Planification de votre mise à niveau

Avant de mettre à niveau le Secure Firewall ASA, vous devez effectuer la préparation suivante :

- Vérifiez le chemin de mise à niveau de la version actuelle vers la version cible. Assurez-vous de planifier les versions intermédiaires requises pour chaque système d'exploitation.
- Vérifiez les directives et les limites qui concernent vos versions intermédiaires et cibles, ou qui influent sur la mise à niveau du basculement et de la mise en grappe sans temps d'arrêt.
- Téléchargez tous les paquets de logiciels requis à partir de Cisco.com.
- Sauvegardez vos configurations, surtout en cas de migration de configuration.

Les rubriques suivantes expliquent comment mettre à niveau votre instance d'ASA.

Directives importantes avant d'effectuer une mise à niveau

Vérifiez les directives et les limites de mise à niveau, ainsi que les migrations de configuration pour chaque système d'exploitation.

Lignes directrices pour la mise à niveau de l'ASA

Avant de procéder à une mise à niveau, vérifiez les migrations et toute autre directive.

Directives et migrations propres à la version

Selon votre version actuelle, vous pourriez rencontrer une ou plusieurs migrations de configuration et devrez peut-être tenir compte des directives de configuration pour toutes les versions entre la version de début et la version de fin lorsque vous effectuez une mise à niveau.

Directives sur 9.22

- **Transport par défaut de la licence Smart modifié dans la version 9.22** : dans la version 9.22, le transport par défaut de la licence Smart est passé de Smart Call Home à Smart Transport. Vous pouvez configurer l'ASA pour utiliser Smart Call Home au besoin en utilisant la commande **transport type callhome**. Lorsque vous effectuez une mise à niveau vers la version 9.22, le transport passe automatiquement à Smart Transport. Si vous effectuez une rétrogradation, le transport est rétabli à Smart Call Home, et si vous souhaitez utiliser Smart Transport, vous devez préciser **transport type smart**.

Directives sur 9.20

- **Les commandes de redistribution OSPFv3 qui précisent une carte de routage correspondant à une liste de préfixes seront supprimées dans la version 9.20(2)** : lorsque vous passez à la version 9.20(2), les commandes de **redistribution** OSPFv3 où la **carte de routage** indiquée utilise une **liste de préfixes d'adresse IP correspondante** seront supprimées de la configuration. Bien que les listes de préfixes n'aient jamais été prises en charge, l'analyseur a toujours accepté la commande. Avant la mise à niveau, vous devez reconfigurer OSPFv3 de manière à utiliser les cartes de routage qui précisent une liste de contrôle d'accès dans la commande **match ip address**.

Rappel La redistribution des cartes de routage avec la liste de préfixes IPv4 sur OSPFv2 est prise en charge.

Directives sur 9.19

- **ASDM 7.19(1) requiert la version 8u261 d'Oracle Java ou une version ultérieure.**– Avant de passer à ASDM 7.19, assurez-vous de mettre à jour Oracle Java (si utilisé) à la version 8u261 ou plus récente. Cette version prend en charge TLSv1.3, qui est nécessaire pour mettre à jour le lanceur ASDM. OpenJRE n'est pas concerné.

Directives sur 9.18

- **Prise en charge des images signées ASDM dans la version 9.18(2)/7.18(1.152) et les versions ultérieures** : l'ASA valide maintenant si l'image ASDM est une image signée numériquement par Cisco. Si vous essayez d'exécuter une ancienne image ASDM avec une version ASA intégrant ce correctif, ASDM sera bloqué, et le message « %ERREUR : signature non valide pour le disque de fichier0:/<nom du fichier> » s'affiche sur l'interface de ligne de commande d'ASA. La version 7.18(1.152) d'ASDM et les versions ultérieures sont rétrocompatibles avec toutes les versions d'ASA, même celles ne disposant pas de ce correctif. (CSCwb05291, CSCwb05264)
- **Problème de mise à niveau de la version 9.18(1) si vous avez activé HTTPS/ASDM (avec authentification HTTPS) et SSL sur la même interface avec le même port** : si vous activez à la fois l'accès SSL (**webvpn** > **activer** *l'interface*) et l'accès HTTPS/ASDM (**http**) sur la même interface, vous pouvez accéder à AnyConnect à partir de l'adresse **https://***ip_address* et à ASDM à partir de l'adresse **https://***ip_address***/admin**, tous deux sur le port 443. Cependant, si vous activez également l'authentification HTTPS (**aaa authentication http console**), vous devez définir un port différent pour l'accès ASDM à partir de la version 9.18(1). Assurez-vous de modifier le port avant de procéder à la mise à niveau à l'aide de la commande **http**. (CSCvz92016)
- **Assistant de mise à niveau ASDM** : en raison de la migration de l'API ASD, vous devez utiliser ASDM 7.18 ou une version ultérieure pour effectuer une mise à niveau vers ASA 9.18 ou une version

ultérieure. Comme ASDM est rétrocompatible avec les versions d'ASA antérieures, vous pouvez mettre à niveau ASDM vers la version 7.18 ou une version ultérieure pour n'importe quelle version d'ASA.

Directives sur 9.17

- **Prise en charge des images signées ASDM dans la version 9.17(1.13)/7.18(1.152) et les versions ultérieures** : l'ASA valide maintenant si l'image ASDM est une image signée numériquement par Cisco. Si vous essayez d'exécuter une ancienne image ASDM avec une version ASA intégrant ce correctif, ASDM sera bloqué, et le message « %ERREUR : signature non valide pour le disque de fichier0:/<nom du fichier> » s'affiche sur l'interface de ligne de commande d'ASA. La version 7.18(1.152) d'ASDM et les versions ultérieures sont rétrocompatibles avec toutes les versions d'ASA, même celles ne disposant pas de ce correctif. (CSCwb05291, CSCwb05264)
- **Aucune prise en charge du VPN SSL sans client dans les versions 9.17(1) et les versions ultérieures** : le VPN SSL sans client n'est plus pris en charge.
  - **webvpn** : les sous-commandes suivantes sont supprimées :
    - **apcf**
    - **java-trustpoint**
    - **onscreen-keyboard**
    - **port-forward**
    - **portal-access-rule**
    - **rewrite**
    - **smart-tunnel**
  - **group-policy webvpn** : les sous-commandes suivantes sont supprimées :
    - **port-forward**
    - **smart-tunnel**
    - **ssl-clientless**
- **Assistant de mise à niveau ASDM** : en raison d'un changement interne, à partir de mars 2022, l'assistant de mise à niveau ne fonctionnera plus avec les versions antérieures à ASDM 7.17(1.152). Vous devez procéder à une mise à niveau manuelle vers la version 7.17(1.152) ou une version ultérieure pour utiliser l'assistant.

Directives sur 9.16

- **Prise en charge des images signées ASDM dans la version 9.16(3.19)/7.18(1.152) et les versions ultérieures** : l'ASA valide maintenant si l'image ASDM est une image signée numériquement par Cisco. Si vous essayez d'exécuter une ancienne image ASDM avec une version ASA intégrant ce correctif, ASDM sera bloqué, et le message « %ERREUR : signature non valide pour le disque de fichier0:/<nom du fichier> » s'affiche sur l'interface de ligne de commande d'ASA. La version 7.18(1.152) d'ASDM et les versions ultérieures sont rétrocompatibles avec toutes les versions d'ASA, même celles ne disposant pas de ce correctif. (CSCwb05291, CSCwb05264)

- **Les utilisateurs SNMPv3 utilisant le hachage MD5 et le chiffrement DES ne sont plus pris en charge, et les utilisateurs seront supprimés lors de la mise à niveau vers la version 9.16(1) :** assurez-vous de modifier toute configuration utilisateur pour utiliser des algorithmes de sécurité plus élevés à l'aide de la commande **snmp-server user** avant d'effectuer la mise à niveau.
- **Action de la clé d'hôte SSH requise dans la version 9.16(1)** : en plus de RSA, nous avons ajouté la prise en charge des clés d'hôte EDDSA et ECDSA pour SSH. L'ASA essaie d'utiliser les clés dans l'ordre suivant, si elles existent : EDDSA, ECDSAA, puis RSA. Lorsque vous effectuez une mise à niveau vers la version 9.16(1), l'ASA utilisera la clé RSA existante. Cependant, nous vous recommandons de générer des clés de sécurité élevée dès que possible à l'aide de la commande **crypto key generate** {**eddsa** | **ecdsa**]. De plus, si vous configurez explicitement l'ASA pour utiliser la clé RSA avec la commande **ssh key-exchange hostkey rsa**, vous devez générer une clé de 2 048 bits ou plus. Pour des raisons de compatibilité avec les mises à niveau, l'ASA utilisera des clés hôtes RSA de plus petite taille uniquement lorsque le paramètre par défaut de la clé hôte est utilisé. La prise en charge de RSA sera supprimée dans une version ultérieure.
- **Dans la version 9.16 et les versions ultérieures, les certificats avec des clés RSA ne sont pas compatibles avec les chiffrements ECDSA** : lorsque vous utilisez le groupe de chiffrement ECDHE_ECDSA, configurez le point de confiance avec un certificat qui contient une clé compatible avec ECDSA.
- **ssh version commande supprimée dans la version 9.16(1)** : cette commande a été supprimée. Seule la version 2 du protocole SSH est prise en charge.
- **Lors de la mise à niveau vers la version 9.16 ou une version ultérieure, il se peut que vous voyiez un numéro de série de certificat différent**. Dans la version 9.16, l'ASA a commencé à utiliser OpenSSL, ce qui entraîne un calcul différent des valeurs négatives dans les certificats. Il se peut donc que vous voyiez un numéro de série différent après la mise à niveau. Cette modification n'a pas d'incidence sur le fonctionnement. (CSCvv30338)
- **Fonctionnalité SAMLv1 supprimée dans la version 9.16(1) :** la prise en charge de SAMLv1 a été supprimée.
- **Aucune prise en charge des groupes DH 2, 5 et 24 dans la version 9.16(1)** : la prise en charge a été supprimée pour les groupes DH 2, 5 et 24 dans la configuration des groupes DH SSL. La commande **ssl dh-group** a été mise à jour pour supprimer les options de commande **group2**, **group5** et **group24**.

Directives sur 9.15

- **L'ASA 9.15(1) et les versions ultérieures ne prennent pas en charge les ASA 5525-X, ASA 5545-X et ASA 5555-X.**L'ASA 9.14(x) est la dernière version prise en charge. Pour le module ASA FirePOWER, la dernière version prise en charge est la version 6.6.
- **Cisco annonce l'abandon de la fonctionnalité pour le VPN SSL sans fil avec la version 9.17(1) de l'ASA.**La prise en charge limitée restera valable pour les versions antérieures à la version 9.17(1).
- **Pour le Firepower 1010, la présence d'identifiants de VLAN non valides peuvent causer des problèmes.** Avant d'effectuer une mise à niveau vers la version 9.15(1), assurez-vous de ne pas utiliser de VLAN pour les ports de commutation de la plage de 3968 à 4047. Ces identifiants sont pour un usage interne uniquement, et la version 9.15(1) comprend une vérification pour vous assurer de ne pas utiliser ces identifiants. Par exemple, si ces identifiants sont utilisés après la mise à niveau d'une paire de basculements, la paire de basculements passera à l'état suspendu. Consultez le bogue CSCvw33057 pour en savoir plus.
- **Abandon de la fonctionnalité SAMLv1** : la prise en charge de SAMLv1 est abandonnée.

- **Suppression du chiffrement à faible sécurité dans l'ASA 9.15(1) :** la prise en charge des chiffrements moins sécurisés suivants utilisés par IKE et IPsec a été supprimée :
  - Groupes Diffie-Hellman : 2 et 24.
  - Algorithmes de chiffrement : DES, 3DES, AES-GMAC, AES-GMAC-192, AES-GMAC-256, NULL, ESP-3DES, ESP-DES, ESP-MD5-HMAC
  - Algorithmes de hachage : MD5

Remarque Les chiffrements SSH et SSL de faible sécurité n'ont pas encore été supprimés.

Avant de passer d'une version antérieure de l'ASA à la version 9.15(1), vous devez mettre à jour votre configuration VPN afin d'utiliser les algorithmes de chiffrement pris en charge dans la version 9.15(1), faute de quoi l'ancienne configuration sera rejetée. Lorsque la configuration est rejetée, l'une des actions suivantes se produit, selon la commande :

- La commande utilisera le chiffrement par défaut.
- La commande sera supprimée.

Il est particulièrement important d'appliquer un correctif à votre configuration avant la mise à niveau pour les déploiements de mise en grappe ou de basculement. Par exemple, si l'unité secondaire est mise à niveau vers la version 9.15(1) et que les chiffrements supprimés sont synchronisés avec cette unité à partir de l'unité principale, l'unité secondaire rejettera la configuration. Ce rejet peut entraîner un comportement imprévu, comme l'impossibilité de rejoindre la grappe.

IKEv1 : les sous-commandes suivantes sont supprimées :

- **crypto ikev1 policy** *priority*:
  - **hash md5**
  - **encryption 3des**
  - **encryption des**
  - **group 2**

IKEv2 : les sous-commandes suivantes sont supprimées :

- **crypto ikev2 policy** *priority*:
  - **prf md5**
  - **integrity md5**
  - **group 2**
  - **group 24**
  - **encryption 3des**
  - **encryption des**
  - **encryption null**

IPsec : les sous-commandes suivantes sont supprimées :

- **crypto ipsec ikev1 transform-set *name* esp-3des esp-des esp-md5-hmac**
- **crypto ipsec ikev2 ipsec-proposal *name***
  - **protocol esp integrity md5**
  - **protocol esp encryption 3des aes-gmac aes-gmac- 192 aes-gmac -256 des**
- **crypto ipsec profile *name***
  - **set pfs group2 group24**

Carte de chiffrement : les sous-commandes suivantes sont supprimées :

- **crypto map *name sequence* set pfs group2**
- **crypto map *name sequence* set pfs group24**
- **crypto map *name sequence* set ikev1 phase1-mode aggressive group2**

- **Réintroduction de la configuration du point de distribution CRL** : l'option de configuration de l'URL statique du CDP, qui a été supprimée dans la version 9.13(1), a été réintroduite dans la commande **match-certificate**.
- **Option de restauration des contrôles de validité du certificat de contournement** : l'option de contournement de la vérification de la révocation en raison de problèmes de connectivité avec le serveur CRL ou OCSP a été restaurée.

  Les sous-commandes suivantes ont été restaurées :

  - **revocation-check crl none**
  - **revocation-check ocsp none**
  - **revocation-check crl ocsp none**
  - **revocation-check ocsp crl none**

Directives sur 9.14

- **Prise en charge des images signées ASDM dans la version 9.14(4.14)/7.18(1.152) et les versions ultérieures** : l'ASA valide maintenant si l'image ASDM est une image signée numériquement par Cisco. Si vous essayez d'exécuter une ancienne image ASDM avec une version ASA intégrant ce correctif, ASDM sera bloqué, et le message « %ERREUR : signature non valide pour le disque de fichier0:/<nom du fichier> » s'affiche sur l'interface de ligne de commande d'ASA. La version 7.18(1.152) d'ASDM et les versions ultérieures sont rétrocompatibles avec toutes les versions d'ASA, même celles ne disposant pas de ce correctif. (CSCwb05291, CSCwb05264)
- **Échec de l'assistant de mise à niveau ASDM Cisco.com sur le Firepower 1000 et 2100 en mode appareil** : l'assistant de mise à niveau ASDM Cisco.com ne permet pas d'effectuer de mise à niveau vers la version 9.14 (**Outils > Vérifier la présence de mises à jour ASA/ASDM**). L'assistant peut mettre à niveau ASDM de la version 7.13 à la version 7.14, mais la mise à niveau de l'image ASA est grisée. (CSCvt72183) Comme solution de contournement, utilisez l'une des méthodes suivantes :

  - Utilisez **Outils > Mettre à niveau le logiciel à partir de l'ordinateur local** pour ASA et ASDM. Notez que l'image ASDM (7.14(1)) dans l'ensemble 9.14(1) comporte également le bogue CSCvt72183. Vous devez télécharger la nouvelle image 7.14(1.46) pour assurer le bon fonctionnement de l'assistant.
  - Utilisez **Outils > Vérifier la présence de mises à jour ASA/ASDM** pour procéder à la mise à niveau vers ASDM 7.14 (la version sera 7.14(1.46)). Utilisez ensuite le nouveau ASDM pour mettre à niveau l'image ASA. Notez que l'erreur **Erreur d'installation fatale** pourrait s'afficher. Dans ce cas, cliquez sur **OK**. Il convient alors de définir l'image de démarrage à l'écran **Configuration** > **Device Management** > **System Image/Configuration** > **Boot Image/Configuration** (Configuration, Gestion des appareils, Image/Configuration du système, Image/Configuration de démarrage). Enregistrez la configuration et rechargez l'ASA.

- **Pour les paires de basculements en version 9.14(1) ou toute version ultérieure, l'ASA ne partage plus les données du moteur client SNMP avec son homologue.**
- **Aucune prise en charge dans ASA 9.14(1) ni toute version ultérieure pour les OID cnatAddrBindNumberOfEntries et cnatAddrBindSessionCount (**CSCv22526**)**.
- **Problème de mise à niveau pour les problèmes liés à la version 9.14(4)24 et à RADIUS pour les utilisateurs mobiles AnyConnect** : pour restaurer la fonctionnalité RADIUS, procédez à une mise à niveau vers la version 9.18(4)22 ou une version ultérieure.
- **Mise à niveau du Firepower 2100 en mode plateforme** : lorsque vous effectuez une mise à niveau vers la version 9.14 ou une version ultérieure, si votre EtherChannel (port-canal) a été désactivé au moment de la mise à niveau, vous devrez activer manuellement l'EtherChannel et ses interfaces membres après la mise à niveau.
- **Problème de rétrogradation du Firepower 2100 en mode plateforme à partir de la version 9.13/9.14 à la version 9.12 ou à une version antérieure** : pour un Firepower 2100 disposant d'une nouvelle installation de la version 9.13 ou 9.14 que vous avez convertie en mode plateforme : si vous rétrogradez le périphérique à la version 9.12 ou à une version antérieure, vous ne pourrez pas configurer de nouvelles interfaces ni modifier des interfaces existantes dans FXOS (notez que la version 9.12 et les versions antérieures ne prennent en charge que le mode plateforme). Vous devez soit restaurer votre version à la version 9.13 ou à une version ultérieure, soit effacer votre configuration à l'aide de la commande de configuration d'effacement FXOS. Ce problème ne se produit pas si vous avez initialement effectué une mise à niveau vers la version 9.13 ou 9.14 à partir d'une version antérieure. Seules les nouvelles installations sont concernées, comme un nouveau périphérique ou un périphérique recréé. (CSCvr19755)
- **Le mot clé tls-proxy et la prise en charge de l'inspection chiffrée SCCP/Skinny ont été supprimés** de la commande **inspect skinny**.
- **Assistant de mise à niveau ASDM** : en raison d'une modification interne, l'assistant est uniquement pris en charge par ASDM 7.10(1) ou les versions ultérieures. De plus, en raison d'une modification de nom d'image, vous devez utiliser ASDM 7.12(1) ou une version ultérieure pour effectuer une mise à niveau vers ASA 9.10(1) ou une version ultérieure. Comme ASDM est rétrocompatible avec les versions d'ASA antérieures, vous pouvez mettre à niveau ASDM, quelle que soit la version d'ASA que vous utilisez. Veuillez noter que les ASDM 7.13 et 7.14 ne prenaient pas en charge les ASA 5512-X, 5515-X, 5585-X ou ASASM. Vous devez effectuer une mise à niveau vers ASDM 7.13(1.101) ou 7.14(1.48) pour rétablir la prise en charge d'ASDM.

Directives sur 9.13

- **ASAv nécessite une mémoire de 2 Go dans la version 9.13(1) et les versions ultérieures**. À compter de la version 9.13(1), la mémoire minimale requise pour l'ASAv est de 2 Go. Si votre instance d'ASAv actuelle fonctionne avec moins de 2 Go de mémoire, vous ne pouvez pas effectuer de mise à niveau vers la version 9.13(1) à partir d'une version antérieure. Vous devez régler la taille de la mémoire avant la mise à niveau. Consultez le guide de démarrage pour ASAv pour en savoir plus sur les allocations de ressources (vCPU et mémoire) prises en charge dans la version 9.13(1).
- **Problème de rétrogradation du Firepower 2100 en mode plateforme à partir de la version 9.13 à la version 9.12 ou à une version antérieure** : pour un Firepower 2100 disposant d'une nouvelle installation de la version 9.13 que vous avez convertie en mode plateforme : si vous rétrogradez le périphérique à la version 9.12 ou à une version antérieure, vous ne pourrez pas configurer de nouvelles interfaces ni modifier des interfaces existantes dans FXOS (notez que la version 9.12 et les versions antérieures ne prennent en charge que le mode plateforme). Vous devez soit restaurer votre version à la version 9.13, soit effacer votre configuration à l'aide de la commande de configuration d'effacement FXOS. Ce problème ne se produit pas si vous avez initialement effectué une mise à niveau vers la version 9.13 à partir d'une version antérieure. Seules les nouvelles installations sont concernées, comme un nouveau périphérique ou un périphérique recréé. (CSCvr19755)
- **Modification de la MTU de la liaison de commande de grappe dans la version 9.13(1)** : à partir de la version 9.13(1), de nombreux paquets de contrôle de grappe sont plus volumineux que dans les versions précédentes. La MTU recommandée pour le lien de contrôle de grappe a toujours été de 1 600 ou plus, et cette valeur est appropriée. Cependant, si vous définissez la MTU à 1 600, mais que vous n'avez pas réussi à faire correspondre la MTU aux commutateurs de connexion (par exemple, vous avez laissé la MTU à 1 500 sur le commutateur), vous commencerez à voir les effets de cette incompatibilité avec les paquets de contrôle de grappe abandonnés. Assurez-vous de définir tous les périphériques de la liaison de commande de grappe sur la même MTU, soit 1 600 ou plus.
- **À partir de la version 9.13(1), l'ASA établit une connexion LDAP/SSL uniquement si l'un des critères de certification suivants est satisfait** :
  - Le certificat du serveur LDAP est de confiance (existe dans un point de confiance ou dans le groupe de confiance d'ASA) et est valide.
  - Un certificat d'autorité de certification des serveurs émettant la chaîne est de confiance (existe dans un point de confiance ou dans le groupe de confiance d'ASA), et tous les certificats d'autorité de certification subordonnés de la chaîne sont complets et valides.
- **Le serveur local de l'autorité de certification est supprimé dans la version 9.13(1)** : lorsque l'ASA est configuré en tant que serveur local d'autorité de certification, il est en mesure d'émettre des certificats numériques, de publier des listes de révocation de certificats (CRL) et de révoquer en toute sécurité les certificats émis. Cette fonctionnalité a été abandonnée et, par conséquent, la commande **crypto ca server** a été supprimée.
- **Suppression des commandes des points de distribution de la CRL** : les commandes de configuration d'URL statique du CDP, à savoir **crypto-ca-trustpoint crl** et **crl url**, ont été supprimées avec d'autres logiques connexes. L'URL du CDP a été déplacée pour correspondre à la commande de certificat.

Remarque La configuration de l'URL du CDP a été améliorée pour permettre plusieurs instances du remplacement du CDP pour une seule carte (consultez le bogue CSCvul05216).

- **Option de suppression des contrôles de validité du certificat de contournement** : l'option de contournement de la vérification de la révocation en raison de problèmes de connectivité avec le serveur CRL ou OCSP a été supprimée.

  Les sous-commandes suivantes sont supprimées :

  - **revocation-check crl none**
  - **revocation-check ocsp none**
  - **revocation-check crl ocsp none**
  - **revocation-check ocsp crl none**

  Ainsi, après une mise à niveau, toute commande revocation-check qui n'est plus prise en charge passera au nouveau comportement en ignorant le caractère de fin none.

Remarque Ces commandes ont été restaurées ultérieurement (consultez le bogue CSCtb41710).

- **Abandon du chiffrement à faible sécurité** : plusieurs chiffrements utilisés par les modules ASA IKE, IPsec et SSH sont considérés comme étant non sécurisés et ont donc été abandonnés. Ils seront supprimés dans une version ultérieure.

  IKEv1 : les sous-commandes suivantes sont abandonnées :

  - **crypto ikev1 policy** *priority*:
    - **hash md5**
    - **encryption 3des**
    - **encryption des**
    - **group 2**
    - **group 5**

  IKEv2 : les sous-commandes suivantes sont abandonnées :

  - **crypto ikev2 policy** *priority*
    - **integrity md5**
    - **prf md5**
    - **group 2**
    - **group 5**
    - **group 24**
    - **encryption 3des**
    - **encrypted des** (cette commande est toujours disponible uniquement lorsque vous disposez de la licence de chiffrement DES)

- **encryption null**

IPsec : les commandes suivantes sont abandonnées :

- **crypto ipsec ikev1 transform-set *name* esp-3des esp-des esp-md5-hmac**
- **crypto ipsec ikev2 ipsec-proposal *name***
  - **protocol esp integrity md5**
  - **protocol esp encryption 3des aes-gmac aes-gmac- 192 aes-gmac -256 des**
- **crypto ipsec profile *name***
  - **set pfs group2 group5 group24**

SSH : Les commandes suivantes sont abandonnées :

- **ssh cipher integrity custom hmac-sha1-96:hmac-md5: hmac-md5-96**
- **ssh key-exchange group dh-group1-sha1**

SSL : Les commandes suivantes sont abandonnées :

- **ssl dh-group group2**
- **ssl dh-group group5**
- **ssl dh-group group24**

Carte de chiffrement : les commandes suivantes sont abandonnées :

- **crypto map *name sequence* set pfs group2**
- **crypto map *name sequence* set pfs group5**
- **crypto map *name sequence* set pfs group24**
- **crypto map *name sequence* set ikev1 phase1-mode aggressive group2**
- **crypto map *name sequence* set ikev1 phase1-mode aggressive group5**

- **Dans la version 9.13(1), le groupe Diffie-Hellman 14 est maintenant la valeur par défaut** pour la commande **group** sous **crypto ikev1 policy**, **ssl dh-group** et **crypto ikev2 policy**pour IPsec PFS à l'aide de **crypto map set pfs**, **crypto ipsec profile**, **crypto dynamic-map set pfs** et **crypto map set ikev1 phase1-mode**. L'ancien groupe Diffie-Hellman par défaut était le groupe 2.

  Lors de la mise à niveau à partir d'une version antérieure à la version 9.13(1), si vous devez utiliser l'ancienne valeur par défaut (Groupe Diffie-Hellman 2), vous devez configurer *manuellement* le groupe DH en tant que **groupe 2**, sans quoi vos tunnels passeront par défaut au groupe 14. Comme le groupe 2 sera supprimé dans une version ultérieure, vous devez déplacer vos tunnels dans le groupe 14 dès que possible.

Directives sur 9.12

- **Prise en charge des images signées ASDM dans la version 9.12(4.50)/7.18(1.152) et les versions ultérieures** : l'ASA valide maintenant si l'image ASDM est une image signée numériquement par Cisco.

Si vous essayez d'exécuter une ancienne image ASDM avec une version ASA intégrant ce correctif, ASDM sera bloqué, et le message « %ERREUR : signature non valide pour le disque de fichier0:/<nom du fichier> » s'affiche sur l'interface de ligne de commande d'ASA. La version 7.18(1.152) d'ASDM et les versions ultérieures sont rétrocompatibles avec toutes les versions d'ASA, même celles ne disposant pas de ce correctif. (CSCwb05291, CSCwb05264)

- Assistant de mise à niveau ASDM : en raison d'une modification interne, l'assistant est uniquement pris en charge par ASDM 7.10(1) ou les versions ultérieures. De plus, en raison d'une modification de nom d'image, vous devez utiliser ASDM 7.12(1) ou une version ultérieure pour effectuer une mise à niveau vers ASA 9.10(1) ou une version ultérieure. Comme ASDM est rétrocompatible avec les versions d'ASA antérieures, vous pouvez mettre à niveau ASDM, quelle que soit la version d'ASA que vous utilisez.
- Améliorations de sécurité SSH et nouvelles valeurs par défaut dans la version 9.12(1) : consultez les améliorations de sécurité SSH suivantes :
  - La version 1 du protocole SSH n'est plus prise en charge; seule la version 2 est prise en charge. La commande **ssh version 1** sera migrée vers **ssh version 2**.
  - Prise en charge de l'échange de clés SHA256, groupe Diffie-Hellman 14. Il s'agit désormais du paramètre par défaut (**ssh key-exchange group dh-group14-sha256**). L'ancienne valeur par défaut était le groupe 1 SHA1. Assurez-vous que votre client SSH prend en charge le groupe Diffie-Hellman SHA256 14. Si ce n'est pas le cas, une erreur de ce type pourrait s'afficher :« Impossible de convenir d'un algorithme d'échange de clés ». Par exemple, l'outil OpenSSH prend en charge le groupe Diffie-Hellman 14 SHA256.
  - Prise en charge du chiffrement d'intégrité HMAC-SHA256. La valeur par défaut est désormais l'ensemble de chiffrements à haute sécurité (hmac-sha1 et hmac-sha2-256, comme défini par la commande **ssh cipher integrity high**). L'ancienne valeur par défaut était l'ensemble moyen.
- Le chiffrement NULL-SHA TLSv1 est abandonné et supprimé dans la version 9.12(1) : étant donné que NULL-SHA n'offre pas de chiffrement et n'est plus considéré comme étant sécurisé contre les menaces modernes, il sera supprimé lors du recensement des chiffrements pris en charge pour TLSv1 dans la sortie des commandes/options du mode **tls-proxy** et **show ssl ciphers all**. Les commandes **ssl cipher tlsv1 all** et **ssl cipher tlsv1 custom NULL-SHA** seront également obsolètes et supprimées.
- Le groupe de confiance par défaut est supprimé dans la version 9.12(1) : afin de se conformer à l'exigence de PSB, SEC-AUT-DEFROOT, l'ensemble d'autorités de certification de confiance « par défaut » est supprimé de l'image ASA. Par conséquent, les commandes **crypto ca trustpool import default** et **crypto ca trustpool import clean default** sont également supprimées, ainsi que les autres logiques connexes. Cependant, dans les déploiements existants, les certificats qui ont été précédemment importés à l'aide de ces commandes resteront présents.
- La commande **ssl encryption** est supprimée dans la version 9.12(1) : dans la version 9.3(2), l'abandon de la commande a été annoncé et celle-ci a été remplacée par **ssl cipher**. Dans 9.12(1), **ssl encryption** est supprimé et n'est plus pris en charge.

Directives sur 9.10

- En raison d'une modification interne, l'assistant de mise à niveau ASDM est uniquement pris en charge par ASDM 7.10(1) ou les versions ultérieures. De plus, en raison d'une modification de nom d'image, vous devez utiliser ASDM 7.12(1) ou une version ultérieure pour effectuer une mise à niveau vers ASA 9.10(1) ou une version ultérieure. Comme ASDM est rétrocompatible avec les versions d'ASA antérieures, vous pouvez mettre à niveau ASDM, quelle que soit la version d'ASA que vous utilisez.

Directives sur 9.9

- Problèmes de mémoire ASA 5506-X avec de grandes configurations sur la version 9.9(2) et les versions ultérieures : si vous effectuez une mise à niveau vers la version 9.9(2) ou une version ultérieure, des parties d'une très grande configuration peuvent être rejetées en raison d'une mémoire insuffisante en présentant le message suivant : « ERREUR : mémoire insuffisante pour installer les règles ». Une option consiste à saisir la commande **object-group-search access-control** pour améliorer l'utilisation de la mémoire pour les listes de contrôle d'accès. Cependant, vos performances risquent d'en pâtir. Sinon, vous pouvez rétrograder le périphérique à la version 9.9(1).

Directives sur 9.8

- **Prise en charge des images signées ASDM dans la version 9.8(4.45)/7.18(1.152) et les versions ultérieures** : l'ASA valide maintenant si l'image ASDM est une image signée numériquement par Cisco. Si vous essayez d'exécuter une ancienne image ASDM avec une version ASA intégrant ce correctif, ASDM sera bloqué, et le message « %ERREUR : signature non valide pour le disque de fichier0:/<nom du fichier> » s'affiche sur l'interface de ligne de commande d'ASA. La version 7.18(1.152) d'ASDM et les versions ultérieures sont rétrocompatibles avec toutes les versions d'ASA, même celles ne disposant pas de ce correctif. (CSCwb05291, CSCwb05264)
- Avant la mise à niveau vers la version 9.8(2) ou une version ultérieure, le mode FIPS exige que la clé de basculement comporte au moins 14 caractères. Avant de procéder à la mise à niveau vers la version 9.8(2) ou une version ultérieure en mode FIPS, vous devez modifier le **failover key** ou le **failover ipsec pre-shared-key** pour être à au moins 14 caractères. Si votre clé de basculement est trop courte, lorsque vous mettez à niveau la première unité, la clé de basculement sera rejetée, et les deux unités deviendront actives jusqu'à ce que vous définissiez la clé de basculement à une valeur valide.
- Ne mettez pas à niveau ASAv vers la version 9.8(1) sur Amazon Web Services : en raison du bogue CSCve56153, il est conseillé de ne pas effectuer la mise à niveau vers la version 9.8(1). Après la mise à niveau, l'ASAv devient inaccessible. Passez plutôt à la version 9.8(1.5) ou à une version ultérieure.

Directives sur 9.7

- Problème de mise à niveau de la version 9.7(1) à la version 9.7(1.x) ou tout version ultérieure pour VTI et VXLAN VNI : si vous configurez à la fois Virtual Tunnel Interface (VTI) et des interfaces VNI (Virtual Network Identifier), vous ne pouvez pas effectuer de mise à niveau sans temps d'arrêt pour le basculement. Les connexions sur ces types d'interfaces ne seront pas répliquées sur l'unité de secours tant que les deux unités n'utiliseront pas la même version. (CSCvc83062)

Directives sur 9.6

- (d'ASA 9.6(2) à ASA 9.7(x)) Incidence sur la mise à niveau lors de l'utilisation de l'authentification par clé publique SSH : en raison des mises à jour de l'authentification SSH, une configuration supplémentaire est requise pour activer l'authentification par clé publique SSH; par conséquent, les configurations SSH existantes utilisant l'authentification par clé publique ne fonctionnent plus après la mise à niveau. L'authentification par clé publique est la valeur par défaut pour l'ASAv sur Amazon Web Services (AWS), donc les utilisateurs AWS verront ce problème. Pour éviter la perte de connectivité SSH, vous pouvez mettre à jour votre configuration *avant* d'effectuer la mise à niveau. Vous pouvez également utiliser ASDM après la mise à niveau (si vous avez activé l'accès ASDM) pour corriger la configuration.

Remarque Le comportement d'origine a été restauré dans la version 9.8(1).

Exemple de configuration d'origine pour un nom d'utilisateur « admin » :

```
username admin nopassword privilege 15
username admin attributes
  ssh authentication publickey 55:06:47:eb:13:75:fc:5c:a8:c1:2c:bb:
  07:80:3a:fc:d9:08:a9:1f:34:76:31:ed:ab:bd:3a:9e:03:14:1e:1b hashed
```

Pour utiliser la commande **ssh authentication**, avant d'effectuer la mise à niveau, saisissez les commandes suivantes :

```
aaa authentication ssh console LOCAL
username admin password <password> privilege 15
```

Nous vous recommandons de définir un mot de passe pour le nom d'utilisateur plutôt que de conserver le mot clé **nopassword**, s'il est présent. Le mot clé **nopassword** signifie que *tout* mot de passe peut être saisi, et non qu'*aucun* mot de passe ne peut être saisi. Avant la version 9.6(2), la commande **aaa** n'était pas requise pour l'authentification par clé publique SSH, le mot clé **nopassword** n'était donc pas déclenché. Maintenant que la commande **aaa** est requise, elle permet également l'authentification par mot de passe normale pour un mot clé **username** si le mot clé **password** (ou **nopassword**) est présent.

Après la mise à niveau, la commande **username** ne requiert plus le mot clé **password** ou **nopassword**. Vous pouvez exiger qu'un utilisateur ne puisse pas saisir de mot de passe. Par conséquent, pour forcer l'authentification par clé publique uniquement, saisissez la commande **username** :

```
username admin privilege 15
```

- Incidence sur la mise à niveau lors de la mise à niveau de l'ASA sur le Firepower 9300. En raison de modifications de nom des droits de licence sur le serveur principal, lors de la mise à niveau vers l'ASA 9.6(1)/FXOS 1.1(4), la configuration de démarrage peut ne pas être analysée correctement lors du rechargement initial; la configuration qui correspond aux droits du module complémentaire est alors rejetée.

  Pour un ASA autonome, après le rechargement de l'unité avec la nouvelle version, attendez que tous les droits soient traités et présentent l'état « Autorisé » (**afficher toutes les licences** ou **Surveillance > Propriétés > Licence Smart**), puis rechargez simplement (**recharger** ou **Outils > Rechargement du système**) *sans* enregistrer la configuration. Après le rechargement, la configuration de démarrage sera analysée correctement.

  Pour une paire de basculements, si vous disposez de droits complémentaires, suivez la procédure de mise à niveau dans les notes de mise à jour de FXOS, mais réinitialisez le basculement après avoir rechargé chaque unité (**failover reset** ou **Surveillance > Propriétés > Basculement > État**, **Surveillance > Basculement > Système**, ou **Surveillance > Basculement > Groupe de basculement**, puis cliquez sur **Réinitialiser le basculement**).

  Pour une grappe, suivez la procédure de mise à niveau dans les notes de mise à jour de FXOS; aucune autre action n'est requise.

Directives et migration sur 9.5

- 9.5(2) Nouvelle licence de transporteur : la nouvelle licence de transporteur remplace la licence GTP/GPRS existante et comprend également la prise en charge de l'inspection SCTP et Diameter. Pour le module de sécurité ASA Firepower 9300, la commande **feature mobile-sp** migrera automatiquement vers la commande **feature carrier**.
- 9.5(2) Commandes de mandataire pour courriels abandonnées : dans la version 9.5(2), les commandes de mandataire pour courriels (**imap4s**, **pop3s** et **smtps**) et les sous-commandes ne sont plus prises en charge.
- 9.5(2) Commandes CSD abandonnées ou migrées : dans la version 9.5(2), les commandes CSD (**csd image**, **show webvpn csd image**, **show webvpn csd**, **show webvpn csd hostscan** et **show webvpn csd hostscan image**) ne sont plus prises en charge.

  Les commandes CSD suivantes seront migrées : **csd enable** migre vers **hostscan enable**; **csd hostscan image** migre vers **hostscan image**.
- 9.5(2) Certaines commandes AAA avandonnées : dans la version 9.5(2) de l'ASA, ces commandes et sous-commandes AAA (**override-account-disable** et **authentication crack**) ne sont plus prises en charge.
- 9.5(1) Nous avons abandonné la commande suivante : **timeout gsn**
- Problème de mise à niveau des ASA 5508-X et 5516-X lors de la mise à niveau vers la version 9.5(x) ou une version ultérieure : avant d'effectuer la mise à niveau vers la version ASA 9.5(x) ou une version ultérieure, si vous n'avez jamais activé la réservation de trames étendues, vous devez vérifier l'empreinte mémoire maximale. En raison d'un défaut de fabrication, une limite de mémoire logicielle incorrecte a peut-être été appliquée. Si vous effectuez la mise à niveau vers la version 9.5(x) ou une version ultérieure avant d'appliquer le correctif ci-dessous, votre périphérique plantera au démarrage. Dans ce cas, vous devez rétrograder à la version 9.4 à l'aide de ROMMON (charger une image pour la gamme ASA 5500-X à l'aide de ROMMON), effectuer la procédure ci-dessous, puis effectuer de nouveau la mise à niveau.

  1. Entrez la commande suivante pour vérifier la condition de défaillance :

     ```
     ciscoasa# show memory detail | include Max memory footprint
     Max memory footprint        =    456384512
     Max memory footprint        =            0
     Max memory footprint        =    456384512
     ```

     Si une valeur inférieure à **456 384 512** est renvoyée pour « Empreinte de mémoire maximale », la condition de défaillance est présente, et vous devez effectuer les étapes restantes avant d'effectuer la mise à niveau. Si la mémoire affichée est de 456 384 512 ou plus, vous pouvez ignorer le reste de cette procédure et la mettre à niveau comme d'habitude.

  2. Accédez au mode de configuration globale :

     ```
     ciscoasa# configure terminal
     ciscoasa(config)#
     ```

  3. Activez temporairement la réservation de trames étendues :

     ```
     ciscoasa(config)# jumbo-frame reservation
     WARNING: This command will take effect after the running-config
     is saved and the system has been rebooted. Command accepted.
     ```

```
INFO: Interface MTU should be increased to avoid fragmenting
jumbo frames during transmit
```

Remarque Ne rechargez pas l'ASA.

4. Enregistrez la configuration :

```
ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: b511ec95 6c90cadb aaf6b306 41579572
14437 bytes copied in 1.320 secs (14437 bytes/sec)
[OK]
```

5. Désactivez la réservation de trame étendue :

```
ciscoasa(config)# no jumbo-frame reservation
WARNING: This command will take effect after the running-config is saved and
the system has been rebooted. Command accepted.
```

Remarque Ne rechargez pas l'ASA.

6. Enregistrez de nouveau la configuration :

```
ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: b511ec95 6c90cadb aaf6b306 41579572
14437 bytes copied in 1.320 secs (14437 bytes/sec)
[OK]
```

7. Vous pouvez maintenant effectuer une mise à niveau vers la version 9.5(x) ou une version ultérieure.

Directives et migration sur 9.4

- 9.4(1) Le mandataire du téléphone des communications unifiées et le mandataire du moteur de médias interentreprises sont abandonnés. Dans la version 9.4 de l'ASA, les mandataires du téléphone et le mandataire du moteur de médias interentreprises ne sont plus pris en charge.

Directives et migration sur 9.3

- 9.3(2) Prise en charge de la version 1.2 du protocole Transport Layer Security (TLS) : nous prenons désormais en charge la version 1.2 du protocole TLS pour la transmission sécurisée des messages pour ASDM, Clientless SSVPN et AnyConnect VPN. Nous avons introduit ou modifié les commandes suivantes : ssl client-version, ssl server-version, ssl cipher, ssl trust-point et ssl dh-group. Nous avons abandonné la commande suivante : ssl encryption
- 9.3(1) Suppression de l'authentification de domaine AAA Windows NT : nous avons supprimé la prise en charge de NTLM pour les utilisateurs de VPN d'accès à distance. Nous avons abandonné la commande suivante : aaa-server protocol nt

Directives et migration sur 9.2

Vérification du certificat du serveur de mise à jour automatique

9.2(1) Vérification du certificat du serveur de mise à jour automatique activée par défaut. La vérification du certificat du serveur de mise à jour automatique est maintenant activée par défaut; pour les nouvelles configurations, vous devez explicitement désactiver la vérification de certificat. Si vous effectuez une mise à niveau à partir d'une version antérieure et que vous n'avez pas activé la vérification de certificat, la vérification de certificat n'est pas activée, et l'avertissement suivant s'affiche :

```
AVERTISSEMENT : Le certificat fourni par les serveurs de mise à jour automatique ne sera
pas vérifié. Pour vérifier ce certificat, utilisez l'option avec le certificat de
vérification.
```

La configuration sera migrée vers la configuration explicite sans vérification :

auto-update server no-verification

Incidence sur la mise à niveau pour la connexion à ASDM

Incidence sur la mise à niveau pour la connexion à ASDM lors de la mise à niveau d'une version antérieure à la version 9.2(2.4) à la version 9.2(2.4), ou toute version ultérieure. Si vous effectuez une mise à niveau d'une version antérieure à la version 9.2(2.4) vers la version 9.2(2.4) d'ASA ou une version ultérieure et que vous utilisez l'autorisation de commande et les rôles d'utilisateur définis par ASDM, les utilisateurs avec un accès en lecture seule ne pourront pas se connecter à ASDM. Vous devez modifier la commande **more** avant ou après la mise à niveau pour être au niveau de privilège 5; seuls les utilisateurs de niveau Administrateur peuvent apporter cette modification. Veuillez noter que la version 7.3(2) et les versions ultérieures d'ASDM comprend la commande **more** au niveau 5 pour les rôles d'utilisateur définis, mais les configurations préexistantes doivent être corrigées manuellement.

ASDM :

1. Choisissez **Configuration > Gestion des périphériques > Utilisateurs/AAA > Accès AAA > Autorisation**, puis cliquez sur **Configurer les privilèges de commande**.
2. Sélectionnez **Plus**, puis cliquez sur **Modifier**.

3. Définissez le **niveau de privilège** sur 5 et cliquez sur **OK**.
4. Cliquez sur **OK**, puis sur **Appliquer**.

Interface de ligne de commande :

```
ciscoasa(config)# privilege cmd level 5 mode exec command more
```

Directives et migration sur 9.1

- La MTU maximale est maintenant de 9 198 octets : si votre MTU a été définie à une valeur supérieure à 9 198, la MTU est automatiquement réduite lors de la mise à niveau. Dans certains cas, cette modification de la MTU peut entraîner une non-concordance de la MTU. Assurez-vous de configurer tout équipement de connexion pour utiliser la nouvelle valeur MTU. La MTU maximale que l'ASA peut utiliser est de 9 198 octets (vérifiez la limite exacte de votre modèle à l'aide de l'interface de ligne de commande).

Cette valeur n'inclut pas l'en-tête de couche 2. L'ASA vous a permis de définir une MTU maximale de 65 535 octets, ce qui était inexact et pourrait causer des problèmes.

Directives et migration sur 9.0

- **Migration des listes de contrôle d'accès IPv6** : les listes de contrôle d'accès IPv6 (**ipv6 access-list**) seront migrées vers les listes de contrôle d'accès étendues (**access-list extended**); les listes de contrôle d'accès IPv6 ne sont plus prises en charge.

  Si les listes de contrôle d'accès IPv4 et IPv6 sont appliquées dans la même direction d'une commande d'interface (**access-group**), les listes de contrôle d'accès sont fusionnées :

  - Si les listes de contrôle d'accès IPv4 et IPv6 ne sont utilisées nulle part ailleurs que dans le groupe d'accès, le nom de la liste de contrôle d'accès IPv4 est utilisé pour la liste de contrôle d'accès fusionnée; la liste de contrôle d'accès IPv6 est supprimée.
  - Si au moins une des listes de contrôle d'accès est utilisée dans une autre fonctionnalité, une nouvelle liste de contrôle d'accès est créée avec le nom *IPv4-ACL-name_IPv6-ACL-name*. La ou les listes de contrôle d'accès en cours d'utilisation continuent d'être utilisées pour d'autres fonctionnalités. Les listes de contrôle d'accès qui ne sont pas utilisées sont supprimées. Si la liste de contrôle d'accès IPv6 est utilisée pour une autre fonctionnalité, elle est migrée vers une liste de contrôle d'accès étendue du même nom.

- **Migration du mot clé « tout » de la liste de contrôle d'accès** : maintenant que les listes de contrôle d'accès prennent en charge les protocoles IPv4 et IPv6, le mot clé **any** représente désormais « tout le trafic IPv4 et IPv6 ». Toutes les listes de contrôle d'accès existantes qui utilisent le mot clé **any** seront modifiées pour utiliser le mot clé **any4**, qui désigne « tout le trafic IPv4 ».

  En outre, un mot clé distinct a été introduit pour désigner « tout le trafic IPv6 » : **any6**.

  Les mots clés **any4** et **any6** ne sont pas disponibles pour toutes les commandes qui utilisent le mot clé **any**. Par exemple, la fonctionnalité NAT utilise uniquement le mot clé **any**; le mot clé « tout » représente le trafic IPv4 ou le trafic IPv6 selon le contexte dans la commande NAT en particulier.

- **Exigences en matière de NAT statique avec traduction de port avant la mise à niveau** : dans la version 9.0 et les versions ultérieures, les règles statiques de NAT avec traduction de port limitent l'accès à l'adresse IP de destination pour le port spécifié uniquement. Si vous essayez d'accéder à l'adresse IP de destination sur un port différent non couvert par une règle NAT, la connexion est bloquée. Ce comportement est également valable pour la NAT Twice. De plus, le trafic qui ne correspond pas à l'adresse IP source de la règle NAT Twice sera abandonné s'il correspond à l'adresse IP de destination, quel que soit le port de destination. Par conséquent, avant de procéder à la mise à niveau, vous devez ajouter des règles supplémentaires pour tout autre trafic autorisé vers l'adresse IP de destination.

  Par exemple, la règle NAT Object suivante permet de traduire le trafic HTTP vers le serveur interne entre le port 80 et le port 8080 :

  ```
  object network my-http-server
    host 10.10.10.1
    nat (inside,outside) static 192.168.1.1 80 8080
  ```

  Si vous souhaitez que d'autres services puissent atteindre le serveur, comme FTP, vous devez les autoriser explicitement :

  ```
  object network my-ftp-server
  ```

```
  host 10.10.10.1
  nat (inside,outside) static 192.168.1.1 ftp ftp
```

Ou, pour autoriser le trafic vers d'autres ports du serveur, vous pouvez ajouter une règle NAT statique générale qui correspondra à tous les autres ports :

```
object network my-server-1
  host 10.10.10.1
  nat (inside,outside) static 192.168.1.1
```

Pour la NAT Twice, la règle suivante permet d'autoriser le trafic HTTP de l'adresse 192.168.1.0/24 vers le serveur interne et de le traduire entre le port 80 et le port 8080 :

```
object network my-real-server
  host 10.10.10.1
object network my-mapped-server
  host 192.168.1.1
object network outside-real-hosts
  subnet 192.168.1.0 255.255.255.0
object network outside-mapped-hosts
  subnet 10.10.11.0 255.255.255.0
object service http-real
  service tcp destination eq 80
object service http-mapped
  service tcp destination eq 8080
object service ftp-real
  service tcp destination eq 21
nat (outside,inside) source static outside-real-hosts outside-mapped-hosts destination
 static my-mapped-server my-real-server service http-mapped http-real
```

Si vous souhaitez que les hôtes externes atteignent un autre service sur le serveur interne, ajoutez une autre règle NAT pour le service, par exemple FTP :

```
nat (outside,inside) source static outside-real-hosts outside-mapped-hosts destination
 static my-mapped-server my-real-server ftp-real ftp-real
```

Si vous souhaitez que d'autres adresses sources atteignent le serveur interne sur tous les autres ports, vous pouvez ajouter une autre règle NAT pour cette adresse IP spécifique ou pour n'importe quelle adresse IP source. Assurez-vous que la règle générale est classée après la règle spécifique.

```
nat (outside,inside) source static any any destination static my-mapped-server
my-real-server
```

Directives et migration sur 8.4

- Migration de la configuration pour le mode transparent : dans la version 8.4, toutes les interfaces en mode transparent appartiennent désormais à un groupe de ponts. Lors de la mise à niveau vers la version 8.4, les deux interfaces existantes sont placées dans le groupe de ponts 1, et l'adresse IP de gestion est attribuée à la BVI (Bridge Group Virtual Interface). La fonctionnalité reste la même lors de l'utilisation d'un groupe de ponts. Vous pouvez désormais profiter de la fonctionnalité de groupe de ponts pour configurer jusqu'à quatre interfaces par groupe de ponts et créer jusqu'à huit groupes de ponts en mode unique ou par contexte.

Remarque Remarque : Dans la version 8.3 et les versions antérieures, en tant que configuration non prise en charge, vous pourriez configurer une interface de gestion sans adresse IP et vous pourriez accéder à l'interface en utilisant l'adresse de gestion des périphériques. Dans la version 8.4, l'adresse de gestion des périphériques est attribuée aux BVI, et l'interface de gestion n'est plus accessible en utilisant cette adresse IP; l'interface de gestion nécessite sa propre adresse IP.

- Lors de la mise à niveau vers la version 8.4(2) à partir des versions 8.3(1), 8.3(2) et 8.4(1), toutes les configurations NAT d'identité incluront désormais les mots clés **no-proxy-arp** et **route-lookup** pour maintenir les fonctionnalités existantes. Le mot clé **unidirectional** est supprimé.

Directives et migration sur 8.3

Consultez le guide suivant qui décrit le processus de migration de la configuration lorsque vous passez d'une version antérieure à la version 8.3 du système d'exploitation Cisco ASA 5500 à la version 8.3 :

Migration du Cisco ASA 5500 vers la version 8.3

Directives de mise en grappe

Il n'y a aucune exigence particulière pour les mises à niveau sans temps d'arrêt pour la mise en grappe ASA, avec les exceptions suivantes.

Remarque *Les rétrogradations* sans temps d'arrêt ne sont pas officiellement prises en charge par la mise en grappe.

- Exigences de mise à niveau transparente du basculement et de la mise en grappe du Firepower 4100/9300 pour le déchargement de flux : en raison de corrections de bogues dans la fonction de déchargement de flux, certaines combinaisons de FXOS et d'ASA ne prennent pas en charge le déchargement de flux (consultez le tableau de compatibilité). Le déchargement de flux est désactivé par défaut pour l'ASA. Pour effectuer une mise à niveau transparente du basculement ou de la mise en grappe lors de l'utilisation du déchargement de flux, vous devez suivre les chemins de mise à niveau ci-dessous pour vous assurer d'exécuter toujours une combinaison compatible lors de la mise à niveau vers FXOS 2.3.1.130 ou une version ultérieure :

  1. Mettre à niveau l'ASA vers la version 9.8(3) ou une version ultérieure
  2. Mettre à niveau FXOS vers la version 2.3.1.130 ou une version ultérieure
  3. Mettre à niveau l'ASA vers votre version finale

  Par exemple, vous utilisez FXOS 2.2.2.26/ASA 9.8(1) et vous souhaitez effectuer une mise à niveau vers FXOS 2.6.1/ASA 9.12(1), vous pouvez :

  1. Mettre à niveau l'ASA vers la version 9.8(4)
  2. Mettre à niveau FXOS vers la version 2.6.1
  3. Mettre à niveau l'ASA vers la version 9.12(1)

- Mise à niveau de la grappe Firepower 4100/9300 vers FXOS 2.3/ASA 9.9(2) : les unités de données sur ASA 9.8 ou les versions antérieures ne peuvent pas joindre une grappe dont l'unité de contrôle se trouve sur FXOS 2.3/9.9(2) ou une version ultérieure. Elles rejoindront la grappe après la mise à niveau d'ASA vers la version 9.9(2) ou toute version ultérieure [CSCvi54844].
- VPN de site à site distribué : les sessions VPN de site à site distribuées sur une unité en panne requièrent jusqu'à 30 minutes pour se stabiliser sur les autres unités. Pendant cette période, des défaillances supplémentaires de l'unité peuvent entraîner la perte de sessions. Par conséquent, lors d'une mise à niveau de grappe, pour éviter une perte de trafic, suivez ces étapes. Reportez-vous à la procédure de mise à niveau de grappe FXOS/ASA afin de pouvoir intégrer ces étapes dans votre tâche de mise à niveau.

Remarque La mise à niveau sans temps d'arrêt n'est pas prise en charge avec le VPN de site à site distribué lors de la mise à niveau de la version 9.9(1) à la version 9.9(2) ou à une version ultérieure. Dans la version 9.9(2), en raison des améliorations de la redistribution active des sessions, vous ne pouvez pas exécuter certaines unités sur la version 9.9(2) et d'autres unités sur la version 9.9(1).

1. Sur les châssis *sans* unité de contrôle, désactivez la mise en grappe sur un module à l'aide de la console ASA.

   cluster group *name*

   no enable

   Si vous mettez à niveau FXOS sur le châssis ainsi que sur l'ASA, enregistrez la configuration pour que la mise en grappe soit désactivée après le redémarrage du châssis :

   write memory

2. Attendez que la grappe se stabilise; vérifiez que toutes les sessions de sauvegarde ont bien été créées.

   show cluster vpn-sessiondb summary

3. Répétez les étapes 1 et 2 pour chaque module de ce châssis.
4. Mettez à niveau FXOS sur le châssis à l'aide de l'interface de ligne de commande de FXOS ou de Firepower Chassis Manager.
5. Une fois que le châssis est en ligne, mettez à jour l'image ASA sur chaque module à l'aide de l'interface de ligne de commande de FXOS ou de Firepower Chassis Manager.
6. Une fois que les modules sont en ligne, réactivez la mise en grappe sur chaque module sur la console de l'ASA.

   cluster group *name*

   enable

   write memory

7. Répétez les étapes 1 à 6 sur le deuxième châssis, en veillant à désactiver la mise en grappe sur les unités de données, puis sur l'unité de contrôle.

   Une nouvelle unité de contrôle sera choisie dans le châssis mis à niveau.

8. Une fois que la grappe est stable, redistribuez les sessions actives entre tous les modules de la grappe à l'aide de la console ASA sur l'unité de contrôle.

cluster redistribute vpn-sessiondb

- Problème de mise à niveau pour la version 9.9(1) et les versions ultérieures avec la mise en grappe. La version 9.9(1) et les versions ultérieures comprennent une amélioration de la distribution des sauvegardes. Vous devez effectuer votre mise à niveau vers la version 9.9(1) ou une version ultérieure comme suit pour profiter de la nouvelle méthode de distribution des sauvegardes. Dans le cas contraire, les unités mises à niveau continueront d'utiliser l'ancienne méthode.

  1. Supprimez toutes les unités secondaires de la grappe (pour que celle-ci ne se compose que de l'unité principale).
  2. Mettez à niveau une unité secondaire et réintégrez-la à la grappe.
  3. Désactivez la mise en grappe sur l'unité principale, mettez-la à niveau et réintégrez-la à la grappe.
  4. Mettez à niveau les unités secondaires restantes et joignez-les à la grappe, une à la fois.

- Mise à niveau de la grappe Firepower 4100/9300 vers ASA 9.8(1) ou versions antérieures : lorsque vous désactivez la mise en grappe sur une unité de données (**no enable**), qui fait partie du processus de mise à niveau, le trafic redirigé vers cette unité peut être abandonné pendant trois secondes avant que le trafic soit redirigé vers un nouveau propriétaire [CSCvc85008].

- La mise à niveau sans temps d'arrêt peut ne pas être prise en charge lors de la mise à niveau vers les versions suivantes avec le correctif pour le bogue CSCvb24585. Ce correctif a déplacé l'algorithme 3DES des chiffrements SSL par défaut (moyen) à l'ensemble de chiffrement faible. Si vous définissez un chiffrement personnalisé qui n'inclut plus l'algorithme 3DES, vous risquez d'avoir une incompatibilité si l'autre côté de la connexion utilise les algorithmes de chiffrement par défaut (moyens) qui n'incluent plus l'algorithme 3DES.
  - 9.1(7.12)
  - 9.2(4.18)
  - 9.4(3.12)
  - 9.4(4)
  - 9.5(3.2)
  - 9.6(2.4)
  - 9.6(3)
  - 9.7(1)
  - 9.8(1)

- Problèmes de mise à niveau pour les listes de contrôle d'accès de nom de domaine complet (FQDN) : en raison du bogue CSCv92371, les listes de contrôle d'accès contenant des noms de domaine complets peuvent entraîner une réplication incomplète des listes de contrôle d'accès sur les unités secondaires d'une paire de grappe ou de basculements. Ce bogue est présent dans les versions 9.1(7), 9.5(2), 9.6(1) et certaines versions provisoires. Nous vous suggérons de procéder à la mise à niveau vers une version qui comprend le correctif pour le bogue CSCuy34265 : la version 9.1(7.6) ou une version ultérieure, la version 9.5(3) ou une version ultérieure, la version 9.6(2) ou une version ultérieure. Cependant, en raison de la nature de la réplication de la configuration, la mise à niveau sans temps d'arrêt n'est pas disponible. Consultez le bogue CSCuy34265 pour en savoir plus sur les différentes méthodes de mise à niveau.

- Les grappes Firepower Threat Defense en version 6.1.0 ne prennent pas en charge la mise en grappe intersite (vous pouvez configurer les fonctionnalités intersite à l'aide de FlexConfig à partir de la version 6.2.0). Si vous avez déployé ou redéployé une grappe 6.1.0 dans FXOS 2.1.1 et que vous avez saisi une valeur pour l'ID de site (non pris en charge), vous devez supprimer l'ID de site (le définir sur **0**) sur chaque unité dans FXOS avant de passer à la version 6.2.3. Sinon, les unités ne pourront pas rejoindre la grappe après la mise à niveau. Si vous avez déjà effectué la mise à niveau, modifiez l'ID de site à **0** sur chaque unité pour résoudre le problème. Consultez le guide de configuration de FXOS pour afficher ou modifier l'ID de site
- Mise à niveau vers la version 9.5(2) ou une version ultérieure (CSCuv82933) : avant de mettre à niveau l'unité de contrôle, si vous saisissez **show cluster info**, les unités de données mises à niveau s'affichent comme « DEPUTY_BULK_SYNC ». D'autres états de non-concordance s'affichent également. Vous pouvez ignorer cet affichage; l'état s'affichera correctement lorsque vous mettrez à niveau toutes les unités.
- Mise à niveau à partir de la version 9.0(1) ou de la version 9.1(1) (CSCue72961) : la mise à niveau sans temps d'arrêt n'est pas prise en charge.

Directives en matière de basculement

Il n'y a aucune exigence particulière concernant les mises à niveau sans temps d'arrêt pour le basculement, avec les exceptions suivantes :

- Pour le Firepower 1010, la présence d'identifiants de VLAN non valides peuvent causer des problèmes.Avant d'effectuer une mise à niveau vers la version 9.15(1), assurez-vous de ne pas utiliser de VLAN pour les ports de commutation de la plage de 3968 à 4047. Ces identifiants sont pour un usage interne uniquement, et la version 9.15(1) comprend une vérification pour vous assurer de ne pas utiliser ces identifiants. Par exemple, si ces identifiants sont utilisés après la mise à niveau d'une paire de basculements, la paire de basculements passera à l'état suspendu. Consultez le bogue CSCvw33057 pour en savoir plus.
- Exigences de mise à niveau transparente du basculement et de la mise en grappe du Firepower 4100/9300 pour le déchargement de flux : en raison de corrections de bogues dans la fonction de déchargement de flux, certaines combinaisons de FXOS et d'ASA ne prennent pas en charge le déchargement de flux (consultez le tableau de compatibilité). Le déchargement de flux est désactivé par défaut pour l'ASA. Pour effectuer une mise à niveau transparente du basculement ou de la mise en grappe lors de l'utilisation du déchargement de flux, vous devez suivre les chemins de mise à niveau ci-dessous pour vous assurer d'exécuter toujours une combinaison compatible lors de la mise à niveau vers FXOS 2.3.1.130 ou une version ultérieure :

  1. Mettre à niveau l'ASA vers la version 9.8(3) ou une version ultérieure
  2. Mettre à niveau FXOS vers la version 2.3.1.130 ou une version ultérieure
  3. Mettre à niveau l'ASA vers votre version finale

  Par exemple, vous utilisez FXOS 2.2.2.26/ASA 9.8(1) et vous souhaitez effectuer une mise à niveau vers FXOS 2.6.1/ASA 9.12(1), vous pouvez :

  1. Mettre à niveau l'ASA vers la version 9.8(4)
  2. Mettre à niveau FXOS vers la version 2.6.1
  3. Mettre à niveau l'ASA vers la version 9.12(1)

- Problèmes de mise à niveau avec les versions 8.4(6), 9.0(2) et 9.1(2) : en raison du bogue CSCum88962, vous ne pouvez pas effectuer de mise à niveau sans temps d'arrêt vers les versions 8.4(6), 9.0(2) ou 9.1(3). Vous devriez plutôt passer à la version 8.4(5) ou 9.0(3). Pour mettre à niveau la version 9.1(1), vous ne pouvez pas effectuer de mise à niveau directement vers la version 9.1(3) en raison du bogue CSCuh25271. Il n'y a donc pas de solution de contournement pour une mise à niveau sans temps d'arrêt. Vous devez effectuer la mise à niveau vers la version 9.1(2) avant de procéder à la mise à niveau vers la version 9.1(3) ou toute version ultérieure.
- Problèmes de mise à niveau pour les listes de contrôle d'accès de nom de domaine complet (FQDN) : en raison du bogue CSCv92371, les listes de contrôle d'accès contenant des noms de domaine complets peuvent entraîner une réplication incomplète des listes de contrôle d'accès sur les unités secondaires d'une paire de grappe ou de basculements. Ce bogue est présent dans les versions 9.1(7), 9.5(2), 9.6(1) et certaines versions provisoires. Nous vous suggérons de procéder à la mise à niveau vers une version qui comprend le correctif pour le bogue CSCuy34265 : la version 9.1(7.6) ou une version ultérieure, la version 9.5(3) ou une version ultérieure, la version 9.6(2) ou une version ultérieure. Cependant, en raison de la nature de la réplication de la configuration, la mise à niveau sans temps d'arrêt n'est pas disponible. Consultez le bogue CSCuy34265 pour en savoir plus sur les différentes méthodes de mise à niveau.
- Problème de mise à niveau de la version 9.7(1) à la version 9.7(1.x) ou tout version ultérieure pour VTI et VXLAN VNI : si vous configurez à la fois Virtual Tunnel Interface (VTI) et des interfaces VNI (Virtual Network Identifier), vous ne pouvez pas effectuer de mise à niveau sans temps d'arrêt pour le basculement. Les connexions sur ces types d'interfaces ne seront pas répliquées sur l'unité de secours tant que les deux unités n'utiliseront pas la même version. (CSCvc83062)
- Avant la mise à niveau vers la version 9.8(2) ou une version ultérieure, le mode FIPS exige que la clé de basculement comporte au moins 14 caractères. Avant de procéder à la mise à niveau vers la version 9.8(2) ou une version ultérieure en mode FIPS, vous devez modifier le **failover key** ou le **failover ipsec pre-shared-key** pour être à au moins 14 caractères. Si votre clé de basculement est trop courte, lorsque vous mettez à niveau la première unité, la clé de basculement sera rejetée, et les deux unités deviendront actives jusqu'à ce que vous définissiez la clé de basculement à une valeur valide.
- Problème de mise à niveau avec l'inspection GTP : il pourrait y avoir un temps d'arrêt pendant la mise à niveau, car les structures de données GTP ne sont pas répliquées sur le nouveau nœud.

Directives supplémentaires

- Vulnérabilité de l'intégrité de la personnalisation du portail du VPN SSL sans client Cisco ASA : plusieurs vulnérabilités ont été corrigées pour le VPN SSL sans client dans le logiciel ASA. Vous devez donc mettre à niveau votre logiciel vers une version fixe. Consultez la page http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20141008-asa pour en savoir plus sur la vulnérabilité et obtenir la liste des versions d'ASA corrigées. En outre, si vous avez déjà exécuté une version antérieure d'ASA dont la configuration était vulnérable, quelle que soit la version que vous utilisez actuellement, vous devez vérifier que la personnalisation du portail n'a pas été compromise. Si un agresseur a compromis un objet personnalisé dans le passé, l'objet compromis reste persistant après la mise à niveau de l'ASA vers une version corrigée. La mise à niveau de l'ASA empêche cette vulnérabilité d'être davantage exploitée, mais elle ne modifiera pas les objets de personnalisation qui ont déjà été compromis et qui sont toujours présents sur le système.

Directives de mise à niveau de FXOS

Avant d'effectuer la mise à niveau, lisez les notes de mise à jour pour chaque version de FXOS dans le chemin de mise à niveau de votre choix. Les notes de mise à jour contiennent des renseignements importants sur chaque version FXOS, y compris les nouvelles fonctionnalités et les fonctionnalités modifiées.

La mise à niveau peut nécessiter des modifications de la configuration que vous devez prendre en compte. Par exemple, un nouveau matériel informatique pris en charge dans une version FXOS peut également nécessiter la mise à jour du micrologiciel FXOS.

Les notes de mise à jour de FXOS sont disponibles ici : https://www.cisco.com/c/en/us/support/security/firepower-9000-series/products-release-notes-list.html.

Liste de contrôle pour la mise à niveau d'ASA

Pour planifier votre mise à niveau, utilisez cette liste de contrôle.

1. Modèle d'ASA (Chemin de mise à niveau : Appareils ASA, à la page 45) : _____

   Version actuelle de l'ASA (Chemin de mise à niveau : Appareils ASA, à la page 45) : _____

2. Vérifiez la compatibilité ASA/ASDM par modèle (Compatibilité ASA et ASDM par modèle, à la page 25).

   Version de l'ASA cible : _____

   Version d'ASDM cible : _____

3. Vérifiez le chemin de mise à niveau du Firepower 2100 en mode plateforme (Chemin de mise à niveau : ASA sur Firepower 2100 en mode plateforme, à la page 52). Des versions intermédiaires sont-elles requises? Oui _____ Non _____

   Si tel est le cas, version(s) d'ASA intermédiaire(s) : _____

4. Téléchargez les versions d'ASA/ASDM cibles (Télécharger le logiciel ASA, à la page 61).

Remarque ASDM est inclus dans le paquet d'images pour toutes les plateformes Firepower et Cisco Secure Firewall.

5. Votre modèle ASA est-il un Firepower 4100 ou 9300? Oui _____ Non _____

   En cas de réponse positive :

   1. Version de FXOS actuelle : _____
   2. Vérifiez la compatibilité de ASA/Firepower 4100 et 9300 (Compatibilité du Firepower 4100/9300 avec l'ASA et Défense contre les menaces, à la page 33).

      Version de FXOS cible : _____
   3. Des versions intermédiaires sont-elles requises? Oui _____ Non _____

      Si oui, versions de FXOS intermédiaires : _____

      Assurez-vous de planifier la mise à niveau de l'ASA conformément aux mises à niveau de FXOS pour maintenir leur compatibilité.

Versions ASA intermédiaires requises pour maintenir la compatibilité. pendant la mise à niveau : _____

4. Téléchargez les versions de FXOS cibles et intermédiaires (Télécharger FXOS pour le Firepower 4100/9300, à la page 73).

   Téléchargez les versions d'ASA intermédiaires (Télécharger le logiciel ASA, à la page 61).

5. Utilisez-vous l'application décorateur Radware DefensePro? Oui _____ Non _____

   En cas de réponse positive :

   1. Version actuelle de DefensePro : _____
   2. Vérifiez la compatibilité de ASA/FXOS/DefensePro (Compatibilité avec Radware DefensePro, à la page 40).

      Version de Target DefensePro : _____
   3. Téléchargez la version de DefensePro cible.

6. Consultez les directives de mise à niveau pour chaque système d'exploitation.
   - Lignes directrices pour la mise à niveau de l'ASA, à la page 1.
   - Directives FXOS : consultez les notes de mise à jour FXOS pour chaque version intermédiaire et cible.

7. Sauvegardez vos configurations. Consultez le guide de configuration de chaque système d'exploitation pour connaître les méthodes de sauvegarde.

Compatibilité

Cette section comprend des tableaux indiquant la compatibilité entre les plateformes, les systèmes d'exploitation et les applications.

Compatibilité ASA et ASDM par modèle

Les tableaux suivants répertorient la compatibilité d'ASA et d'ASDM pour les modèles actuels. Pour les anciennes versions et les anciens modèles, consultez Compatibilité de Cisco ASA.

ASA 9.22

Les versions recommandées sont en **gras**.

Remarque

- Les versions d'ASDM sont rétrocompatibles avec toutes les versions d'ASA précédentes, sauf indication contraire. Par exemple, ASDM 7.22(1) peut gérer un ASA 5516-X sur ASA 9.10(1).
- Les nouvelles versions d'ASA requièrent la version d'ASDM de coordination ou une version ultérieure. Vous ne pouvez pas utiliser une ancienne version d'ASDM avec une nouvelle version d'ASA. Par exemple, vous ne pouvez pas utiliser ASDM 7.20 avec ASA 9.22. Pour les versions de maintenance ASA et les versions provisoires, vous pouvez continuer à utiliser la version d'ASDM actuelle, sauf indication contraire. Par exemple, vous pouvez utiliser ASA 9.22(1.2) avec ASDM 7.22(1). Si une version de maintenance ASA comporte de nouvelles fonctionnalités importantes, une nouvelle version d'ASDM sera généralement requise.

Tableau 1 : Compatibilité ASA et ASDM : la version 9.22

ASA	ASDM	Modèle ASA								
		ASA virtuel	Firepower 1010 1010E 1120 Série 1150	Secure Firewall 1210CE 1210CP 1220CX		Secure Firewall 3105 3110 3120 3130 3140	Firepower 4112 4115 4125 4145	Secure Firewall 4215 4225 4245	Firepower 9300	ISA 3000
9.22(1.1)	7.22(1)	**OUI**	**OUI**	**OUI**		**OUI**	**OUI**	**OUI**	**OUI**	**OUI**

ASA 9.20 et 9.19

Les versions recommandées sont en **gras**.

Remarque

- ASA 9.20(x) était la version finale pour la série Firepower 2100.
- ASA 9.18(x) était la version finale pour les Firepower 4110, 4120, 4140 et 4150, et les modules de sécurité SM-24, SM-36 et SM-44 pour le Firepower 9300.
- Les versions d'ASDM sont rétrocompatibles avec toutes les versions d'ASA précédentes, sauf indication contraire. Par exemple, ASDM 7.19(1) peut gérer un ASA 5516-X sur ASA 9.10(1).
- Les nouvelles versions d'ASA requièrent la version d'ASDM de coordination ou une version ultérieure. Vous ne pouvez pas utiliser une ancienne version d'ASDM avec une nouvelle version d'ASA. Par exemple, vous ne pouvez pas utiliser ASDM 7.18 with ASA 9.19. Pour les versions de maintenance ASA et les versions provisoires, vous pouvez continuer à utiliser la version d'ASDM actuelle, sauf indication contraire. Par exemple, vous pouvez utiliser ASA 9.20(1.5) avec ASDM 7.20(1). Si une version de maintenance ASA comporte de nouvelles fonctionnalités importantes, une nouvelle version d'ASDM sera généralement requise.

Tableau 2 : Compatibilité ASA et ASDM : de la version 9.20 à la version 9.19

ASA	ASDM	Modèle ASA								
		ASA virtuel	Firepower 1010 1120 Série 1150		Firepower de la série 2110 2120 2130 2140	Secure Firewall 3105 3110 3120 3130 3140	Firepower 4112 4115 4125 4145	Secure Firewall 4215 4225 4245	Firepower 9300	ISA 3000
9.20(3)	7.20(2)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**
9.20(2)	7.20(2)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**
9.20(1)	7.20(1)	—	—	—	—	—	—	**OUI**	—	—
9.19(1)	7.19(1)	**OUI**	**OUI**		**OUI**	**OUI**	**OUI**	—	**OUI**	**OUI**

ASA 9.18 à 9.17

Les versions recommandées sont en **gras**.

Remarque

- ASA 9.16(x) était la version finale pour les ASA 5506-X, 5506H-X, 5506W-X, 5508-X et 5516-X.
- Les versions d'ASDM sont rétrocompatibles avec toutes les versions d'ASA précédentes, sauf indication contraire. Par exemple, ASDM 7.17(1) peut gérer un ASA 5516-X sur ASA 9.10(1).
- Les nouvelles versions d'ASA requièrent la version d'ASDM de coordination ou une version ultérieure. Vous ne pouvez pas utiliser une ancienne version d'ASDM avec une nouvelle version d'ASA. Par exemple, vous ne pouvez pas utiliser ASDM 7.17 avec ASA 9.18. Pour les versions de maintenance ASA et les versions provisoires, vous pouvez continuer à utiliser la version d'ASDM actuelle, sauf indication contraire. Par exemple, vous pouvez utiliser ASA 9.17(1.2) avec ASDM 7.17(1). Si une version de maintenance ASA comporte de nouvelles fonctionnalités importantes, une nouvelle version d'ASDM sera généralement requise.
- ASA 9.17(1.13) et 9.18(2) ou les versions ultérieures nécessitent ASDM 7.18(1.152) ou une version ultérieure. L'ASA valide maintenant si l'image ASDM est une image signée numériquement par Cisco. Si vous essayez d'exécuter une image ASDM antérieure à la version 7.18(1.152) avec une version ASA intégrant ce correctif, ASDM sera bloqué, et le message « %ERREUR : signature non valide pour le disque de fichier0:/<nom du fichier> » s'affiche sur l'interface de ligne de commande d'ASA. (CSCwb05291, CSCwb05264)

Tableau 3 : Compatibilité ASA et ASDM : de la version 9.18 à la version 9.17

ASA	ASDM	Modèle ASA							
		ASA virtuel	Firepower 1010 1120 Série 1150		Firepower de la série 2110 2120 2130 2140	Secure Firewall 3110 3120 3130 3140	Firepower 4110 4112 4115 4120 4125 4140 4145 4150	Firepower 9300	ISA 3000
9.18(4)	7.19(1)95	**OUI**	**OUI**		**OUI**	**OUI**	**OUI**	**OUI**	**OUI**
9.18(3)	7.18(1.152)	**OUI**	**OUI**		**OUI**	**OUI**	**OUI**	**OUI**	**OUI**
9.18(2)	7.18(1.152)	**OUI**	**OUI**	—	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**
9.18(1)	7.18(1)	**OUI**	**OUI**	—	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**
9.17(1.13)	7.18(1.152)	**OUI**	**OUI**	—	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**
9.17(1)	7.17(1.155)	**OUI**	**OUI**	—	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**

ASA 9.16 à 9.15

Les versions recommandées sont en **gras**.

Remarque

- ASA 9.16(x) était la version finale pour les ASA 5506-X, 5506H-X, 5506W-X, 5508-X et 5516-X.
- ASA 9.14(x) est la version finale pour les ASA 5525-X, 5545-X et 5555-X.
- Les versions d'ASDM sont rétrocompatibles avec toutes les versions d'ASA précédentes, sauf indication contraire. Par exemple, ASDM 7.15(1) peut gérer un ASA 5516-X sur ASA 9.10(1).
- Les nouvelles versions d'ASA requièrent la version d'ASDM de coordination ou une version ultérieure. Vous ne pouvez pas utiliser une ancienne version d'ASDM avec une nouvelle version d'ASA. Par exemple, vous ne pouvez pas utiliser ASDM 7.15 with ASA 9.16. Pour les versions de maintenance ASA et les versions provisoires, vous pouvez continuer à utiliser la version d'ASDM actuelle, sauf indication contraire. Par exemple, vous pouvez utiliser ASA 9.16(1.15) avec ASDM 7.16(1). Si une version de maintenance ASA comporte de nouvelles fonctionnalités importantes, une nouvelle version d'ASDM sera généralement requise.
- ASA 9.16(3.19) et les versions ultérieures nécessitent ASDM 7.18(1.152) ou une version ultérieure. L'ASA valide maintenant si l'image ASDM est une image signée numériquement par Cisco. Si vous essayez d'exécuter une image ASDM antérieure à la version 7.18(1.152) avec une version ASA intégrant ce correctif, ASDM sera bloqué, et le message « %ERREUR : signature non valide pour le disque de fichier0:/<nom du fichier> » s'affiche sur l'interface de ligne de commande d'ASA. (CSCwb05291, CSCwb05264)

Tableau 4 : Compatibilité ASA et ASDM : de la version 9.16 à la version 9.15

ASA	ASDM	Modèle ASA						
		ASA 5506-X 5506H-X 5506W-X 5508-X 5516-X	ASAv	Firepower 1010 1120 Série 1150	Firepower de la série 2110 2120 2130 2140	Firepower 4110 4112 4115 4120 4125 4140 4145 4150	Firepower 9300	ISA 3000
9.16(4)	7.18(1.152)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**
9.16(3.19)	7.18(1.152)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**
9.16(3)	7.16(1.150)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**
9.16(2)	7.16(1.150)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**
9.16(1)	7.16(1)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**
9.15(1)	7.15(1)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**

ASA 9.14 à 9.13

Les versions recommandées sont en **gras**.

Remarque

- ASA 9.14(x) est la version finale pour les ASA 5525-X, 5545-X et 5555-X.
- ASA 9.12(x) est la version finale pour les ASA 5512-X, 5515-X, 5585-X et ASASM.
- Les versions d'ASDM sont rétrocompatibles avec toutes les versions d'ASA précédentes, sauf indication contraire. Par exemple, ASDM 7.13(1) peut gérer un ASA 5516-X sur ASA 9.10(1). Les ASDM 7.13(1) et ASDM 7.14(1) ne prenaient pas en charge les ASA 5512-X, 5515-X, 5585-X et ASASM. Vous devez effectuer une mise à niveau vers ASDM 7.13(1.101) ou 7.14(1.48) pour rétablir la prise en charge d'ASDM.
- Les nouvelles versions d'ASA requièrent la version d'ASDM de coordination ou une version ultérieure. Vous ne pouvez pas utiliser une ancienne version d'ASDM avec une nouvelle version d'ASA. Par exemple, vous ne pouvez pas utiliser ASDM 7.13 avec ASA 9.14. Pour les versions de maintenance ASA et les versions provisoires, vous pouvez continuer à utiliser la version d'ASDM actuelle, sauf indication contraire. Par exemple, vous pouvez utiliser ASA 9.14(1.2) avec ASDM 7.14(1). Si une version de maintenance ASA comporte de nouvelles fonctionnalités importantes, une nouvelle version d'ASDM sera généralement requise.
- ASA 9.14(4.14) et les versions ultérieures nécessitent ASDM 7.18(1.152) ou une version ultérieure. L'ASA valide maintenant si l'image ASDM est une image signée numériquement par Cisco. Si vous essayez d'exécuter une image ASDM antérieure à la version 7.18(1.152) avec une version ASA intégrant ce correctif, ASDM sera bloqué, et le message « %ERREUR : signature non valide pour le disque de fichier0:/<nom du fichier> » s'affiche sur l'interface de ligne de commande d'ASA. (CSCwb05291, CSCwb05264)

Tableau 5 : Compatibilité ASA et ASDM : de la version 9.14 à la version 9.13

ASA	ASDM	Modèle ASA							
		ASA 5506-X 5506H-X 5506W-X 5508-X 5516-X	ASA 5525-X 5545-X 5555-X	ASAv	Firepower 1010 1120 Série 1150	Firepower de la série 2110 2120 2130 2140	Firepower 4110 4112 4115 4120 4125 4140 4145 4150	Firepower 9300	ISA 3000
9.14(4.14)	7.18(1.152)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**
9.14(4)	7.14(1)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**
9.14(3)	7.14(1)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**

ASA	ASDM	Modèle ASA							
		ASA 5506-X **5506H-X** **5506W-X** **5508-X** **5516-X**	**ASA 5525-X** **5545-X** **5555-X**	**ASAv**	**Firepower 1010** **1120** **Série 1150**	**Firepower de la série 2110** **2120** **2130** **2140**	**Firepower4110** **4112** **4115** **4120** **4125** **4140** **4145** **4150**	**Firepower9300**	**ISA 3000**
9.14(2)	7.14(1)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**
9.14(1.30)	7.14(1)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**
9.14(1.6)	7.14(1.48)	—	—	**OUI** (+ASAv100)	—	—	—	—	—
9.14(1)	7.14(1)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**
9.13(1)	7.13(1)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI** (sauf 4112)	**OUI**	**OUI**

ASA 9.12 à 9.5

Les versions recommandées sont en **gras**.

Remarque

- ASA 9.12(x) est la version finale pour les ASA 5512-X, 5515-X, 5585-X et ASASM.
- Les versions d'ASDM sont rétrocompatibles avec toutes les versions d'ASA précédentes, sauf indication contraire. Par exemple, ASDM 7.12(1) peut gérer un ASA 5515-X sur ASA 9.10(1).
- Les nouvelles versions d'ASA requièrent la version d'ASDM de coordination ou une version ultérieure. Vous ne pouvez pas utiliser une ancienne version d'ASDM avec une nouvelle version d'ASA. Par exemple, vous ne pouvez pas utiliser ASDM 7.10 avec ASA 9.12. Pour les versions de maintenance ASA et les versions provisoires, vous pouvez continuer à utiliser la version d'ASDM actuelle, sauf indication contraire. Par exemple, vous pouvez utiliser ASA 9.12(1.15) avec ASDM 7.12(1). Si une version de maintenance ASA comporte de nouvelles fonctionnalités importantes, une nouvelle version d'ASDM sera généralement requise.
- ASA 9.8(4.45) et 9.12(4.50) ou les versions ultérieures nécessitent ASDM 7.18(1.152) ou une version ultérieure. L'ASA valide maintenant si l'image ASDM est une image signée numériquement par Cisco. Si vous essayez d'exécuter une image ASDM antérieure à la version 7.18(1.152) avec une version ASA intégrant ce correctif, ASDM sera bloqué, et le message « %ERREUR : signature non valide pour le disque de fichier0:/<nom du fichier> » s'affiche sur l'interface de ligne de commande d'ASA. (CSCwb05291, CSCwb05264)

Tableau 6 : Compatibilité ASA et ASDM : de la version 9.12 à la version 9.5

ASA	ASDM	Modèle ASA									
		ASA 5506-X 5506H-X 5506W-X 5508-X 5516-X	ASA 5512-X 5515-X 5525-X 5545-X 5555-X	ASA 5585-X	ASAv	ASASM	Firepower de la série 2110 2120 2130 2140	Firepower 4110 4120 4140 4150	Firepower 4115 4125 4145	Firepower 9300	ISA 3000
9.12(4.50)	7.18(1.152)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**
9.12(4)	7.12(2)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**
9.12(3)	7.12(2)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**
9.12(2)	7.12(2)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**
9.12(1)	7.12(1)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**
9.10(1)	7.10(1)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	—	**OUI**	**OUI**
9.9(2)	7.9(2)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	—	**OUI**	**OUI**
9.9(1)	7.9(1)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	—	**OUI**	**OUI**
9.8(4.45)	7.18(1.152)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	—	**OUI**	**OUI**
9.8(4)	7.8(2)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	—	**OUI**	**OUI**
9.8(3)	7.8(2)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	—	**OUI**	**OUI**
9.8(2)	7.8(2)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	—	**OUI**	**OUI**
9.8(1.200)	Aucun soutien	—	—	—	**OUI**	—	—	—	—	—	—
9.8(1)	7.8(1)	**OUI**	**OUI**	**OUI**	**OUI** (+ASAv50)	**OUI**	—	**OUI**	—	**OUI**	**OUI**
9.7(1.4)	7.7(1)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	—	**OUI**	—	**OUI**	**OUI**
9.6(4)	7.9(1)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	—	**OUI**	—	**OUI**	**OUI**
9.6(3.1)	7.7(1)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	—	**OUI**	—	**OUI**	**OUI**
9.6(2)	7.6(2)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	—	**OUI**	—	**OUI**	**OUI**
9.6(1)	7.6(1)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	—	**OUI** (sauf 4 150)	—	**OUI**	**OUI**

ASA	ASDM	Modèle ASA									
		ASA 5506-X 5506H-X 5506W-X 5508-X 5516-X	ASA 5512-X 5515-X 5525-X 5545-X 5555-X	ASA 5585-X	ASAv	ASASM	Firepower de la série 2110 2120 2130 2140	Firepower 4110 4120 4140 4150	Firepower 4115 4125 4145	Firepower 9300	ISA 3000
9.5(3.9)	7.6(2)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	—	—	—	—	**OUI**
9.5(2.200)	7.5(2.153)	—	—	—	**OUI**	—	—	—	—	—	—
9.5(2.2)	7.5(2)	—	—	—	—	—	—	—	—	**OUI**	—
9.5(2.1)	7.5(2)	—	—	—	—	—	—	—	—	**OUI**	—
9.5(2)	7.5(2)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	—	—	—	—	**OUI**
9.5(1.200)	7.5(1)	—	—	—	**OUI**	—	—	—	—	—	—
9.5(1.5)	7.5(1.112)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	—	—	—	—	—
9.5(1)	7.5(1)	**OUI**	**OUI**	**OUI**	**OUI**	**OUI**	—	—	—	—	—

Compatibilité du Firepower 4100/9300 avec l'ASA et Défense contre les menaces

Pour les périphériques Firepower 4100/9300, vous devez maintenir la compatibilité entre FXOS et tous les périphériques logiques ASA et défense contre les menaces . Mettez à niveau FXOS avant de mettre à niveau le logiciel. Les versions **en gras** dans le tableau suivant sont des versions associées spécialement qualifiées (test amélioré). Utilisez ces combinaisons chaque fois que cela est possible.

Notez que pour les autres modèles de périphériques, le travail de compatibilité FXOS est effectué pour vous. Dans la plupart des cas, la mise à niveau du logiciel met automatiquement à niveau FXOS. Pour Secure Firewall 3100/4200 en mode multi-instance, le centre de gestion vous guide tout au long de la mise à niveau de FXOS, puis défense contre les menaces .

Pour mettre à niveau :

- FXOS : À partir de FXOS 2.2.2 et les versions ultérieures, vous pouvez effectuer une mise à niveau directement vers n'importe quelle version ultérieure. (FXOS 2.0.1–2.2.1 peut être mis à niveau jusqu'à la version 2.8.1. Pour les versions antérieures à la version 2.0.1, vous devez effectuer une mise à niveau à chaque version intermédiaire.) Veuillez noter que vous ne pouvez pas mettre à niveau FXOS vers une version qui ne prend pas en charge votre version de périphérique logique actuelle. Vous devrez effectuer la mise à niveau en étapes : mettez à niveau FXOS vers la version la plus élevée qui prend en charge votre périphérique logique actuel; mettez à niveau votre périphérique logique vers la version la plus élevée prise en charge avec cette version de FXOS. Par exemple, si vous souhaitez effectuer une mise à niveau de FXOS 2.2/ASA 9.8 vers FXOS 2.13/ASA 9.19, vous devrez effectuer les mises à niveau suivantes :

1. FXOS 2.2 → FXOS 2.11 (la version la plus élevée qui prend en charge la version 9.8)
2. ASA 9.8 → ASA 9.17 (la version la plus élevée prise en charge par la version 2.11)
3. FXOS 2.11 → FXOS 2.13
4. ASA 9.17 → ASA 9.19

- Défense contre les menaces : des mises à niveau provisoires peuvent être nécessaires pour défense contre les menaces , en plus des exigences FXOS ci-dessus. Pour le chemin de mise à niveau exact, consultez le centre de gestion guide de mise à niveau de votre version.
- ASA : ASA vous permet de procéder à une mise à niveau directement de votre version actuelle vers toute version supérieure, en notant les exigences FXOS ci-dessus.

Remarque FXOS 2.8(1.125) et les versions ultérieures ne prennent pas en charge ASA 9.14(1) ou 9.14(1.10) pour les sondages et les interruptions SNMP ASA; vous devez utiliser 9.14(1.15) ou une version ultérieure. Les autres versions, comme la version 9.13 ou 9.12, ne sont pas concernées.

Tableau 7 : Compatibilité du Firepower 4100/9300 avec l'ASA et Défense contre les menaces

Version de FXOS	Modèle	Version d'ASA	Défense contre les menacesVersion
2.16	Firepower 4112	**9.22 (recommandé)** 9.20 9.19 9,18 9.17	**7.6** (recommandé) 7.4 7.3 7.2 7.1
	Firepower 4145 Firepower 4125 Firepower 4115	**9.22 (recommandé)** 9.20 9.19	**7.6** (recommandé) 7.4 7.3
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40	9,18 9.17	7.2 7.1

Version de FXOS	Modèle	Version d'ASA	Défense contre les menacesVersion
2.14(1)	Firepower 4112	**9.20** (recommandé) 9.19 9,18 9.17 9.16 9.14	**7.4** (recommandé) 7.3 7.2 7.1 7.0 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	**9.20** (recommandé) 9.19 9,18 9.17 9.16 9.14	**7.4** (recommandé) 7.3 7.2 7.1 7.0 6.6
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
2.13	Firepower 4112	**9.19 (recommandé)** 9,18 9.17 9.16 9.14	**7.3** (recommandé) 7.2 7.1 7.0 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	**9.19 (recommandé)** 9,18 9.17 9.16 9.14	**7.3** (recommandé) 7.2 7.1 7.0 6.6
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		

Version de FXOS	Modèle	Version d'ASA	Défense contre les menacesVersion
2.12	Firepower 4112	**9.18** (recommandé) 9.17 9.16 9.14	**7.2** (recommandé) 7.1 7.0 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	**9.18** (recommandé) 9.17 9.16 9.14 9.12	**7.2** (recommandé) 7.1 7.0 6.6 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.18** (recommandé) 9.17 9.16 9.14 9.12	**7.2** (recommandé) 7.1 7.0 6.6 6.4
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

Version de FXOS	Modèle	Version d'ASA	Défense contre les menacesVersion
2,11	Firepower 4112	**9.17** (recommandé) 9.16 9.14	**7.1** (recommandé) 7.0 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	**9.17** (recommandé) 9.16 9.14 9.12	**7.1** (recommandé) 7.0 6.6 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.17** (recommandé) 9.16 9.14 9.12 9.8	**7.1** (recommandé) 7.0 6.6 6.4
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.10 **Remarque** Pour la compatibilité avec la version 7.0.2 et 9.16 (3.11) ou toute version ultérieure, vous avez besoin de FXOS 2.10 (1.179) ou une version ultérieure.	Firepower 4112	**9.16** (recommandé) 9.14	**7.0** (recommandé) 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	**9.16** (recommandé) 9.14 9.12	**7.0** (recommandé) 6.6 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.16** (recommandé) 9.14 9.12 9.8	**7.0** (recommandé) 6.6 6.4
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

Version de FXOS	Modèle	Version d'ASA	Défense contre les menacesVersion
2.9	Firepower 4112	9.14	6.6
	Firepower 4145 Firepower 4125 Firepower 4115	9.14 9.12	6.6 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	9.14 9.12 9.8	6.6 6.4
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2,8	Firepower 4112	**9.14**	**6.6** **Remarque** La version 6.6.1 et les versions ultérieures nécessitent FXOS 2.8(1.125) ou une version ultérieure.
	Firepower 4145 Firepower 4125 Firepower 4115	**9.14** (recommandé) 9.12 **Remarque** Le Firepower 9300 SM-56 nécessite un ASA 9.12(2) ou une version ultérieure	**6.6** (recommandé) **Remarque** La version 6.6.1 et les versions ultérieures nécessitent FXOS 2.8(1.125) ou une version ultérieure. 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.14** (recommandé) 9.12 9.8	**6.6** (recommandé) **Remarque** La version 6.6.1 et les versions ultérieures nécessitent FXOS 2.8(1.125) ou une version ultérieure.
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		6.4 6.2.3

Version de FXOS	Modèle	Version d'ASA	Défense contre les menacesVersion
2.6(1.157) **Remarque** Vous pouvez désormais exécuter un ASA 9.12 et FTD 6.4 ou toute version ultérieure sur des modules distincts du même châssis Firepower 9300	Firepower 4145 Firepower 4125 Firepower 4115	**9.12** **Remarque** Le Firepower 9300 SM-56 nécessite un ASA 9.12.2 ou une version ultérieure	**6.4**
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.12** (recommandé) 9.8	**6.4** (recommandé) 6.2.3
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.6(1.131)	Firepower 9300 SM-48 Firepower 9300 SM-40	**9.12**	Aucune prise en charge
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.12** (recommandé) 9.8	
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.3(1.73)	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	9.8 **Remarque** La version 9.8(2.12) ou une version ultérieure est requise pour le déchargement de flux lors de l'exécution de FXOS 2.3(1.130) ou une version ultérieure.	**6.2.3** (recommandé) **Remarque** 6.2.3.16+ nécessite FXOS 2.3.1.157 ou ultérieure.
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

Version de FXOS	Modèle	Version d'ASA	Défense contre les menacesVersion
2.3(1.66) 2.3(1.58)	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	9.8 **Remarque** La version 9.8(2.12) ou une version ultérieure est requise pour le déchargement de flux lors de l'exécution de FXOS 2.3(1.130) ou une version ultérieure.	
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.2	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.8**	Les versions de Défense contre les menaces sont en fin de vie
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

Compatibilité avec Radware DefensePro

Le tableau suivant répertorie les versions de Radware DefensePro prises en charge pour chaque appareil de sécurité et chaque périphérique logique associé.

Tableau 8 : Compatibilité avec Radware DefensePro

Version de FXOS	ASA	Défense contre les menaces	Radware DefensePro	Modèles d'appareils de sécurité
2.16	9.22(1)	7.6	8.13.01.09-3 8.22.2	Firepower 9300 Firepower 4112 Firepower 4115 Firepower 4125 Firepower 4145
2.14(1)	9.20(1)	7.4(1)	8.13.01.09-3 8.22.2	Firepower 9300 Firepower 4112 Firepower 4115 Firepower 4125 Firepower 4145

Version de FXOS	ASA	Défense contre les menaces	Radware DefensePro	Modèles d'appareils de sécurité
2.13.0	9.19(1)	7.3	8.13.01.09-3 8.22.2	Firepower 9300 Firepower 4112 Firepower 4115 Firepower 4125 Firepower 4145
2.12.0	9.18(1)	7.2	8.13.01.09-3 8.22.2	Firepower 9300 Firepower 4110 Firepower 4112 Firepower 4115 Firepower 4120 Firepower 4125 Firepower 4140 Firepower 4145 Firepower 4150
2.11.1	9.17(1)	7.1	8.13.01.09-3 8.22.2	Firepower 9300 Firepower 4110 Firepower 4112 Firepower 4115 Firepower 4120 Firepower 4125 Firepower 4140 Firepower 4145 Firepower 4150

Version de FXOS	ASA	Défense contre les menaces	Radware DefensePro	Modèles d'appareils de sécurité
2.10.1	9.16(1)	7.0	8.13.01.09-3 8.22.2	Firepower 9300 Firepower 4110 Firepower 4112 Firepower 4115 Firepower 4120 Firepower 4125 Firepower 4140 Firepower 4145 Firepower 4150
2.10.1	9.16(1)	7.0	8.13.01.09-3 8.22.2	Firepower 9300 Firepower 4110 Firepower 4112 Firepower 4115 Firepower 4120 Firepower 4125 Firepower 4140 Firepower 4145 Firepower 4150
2.9.1	9.15(1)	6.7.0	8.13.01.09-3 8.22.2	Firepower 9300 Firepower 4110 Firepower 4112 Firepower 4115 Firepower 4120 Firepower 4125 Firepower 4140 Firepower 4145 Firepower 4150

Version de FXOS	ASA	Défense contre les menaces	Radware DefensePro	Modèles d'appareils de sécurité
2.8.1	9.14(1)	6.6.0	8.13.01.09-3 8.22.2	Firepower 9300 Firepower 4110 Firepower 4112 Firepower 4115 Firepower 4120 Firepower 4125 Firepower 4140 Firepower 4145 Firepower 4150
2.7(1)	9.13(1)	6.5	8.13.01.09-3	Firepower 9300 Firepower 4110 Firepower 4115 Firepower 4120 Firepower 4125 Firepower 4140 Firepower 4145 Firepower 4150
2.6(1)	9.12(1) 9.10(1)	6.4.0 6.3.0	8.13.01.09-3	Firepower 9300 Firepower 4110 Firepower 4115 Firepower 4120 Firepower 4125 Firepower 4140 Firepower 4145 Firepower 4150
2.4(1)	9.9(2) 9.10(1)	6.2.3 6.3	8.13.01.09-2	Firepower 9300 Firepower 4110 Firepower 4120 Firepower 4140 Firepower 4150

Version de FXOS	ASA	Défense contre les menaces	Radware DefensePro	Modèles d'appareils de sécurité
2.3(1)	9.9(1) 9.9(2)	6.2.2 6.2.3	8.13.01.09-2	Firepower 9300 Firepower 4110 (Firepower Threat Defense seulement) Firepower 4120 Firepower 4140 Firepower 4150
2.2(2)	9.8(1) 9.8(2) 9.8(3)	6.2.0 6.2.2	8.10.01.17-2	Firepower 9300 Firepower 4110 (Firepower Threat Defense seulement) Firepower 4120 Firepower 4140 Firepower 4150
2.2(1)	9.7(1) 9.8(1)	6.2.0	8.10.01.17-2	Firepower 9300 Firepower 4110 (Firepower Threat Defense seulement) Firepower 4120 Firepower 4140 Firepower 4150
2.1(1)	9.6(2) 9.6(3) 9.6(4) 9.7(1)	Aucune prise en charge	8.10.01.16-5	Firepower 9300 Firepower 4120 Firepower 4140 Firepower 4150
2.0(1)	9.6(1) 9.6(2) 9.6(3) 9.6(4)	Aucune prise en charge	8.10.01.16-5	Firepower 9300 Firepower 4120 Firepower 4140 Firepower 4150
1.1(4)	9.6(1)	Aucune prise en charge	1.1(2.32-3)	9300

Chemin de mise à niveau

Pour chaque système d'exploitation que vous mettez à niveau, vérifiez le chemin de mise à niveau pris en charge. Dans certains cas, vous devrez peut-être installer des mises à niveau intermédiaires avant de pouvoir passer à la version finale.

Chemin de mise à niveau : Appareils ASA

Pour afficher la version et le modèle actuels, utilisez l'une des méthodes suivantes :

- ASDM : Choisissez **Home** > **Device Dashboard** > **Device Information (Accueil > Tableau de bord des appareils > Informations sur les appareils)**.
- Interface de ligne de commande : Utilisez la commande **show version** .

Ce tableau fournit des chemin sde mise à niveau pour l'ASA. Certaines versions plus anciennes nécessitent une mise à niveau intermédiaire avant de pouvoir passer à une version plus récente. Les versions recommandées sont en **gras**.

Veillez à vérifier les instructions de mise à niveau pour chaque version entre votre version de départ et votre version d'arrivée. Dans certains cas, vous devrez modifier votre configuration avant de procéder à la mise à niveau, faute de quoi vous risquez de subir une panne. Voir Lignes directrices pour la mise à niveau de l'ASA, à la page 1.

Pour obtenir des informations sur les problèmes de sécurité de l'ASA et savoir quelles versions contiennent des correctifs pour chaque problème, consultez les ASA Security Advisories (avis de sécurité de l'ASA).

Remarque

ASA 9.20(x) était la version finale pour le Firepower 2100.

ASA 9.18 était la version finale pour les Firepower 4110, 4120, 4140 et 4150, et les modules de sécurité SM-24, SM-36 et SM-44 pour le Firepower 9300.

ASA 9.16 était la version finale pour les ASA 5506-X, 5508-X et 5516-X.

ASA 9.14 était la version finale pour les ASA 5525-X, 5545-X et 5555-X.

ASA 9.12 était la version finale pour les ASA 5512-X, 5515-X, 5585-X et ASASM.

ASA 9.2 était la version finale pour l'ASA 5505.

ASA 9.1(x) était la version finale pour les ASA 5510, 5520, 5540, 5550 et 5580.

Tableau 9 : Chemin de mise à niveau

Version actuelle	Version de mise à jour provisoire	Version cible
9.20	—	L'un des éléments suivants : → **9.22**

Version actuelle	Version de mise à jour provisoire	Version cible
9.19	—	L'un des éléments suivants : → **9.22** → **9.20**
9,18	—	L'un des éléments suivants : → **9.22** → **9.20** → **9.19**
9.17	—	L'un des éléments suivants : → **9.22** → **9.20** → **9.19** → **9.18**
9.16	—	L'un des éléments suivants : → **9.22** → **9.20** → **9.19** → **9.18** → 9.17
9.15	—	L'un des éléments suivants : → **9.22** → **9.20** → **9.19** → **9.18** → 9.17 → **9.16**
9.14	—	L'un des éléments suivants : → **9.22** → **9.20** → **9.19** → **9.18** → 9.17 → **9.16**

Version actuelle	Version de mise à jour provisoire	Version cible
9.13	—	L'un des éléments suivants : → **9.22** → **9.20** → **9.19** → **9.18** → 9.17 → **9.16** → 9.14
9.12	—	L'un des éléments suivants : → **9.22** → **9.20** → **9.19** → **9.18** → 9.17 → **9.16** → 9.14
9.10	—	L'un des éléments suivants : → **9.22** → **9.20** → **9.19** → **9.18** → 9.17 → **9.16** → 9.14 → 9.12

Version actuelle	Version de mise à jour provisoire	Version cible
9.9	—	L'un des éléments suivants : → **9.22** → **9.20** → **9.19** → **9.18** → 9.17 → **9.16** → 9.14 → 9.12
9.8	—	L'un des éléments suivants : → **9.22** → **9.20** → **9.19** → **9.18** → 9.17 → **9.16** → 9.14 → 9.12
9.7	—	L'un des éléments suivants : → **9.22** → **9.20** → **9.19** → **9.18** → 9.17 → **9.16** → 9.14 → 9.12 → 9.8

Version actuelle	Version de mise à jour provisoire	Version cible
9.6	—	L'un des éléments suivants : → **9.22** → **9.20** → **9.19** → **9.18** → 9.17 → **9.16** → 9.14 → 9.12 → 9.8
9.5	—	L'un des éléments suivants : → **9.22** → **9.20** → **9.19** → **9.18** → 9.17 → **9.16** → 9.14 → 9.12 → 9.8
9.4	—	L'un des éléments suivants : → **9.22** → **9.20** → **9.19** → **9.18** → 9.17 → **9.16** → 9.14 → 9.12 → 9.8

Version actuelle	Version de mise à jour provisoire	Version cible
9.3	—	L'un des éléments suivants : → **9.22** → **9.20** → **9.19** → **9.18** → 9.17 → **9.16** → 9.14 → 9.12 → 9.8
9.2	—	L'un des éléments suivants : → **9.22** → **9.20** → **9.19** → **9.18** → 9.17 → **9.16** → 9.14 → 9.12 → 9.8
9.1(2), 9.1(3), 9.1(4), 9.1(5), 9.1(6), ou 9.1(7.4)	—	L'un des éléments suivants : → 9.14 → **9.12** → 9.8 → 9.1(7.4)
9.1(1)	→ 9.1(2)	L'un des éléments suivants : → 9.14 → **9.12** → 9.8 → 9.1(7.4)

Version actuelle	Version de mise à jour provisoire	Version cible
9.0(2), 9.0(3) ou 9.0(4)	—	L'un des éléments suivants : → 9.14 → **9.12** → 9.8 → 9.6 → 9.1(7.4)
9.0(1)	→ 9.0(4)	L'un des éléments suivants : → 9.14 → **9.12** → 9.8 → 9.1(7.4)
8.6(1)	→ 9.0(4)	L'un des éléments suivants : → 9.14 → **9.12** → 9.8 → 9.1(7.4)
8.5(1)	→ 9.0(4)	L'un des éléments suivants : → **9.12** → 9.8 → 9.1(7.4)
8.4(5+)	—	L'un des éléments suivants : → **9.12** → 9.8 → 9.1(7.4) → 9.0(4)
8.4(1) à 8.4(4)	→ 9.0(4)	→ **9.12** → 9.8 → 9.1(7.4)
8.3	→ 9.0(4)	L'un des éléments suivants : → **9.12** → 9.8 → 9.1(7.4)

Version actuelle	Version de mise à jour provisoire	Version cible
8.2 ou version antérieure	→ 9.0(4)	L'un des éléments suivants : → **9.12** → 9.8 → 9.1(7.4)

Chemin de mise à niveau : ASA sur Firepower 2100 en mode plateforme

Pour afficher la version et le modèle actuels, utilisez l'une des méthodes suivantes :

- ASDM : Choisissez **Home** > **Device Dashboard** > **Device Information (Accueil > Tableau de bord des appareils > Informations sur les appareils)**.
- Interface de ligne de commande : Utilisez la commande **show version** .

Ce tableau fournit des chemins de mise à niveau pour l'ASA sur le Firepower 2100 en mode plateforme. Certaines versions nécessitent une mise à niveau intermédiaire avant de pouvoir passer à une version plus récente. Les versions recommandées sont en **gras**.

Veillez à vérifier les instructions de mise à niveau pour chaque version entre votre version de départ et votre version d'arrivée. Dans certains cas, vous devrez modifier votre configuration avant de procéder à la mise à niveau, faute de quoi vous risquez de subir une panne. Voir Lignes directrices pour la mise à niveau de l'ASA, à la page 1.

Pour obtenir des informations sur les problèmes de sécurité de l'ASA et savoir quelles versions contiennent des correctifs pour chaque problème, consultez les ASA Security Advisories (avis de sécurité de l'ASA).

Remarque ASA 9.20(x) était la version finale pour le Firepower 2100.

Tableau 10 : Chemin de mise à niveau

Version actuelle	Version de mise à jour provisoire	Version cible
9.19	—	L'un des éléments suivants : → **9.20**
9,18	—	L'un des éléments suivants : → **9.20** → **9.19**
9.17	—	L'un des éléments suivants : → **9.20** → **9.19** → **9.18**

Version actuelle	Version de mise à jour provisoire	Version cible
9.16	—	L'un des éléments suivants : → **9.20** → **9.19** → **9.18** → 9.17
9.15	—	L'un des éléments suivants : → **9.20** → **9.19** → **9.18** → 9.17 → **9.16**
9.14	—	L'un des éléments suivants : → **9.20** → **9.19** → **9.18** → 9.17 → **9.16** → 9.15
9.13	→ 9.18	L'un des éléments suivants : → **9.20** → **9.19**
9.13	—	L'un des éléments suivants : → **9.18** → 9.17 → **9.16** → 9.15 → 9.14
9.12	→ 9.18	L'un des éléments suivants : → **9.20** → **9.19**

Version actuelle	Version de mise à jour provisoire	Version cible
9.12	—	L'un des éléments suivants : → **9.18** → 9.17 → **9.16** → 9.15 → 9.14
9.10	→ 9.17	L'un des éléments suivants : → **9.20** → **9.19** → **9.18**
9.10	—	L'un des éléments suivants : → 9.17 → **9.16** → 9.15 → 9.14 → 9.12
9.9	→ 9.17	L'un des éléments suivants : → **9.20** → **9.19** → **9.18**
9.9	—	L'un des éléments suivants : → 9.17 → **9.16** → 9.15 → 9.14 → 9.12
9.8	→ 9.17	L'un des éléments suivants : → **9.20** → **9.19** → **9.18**

Version actuelle	Version de mise à jour provisoire	Version cible
9.8	—	L'un des éléments suivants : → 9.17 → **9.16** → 9.15 → 9.14 → 9.12

Chemin de mise à niveau : périphériques logiques ASA pour le Firepower 4100/9300

Pour afficher la version et le modèle actuels, utilisez l'une des méthodes suivantes :

- Firepower Chassis Manager : choisissez **Aperçu**et examinez les champs **Modèle** et **Version** dans la partie supérieure de l'écran.
- Interface de ligne de commande : pour la version, utilisez la commande **show version** et consultez le champ Paquet-Vers:. Pour le modèle, saisissez **scope chassis 1**, puis **show inventory**.
- FXOS : À partir de FXOS 2.2.2 et les versions ultérieures, vous pouvez effectuer une mise à niveau directement vers n'importe quelle version ultérieure. (FXOS 2.0.1–2.2.1 peut être mis à niveau jusqu'à la version 2.8.1. Pour les versions antérieures à la version 2.0.1, vous devez effectuer une mise à niveau à chaque version intermédiaire.) Veuillez noter que vous ne pouvez pas mettre à niveau FXOS vers une version qui ne prend pas en charge votre version de périphérique logique actuelle. Vous devrez effectuer la mise à niveau en étapes : mettez à niveau FXOS vers la version la plus élevée qui prend en charge votre périphérique logique actuel; mettez à niveau votre périphérique logique vers la version la plus élevée prise en charge avec cette version de FXOS. Par exemple, si vous souhaitez effectuer une mise à niveau de FXOS 2.2/ASA 9.8 vers FXOS 2.13/ASA 9.19, vous devrez effectuer les mises à niveau suivantes :
  1. FXOS 2.2 → FXOS 2.11 (la version la plus élevée qui prend en charge la version 9.8)
  2. ASA 9.8 → ASA 9.17 (la version la plus élevée prise en charge par la version 2.11)
  3. FXOS 2.11 → FXOS 2.13
  4. ASA 9.17 → ASA 9.19
- Défense contre les menaces : des mises à niveau provisoires peuvent être nécessaires pour défense contre les menaces , en plus des exigences FXOS ci-dessus. Pour le chemin de mise à niveau exact, consultez le centre de gestion guide de mise à niveau de votre version.
- ASA : ASA vous permet de procéder à une mise à niveau directement de votre version actuelle vers toute version supérieure, en notant les exigences FXOS ci-dessus.

Tableau 11 : Compatibilité du Firepower 4100/9300 avec l'ASA et Défense contre les menaces

Version de FXOS	Modèle	Version d'ASA	Défense contre les menacesVersion
2.16	Firepower 4112	**9.22 (recommandé)** 9.20 9.19 9,18 9.17	**7.6** (recommandé) 7.4 7.3 7.2 7.1
	Firepower 4145 Firepower 4125 Firepower 4115 Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40	**9.22 (recommandé)** 9.20 9.19 9,18 9.17	**7.6** (recommandé) 7.4 7.3 7.2 7.1
2.14(1)	Firepower 4112	**9.20** (recommandé) 9.19 9,18 9.17 9.16 9.14	**7.4** (recommandé) 7.3 7.2 7.1 7.0 6.6
	Firepower 4145 Firepower 4125 Firepower 4115 Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40	**9.20** (recommandé) 9.19 9,18 9.17 9.16 9.14	**7.4** (recommandé) 7.3 7.2 7.1 7.0 6.6

Version de FXOS	Modèle	Version d'ASA	Défense contre les menacesVersion
2.13	Firepower 4112	**9.19 (recommandé)** 9,18 9.17 9.16 9.14	**7.3** (recommandé) 7.2 7.1 7.0 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	**9.19 (recommandé)** 9,18 9.17 9.16 9.14	**7.3** (recommandé) 7.2 7.1 7.0 6.6
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
2.12	Firepower 4112	**9.18** (recommandé) 9.17 9.16 9.14	**7.2** (recommandé) 7.1 7.0 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	**9.18** (recommandé) 9.17 9.16 9.14 9.12	**7.2** (recommandé) 7.1 7.0 6.6 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.18** (recommandé) 9.17 9.16 9.14 9.12	**7.2** (recommandé) 7.1 7.0 6.6 6.4
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

Version de FXOS	Modèle	Version d'ASA	Défense contre les menacesVersion
2,11	Firepower 4112	**9.17** (recommandé) 9.16 9.14	**7.1** (recommandé) 7.0 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	**9.17** (recommandé) 9.16 9.14 9.12	**7.1** (recommandé) 7.0 6.6 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.17** (recommandé) 9.16 9.14 9.12 9.8	**7.1** (recommandé) 7.0 6.6 6.4
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.10 **Remarque** Pour la compatibilité avec la version 7.0.2 et 9.16 (3.11) ou toute version ultérieure, vous avez besoin de FXOS 2.10 (1.179) ou une version ultérieure.	Firepower 4112	**9.16** (recommandé) 9.14	**7.0** (recommandé) 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	**9.16** (recommandé) 9.14 9.12	**7.0** (recommandé) 6.6 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.16** (recommandé) 9.14 9.12 9.8	**7.0** (recommandé) 6.6 6.4
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

Version de FXOS	Modèle	Version d'ASA	Défense contre les menacesVersion
2.9	Firepower 4112	9.14	6.6
	Firepower 4145 Firepower 4125 Firepower 4115	9.14 9.12	6.6 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	9.14 9.12 9.8	6.6 6.4
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2,8	Firepower 4112	**9.14**	**6.6** **Remarque** La version 6.6.1 et les versions ultérieures nécessitent FXOS 2.8(1.125) ou une version ultérieure.
	Firepower 4145 Firepower 4125 Firepower 4115	**9.14** (recommandé) 9.12 **Remarque** Le Firepower 9300 SM-56 nécessite un ASA 9.12(2) ou une version ultérieure	**6.6** (recommandé) **Remarque** La version 6.6.1 et les versions ultérieures nécessitent FXOS 2.8(1.125) ou une version ultérieure. 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.14** (recommandé) 9.12 9.8	**6.6** (recommandé) **Remarque** La version 6.6.1 et les versions ultérieures nécessitent FXOS 2.8(1.125) ou une version ultérieure. 6.4 6.2.3
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

Version de FXOS	Modèle	Version d'ASA	Défense contre les menacesVersion
2.6(1.157) **Remarque** Vous pouvez désormais exécuter un ASA 9.12 et FTD 6.4 ou toute version ultérieure sur des modules distincts du même châssis Firepower 9300	Firepower 4145 Firepower 4125 Firepower 4115	**9.12** **Remarque** Le Firepower 9300 SM-56 nécessite un ASA 9.12.2 ou une version ultérieure	**6.4**
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.12** (recommandé) 9.8	**6.4** (recommandé) 6.2.3
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.6(1.131)	Firepower 9300 SM-48 Firepower 9300 SM-40	**9.12**	Aucune prise en charge
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.12** (recommandé) 9.8	
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.3(1.73)	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	9.8 **Remarque** La version 9.8(2.12) ou une version ultérieure est requise pour le déchargement de flux lors de l'exécution de FXOS 2.3(1.130) ou une version ultérieure.	**6.2.3** (recommandé) **Remarque** 6.2.3.16+ nécessite FXOS 2.3.1.157 ou ultérieure.
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

Version de FXOS	Modèle	Version d'ASA	Défense contre les menacesVersion
2.3(1.66) 2.3(1.58)	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	9.8 **Remarque** La version 9.8(2.12) ou une version ultérieure est requise pour le déchargement de flux lors de l'exécution de FXOS 2.3(1.130) ou une version ultérieure.	
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.2	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.8**	Les versions de Défense contre les menaces sont en fin de vie
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

Remarque sur les rétrogradations

La rétrogradation des images FXOS n'est pas officiellement prise en charge. La seule méthode prise en charge par Cisco pour rétrograder une version d'image FXOS consiste à effectuer une recréation d'image complète de l'appareil.

Télécharger le logiciel à partir de Cisco.com

Téléchargez tous les paquets de logiciels à partir de Cisco.com avant de commencer la mise à niveau. Selon le système d'exploitation et si vous utilisez l'interface de ligne de commande ou l'interface graphique, vous devez placer les images sur un serveur ou sur votre ordinateur de gestion. Consultez chaque procédure d'installation pour connaître les détails sur les emplacements de fichiers pris en charge.

Remarque Un identifiant Cisco.com et un contrat de service Cisco sont requis.

Télécharger le logiciel ASA

Si vous utilisez l'assistant de mise à niveau ASDM, vous n'avez pas besoin de prétélécharger le logiciel. Si vous effectuez une mise à niveau manuelle, par exemple pour une mise à niveau de basculement, téléchargez les images sur votre ordinateur local.

Pour procéder à une mise à niveau de l'interface de ligne de commande, vous pouvez placer le logiciel sur de nombreux types de serveurs, notamment TFTP, HTTP et FTP. Consultez les commandes **copy** dans la référence de commande ASA.

Le logiciel ASA peut être téléchargé à partir du site Cisco.com. Ces tableaux comprennent des conventions de dénomination et des informations sur les paquets ASA.

Tableau 12 : Plateformes actuelles

Modèle ASA	Emplacement de téléchargement	Progiciels
ASA virtuel	http://www.cisco.com/go/asav-software	
	Logiciel ASA (mise à niveau) Choisissez **Logiciel d'appareils de sécurité adaptables (ASA)** > *version*.	Le fichier de mise à niveau virtuelle ASA porte un nom de fichier de type asa962-**smp-k8.bin**; utilisez ce fichier de mise à niveau pour tous les hyperviseurs. **Remarque :** Les fichiers .zip (VMware), .vhdx (Hyper-V) et .qcow2 (KVM) sont réservés au déploiement initial. **Remarque** Pour mettre à niveau l'ASA virtuel pour les services en nuage public tels que Amazon Web Services, vous pouvez télécharger l'image ci-dessus à partir de Cisco.com (qui nécessite un identifiant Cisco.com et un contrat de service Cisco) et effectuer la mise à niveau comme décrit dans ce guide. Il n'y a aucun moyen d'obtenir une image de *mise à niveau* à partir du service de nuage public.
	Logiciel ASDM (mise à niveau) Choisissez **Gestionnaire d'appareils de sécurité adaptables (ASA)** > *version*.	Exemple de nom de fichier utilisé pour le logiciel ASDM : asdm-762**.bin**.
	Logiciel API REST Choisissez **Module d'extension API REST d'appareils de sécurité adaptables** > *version*.	Exemple de nom de fichier utilisé pour le logiciel API : asa-restapi-132-**lfbff-k8.SPA**. Pour installer l'API REST, consultez le guide de démarrage rapide de l'API.
	Paquet de périphérique ASA pour APIC (Cisco Application Policy Infrastructure Controller) Choisissez **Paquets de périphériques ASA pour l'infrastructure axée sur les applications (ACI)** > *version*.	Pour APIC 1.2(7) et les versions ultérieures, choisissez le paquet Policy Orchestration avec Fabric Insertion ou le paquet Fabric Insertion seul. Exemple de nom de fichier utilisé pour le paquet de périphérique : asa-device-pkg-1.2.7.10**.zip**. Pour installer le paquet de périphérique ASA, consultez le chapitre « Importation d'un paquet de périphérique » du Guide de déploiement des services APIC de Cisco pour les couches 4 à 7.

Modèle ASA	Emplacement de téléchargement	Progiciels
Firepower 1000	http://www.cisco.com/go/asa-firepower-sw	
	Logiciels ASA, ASDM et FXOS Choisissez votre *modèle* > **Logiciel d'appareils de sécurité adaptables (ASA)(** > *version*.	Le paquet ASA comprend les logiciels ASA, ASDM et FXOS. Exemple de nom de fichier pour le paquet ASA : cisco-asa-fp1k.9.13.1**.SPA**.
	Logiciel ASDM (mise à niveau) Choisissez votre *modèle* > **Gestionnaire d'appareils de sécurité adaptables (ASA)** > *version*.	Utilisez cette image pour effectuer une mise à niveau vers une version ultérieure d'ASDM en utilisant votre ASDM actuel ou l'interface de ligne de commande d'ASA. Exemple de nom de fichier utilisé pour le logiciel ASDM : asdm-7131**.bin**. **Remarque** Lorsque vous mettez à niveau le paquet de l'ASA, l'image ASDM de l'offre groupée remplace l'image du groupe ASDM précédent sur l'ASA, car elles portent le même nom (**asdm.bin**). Toutefois, si vous avez choisi manuellement une autre image ASDM que vous avez téléversée (par exemple, **asdm-7131.bin**), vous continuez à utiliser cette image même après une mise à niveau groupée. Pour vous assurer d'exécuter une version compatible d'ASDM, vous devez soit mettre à niveau ASDM avant de mettre à niveau l'ensemble, soit reconfigurer l'ASA pour utiliser l'image ASDM fournie (**asdm.bin**) juste avant de mettre à niveau l'ensemble ASA.

Modèle ASA	Emplacement de téléchargement	Progiciels
Secure Firewall 1200	http://www.cisco.com/go/asa-firepower-sw	
	Logiciels ASA, ASDM et FXOS Choisissez votre *modèle* > **Logiciel d'appareils de sécurité adaptables (ASA)(** > *version*.	Le paquet ASA comprend les logiciels ASA, ASDM et FXOS. Exemple de nom de fichier pour le paquet ASA : cisco-asa-csf1200.9.22.1.3**.SPA**.
	Logiciel ASDM (mise à niveau) Choisissez votre *modèle* > **Gestionnaire d'appareils de sécurité adaptables (ASA)** > *version*.	Utilisez cette image pour effectuer une mise à niveau vers une version ultérieure d'ASDM en utilisant votre ASDM actuel ou l'interface de ligne de commande d'ASA. Exemple de nom de fichier utilisé pour le logiciel ASDM : asdm-7221**.bin**. **Remarque** Lorsque vous mettez à niveau le paquet de l'ASA, l'image ASDM de l'offre groupée remplace l'image du groupe ASDM précédent sur l'ASA, car elles portent le même nom (**asdm.bin**). Toutefois, si vous avez choisi manuellement une autre image ASDM que vous avez téléversée (par exemple, **asdm-7221.bin**), vous continuez à utiliser cette image même après une mise à niveau groupée. Pour vous assurer d'exécuter une version compatible d'ASDM, vous devez soit mettre à niveau ASDM avant de mettre à niveau l'ensemble, soit reconfigurer l'ASA pour utiliser l'image ASDM fournie (**asdm.bin**) juste avant de mettre à niveau l'ensemble ASA.

Modèle ASA	Emplacement de téléchargement	Progiciels
Secure Firewall 3100	https://cisco.com/go/asa-secure-firewall-sw	
	Logiciels ASA, ASDM et FXOS Choisissez votre *modèle* > **Logiciel d'appareils de sécurité adaptables (ASA)(** > *version*.	Le paquet ASA comprend les logiciels ASA, ASDM et FXOS. Exemple de nom de fichier pour le paquet ASA : cisco-asa-fp3k.9.17.1**.SPA**.
	Logiciel ASDM (mise à niveau) Choisissez votre *modèle* > **Gestionnaire d'appareils de sécurité adaptables (ASA)** > *version*.	Utilisez cette image pour effectuer une mise à niveau vers une version ultérieure d'ASDM en utilisant votre ASDM actuel ou l'interface de ligne de commande d'ASA. Exemple de nom de fichier utilisé pour le logiciel ASDM : asdm-7171**.bin**. **Remarque** Lorsque vous mettez à niveau le paquet de l'ASA, l'image ASDM de l'offre groupée remplace l'image du groupe ASDM précédent sur l'ASA, car elles portent le même nom (**asdm.bin**). Toutefois, si vous avez choisi manuellement une autre image ASDM que vous avez téléversée (par exemple, **asdm-7171.bin**), vous continuez à utiliser cette image même après une mise à niveau groupée. Pour vous assurer d'exécuter une version compatible d'ASDM, vous devez soit mettre à niveau ASDM avant de mettre à niveau l'ensemble, soit reconfigurer l'ASA pour utiliser l'image ASDM fournie (**asdm.bin**) juste avant de mettre à niveau l'ensemble ASA.

Modèle ASA	Emplacement de téléchargement	Progiciels
Firepower 4100	http://www.cisco.com/go/firepower4100-software	
	Logiciels ASA et ASDM Choisissez votre *modèle* > **Logiciel d'appareils de sécurité adaptables (ASA)(** > *version*.	Ce paquet comprend ASA et ASDM. Exemple de nom de fichier pour le paquet ASA : cisco-ASA.9.6.2**.SPA.csp**.
	Logiciel ASDM (mise à niveau) Choisissez votre *modèle* > **Gestionnaire d'appareils de sécurité adaptables (ASA)** > *version*.	Utilisez cette image pour effectuer une mise à niveau vers une version ultérieure d'ASDM en utilisant votre ASDM actuel ou l'interface de ligne de commande d'ASA. Exemple de nom de fichier utilisé pour le logiciel ASDM : asdm-762**.bin**. **Remarque** Lorsque vous mettez à niveau le paquet de l'ASA dans FXOS, l'image ASDM de l'offre groupée remplace l'image du groupe ASDM précédent sur l'ASA, car elles portent le même nom (**asdm.bin**). Toutefois, si vous avez choisi manuellement une autre image ASDM que vous avez téléversée (par exemple, **asdm-782.bin**), vous continuez à utiliser cette image même après une mise à niveau groupée. Pour vous assurer d'exécuter une version compatible d'ASDM, vous devez soit mettre à niveau ASDM avant de mettre à niveau l'ensemble, soit reconfigurer l'ASA pour utiliser l'image ASDM fournie (**asdm.bin**) juste avant de mettre à niveau l'ensemble ASA.
	Logiciel API REST Choisissez votre *modèle* > **Module d'extension API REST d'appareils de sécurité adaptables** > *version*.	Exemple de nom de fichier utilisé pour le logiciel API : asa-restapi-132-**lfbff-k8.SPA**. Pour installer l'API REST, consultez le guide de démarrage rapide de l'API.

Modèle ASA	Emplacement de téléchargement	Progiciels
Secure Firewall 4200	https://cisco.com/go/asa-secure-firewall-sw	
	Logiciels ASA, ASDM et FXOS Choisissez votre *modèle* > **Logiciel d'appareils de sécurité adaptables (ASA)(** > *version*.	Le paquet ASA comprend les logiciels ASA, ASDM et FXOS. Exemple de nom de fichier pour le paquet ASA : cisco-asa-fp4200.9.20.1**.SPA**.
	Logiciel ASDM (mise à niveau) Choisissez votre *modèle* > **Gestionnaire d'appareils de sécurité adaptables (ASA)** > *version*.	Utilisez cette image pour effectuer une mise à niveau vers une version ultérieure d'ASDM en utilisant votre ASDM actuel ou l'interface de ligne de commande d'ASA. Exemple de nom de fichier utilisé pour le logiciel ASDM : asdm-7201**.bin**. **Remarque** Lorsque vous mettez à niveau le paquet de l'ASA, l'image ASDM de l'offre groupée remplace l'image du groupe ASDM précédent sur l'ASA, car elles portent le même nom (**asdm.bin**). Toutefois, si vous avez choisi manuellement une autre image ASDM que vous avez téléversée (par exemple, **asdm-7201.bin**), vous continuez à utiliser cette image même après une mise à niveau groupée. Pour vous assurer d'exécuter une version compatible d'ASDM, vous devez soit mettre à niveau ASDM avant de mettre à niveau l'ensemble, soit reconfigurer l'ASA pour utiliser l'image ASDM fournie (**asdm.bin**) juste avant de mettre à niveau l'ensemble ASA.

Modèle ASA	Emplacement de téléchargement	Progiciels
Firepower 9300	http://www.cisco.com/go/firepower9300-software	
	Logiciels ASA et ASDM Choisissez **Logiciel d'appareils de sécurité adaptables (ASA)** > *version*.	Ce paquet comprend ASA et ASDM. Exemple de nom de fichier pour le paquet ASA : cisco-ASA.9.6.2**.SPA.csp**.
	Logiciel ASDM (mise à niveau) Choisissez **Gestionnaire d'appareils de sécurité adaptables (ASA)** > *version*.	Utilisez cette image pour effectuer une mise à niveau vers une version ultérieure d'ASDM en utilisant votre ASDM actuel ou l'interface de ligne de commande d'ASA. Exemple de nom de fichier utilisé pour le logiciel ASDM : asdm-762**.bin**. **Remarque** Lorsque vous mettez à niveau le paquet de l'ASA dans FXOS, l'image ASDM de l'offre groupée remplace l'image du groupe ASDM précédent sur l'ASA, car elles portent le même nom (**asdm.bin**). Toutefois, si vous avez choisi manuellement une autre image ASDM que vous avez téléversée (par exemple, **asdm-782.bin**), vous continuez à utiliser cette image même après une mise à niveau groupée. Pour vous assurer d'exécuter une version compatible d'ASDM, vous devez soit mettre à niveau ASDM avant de mettre à niveau l'ensemble, soit reconfigurer l'ASA pour utiliser l'image ASDM fournie (**asdm.bin**) juste avant de mettre à niveau l'ensemble ASA.
	Logiciel API REST Choisissez **Module d'extension API REST d'appareils de sécurité adaptables** > *version*.	Exemple de nom de fichier utilisé pour le logiciel API : asa-restapi-132-**lfbff-k8.SPA**. Pour installer l'API REST, consultez le guide de démarrage rapide de l'API.

Modèle ASA	Emplacement de téléchargement	Progiciels
ISA 3000	http://www.cisco.com/go/isa3000-software	
	Logiciel ASA Choisissez votre *modèle* > **Logiciel d'appareils de sécurité adaptables (ASA)(** > *version*.	Exemple de nom de fichier utilisé pour le logiciel ASA : asa962-**lfbff-k8.SPA**.
	Logiciel ASDM Choisissez votre *modèle* > **Gestionnaire d'appareils de sécurité adaptables (ASA)** > *version*.	Exemple de nom de fichier utilisé pour le logiciel ASDM : asdm-762**.bin**.
	Logiciel API REST Choisissez votre *modèle* > **Module d'extension API REST d'appareils de sécurité adaptables** > *version*.	Exemple de nom de fichier utilisé pour le logiciel API : asa-restapi-132-**lfbff-k8.SPA**. Pour installer l'API REST, consultez le guide de démarrage rapide de l'API.

Tableau 13 : Plateformes existantes

Modèle ASA	Emplacement de téléchargement	Progiciels
ASA 5506-X, ASA 5508-X et ASA 5516-X	http://www.cisco.com/go/asa-firepower-sw	
	Logiciel ASA Choisissez votre *modèle* > **Logiciel d'appareils de sécurité adaptables (ASA)(** > *version*.	Exemple de nom de fichier utilisé pour le logiciel ASA : asa962-**lfbff-k8.SPA**.
	Logiciel ASDM Choisissez votre *modèle* > **Gestionnaire d'appareils de sécurité adaptables (ASA)** > *version*.	Exemple de nom de fichier utilisé pour le logiciel ASDM : asdm-762**.bin**.
	Logiciel API REST Choisissez votre *modèle* > **Module d'extension API REST d'appareils de sécurité adaptables** > *version*.	Exemple de nom de fichier utilisé pour le logiciel API : asa-restapi-132-**lfbff-k8.SPA**. Pour installer l'API REST, consultez le guide de démarrage rapide de l'API.
	Logiciel ROMMON Choisissez votre *modèle* > **Logiciel Rommon pour ASA** > *version*.	Exemple de nom de fichier utilisé pour le logiciel ROMMON : asa5500-firmware-1108**.SPA**.

Modèle ASA	Emplacement de téléchargement	Progiciels
ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X et ASA 5555-X	http://www.cisco.com/go/asa-software	
	Logiciel ASA Choisissez votre *modèle* > **Logiciels sur châssis** > **Logiciel d'appareils de sécurité adaptables (ASA)** > *version*.	Exemple de nom de fichier utilisé pour le logiciel ASA : asa962-**smp-k8.bin**.
	Logiciel ASDM Choisissez votre *modèle* > **Logiciels sur châssis** > **Gestionnaire d'appareils de sécurité adaptables (ASA)** > *version*.	Exemple de nom de fichier utilisé pour le logiciel ASDM : asdm-762**.bin**.
	Logiciel API REST Choisissez votre *modèle* > **Logiciels sur châssis** > **Module d'extension API REST d'appareils de sécurité adaptables** > *version*.	Exemple de nom de fichier utilisé pour le logiciel API : asa-restapi-132-**lfbff-k8.SPA**. Pour installer l'API REST, consultez le guide de démarrage rapide de l'API.
	Paquet de périphérique ASA pour APIC (Cisco Application Policy Infrastructure Controller) Choisissez votre *modèle* > **Logiciels sur châssis** > **Paquets de périphériques ASA pour l'infrastructure axée sur les applications (ACI)** > *version*.	Pour APIC 1.2(7) et les versions ultérieures, choisissez le paquet Policy Orchestration avec Fabric Insertion ou le paquet Fabric Insertion seul. Exemple de nom de fichier utilisé pour le paquet de périphérique : asa-device-pkg-1.2.7.10**.zip**. Pour installer le paquet de périphérique ASA, consultez le chapitre « Importation d'un paquet de périphérique » du Guide de déploiement des services APIC de Cisco pour les couches 4 à 7.

Modèle ASA	Emplacement de téléchargement	Progiciels
ASA 5585-X	http://www.cisco.com/go/asa-software	
	Logiciel ASA Choisissez votre *modèle* > **Logiciels sur châssis** > **Logiciel d'appareils de sécurité adaptables (ASA)** > *version*.	Exemple de nom de fichier utilisé pour le logiciel ASA : asa962-**smp-k8.bin**.
	Logiciel ASDM Choisissez votre *modèle* > **Logiciels sur châssis** > **Gestionnaire d'appareils de sécurité adaptables (ASA)** > *version*.	Exemple de nom de fichier utilisé pour le logiciel ASDM : asdm-762**.bin**.
	Logiciel API REST Choisissez votre *modèle* > **Logiciels sur châssis** > **Module d'extension API REST d'appareils de sécurité adaptables** > *version*.	Exemple de nom de fichier utilisé pour le logiciel API : asa-restapi-132-**lfbff-k8.SPA**. Pour installer l'API REST, consultez le guide de démarrage rapide de l'API.
	Paquet de périphérique ASA pour APIC (Cisco Application Policy Infrastructure Controller) Choisissez votre *modèle* > **Logiciels sur châssis** > **Paquets de périphériques ASA pour l'infrastructure axée sur les applications (ACI)** > *version*.	Pour APIC 1.2(7) et les versions ultérieures, choisissez le paquet Policy Orchestration avec Fabric Insertion ou le paquet Fabric Insertion seul. Exemple de nom de fichier utilisé pour le paquet de périphérique : asa-device-pkg-1.2.7.10**.zip**. Pour installer le paquet de périphérique ASA, consultez le chapitre « Importation d'un paquet de périphérique » du Guide de déploiement des services APIC de Cisco pour les couches 4 à 7.

Modèle ASA	Emplacement de téléchargement	Progiciels
Firepower de la série 2100	http://www.cisco.com/go/asa-firepower-sw	
	Logiciels ASA, ASDM et FXOS Choisissez votre *modèle* > **Logiciel d'appareils de sécurité adaptables (ASA)(** > *version*.	Le paquet ASA comprend les logiciels ASA, ASDM et FXOS. Exemple de nom de fichier pour le paquet ASA : cisco-asa-fp2k.9.8.2**.SPA**.
	Logiciel ASDM (mise à niveau) Choisissez votre *modèle* > **Gestionnaire d'appareils de sécurité adaptables (ASA)** > *version*.	Utilisez cette image pour effectuer une mise à niveau vers une version ultérieure d'ASDM en utilisant votre ASDM actuel ou l'interface de ligne de commande d'ASA. Exemple de nom de fichier utilisé pour le logiciel ASDM : asdm-782**.bin**. **Remarque** Lorsque vous mettez à niveau le paquet de l'ASA, l'image ASDM de l'offre groupée remplace l'image du groupe ASDM précédent sur l'ASA, car elles portent le même nom (**asdm.bin**). Toutefois, si vous avez choisi manuellement une autre image ASDM que vous avez téléversée (par exemple, **asdm-782.bin**), vous continuez à utiliser cette image même après une mise à niveau groupée. Pour vous assurer d'exécuter une version compatible d'ASDM, vous devez soit mettre à niveau ASDM avant de mettre à niveau l'ensemble, soit reconfigurer l'ASA pour utiliser l'image ASDM fournie (**asdm.bin**) juste avant de mettre à niveau l'ensemble ASA.
ISA 3000	http://www.cisco.com/go/isa3000-software	
	Logiciel ASA Choisissez votre *modèle* > **Logiciel d'appareils de sécurité adaptables (ASA)(** > *version*.	Exemple de nom de fichier utilisé pour le logiciel ASA : asa962-**lfbff-k8.SPA**.
	Logiciel ASDM Choisissez votre *modèle* > **Gestionnaire d'appareils de sécurité adaptables (ASA)** > *version*.	Exemple de nom de fichier utilisé pour le logiciel ASDM : asdm-762**.bin**.
	Logiciel API REST Choisissez votre *modèle* > **Module d'extension API REST d'appareils de sécurité adaptables** > *version*.	Exemple de nom de fichier utilisé pour le logiciel API : asa-restapi-132-**lfbff-k8.SPA**. Pour installer l'API REST, consultez le guide de démarrage rapide de l'API.

Télécharger FXOS pour le Firepower 4100/9300

Les paquets FXOS pour les périphériques Firepower 4100/9300 sont disponibles sur le Site d'assistance et de téléchargement Cisco.

- Firepower 4100 : http://www.cisco.com/go/firepower4100-software
- Firepower 9300 : http://www.cisco.com/go/firepower9300-software

Pour trouver des progiciels FXOS, sélectionnez ou recherchez votre modèle d'appareil Firepower, puis accédez à la page de téléchargement de Firepower Extensible Operating System pour obtenir la version cible.

Remarque Si vous prévoyez d'utiliser l'interface de ligne de commande pour mettre à niveau FXOS, copiez le paquet de mise à niveau sur un serveur auquel Firepower 4100/9300 peut accéder en utilisant le protocole SCP, SFTP, TFTP ou FTP.

Tableau 14 : Paquets FXOS pour Firepower 4100/9300

Type de package	Ensemble
Image FXOS	fxos-k9.*version*.**SPA**
Récupération (démarrage)	fxos-k9-**kickstart**.*version*.**SPA**
Récupération (gestionnaire)	fxos-k9-**manager**.*version*.**SPA**
Récupération (système)	fxos-k9-**system**.*version*.**SPA**
Bases d'informations de gestion (MIB)	fxos-**mibs**-fp9k-fp4k.*version*.**zip**
Micrologiciel : Firepower 4100	fxos-k9-fpr4k-**firmware**.*version*.**SPA**
Micrologiciel : Firepower 9300	fxos-k9-fpr9k-**firmware**.*version*.**SPA**

Sauvegarder vos configurations

Nous vous recommandons de sauvegarder vos configurations et autres fichiers critiques avant d'effectuer la mise à niveau, en particulier s'il y a migration de configuration. Chaque système d'exploitation utilise une méthode différente pour effectuer les sauvegardes. Pour en savoir plus, consultez les guides de configuration d'ASA, d'ASDM, de gestion locale ASA FirePOWER, de Firepower Management Center et de FXOS.

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.