents.

**Étape 3** Cliquez sur la liste déroulante **Date** pour afficher un calendrier. Trouvez ensuite la bonne date en utilisant les méthodes suivantes :

- Cliquez sur le nom du mois pour afficher une liste des mois, puis cliquez sur le mois souhaité. Le calendrier se met à jour pour ce mois.
- Cliquez sur l'année pour changer d'année. Utilisez les flèches vers le haut et le bas pour faire défiler les années ou saisissez une année dans le champ de saisie.
- Cliquez sur les flèches vers la droite et la gauche du mois et de l'année pour faire défiler le calendrier vers l'avant et l'arrière d'un mois à la fois.
- Cliquez sur un jour du calendrier pour définir la date.

**Étape 4** Saisissez la durée manuellement en heures, en minutes et en secondes.

**Étape 5** Cliquez sur **Update Display Time** (Mettre à jour l'heure d'affichage) pour mettre à jour l'heure affichée dans le coin inférieur droit du volet ASDM. L'heure actuelle est mise à jour automatiquement toutes les dix secondes.

# 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** Sélectionnez **Configuration** > **Device Management (Gestion des périphériques)** > **PTP**.

**Étape 2** Renseignez le champ **Domain value** (Valeur du domaine).

Il s'agit du numéro de domaine pour 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 3** (Facultatif) Sélectionnez **Enable End-to-End Transparent Clock Mode** (Activer le mode d'horloge transparent de bout en bout) pour activer le mode transparent de bout en bout sur toutes les interfaces compatibles avec PTP.

Une horloge transparente est une horloge qui compense ses retards en mesurant les temps de résidence et en mettant à jour le champ `correctionField` dans le paquet PTP.

**Étape 4** Activez PTP sur une ou plusieurs interfaces de périphérique en sélectionnant une interface et en cliquant sur **Enable** (Activer) ou **Disable** (Désactiver).

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

**Étape 5** Cliquez sur **Apply** (Appliquer).

### Prochaine étape

Vous pouvez sélectionner **Monitoring (Supervision)** > **Properties (Propriétés)** > **PTP** pour afficher les renseignements relatifs à l'horloge PTP et à l'interface/au port.

# 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.

  Choisissez **Configuration > Device Management (Gestion des périphériques) > High Availability (Haute disponibilité) > Failover (Basculement)**, saisissez un caractère dans le champ **Shared Key** (Clé partagée) ou 32 chiffres hexadécimaux (0-9A-Fa-f) si une clé hexadécimale de basculement est sélectionnée, à l'exception de la touche retour arrière. Cliquez ensuite sur **Apply** (Appliquer).
- 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** Choisissez une des options suivantes :

- En mode de contexte unique, choisissez **Configuration > Device Management (Gestion des périphériques) > Advanced (Avancé) > Master Passphrase (Phrase secrète principale)**.
- En mode de contexte multiple, choisissez **Configuration > Device Management (Gestion des périphériques) > Device Administration (Administration des périphériques) > Master Passphrase (Phrase secrète principale)**.

**Étape 2** Cochez la case **Advanced Encryption Standard (AES) password encryption** (Chiffrement du mot de passe AES (norme de chiffrement avancé)).

Si aucune phrase secrète principale n'est en vigueur, un message d'avertissement s'affiche lorsque vous cliquez sur Apply (Appliquer). Vous pouvez cliquer sur OK ou Cancel (Annuler) pour continuer.

Si vous désactivez ultérieurement le chiffrement des mots de passe, 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** Cochez la case **Change the encryption master passphrase** (Modifier la phrase secrète principale de chiffrement) pour pouvoir saisir et confirmer vos nouvelles phrases secrètes principales. Par défaut, elles sont désactivées.

Votre nouvelle phrase secrète principale doit comporter entre 8 et 128 caractères.

Si vous modifiez une phrase secrète existante, vous devez saisir l'ancienne phrase secrète avant de pouvoir en saisir une nouvelle.

Laissez les champs **New** (Nouveau) et **Confirm Master passphrase** (Confirmer la phrase secrète principale) vides pour supprimer la phrase secrète principale.

**Étape 4** Cliquez sur **Apply** (Appliquer).

# 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.
- 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** Choisissez une des options suivantes :

- En mode de contexte unique, choisissez **Configuration > Device Management (Gestion des périphériques) > Advanced (Avancé) > Master Passphrase (Phrase secrète principale)**.
- En mode de contexte multiple, choisissez **Configuration > Device Management (Gestion des périphériques) > Device Administration (Administration des périphériques) > Master Passphrase (Phrase secrète principale)**.

**Étape 2** Cochez la case **Advanced Encryption Standard (AES) password encryption** (Chiffrement du mot de passe AES (norme de chiffrement avancé)).

Si aucune phrase secrète principale n'est en vigueur, une instruction d'avertissement s'affiche lorsque vous cliquez sur Apply (Appliquer). Cliquez sur OK ou Cancel (Annuler) pour continuer.

**Étape 3** Cochez la case Change the encryption master passphrase (Modifier la phrase secrète principale de chiffrement).

**Étape 4** Saisissez l'ancienne phrase secrète principale dans le champ **Old master passphrase** (Ancienne phrase secrète principale). Vous devez fournir l'ancienne phrase secrète principale pour la désactiver.

**Étape 5** Laissez les champs **New Master passphrase** (Nouvelle phrase secrète principale) et **Confirm Master passphrase** (Confirmer la phrase secrète principale) vides.

**Étape 6** Cliquez sur **Apply** (Appliquer).

# 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.

### 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** Choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **DNS** > **DNS Client (Client DNS)**.

**Étape 2** Choisissez l'une des options suivantes dans la zone **DNS Setup** (Configuration DNS) :

- **Configure one DNS server group** (Configurer un groupe de serveurs DNS) : cette option définit les serveurs du groupe DefaultDNS.

- **Configure multiple DNS server groups** (Configurer plusieurs groupes de serveurs DNS) : avec cette option, vous pouvez configurer le groupe DefaultDNS ainsi que d'autres groupes que vous pouvez associer à des domaines spécifiques et des groupes à utiliser avec les stratégies de groupe SSL VPN d'accès à distance. Même si vous configurez uniquement le groupe DefaultDNS, vous devez sélectionner cette option si vous souhaitez modifier le délai d'expiration et d'autres caractéristiques utilisées avec le groupe.

**Étape 3** Si vous sélectionnez **Configure one DNS server group** (Configurer un groupe de serveurs DNS), configurez les serveurs dans le groupe DefaultDNS.

a) Dans **Primary DNS Server** (Serveur DNS principal), saisissez l'adresse IP du serveur DNS qui doit être utilisé chaque fois qu'il est disponible. Pour ce serveur et chaque serveur secondaire, spécifiez éventuellement le *nom d'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.

b) Cliquez sur **Add** (Ajouter) pour ajouter des serveurs DNS secondaires.

Vous pouvez ajouter jusqu'à six serveurs DNS. L'ASA essaie chaque serveur DNS dans l'ordre jusqu'à ce qu'il reçoive une réponse. Utilisez les boutons **Move Up** (Déplacer vers le haut)/**Move Down** (Déplacer vers le bas) pour classer les serveurs par ordre de priorité.

c) Saisissez un nom de domaine DNS ajouté au nom d'hôte s'il n'est pas entièrement qualifié.

**Étape 4** Si vous sélectionnez **Configure multiple DNS server groups** (Configurer plusieurs groupes de serveurs DNS), définissez les propriétés du groupe de serveurs.

a) Cliquez sur **Add** (Ajouter) pour créer un nouveau groupe, ou sélectionnez un groupe et cliquez sur **Edit** (Modifier).

Le groupe DefaultDNS est toujours répertorié.

b) Configurez les propriétés du groupe.

- **Server IP Address to Add**, **Source Interface** (Adresse IP du serveur à ajouter, interface source) : saisissez l'adresse IP d'un serveur DNS et cliquez sur **Add>>** (Ajouter>>). Pour chaque serveur, spécifiez éventuellement le *nom d'interface* par lequel l'ASA communique avec le serveur. Si vous ne spécifiez pas d'interface, l'ASA vérifie la table de routage de gestion uniquement; s'il n'y a aucune correspondance, il vérifie la table de routage des données.

  Vous pouvez ajouter jusqu'à six serveurs DNS. L'ASA essaie chaque serveur DNS dans l'ordre jusqu'à ce qu'il reçoive une réponse. Utilisez les boutons **Move Up** (Déplacer vers le haut)/**Move Down** (Déplacer vers le bas) pour classer les serveurs par ordre de priorité.

- **Timeout** (Délai d'attente) : 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** (Nouvelles tentatives) : 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** (Délai d'expiration de l'entrée) (DefaultDNS ou groupe actif uniquement) : 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** (Délai d'interrogation) (DefaultDNS ou groupe actif uniquement) : 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.
- **Domain Name** (Nom de domaine) (DefaultDNS ou groupe actif uniquement) : le nom de domaine ajouté au nom d'hôte s'il n'est pas entièrement qualifié.

c) Cliquez sur **OK**.

d) Si vous avez plusieurs groupes, vous pouvez modifier le groupe par défaut en le sélectionnant et en cliquant sur **Set Active** (Activer).

Vous ne pouvez utiliser un groupe comme valeur par défaut que s'il n'y a aucun domaine mappé à celui-ci (voir Étape 8, à la page 13).

**Étape 5** Assurez-vous que la recherche DNS est activée sur au moins une interface. Dans la liste d'interfaces **DNS Lookup** (Recherche DNS), sous le tableau des groupes de serveurs DNS, cliquez dans la colonne **DNS Enabled** (DNS activé) et sélectionnez **True** (Vrai) pour activer la recherche sur l'interface.

Assurez-vous d'activer la recherche DNS sur toutes les interfaces qui seront utilisées pour accéder aux serveurs DNS.

Si vous n'activez pas la recherche DNS sur une interface, la **Source Interface** (Interface source) du serveur DNS ou l'interface trouvée à l'aide de la table de routage ne peut pas être utilisée.

**Étape 6** (Facultatif) Sous **Trusted DNS Server** (Serveur DNS de confiance), configurez les options pour déterminer les serveurs de confiance lors de la résolution des noms de domaine dans les objets de service réseau.

a) (Facultatif) Ajoutez ou supprimez des serveurs DNS de confiance configurés de manière explicite.

- Cliquez sur **Add** (Ajouter) pour ajouter un nouveau serveur, sélectionnez le type d'adresse IP (IPv4 ou IPv6), saisissez l'adresse IP du serveur et cliquez sur **OK**.
- Sélectionnez un serveur et cliquez sur **Edit** (Modifier) pour modifier l'adresse.
- Sélectionnez un serveur et cliquez sur **Delete** (Supprimer) pour le supprimer de la liste des serveurs de confiance.

b) Sélectionnez ou désélectionnez les options suivantes :

- **Any** (Tous) : faites confiance à tous les serveurs DNS, surveillez-les tous. Cette option est désactivée par défaut.
- **Configured-Servers** (Serveurs configurés) : indique si les serveurs configurés dans les groupes de serveurs DNS doivent être considérés comme fiables. Par défaut, cette option est activée.

- **DHCP-Client** (Client DHCP) : indique si les serveurs identifiés par la surveillance des messages entre un client DHCP et un serveur DHCP sont considérés comme des serveurs DNS de confiance. Par défaut, cette option est activée.
- **DHCP-Pools** (Ensembles DHCP) : indique si les serveurs DNS configurés dans les ensembles DHCP pour les clients qui obtiennent des adresses par l'intermédiaire des serveurs DHCP exécutés sur les interfaces d'appareils doivent être considérés comme fiables. Par défaut, cette option est activée.
- **DHCP-Relay** (Relais DHCP) : indique si les serveurs identifiés par la surveillance des messages de relais DHCP entre un client DHCP et un serveur DHCP sont considérés comme des serveurs DNS de confiance. Par défaut, cette option est activée.

**Étape 7** (Facultatif) Cochez la case **Enable DNS Guard on all interfaces** (Activer la protection DNS sur toutes les interfaces) pour appliquer une réponse DNS par requête.

Vous pouvez également définir la protection DNS lors de la configuration de l'inspection DNS. Pour une interface donnée, le paramètre de protection DNS configuré dans l'inspection DNS a priorité sur ce paramètre global. Par défaut, l'inspection DNS est activée sur toutes les interfaces avec l'option de protection DNS activée.

**Étape 8** (Facultatif) Mappez les domaines à des groupes de serveurs DNS spécifiques.

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).

a) Dans la zone **DNS Group Map** (Carte de groupe DNS), cochez **Enable DNS Group Map** (Activer la carte de groupe DNS).
b) Cliquez sur **Add** (ajouter).

   La boîte de dialogue **Add Domains to DNS Server Group** (Ajouter des domaines au groupe de serveurs DNS) apparaît.

c) Dans la liste déroulante **DNS server group to domain name mapping** (Mappage du groupe de serveurs DNS au nom de domaine), sélectionnez le nom du groupe de serveurs DNS.
d) Dans le champ **Domain Name** (Nom de domaine), saisissez le nom de domaine que vous souhaitez mapper au groupe DNS.
e) Cliquez sur **OK**.
f) Répétez ces étapes pour ajouter d'autres mappages.

**Étape 9** Cliquez sur **Apply** pour enregistrer vos modifications.

# 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** Pour configurer le contournement matériel, sélectionnez **Configuration** > **Device Management (Gestion des périphériques)** > **Hardware Bypass (Contournement matériel)**.

**Étape 2** Configurez le contournement matériel pour qu'il s'active pour chaque paire d'interfaces en cochant la case **Enable Bypass during Power Down** (Activer le contournement pendant une panne de courant).

**Étape 3** (Facultatif) Configurez chaque paire d'interfaces pour qu'elle reste en mode de contournement matériel après le rétablissement du courant et le démarrage du périphérique en cochant la case **Stay in Bypass after Power Up (Rester en contournement après le redémarrage)**.

Lorsque le contournement matériel est désactivé, il y a une brève interruption de la connexion lorsque l'ASA prend en charge les flux. 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 se produit.

**Étape 4** Pour une paire d'interfaces, activez ou désactivez manuellement le contournement matériel en cochant la case **Bypass Immediately** (Contourner immédiatement).

**Étape 5** (Facultatif) Configurez le contournement matériel pour qu'il reste actif jusqu'après le démarrage du module ASA FirePOWER en cochant la case **Stay in Bypass Mode until after the ASA Firepower Module Boots Up** (Rester en mode de contournement jusqu'après le démarrage du module ASA Firepower).

Vous devez activer le contournement matériel sans l'option **Stay in Bypass after Power Up** (Rester en contournement après le redémarrage) pour que le délai de démarrage fonctionne. Sans cette option, 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 6** Cliquez sur **Apply** (Appliquer).

**Étape 7** Désactivez la répartition 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.

a) Choisissez **Configuration** > **Firewall (Pare-feu)** > **Service Policy (Politique de service)**.
b) Sélectionnez la règle **sfrclass** et cliquez sur **Edit** (Modifier).
c) Cliquez sur **Rule Actions** (Actions de règles), puis sur **Connection Settings** (Paramètres de connexion).
d) Décochez la case **Randomize Sequence Number** (Numéro de séquence aléatoire).
e) Cliquez sur **OK**, puis sur **Apply**(appliquer).

**Étape 8** Pour établir les alimentations doubles comme configuration attendue, sélectionnez **Configuration** > **Device Management (Gestion des périphériques)** > **Power Supply (Alimentation)**, cochez la case **Enable Redundant Power Supply** (Activer l'alimentation redondante), puis cliquez sur **Apply** (Appliquer).

Cet écran affiche également les alimentations disponibles.

**Étape 9** Cliquez sur **Save** (Enregistrer).

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.<br>(Le débit de connexions par seconde diminue.) | Correspond aux nouvelles règles. |
| Transactionnel | Correspond aux anciennes règles. | Correspondance avec les anciennes règles.<br>(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

Choisissez **Configuration > Device Management (Gestion des périphériques) > Advanced (Avancé) > Rule Engine (Moteur de règles)** et sélectionnez les options souhaitées :

- **Groupe d'accès** : critères d'accès appliqués globalement ou aux interfaces.
- **NAT** : règles de traduction des adresses réseau.

# 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** Pour activer et désactiver automatiquement l'équilibrage de charges ASP, choisissez **Configuration** > **Device Management (Gestion des périphériques)** > **Advanced (Avancé)** > **ASP Load Balancing (Équilibrage de charges ASP)** et cochez la case **Dynamically enable or disable ASP load balancing based on traffic monitoring** (Activer ou désactiver dynamiquement l'équilibrage de charges ASP en fonction de la supervision du trafic).

**Étape 2** Pour activer ou désactiver manuellement l'équilibrage de charges ASP, cochez ou décochez la case **Enable ASP load balancing** (Activer l'équilibrage de charges ASP).

Lorsque vous activez manuellement l'équilibrage de charges ASP, il est activé jusqu'à ce que vous le désactiviez manuellement, même si l'option Dynamic (Dynamique) est également activée. La désactivation manuelle de l'équilibrage de charges ASP s'applique uniquement si vous avez activé manuellement l'équilibrage de charges ASP. Si vous avez également activé l'option Dynamic (Dynamique), 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.<br><br>Écrans nouveaux ou modifiés : **Configuration** > **Device Management (Gestion des périphériques)** > **DNS** > **DNS Client (Client DNS)** |
| 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.<br><br>Écrans nouveaux ou modifiés : **Configuration** > **Device Management (Gestion des périphériques)** > **DNS** > **DNS Client (Client DNS)** |
| 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.<br><br>Écrans nouveaux ou modifiés : **Configuration** > **Device Management (Gestion des périphériques)** > **DNS** > **DNS Client (Client DNS)** > **Configure multiple DNS server groups (Configurer plusieurs groupes de serveurs DNS)** |

| 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 :<br>• Longueur du mot de passe : au moins 8 caractères. Auparavant, le minimum était de 3 caractères.<br>• Caractères répétitifs et séquentiels : trois caractères ASCII ou plus consécutifs ne sont pas autorisés. Par exemple, les mots de passe suivants seront refusés :<br>• **abc**utilisateur1<br>• utilisateur**543**<br>• utilisateur**aaaa**<br>• utilisateur2**666**<br>Écrans Nouveaux ou modifiés :<br>• **Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **User Accounts (Comptes d'utilisateurs)**<br>• **Configuration** > **Device Setup (Configuration de l'appareil)** > **Device Name/Password (Nom de l'appareil/Mot de passe)** |
| Prise en charge NTPv4 | 9.14(1) | L'ASA prend désormais en charge NTPv4.<br>Aucun écran modifié. |
| 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 :<br>• MD5<br>• SHA-1<br>• SHA-256<br>• SHA-512<br>• AES-CMAC<br>Écrans Nouveaux ou modifiés :<br>**Configuration** > **Device Setup (Configuration de l'appareil)** > **System Time (Heure du système)** > **NTP** > **bouton Add (Ajouter) > boîte de dialogue Add NTP Server Configuration (Ajouter une configuration de serveur NTP) > liste déroulante Key Algorithm (Algorithme de clé)** |

| Nom de la caractéristique | Versions de plateforme | Description |
|---|---|---|
| Prise en charge de NTP sur IPv6 | 9.12(1) | Vous pouvez maintenant spécifier une adresse IPv6 pour le serveur NTP.<br>Écrans Nouveaux ou modifiés :<br>**Configuration** > **Device Setup (Configuration de l'appareil)** > **System Time (Heure du système)** > **NTP** > **bouton Add (Ajouter) > boîte de dialogue Add NTP Server Configuration (Ajouter une configuration de serveur NTP)** |
| 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.<br>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.<br>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**.<br>Aucun écran modifié. |
| 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.<br>Nous avons modifié l'écran suivant : **Configuration > Device Management (Gestion des périphériques) > Advanced (Avancé) > ASP Load Balancing (Équilibrage de charges ASP)** |
| 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.<br>Nous avons modifié les écrans suivants :<br>**Configuration** > **Device Setup (Configuration de l'appareil)** > **Device Name/Password (Nom de l'appareil/Mot de passe)** > **Enable Password (Mot de passe d'activation)**<br>**Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **User Accounts (Comptes d'utilisateurs)** > **Add/Edit User Account (Ajouter/Modifier un compte d'utilisateur)** > **Identity (Identité)** |

| Nom de la caractéristique | Versions de plateforme | Description |
|---|---|---|
| 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.<br><br>Nous avons introduit l'écran suivant : **Configuration** > **Device Management (Gestion des périphériques)** > **Power Supply (Alimentation)** |
| 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.<br><br>Nous avons modifié les écrans suivants :<br><br>**Configuration** > **Device Setup (Configuration de l'appareil)** > **Device Name/Password (Nom de l'appareil/Mot de passe)** > **Enable Password (Mot de passe d'activation)**<br><br>**Configuration** > **Device Management (Gestion des périphériques)** > **Users/AAA (Utilisateurs/AAA)** > **User Accounts (Comptes d'utilisateurs)** > **Add/Edit User Account (Ajouter/Modifier un compte d'utilisateur)** > **Identity (Identité)** |
| 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.<br><br>Nous avons introduit l'écran suivant : **Configuration** > **Device Management (Gestion des périphériques)** > **Hardware Bypass (Contournement matériel)**<br><br>*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.<br><br>**Remarque**<br>La fonction automatique n'est pas prise en charge sur l'ASA virtuel; seules l'activation et la désactivation manuelles sont prises en charge.<br><br>Nous avons modifié l'écran suivant : **Configuration > Device Management (Gestion des périphériques) > Advanced (Avancé) > ASP Load Balancing (Équilibrage de charges ASP)** |

| Nom de la caractéristique | Versions de plateforme | Description |
|---|---|---|
| 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.<br>**Remarque**<br>Le mot de passe de connexion n'est utilisé pour Telnet que si vous ne configurez pas l'authentification de l'utilisateur Telnet.<br><br>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.<br><br>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.<br><br>Nous n'avons pas modifié d'écrans ASDM. |
| 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.<br><br>Nous avons introduit les écrans suivants :<br><br>**Configuration > Device Management (Gestion des périphériques) > Advanced (Avancé) > Master Passphrase (Phrase secrète principale)**<br><br>**Configuration > Device Management (Gestion des périphériques) > Device Administration (Administration des périphériques) > Master Passphrase (Phrase secrète principale)** |

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.