Cisco ASA 5580
Guide de démarrage

Version logicielle 8.3

Siège social aux États-Unis
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
États-Unis
http://www.cisco.com
Tél. : + 1 408 526-4000
800 553-NETS (6387)
Fax : + 1 408 527-0883

Numéro de commande client : DOC-78-19547-01
Numéro de référence du texte : 78-19547-01

Guide de démarrage de Cisco ASA 5580

TABLE DES MATIÈRES

CHAPITRE 1

Avant de commencer

Remarque Des traductions en français de ces documents sont régulièrement mises en ligne à la page : http://www.cisco.com/cisco/web/CA/fr/support/index.html

Utilisez le tableau ci-après pour trouver les étapes d'installation et de configuration requises pour votre implémentation du Serveur de sécurité adaptatif Cisco ASA 5505.

Pour effectuer l'action suivante...	Voir...
Installer le châssis	Chapitre 3, « Installation de l'ASA 5580 »
Connecter les câbles d'interface	Chapitre 3, « Installation de l'ASA 5580 »
Effectuer la configuration initiale du serveur de sécurité adaptatif	Chapitre 4, « Configuration du serveur de sécurité adaptatif » *Guide de configuration des serveurs de sécurité Cisco utilisant l'ASDM*

Pour effectuer l'action suivante...	Voir...
Configurer le serveur de sécurité adaptatif pour votre implémentation	Chapitre 5, « Scénario : configuration de connexions pour un client VPN AnyConnect de Cisco » Chapitre 6, « Scénario : connexions VPN SSL sans client » Chapitre 7, « Scénario : configuration du VPN site à site » Chapitre 8, « Scénario : configuration du VPN d'accès à distance IPsec »
Configurer les fonctionnalités facultatives et avancées	*Guide de configuration de la gamme Cisco ASA 5500 utilisant l'interface CLI*
Travailler sur le système au jour le jour	*Référence des commandes de la gamme Cisco ASA 5500* *Messages de journalisation système de la gamme Cisco ASA 5500* *Guide de configuration des serveurs de sécurité Cisco utilisant l'ASDM*

CHAPITRE 2

Optimisation du débit de l'ASA 5580

Le modèle Cisco ASA 5580 a été conçu pour fournir un débit maximal, lorsqu'il est configuré selon les instructions fournies dans ce chapitre.

Ce chapitre comprend les sections suivantes :

Interfaces réseau

Cette section comprend les rubriques suivantes :

À propos des interfaces réseau

L'ASA 5580 est doté de deux ports réseau Gigabit Ethernet intégrés et de neuf logements d'extension. Les ports réseau sont numérotés de 0 à 4, de haut en bas. Les numéros des logements d'extension sont incrémentés de droite à gauche.

Les deux ports Gigabit Ethernet intégrés sont utilisés pour la gestion et sont nommés Management0/0 et Management0/1.

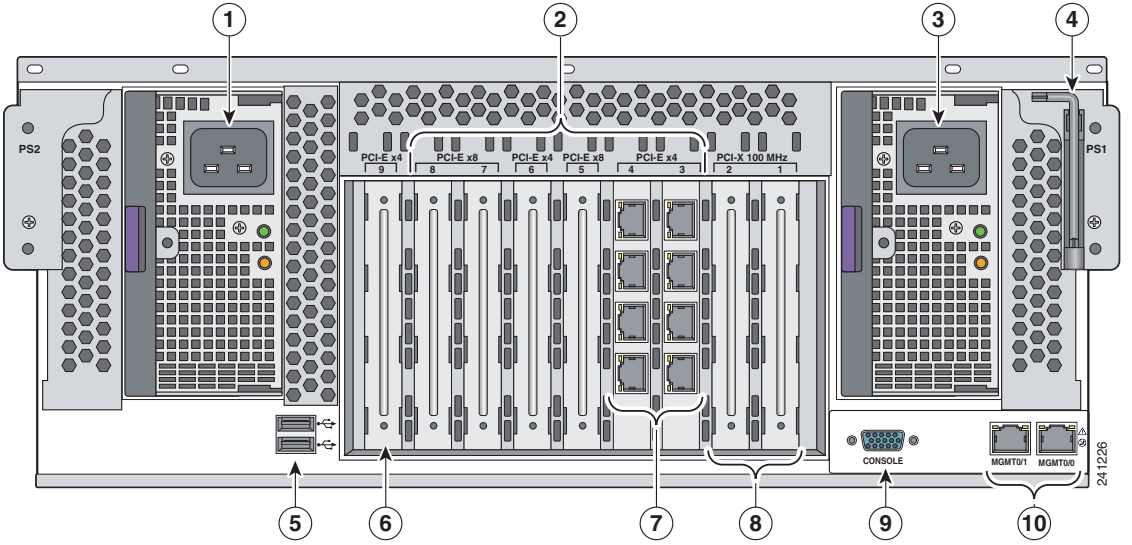
L'ASA 5580 comprend neufs logements d'extension d'interface. Les logements 1, 2 et 9 sont réservés. Le logement 1 est occupé par l'accélérateur de cryptographie et n'est pas destiné aux cartes d'interface réseau. Le logement 2 est réservé pour une utilisation ultérieure.

Les logements 3 à 8 peuvent être destinés aux cartes d'interface réseau prises en charge.

Le serveur de sécurité adaptatif présente deux ponts E/S et les logements E/S se connectent à l'un des deux bus. Les adaptateurs et les ports de gestion des logements 3, 4, 5 et 6 figurent sur le pont E/S 1 et les logements 7 et 8, sur le pont E/S 2.

La Figure 2-1 illustre les logements et les ports intégrés du ASA 5580.

Figure 2-1 Logements et ports intégrés de l'ASA 5580



1	Alimentation	**6**	Logement réservé
2	Logements d'extension d'interface	**7**	Exemple de logement occupé
3	Alimentation	**8**	Logement réservé
4	Tournevis Torx -15	**9**	Port de console
5	Ports USB	**10**	Ports de gestion

Cartes d'extension

Les logements 1, 2 et 9 sont réservés. Les logements 3 à 9 sont des logements PCI-Express.

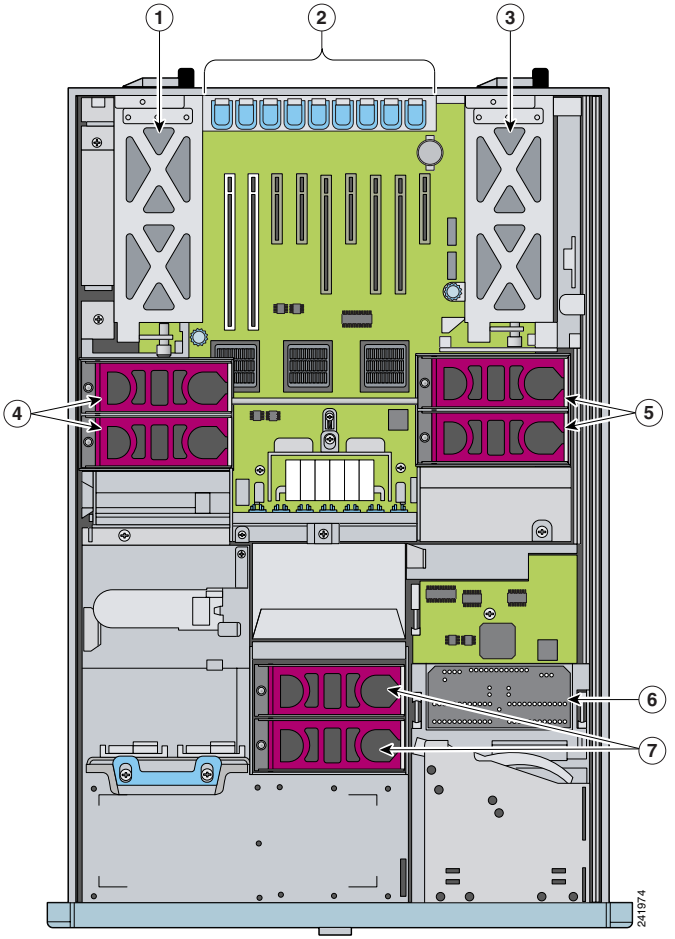
Le serveur de sécurité adaptatif est constitué de deux ponts E/S internes offrant une connectivité cuivre et fibre Gigabit Ethernet.

Les logements 5, 7 et 8 utilisent un bus haute-capacité (PCIe x8) et les logements 3, 4 et 6 utilisent un bus PCIe x4, pour les logements.

La Figure 2-2 illustre les logements d'extension d'interface disponibles sur l'ASA 5580.

Logement	Description
1	Logement PCI-X réservé, non enfichable à chaud, 64-bits/100-MHz
2	Logement PCI-X réservé, non enfichable à chaud, 64-bits/100-MHz
3	Logement d'extension PCI Express non enfichable à chaud x4
4	Logement d'extension PCI Express non enfichable à chaud x4
5	Logement d'extension PCI Express non enfichable à chaud x8
6	Logement d'extension PCI Express non enfichable à chaud x4
7	Logement d'extension PCI Express non enfichable à chaud x8
8	Logement d'extension PCI Express non enfichable à chaud x4
9	Logement d'extension PCI Express non enfichable à chaud x8

Figure 2-2 Logements d'extension d'interface



1, 3	Alimentation
4, 5, 7	Ventilateurs
6	Panneau de diagnostic

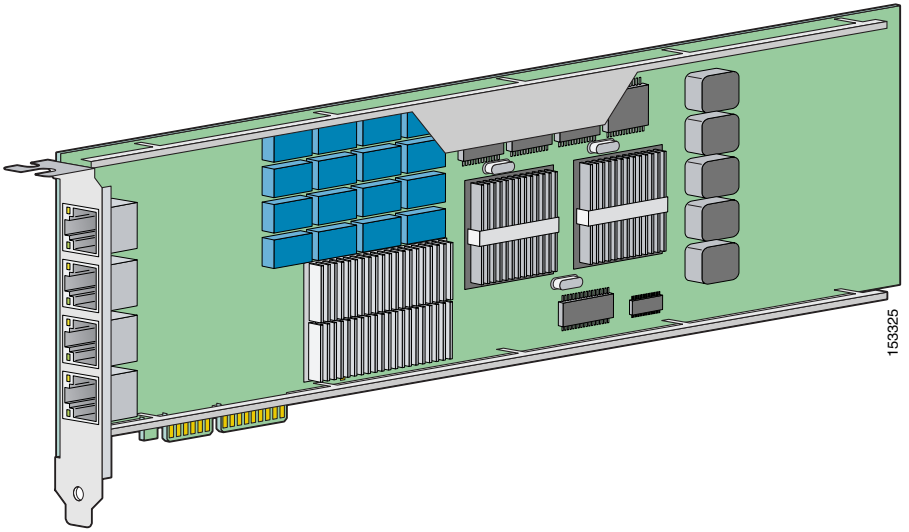
Cartes PCI prises en charge

L'ASA 5580 prend en charge les cartes PCI suivantes :

- Carte PCI cuivre Gigabit Ethernet 4 ports

  Fournit quatre interfaces 10/100/1000BASE-T, qui autorisent un maximum de 24 interfaces Gigabit Ethernet. La Figure 2-3 illustre la carte d'interface Gigabit Ethernet.

Figure 2-3 Carte PCI cuivre Gigabit Ethernet 4 ports

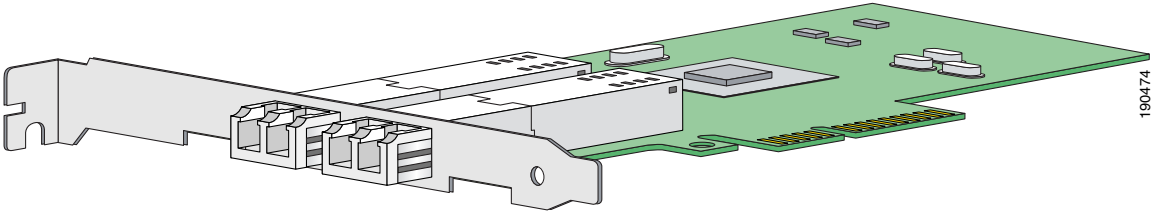


- Carte PCI fibre 10-Gigabit Ethernet 2 ports

  Fournit deux interfaces 1000BASE-SX (fibre) (autorisant un maximum de 12 interfaces fibre 10-Gigabit Ethernet, dans un châssis totalement occupé).

  Les ports de carte requièrent un câble fibre optique multimodes muni d'un connecteur LC, pour se connecter à l'interface SX du capteur. La Figure 2-4 illustre la carte PCI fibre 10-Gigabit Ethernet 2 ports

Figure 2-4 Carte PCI fibre 10-Gigabit Ethernet 2 ports



- Carte PCI fibre Gigabit Ethernet 4 ports

  Fournit quatre interfaces 1000BASE-SX (fibre) (autorisant un maximum de 24 interfaces fibre 10-Gigabit Ethernet, dans un châssis totalement occupé).

  Les ports de carte requièrent un câble fibre optique multimodes muni d'un connecteur LC, pour se connecter à l'interface SX du capteur.

Remarque Les cartes PCI fibre Gigabit Ethernet avec connexion optique courte portée (SR) peuvent supporter une distance de 300 mètres. Ces cartes sont conçues pour prendre en charge de courtes distances sur un câble fibre multimodes déployé dont la portée est comprise entre 26 et 82 mètres (85 et 270 pieds), en fonction du type de câble utilisé.
Elles peuvent également prendre en charge des distances de 300 mètres (980 pieds) sur le nouveau câble fibre multimodes OM3 50 µm 2000 MHz·km. Le transmetteur peut être implémenté avec un laser à cavité verticale et à émission par la surface (VCSEL-Vertical Cavity Surface Emitting Laser).

Optimisation des performances

Pour optimiser le débit du trafic, assurez-vous que le flux du trafic et la configuration matérielle du serveur de sécurité adaptatif correspondent aux directives suivantes :

- Les performances optimales sont atteintes lorsque le trafic entre et sort des ports sur le même adaptateur ou entre et sort des ports sur des adaptateurs gérés par le même pont E/S.

  L'ASA 5580 présente deux ponts E/S et les logements E/S se connectent à l'un des deux bus E/S. Les adaptateurs des logements 3, 4, 5 et 6 figurent sur un pont E/S et les logements 7 et 8, sur l'autre pont E/S.

Vous atteindrez des performances optimales si le trafic ne traverse pas les deux ponts E/S. Plus précisément, le trafic doit circuler entre des ports placés sur différents adaptateurs d'un même pont E/S.

Pour obtenir des performances optimales, configurez le dispositif de sorte que le trafic traverse les ports placés sur les adaptateurs,des logements 7 et 8. Si vous utilisez une carte PCI à fibre optique 10 Gigabit Ethernet à deux ports, installez-la dans le logement 7. Configurez le dispositif de sorte que le trafic supplémentaire traverse les ports placés sur les adaptateurs des logements 3 à 6.

Pour obtenir un exemple de configuration dans laquelle le trafic traverse les ports des logements 7 et 8 du pont d'E/S haute capacité (PCIE x8), reportez-vous à la Figure 2-5.

- Si vous utilisez des adaptateurs 10 Gigabit Ethernet, qui requièrent des performances optimales, placez les adaptateurs dans des logements du pont d'E/S haute capacité (PCIe X8) : logement 5, logement 7 et logement 8.

Remarque Un adaptateur et un port 10 Gigabit Ethernet sont capables de fournir 10 Gigabit Ethernet en duplex intégral sur un port associé au profil de trafic approprié. La bande passante de bus limite à une valeur de 16 Gbit/s en duplex intégral les performances des deux ports 10 Gigabit Ethernet d'un même adaptateur.

- Les adaptateurs à quatre ports peuvent être placés dans n'importe quel logement, mais le bus peut constituer un goulot d'étranglement si chaque port a un trafic de 1 Gigabit, en mode duplex intégral. La bande passante du bus sur le bus à vitesse normale limite la bande passante agrégée sur un adaptateur à moins de 8 Gbits/s.

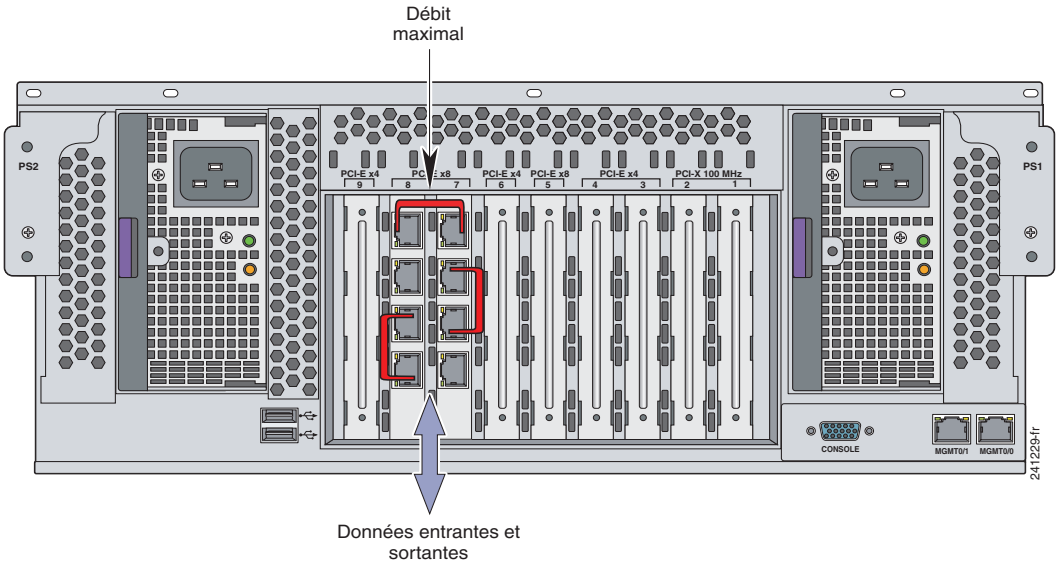
Remarque Pour voir le débit du trafic sur chaque bus, vous pouvez utiliser la commande **show io-bridge**. Pour obtenir plus d'informations sur l'utilisation de cette commande, consultez le document *Référence des commandes de la gamme Cisco ASA 5500*.

- Tenez compte des indications suivantes concernant les boucles des ports 10 Gigabit et 1 Gigabit :
  - Les ports 10 Gigabit sont dotés de quatre boucles RX et de quatre boucles TX, qui nécessitent un équilibrage de la charge. Les ports 1 Gigabit sont dotés d'une boucle RX et d'une boucle TX uniquement ; l'équilibrage de la charge n'est donc pas nécessaire.

  - Les mémoires tampon des boucles RX subissent un équilibrage de la charge déterminé par l'algorithme src-dst-ip-port. Il est impossible de modifier l'algorithme.
  - Pour bénéficier d'un équilibrage approprié de la charge, les quatre boucles RX des ports 10 Gigabit nécessitent 64 connexions.
- Les ports de gestion peuvent traverser le trafic, en supprimant la commande **management-only**. Cependant, les ports uniquement dédiés à la gestion n'ont pas été optimisés pour traverser le trafic de données et ils ne seront pas aussi performants que les ports des adaptateurs.

Pour voir un exemple de trafic configuré pour transiter par les ports des logements 7 et 8 sur le pont E/S haute-capacité (PCIe x8), reportez-vous à la Figure 2-5.

Figure 2-5 Exemple de flux de trafic permettant d'obtenir des performances optimales



Étapes suivantes

Passez au Chapitre 3, « Installation de l'ASA 5580 »

CHAPITRE 3

Installation de l'ASA 5580

Avertissement Lisez les mises en garde figurant dans le document *Informations relatives à la conformité et à la sécurité, pour la gamme Cisco ASA 5500* et respectez les consignes de sécurité pendant l'installation.

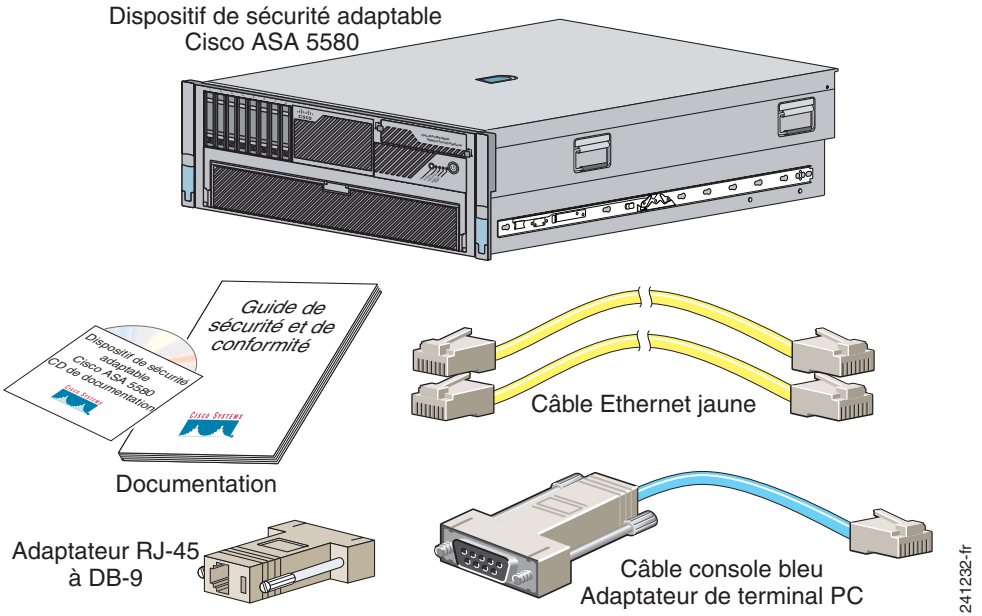
Attention **Seul le personnel spécialisé et qualifié doit installer, remplacer ou faire l'entretien de cet équipement.** Énoncé 49

Ce chapitre présente le serveur de sécurité adaptatif et décrit les procédures d'installation et de montage du serveur de sécurité adaptatif sur bâti. Ce document comprend les sections suivantes :

Vérification du contenu du coffret

Vérifiez le contenu du coffret illustré à la Figure 3-1. Assurez-vous que vous avez reçu tous les éléments nécessaires à l'installation des produits de la gamme ASA 5580.

Figure 3-1 Contenu du coffret ASA 5580



En plus des éléments illustrés à la Figure 3-1, le serveur de sécurité adaptatif de la gamme ASA 5580 est fourni avec un système de rails en kit. Le kit de système de rails contient les éléments suivants :

- Une paire d'assemblages à glissières
- Deux rails de châssis
- Quatre bandes Velcro
- Six attaches autobloquantes
- Un bras de maniement des câbles

- Un sachet contenant différentes pièces (vis, etc.)
- Un support de blocage du bras de maniement des câbles

Installation du châssis

Cette section décrit comment monter sur bâti et installer le serveur de sécurité adaptatif.

Attention **Pour prévenir les blessures corporelles lors de la fixation ou de l'entretien de cette unité dans un bâti, vous devez prendre des précautions spéciales afin de vous assurer que le système demeure stable. Les consignes suivantes sont fournies dans le but d'assurer votre sécurité.**

Les informations ci-après peuvent vous aider à planifier l'installation de l'équipement sur bâti :

- Conservez un espace suffisant autour du bâti pour la maintenance.
- Lorsque vous montez un périphérique dans un bâti fermé, assurez-vous que la ventilation est adéquate. Un bâti fermé ne doit jamais être surchargé. Assurez-vous que le bâti n'est pas surchargé car chaque unité génère de la chaleur.
- Lorsque vous montez un périphérique dans un bâti ouvert, assurez-vous que le cadre du bâti ne bloque pas les orifices d'entrée et d'évacuation d'air.
- Si le bâti contient une seule unité, montez-la au fond du bâti.
- Si le bâti est partiellement rempli, chargez-le en commençant par le bas, en prenant soin de placer les composants les plus lourds au fond du bâti.
- Si des dispositifs de stabilisation sont fournis avec le bâti, installez-les avant de monter l'unité sur le bâti ou d'effectuer une maintenance.

Attention **Avant d'exécuter l'une des procédures suivantes, assurez-vous que l'alimentation est hors tension. (CA ou CC.) Pour ce faire, repérez le disjoncteur sur le panneau de commande du circuit CC, placez-le dans la position OFF, puis placez la poignée de commutation du disjoncteur du circuit dans la position OFF.**

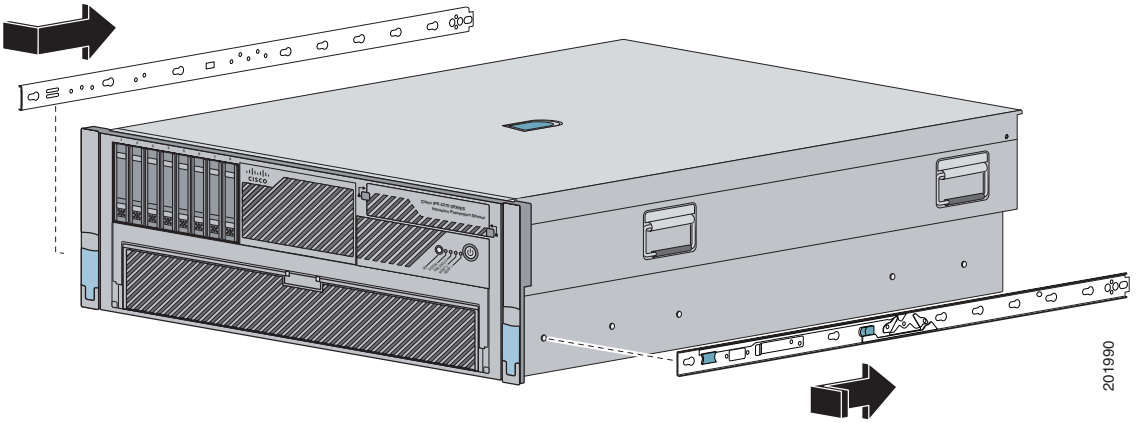
Montage sur bâti du châssis

Attention **Pour prévenir les blessures corporelles lors de la fixation ou de l'entretien de cette unité dans un bâti, vous devez prendre des précautions spéciales pour vous assurer que le système demeure stable. Les consignes suivantes sont fournies dans le but d'assurer votre sécurité :**
Cette unité doit être fixée au fond du bâti s'il s'agit de la seule unité du bâti.
Lorsque vous fixez cette unité dans un bâti partiellement rempli, chargez ce dernier en commençant par le fond, jusqu'en haut, en prenant soin de placer les composants les plus lourds au fond du bâti.
Si des dispositifs de stabilisation sont fournis avec le bâti, installez-les avant de monter l'unité sur le bâti ou d'effectuer une maintenance. Énoncé 1006
Cette procédure requiert au moins deux personnes pour placer le serveur de sécurité adaptatif sur les assemblages à glissières avant de le pousser dans le bâti.

Pour installer le serveur de sécurité adaptatif dans le bâti, procédez comme suit :

Étape 1 Fixez le rail latéral du châssis au serveur de sécurité adaptatif en alignant le rail du châssis sur le goujon du serveur de sécurité adaptatif. Insérez le rail latéral du châssis sur le goujon en appuyant, puis faites glisser le rail latéral du châssis en arrière jusqu'à enclenchement, comme illustré à la Figure 3-2.

Figure 3-2 Fixation du rail latéral du châssis

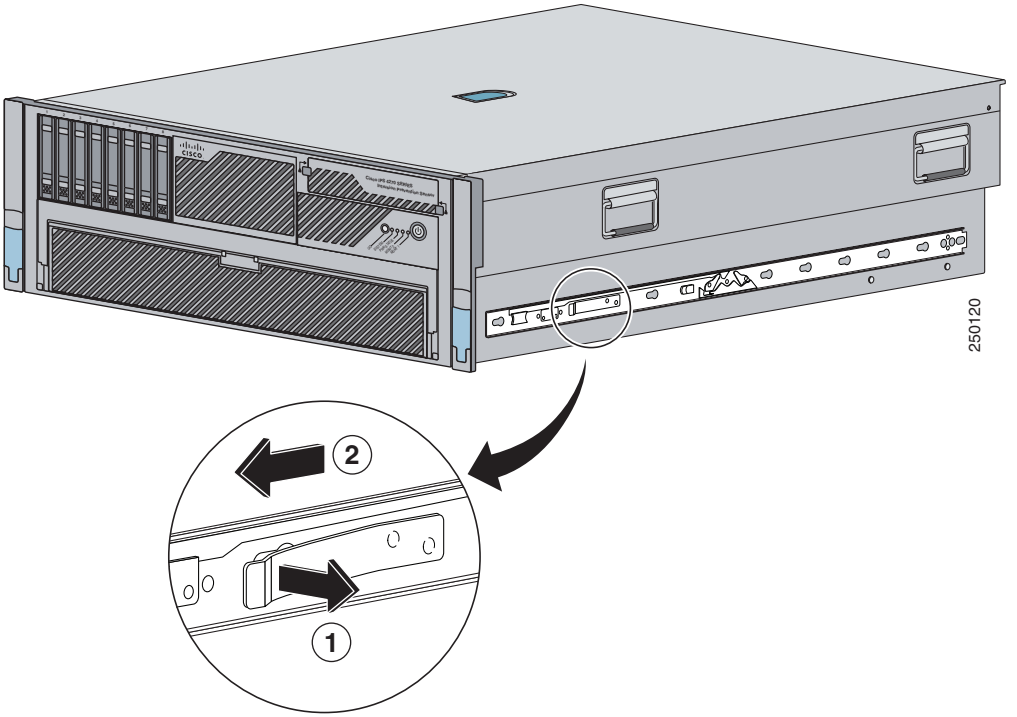


Remarque L'extrémité conique du rail latéral du châssis doit se trouver à l'arrière du serveur de sécurité adaptatif. Le rail latéral du châssis est maintenu en place grâce au verrou intérieur.

Étape 2 Répétez l'étape 1 pour chaque rail latéral du châssis.

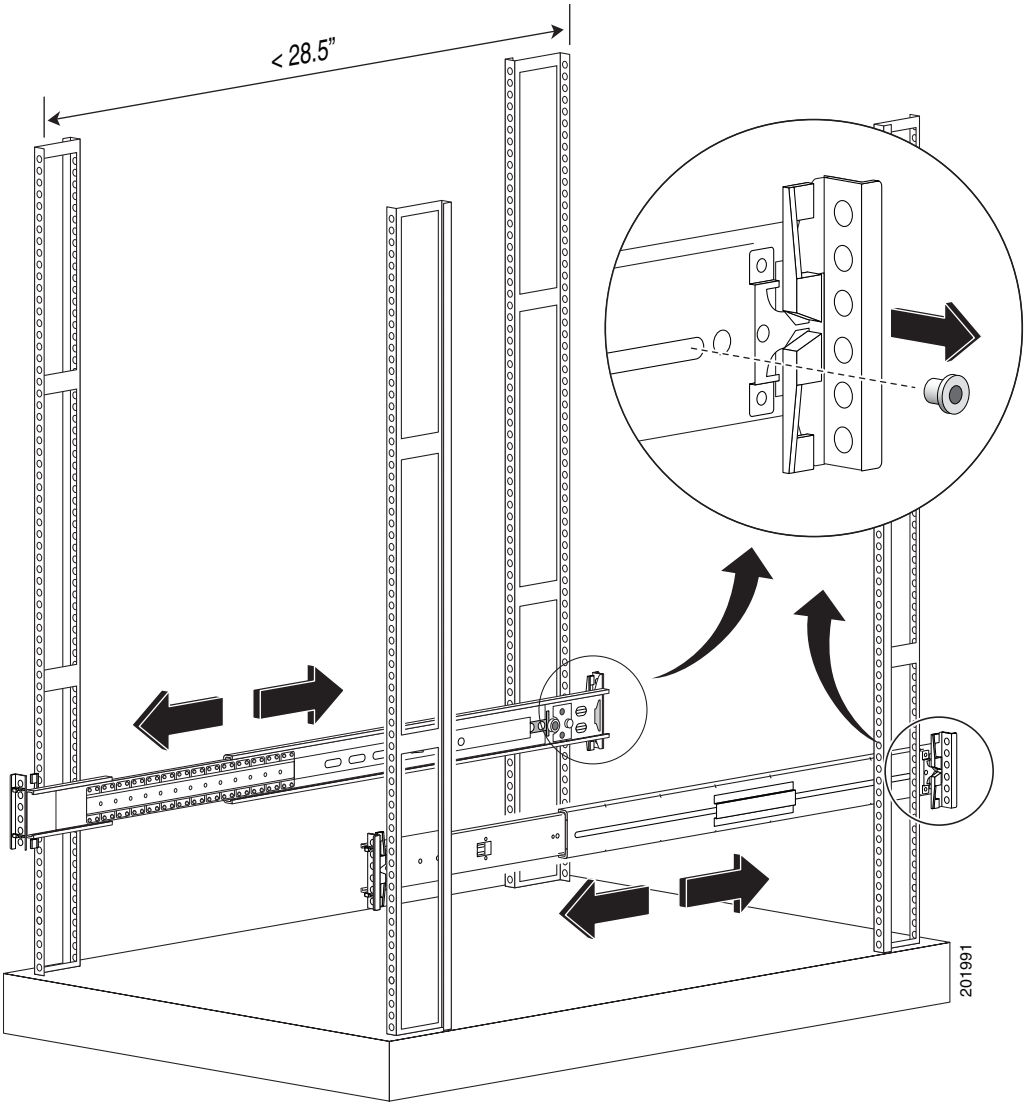
Étape 3 Pour retirer le rail latéral du châssis, soulevez le verrou, puis faites glisser le rail vers l'avant, comme illustré à la Figure 3-3.

Figure 3-3 Retrait du rail latéral du châssis



Étape 4 Si vous installez le serveur de sécurité adaptatif dans un bâti peu profond, c'est-à-dire, de moins de 72,39 cm (28,5 po), retirez la vis se trouvant à l'intérieur de l'assemblage à glissières avant de passer à l'étape 5, comme illustré à la Figure 3-4.

Figure 3-4 Vis située à l'intérieur de l'assemblage à glissières



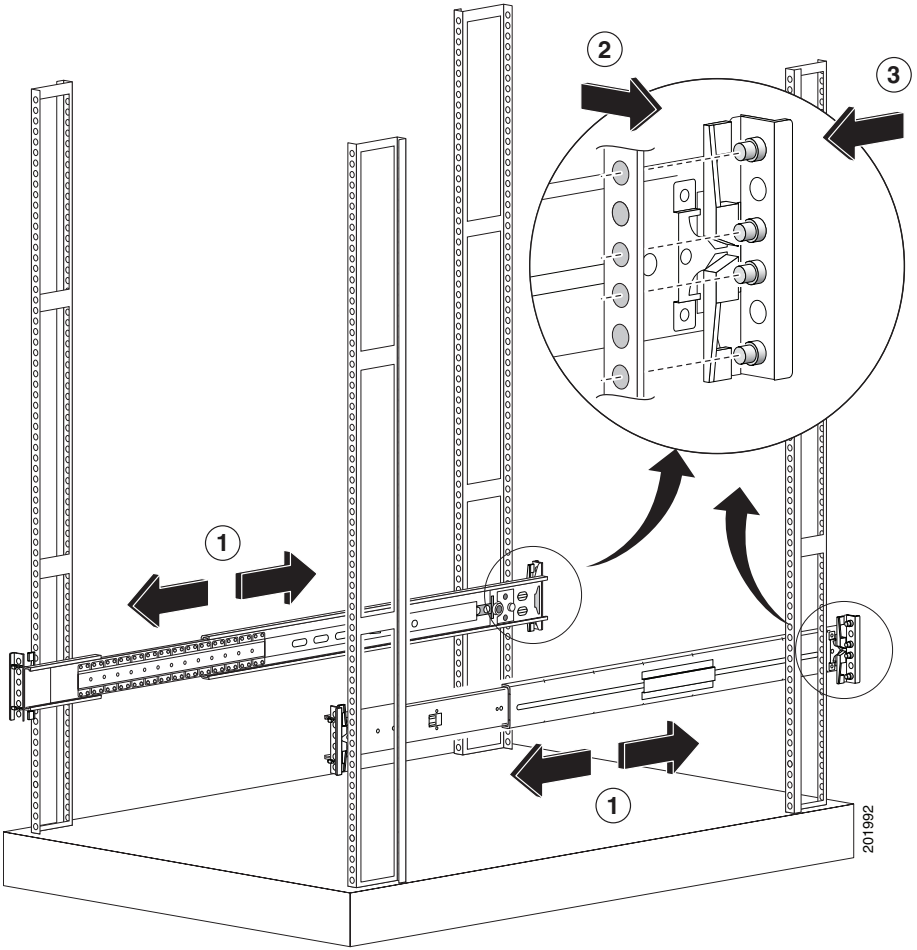
Étape 5 Fixez les assemblages à glissières sur le bâti, comme illustré à la Figure 3-5.

Pour les bâtis à trous de montage carrés et ronds :

a. Alignez les goujons sur l'assemblage à glissières en plaçant les trous de montage à l'intérieur du bâti et emboîtez-les.

b. Ajustez l'assemblage à glissières en longueur pour qu'il s'ajuste au bâti. Le verrou à ressort verrouille l'assemblage à glissières en place.

Figure 3-5 Fixation de l'assemblage à glissières



c. Répétez ce processus pour chaque assemblage à glissières.

Assurez-vous que les assemblages à glissières sont alignés les uns par rapport aux autres dans le bâti.

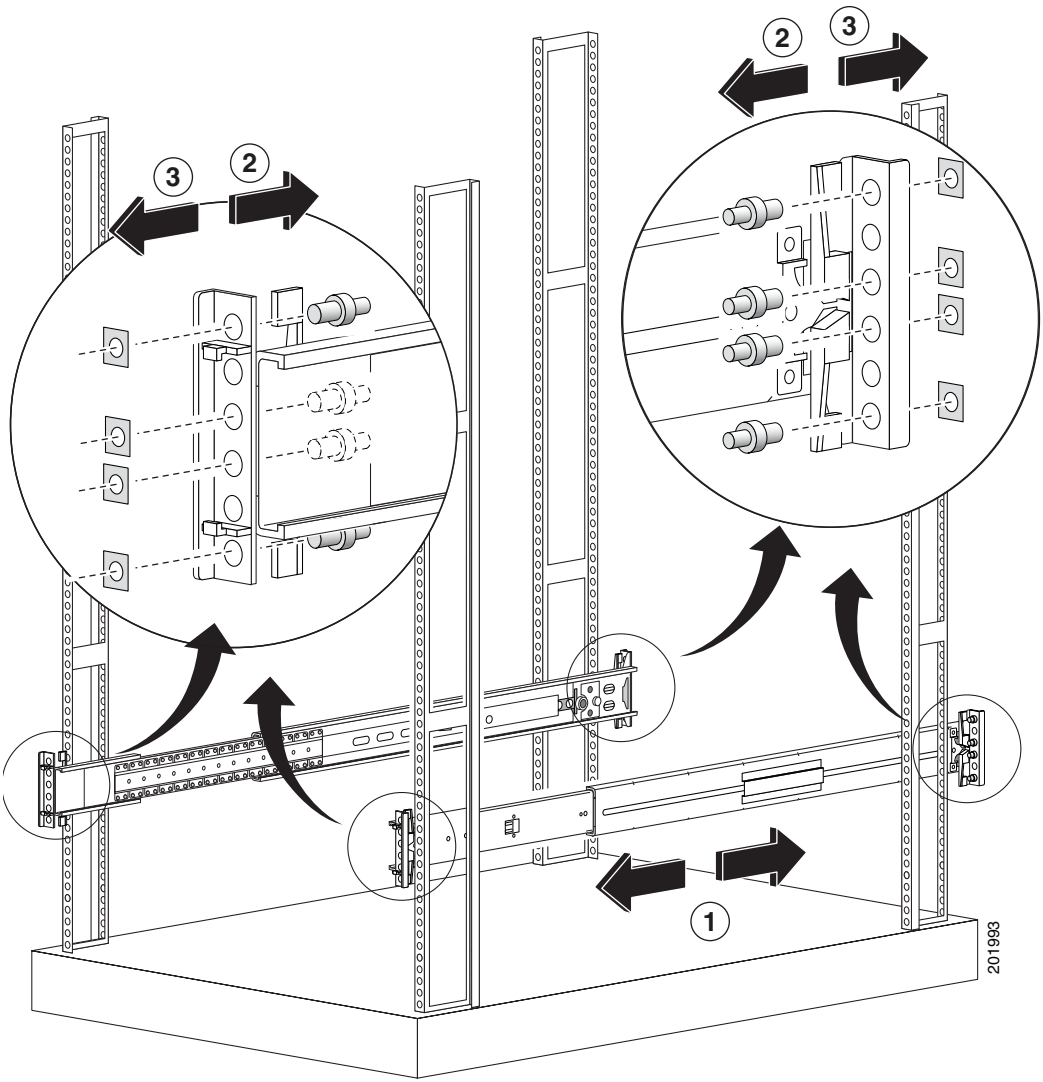
d. Soulevez le verrou à ressort pour libérer l'assemblage à glissières si vous devez le repositionner.

Pour les bâtis à trous de montage filetés :

a. Retirez les huit goujons à trous de montage carrés ou ronds sur chaque assemblage à glissières à l'aide d'un tournevis standard, comme illustré à la Figure 3-6.

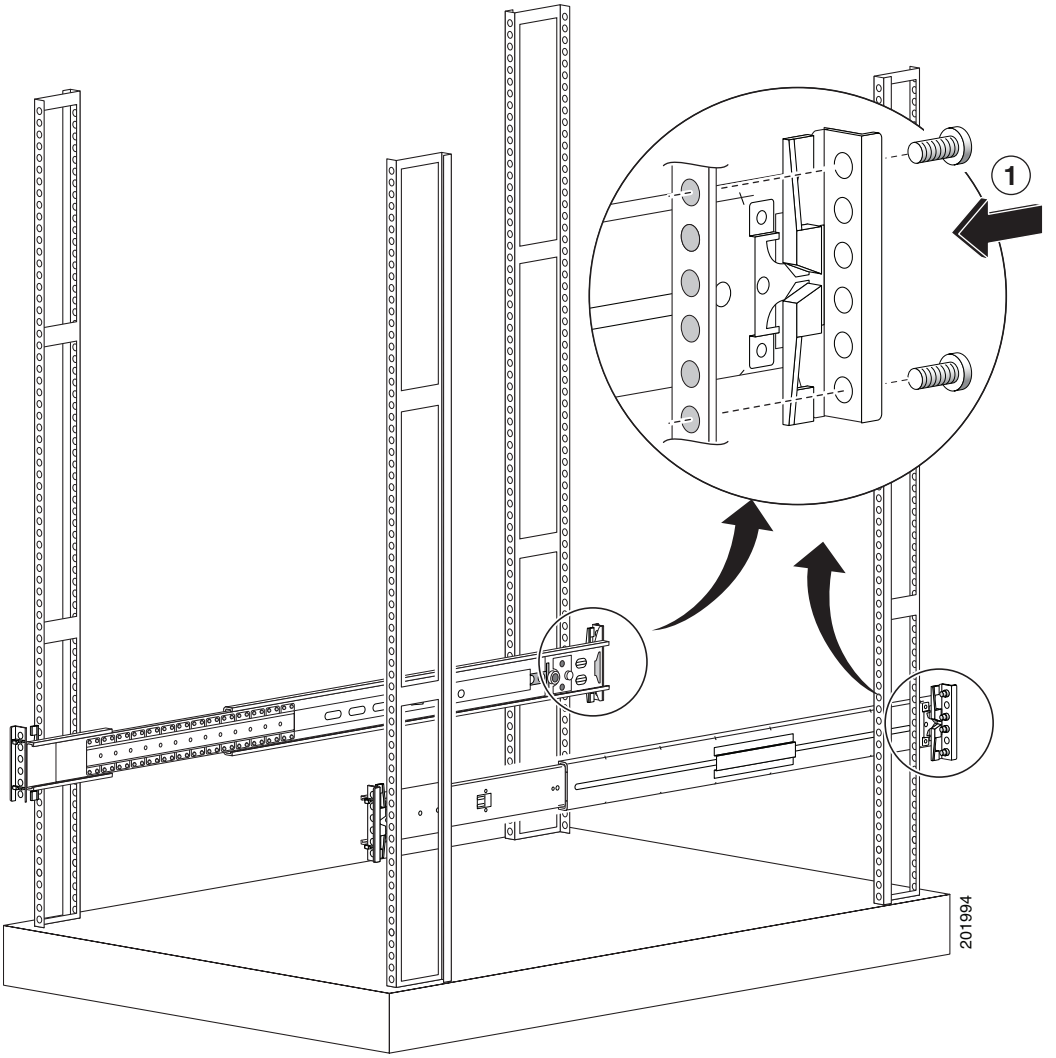
Remarque Vous devrez peut-être utiliser des pinces pour tenir l'écrou de retenue.

Figure 3-6 Fixation dans des bâtis à trous de montage filetés



b. Alignez le support de l'assemblage à glissières sur les trous de montage du bâti, installez deux vis (en haut et en bas) sur chaque extrémité de l'assemblage à glissières, comme illustré à la Figure 3-7.

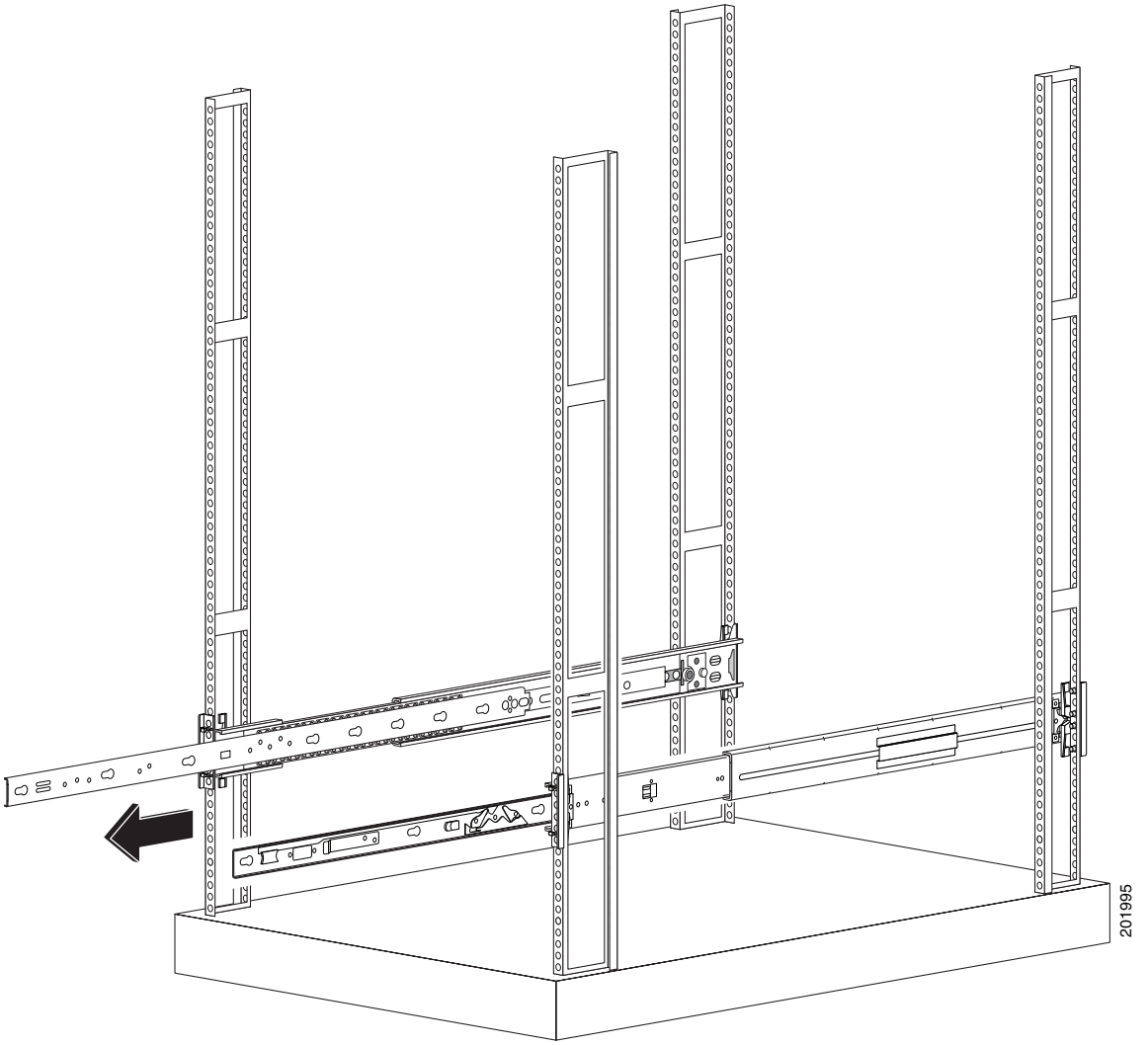
Figure 3-7 Alignement du support



c. Répétez ce processus pour chaque assemblage à glissières.

Étape 6 Étendez les assemblages à glissières hors du bâti, comme illustré à la Figure 3-8.

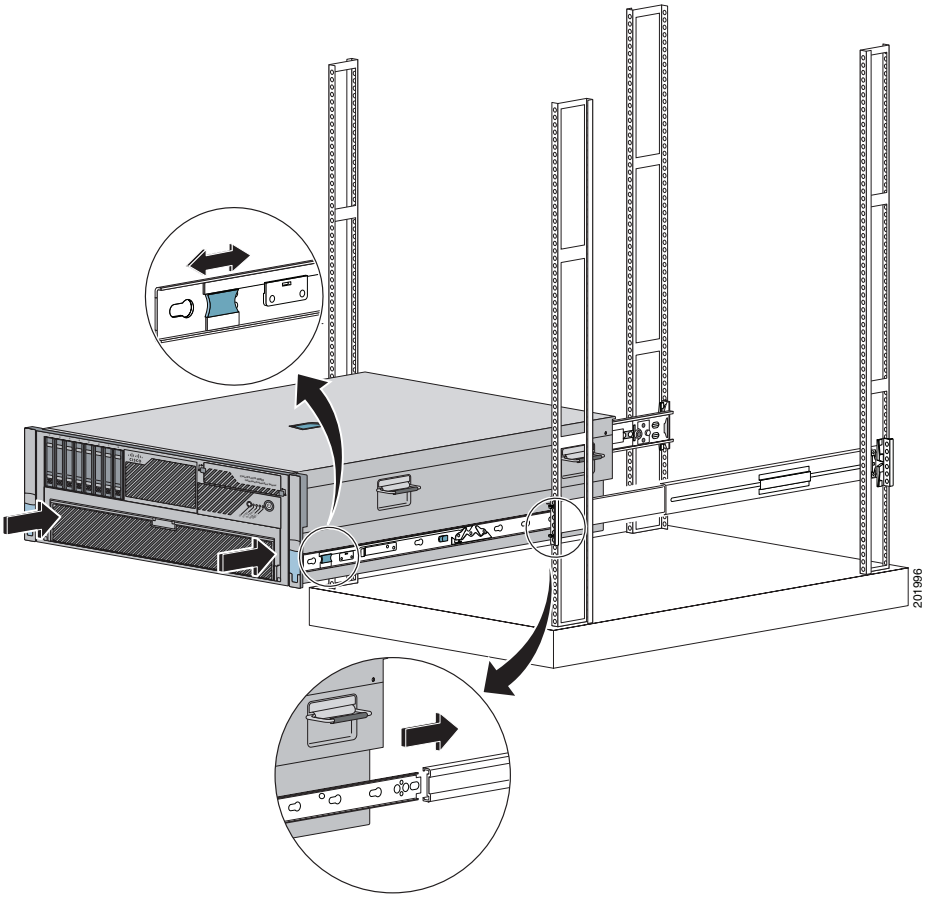
Figure 3-8 Assemblages à glissières en extension



Étape 7 Alignez les rails latéraux du châssis du serveur de sécurité adaptatif sur l'assemblage à glissières de chaque côté du bâti, dégagez la languette bleue (soit en la tirant vers l'avant, soit en la repoussant), puis appuyez avec précaution sur le serveur de sécurité adaptatif pour le remettre en place, comme illustré à la Figure 3-9.

Attention **Lorsque vous installez un serveur de sécurité adaptatif dans un bâti vide, vous devez tenir le serveur de sécurité adaptatif par sa front panel jusqu'à ce que les languettes latérales bleues soient activées et que le serveur de sécurité adaptatif soit entièrement inséré dans le bâti, sinon le bâti peut basculer.**

Figure 3-9 Alignement des rails latéraux du châssis



Avertissement Placez le serveur de sécurité adaptatif parallèlement au sol lorsque vous l'insérez dans les rails. Si vous inclinez le serveur de sécurité adaptatif vers le haut ou vers le bas, vous risquez d'endommager les rails.

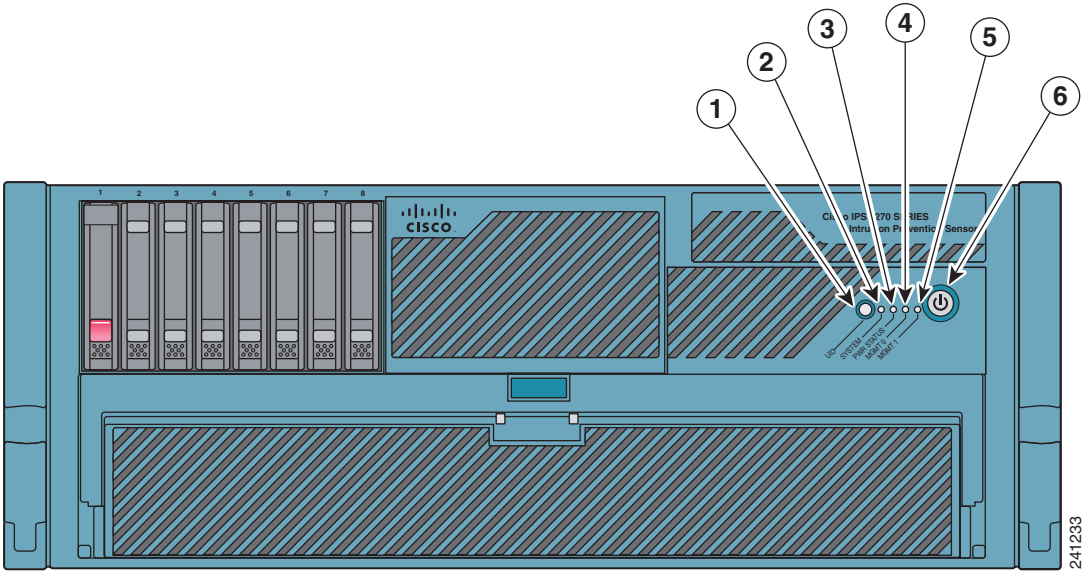
Ports et voyants DEL

Cette section décrit le panneau avant et arrière. Elle comprend les rubriques suivantes :

Voyants DEL de la front panel

La Figure 3-10 illustre les voyants DEL de la front panel du serveur de sécurité adaptatif.

Figure 3-10 Vue de face



1	DEL actif	**4**	DEL Management 0/0
2	DEL système	**5**	DEL Management 0/1
3	DEL d'indication d'état	**6**	Alimentation

Le Tableau 3-1 décrit les commutateurs et indicateurs situés en front panel de l'ASA 5580.

Tableau 3-1 Commutateurs et indicateurs situés en front panel

Indicateur	Description
Actif[1]	Indique l'état de basculement actif/veille du châssis : • Allumé - basculement actif • Éteint - état de veille
Indicateur système	Indique l'état de santé du système interne : • Vert - système actif • Orange clignotant - état de santé du système dégradé • Rouge clignotant - état de santé du système critique • Éteint - système désactivé
Indicateur d'état de l'alimentation	Indique l'état de l'alimentation : • Vert - sous tension • Orange clignotant - état de santé de l'alimentation dégradé • Rouge clignotant - état de santé de l'alimentation critique • Éteint - hors tension
Indicateur MGMT0/0	Indique l'état du port de gestion : • Vert - connexion au réseau • Vert clignotant - connexion avec activité sur le réseau • Éteint - aucune connexion réseau

Tableau 3-1 Commutateurs et indicateurs situés en front panel (suite)

Indicateur	Description
Indicateur MGMT0/1	Indique l'état du port de gestion : • Vert - connexion au réseau • Vert clignotant - connexion avec activité sur le réseau • Éteint - aucune connexion réseau
Commutateur et indicateur d'alimentation	Met l'alimentation sous ou hors tension : • Orange - le système est alimenté et en mode veille • Vert - le système est alimenté et activé • Éteint - le système est hors tension

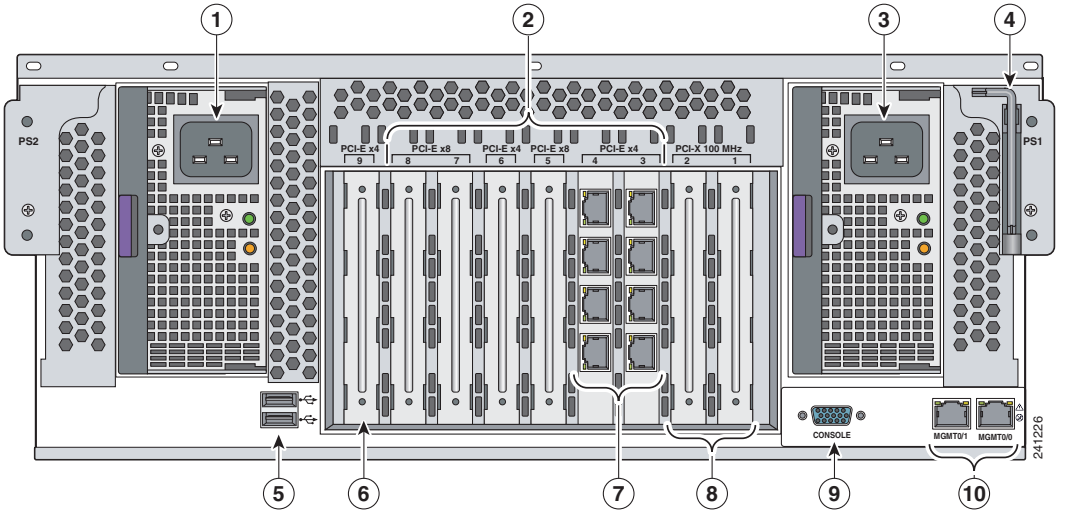
1. Sur un périphérique autonome, ce bouton est toujours allumé. Dans le cas de paires actif/veille, il est allumé pour l'unité active et éteint pour l'unité en veille. Dans le cas de paires actif/actif, il est allumé pour toute unité d'un groupe de basculement actif. Par ailleurs, lorsque le logiciel du système active l'éclairage du bouton (car il est actif ou autonome), appuyer sur ce bouton n'aura aucun effet. Il restera allumé. Lorsque le logiciel du système désactive l'éclairage du bouton, vous pourrez l'allumer en appuyant dessus. Si vous appuyez de nouveau sur ce bouton, il s'éteindra de nouveau.

Pour obtenir plus d'informations sur le port de gestion, reportez-vous à section relative à la commande **management-only** dans le document *Référence des commandes de la gamme Cisco ASA 5500.*

Ports et voyants DEL du panneau arrière

La Figure 3-11 illustre les ports et voyants DEL du panneau arrière.

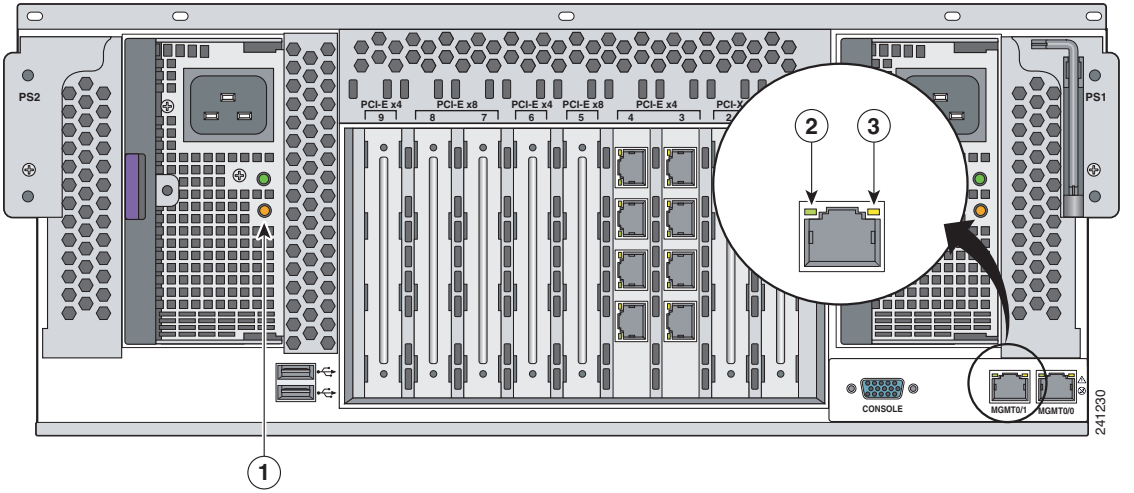
Figure 3-11 Caractéristiques du panneau arrière



1	Alimentation	**6**	Logement réservé
2	Logements d'extension d'interface	**7**	Exemple d'un logement occupé
3	Alimentation	**8**	Logement réservé
4	Tournevis Torx T-15	**9**	Port de console
5	Ports USB	**10**	Ports de gestion

La Figure 3-12 illustre les indicateurs d'activité sur les ports Ethernet, avec deux indicateurs par port et les indicateurs d'alimentation.

Figure 3-12 Voyants DEL du panneau arrière



1	Alimentation	**2**	Indicateur de liaison
3	Indicateur d'activité		

Le Tableau 3-2 décrit les indicateurs du port Ethernet. Le comportement des indicateurs du port varie en fonction du type de port (port de gestion, port d'une carte interface Gigabit Ethernet, port d'une carte d'interface fibre 10 Gigabit Ethernet ou port d'une carte d'interface fibre Gigabit Ethernet).

Tableau 3-2 Indicateurs du port Ethernet

Indicateur	Description
Gigabit Ethernet	Vert (supérieur) : connexion au réseau Vert clignotant (supérieur) : connexion avec activité sur le réseau Orange (inférieur) : vitesse 1000 Vert (inférieur) : vitesse 100 Éteint (inférieur) : vitesse 10
Fibre 10 Gigabit Ethernet (un voyant DEL)	Vert : connexion au réseau Vert clignotant : connexion avec activité sur le réseau
Fibre Gigabit Ethernet (un voyant DEL)	Vert : connexion au réseau Vert clignotant : connexion avec activité sur le réseau
Port de gestion	Vert (droit) : connexion au réseau Vert clignotant (gauche) : connexion avec activité sur le réseau **Remarque** L'indicateur des ports de gestion allume un voyant DEL vert quelle que soit la vitesse négociée (10/100/1000) ; cependant, les cartes d'interface Gigabit Ethernet allument un voyant DEL orange lorsqu'une liaison de 1 000 Mbits/s est négociée.

Le Tableau 3-3 décrit les indicateurs d'alimentation.

Tableau 3-3 Indicateurs d'alimentation

Indicateur de panne 1 Orange	Indicateur d'alimentation 2 Vert	Description
Éteint	Éteint	Pas d'alimentation CA pour aucune des alimentations
Clignotement	Éteint	Panne d'alimentation (sur courant)
Allumé	Éteint	Aucune alimentation CA pour cette alimentation
Éteint	Clignotement	• Présence d'alimentation CA • Mode veille
Éteint	Allumé	Normal

Connexion des câbles d'interface

Cette section décrit comment connecter les câbles appropriés aux ports de console, de gestion, cuivre et fibre Ethernet.

Pour connecter les câbles aux interfaces réseau, procédez comme suit :

Étape 1 Placez le châssis sur une surface plate et stable ou dans un bâti (si vous le montez sur bâti).

Étape 2 Connexion au port de gestion.

Le serveur de sécurité adaptatif dispose d'une interface dédiée pour la gestion des périphériques appelée port Management0/0. Les ports de gestion (port Management0/0 et port Management 0/1) sont des interfaces Fast Ethernet. Ils sont semblables à un port de console, mais ils acceptent uniquement un trafic destiné « to-the-box » (contrairement à un trafic « through-the-box »). Management0/0 (MGMT0/0) est le port de commande et de contrôle.

Remarque Vous pouvez configurer n'importe quelle interface de façon à ce qu'elle soit uniquement une interface de gestion à l'aide de la commande **management-only**. Vous pouvez également désactiver le mode de configuration management-only à partir de l'interface de gestion. Pour obtenir plus d'informations sur cette commande, reportez-vous à la commande **management-only** décrite dans le document *Référence des commandes de la gamme Cisco ASA 5500*.

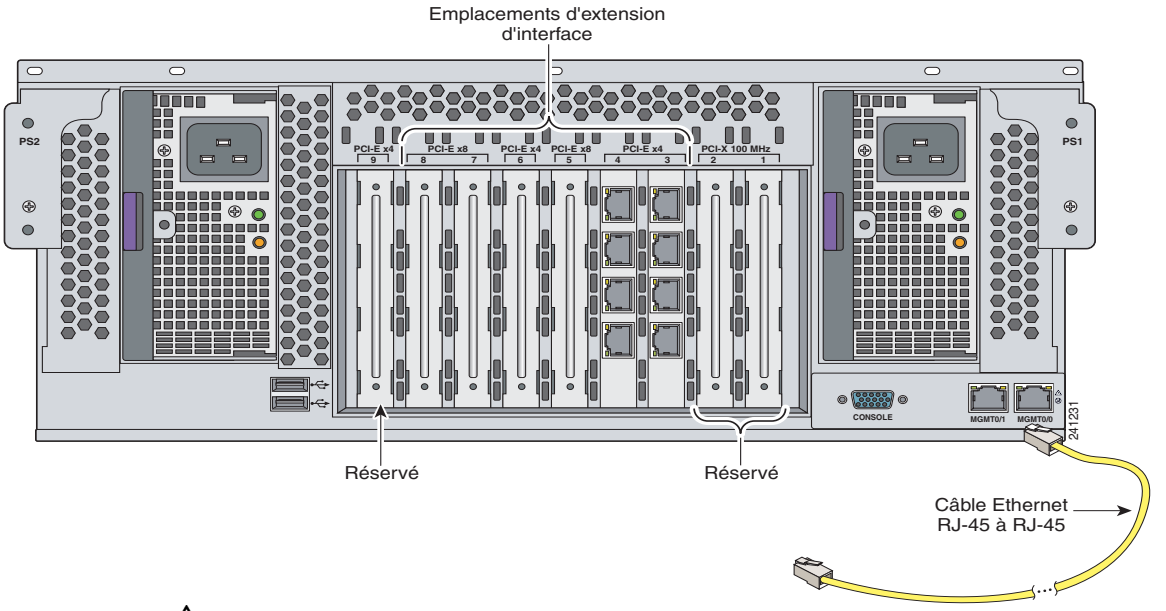
a. Repérez un câble Ethernet doté d'un connecteur RJ-45 à chaque extrémité.

b. Connectez un connecteur RJ-45 au port Management0/0, comme illustré à la Figure 3-13.

c. Connectez l'autre extrémité du câble Ethernet au port Ethernet de votre ordinateur ou à votre réseau de gestion.

Remarque Lorsque vous connectez un ordinateur directement au port de gestion du serveur de sécurité adaptatif, utilisez un câble Ethernet croisé. Lorsque vous connectez un ordinateur au serveur de sécurité adaptatif via un concentrateur ou un commutateur, utilisez un câble Ethernet direct pour connecter le concentrateur ou le commutateur au port de gestion du serveur de sécurité adaptatif.

Figure 3-13 Connexion au port de gestion



Avertissement Les ports de console et de gestion sont des ports administratifs privilégiés. Le fait de les connecter à un réseau non fiable peut engendrer des problèmes de sécurité.

Étape 3 Établissez la connexion au port de console. Utilisez le port de console pour vous connecter à un ordinateur afin de saisir des commandes de configuration.

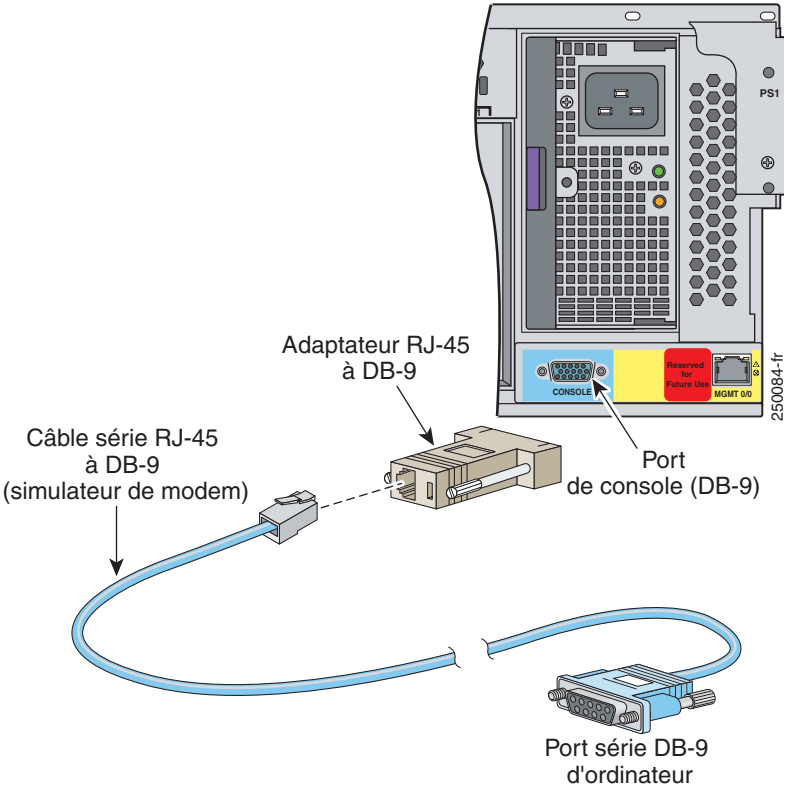
a. Avant de connecter un ordinateur ou un terminal à un port, vérifiez la vitesse de transmission en bauds du port série. La vitesse de transmission en bauds de l'ordinateur ou du terminal doit correspondre à la vitesse de transmission en bauds par défaut (9 600 bauds) du port de console du serveur de sécurité adaptatif.

Configurez le terminal comme suit : 9 600 bauds (par défaut), 8 bits de données, aucun bit de parité, 1 bit d'arrêt et contrôle de flux = matériel.

b. Connectez le connecteur d'adaptateur RJ-45-to-DB-9 au port de console, puis connectez l'autre extrémité du connecteur DB-9 sur votre ordinateur, comme illustré à la Figure 3-14.

Remarque Vous pouvez utiliser un câble de raccordement direct ou un câble de renvoi/180 pour connecter le serveur de sécurité adaptatif de la gamme ASA à un port du serveur de terminaux avec des connexions d'assemblage RJ-45 ou câble hydra. Connectez le câble approprié du port de console du serveur de sécurité adaptatif de la gamme ASA sur un port du serveur de terminaux.

Figure 3-14 Connexion de l'adaptateur RJ-45-to-DB-9

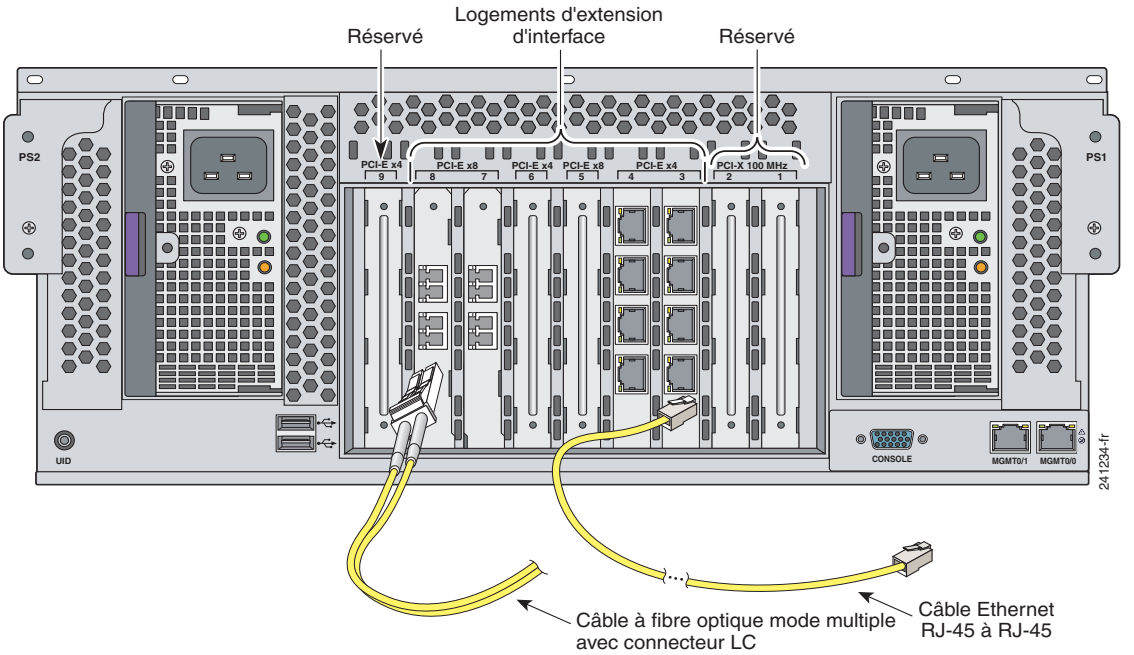


Étape 4 Connectez les ports cuivre et fibre Ethernet à utiliser pour les connexions réseau. Ceux-ci sont disponibles dans les logements 3 à 8.

Par défaut, ces logements sont disponibles sur l'ASA 5580. Vous pouvez acheter des packs pour les options d'adaptateur E/S. Voir aussi *Optimisation des performances* au Chapitre 2, « Optimisation du débit de l'ASA 5580 ».

a. Connectez une extrémité d'un câble Ethernet à un port Ethernet dans les logements 3 à 8, comme illustré à la Figure 3-15.

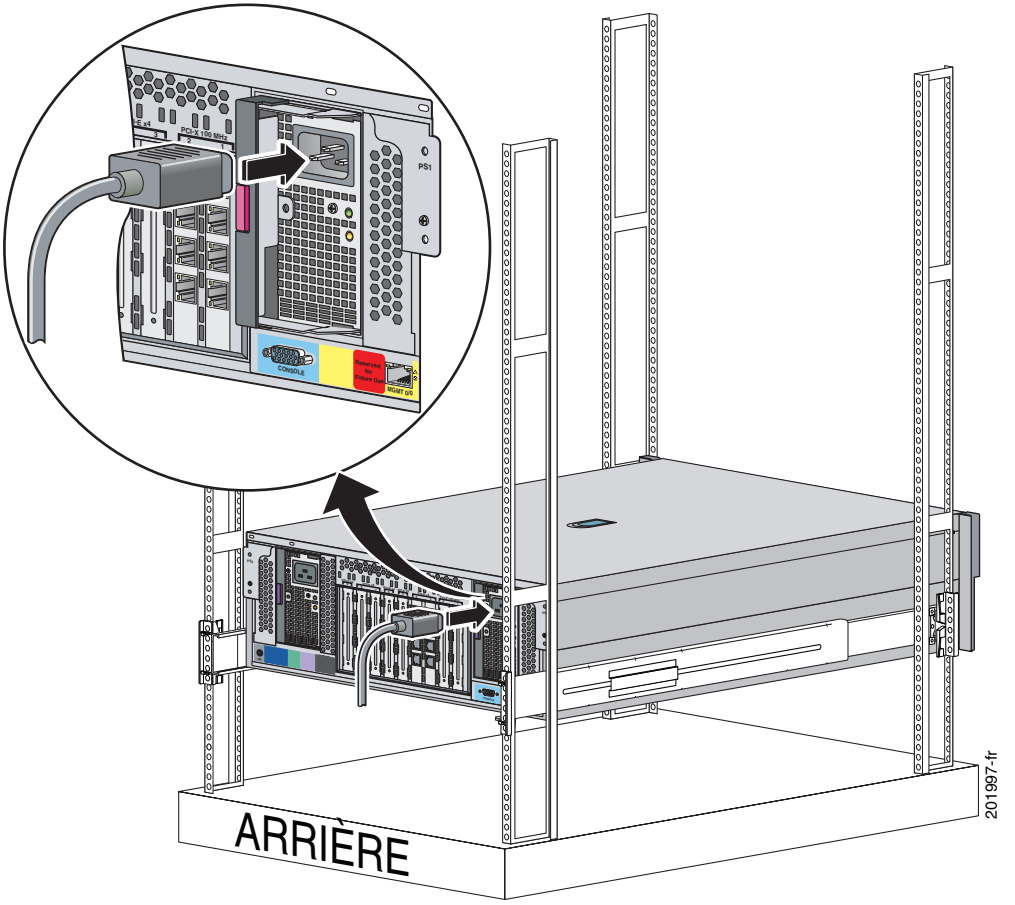
Figure 3-15 Interface cuivre Ethernet ou fibre Ethernet



b. Connectez l'autre extrémité des câbles Ethernet à un périphérique réseau, tel qu'un routeur ou un commutateur.

Étape 5 Installez les câbles électriques à l'arrière du serveur de sécurité adaptatif. Fixez les câbles d'alimentation, puis branchez-les à une alimentation (UPS recommandée), comme illustré à la Figure 3-16.

Figure 3-16 Installation de câble électrique



Étape 6 Mettez le châssis sous tension.

Étapes suivantes

Passez au Chapitre 4, « Configuration du serveur de sécurité adaptatif »

CHAPITRE 4

Configuration du serveur de sécurité adaptatif

Ce chapitre décrit la configuration initiale du serveur de sécurité adaptatif. Cette configuration peut s'effectuer depuis un navigateur à l'aide de l'ASDM (Adaptive Security Device Manager) de Cisco ou via l'interface de ligne de commande (CLI). Les procédures décrites dans le présent chapitre permettent de configurer le serveur de sécurité adaptatif à l'aide de l'ASDM.

Ce chapitre comprend les sections suivantes :

À propos de la configuration par défaut

Chaque serveur de sécurité adaptatif de Cisco est livré avec une configuration par défaut permettant un démarrage rapide. La configuration par défaut du ASA 5580 serveur de sécurité adaptatif concerne les éléments suivants :

- L'interface de gestion, Management 0/0. Si vous n'avez pas configuré l'adresse IP via la commande **configure factory-default**, l'adresse IP et le masque sont 192.168.1.1 et 255.255.255.0.
- Le serveur DHCP est activé sur le serveur de sécurité adaptatif de sorte qu'un PC se connectant à l'interface reçoit une adresse entre 192.168.1.2 et 192.168.1.254.
- Le serveur HTTP est activé pour l'ASDM et est accessible aux utilisateurs sur le réseau 192.168.1.0.

La configuration inclut les commandes suivantes :

```
interface management 0/0
   ip address 192.168.1.1 255.255.255.0
   nameif management
   security-level 100
   no shutdown
asdm logging informational 100
asdm history enable
http server enable
http 192.168.1.0 255.255.255.0 management
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd enable management
```

Utilisation de l'interface de ligne de commande pour la configuration

En plus de l'outil de configuration Web ASDM, vous pouvez configurer le serveur de sécurité adaptatif à l'aide de l'interface de ligne de commande.

Pour obtenir des procédures de configuration étape par étape de tous les domaines fonctionnels du serveur de sécurité adaptatif, reportez-vous au document *Guide de configuration de la gamme Cisco ASA 5500 utilisant l'interface CLI.*

Utilisation de l'ASDM (Adaptive Security Device Manager) pour la configuration

L'ASDM (Adaptive Security Device Manager) est une interface graphique riche en fonctionnalités qui vous permet de gérer et de surveiller le serveur de sécurité adaptatif. Cette conception basée sur le Web fournit un accès sécurisé et vous permet ainsi de gérer et de vous connecter au serveur de sécurité adaptatif à partir de n'importe quel emplacement en utilisant un navigateur Web.

En plus de fonctionnalités de gestion et de configuration complètes, l'ASDM propose des assistants intelligents pour simplifier et accélérer le déploiement du serveur de sécurité adaptatif.

Cette section comprend les rubriques suivantes :

Étapes de préparation pour utiliser l'ASDM

Avant de pouvoir utiliser l'ASDM, procédez comme suit :

Étape 1 Si vous ne l'avez pas encore fait, connectez l'interface Management 0/0 sur un commutateur ou un concentrateur à l'aide du câble Ethernet. Sur ce même commutateur, connectez un PC pour configurer le serveur de sécurité adaptatif.

Étape 2 Configurez votre PC pour utiliser DHCP (et recevoir une adresse IP automatiquement à partir du serveur de sécurité adaptatif), afin que votre PC puisse communiquer avec le serveur de sécurité adaptatif et Internet, et exécuter l'ASDM pour les tâches de configuration et de gestion.

Vous pouvez également affecter une adresse IP statique à votre PC en sélectionnant une adresse dans le sous-réseau 192.168.1.0. (Les adresses valides se situent entre 192.168.1.2 et 192.168.1.254, avec un masque de 255.255.255.0 et une route par défaut de 192.168.1.1.)

Lorsque vous connectez d'autres périphériques à l'un des ports internes, assurez-vous qu'ils n'ont pas la même adresse IP.

Remarque L'adresse par défaut de l'interface Management 0/0 du serveur de sécurité adaptatif est 192.168.1.1. Cette adresse est donc indisponible.

Étape 3 Vérifiez le voyant DEL LINK sur l'interface Management 0/0.

Lorsqu'une connexion est établie, le voyant DEL LINK du serveur de sécurité adaptatif et le voyant DEL LINK correspondant sur le commutateur ou le concentrateur deviennent vert fixe.

Collecte d'informations pour la configuration initiale

Collectez les informations suivantes pour l'assistant de démarrage de l'ASDM :

- Un nom d'hôte unique pour identifier le serveur de sécurité adaptatif sur votre réseau.
- Le nom de domaine.

- Les adresses IP de votre interface externe, interface interne et de toute autre interface à configurer.
- Les adresses IP des hôtes devant disposer d'un accès administratif à ce périphérique en utilisant HTTPS pour l'ASDM, SSH ou Telnet.
- Le mot de passe du mode privilégié pour l'accès administratif.
- Les adresses IP à utiliser pour la traduction d'adresse de port (PAT) ou de réseau (NAT), le cas échéant.
- La plage d'adresses IP pour le serveur DHCP.
- La plage d'adresses IP pour les serveur WINS.
- Les routes statiques à configurer.
- Si vous souhaitez créer un DMZ, vous devez créer un troisième VLAN et affecter des ports à ce VLAN. (Par défaut, deux VLAN sont configurés.)
- Informations concernant la configuration de l'interface : que le trafic soit autorisé entre les interfaces au même niveau de sécurité et qu'il soit autorisé entre les hôtes sur la même interface.
- Si vous configurez un client matériel Easy VPN, les adresses IP des serveurs Easy VPN primaire et secondaire ; si le client doit s'exécuter en mode d'extension réseau ou client ; et les informations d'authentification de connexion du groupe et de l'utilisateur pour correspondre à celles configurées sur les serveurs Easy VPN primaire et secondaire.

Installation de l'utilitaire d'application d'ASDM

Vous pouvez lancer l'ASDM de deux façons différentes : en téléchargeant l'utilitaire de lancement d'ASDM afin qu'ASDM s'exécute en local sur votre PC, ou en activant Java et JavaScript dans votre navigateur Web et en accédant à ASDM à distance à partir de votre PC. Cette procédure décrit comment paramétrer votre système pour exécuter l'ASDM en local.

Pour installer l'utilitaire d'application d'ASDM, procédez comme suit :

Étape 1 Sur le PC connecté au commutateur ou au concentrateur, démarrez une session de navigation sur Internet.

a. Dans le champ d'adresse du navigateur, saisissez l'URL suivant : https://192.168.1.1/admin

Remarque L'adresse IP par défaut du serveur de sécurité adaptatif est 192.168.1.1. N'oubliez pas d'ajouter le « **s** » de « **https** » sinon la connexion échouera. HTTPS (HTTP over SSL) fournit une connexion sécurisée entre votre navigateur et le serveur de sécurité adaptatif.

L'écran de démarrage de l'ASDM de Cisco apparaît.

b. Cliquez sur **Install ASDM Launcher and Run ASDM** (Installer l'utilitaire d'application d'ASDM et exécuter ASDM).

c. Dans la boîte de dialogue vous invitant à saisir un nom d'utilisateur et un mot de passe, laissez ces deux champs vides. Cliquez sur **OK**.

d. Cliquez sur **Yes** (Oui) pour accepter les certificats. Cliquez sur **Yes** (Oui) dans toutes les boîtes de dialogue concernant l'authentification et les certificats.

e. Lorsque la boîte de dialogue de téléchargement de fichier apparaît, cliquez sur **Open** (Ouvrir) pour exécuter directement le programme d'installation. Il n'est pas nécessaire de sauvegarder le logiciel d'installation sur votre disque dur.

f. Lorsque l'assistant InstallShield apparaît, suivez les instructions pour installer l'utilitaire d'application d'ASDM.

Étape 2 Démarrez l'utilitaire d'application d'ASDM de Cisco à partir de votre bureau.

Une boîte de dialogue apparaît.

Étape 3 Saisissez l'adresse IP ou le nom d'hôte du serveur de sécurité adaptatif.

Étape 4 Ne renseignez pas les champs Username (Nom d'utilisateur) et Password (Mot de passe).

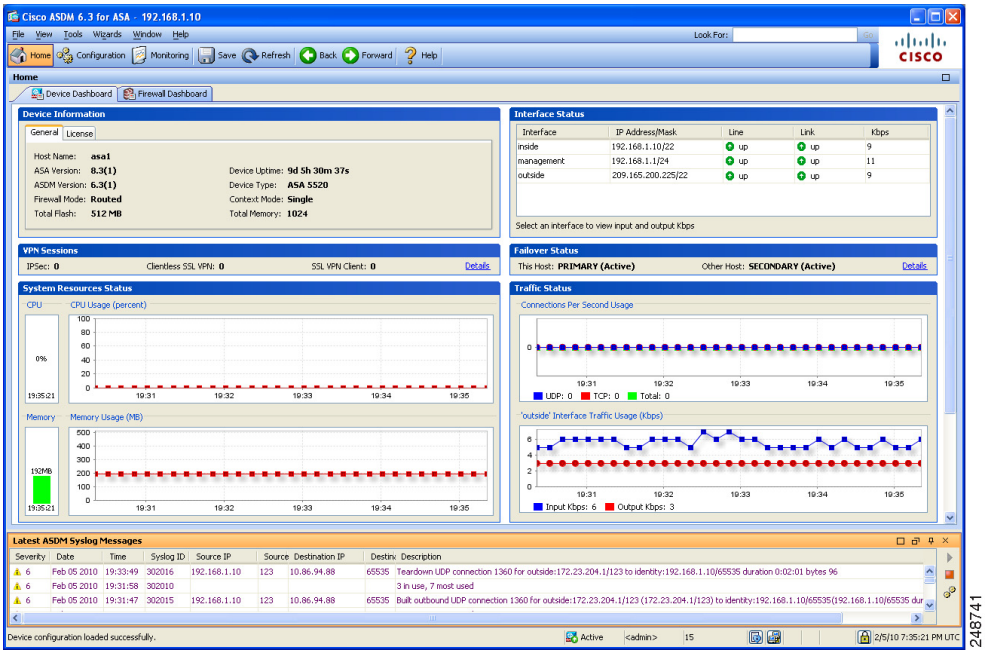
Remarque Par défaut, aucun nom d'utilisateur ni mot de passe n'est défini pour l'utilitaire d'application d'ASDM de Cisco.

Étape 5 Cliquez sur **OK**.

Étape 6 Si un message de sécurité vous invite à accepter un certificat, cliquez sur **Yes** (Oui).

Le serveur de sécurité adaptatif vérifie l'existence d'une mise à jour et le cas échéant, la télécharge automatiquement.

La fenêtre principale de l'ASDM apparaît.



Lancement d'ASDM via un navigateur Web

Pour exécuter l'ASDM dans un navigateur Web, saisissez l'adresse IP par défaut dans le champ d'adresse : **https://192.168.1.1/admin/**.

Remarque N'oubliez pas de saisir le « **s** » de « **https** » sinon la connexion échoue. HTTPS (HTTP over SSL) fournit une connexion sécurisée entre votre navigateur et le serveur de sécurité adaptatif.

La fenêtre principale de l'ASDM apparaît.

Exécution de l'assistant de démarrage d'ASDM

L'ASDM comprend un assistant de démarrage pour simplifier la configuration initiale du serveur de sécurité adaptatif. En quelques étapes, cet assistant vous permet de configurer le serveur de sécurité adaptatif afin de permettre aux paquets de circuler de façon sécurisée entre les réseaux interne et externe.

Pour utiliser l'assistant de configuration afin de paramétrer une configuration de base du serveur de sécurité adaptatif, procédez comme suit :

Étape 1 À partir du menu Wizards (Assistants) situé dans la partie supérieure de la fenêtre de l'ASDM, sélectionnez **Startup Wizard**.

Étape 2 Suivez les instructions du Startup Wizard pour paramétrer le serveur de sécurité adaptatif.

Pour obtenir des informations sur un champ de l'assistant de démarrage, cliquez sur le menu **Help** (Aide) situé dans la partie inférieure de la fenêtre.

Remarque Si un message d'erreur s'affiche et que la licence DES ou 3DES-AES vous est demandée, reportez-vous à l'Annexe A, « Obtention d'une licence 3DES/AES » pour obtenir des informations.

Remarque Selon votre politique de sécurité réseau, vous devez également envisager de configurer la plate-forme serveur de sécurité adaptatif pour qu'elle rejette l'ensemble du trafic ICMP via l'interface externe ou toute autre interface nécessaire. Vous pouvez configurer cette politique de contrôle d'accès à l'aide d'ASDM. À partir de la page principale ASDM, sélectionnez **Configuration > Properties > ICMP Rules** (Configuration > Propriétés > Règles ICMP). Ajoutez une entrée pour l'interface externe. Configurez l'adresse IP sur 0.0.0.0, le masque réseau à 0.0.0.0 et l'action à rejeter.

Étapes suivantes

Configurez le serveur de sécurité adaptatif pour votre déploiement en vous référant aux chapitres suivants.

Pour effectuer l'action suivante...	Voir...
Configurer le serveur de sécurité adaptatif pour les connexions VPN SSL à l'aide de clients logiciels	Chapitre 5, « Scénario : configuration de connexions pour un client VPN AnyConnect de Cisco »
Configurer le serveur de sécurité adaptatif pour les connexions VPN SSL à l'aide d'un navigateur Web	Chapitre 6, « Scénario : connexions VPN SSL sans client »
Configurer le serveur de sécurité adaptatif pour un VPN site à site	Chapitre 7, « Scénario : configuration du VPN site à site »
Configurer le serveur de sécurité adaptatif pour un VPN d'accès à distance	Chapitre 8, « Scénario : configuration du VPN d'accès à distance IPsec »

CHAPITRE 5

Scénario : configuration de connexions pour un client VPN AnyConnect de Cisco

Ce chapitre explique comment configurer le serveur de sécurité adaptatif pour permettre à des utilisateurs distants d'établir des connexions SSL à l'aide d'un client VPN AnyConnect de Cisco.

Ce chapitre comprend les sections suivantes :

À propos des connexions client VPN SSL

Pour pouvoir utiliser le client VPN SSL (AnyConnect), les utilisateurs distants doivent saisir dans leur navigateur l'adresse IP ou le nom de domaine complet (FQDN) de l'interface VPN SSL du dispositif de sécurité adaptatif. Le navigateur se connecte alors à l'interface compatible VPN SSL et affiche l'écran de connexion.

Remarque Lorsque le client VPN AnyConnect de Cisco est installé ou téléchargé pour la première fois, les droits administratifs sont requis.

Une fois que le téléchargement est terminé, le client s'installe et se configure automatiquement, puis établit une connexion SSL sécurisée. Lorsque la connexion prend fin, le logiciel client reste ou se désinstalle, selon la façon dont vous avez configuré le serveur de sécurité adaptatif.

Si un utilisateur distant a déjà établi une connexion VPN SSL et que le logiciel client n'a pas été configuré pour se désinstaller, le serveur de sécurité adaptatif examine la version du client, lorsque l'utilisateur s'authentifie et il effectue une mise à niveau, le cas échéant.

Obtention du logiciel client VPN AnyConnect de Cisco

Le serveur de sécurité adaptatif obtient le logiciel client VPN AnyConnect à partir du site Web de Cisco. Ce chapitre fournit des instructions pour configurer le VPN SSL avec l'assistant de configuration. Le logiciel VPN SSL de Cisco peut être téléchargé pendant le processus de configuration.

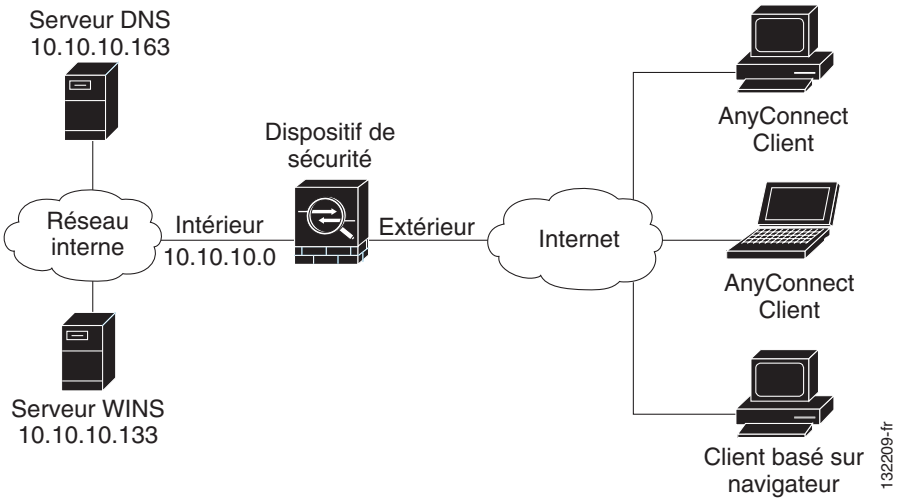
Les utilisateurs peuvent télécharger le client VPN AnyConnect VPN à partir du serveur de sécurité adaptatif. En outre, il peut être installé manuellement sur le PC distant, par l'administrateur système. Pour obtenir plus d'informations sur l'installation manuelle du logiciel client, consultez le *Guide d'administration du client VPN AnyConnect de Cisco*.

Le serveur de sécurité adaptatif pousse le logiciel client en fonction de la politique de groupe ou des attributs de nom de l'utilisateur établissant la connexion. Vous pouvez configurer le serveur de sécurité adaptatif pour qu'il pousse automatiquement le client à chaque fois que l'utilisateur établit une connexion, ou le configurer pour inviter l'utilisateur à télécharger le client. Dans ce dernier cas, si l'utilisateur ne répond pas à cette invite, vous pouvez configurer le serveur de sécurité adaptatif pour qu'il pousse le client après une période d'inactivité ou qu'il présente l'écran de connexion VPN SSL.

Exemple de topologie utilisant des clients VPN SSL AnyConnect

La Figure 5-1 illustre un serveur de sécurité adaptatif configuré pour accepter des requêtes de clients et établir des connexions SSL à partir de clients exécutant le logiciel VPN SSL AnyConnect. Le serveur de sécurité adaptatif peut prendre en charge des connexions de clients exécutant le logiciel VPN AnyConnect et de clients basés sur navigateur.

Figure 5-1 Topologie réseau du scénario VPN SSL



Implémentation du scénario VPN SSL de Cisco

Cette section explique comment configurer le serveur de sécurité adaptatif pour accueillir des connexions VPN SSL AnyConnect de Cisco. Les valeurs utilisées pour les paramètres de configuration de l'exemple ci-après sont tirées du scénario VPN SSL illustré à la Figure 5-1.

Cette section comprend les rubriques suivantes :

Informations à garder à portée de main

Avant de commencer à configurer le serveur de sécurité adaptatif pour accepter des connexions VPN SSL AnyConnect, assurez-vous que vous disposez des informations suivantes :

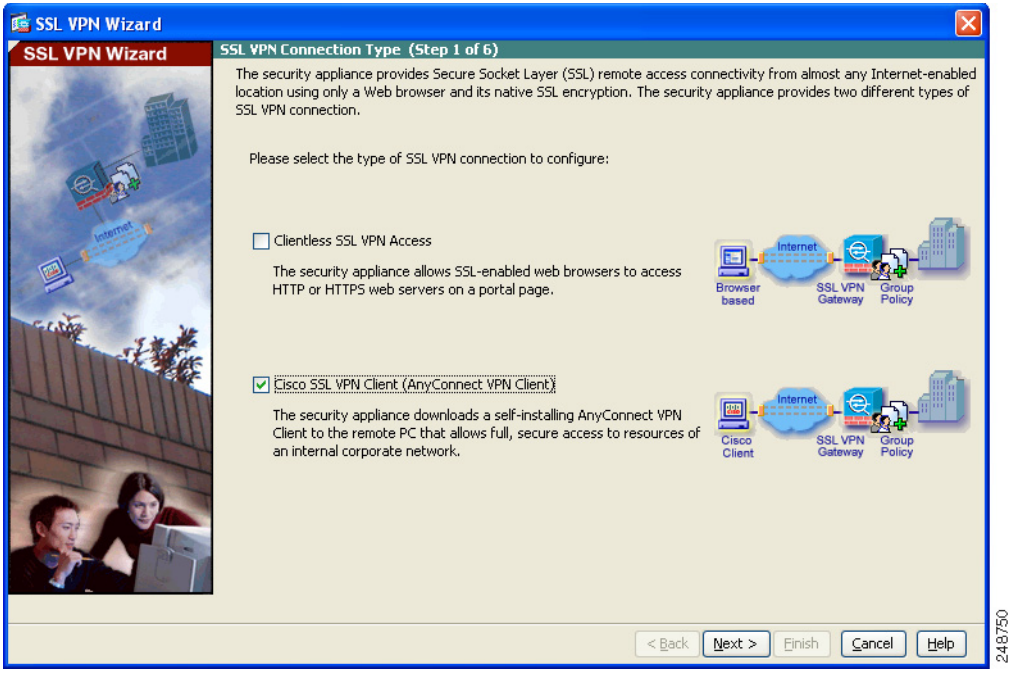
- Nom de l'interface du serveur de sécurité adaptatif auquel les utilisateurs distants se connecteront.
- Certificat numérique

  L'ASA 5580 génère un certificat auto-signé par défaut. Pour une sécurité accrue, vous pouvez cependant acheter un certificat VPN SSL dont la fiabilité est reconnue, avant de placer le système dans un environnement de production.
- Plage d'adresses IP à utiliser dans un pool IP. Ces adresses sont affectées aux clients VPN SSL AnyConnect au fur et à mesure que leur connexion est établie.
- Liste des utilisateurs à prendre en compte pour créer une base de données d'authentification locale, sauf si vous utilisez un serveur AAA pour l'authentification.
- Si vous utilisez un serveur AAA pour l'authentification :
  - Nom du groupe de serveurs AAA
  - Protocole d'authentification à utiliser (TACACS, SDI, NT, Kerberos, LDAP)
  - Adresse IP du serveur AAA
  - Interface du serveur de sécurité adaptatif à utiliser pour l'authentification
  - Clé secrète pour s'authentifier avec le serveur AAA

Configuration du serveur de sécurité adaptatif pour le client VPN AnyConnect de Cisco

Pour commencer le processus de configuration, procédez comme suit :

Étape 1 Dans la fenêtre ASDM principale, sélectionnez **SSL VPN Wizard** (Assistant VPN SSL), dans le menu déroulant. Vous accédez à l'étape 1 de l'assistant VPN SSL.



Étape 2 Dans cet écran, procédez comme suit :

a. Cochez la case d'option **Cisco SSL VPN Client** (Client VPN SSL Cisco).

b. Cliquez sur **Next** (Suivant) pour continuer.

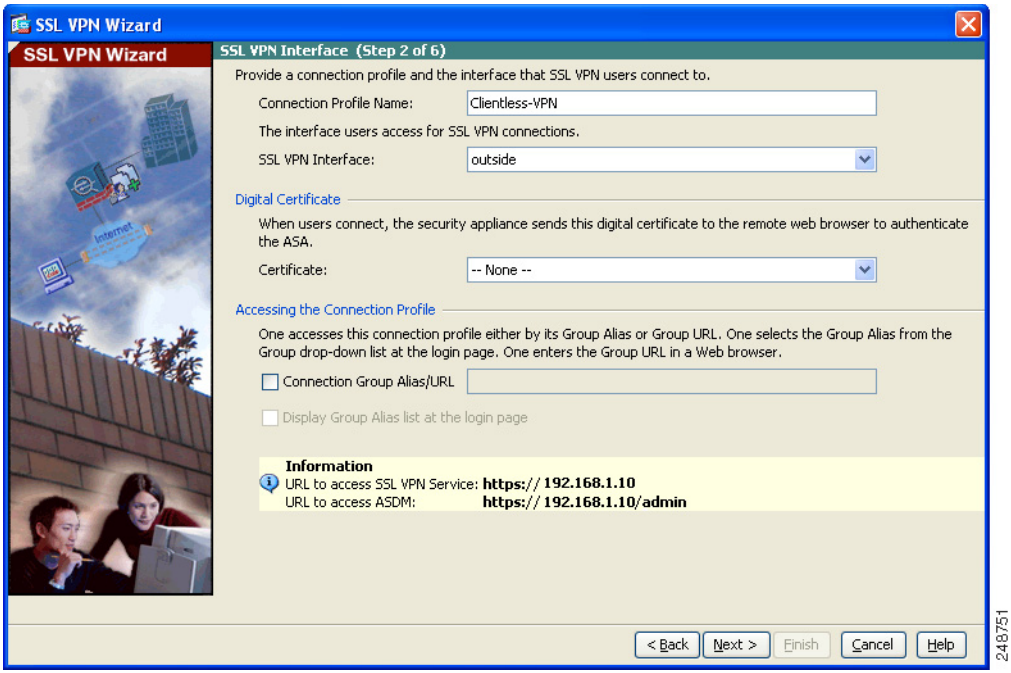
Spécification de l'interface VPN SSL

À l'étape 2 de l'assistant VPN SSL, procédez comme suit :

Étape 1 Spécifiez un nom de connexion auquel les utilisateurs distants se connectent.

Étape 2 Dans la liste déroulante SSL VPN Interface (Interface VPN SSL), sélectionnez l'interface à laquelle les utilisateurs distants se connectent. Lorsque des utilisateurs établissent une connexion sur cette interface, la page du portail VPN SSL apparaît.

Étape 3 Dans la liste déroulante Certificate (Certificat), sélectionnez le certificat que le serveur de sécurité adaptatif envoie à l'utilisateur distant pour authentifier le serveur de sécurité adaptatif.



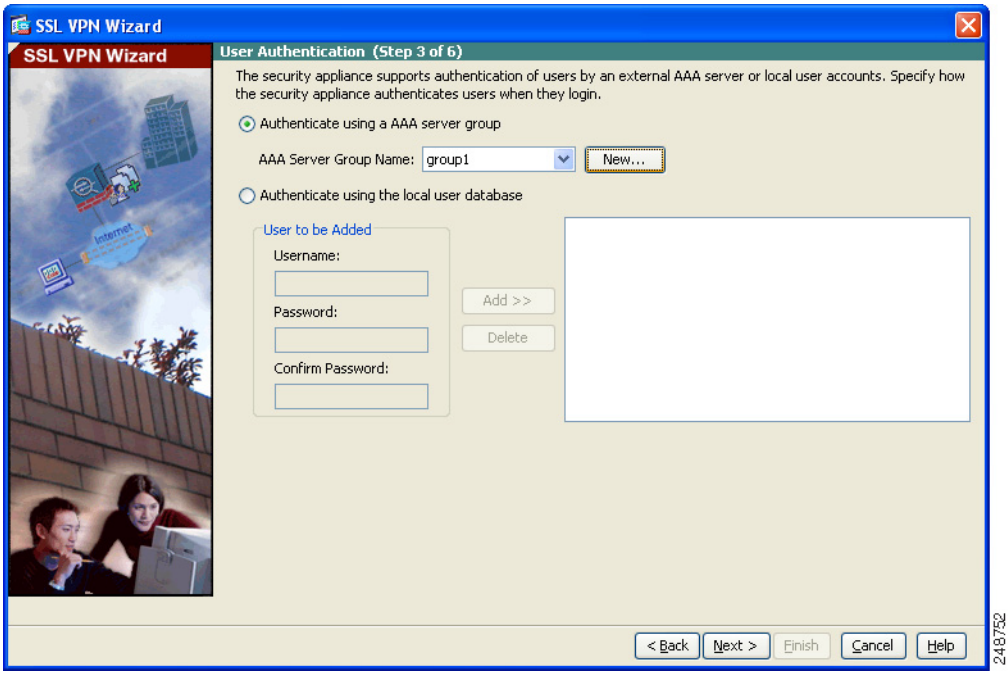
Étape 4 Cliquez sur **Next** (Suivant) pour continuer.

Spécification d'une méthode d'authentification utilisateur

À l'étape 3 de l'assistant VPN SSL, procédez comme suit :

Étape 1 Si vous utilisez un serveur AAA ou un groupe de serveurs pour l'authentification, procédez comme suit :

a. Cochez la case d'option **Authenticate using a AAA server group** (S'authentifier via un groupe de serveurs AAA).



b. Spécifiez un nom de groupe de serveurs AAA.

c. Vous pouvez choisir un nom de groupe de serveurs AAA existant dans la liste déroulante ou en créer un nouveau, en cliquant sur **New** (Nouveau).

Pour créer un nouveau groupe de serveurs AAA, cliquez sur **New** (Nouveau). La boîte de dialogue New Authentication Server Group (Nouveau groupe de serveurs d'authentification) apparaît.

Dans cette boîte de dialogue, spécifiez ce qui suit :

- Un nom de groupe de serveurs
- Le protocole d'authentification à utiliser (RADIUS, TACACS, SDI, NT, Kerberos, LDAP)
- L'adresse IP du serveur AAA
- L'interface du serveur de sécurité adaptatif
- La clé secrète à utiliser pour communiquer avec le serveur AAA.

d. Cliquez sur **OK**.

Étape 2 Si vous avez choisi d'authentifier des utilisateurs avec la base de données d'utilisateurs locale, vous pouvez créer de nouveaux comptes utilisateurs ici. Vous pouvez également ajouter des utilisateurs ultérieurement, via l'interface de configuration ASDM.

Pour ajouter un nouvel utilisateur, saisissez un nom d'utilisateur et un mot de passe, puis cliquez sur **Add** (Ajouter).

Étape 3 Une fois que vous avez terminé d'ajouter de nouveaux utilisateurs, cliquez sur **Next** (Suivant), pour continuer.

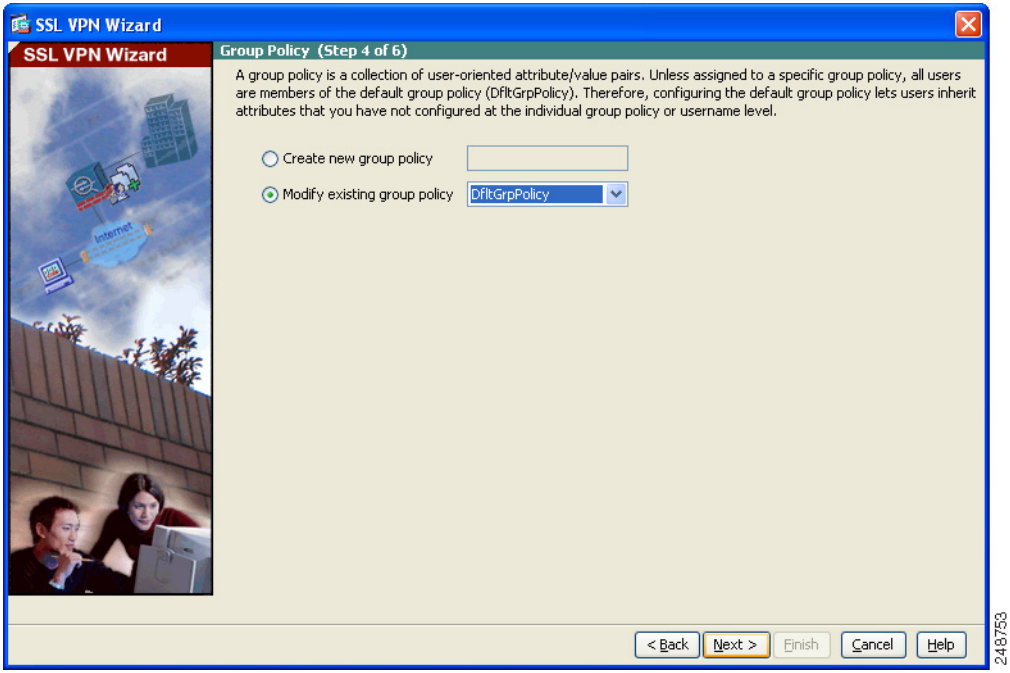
Spécification d'une politique de groupe

À l'étape 4 de l'assistant VPN SSL, spécifiez une politique de groupe, en procédant comme suit :

Étape 1 Cochez la case d'option **Create new group policy** (Créer une nouvelle politique de groupe), puis spécifiez un nom de groupe.

OU

Étape 2 Cochez la case d'option **Modify an existing group policy** (Modifier une politique de groupe existante), puis sélectionnez un groupe, dans la liste déroulante.



Étape 3 Cliquez sur **Next** (Suivant).

Étape 4 L'étape 5 de l'assistant VPN SSL apparaît. Comme cette étape ne concerne pas les connexions client VPN AnyConnect, cliquez de nouveau sur **Next** (Suivant).

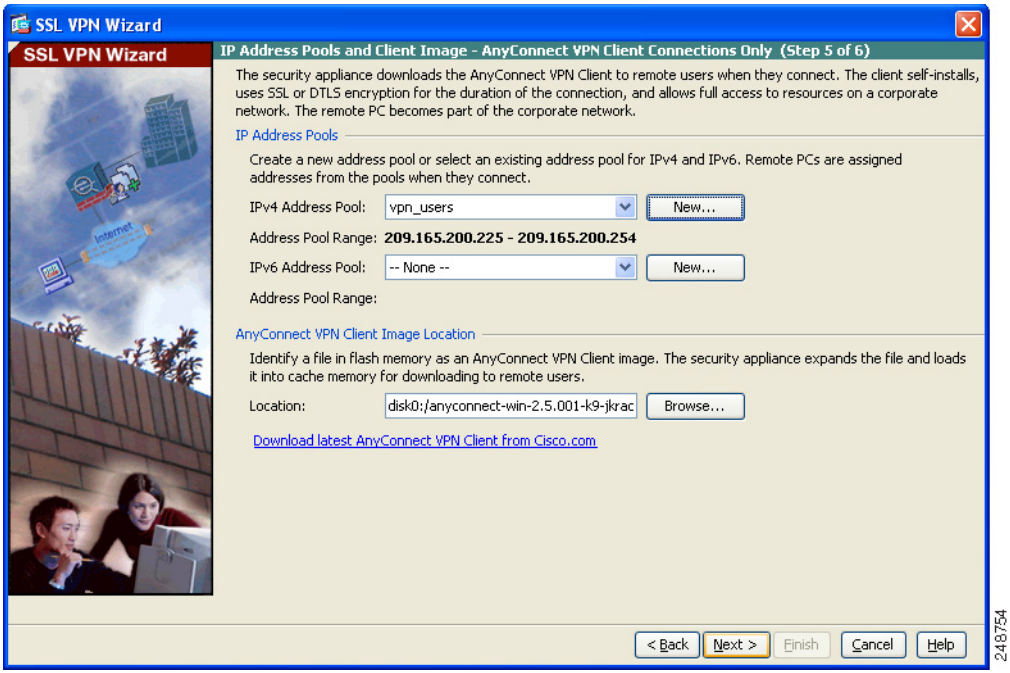
Configuration du client VPN AnyConnect de Cisco

Pour que les clients distants aient accès à votre réseau avec un client VPN AnyConnect de Cisco, vous devez configurer un pool d'adresses IP pouvant être affectées aux clients VPN distants, lorsqu'ils se connectent. Dans un tel cas, le pool est configuré pour utiliser la plage d'adresses IP 209.165.201.1–209.166.201.20.

Vous devez également spécifier l'emplacement du logiciel AnyConnect, pour que le serveur de sécurité adaptatif puisse le transmettre aux utilisateurs.

À l'étape 6 de l'assistant VPN SSL, procédez comme suit :

Étape 1 Pour utiliser un pool d'adresses préconfigurées, choisissez le nom du pool dans les listes déroulantes IPv4 Address Pool (Pool d'adresses IPv4) ou IPv6 Address Pool (Pool d'adresses IPv6).



Étape 2 Vous pouvez également cliquer sur **New** (Nouveau), pour créer un nouveau pool d'adresses.

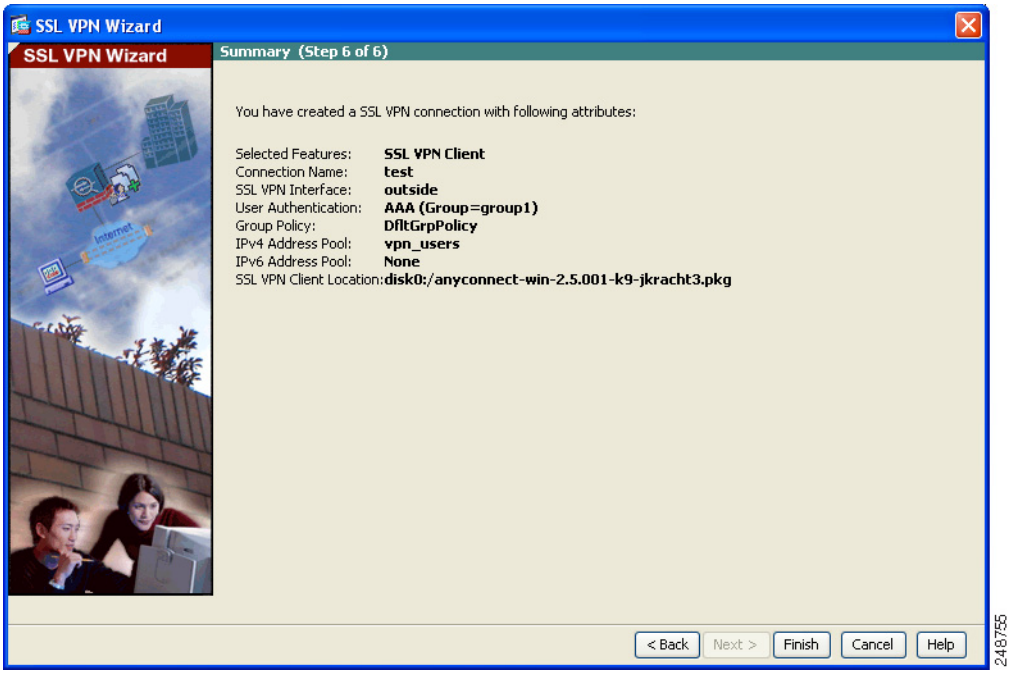
Étape 3 Précisez l'emplacement de l'image logicielle du client VPN AnyConnect.

Pour obtenir la dernière version du logiciel, cliquez sur Download Latest AnyConnect VPN client (Télécharger le dernier client VPN AnyConnect), depuis le site Web de cisco.com. Le logiciel client est alors téléchargé sur votre PC.

Étape 4 Cliquez sur **Next** (Suivant) pour continuer.

Vérification de la configuration VPN d'accès à distance

À l'étape 7 de l'assistant VPN SSL, vérifiez les paramètres de configuration, pour vous assurer qu'ils sont corrects. La configuration affichée doit être similaire à ce qui suit.



Si cette configuration vous convient, cliquez sur **Finish** (Terminer), pour appliquer les modifications au serveur de sécurité adaptatif.

Pour enregistrer les modifications apportées à la configuration de démarrage, de façon qu'elles entrent au vigueur lors du prochain démarrage du périphérique, cliquez sur **Save** (Enregistrer), dans le menu File (Fichier). Dans la négative, ASDM vous invite à enregistrer les modifications de configuration de manière permanente, lorsque vous quittez l'application.

Si vous n'enregistrez pas les modifications de configuration, l'ancienne configuration est appliquée au prochain démarrage du périphérique.

Étapes suivantes

Si vous ne déployez le serveur de sécurité adaptatif que pour prendre en charge des connexions VPN AnyConnect, vous avez terminé la configuration initiale. Par ailleurs, vous pouvez envisager de réaliser l'une des étapes suivantes.

Pour effectuer l'action suivante...	Voir...
Affiner la configuration et configurer des fonctionnalités facultatives et avancées	*Guide de configuration de la gamme Cisco ASA 5500 utilisant l'interface CLI*
En savoir plus sur les opérations quotidiennes	*Référence des commandes de la gamme Cisco ASA 5500* *Messages de journalisation système de la gamme Cisco ASA 5500*

Vous pouvez configurer le serveur de sécurité adaptatif pour plusieurs applications. Les sections suivantes fournissent les procédures de configuration à mettre en oeuvre pour les autres applications communes du serveur de sécurité adaptatif.

Pour effectuer l'action suivante...	Voir...
Configurer un VPN SSL sans client (basé sur le navigateur)	Chapitre 6, « Scénario : connexions VPN SSL sans client »
Configurer un VPN site à site	Chapitre 7, « Scénario : configuration du VPN site à site »
Configurer un VPN d'accès à distance IPsec	Chapitre 8, « Scénario : configuration du VPN d'accès à distance IPsec »

CHAPITRE 6

Scénario : connexions VPN SSL sans client

Ce chapitre explique comment utiliser le serveur de sécurité adaptatif pour accueillir des connexions VPN SSL d'accès à distance sans client logiciel (clientless). Un VPN SSL sans client permet de créer des connexions sécurisées, ou tunnels, à travers Internet en utilisant un navigateur Web. Cela fournit un accès sécurisé aux utilisateurs hors site sans client logiciel ni matériel.

Ce chapitre comprend les sections suivantes :

À propos du VPN SSL sans client

Les connexions VPN SSL sans client permettent un accès facile et sécurisé à un grand nombre de ressources Web et d'applications Web à partir de pratiquement n'importe quel ordinateur sur Internet. Notamment :

- Les sites Web internes
- Les applications Web
- Les partages de fichier FTP et NT/Active Directory
- Les proxy e-mail, y compris POP3S, IMAP4S et SMTPS

- MS Outlook Web Access
- MAPI
- L'accès à l'application (c'est-à-dire, le transfert de port pour accéder à d'autres applications basées sur TCP) et les Smart Tunnels

Le VPN SSL sans client utilise le protocole SSL (Secure Sockets Layer Protocol) et son successeur, TLSI (Transport Layer Security) pour fournir une connexion sécurisée entre des utilisateurs distants et des ressources internes prises en charge spécifiques que vous configurez sur un site central. Le serveur de sécurité adaptatif reconnaît les connexions devant être mises en proxy et le serveur HTTP interagit avec le sous-système d'authentification pour authentifier les utilisateurs.

L'administrateur réseau fournit un accès aux ressources aux utilisateurs de VPN SSL sans client en fonction d'un groupe.

Observations concernant la sécurité des connexions VPN SSL sans client

Les connexions VPN SSL sans client du serveur de sécurité adaptatif sont différentes des connexions IPsec d'accès à distance, en particulier en ce qui concerne leur façon d'interagir avec les serveurs SSL et la validation des certificats.

Dans une connexion VPN SSL sans client, le serveur de sécurité adaptatif agit comme un proxy entre le navigateur Web de l'utilisateur final et les serveurs Web cibles. Lorsqu'un utilisateur se connecte à un serveur Web SSL, le serveur de sécurité adaptatif établit une connexion sécurisée et valide le certificat SSL du serveur. Le navigateur de l'utilisateur final ne reçoit jamais le certificat présenté ; il ne peut par conséquent ni l'examiner, ni le valider.

L'implémentation actuelle du VPN SSL sans client sur le serveur de sécurité adaptatif ne permet aucune communication avec les sites dont les certificats sont expirés. De même, le serveur de sécurité adaptatif n'effectue aucune validation de certificat CA fiable. Les utilisateurs ne peuvent donc pas analyser le certificat d'un serveur Web SSL avant de communiquer avec lui.

Pour réduire les risques induits par les certificats SSL :

1. Configurez une politique de groupe englobant tous les utilisateurs ayant besoin d'un accès VPN SSL sans client, et activez-le uniquement pour cette politique de groupe.
2. Restreignez l'accès Internet des utilisateurs VPN SSL sans client, par exemple, en limitant les ressources disponibles lors d'une connexion VPN SSL sans client. Pour ce faire, vous pouvez empêcher l'utilisateur d'accéder à du contenu général à Internet. Vous pouvez ensuite configurer des liens vers les cibles souhaitées sur le réseau interne, auxquelles les utilisateurs de VPN SSL sans client peuvent avoir accès.
3. Informez les utilisateurs. Si un site SSl ne se trouve pas dans le réseau privé, les utilisateurs ne doivent pas le visiter via une connexion VPN SSL sans client. Ils doivent dans ce cas ouvrir une fenêtre de navigation séparée, et utiliser ce navigateur pour visualiser le certificat présenté.

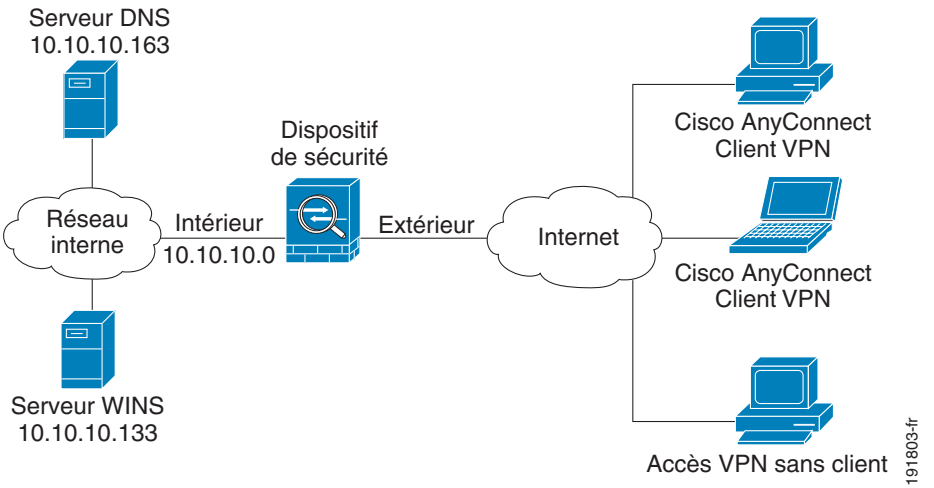
Le serveur de sécurité adaptatif ne prend pas en charge les fonctionnalités suivantes des connexions VPN SSL sans client :

- NAT, qui permet de limiter les besoins en adresses IP uniques au niveau mondial.
- PAT, qui permet de faire apparaître plusieurs sessions sortantes comme provenant d'une adresse IP unique.

Exemple de réseau avec accès VPN SSL basé sur navigateur

La Figure 6-1 illustre un serveur de sécurité adaptatif configuré pour accepter des demandes de connexions VPN SSL sur Internet via un navigateur Web.

Figure 6-1 Topologie réseau pour les connexions VPN SSL



Implémentation du scénario VPN SSL sans client

Cette section explique comment configurer le serveur de sécurité adaptatif pour accepter des demandes VPN SSL de navigateurs Web. Les valeurs des paramètres de configuration de l'exemple sont tirées du scénario d'accès à distance illustré à la Figure 6-1.

Cette section comprend les rubriques suivantes :

Informations à garder à portée de main

Avant de commencer à configurer le serveur de sécurité adaptatif de sorte qu'il accepte les connexions VPN à accès à distance de type IPsec, assurez-vous que vous disposez des informations suivantes :

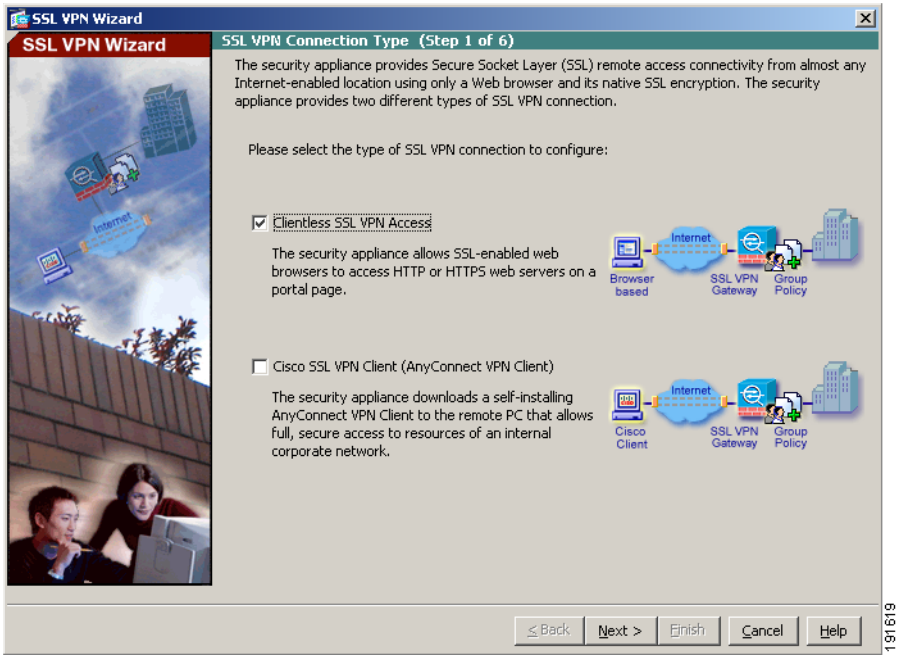
- Nom de l'interface du serveur de sécurité adaptatif auquel les utilisateurs distants se connecteront. Lorsque des utilisateurs distants se connectent à cette interface, la page du portail VPN SSL apparaît.
- Certificat numérique

  L'ASA 5580 génère un certificat auto-signé par défaut. Pour améliorer la sécurité et éliminer les messages d'avertissement du navigateur, vous pouvez envisager d'acheter un certificat VPN SSL reconnu comme étant fiable avant de placer le système dans un environnement de production.
- Liste des utilisateurs à prendre en compte pour créer une base de données d'authentification locale, sauf si vous utilisez un serveur AAA pour l'authentification.
- Si vous utilisez un serveur AAA pour l'authentification, le nom du groupe de serveurs AAA
- Les informations suivantes sur les politiques de groupe sur le serveur AAA :
  - Nom du groupe de serveurs
  - Protocole d'authentification à utiliser (TACACS, SDI, NT, Kerberos, LDAP)
  - Adresse IP sur le serveur AAA
  - Interface du serveur de sécurité adaptatif à utiliser pour l'authentification
  - Clé secrète pour s'authentifier sur le serveur AAA
- Liste des pages ou sites Web internes que vous souhaitez voir apparaître sur la page du portail VPN SSL lorsque des utilisateurs distants établissent une connexion. S'agissant de la page vue par les utilisateurs lorsqu'ils établissent une connexion pour la première fois, cette page doit contenir les cibles les plus utilisées des utilisateurs distants.

Configuration de la plate-forme Adaptive Security Appliance pour les connexions SSL VPN sur navigateur

Pour commencer le processus de configuration d'un VPN SSL basé sur navigateur, procédez comme suit :

Étape 1 Dans la fenêtre ASDM principale, sélectionnez **SSL VPN Wizard** (Assistant VPN SSL) dans le menu déroulant. Vous accédez à l'étape 1 de l'assistant VPN SSL.



Étape 2 Dans cet écran, procédez comme suit :

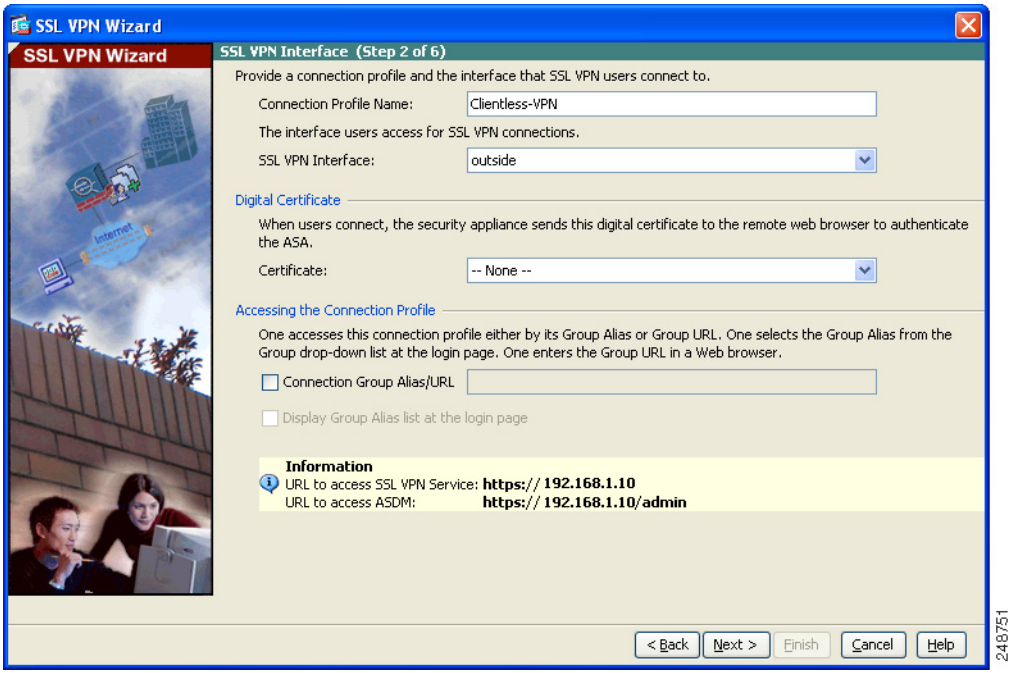
a. Cochez la case d'option **Browser-based SSL VPN (Web VPN)** (VPN SSL basé sur navigateur (VPN Web)).

b. Cliquez sur **Next** (Suivant) pour continuer.

Spécification de l'interface VPN SSL

À l'étape 2 de l'assistant VPN SSL, procédez comme suit :

Étape 1 Spécifiez un nom de connexion que les utilisateurs distants doivent sélecionner.



Étape 2 Dans la liste déroulante SSL VPN Interface (Interface VPN SSL), sélectionnez l'interface à laquelle les utilisateurs distants doivent se connecter. Lorsque des utilisateurs établissent une connexion sur cette interface, la page du portail VPN SSL apparaît.

Étape 3 Dans la liste déroulante Certificate (Certificat), sélectionnez le certificat que le serveur de sécurité adaptatif envoie à l'utilisateur distant pour authentifier le serveur de sécurité adaptatif.

Remarque L'ASA 5580 génère un certificat auto-signé par défaut. Pour améliorer la sécurité et éliminer les messages d'avertissement du navigateur, vous pouvez envisager d'acheter un certificat VPN SSL reconnu comme étant fiable avant de placer le système dans un environnement de production.

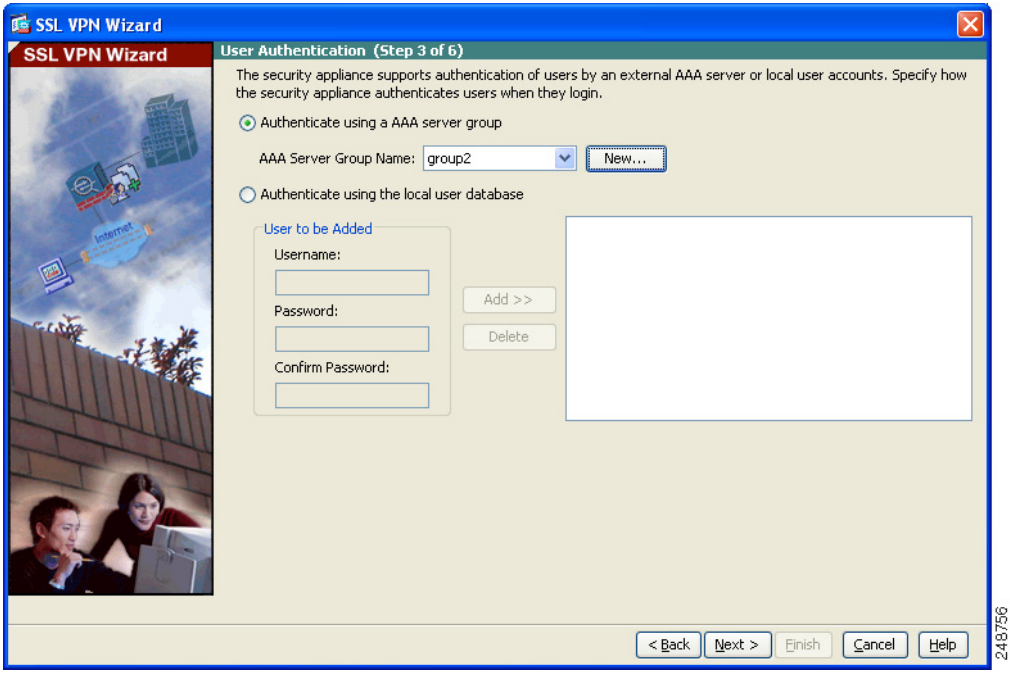
Spécification d'une méthode d'authentification des utilisateurs

Les utilisateurs peuvent être authentifiés soit par une base de données d'authentification locale, soit via des serveurs AAA (Authentication, Authorization and Accounting) tels que RADIUS, TACACS+, SDI, NT, Kerberos et LDAP.

À l'étape 3 de l'assistant VPN SSL, procédez comme suit :

Étape 1 Si vous utilisez un serveur AAA ou un groupe de serveurs pour l'authentification, procédez comme suit :

a. Cochez la case d'option **Authenticate using a AAA server group** (S'authentifier via un groupe de serveurs AAA).



b. Sélectionnez un groupe de serveurs préconfiguré dans la liste déroulante Authenticate using a AAA server group (S'authentifier via un groupe de serveurs AAA) ou cliquez sur **New** (Nouveau) pour ajouter un nouveau groupe de serveurs AAA.

Pour créer un nouveau groupe de serveurs AAA, cliquez sur **New** (Nouveau). La boîte de dialogue New Authentication Server Group (Nouveau groupe de serveurs d'authentification) apparaît.

Dans cette boîte de dialogue, spécifiez ce qui suit :

- Un nom de groupe de serveurs
- Le protocole d'authentification à utiliser (TACACS, SDI, NT, Kerberos, LDAP)
- L'adresse IP du serveur AAA
- L'interface duserveur de sécurité adaptatif
- La clé secrète à utiliser pour communiquer avec le serveur AAA

Cliquez sur **OK**.

Étape 2 Si vous avez choisi d'authentifier des utilisateurs avec la base de données d'utilisateurs locale, vous pouvez créer de nouveaux comptes utilisateurs ici. Vous pouvez également ajouter des utilisateurs ultérieurement à l'aide de l'interface de configuration ASDM.

Pour ajouter un nouvel utilisateur, saisissez un nom d'utilisateur et un mot de passe, puis cliquez sur **Add** (Ajouter).

Étape 3 Lorsque vous avez ajouté tous les utilisateurs souhaités, cliquez sur **Next** pour continuer.

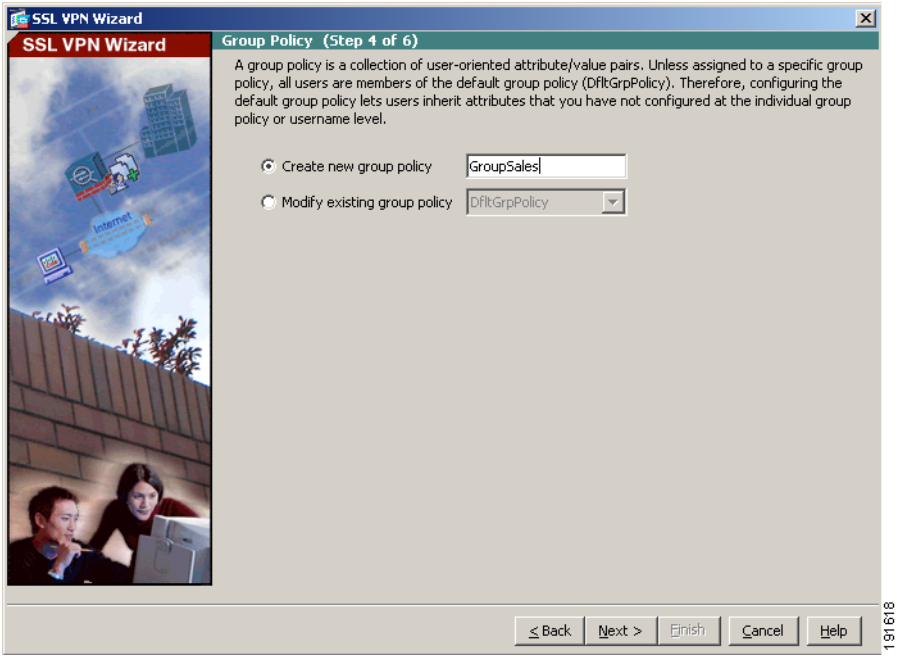
Spécification d'une politique de groupe

À l'étape 4 de l'assistant VPN SSL, spécifiez une politique de groupe en procédant comme suit :

Étape 1 Cochez la case d'option **Create new group policy** (Créer une nouvelle politique de groupe), puis spécifiez un nom de groupe.

OU

Cochez la case d'option **Modify an existing group policy**(Modifier une politique de groupe existante), puis sélectionnez un groupe à partir de la liste déroulante.



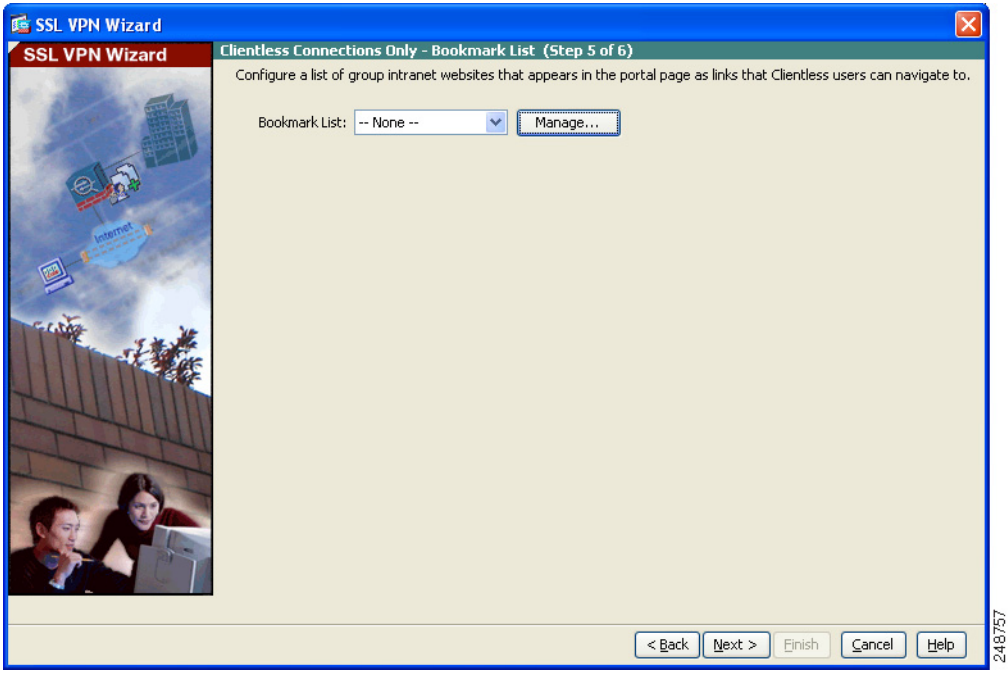
Étape 2 Cliquez sur **Next** (Suivant).

Création d'une liste de signets pour les utilisateurs distants

Vous pouvez créer une page de portail, une page Web spéciale s'affichant lorsque des clients basés sur navigateur établissent des connexions VPN au serveur de sécurité adaptatif, en spécifiant une liste d'URL auxquelles les utilisateurs doivent pouvoir facilement accéder.

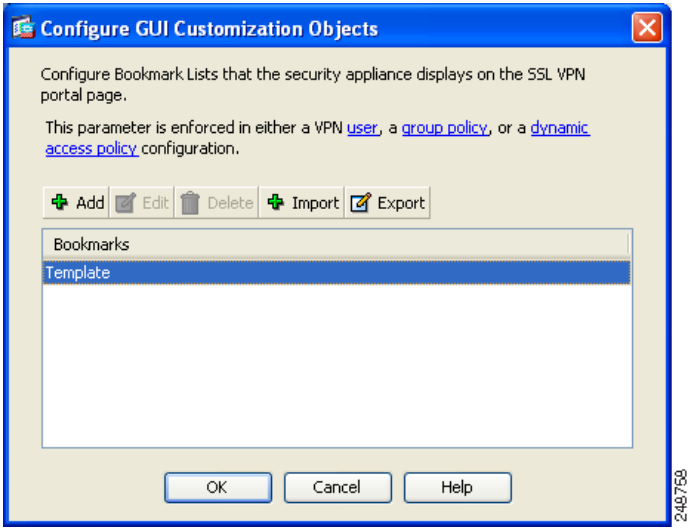
À l'étape 5 de l'assistant VPN SSL, spécifiez les URL devant apparaître sur la page du portail VPN en procédant comme suit :

Étape 1 Pour spécifier une liste de signets existante, sélectionnez-la dans la liste déroulante Bookmark List (Liste de signets).



Pour ajouter une nouvelle liste ou modifier une liste existante, cliquez sur **Manage** (Gérer).

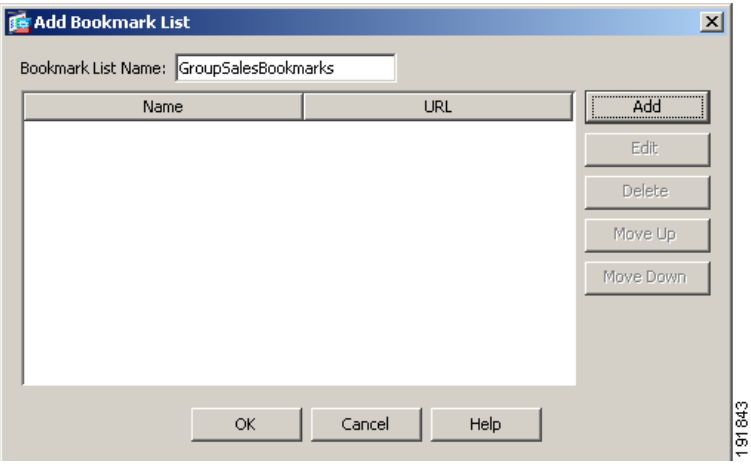
La boîte de dialogue Configure GUI Customization Objects (Configurer les objets de personnalisation de l'interface) apparaît.



Étape 2 Pour créer une nouvelle liste de signets, cliquez sur **Add** (Ajouter).

Pour modifier une liste de signets existante, sélectionnez la liste, puis cliquez sur **Edit** (Modifier).

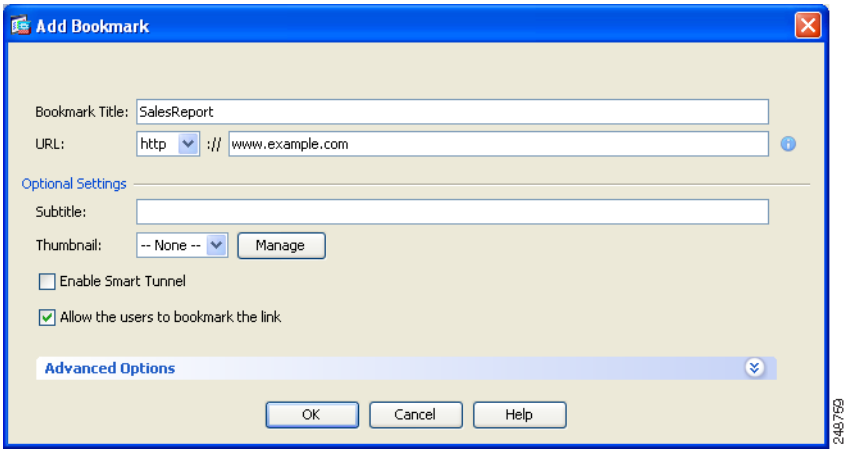
La boîte de dialogue Add Bookmark List (Ajouter une liste de signets) apparaît.



Étape 3 Dans le champ URL List Name (Nom de la liste URL), spécifiez un nom pour la liste de signets que vous créez. Ce nom s'affichera comme titre de votre page de portail VPN.

Étape 4 Cliquez sur **Add** (Ajouter) pour ajouter une nouvelle URL à la liste de signets.

La boîte de dialogue Add Bookmark Entry (Ajouter une entrée de signet) apparaît.



Étape 5 Spécifiez un titre pour la liste dans le champ Bookmark Title (Titre de signet).

Étape 6 Dans la liste déroulante URL Value (Valeur de l'URL), sélectionnez le type d'URL souhaité. Par exemple, choisissez http, https, ftp, etc.

Ensuite, spécifiez l'URL complet pour la page.

Étape 7 Cliquez sur **OK** pour revenir à la boîte de dialogue Add Bookmark List (Ajouter une liste de signets).

Étape 8 Si vous avez terminé d'ajouter des listes de signets, cliquez sur **OK** pour revenir à la boîte de dialogue Configure GUI Customization Objects (Configurer les objets de personnalisation de l'interface).

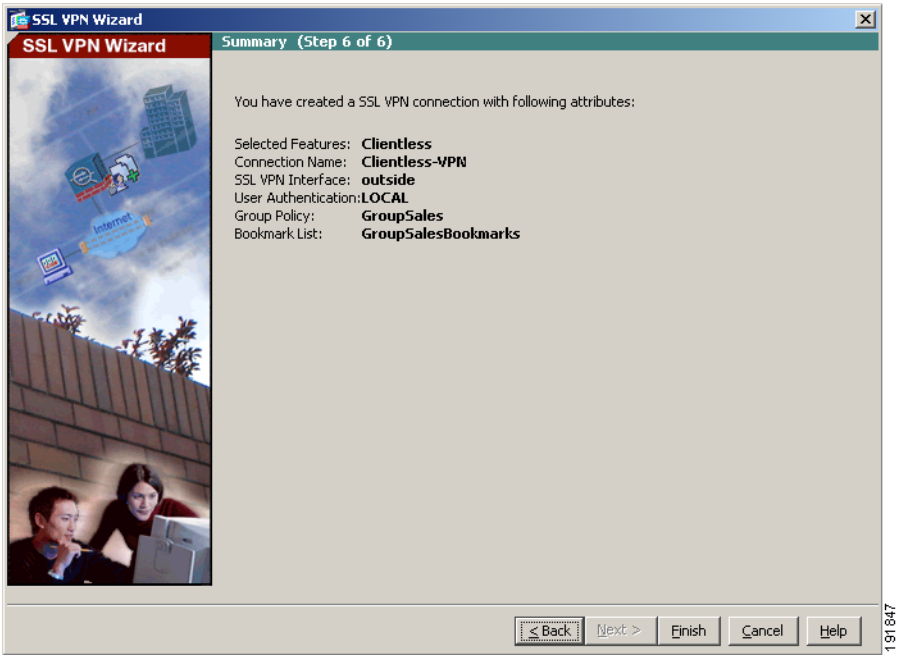
Étape 9 Après avoir ajouté ou modifié des listes de signets, cliquez sur **OK** pour revenir à l'étape 5 de l'assistant VPN SSL.

Étape 10 Choisissez le nom de la liste de signets de ce groupe VPN dans la liste déroulante Bookmark List (Liste de signets).

Étape 11 Cliquez sur **Next** (Suivant) pour continuer.

Vérification de la configuration

À l'étape 7 de l'assistant VPN SSL, vérifiez que les paramètres de configuration sont corrects. La configuration affichée doit être similaire à ce qui suit.



Si cette configuration vous convient, cliquez sur **Finish** (Terminer) pour appliquer les modifications au serveur de sécurité adaptatif.

Si vous souhaitez enregistrer les modifications apportées à la configuration de démarrage de façon à ce que ces modifications s'appliquent au prochain démarrage du périphérique, cliquez sur **Save** (Enregistrer) dans le menu File (Fichier). Sinon, ASDM vous invite à enregistrer les modifications de configuration de manière permanente lorsque vous quittez l'application.

Si vous n'enregistrez pas les modifications de configuration, l'ancienne configuration sera appliquée au prochain démarrage du périphérique.

Étapes suivantes

Si vous déployez le serveur de sécurité adaptatif uniquement dans un environnement VPN SSL sans client, vous avez terminé la configuration initiale. Vous avez toutefois la possibilité d'appliquer les procédures complémentaires suivantes.

Pour effectuer l'action suivante...	Voir...
Affiner la configuration et configurer des fonctionnalités facultatives et avancées	*Guide de configuration de la gamme Cisco ASA 5500 utilisant l'interface CLI*
En savoir plus sur les opérations quotidiennes	*Référence des commandes de la gamme Cisco ASA 5500* *Messages de journalisation système de la gamme Cisco ASA 5500*

Vous pouvez configurer le serveur de sécurité adaptatif pour plusieurs applications. Les sections suivantes indiquent les procédures de configuration à suivre pour les autres applications courantes de la plate-forme serveur de sécurité adaptatif.

Pour effectuer l'action suivante...	Voir...
Configurer un VPN d'accès à distance	Chapitre 8, « Scénario : configuration du VPN d'accès à distance IPsec »
Configurer un VPN AnyConnect	Chapitre 5, « Scénario : configuration de connexions pour un client VPN AnyConnect de Cisco »
Configurer un VPN site à site	Chapitre 7, « Scénario : configuration du VPN site à site »

CHAPITRE 7

Scénario : configuration du VPN site à site

Ce chapitre explique comment utiliser le serveur de sécurité adaptatif pour créer un VPN site à site.

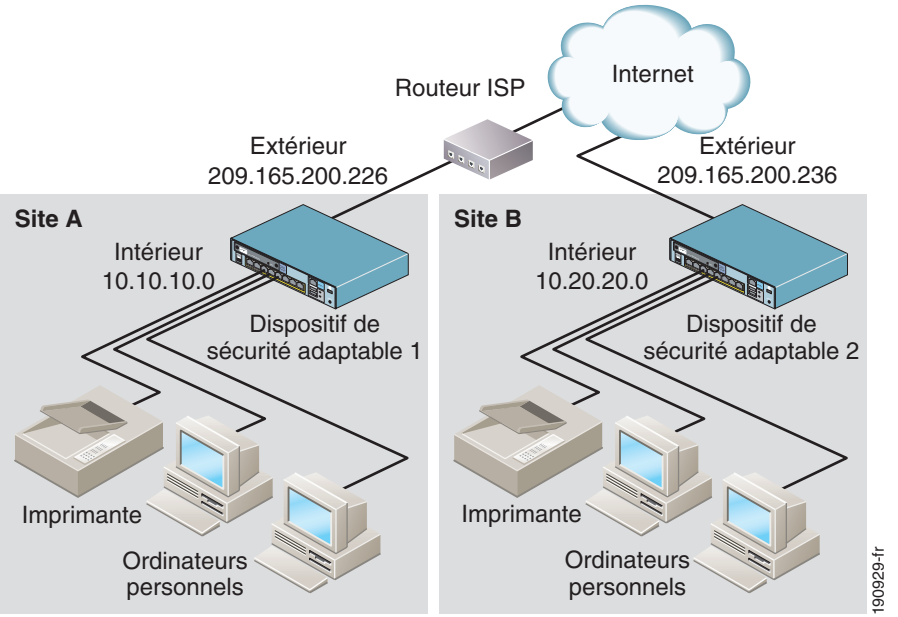
Les fonctionnalités VPN site à site du serveur de sécurité adaptatif permettent aux entreprises d'étendre leurs réseaux à travers des connexions Internet publiques à faible coût jusqu'à leurs partenaires et bureaux distants du monde entier, tout en conservant leur sécurité réseau. Une connexion VPN permet d'envoyer des données d'un emplacement à un autre via une connexion sécurisée, ou tunnel, en authentifiant tout d'abord les deux extrémités de la connexion, puis en cryptant automatiquement toutes les données envoyées entre ces deux sites.

Ce chapitre comprend les sections suivantes :

Exemple de topologie réseau d'un VPN site à site

La Figure 7-1 illustre un exemple de tunnel VPN entre deux serveur de sécurité adaptatif.

Figure 7-1 Topologie réseau du scénario de configuration VPN site à site



Pour déployer un VPN site à site tel que celui illustré à la Figure 7-1, vous devez configurer un serveur de sécurité adaptatif à chaque extrémité de la connexion.

Implémentation du scénario site à site

Cette section explique comment configurer la plate-forme serveur de sécurité adaptatif dans le cadre du déploiement d'un VPN site à site, en prenant les exemples de paramètres issus du cas d'accès à distance, qui paraissent dans la Figure 7-1.

Cette section comprend les rubriques suivantes :

Informations à garder à portée de main

Avant de commencer la procédure de configuration, recherchez les informations suivantes :

- Adresse IP de l'homologue du serveur de sécurité adaptatif distant
- Adresses IP des réseaux et hôtes locaux autorisés à utiliser le tunnel pour communiquer avec les ressources sur le site distant
- Adresses IP des réseaux et hôtes distants IP autorisés à utiliser le tunnel pour communiquer avec les ressources sur le site local.

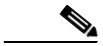
Configuration du VPN site à site

Cette section explique comment utiliser l'assistant VPN ASDM pour configurer le serveur de sécurité adaptatif pour un VPN site à site.

Cette section comprend les rubriques suivantes :

Les sections suivantes fournissent des instructions détaillées pour chaque étape de la configuration.

Configuration du serveur de sécurité sur le site local



Remarque Dans ce scénario, le serveur de sécurité adaptatif du premier site est appelé Serveur de sécurité 1.

Pour configurer le Serveur de sécurité 1, procédez comme suit :

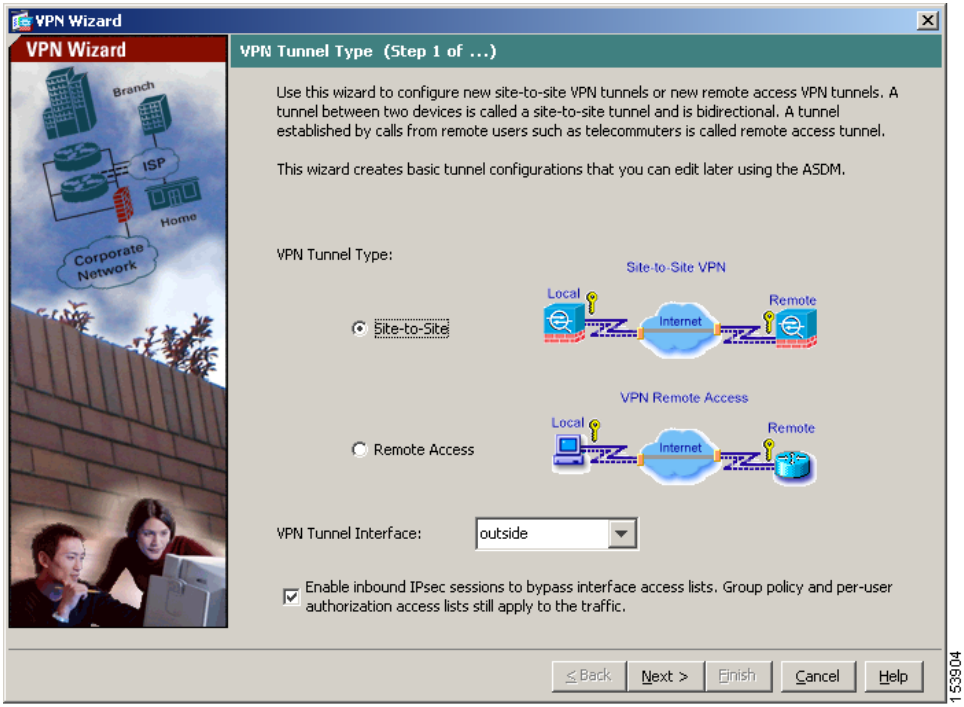
Étape 1 Dans la fenêtre ASDM principale, sélectionnez **IPsec VPN Wizard** (Assistant VPN IPsec) dans menu déroulant. ASDM ouvre le premier écran de l'assistant VPN.

À l'étape 1, procédez comme suit :

a. Dans la zone VPN Tunnel Type (Type de tunnel VPN), cochez la case d'option **Site-to-Site** (Site à site).

Remarque L'option VPN site à site permet de connecter deux passerelles de sécurité IPsec pouvant inclure un serveur de sécurité adaptatif ou plusieurs, des concentrateurs VPN ou d'autres périphériques prenant en charge la connectivité IPsec site à site.

b. Dans la liste déroulante VPN tunnel Interface (Interface tunnel VPN), sélectionnez **Outside** (Externe) comme interface activée du tunnel VPN actuel.



c. Cliquez sur **Next** (Suivant) pour continuer.

Saisie des informations sur l'homologue VPN distant

L'homologue VPN est le système situé à l'autre extrémité de la connexion que vous configurez. Il se trouve généralement sur un site distant.

Remarque Dans ce scénario, l'homologue VPN est appelé Serveur de sécurité 2.

À l'étape 2 de l'assistant VPN, procédez comme suit :

Étape 1 Saisissez l'adresse IP de l'homologue (l'adresse IP du Serveur de sécurité 2, soit dans ce scénario, 209.165.200.236) ainsi qu'un nom de groupe de tunnel (par exemple, « Cisco »).

Étape 2 Précisez le type d'authentification que vous souhaitez utiliser en sélectionnant l'une des méthodes d'authentification suivantes :

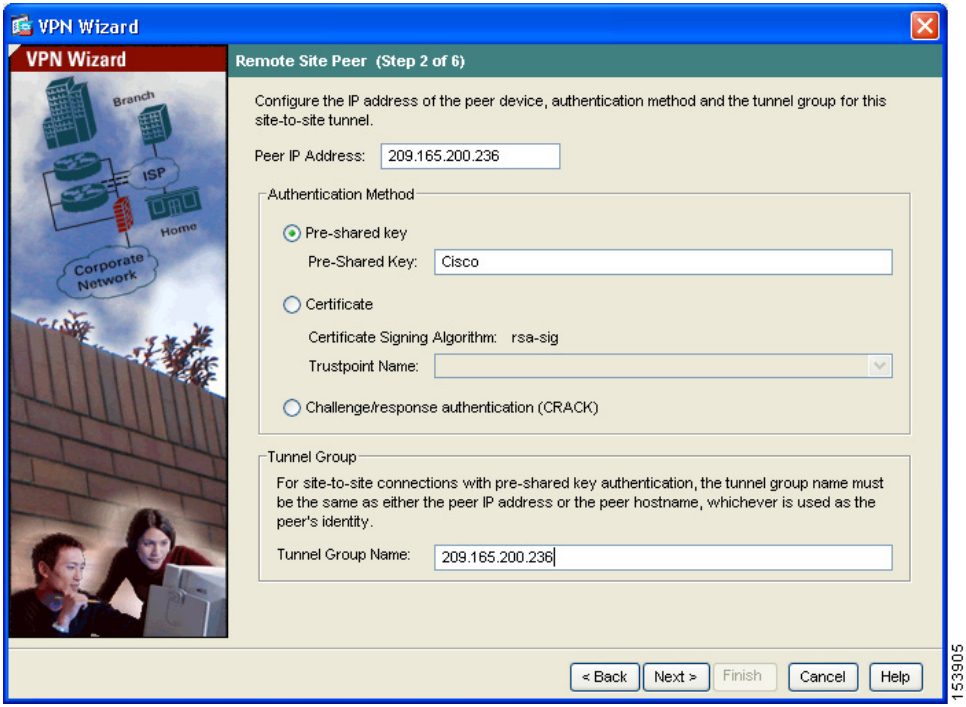
- Pour utiliser une clé pré-partagée statique pour l'authentification, cochez la case d'option **Pre-Shared Key** (Clé pré-partagée), puis saisissez une clé pré-partagée (par exemple, « Cisco »). Cette clé est utilisée pour les négociations IPsec entre les serveur de sécurité adaptatif.

  Remarque Lorsque vous utilisez une authentification de clé pré-partagée, le nom du groupe de tunnel doit être l'adresse IP de l'homologue.

- Pour utiliser des certificats numériques pour l'authentification, cochez la case d'option **Certificate** (Certificat), choisissez l'algorithme de signature de certificat dans la liste déroulante Certificate Signing Algorithm (Algorithme de signature du certificat), puis choisissez un nom de trustpoint préconfiguré dans la liste déroulante Trustpoint Name (Nom de trustpoint).

  Si vous souhaitez utiliser des certificats numériques pour l'authentification mais que vous n'avez pas encore configuré de nom de trustpoint, vous pouvez continuer la configuration avec l'assistant en utilisant l'une des deux autres options. Vous pouvez modifier la configuration d'authentification ultérieurement via les fenêtres ASDM standard.

- Cochez la case d'option **Challenge/Response Authentication** (CRACK) pour utiliser cette méthode d'authentification.



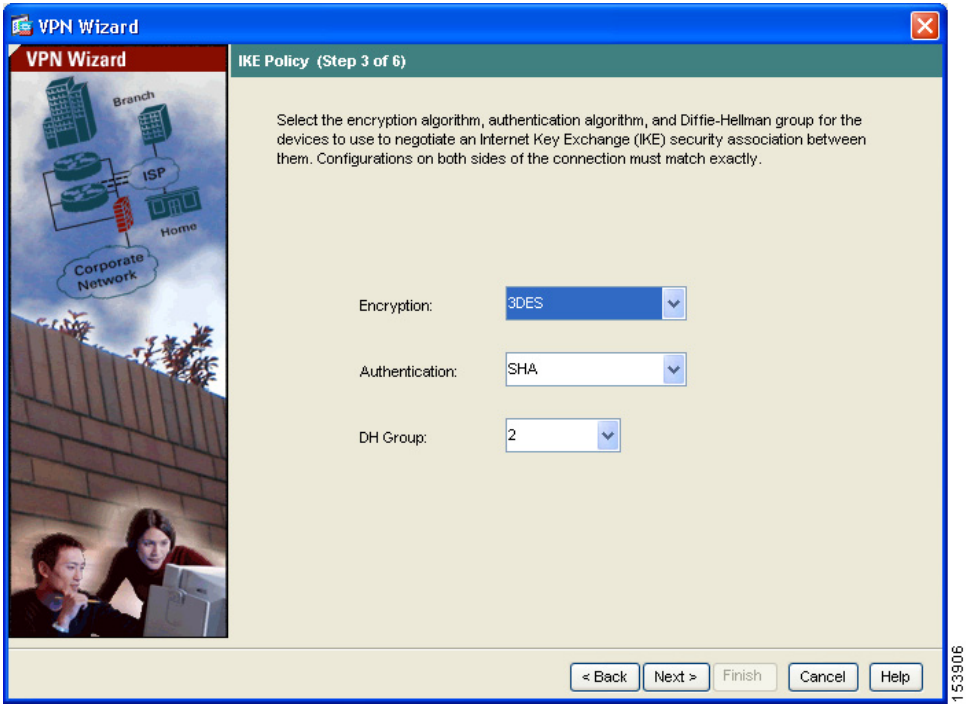
Étape 3 Cliquez sur **Next** (Suivant) pour continuer.

Configuration de la politique IKE

IKE est un protocole de négociation comprenant une méthode de cryptage pour protéger les données et garantir la confidentialité ; il fournit également l'authentification permettant de garantir l'identité des homologues. Dans la plupart des cas, les valeurs par défaut ASDM suffisent pour établir des tunnels VPN sécurisés entre deux homologues.

À l'étape 3 de l'assistant VPN, procédez comme suit :

Étape 1 Sélectionnez le type de cryptage (DES/3DES/AES), l'algorithme d'authentification (MD5/SHA) et le groupe Diffie-Hellman (1/2/5), utilisés par la plate-forme serveur de sécurité adaptatif lors d'une association de sécurité IKE.



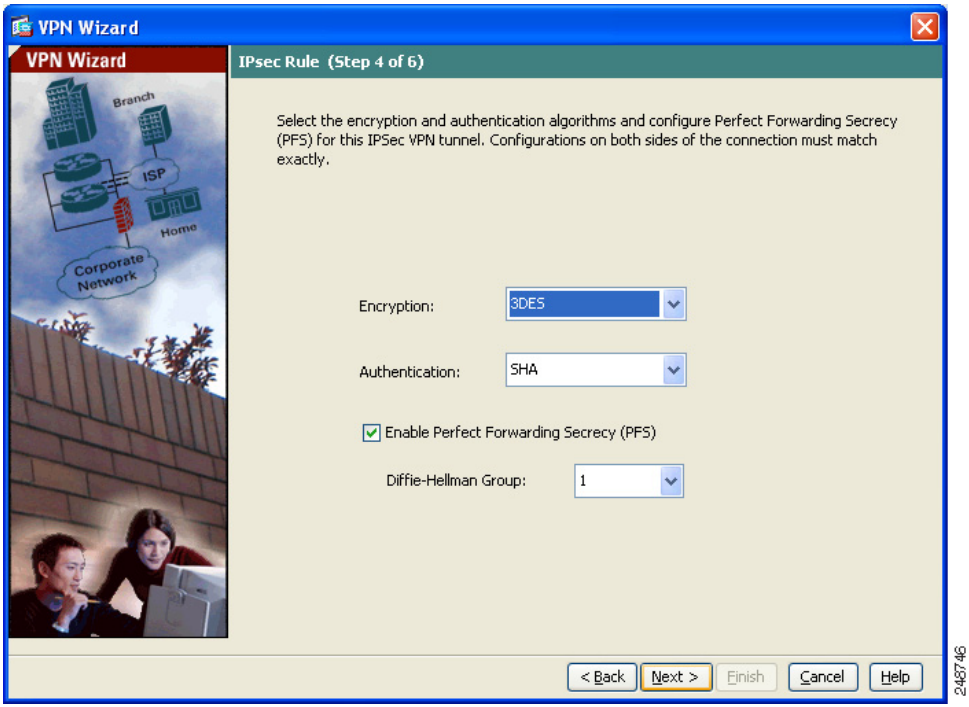
Remarque Lorsque vous configurez le Serveur de sécurité 2, saisissez les valeurs exactes pour chaque option choisie pour le Serveur de sécurité 1. Les non-correspondances de cryptage sont une cause courante d'échecs de tunnel VPN et peuvent ralentir le processus.

Étape 2 Cliquez sur **Next** (Suivant) pour continuer.

Configuration des paramètres d'authentification et du cryptage IPsec

À l'étape 4 de l'assistant VPN, procédez comme suit :

Étape 1 Choisissez l'algorithme de cryptage (DES/3DES/AES) dans la liste déroulante Encryption (Cryptage), puis l'algorithme d'authentification (MD5/SHA) dans la liste déroulante Authentication (Authentification).



Étape 2 Cochez la case d'option **Enable Perfect Forwarding Secrecy (PFS)** (Activer la parfaite confidentialité de transmission (PFS)) pour préciser si vous souhaitez utiliser la parfaite confidentialité de transmission, puis indiquez la taille des numéros à utiliser dans la liste déroulante Diffie-Hellman Group (Groupe Diffie-Hellman) pour générer les clés IPsec Phase 2.

PFS est un concept cryptographique où chaque nouvelle clé est différente des clés précédentes. Dans les négociations IPsec, les clés de phase 2 sont basées sur les clés de phase 1 sauf si la parfaite confidentialité de transmission est activée. PFS utilise des techniques Diffie-Hellman pour générer les clés.

Étape 3 Cliquez sur **Next** (Suivant) pour continuer.

Spécification des réseaux et des hôtes

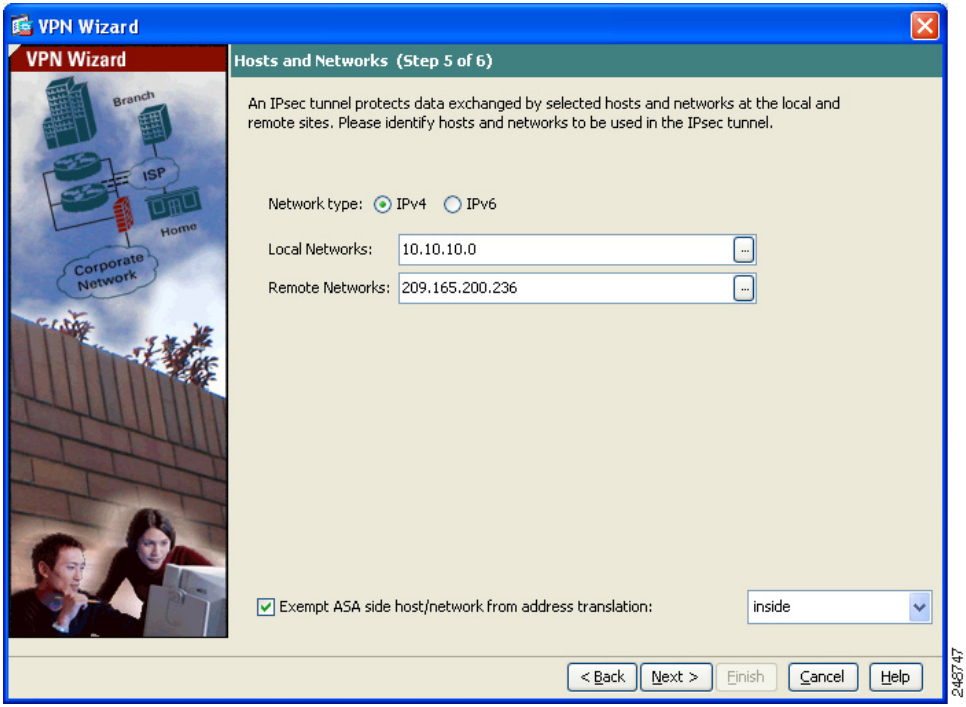
Identifiez les hôtes et réseaux sur le site local qui sont autorisés à utiliser ce tunnel IPsec pour communiquer avec les hôtes et réseaux situés à l'autre extrémité du tunnel. Précisez les hôtes et réseaux autorisés à accéder au tunnel en cliquant sur **Add** (Ajouter) ou sur **Delete** (Supprimer). Dans le scénario actuel, le trafic du Réseau A (10.10.10.0) est crypté par le Serveur de sécurité 1 et transmis via le tunnel VPN.

Par ailleurs, identifiez les hôtes et réseaux du site distant qui doivent pouvoir utiliser ce tunnel IPsec pour accéder aux hôtes et réseaux locaux. Ajoutez ou supprimez les hôtes et les réseaux de manière dynamique en cliquant respectivement sur **Add** (Ajouter) ou sur **Delete** (Supprimer). Dans ce scénario, pour le Serveur de sécurité 1, le réseau distant est le Réseau B (10.20.20.0), de manière que le trafic crypté à partir de ce réseau est autorisé via le tunnel.

À l'étape 5 de l'assistant VPN, procédez comme suit :

Étape 1 Saisissez l'adresse IP des réseaux locaux devant être protégés ou non, ou cliquez sur le bouton de points de suspension (...) pour effectuer votre sélection à partir d'une liste d'hôtes et de réseaux.

Étape 2 Saisissez l'adresse IP des réseaux distants devant être protégés ou non, ou cliquez sur le bouton de points de suspension (...) pour effectuer votre sélection à partir d'une liste d'hôtes et de réseaux.

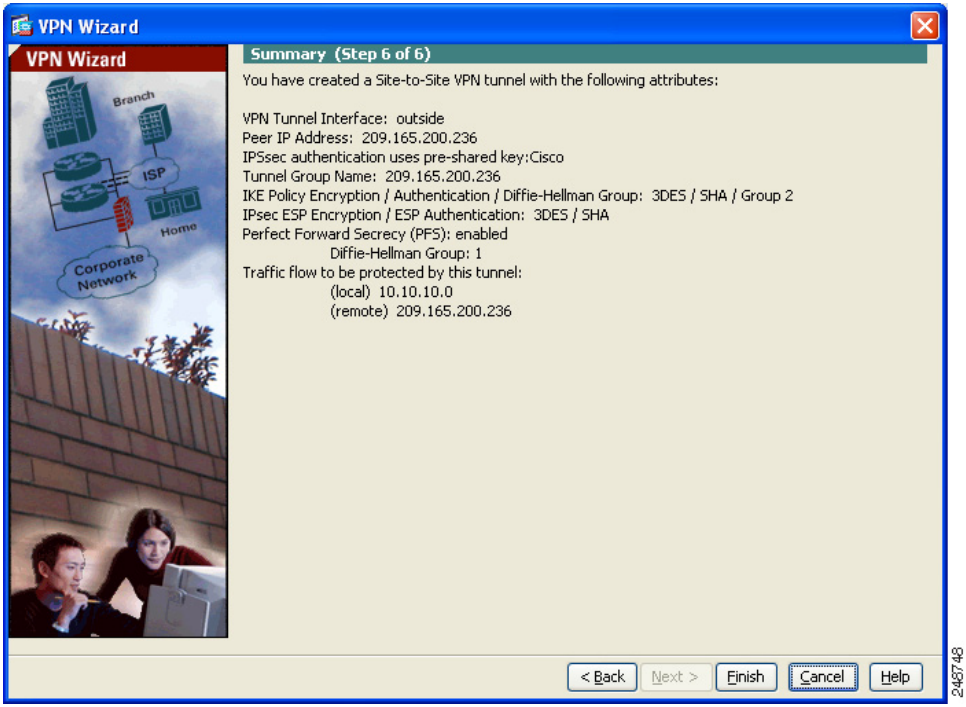


Étape 3 Si vous n'utilisez pas de traduction d'adresses de réseau (NAT) ni de traduction d'adresses de port (PAT), vérifiez la case **Exempt ASA side host network from address translation** et choisissez l'interface interne dans la liste déroulante.

Étape 4 Cliquez sur **Next** (Suivant) pour continuer.

Affichage des attributs du VPN et finalisation de la procédure à l'aide de l'assistant

À l'étape 6 de l'assistant VPN, vérifiez la liste de configuration du tunnel VPN que vous venez de créer.



Si cette configuration vous convient, cliquez sur **Finish** (Terminer) pour appliquer ces modifications au serveur de sécurité adaptatif.

Si vous souhaitez enregistrer les modifications apportées à la configuration de démarrage de façon que ces modifications s'appliquent au prochain démarrage du périphérique, cliquez sur **Save** (Enregistrer) dans le menu File (Fichier).

Sinon, ASDM vous invite à enregistrer les modifications de configuration de manière permanente lorsque vous quittez l'application.

Si vous n'enregistrez pas les modifications de configuration, l'ancienne configuration sera appliquée au prochain démarrage du périphérique.

Ainsi se termine le processus de configuration du Serveur de sécurité 1.

Configuration de l'autre extrémité de la connexion VPN

Vous venez de terminer la configuration du serveur de sécurité adaptatif local. À présent, vous devez configurer le serveur de sécurité adaptatif sur le site distant.

Au niveau du site distant, configurez le deuxième serveur de sécurité adaptatif de façon à servir d'homologue VPN. Répétez la procédure utilisée pour configurer le serveur de sécurité adaptatif local, en commençant par section « Configuration du serveur de sécurité sur le site local » à la page 7-3 et en finissant par section *« Affichage des attributs du VPN et finalisation de la procédure à l'aide de l'assistant » à la page 7-12*.

Remarque Lorsque vous configurez le Serveur de sécurité 2, utilisez les mêmes valeurs pour chaque option sélectionnée pour le Serveur de sécurité 1, à l'exception des réseaux et hôtes locaux. Les non-correspondances sont une cause courante d'échecs de configuration VPN.

Pour obtenir des informations sur la vérification et le dépannage de la configuration d'un VPN site à site, consultez la section « Dépannage du Serveur de sécurité » du document *Guide de configuration de la gamme Cisco ASA 5500 utilisant l'interface CLI*.

Si vous rencontrez des problèmes spécifiques, consultez les notes techniques de dépannage disponibles à l'adresse URL suivante :

http://www.cisco.com/en/US/products/ps6120/prod_tech_notes_list.html

Pour obtenir de l'aide relative à des problèmes de configuration, consultez les exemples de configuration et notes techniques à l'adresse URL suivante :

http://www.cisco.com/en/US/products/ps6120/prod_configuration_examples_list.html

En particulier, lisez les notes concernant le VPN site à site (L2L) avec ASA des notes techniques traitant du dépannage. Les notes techniques traitant du dépannage vous expliquent en détail l'utilisation de commandes qui vous permettront de résoudre des problèmes de configuration du VPN site à site. Ces commandes sont :

- **show run isakmp**
- **show run ipsec**
- **show run tunnel-group**

- **show run crypto map**
- **debug crypto ipsec sa**
- **debug crypto isakmp sa.**

Consultez également le document *Référence des commandes de la gamme Cisco ASA 5500* pour obtenir des informations détaillées sur chacune de ces commandes.

Étapes suivantes

Si vous déployez le serveur de sécurité adaptatif uniquement dans un environnement VPN site à site, vous avez terminé la configuration initiale. Par ailleurs, vous pouvez envisager d'effectuer l'une des étapes suivantes.

Pour effectuer l'action suivante...	Voir...
Affiner la configuration et configurer des fonctionnalités facultatives et avancées	*Guide de configuration de la gamme Cisco ASA 5500 utilisant l'interface CLI*
En savoir plus sur les opérations quotidiennes	*Référence des commandes de la gamme Cisco ASA 5500* *Messages de journalisation système de la gamme Cisco ASA 5500*

Vous pouvez configurer le serveur de sécurité adaptatif pour plusieurs applications. Les sections suivantes fournissent les procédures de configuration pour les autres applications communes du serveur de sécurité adaptatif.

Pour effectuer l'action suivante...	Voir...
Configurer un VPN d'accès à distance	Chapitre 8, « Scénario : configuration du VPN d'accès à distance IPsec »
Configurer un VPN SSL sans client (basé sur le navigateur)	Chapitre 6, « Scénario : connexions VPN SSL sans client »
Configure un VPN SSL pour le client logiciel AnyConnect de Cisco	Chapitre 5, « Scénario : configuration de connexions pour un client VPN AnyConnect de Cisco »

CHAPITRE 8

Scénario : configuration du VPN d'accès à distance IPsec

Ce chapitre explique comment utiliser le serveur de sécurité adaptatif pour accueillir des connexions VPN d'accès à distance de type IPsec. Un VPN d'accès à distance permet de créer des connexions sécurisées, ou tunnels, sur Internet, afin de fournir un accès sécurisé à tous les utilisateurs hors site. Dans ce type de configuration VPN, les utilisateurs distants doivent exécuter le client VPN Cisco pour se connecter au serveur de sécurité adaptatif.

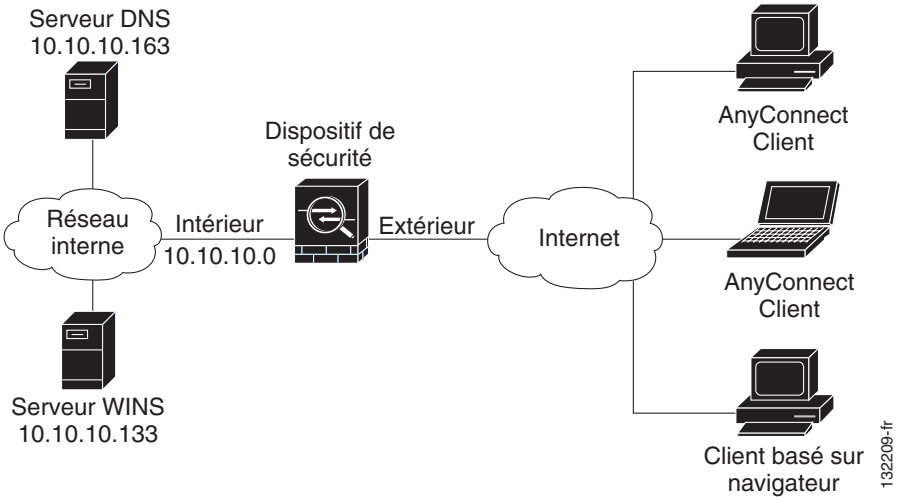
Si vous implémentez une solution Easy VPN, ce chapitre vous explique comment configurer le serveur Easy VPN (parfois appelé périphérique de tête de réseau).

Ce chapitre comprend les sections suivantes :

Exemple de topologie réseau VPN d'accès à distance IPsec

La Figure 8-1 illustre un serveur de sécurité adaptatif configuré pour accepter des demandes de clients VPN et pour établir des connexions IPsec avec des clients VPN, tels qu'un logiciel Easy VPN de Cisco ou des clients matériel sur Internet.

Figure 8-1 Configuration réseau du scénario VPN d'accès à distance



Implémentation du scénario VPN d'accès à distance IPsec

Cette section explique comment configurer le serveur de sécurité adaptatif de sorte qu'il accueille des connexions VPN IPsec issues de périphériques et de clients distants. Si vous implémentez une solution Easy VPN, cette section vous explique comment configurer un serveur Easy VPN (également connu sous le nom de périphérique de tête de réseau).

Les valeurs des paramètres de configuration de l'exemple sont tirées du scénario d'accès à distance illustré à la Figure 8-1.

Cette section comprend les rubriques suivantes :

Informations à garder à portée de main

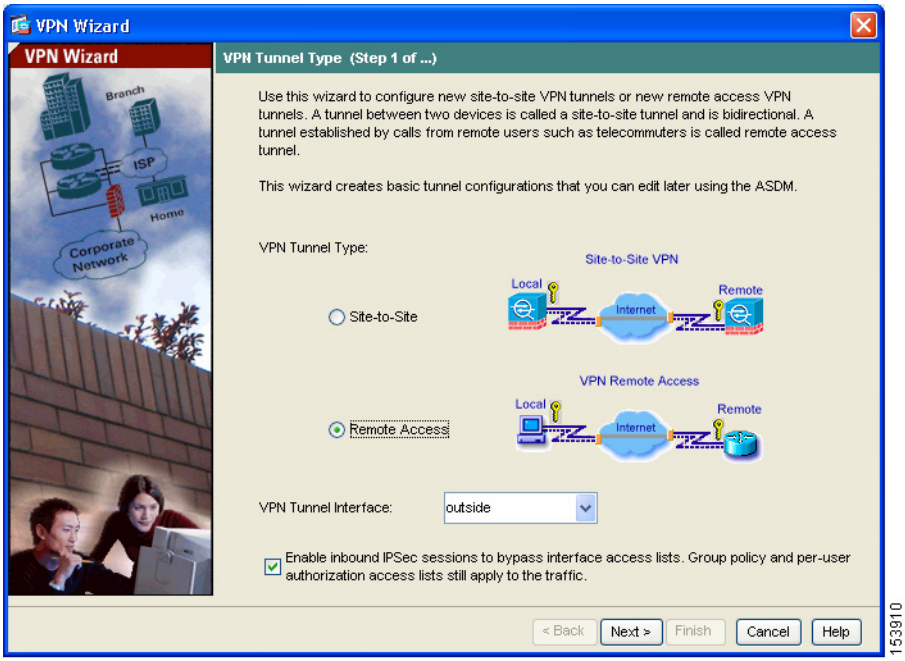
Avant de commencer à configurer le serveur de sécurité adaptatif pour accepter les connexions VPN d'accès à distance IPsec, assurez-vous que vous disposez des informations suivantes :

- Plage d'adresses IP à utiliser dans un pool IP. Ces adresses sont affectées aux clients VPN distants au fur et à mesure que leur connexion est établie.
- Liste des utilisateurs à prendre en compte pour créer une base de données d'authentification locale, sauf si vous utilisez un serveur AAA pour l'authentification.
- Informations concernant le réseau destinées aux clients distants lorsqu'ils se connectent au VPN, notamment les suivantes :
  - Adresses IP des serveurs DNS primaires et secondaires
  - Adresses IP des serveurs WINS primaires et secondaires
  - Nom de domaine par défaut
  - Liste des adresses IP pour les réseaux, groupes et hôtes locaux devant être accessibles aux clients distants authentifiés.

Configuration d'un VPN d'accès à distance IPsec

Pour configurer un VPN d'accès à distance, procédez comme suit :

Étape 1 Dans la fenêtre ASDM principale, choisissez **IPsec VPN Wizard** (Assistant VPN IPsec) dans le menu déroulant Wizards (Assistants). Vous accédez à l'étape 1 de l'assistant VPN.



Étape 2 Dans cet écran, procédez comme suit :

a. Cochez la case d'option **Remote Access** (Accès distant).

b. Dans la liste déroulante, sélectionnez **Outside** (Externe) comme interface activée pour les tunnels VPN entrants.

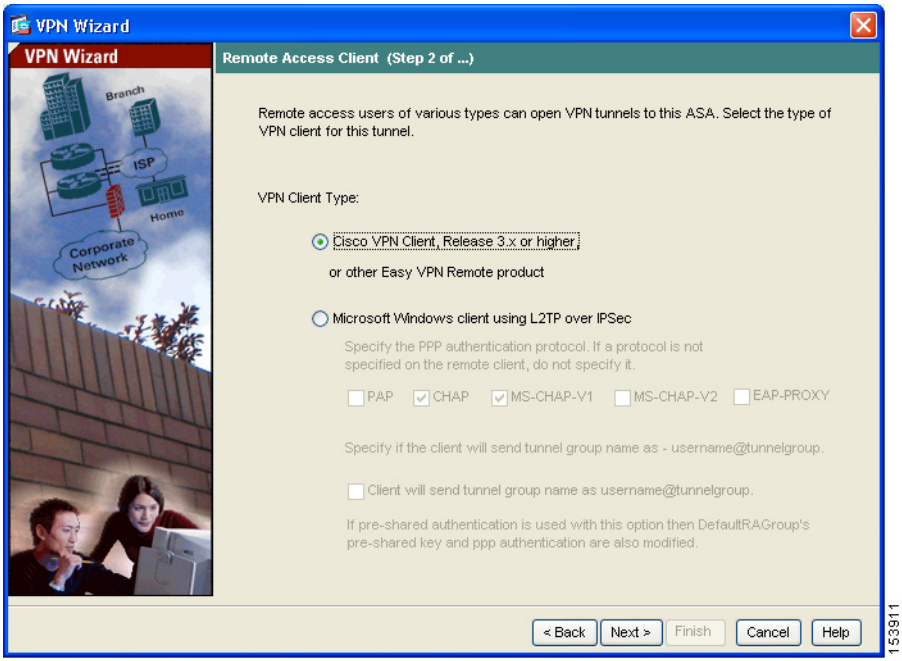
c. Cliquez sur **Next** (Suivant) pour continuer.

Sélection des types de client VPN

À l'étape 2 de l'assistant VPN, procédez comme suit :

Étape 1 Spécifiez le type de client VPN qui permettra aux utilisateurs distants de se connecter à ce serveur de sécurité adaptatif. Pour ce scénario, cochez la case d'option **Cisco VPN Client** (Client VPN Cisco).

Vous pouvez également utiliser tout autre produit distant Easy VPN de Cisco.



Étape 2 Cliquez sur **Next** (Suivant) pour continuer.

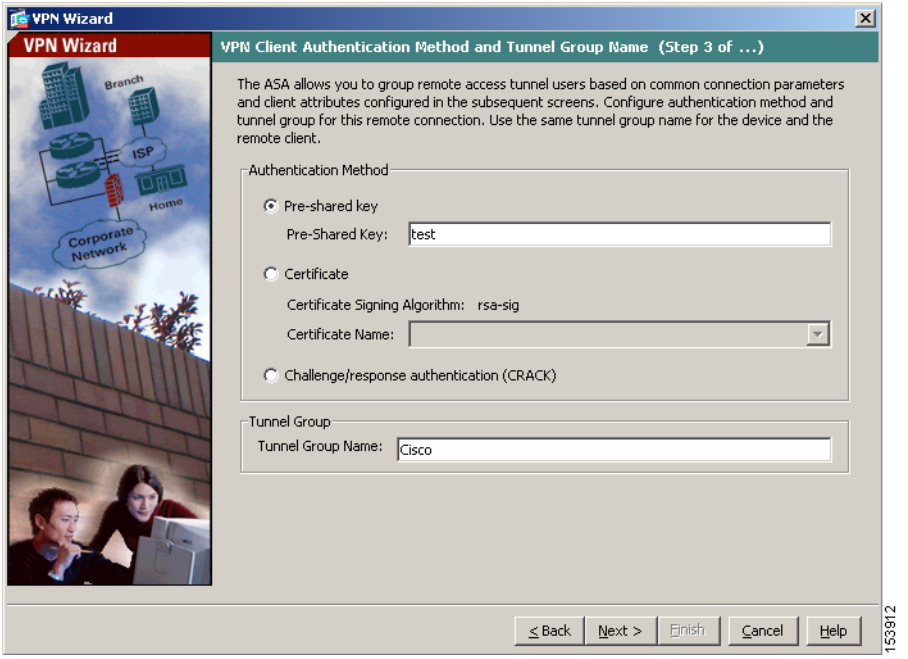
Spécification du nom de groupe du tunnel VPN et méthode d'authentification

À l'étape 3 de l'assistant VPN, procédez comme suit :

Étape 1 Précisez le type d'authentification que vous souhaitez utiliser en effectuant l'une des étapes suivantes :

- Pour utiliser une clé pré-partagée statique pour l'authentification, cochez la case d'option **Pre-Shared Key** (Clé pré-partagée) puis saisissez une clé pré-partagée (par exemple, « Cisco »). Cette clé est utilisée pour les négociations IPsec.
- Pour utiliser des certificats numériques pour l'authentification, cochez la case d'option **Certificate** (Certificat), sélectionnez Certificate Signing Algorithm (Algorithme de signature du certificat) dans la liste déroulante, puis choisissez un nom de trustpoint dans la liste déroulante.

  Si vous souhaitez utiliser des certificats numériques pour l'authentification mais que vous n'avez pas encore configuré de nom de trustpoint, vous pouvez continuer la configuration avec l'assistant en utilisant l'une des deux autres options. Vous pouvez modifier la configuration d'authentification ultérieurement via les fenêtres ASDM standard.
- Cochez la case d'option **Challenge/Response Authentication (CRACK)** pour utiliser cette méthode d'authentification.



Étape 2 Saisissez un nom de groupe de tunnel (par exemple, « Cisco ») pour l'ensemble des utilisateurs qui se servent d'attributs client et de paramètres de connexion communs pour se connecter à ce serveur de sécurité adaptatif.

Étape 3 Cliquez sur **Next** (Suivant) pour continuer.

Spécification d'une méthode d'authentification des utilisateurs

Les utilisateurs peuvent être authentifiés soit par une base de données d'authentification locale, soit par des serveurs AAA (Authentication, Authorization and Accounting) (RADIUS, TACACS+, SDI, NT, Kerberos et LDAP).

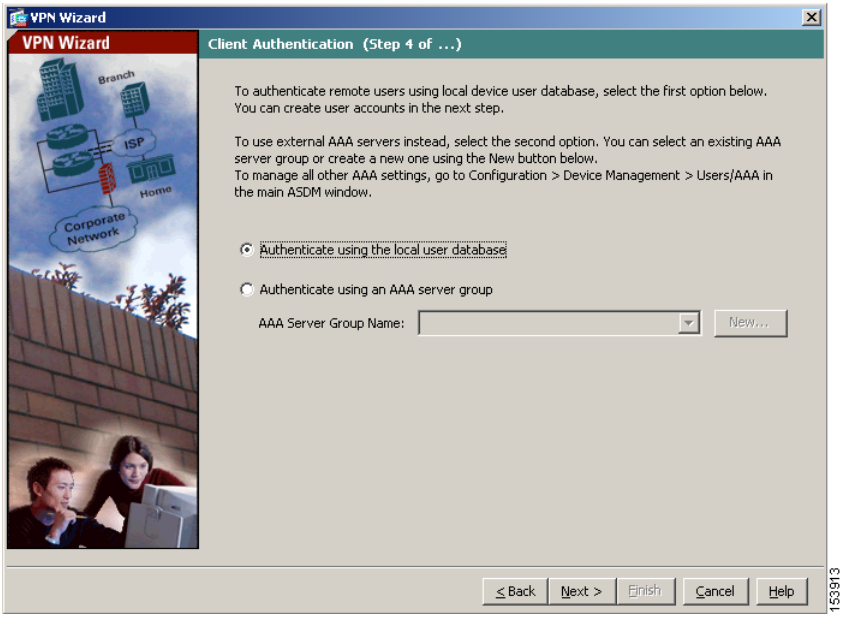
À l'étape 4 de l'assistant VPN, procédez comme suit :

Étape 1 Si vous souhaitez authentifier des utilisateurs en créant une base de données d'utilisateurs sur le serveur de sécurité adaptatif, cochez la case d'option **Authenticate Using the Local User Database** (Authentifier via la base de données d'utilisateurs locale).

Étape 2 Si vous souhaitez authentifier les utilisateurs via un groupe de serveurs AAA externe :

a. Cochez la case d'option **Authenticate Using an AAA Server Group** (Authentifier via un groupe de serveurs AAA).

b. Sélectionnez un groupe de serveurs préconfiguré dans la liste déroulante Authenticate using a AAA server group (Authentifier via un groupe de serveurs AAA) ou cliquez sur **New** (Nouveau) pour ajouter un nouveau groupe de serveurs AAA.



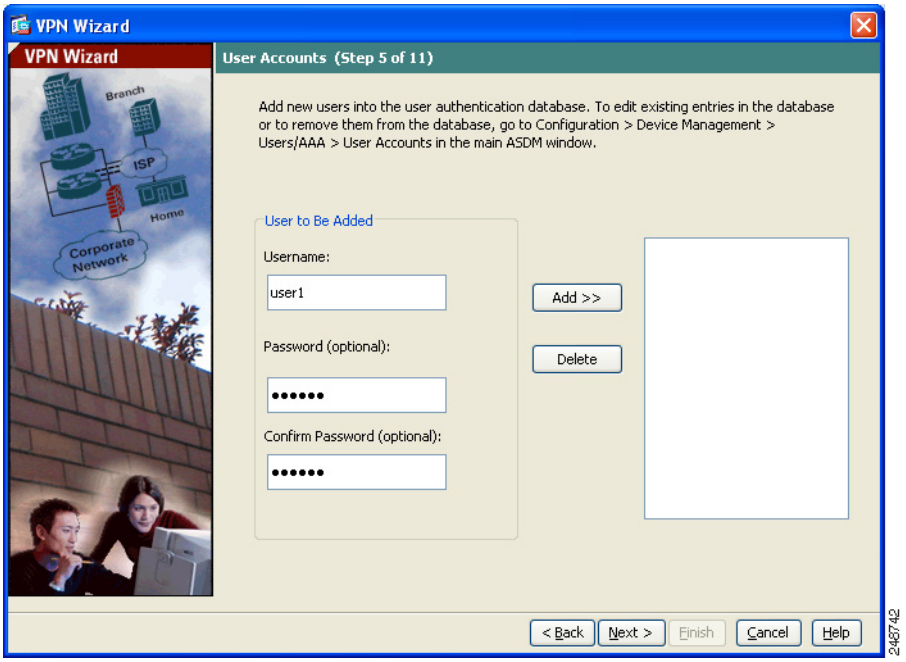
Étape 3 Cliquez sur **Next** (Suivant) pour continuer.

Configuration des comptes utilisateurs (facultatif)

Si vous avez choisi d'authentifier les utilisateurs via la base de données d'utilisateurs locale, vous pouvez y créer de nouveaux comptes utilisateurs. Vous pouvez également ajouter des utilisateurs ultérieurement via l'interface de configuration ASDM.

À l'étape 5 de l'assistant VPN, procédez comme suit :

Étape 1 Pour ajouter un nouvel utilisateur, saisissez un nom d'utilisateur et un mot de passe, puis cliquez sur **Add** (Ajouter).



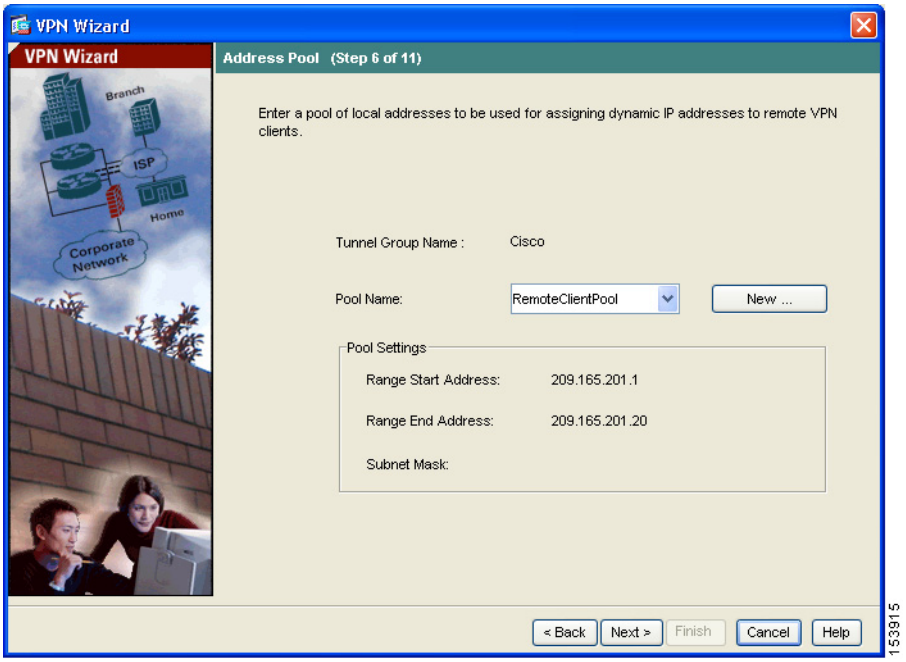
Étape 2 Lorsque vous avez ajouté de nouveaux utilisateurs, cliquez sur **Next** (Suivant) pour continuer.

Configuration de pools d'adresse

Pour permettre aux clients distants d'accéder à votre réseau, vous devez configurer un pool d'adresses IP pouvant être affectées aux clients VPN distants lorsqu'ils se connectent. Dans un tel cas, le pool est configuré pour utiliser la plage d'adresses IP 209.165.201.1–209.166.201.20.

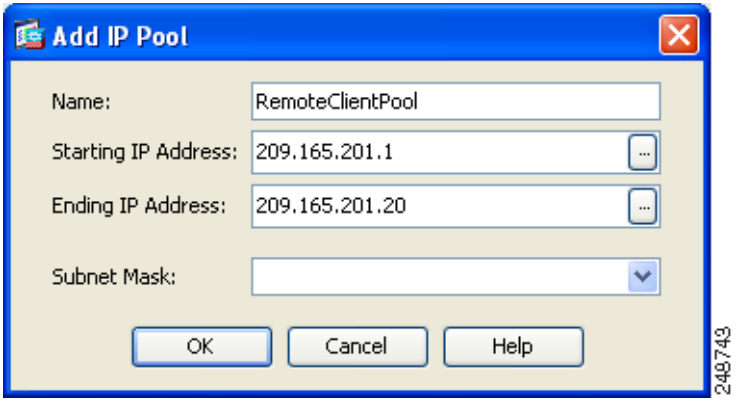
À l'étape 6 de l'assistant VPN, procédez comme suit :

Étape 1 Saisissez un nom de pool ou choisissez un pool préconfiguré à partir de la liste déroulante Pool Name (Nom du pool).



Vous pouvez également cliquer sur **New** (Nouveau) pour créer un nouveau pool d'adresses.

La boîte de dialogue Add IP Pool (Ajouter Pool ID) apparaît.



Étape 2 Dans cette dernière, procédez comme suit :

a. Saisissez l'adresse IP de début et l'adresse IP de fin de la plage.

b. (Facultatif) Saisissez ou choisissez un masque de sous-réseau pour la plage d'adresses IP dans la liste déroulante Subnet Mask (Masque de sous-réseau).

c. Cliquez sur **OK** pour revenir au sixième écran (Étape 6) de l'assistant VPN.

Étape 3 Cliquez sur **Next** (Suivant) pour continuer.

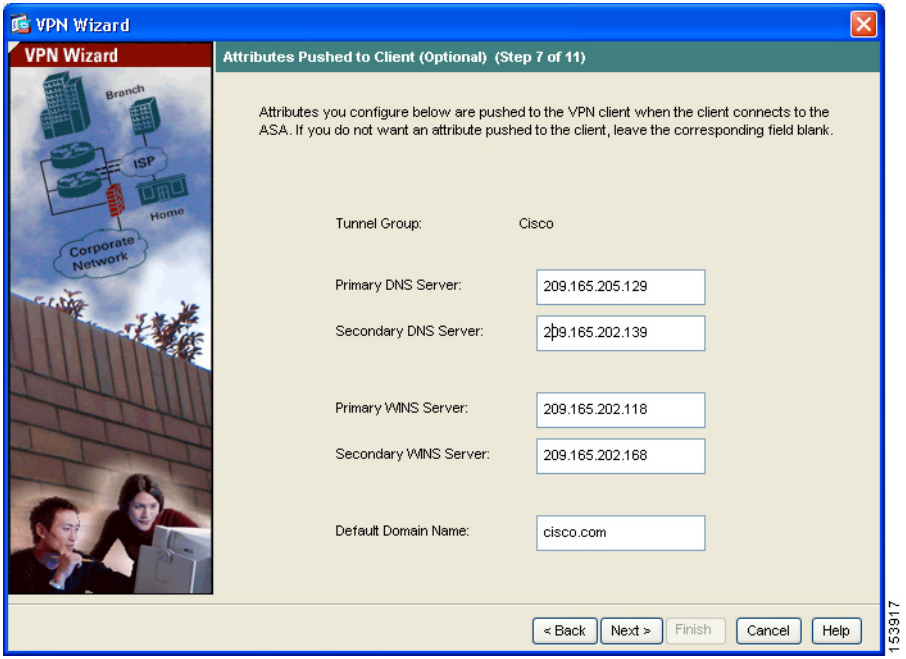
Configuration des attributs du client

Pour accéder à votre réseau, chaque client distant requiert des informations concernant la configuration réseau de base, telles que le nom des serveurs DNS et WINS à utiliser et le nom de domaine par défaut. Au lieu de configurer individuellement chaque client distant, vous pouvez fournir à ASDM les informations client. Le serveur de sécurité adaptatif transmet ces informations au client distant ou au client matériel Easy VPN lorsqu'une connexion est établie.

Vérifiez que vous avez saisi des valeurs correctes sinon, les clients distants ne pourront pas utiliser les noms DNS pour la résolution ou l'utilisation du réseau Windows.

À l'étape 7 de l'assistant VPN, procédez comme suit :

Étape 1 Saisissez les informations concernant la configuration réseau à transmettre aux clients distants.



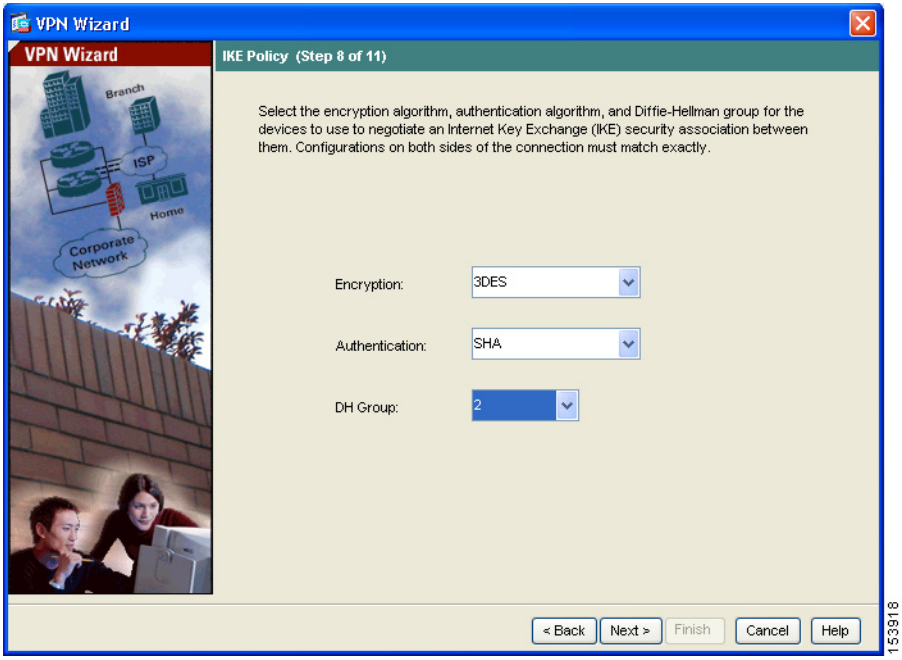
Étape 2 Cliquez sur **Next** (Suivant) pour continuer.

Configuration de la politique IKE

IKE est un protocole de négociation comprenant une méthode de cryptage pour protéger les données et garantir la confidentialité ; il s'agit également d'une méthode d'authentification qui permet de garantir l'identité des homologues. Dans la plupart des cas, les valeurs par défaut ASDM suffisent pour établir des tunnels VPN sécurisés.

Pour spécifier la politique IKE à l'étape 8 de l'assistant VPN, procédez comme suit :

Étape 1 Choisissez le cryptage (DES/3DES/AES), les algorithmes d'authentification (MD5/SHA) et le groupe Diffie-Hellman (02/01/05/7) utilisés par le serveur de sécurité adaptatif lors d'une association de sécurité IKE.



Étape 2 Cliquez sur **Next** (Suivant) pour continuer.

Spécification de l'exception de traduction de l'adresse et contrôle de séparation des flux

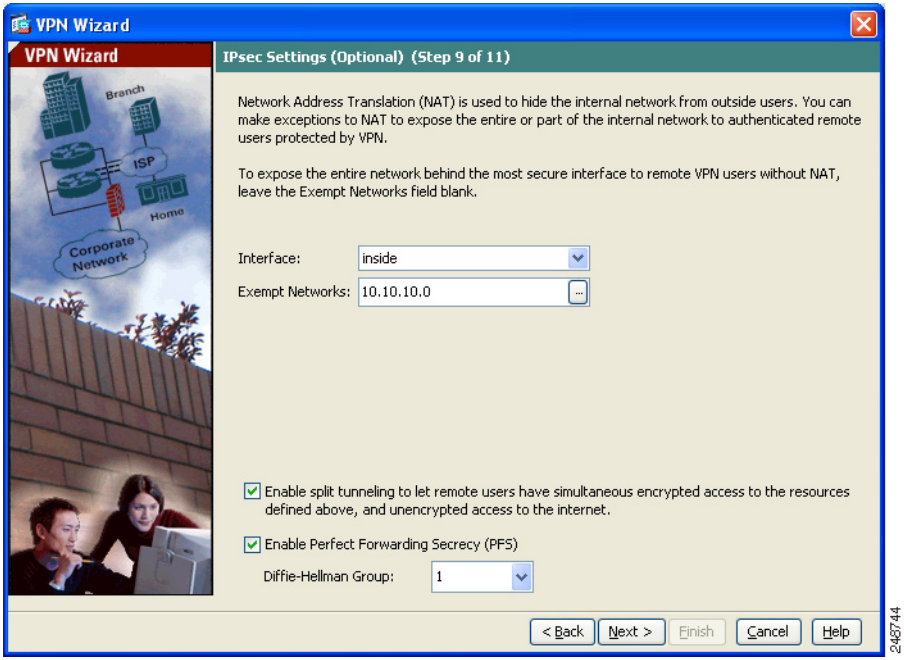
Le contrôle de séparation des flux (split tunneling) permet aux clients IPsec distants d'envoyer des paquets, sous certaines conditions, dans un tunnel IPsec en format crypté ou vers une interface réseau en format texte.

Le serveur de sécurité adaptatif utilise la Traduction d'adresses de réseau (NAT) pour éviter une exposition externe des adresses IP internes. Vous pouvez définir des exceptions pour cette protection réseau en identifiant des réseaux et des hôtes locaux auxquels des utilisateurs distants authentifiés doivent pouvoir accéder.

À l'étape 9 de l'assistant VPN, procédez comme suit :

Étape 1 Indiquez les hôtes, groupes et réseaux devant se trouver dans la liste des ressources internes accessibles par des utilisateurs distants authentifiés.

Pour ajouter ou retirer des hôtes, groupes et réseaux de manière dynamique de la zone Selected Hosts/Networks (Réseaux/hôtes sélectionnés), cliquez respectivement sur **Add** (Ajouter) ou **Delete** (Supprimer).



Étape 2 Pour activer le contrôle de séparation des flux (split tunneling), cochez la case d'option **Enable Split Tunneling** (Activer le contrôle de séparation des flux). Le contrôle de séparation des flux permet au trafic extérieur aux réseaux configurés d'être envoyé directement vers Internet et non via un tunnel VPN crypté.

Étape 3 Pour activer la confidentialité de transmission parfaite (PFS), cochez la case d'option **Enable Perfect Forwarding Secrecy** (Activer la parfaite confidentialité de transmission). L'activation de la PFS définit la taille des numéros à utiliser pour générer les clés IPsec phase 2.

PFS est un concept cryptographique où chaque nouvelle clé est différente des clés précédentes. Dans les négociations IPsec, les clés de la phase 2 sont basées sur les clés de la phase 1 sauf si la parfaite confidentialité de transmission est activée. PFS utilise des techniques Diffie-Hellman pour générer les clés. PFS garantit qu'une clé de session provenant d'un ensemble de clés privées et publiques à long terme n'est pas compromise si l'une des clés privées est compromise ultérieurement.

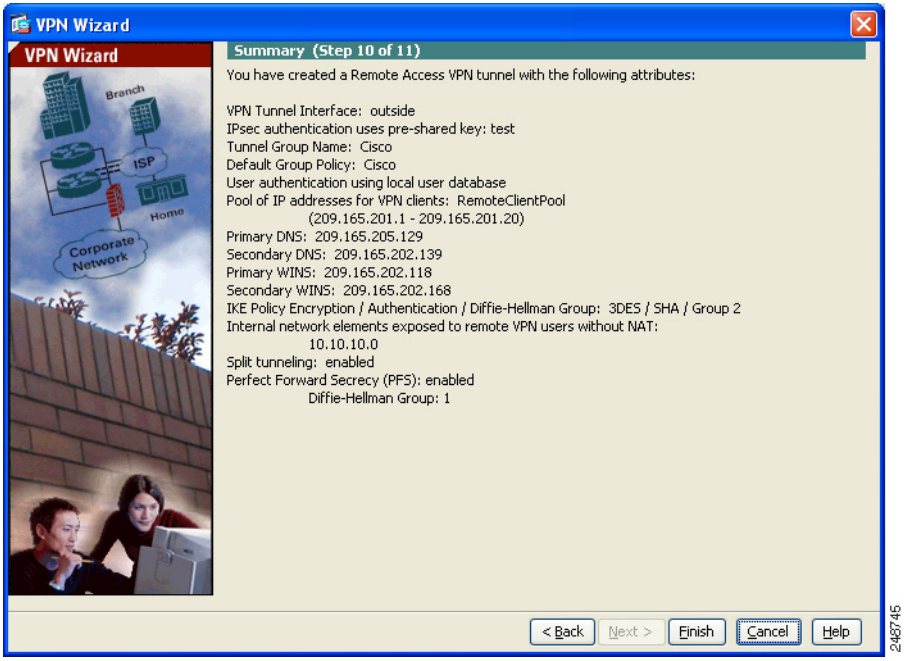
Remarque PFS doit être activée aux deux extrémités de la connexion.

Étape 4 Sélectionnez l'identifiant de groupe Diffie-Hellman que les deux homologues IPsec utilisent pour dériver un secret partagé sans se le transmettre. Le groupe par défaut, le groupe 2 (1024-bit Diffie-Hellman), requiert moins de temps CPU pour s'exécuter, mais il est moins sécurisé que le groupe 5 (1536-bit). Le groupe 7 doit être utilisé avec le client VPN Movian mais fonctionne avec tout homologue qui le prend en charge (ECC).

Étape 5 Cliquez sur **Next** (Suivant) pour continuer.

Vérification des configurations VPN d'accès à distance

À l'étape 10 de l'assistant VPN, vérifiez les attributs de configuration du nouveau tunnel VPN. La configuration affichée doit être similaire à la suivante :



Si cette configuration vous convient, cliquez sur **Finish** (Terminer) pour appliquer les modifications au serveur de sécurité adaptatif.

Si vous souhaitez enregistrer les modifications apportées à la configuration de démarrage de façon que ces modifications s'appliquent au prochain démarrage du périphérique, cliquez sur **Save** (Enregistrer) dans le menu File (Fichier). Sinon, ASDM vous invite à enregistrer les modifications de configuration de manière permanente lorsque vous quittez l'application.

Si vous n'enregistrez pas les modifications de configuration, l'ancienne configuration sera appliquée au prochain démarrage du périphérique.

Étapes suivantes

Pour établir des tunnels VPN cryptés de bout en bout et permettre ainsi aux employés en déplacement ou au télétravailleurs de bénéficier d'une connectivité sécurisée, faites l'acquisition du logiciel client VPN de Cisco.

Pour obtenir plus d'informations sur le client VPN de Cisco Systems, consultez l'URL suivante :
http://www.cisco.com/en/US/products/sw/secursw/ps2308/index.html

Si vous déployez le serveur de sécurité adaptatif uniquement dans un environnement VPN d'accès à distance, vous avez terminé la configuration initiale. Par ailleurs, vous pouvez envisager d'effectuer l'une des étapes suivantes.

Pour effectuer l'action suivante...	Voir...
Affiner la configuration et configurer des fonctionnalités facultatives et avancées	*Guide de configuration de la gamme Cisco ASA 5500 utilisant l'interface CLI*
En savoir plus sur les opérations quotidiennes	*Référence des commandes de la gamme Cisco ASA 5500* *Messages de journalisation système de la gamme Cisco ASA 5500*

Vous pouvez configurer le serveur de sécurité adaptatif pour plusieurs applications. Les sections suivantes fournissent les procédures de configuration pour les autres applications communes du serveur de sécurité adaptatif.

Pour effectuer l'action suivante...	Voir...
Configurer un VPN SSL pour le client logiciel AnyConnect de Cisco	Chapitre 5, « Scénario : configuration de connexions pour un client VPN AnyConnect de Cisco »
Configurer un VPN SSL sans client (basé sur le navigateur)	Chapitre 5, « Scénario : configuration de connexions pour un client VPN AnyConnect de Cisco »
Configurer un VPN site à site	Chapitre 7, « Scénario : configuration du VPN site à site »

ANNEXE A

Obtention d'une licence 3DES/AES

L'ASA 5580 de Cisco est livré avec une licence DES qui fournit le cryptage. Vous pouvez obtenir une licence 3DES/AES fournissant la technologie de cryptage permettant d'activer des fonctionnalités spécifiques, telles que la gestion à distance sécurisée (SSH, ASDM, etc.), le VPN site à site et le VPN d'accès à distance. Une clé de licence de cryptage est requise pour activer cette licence.

Si vous êtes inscrit sur Cisco.com, vous pouvez obtenir une licence de cryptage 3DES/AES à partir du site Web suivant :

http://www.cisco.com/go/license.

Sinon, consultez le site Web suivant :

https://tools.cisco.com/SWIFT/Licensing/RegistrationServlet.

Indiquez votre nom, votre adresse e-mail et le numéro de série du serveur de sécurité adaptatif tel qu'il apparaît dans la sortie de commande **show version**.

Remarque Vous recevrez la nouvelle clé d'activation de votre serveur de sécurité adaptatif dans les deux heures suivant la demande de mise à niveau de licence.

Pour obtenir plus d'informations sur les exemples de clé d'activation ou la mise à niveau du logiciel, consultez le document *Guide de configuration de la gamme Cisco ASA 5500 utilisant l'interface CLI*.

Pour utiliser la clé d'activation, procédez comme suit :

	Commande	Objectif
Step 1	`hostname# show version`	Affiche la version du logiciel, la configuration matérielle, la clé de licence et le temps de disponibilité associé.
Step 2	`hostname# activation-key activation-5-tuple-key`	Met à jour la clé d'activation de cryptage en remplaçant la variable *activation-5-tuple-key* par la clé d'activation obtenue avec votre nouvelle licence. La variable *activation-5-tuple-key* est une chaîne hexadécimale composée de 5 éléments séparés par un espace. Exemple : 0xe02888da 0x4ba7bed6 0xf1c123ae 0xffd8624e 0x1234abcd. Où « 0x » est facultatif ; toutes les valeurs sont censées être hexadécimales. **Remarque** Il est inutile de recharger la configuration, si vous réduisez le nombre de fonctionnalités sous licence.