Guide de l'utilisateur de Cisco SDM Express

Siège social
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
États-Unis
http://www.cisco.com
Tél. : 408 526-4000
+1 800 553-NETS (6387)
Télécopie : 408 526-4100

Numéro de commande client :
Numéro de série du texte : OL-7141-04

LES SPÉCIFICATIONS ET LES INFORMATIONS CONCERNANT LES PRODUITS DÉCRITS DANS CE MANUEL PEUVENT ÊTRE MODIFIÉES SANS PRÉAVIS. TOUTES LES DÉCLARATIONS, INFORMATIONS ET RECOMMANDATIONS FIGURANT DANS CE MANUEL SONT CENSÉES ÊTRES EXACTES, MAIS SONT PRÉSENTÉES SANS GARANTIE D'AUCUNE SORTE, EXPLICITE OU IMPLICITE. LES UTILISATEURS ASSUMENT LA PLEINE ET ENTIÈRE RESPONSABILITÉ DE L'UTILISATION DES PRODUITS.

LA LICENCE LOGICIELLE ET LA GARANTIE LIMITÉE DES PRODUITS D'ACCOMPAGNEMENT SONT PRÉSENTÉES DANS LES NOTICES INFORMATIVES ACCOMPAGNANT LE PRODUIT. ELLES SONT FOURNIES ICI À TITRE DE RÉFÉRENCE. SI VOUS NE TROUVEZ PAS LA LICENCE DU LOGICIEL OU LA GARANTIE LIMITÉE, CONTACTEZ VOTRE REPRÉSENTANT CISCO QUI VOUS EN FOURNIRA UNE COPIE.

L'implémentation Cisco de la compression d'en-têtes TCP est une adaptation d'un programme développé par l'Université de Californie, Berkeley (UCB) dans le cadre de la version publique du système d'exploitation UNIX d'UCB. Tous droits réservés. Copyright © 1981, Regents of the University of California.

MALGRÉ LES DIVERSES GARANTIES EXPOSÉES ICI, TOUS LES DOCUMENTS, FICHIERS ET LOGICIELS DES DIFFÉRENTS FOURNISSEURS SONT PROPOSÉS « TELS QUELS » AVEC LEURS ÉVENTUELS DÉFAUTS. CISCO ET LES FOURNISSEURS SUSNOMMÉS DÉCLINENT TOUTE RESPONSABILITÉ, IMPLICITE OU EXPLICITE, CONCERNANT, SANS QUE CETTE LISTE SOIT EXHAUSTIVE, LA QUALITÉ MARCHANDE DES PRODUITS, LEUR ADAPTATION À UNE UTILISATION PARTICULIÈRE,LA NON-TRANSGRESSION OU TOUT AUTRE PROBLÈME CONSÉCUTIF À UNE VENTE, UN USAGE OU UNE PRATIQUE COMMERCIALE.

CISCO OU SES REPRÉSENTANTS NE POURRONT, EN AUCUN CAS, ÊTRE TENUS POUR RESPONSABLES DES DOMMAGES INDIRECTS, SPÉCIAUX, CONSÉCUTIFS OU INDUITS, Y COMPRIS, SANS QUE CETTE LISTE SOIT EXHAUSTIVE, LES PERTES DE PROFIT, PERTES OU ENDOMMAGEMENT DES DONNÉES, CONSÉCUTIFS À L'UTILISATION OU À L'INCAPACITÉ D'UTILISATION DE CE MANUEL, MÊME SI CISCO OU SES REPRÉSENTANTS ONT ÉTÉ INFORMÉS DE L'ÉVENTUALITÉ D'UNE DEMANDE DE DOMMAGES ET INTÉRÊTS.

Toutes les adresses IP utilisées dans le présent document sont des adresses fictives. Tous les exemples, sorties d'affichage de commandes et images du présent document sont uniquement utilisés à titre indicatif. Toute utilisation d'adresses IP réelles dans les illustrations est involontaire et n'est que pure coïncidence.

Guide de l'utilisateur de Cisco SDM Express

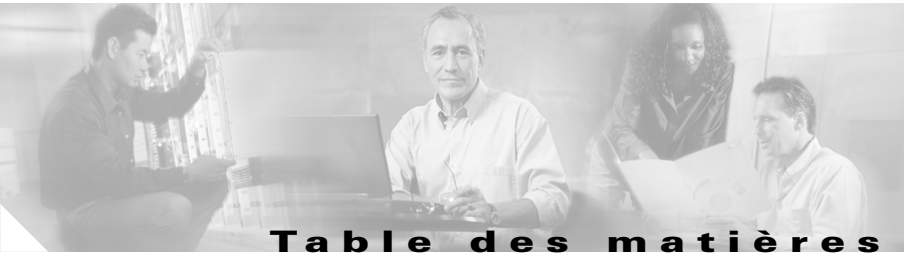

Table des matières

Cisco SDM Express

La fenêtre Cisco SDM Express vous guide tout au long de la configuration de base du routeur. Une fois cette configuration de base effectuée, le routeur est disponible sur le LAN et dispose d'une connexion WAN et d'un pare-feu.

Bienvenue

Cet assistant vous permet de définir une configuration de base pour effectuer les opérations suivantes :

- Nommer le routeur.
- Spécifier un nom d'utilisateur et des mots de passe.
- Le routeur peut être configuré manuellement à l'aide de l'assistant Cisco SDM Express. Vous pouvez également fournir au routeur un fichier de configuration chargé à partir d'une unité USB ou d'un périphérique flash USB, de SDP (Secure Device Provisioning) ou de Cisco Network Services, si pris en charge par la version de Cisco IOS.

  Si vous utilisez Cisco Network Services pour configurer votre routeur, vous pouvez spécifier les paramètres Cisco Network Services qui permettront au routeur de prendre contact avec le serveur Cisco Network Services pour obtenir de celui-ci une configuration.
- Modifier l'adresse IP du LAN par défaut, définie en usine.

  Cette tâche est contournée si SDP ou Cisco Network Services est sélectionné pour le déploiement du routeur.

- Créer un pool d'adresses DHCP pour le LAN.

  Cette tâche est contournée si SDP ou Cisco Network Services est sélectionné pour le déploiement du routeur.

- Entrez les noms des serveurs DNS et le nom de domaine de votre entreprise. Consultez votre administrateur réseau ou votre fournisseur d'accès Internet pour obtenir ces informations.

  Cette tâche est contournée si SDP ou Cisco Network Services est sélectionné pour le déploiement du routeur.

- Créer une connexion WAN.
- Créer un pare-feu pour les connexions LAN et WAN.
- Configurer des paramètres qui améliorent les performances et la sécurité du réseau.

Pour configurer des interfaces supplémentaires et procéder à des réglages de configuration plus avancés, utilisez Cisco Router and Security Device Manager (Cisco SDM). Pour plus d'informations, reportez-vous à Cisco Router and Security Device Manager.

Configuration de base

La fenêtre Configuration de base vous permet de nommer le routeur que vous configurez, de spécifier le nom de domaine de votre entreprise et de contrôler l'accès à Cisco SDM Express, Cisco Router and Security Device Manager et à l'interface de ligne de commande.

Champ Nom d'hôte

Indiquez le nom que vous souhaitez attribuer au routeur.

Champ Nom de domaine

Entrez le nom de domaine de votre entreprise. Un exemple de nom de domaine pourrait être *cisco.com*, mais il est possible que votre nom de domaine se termine par un suffixe différent, comme *.org* ou *.net*.

Champs Nom d'utilisateur et Mot de passe

Définissez le nom d'utilisateur et le mot de passe des utilisateurs de Cisco SDM Express et de Telnet.

Remarque Le nom d'utilisateur et le mot de passe définis dans cette fenêtre sont ceux que vous saisirez désormais dans Cisco SDM Express (jusqu'à leur prochaine modification). Le mot de passe doit être difficile à trouver pour une tierce personne mais facile à retenir.

Champ Nom d'utilisateur

Saisissez un nom d'utilisateur dans ce champ.

Champ Entrez un nouveau mot de passe

Saisissez le nouveau mot de passe dans ce champ. Ce mot de passe doit contenir au moins 6 caractères.

Champ Confirmer le mot de passe

Confirmez le nouveau mot de passe en le retapant.

Champ Activer le mot de passe secret

La fonction Mot de passe secret d'activation permet de contrôler l'accès en mode privilégié EXEC par les utilisateurs qui se connectent au routeur via Telnet ou le port de console. En mode EXEC privilégié, les utilisateurs peuvent modifier la configuration du routeur et ont accès à des commandes qui ne sont pas accessibles autrement. Entrez le mot de passe secret dans le champ **Entrez un nouveau mot de passe**, puis confirmez-le dans le champ **Confirmer le mot de passe**. Ce mot de passe doit contenir au moins 6 caractères.

Remarque Le mot de passe doit être difficile à trouver pour une tierce personne mais vous devez pouvoir vous en souvenir facilement. Sachez que ce mot de passe est illisible dans le fichier de configuration, car stocké sous forme cryptée.

Dimensionnement du routeur

Cette fenêtre contient les options disponibles pour le dimensionnement du routeur. Certaines de ces fonctions sont visibles uniquement si elles sont prises en charge par votre version de Cisco IOS.

SDM Express

Sélectionnez cette option pour utiliser Cisco SDM Express manuellement pour le déploiement du routeur.

Unité USB ou flash USB

Sélectionnez cette option si vous disposez d'une unité USB ou d'un périphérique flash associé au routeur et ayant le fichier de configuration adéquat.

Remarque Si les deux sont connectés au routeur, Cisco SDM Express utilise l'unité USB. Si vous souhaitez utiliser le périphérique flash USB connecté au routeur, toutes les unités USB doivent être supprimées du routeur avant d'exécuter Cisco SDM Express.

Secure Device Provisioning

Sélectionnez SDP (Secure Device Provisioning) si votre administrateur réseau vous a donné les instructions pour déployer votre routeur avec SDP.

Vérifiez les éléments suivants avant de sélectionner l'option SDP :

- Le routeur et le serveur SDP sont reliés par une connexion IP.
- Votre navigateur Web prend en charge JavaScript.

Si vous sélectionnez SDP, une nouvelle fenêtre de navigateur s'ouvre automatiquement à l'issue de l'exécution de l'assistant Cisco SDM Express. Cette nouvelle fenêtre dispose d'un assistant qui vous guide pour déployer votre routeur avec SDP.

Pour plus d'informations sur SDP (en anglais), cliquez sur le lien suivant :

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a008028afbd.html#wp1043332

Serveur CNS

Si votre fournisseur d'accès vous a fourni les informations du serveur Cisco Network Services, choisissez cette option. Pour plus d'informations, reportez-vous à Cisco Network Services.

Déploiement à partir d'une unité USB

Cette fenêtre vous permet de déployer votre routeur avec un fichier de configuration CCCD chargé à partir d'une unité USB connectée à votre routeur. Les CCCD sont des fichiers de configuration de démarrage chargés sur des unités USB à l'aide du logiciel TMS.

Remarque Cette fenêtre est uniquement disponible si une unité USB est connectée à votre routeur. Si les deux sont connectés au routeur, Cisco SDM Express utilise l'unité USB. Si vous souhaitez utiliser le périphérique flash USB connecté au routeur, toutes les unités USB doivent être supprimées du routeur avant d'exécuter Cisco SDM Express.

Si vous déployez votre routeur avec un fichier de configuration CCCD, le fichier est fusionné avec la configuration en cours et fait également partie de la configuration de démarrage.

Attention Cisco SDM ne vérifie pas la validité des fichiers de configuration utilisés pour déployer votre routeur. Vérifiez qu'ils contiennent les paramètres adéquats.

Pour déployer votre routeur à partir d'une unité USB, procédez comme suit :

Étape 1 Sélectionnez le nom de l'unité USB dans le menu déroulant **Nom de l'unité**.

Étape 2 Sélectionnez **Spécifiez le périphérique et le PIN** et entrez le PIN dans le champ PIN de l'unité si vous ne souhaitez *pas* utiliser le PIN par défaut pour vous connecter à l'unité USB.

Si vous sélectionnez **Spécifiez le périphérique et le PIN par défaut**, le PIN par défaut 1234567890 est utilisé pour se connecter à l'unité USB.

Étape 3 Cliquez sur **Connexion** pour vous connecter à l'unité USB.

Si vous ne pouvez pas vous connecter à l'unité USB, le routeur ne peut pas être déployé à partir de celle-ci. Cliquez sur le bouton **Précédent** et sélectionnez une autre méthode de déploiement du routeur.

Étape 4 Cliquez sur **Prévisualiser CCCD** pour afficher le contenu du fichier dans le panneau inférieur.

Acheminement à partir du flash USB

Cette fenêtre vous permet de déployer votre routeur avec un fichier de configuration chargé à partir d'un périphérique flash USB connecté à votre routeur. Cette fenêtre est uniquement disponible si un périphérique flash USB est connecté à votre routeur.

Si vous déployez votre routeur avec un fichier de configuration, le fichier est fusionné avec la configuration en cours et fait également partie de la configuration de démarrage.

Attention Cisco SDM ne vérifie pas la validité des fichiers de configuration utilisés pour déployer votre routeur. Vérifiez qu'ils contiennent les données adéquates.

Pour déployer votre routeur à partir d'un périphérique flash USB, procédez comme suit :

Étape 1 Entrez le nom du fichier de configuration, avec le chemin complet dans le champ Nom du fichier ou cliquez sur **Parcourir** pour ouvrir la fenêtre de sélection du fichier.

Le fichier doit avoir l'extension .cfg ou le nom de fichier doit être un fichier CCCD. Les fichiers CCCD sont des fichiers de configuration de démarrage.

Étape 2 Cliquez sur **Aperçu fichier** pour afficher le contenu du fichier dans le panneau inférieur.

Sélection de fichier

Cette fenêtre vous permet de charger un fichier à partir de votre routeur. Seuls les fichiers système DOSFS sont affichés dans cette fenêtre.

Le côté gauche de la fenêtre affiche un arbre déroulant représentant le système de répertoire sur la mémoire flash du routeur Cisco et sur les périphériques USB connectés sur le routeur.

Le côté droit de la fenêtre affiche une liste des noms de fichiers et des répertoires trouvés dans le répertoire indiqué dans le côté gauche de la fenêtre. Sont également affichées, la taille de chaque fichier en octets ainsi que la date et l'heure de la dernière modification des fichiers et des répertoires.

Choisissez un fichier à charger dans la liste sur le côté droit de la fenêtre. En dessous de la liste des fichiers se trouve le champ Nom de fichier contenant le chemin entier du fichier indiqué.

Remarque Si un fichier de configuration est choisi pour déployer votre routeur, le fichier doit être un fichier CCCD ou avoir une extension .cfg.

Nom

Cliquez sur **Nom** pour classer les fichiers et les répertoires par ordre alphabétique. Cliquez à nouveau sur **Nom** pour inverser l'ordre.

Taille

Cliquez sur **Taille** pour classer les fichiers et les répertoires par taille. Les répertoires ont toujours une taille de zéro octet même s'ils ne sont pas vides. Cliquez à nouveau sur **Taille** pour inverser l'ordre.

Heure modifiée

Cliquez sur **Heure modifiée** pour classer les fichiers et les répertoires selon la date et l'heure de leur dernière modification. Cliquez à nouveau sur **Heure modifiée** pour inverser l'ordre.

Configuration de l'interface sans fil

Pour configurer l'interface sans fil du routeur, cliquez sur **Oui**. Cisco SDM Express configure le routeur pour raccorder le trafic sans fil à l'interface LAN. Cliquez sur **Non** si vous ne souhaitez pas configurer l'interface sans fil. Vous pouvez toujours configurer les paramètres d'interface LAN si vous cliquez sur **Non**.

Cisco SDM Express vous permet de configurer une seule interface sans fil. S'il y a des interfaces sans fil supplémentaires sur votre routeur, utilisez l'application sans fil pour les configurer.

Configuration de l'interface LAN

Cette fenêtre vous permet de configurer l'adresse IP et le masque de sous-réseau de l'interface Ethernet du LAN.

Si vous devez modifier l'adresse IP et les informations de sous-réseau de l'interface Ethernet du réseau LAN à l'issue de l'exécution de l'Assistant Cisco SDM Express, vous pouvez redémarrer Cisco SDM Express, cliquer sur LAN et modifier l'adresse en conséquence.

Liste Interface/Raccordement à l'interface

Si le routeur possède plusieurs interfaces LAN, celles-ci s'affichent dans cette liste. Sélectionnez l'interface LAN à configurer.

Si le routeur possède une interface sans fil et si vous avez cliqué sur **Oui** dans la fenêtre Configuration de l'interface sans fil, cette liste est libellée Raccordement à l'interface. Sélectionnez l'interface à laquelle vous souhaitez raccorder le trafic sans fil.

Champ Adresse IP

Saisissez l'adresse IP de l'interface LAN en séparant chaque nombre par un point. Il peut s'agir d'une adresse IP privée si vous prévoyez d'utiliser la conversion d'adresse réseau (NAT) ou la conversion d'adresse de port (PAT).

Remarque Notez cette adresse par écrit. Á l'issue de l'exécution de l'assistant Cisco SDM Express et après avoir redémarré le routeur, utilisez cette adresse pour exécuter Cisco SDM Express. N'utilisez pas l'adresse fournie dans le guide de démarrage rapide du routeur.

Champ Masque de sous-réseau

Indiquez le masque de sous-réseau du réseau. Demandez cette valeur à votre administrateur réseau ou à votre fournisseur d'accès. Le masque de sous-réseau permet au routeur de déterminer quelle partie de l'adresse IP correspond au réseau et quelle partie correspond au sous-réseau. La valeur du masque de sous-réseau détermine également le nombre d'hôtes pouvant être présents dans le LAN auquel ce routeur est connecté.

Champ Bits de sous-réseau

Vous pouvez également indiquer le nombre de bits utilisés pour définir la partie réseau et la partie sous-réseau de l'adresse IP. Il est possible que votre administrateur réseau ou votre fournisseur d'accès vous fournisse le masque de sous-réseau sous cette forme.

Champs Paramètres sans fil

Au cours de la configuration initiale, ces champs s'affichent si le routeur possède une interface sans fil et si vous avez cliqué sur **Oui** dans la fenêtre Configuration de l'interface sans fil. Si vous modifiez une configuration, ces champs apparaissent si vous avez effectué des réglages sans fil au cours de la configuration initiale. Le trafic sans fil sera raccordé à cette interface LAN.

Saisissez un identificateur de jeu de services (SSID) pour ce trafic sans fil. La valeur de SSID est un identifiant unique utilisé par les périphériques de réseau sans fil pour établir et maintenir la connectivité sans fil.

Remarque La modification d'une valeur SSID configurée met fin à la connexion sans fil.

Si vous modifiez une configuration LAN à l'issue de l'exécution de l'Assistant Cisco SDM Express et si vous souhaitez configurer des paramètres sans fil avancés, cliquez sur **Sans fil** dans la barre Catégorie.

Boutons Actualiser, Appliquer les modifications, Annuler les modifications

Ces boutons sont visibles si vous modifiez une configuration initiale. Pour plus d'informations, cliquez sur Boutons Cisco SDM Express**.**

Configuration du serveur DHCP

Le protocole DHCP (Dynamic Host Configuration Protocol) est un type simple d'adressage utilisé lorsque l'adressage statique n'est pas nécessaire ou lorsque vous n'avez pas besoin d'utiliser des numéros de port pour des services particuliers. DHCP alloue dynamiquement une adresse IP à un hôte dès sa connexion au réseau et la lui retire dès qu'il se déconnecte. Ainsi, les adresses sont réutilisables à partir du moment où les hôtes n'en ont plus besoin. Utilisez DHCP pour attribuer des adresses à des ressources (des PC, par exemple) dans votre réseau interne.

Case à cocher Activer le serveur DHCP sur l'interface de réseau local

Cochez cette case pour autoriser le routeur à attribuer des adresses IP privées à des périphériques sur le réseau LAN. Lorsque cette case est cochée, le serveur DHCP assigne des adresses IP à des hôtes pour une période d'une journée. Si vous cochez cette case, vous devez entrer des valeurs dans les champs Adresse IP de début et Adresse IP de fin.

Champ Adresse IP de début

Cisco SDM Express entre dans ce champ l'adresse la plus basse de la plage d'adresses IP, en fonction de l'adresse et du masque de sous-réseau que vous avez attribués à l'interface LAN. Vous pouvez remplacer cette valeur par une valeur supérieure si vous souhaitez réduire le pool d'adresses DHCP, mais cette adresse doit appartenir au même sous-réseau que l'adresse de l'interface LAN. Sinon, Cisco SDM Express affiche un message précisant que l'adresse n'est pas correcte.

Champ Adresse IP de fin

Cisco SDM Express entre dans ce champ l'adresse la plus élevée de la plage d'adresses IP, en fonction de l'adresse IP et du masque de sous-réseau que vous avez attribués à l'interface LAN. Vous pouvez remplacer cette valeur par une valeur inférieure si vous souhaitez réduire le pool d'adresses DHCP, mais cette adresse doit appartenir au même sous-réseau que l'adresse de l'interface LAN. Sinon, Cisco SDM Express affiche un message précisant que l'adresse n'est pas correcte.

Champ Nom de domaine

Ce champ est visible une fois que vous avez terminé la configuration initiale. Vous pouvez spécifier le nom de domaine de votre entreprise. Un exemple de nom de domaine pourrait être *cisco.com*, mais il est possible que votre nom de domaine se termine par un suffixe différent, comme *.org* ou *.net*.

Case à cocher Importer toutes les options DHCP dans la base de données du serveur DHCP

Ce champ est visible une fois que vous avez terminé la configuration initiale. Cochez cette option si vous souhaitez importer les paramètres d'option DHCP dans la base de données du serveur DHCP et envoyer également ces informations aux clients DHCP sur le réseau LAN lorsqu'ils demandent une adresse IP.

Champ DNS principal

Saisissez l'adresse IP du serveur DNS principal utilisé par le routeur. Cette adresse IP vous est fournie par votre administrateur réseau ou votre fournisseur d'accès.

Le serveur DNS principal est le serveur contacté en premier par le routeur lorsqu'il tente de résoudre une adresse IP.

Champ DNS secondaire

Saisissez l'adresse IP du serveur DNS secondaire utilisé par le routeur (si un tel serveur est disponible). Cette adresse IP vous est fournie par votre administrateur réseau ou votre fournisseur d'accès.

Saisissez l'adresse IP du serveur DNS secondaire utilisé par le routeur si le serveur principal n'est pas disponible.

Case à cocher Utiliser ces valeurs DNS pour les clients DHCP

Cette case est disponible si un serveur DHCP est activé sur l'interface LAN. Cochez-la si vous souhaitez que les clients DHCP du routeur puissent utiliser les serveurs DNS dont vous saisissez les adresses IP dans cette fenêtre.

Boutons Actualiser, Appliquer les modifications, Annuler les modifications

Ces boutons sont visibles si vous modifiez une configuration initiale. Pour plus d'informations, reportez-vous à Boutons Cisco SDM Express.

Internet (WAN) : Interface Ethernet

Utilisez cette fenêtre pour configurer une interface WAN Ethernet.

Case à cocher Activer PPPoE

Si votre fournisseur d'accès requiert que le routeur utilise PPPoE, cochez cette case pour activer l'encapsulation PPPoE. Dans le cas contraire, décochez-la. Cette case n'est pas disponible si votre routeur exécute une version de Cisco IOS ne prenant pas en charge l'encapsulation PPPoE.

Liste des types d'adresse

Sélectionnez l'une des options suivantes :

Option Adresse IP statique

Si vous choisissez une adresse IP statique, entrez l'adresse IP et le masque de sous-réseau ou les bits de sous-réseau dans les champs proposés.

Option Dynamique (Client DHCP)

Si vous choisissez Dynamique, le routeur loue une adresse IP à partir d'un serveur DHCP distant. Entrez le nom du serveur DHCP qui va attribuer les adresses.

Option IP non numérotée

Sélectionnez **IP non numérotée** si vous souhaitez que l'interface partage une adresse IP déjà attribuée à une autre interface. Choisissez ensuite l'interface ayant l'adresse IP que l'interface en cours de configuration doit utiliser. Si l'option Activer PPPoE n'est pas sélectionnée, cette option n'est pas disponible.

Easy IP (IP Négociée)

Sélectionnez **Easy IP (IP Négociée)** si le routeur obtient une adresse IP suite à une négociation d'adresse PPP/IPCP. Si l'option Activer PPPoE n'est pas sélectionnée, cette option n'est pas disponible.

Case à cocher Type d'authentification

Cochez la case correspondant au type d'authentification utilisé par votre fournisseur d'accès. Si vous ne le connaissez pas, cochez les deux cases : le routeur essaie les deux types d'authentification. L'une de ces tentatives doit aboutir.

L'authentification CHAP est plus sûre que l'authentification PAP.

Champ Nom d'utilisateur

Le nom d'utilisateur vous est fourni par votre fournisseur d'accès à Internet ou par votre administrateur réseau. Il est utilisé pour l'authentification CHAP et/ou PAP.

Champ Mot de passe

Entrez le mot de passe tel qu'il vous a été fourni par votre fournisseur d'accès. Les mots de passe sont sensibles à la casse. Par exemple, le mot de passe « test » est différent du mot de passe « Test ».

Champ Confirmer le mot de passe

Tapez à nouveau le mot de passe indiqué dans le champ précédent.

Boutons Actualiser, Appliquer les modifications, Annuler les modifications

Ces boutons sont visibles si vous modifiez une configuration initiale. Pour plus d'informations, cliquez sur Boutons Cisco SDM Express**.**

Internet (WAN) : Détection auto d'encapsulation

Cisco SDM Express prend en charge la détection automatique sur les routeurs SB 106, SB 107, Cisco 836 et Cisco 837. Cependant, si vous configurez un routeur Cisco 837 fonctionnant avec la version 12.3(8)T ou 12.3(8.3)T de Cisco IOS la fonction de détection automatique n'est pas prise en charge.

Cliquez sur le bouton **Détection auto** pour que Cisco SDM Express découvre le type d'encapsulation. Si Cisco SDM Express aboutit, il indique automatiquement le type d'encapsulation ainsi que d'autres paramètres de configuration.

Si Cisco SDM Express n'est pas capable de détecter le type d'encapsulation, vous devez spécifier les types d'encapsulation et d'authentification en cliquant sur **Indiqué par l'utilisateur**.

Icône État et bouton Activer ou Désactiver

L'icône État s'affiche lorsque vous utilisez Cisco SDM Express pour modifier une configuration initiale. L'icône représentant une flèche vers le haut indique que l'interface est en service. L'icône représentant une flèche vers le bas indique que l'interface est arrêtée.

Le bouton **Activer** ou **Désactiver** est disponible lorsque vous utilisez Cisco SDM Express pour modifier une configuration initiale. Si une interface sélectionnée est activée, vous pouvez utiliser le bouton **Désactiver** pour l'arrêter. Si une interface sélectionnée est arrêtée, vous pouvez utiliser le bouton **Activer** pour l'activer.

Internet (WAN) : Encapsulation indiquée par l'utilisateur

Cette fenêtre vous permet de configurer une interface WAN lors de la définition de l'encapsulation.

Icône État et bouton Activer ou Désactiver

L'icône État s'affiche lorsque vous utilisez Cisco SDM Express pour modifier une configuration initiale. L'icône représentant une flèche vers le haut indique que l'interface est en service. L'icône représentant une flèche vers le bas indique que l'interface est arrêtée.

Le bouton **Activer** ou **Désactiver** est disponible lorsque vous utilisez Cisco SDM Express pour modifier une configuration initiale. Si une interface sélectionnée est activée, vous pouvez utiliser le bouton **Désactiver** pour l'arrêter. Si une interface sélectionnée est arrêtée, vous pouvez utiliser le bouton **Activer** pour l'activer.

Liste Encapsulation

Les encapsulations disponibles pour une interface ADSL, G.SHDSL ou ADSL sur RNIS sont répertoriées dans le tableau ci-dessous.

Encapsulation	Description
PPPoE	Offre une encapsulation Point-to-Point Protocol over Ethernet. Une sous-interface ATM et une interface de numéroteur sont créées lorsque vous configurez PPPoE sur une interface ATM. Ces interfaces logiques seront visibles dans la fenêtre Synthèse. L'option radio PPPoE est désactivée si votre routeur exécute une version de Cisco IOS ne prenant pas en charge l'encapsulation PPPoE.
PPPoA	Offre une encapsulation Point-to-Point Protocol over ATM (AAL5 SNAP et AAL5 MUX). L'option radio PPPoA est désactivée si votre routeur exécute une version de Cisco IOS ne prenant pas en charge l'encapsulation PPPoA.
Routage RFC 1483 avec AAL5 SNAP	Cette option est disponible si vous avez sélectionné une interface ATM. Une sous-interface ATM est créée lorsque vous configurez une connexion RFC 1483. Cette sous-interface apparaît dans la fenêtre Synthèse.
Routage RFC 1483 avec AAL5 MUX	Cette option est disponible si vous avez sélectionné une interface ATM. Une sous-interface ATM est créée lorsque vous configurez une connexion RFC 1483. Cette sous-interface apparaît dans la fenêtre Synthèse.

Champ Identificateur de chemin virtuel

Saisissez la valeur du VPI (Identificateur de chemin virtuel) qui vous a été fournie par votre administrateur réseau ou votre fournisseur d'accès. Le VPI est utilisé dans le routage et la commutation ATM pour identifier le chemin utilisé par un certain nombre de connexions.

Champ Identificateur de circuit virtuel

Saisissez la valeur du VCI (Identificateur de circuit virtuel) qui vous a été fournie par votre administrateur réseau ou votre fournisseur d'accès. Le VCI est utilisé dans le routage et la commutation ATM pour identifier une connexion dans un chemin qu'elle peut partager avec d'autres connexions.

Liste des types d'adresse

Sélectionnez l'une des options suivantes :

- **Adresse IP statique** : si vous choisissez une adresse IP statique, saisissez l'adresse IP et le masque de sous-réseau ou les bits de sous-réseau dans les champs proposés.
- **Dynamique** (**Client DHCP**) : si vous choisissez Dynamique, le routeur loue une adresse IP à partir d'un serveur DHCP distant. Entrez le nom du serveur DHCP qui va attribuer les adresses.
- **IP non numérotée** : sélectionnez cette option si vous souhaitez que l'interface partage une adresse IP qui a déjà été affectée à une autre interface. Choisissez ensuite l'interface ayant l'adresse IP que l'interface en cours de configuration doit utiliser.
- **Easy IP** (**IP Négociée**) : sélectionnez **Easy IP (IP Négociée)** pour que le routeur obtienne une adresse IP via la négociation d'adresse PPP/IPCP.

Adresse IP de la connexion distante au bureau central

Si vous configurez une connexion G.SHDSL, saisissez l'adresse IP de la passerelle à laquelle la liaison est connectée. Cette adresse IP vous est communiquée par votre fournisseur d'accès ou votre administrateur réseau. La passerelle correspond au système auquel le routeur doit se connecter pour accéder à Internet ou au WAN de votre entreprise.

Case à cocher Type d'authentification

Cochez la case correspondant au type d'authentification utilisé par votre fournisseur d'accès. Si vous ne le connaissez pas, cochez les deux cases : le routeur essaie les deux types d'authentification. L'une de ces tentatives doit aboutir.

L'authentification CHAP est plus sûre que l'authentification PAP.

Champ Nom d'utilisateur

Entrez le nom d'utilisateur qui vous est fourni par votre fournisseur d'accès à Internet ou par votre administrateur réseau. Il est utilisé pour l'authentification CHAP et/ou PAP.

Champ Mot de passe

Entrez le mot de passe tel qu'il vous a été fourni par votre fournisseur d'accès. Les mots de passe sont sensibles à la casse. Par exemple, le mot de passe « test » est différent du mot de passe « Test ».

Champ Confirmer le mot de passe

Tapez à nouveau le mot de passe indiqué dans le champ précédent.

Boutons Actualiser, Appliquer les modifications, Annuler les modifications

Ces boutons sont visibles si vous modifiez une configuration initiale. Pour plus d'informations, cliquez sur Boutons Cisco SDM Express**.**

Sélection d'une interface WAN

Cisco SDM Express vous permet de configurer une connexion WAN. Si votre routeur possède plusieurs interfaces WAN, sélectionnez celle que vous souhaitez configurer dans cette fenêtre. Sélectionnez l'interface à configurer dans la liste, cliquez sur **Ajouter une connexion** et configurez la connexion dans la boîte de dialogue qui s'affiche.

Remarque Si vous ne configurez pas de connexion WAN, vous ne pouvez pas configurer de pare-feu, de routage, de Cisco Network Services ou de SDP.

Boutons Ajouter une connexion, Modifier, Supprimer

Le bouton **Ajouter une connexion** est activé si aucune configuration WAN n'est encore configurée. Les boutons **Modifier** et **Supprimer** sont activés si au moins une connexion WAN a été configurée.

Pour configurer une interface, sélectionnez-la et cliquez sur **Ajouter une connexion**. Si ce bouton est désactivé, vous pouvez configurer des connexions WAN supplémentaires à l'aide de Cisco SDM ou supprimer une connexion configurée et en configurer une nouvelle.

Pour modifier une configuration existante, sélectionnez l'interface et cliquez sur **Modifier**.

Pour supprimer une configuration, sélectionnez l'interface et cliquez sur **Supprimer**.

Bouton Activer ou Désactiver

Ce bouton est disponible lorsque vous utilisez Cisco SDM Express pour modifier une configuration initiale. Si une interface sélectionnée est activée, vous pouvez utiliser le bouton **Désactiver** pour l'arrêter. Si une interface sélectionnée est arrêtée, vous pouvez utiliser le bouton **Activer** pour l'activer.

Liste d'interfaces

La liste d'interfaces contient le nom, l'adresse IP et le type d'interface pour toutes les interfaces WAN. Si aucune adresse IP n'a été configurée pour une interface, le texte « Aucune adresse IP » s'affiche.

Remarque Si vous n'avez pas configuré l'interface LAN par défaut avec la nouvelle adresse dans la fenêtre Configuration de l'interface LAN, elle est répertoriée dans cette fenêtre et peut être configurée en tant qu'interface WAN.

Bouton Actualiser

Ces boutons sont visibles si vous modifiez une configuration initiale. Pour plus d'informations, cliquez sur Boutons Cisco SDM Express**.**

Connexion série

Utilisez cette fenêtre pour créer ou modifier une connexion série.

Liste Encapsulation

Sélectionnez l'encapsulation pour cette connexion. Si vous procédez à la modification d'une connexion, vous ne pouvez pas modifier le type d'encapsulation dans cette fenêtre. Vous devez supprimer la connexion, puis en créer une nouvelle avec le type d'encapsulation souhaité.

- **Relais de trame** : protocole de l'industrie des télécommunications, applicable à la couche de liaison commutée, capable de gérer plusieurs circuits virtuels en utilisant l'encapsulation HDLC entre les périphériques connectés.

- **HDLC** : abréviation de High-Level Data Link Control. Protocole de niveau binaire de la couche de liaison synchrone développé par l'ISO (International Standards Organization), qui préconise une méthode d'encapsulation des données sur les liaisons série synchrones utilisant les caractères de trame et les sommes de contrôle.
- **PPP** : protocole point à point.

Détails sur l'authentification

Si vous sélectionnez l'encapsulation PPP, vous pouvez fournir les informations d'authentification que votre fournisseur d'accès Internet est susceptible d'exiger.

- **Nom d'utilisateur** : entrez exactement le nom d'utilisateur tel qu'il vous a été fourni par votre fournisseur d'accès à Internet ou par votre administrateur réseau. Il est utilisé pour l'authentification CHAP et/ou PAP.
- **Mot de passe** : entrez le mot de passe tel qu'il vous a été fourni par votre fournisseur d'accès. Les mots de passe sont sensibles à la casse. Par exemple, le mot de passe « test » est différent du mot de passe « Test ».
- **Confirmer le mot de passe** : tapez à nouveau le mot de passe indiqué dans le champ précédent.

Liste des types d'adresse

- **Adresse IP statique** : disponible avec les types d'encapsulation Relais de trame, PPP et HDLC. Si vous choisissez une adresse IP statique, entrez l'adresse IP et le masque de sous-réseau ou les bits de sous-réseau dans les champs proposés.
- **IP non numérotée** : disponible avec les types d'encapsulation Relais de trame, PPP et HDLC. Sélectionnez **IP non numérotée** si vous souhaitez que l'interface partage une adresse IP déjà attribuée à une autre interface. Choisissez ensuite l'interface ayant l'adresse IP que l'interface en cours de configuration doit utiliser.
- **IP Négociée** : disponible uniquement avec le type d'encapsulation PPP. Sélectionnez **Easy IP (IP Négociée)** si le routeur obtient une adresse IP suite à une négociation d'adresse PPP/IPCP.

Champs Adresse IP et Masque de sous-réseau

Si vous sélectionnez Adresse IP statique, indiquez dans ces champs l'adresse IP et les masques de sous-réseau.

Lien Paramètres de la configuration Relais de trame

Pour obtenir une description des champs DLCI, LMI et Utiliser l'encapsulation de relais de trame IETF, reportez-vous à Paramètres de la configuration Relais de trame.

Paramètres de la configuration Relais de trame

Champ DLCI

Entrez dans ce champ l'identification DLCI (Data Link Connection Identifier). Ce numéro doit être unique pour tous les DLCI utilisés sur cette interface. Le DLCI fournit une identification de relais de trame unique pour cette connexion.

En cas de modification d'une connexion existante, ce champ n'est pas disponible. Si vous devez modifier le DLCI, supprimez la connexion et recréez-la à nouveau.

Champ Type LMI

Renseignez-vous auprès de votre fournisseur d'accès pour connaître les types de LMI (Local Management Interface) à utiliser. Le type de LMI correspond au protocole utilisé pour surveiller la connexion :

Option ANSI

Annexe D définie par la norme ANSI (American National Standards Institute) T1.617.

Option Cisco

Type LMI défini conjointement par Cisco Systems et trois autres sociétés.

Option UIT-T Q.933

UIT-T Q.933 Annexe A.

Option Autodétection

Valeur par défaut. Ce paramètre permet au routeur de détecter le type LMI utilisé pour communiquer avec le commutateur, et d'utiliser ce type. Si l'autodétection échoue, le routeur utilise le type LMI Cisco.

Case à cocher Utiliser l'encapsulation de relais de trame IETF

Cochez cette case pour utiliser l'encapsulation IETF (Internet Engineering Task Force). Cette option est utilisée pour se connecter à des routeurs non fabriqués par Cisco. Cochez cette case si vous utilisez cette interface pour vous connecter à des routeurs non fabriqués par Cisco.

Internet (WAN) : Options avancées

Cette fenêtre vous permet de spécifier un routage statique par défaut et d'activer la conversion NAT sur le réseau.

Case à cocher Créer le routage par défaut

Un routage statique par défaut spécifie une adresse IP ou une interface vers laquelle le routeur envoie le trafic lorsque celui-ci est lié à un réseau que le routeur ne connaît pas. Si vous sélectionnez **Utiliser cette interface comme interface de Transmission**, le routeur envoie ce type de trafic vers une interface WAN que vous configurez. Si vous sélectionnez **Adresse IP de relais suivant**, indiquez l'adresse vers laquelle vous souhaitez que le routeur transfère ce type de trafic.

Ces champs ne s'affichent pas si vous avez sélectionné une interface WAN avec une adresse IP dynamique.

Informations du serveur CNS

Cette fenêtre apparaît si vous avez configuré une connexion WAN et choisi de déployer le routeur à l'aide de l'option Cisco Network Services. Elle vous permet de saisir les informations du serveur Cisco Network Services fournies par votre fournisseur d'accès. Entrez l'adresse IP et les informations de connexion des serveurs Cisco Network Services pour que Cisco SDM Express puisse télécharger les informations de configuration de votre routeur.

Champ Entrez le nom d'hôte/l'adresse IP du serveur CNS

Vous devez entrer soit une adresse IP ou un nom d'hôte du serveur Cisco Network Services sur votre réseau. Si vous indiquez un nom d'hôte, vous devez préciser l'adresse IP d'un serveur DNS capable de résoudre le nom d'hôte en une adresse IP.

Champ Entrez la chaîne d'identification du CNS

Saisissez l'ID de périphérique requis pour télécharger le fichier de configuration depuis le serveur Cisco Network Services.

Champ Entrez le mot de passe du CNS

Saisissez le mot de passe utilisé pour se connecter au serveur Cisco Network Services avec l'ID utilisateur saisie précédemment.

Champ DNS principal

Saisissez l'adresse IP du serveur DNS principal utilisé par le routeur. Cette adresse IP vous est fournie par votre administrateur réseau ou votre fournisseur d'accès.

Le serveur DNS principal est le serveur contacté en premier par le routeur lorsqu'il tente de résoudre une adresse IP.

Remarque Si vous indiquez un nom d'hôte pour identifier un serveur Cisco Network Services dans le champ Entrez l'adresse IP/nom d'hôte du serveur CNS, vous devez saisir l'adresse IP d'un serveur DNS dans le champ DNS principal.

Champ DNS secondaire

Saisissez l'adresse IP du serveur DNS secondaire utilisé par le routeur (si un tel serveur est disponible). Cette adresse IP vous est fournie par votre administrateur réseau ou votre fournisseur d'accès.

Saisissez l'adresse IP du serveur DNS secondaire utilisé par le routeur si le serveur principal n'est pas disponible.

Configuration du pare-feu

La fenêtre Configuration du pare-feu vous permet de laisser Cisco SDM Express configurer un pare-feu sur vos interfaces WAN et LAN. Vous pouvez appliquer un pare-feu pendant la configuration initiale ou utiliser Cisco SDM Express pour l'appliquer après avoir attribué au routeur sa configuration initiale.

Si vous laissez Cisco SDM Express configurer le pare-feu, vous pouvez modifier la configuration du pare-feu ultérieurement à l'aide de la fonction de configuration de stratégie de pare-feu de Cisco SDM.

Remarque

- Cette fonction est disponible si la version de Cisco IOS exécutée sur le routeur prend en charge le jeu de fonctions du pare-feu.
- La fenêtre Configuration du pare-feu ne s'affiche pas si vous n'avez pas configuré d'interface WAN.

Le pare-feu assure à votre réseau les protections suivantes :

- Appliquez les règles d'accès par défaut à l'interface interne et à l'interface externe : Cisco SDM Express crée et applique une liste de règles d'accès par défaut qui, entre autres, autorisent les trafics DNS et HTTP, et bloquent l'espace d'adresses IP privées.
- Appliquez une règle d'inspection par défaut à l'interface externe Cisco SDM Express : SDM crée et applique une liste de règles d'inspection par défaut.
- Activez la réémission en sens inverse de la source (Unicast RPF) sur l'interface externe : La fonction IP Unicast RPF permet au routeur de comparer l'adresse source de chaque paquet à celle de l'interface via laquelle le paquet est entré dans le routeur. Si le chemin d'accès à l'interface d'entrée ne correspond pas à l'adresse source indiquée dans la table de routage, le paquet est supprimé. Cette vérification de l'adresse source permet d'empêcher l'usurpation d'adresse IP.

Si vous choisissez de laisser Cisco SDM Express configurer le pare-feu, vous pouvez modifier la configuration de pare-feu ultérieurement à l'aide de Cisco SDM. Si vous préférez ne pas avoir de pare-feu configuré, vous pourrez en configurer un plus tard à l'aide de Cisco SDM Express ou de Cisco SDM. Pour plus d'informations, reportez-vous à la section Cisco Router and Security Device Manager.

Paramètres de sécurité

Cette fenêtre vous permet de désactiver les fonctions activées par défaut dans le logiciel Cisco IOS et qui peuvent générer des risques pour la sécurité ou qui forcent le routeur à envoyer des messages trop volumineux pour la mémoire disponible. Laissez ces cases cochées sauf si vos besoins sont différents. Cette rubrique d'aide vous dirige vers les descriptions de chacun des paramètres de sécurité que Cisco SDM Express réalise.

Vous pouvez utiliser Cisco SDM Express pour modifier les paramètres de sécurité définis dans cette fenêtre une fois la configuration initiale terminée. Si vous souhaitez modifier l'un des paramètres de ces groupes de paramètres décrits dans cette rubrique d'aide, vous pouvez le faire à l'aide de Cisco SDM. Pour plus d'informations, reportez-vous à la section Cisco Router and Security Device Manager.

Case à cocher Désactiver les services SNMP sur le routeur

Cochez cette case pour désactiver le service SNMP sur le routeur. Pour savoir pourquoi SNMP doit être désactivé, reportez-vous à Désactiver SNMP.

Case à cocher Désactiver les services entraînant des risques pour la sécurité

Cochez cette case pour désactiver les services suivants sur le routeur. Pour savoir pourquoi ces services doivent être désactivés, cliquez sur les liens ci-dessous :

- Désactiver le service Finger
- Désactiver le service PAD
- Désactiver le service TCP Small Servers
- Désactiver le service UDP Small Servers
- Désactiver le service IP Bootp Server
- Désactiver le service IP Ident
- Désactiver CDP
- Désactiver le routage d'IP source
- Désactiver les messages ARP
- Désactiver la redirection d'IP
- Désactiver le Proxy IP ARP

- Désactiver la diffusion d'IP dirigée
- Désactiver le service MOP
- Désactiver les IP injoignables
- Désactiver la réponse au masque IP

Case à cocher Activer les services renforçant la sécurité sur le routeur/le réseau

Cochez cette case pour activer sur le routeur les fonctions et services améliorant la sécurité. Pour plus d'informations sur ces services et fonctions, cliquez sur les liens ci-dessous :

- Activer la commutation Netflow
- Activer le maintien des connexions TCP pour les sessions Telnet entrantes
- Activer le maintien des connexions TCP pour les sessions Telnet sortantes
- Activer les numéros de séquence et les horodatages sur les débogages
- Activer IP CEF
- Définir l'intervalle de planification
- Définir l'allocation de planification
- Définir la durée de TCP Synwait
- Activer la connexion
- Activer Unicast RPF sur toutes les interfaces externes

Case à cocher Renforcer la sécurité sur l'accès au routeur

Cochez cette case pour mettre en œuvre sur le routeur des configurations renforçant la sécurité. Pour plus d'informations sur ces services et fonctions, cliquez sur les liens ci-dessous :

- Définir la longueur minimum du mot de passe pour qu'il ne dépasse pas 6 caractères
- Définir le nombre d'échecs d'identification pour qu'il ne dépasse pas 3 tentatives de réidentification
- Définir la bannière
- Activer les paramètres Telnet
- Activer SSH pour l'accès au routeur

Case à cocher Crypter les mots de passe

Cochez cette case pour activer le cryptage des mots de passe. Pour plus d'informations, reportez-vous à Activer le service de cryptage des mots de passe.

Case à cocher Synchroniser les paramètres d'horodatage du routeur avec ceux du PC

Activée par défaut. Si vous ne souhaitez pas attribuer au routeur les paramètres de date et d'heure du PC sur lequel vous exécutez Cisco SDM Express, décochez cette case.

Synthèse

La fenêtre Synthèse vous montre les modifications que vous avez apportées à la configuration du routeur. Si vous souhaitez apporter des modifications supplémentaires, cliquez sur **Précédent** pour revenir à la fenêtre appropriée.

Cliquez sur **Terminer** pour enregistrer les données que vous avez saisies dans le fichier de configuration du routeur.

Remarque Lorsque vous cliquez sur **Terminer**, vous perdez la connexion au routeur si vous avez donné à l'interface LAN une nouvelle adresse IP comme il vous a été recommandé de le faire. Pour rétablir la connexion au routeur, vous devez vérifier que le PC appartient toujours au même sous-réseau que le routeur, puis saisir la nouvelle adresse IP donnée à l'interface LAN. Pour plus d'informations, reportez-vous à Reconnexion au routeur à l'issue de la configuration initiale.

Aide complémentaire

Les rubriques d'aide suivantes fournissent des informations complémentaires.

Cisco Router and Security Device Manager

Une fois que vous avez utilisé Cisco SDM Express pour attribuer à votre routeur une configuration de base, vous pouvez utiliser Cisco Router and Security Device Manager (Cisco SDM) pour configurer des connexions supplémentaires, affiner les configurations réalisées à l'aide de Cisco SDM Express et paramétrer des fonctions avancées telles que les réseaux privés virtuels (RPV) et les certificats numériques.

Cisco SDM est peut-être installé sur votre routeur ou vous avez peut-être reçu un CD que vous pouvez utiliser pour installer Cisco SDM sur votre PC ou sur votre routeur. Si vous avez téléchargé Cisco SDM à partir de Cisco.com, vous pouvez utiliser le programme d'installation pour installer Cisco SDM sur votre PC ou routeur.

Pour démarrer Cisco SDM, cliquez sur **Cisco SDM** dans le menu Outils.

Cisco Network Services

Si votre fournisseur d'accès vous a fourni les informations du serveur Cisco Network Services, choisissez cette option. Lorsque vous sélectionnez cette option, l'assistant Cisco SDM Express collecte des informations sur votre serveur Cisco Network Services, puis affiche les fenêtres vous permettant de configurer la connexion WAN au serveur Cisco Network Services et de télécharger cette configuration. Si votre fournisseur d'accès ne vous a pas fourni les informations du serveur Cisco Network Services ou si vous souhaitez configurer le routeur à l'aide de Cisco SDM Express, ne sélectionnez pas cette option.

Vous ne pouvez pas utiliser Cisco Network Services dans les cas suivants :

- Aucune interface WAN n'est installée sur votre routeur ou Cisco SDM Express ne prend pas en charge l'interface WAN installée sur votre routeur. Cisco SDM Express doit pouvoir configurer une interface WAN pour que le routeur puisse télécharger le fichier de configuration Cisco Network Services. Si Cisco SDM Express ne parvient pas à configurer une interface WAN, il affiche un message d'erreur indiquant que vous ne pouvez pas utiliser Cisco Network Services. Si aucune interface WAN n'est installée sur le routeur et que vous souhaitez tout de même utiliser Cisco Network Services, cliquez sur Annuler pour quitter l'assistant Démarrage et fermez Cisco SDM Express. Ensuite, installez une carte d'interface WAN prise en charge par Cisco SDM Express, redémarrez Cisco SDM Express et sélectionnez **Serveur CNS** (Cisco Network Services server) dans l'assistant Démarrage.

  Pour consulter la liste des cartes d'interface prises en charge par Cisco SDM, reportez-vous aux Notes sur la version de SDM (en anglais) à l'adresse :

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

- Vous n'avez pas sélectionné cette option, vous avez configuré une interface LAN et une interface WAN à l'aide de Cisco SDM Express, puis vous êtes revenu à la fenêtre Dimensionnement du routeur et avez sélectionné **Serveur CNS**. Si vous souhaitez utiliser Cisco Network Services, cliquez sur **Annuler** pour quitter l'assistant Démarrage et fermez Cisco SDM Express. Redémarrez ensuite Cisco SDM Express et sélectionnez **Serveur CNS** dans la fenêtre Dimensionnement du routeur.

Paramètres de sécurité

Les rubriques suivantes décrivent les paramètres de sécurité que Cisco SDM Express peut définir.

Désactiver SNMP

Cisco SDM Express désactive le protocole SNMP (Simple Network Management Protocol) lorsque c'est possible. SNMP est un protocole réseau qui permet de récupérer et d'envoyer des données sur les performances et processus du réseau. Il est largement utilisé pour surveiller les routeurs et en modifier la configuration. Cependant, la version 1 de ce protocole, la plus répandue, présente un risque de sécurité pour les raisons suivantes :

- Il utilise des chaînes d'authentification (mots de passe) appelées *chaînes communautaires* qui sont stockées et envoyées sur le réseau au format texte.
- En majorité, les versions SNMP mises en œuvre envoient ces chaînes à maintes reprises dans le cadre d'une interrogation périodique.
- Il s'agit d'un protocole de transaction basé sur des datagrammes, pouvant facilement faire l'objet d'usurpation.

Dans la mesure où SNMP permet de récupérer une copie de la table de routage du réseau, ainsi que d'autres informations sensibles concernant le réseau, nous vous recommandons de désactiver SNMP si votre réseau ne le requiert pas.
Cisco SDM Express envoie une demande de désactivation de SNMP.

La configuration transmise au routeur pour désactiver SNMP est la suivante :

```
no snmp-server
```

Désactiver le service Finger

Cisco SDM Express désactive le service Finger lorsque c'est possible. Ce service permet d'identifier les utilisateurs connectés à un périphérique réseau. Bien que ces informations ne soient pas très sensibles, elles peuvent parfois être utiles à un pirate.

De plus, le service Finger peut être utilisé dans un type particulier d'attaque par déni de service, appelé Finger of death, qui implique l'envoi d'une demande Finger à un ordinateur chaque minute, et ce indéfiniment.

La configuration transmise au routeur pour désactiver le service Finger est la suivante :

```
no service finger
```

Vous pouvez annuler ce correctif à l'aide de la fonction Audit de sécurité de SDM. Pour plus d'informations, cliquez sur Cisco Router and Security Device Manager.

Désactiver le service PAD

Cisco SDM Express désactive toutes les commandes d'assembleur/désassembleur de paquets (PAD) et les connexions entre des périphériques PAD et des serveurs d'accès, lorsque c'est possible.

La configuration transmise au routeur pour désactiver le service PAD est la suivante :

```
no service pad
```

Vous pouvez annuler ce correctif à l'aide de la fonction Audit de sécurité de Cisco SDM. Pour connaître la procédure, reportez-vous à l'aide en ligne de l'audit de sécurité dans Cisco SDM. Pour plus d'informations, cliquez sur Cisco Router and Security Device Manager.

Désactiver le service TCP Small Servers

Cisco SDM Express désactive les Small Services lorsque c'est possible. Par défaut, les périphériques Cisco qui exécutent Cisco IOS version 11.3 ou antérieure offrent les Small Services suivants : echo, chargen et discard. Les Small Services sont désactivés par défaut dans le logiciel Cisco IOS version 12.0 et ultérieure. Ces services, et plus particulièrement leurs versions UDP (User Datagram Protocol), sont rarement utilisés à des fins légitimes, mais ils permettent de lancer des attaques par déni de service, ainsi que d'autres attaques, qui autrement seraient bloquées par le filtrage des paquets.

Par exemple, un pirate peut envoyer un paquet DNS (Domain Name System) en lui donnant une fausse adresse source d'un serveur DNS qui, dans le cas contraire, serait inaccessible, et en lui attribuant le port source d'un service DNS (port 53). Si un tel paquet était envoyé au port de réponse UDP du routeur, ce dernier enverrait un paquet DNS au serveur en question. Aucun contrôle de liste d'accès sortant ne serait appliqué à ce paquet, car il serait considéré comme généré localement par le routeur lui-même.

Bien que les utilisations abusives des Small Services puissent être en majorité évitées ou affaiblies par des listes d'accès anti-usurpation, il est recommandé de désactiver ces services dans un routeur faisant partie d'un pare-feu ou jouant un rôle important dans la sécurité du réseau. Comme ces services sont rarement utilisés, la meilleure stratégie consiste à les désactiver sur tous les routeurs.

La configuration transmise au routeur pour désactiver le service TCP Small Servers est la suivante :

```
no service tcp-small-servers
```

Vous pouvez annuler ce correctif à l'aide de la fonction Audit de sécurité de Cisco SDM. Pour connaître la procédure, reportez-vous à l'aide en ligne de l'audit de sécurité dans Cisco SDM. Pour plus d'informations, cliquez sur Cisco Router and Security Device Manager.

Désactiver le service UDP Small Servers

Cisco SDM Express désactive les Small Services lorsque c'est possible. Par défaut, les périphériques Cisco qui exécutent Cisco IOS version 11.3 ou antérieure offrent les Small Services suivants : echo, chargen et discard. Les Small Services sont désactivés par défaut dans le logiciel Cisco IOS version 12.0 et ultérieure. Ces services, et plus particulièrement leurs versions UDP, sont rarement utilisés à des fins légitimes, mais ils permettent de lancer des attaques par déni de service, ainsi que d'autres attaques, qui autrement seraient bloquées par le filtrage des paquets.

Par exemple, un pirate peut envoyer un paquet DNS en lui donnant une fausse adresse source d'un serveur DNS qui, dans le cas contraire, serait inaccessible, et en lui attribuant le port source d'un service DNS (port 53). Si un tel paquet était envoyé au port de réponse UDP du routeur, ce dernier enverrait un paquet DNS au serveur en question. Aucun contrôle de liste d'accès sortant ne serait appliqué à ce paquet, car il serait considéré comme généré localement par le routeur lui-même.

Bien que les utilisations abusives des Small Services puissent être en majorité évitées ou affaiblies par des listes d'accès anti-usurpation, il est recommandé de désactiver ces services dans un routeur faisant partie d'un pare-feu ou qui joue un rôle important dans la sécurité du réseau. Comme ces services sont rarement utilisés, la meilleure stratégie consiste à les désactiver sur tous les routeurs.

La configuration transmise au routeur pour désactiver UDP Small Servers est la suivante :

```
no service udp-small-servers
```

Vous pouvez annuler ce correctif à l'aide de la fonction Audit de sécurité de Cisco SDM. Pour connaître la procédure, reportez-vous à l'aide en ligne de l'audit de sécurité dans Cisco SDM. Pour plus d'informations, cliquez sur Cisco Router and Security Device Manager.

Désactiver le service IP Bootp Server

Cisco SDM Express désactive le service Bootstrap Protocol (BOOTP) lorsque c'est possible. BOOTP autorise les routeurs et les ordinateurs à configurer automatiquement au démarrage les informations Internet nécessaires à partir d'un serveur central, y compris le téléchargement du logiciel Cisco IOS. Par conséquent, un pirate peut potentiellement utiliser BOOTP pour télécharger une copie du logiciel Cisco IOS du routeur.

De plus, le service BOOTP est vulnérable aux attaques par déni de service. Il doit donc être désactivé ou filtré par un pare-feu.

La configuration transmise au routeur pour désactiver le service BOOTP est la suivante :

```
no ip bootp server
```

Vous pouvez annuler ce correctif à l'aide de la fonction Audit de sécurité de Cisco SDM. Pour connaître la procédure, reportez-vous à l'aide en ligne de l'audit de sécurité dans Cisco SDM. Pour plus d'informations, cliquez sur Cisco Router and Security Device Manager.

Désactiver le service IP Ident

Cisco SDM Express désactive le support d'identification lorsque c'est possible. Le support d'identification vous permet d'interroger un port TCP pour l'identifier. Cette fonction permet à un protocole non sécurisé de signaler l'identité d'un client qui établit une connexion TCP et de l'hôte qui répond à cette connexion. Avec le support d'identification, vous pouvez vous connecter à un port TCP sur un hôte, envoyer une chaîne de caractères simple pour demander des informations, et recevoir une chaîne de caractères simple en réponse.

Il est dangereux d'autoriser un système d'un segment directement connecté à savoir que le routeur est un périphérique Cisco, et à déterminer le numéro de modèle et la version du logiciel Cisco IOS exécutée. Ces informations peuvent être exploitées pour créer des attaques contre le routeur.

La configuration transmise au routeur pour désactiver le service IP Ident est la suivante :

```
no ip identd
```

Vous pouvez annuler ce correctif à l'aide de la fonction Audit de sécurité de Cisco SDM. Pour connaître la procédure, reportez-vous à l'aide en ligne de l'audit de sécurité dans Cisco SDM. Pour plus d'informations, cliquez sur Cisco Router and Security Device Manager.

Désactiver CDP

Cisco SDM Express désactive le protocole CDP (Cisco Discovery Protocol) lorsque c'est possible. Cisco Discovery Protocol est un protocole propriétaire utilisé par les routeurs Cisco pour s'identifier entre eux sur un segment de LAN. Son inconvénient est qu'il permet à un système d'un segment directement connecté, d'apprendre que le routeur est un périphérique Cisco, d'en déterminer le numéro de modèle et d'identifier la version du logiciel Cisco IOS exécutée. Ces informations peuvent être exploitées pour créer des attaques contre le routeur.

La configuration transmise au routeur pour désactiver Cisco Discovery Protocol est la suivante :

```
no cdp run
```

Vous pouvez annuler ce correctif à l'aide de la fonction Audit de sécurité de Cisco SDM. Pour connaître la procédure, reportez-vous à l'aide en ligne de l'audit de sécurité dans Cisco SDM. Pour plus d'informations, cliquez sur Cisco Router and Security Device Manager.

Désactiver le routage d'IP source

Cisco SDM Express désactive le routage d'IP source lorsque c'est possible. Le protocole IP prend en charge les options de routage source qui permettent à l'expéditeur d'un datagramme IP de contrôler le routage du datagramme vers sa destination finale, et généralement, l'itinéraire suivi par la réponse. Ces options sont rarement utilisées à des fins légitimes dans les réseaux. Certaines anciennes versions d'IP ne gèrent pas les paquets routés par la source correctement. Il est possible de bloquer les machines qui exécutent ces versions en leur envoyant des datagrammes avec des options de routage source.

La désactivation du routage d'IP source empêche un routeur Cisco de transmettre un paquet IP contenant une option de routage source.

La configuration transmise au routeur pour désactiver le routage d'IP source est la suivante :

```
no ip source-route
```

Vous pouvez annuler ce correctif à l'aide de la fonction Audit de sécurité de Cisco SDM. Pour connaître la procédure, reportez-vous à l'aide en ligne de l'audit de sécurité dans Cisco SDM. Pour plus d'informations, cliquez sur Cisco Router and Security Device Manager.

Activer le service de cryptage des mots de passe

Cisco SDM Express active le cryptage des mots de passe lorsque c'est possible. Le cryptage des mots de passe permet au logiciel CiscoIOS de crypter les mots de passe, les secrets CHAP (Challenge Handshake Authentication Protocol) et des données similaires qui sont enregistrées dans son fichier de configuration. Ainsi, vous empêchez quiconque de lire les mots de passe, notamment lorsque des personnes regardent à la dérobée ce que tape un administrateur.

La configuration transmise au routeur pour activer le cryptage des mots de passe est la suivante :

```
service password-encryption
```

Vous pouvez annuler ce correctif à l'aide de la fonction Audit de sécurité de Cisco SDM. Pour connaître la procédure, reportez-vous à l'aide en ligne de l'audit de sécurité dans Cisco SDM. Pour plus d'informations, cliquez sur Cisco Router and Security Device Manager.

Activer la commutation Netflow

Cisco SDM Express active la commutation Netflow lorsque c'est possible. La commutation Netflow est une fonction Cisco IOS qui améliore les performances de routage, tout en utilisant des listes de contrôles d'accès (ACL) et d'autres fonctions qui créent et améliorent la sécurité du réseau. Netflow identifie les flux de paquets de réseau en fonction des adresses IP source et cible et des numéros de port TCP. Il compare ensuite le premier paquet d'un flux aux ACL et à d'autres contrôles de sécurité, au lieu d'utiliser chaque paquet du flux. Ceci améliore les performances en vous permettant d'utiliser l'ensemble des fonctions de sécurité du routeur.

La configuration transmise au routeur pour activer Netflow est la suivante :

```
ip route-cache flow
```

Vous pouvez annuler ce correctif à l'aide de la fonction Audit de sécurité de Cisco SDM. Pour connaître la procédure, reportez-vous à l'aide en ligne de l'audit de sécurité dans Cisco SDM. Pour plus d'informations, cliquez sur Cisco Router and Security Device Manager.

Activer le maintien des connexions TCP pour les sessions Telnet entrantes

Cisco SDM Express active le maintien des connexions TCP pour les sessions Telnet entrantes et sortantes, lorsque c'est possible. Lorsque cette protection est activée, le routeur génère périodiquement des messages de maintien, ce qui lui permet de détecter et de supprimer les connexions Telnet interrompues.

La configuration transmise au routeur pour activer le maintien des connexions TCP pour les sessions Telnet entrantes est la suivante :

```
service tcp-keepalives-in
```

Vous pouvez annuler ce correctif à l'aide de la fonction Audit de sécurité de Cisco SDM. Pour connaître la procédure, reportez-vous à l'aide en ligne de l'audit de sécurité dans Cisco SDM. Pour plus d'informations, cliquez sur Cisco Router and Security Device Manager.

Activer le maintien des connexions TCP pour les sessions Telnet sortantes

Cisco SDM Express active le maintien des connexions TCP pour les sessions Telnet entrantes et sortantes, lorsque c'est possible. Lorsque cette protection est activée, le routeur génère périodiquement des messages de maintien, ce qui lui permet de détecter et de supprimer les connexions Telnet interrompues.

La configuration transmise au routeur pour activer le maintien des connexions TCP pour les sessions Telnet sortantes est la suivante :

```
service tcp-keepalives-out
```

Vous pouvez annuler ce correctif à l'aide de la fonction Audit de sécurité de Cisco SDM. Pour connaître la procédure, reportez-vous à l'aide en ligne de l'audit de sécurité dans Cisco SDM. Pour plus d'informations, cliquez sur Cisco Router and Security Device Manager.

Activer les numéros de séquence et les horodatages sur les débogages

Cisco SDM Express active les numéros de séquence et les horodatages sur tous les messages de dépannage et de journal lorsque c'est possible. Les horodatages sur les messages de dépannage et de journal indiquent la date et l'heure auxquelles le message a été généré. Les numéros de séquence indiquent l'ordre dans lequel les messages ayant des horodatages identiques ont été générés. Connaître l'heure et la séquence de génération des messages est très important pour diagnostiquer des attaques potentielles.

La configuration transmise au routeur pour activer les horodatages et les numéros de séquence est la suivante :

```
service timestamps debug datetime localtime show-timezone msec
service timestamps log datetime localtime show-timeout msec
service sequence-numbers
```

Activer IP CEF

Cisco SDM Express active Cisco Express Forwarding (CEF) ou Distributed Cisco Express Forwarding lorsque c'est possible. Comme il n'est pas nécessaire de créer des entrées de cache lorsque le trafic commence à atteindre de nouvelles destinations, Cisco Express Forwarding se comporte de manière plus prévisible que les autres modes lorsque des volumes importants de trafic sont envoyés à de nombreuses destinations. Les routeurs configurés en mode Cisco Express Forwarding offrent une meilleure protection contre les attaques par inondation, que les routeurs utilisant le cache traditionnel.

La configuration transmise au routeur pour activer Cisco Express Forwarding est la suivante :

```
ip cef
```

Définir l'intervalle de planification

Cisco SDM Express configure l'intervalle de planification sur le routeur lorsque c'est possible. Lorsqu'un routeur commute rapidement un grand nombre de paquets, il est possible que le routeur réponde si lentement aux interruptions des interfaces de réseau que plus aucun travail n'est possible. Cette situation peut être due à une inondation très rapide de paquets. Elle peut bloquer l'accès administratif au routeur, ce qui est très dangereux lorsque le périphérique est soumis à des attaques. L'ajustement de l'intervalle de planification garantit un accès administratif permanent au routeur, ce dernier exécutant les processus système après l'intervalle configuré même lorsque l'unité centrale est utilisée à 100 %.

La configuration transmise au routeur pour ajuster l'intervalle de planification est la suivante :

```
scheduler interval 500
```

Définir l'allocation de planification

Sur les routeurs qui ne prennent pas en charge la commande **scheduler interval**, Cisco SDM Express configure la commande **scheduler allocate** lorsque c'est possible. Lorsqu'un routeur commute rapidement un grand nombre de paquets, il est possible que le routeur réponde si lentement aux interruptions des interfaces de réseau que plus aucun travail n'est possible. Cette situation peut être due à certaines inondations très rapides de paquets. Elle peut bloquer l'accès administratif au routeur, ce qui est très dangereux lorsque le périphérique est soumis à des attaques. La commande **scheduler allocate** garantit qu'un pourcentage des processus de l'unité centrale reste disponible pour les activités autres que la commutation de réseau, comme les processus d'administration.

La configuration transmise au routeur pour définir le pourcentage d'allocation de planification est la suivante :

```
scheduler allocate 4000 1000
```

Définir la durée de TCP Synwait

Cisco SDM Express définit la durée de TCP Synwait à 10 secondes, lorsque c'est possible. Cette durée est très utile pour contrer les attaques par inondation SYN, une forme d'attaque par déni de service. Pour être établie, une connexion TCP requiert une négociation en trois phases. L'expéditeur envoie une demande de connexion, le destinataire renvoie un accusé de réception, puis l'expéditeur renvoie l'acceptation de l'accusé de réception. Une fois cette négociation en trois phases terminée, la connexion est établie et le transfert de données peut commencer. Une attaque par inondation SYN envoie des demandes de connexion répétées à un hôte, sans renvoyer l'acceptation des accusés de réception qui permettent d'établir la connexion, créant ainsi de plus en plus de connexions incomplètes sur l'hôte. Comme le tampon des connexions incomplètes est généralement plus petit que celui des connexions établies, l'hôte peut être submergé et désactivé. La définition d'une durée de TCP Synwait de 10 secondes entraîne l'interruption d'une connexion incomplète après 10 secondes, empêchant la création de connexions incomplètes sur l'hôte.

La configuration transmise au routeur pour définir une durée de TCP Synwait de 10 secondes est la suivante :

```
ip tcp synwait-time <10>
```

Activer la connexion

Cisco SDM Express active la journalisation avec des horodates et des numéros de séquence, lorsque c'est possible. Dans la mesure où elle fournit des informations détaillées sur les événements du réseau, la journalisation est indispensable pour identifier les événements de sécurité et y répondre. Les horodatages et les numéros de séquence fournissent des informations sur la date, l'heure et la séquence de survenance des événements réseau.

La configuration transmise au routeur pour activer et configurer la journalisation la suivante (remplacez *<taille du tampon de journal>* et *<adresse IP du serveur de journalisation>* par les valeurs appropriées saisies dans Cisco SDM Express) :

```
logging console critical
logging trap debugging
logging buffered <taille du tampon de journal>
logging <adresse IP du serveur de journalisation>
```

Activer Unicast RPF sur toutes les interfaces externes

Cisco SDM Express active Unicast Reverse Path Forwarding (RPF) sur toutes les interfaces qui se connectent à Internet, lorsque c'est possible. RPF permet au routeur de comparer l'adresse source de chaque paquet à celle de l'interface via laquelle le paquet est entré dans le routeur. Si le chemin d'accès à l'interface d'entrée ne correspond pas à l'adresse source indiquée dans la table de routage, le paquet est supprimé. Cette vérification de l'adresse source permet d'empêcher l'usurpation d'adresse IP.

Ceci ne fonctionne que lorsque le routage est symétrique. Si le réseau est conçu de sorte que le trafic entre un hôte A et un hôte B puisse suivre un itinéraire différent de celui emprunté par le trafic entre l'hôte B et l'hôte A, le contrôle échoue systématiquement et la communication entre les deux hôtes est impossible. Ce type de routage asymétrique est courant sur Internet. Vérifiez que votre réseau n'utilise pas le routage asymétrique avant d'activer cette fonction.

De plus, unicast RPF ne peut être activé que lorsque le mode IP Cisco Express Forwarding est activé. Cisco SDM Express vérifie dans la configuration du routeur si IP Cisco Express Forwarding est activé. Si tel n'est pas le cas, Cisco SDM Express recommande de l'activer. Si vous acceptez, il l'active. Si IP Cisco Express Forwarding n'est pas activé par Cisco SDM Express ou par un autre moyen, unicast RPF reste désactivé.

Pour activer unicast RPF, la configuration suivante est transmise au routeur pour chaque interface qui se connecte hors du réseau privé (remplacez *<interface externe>* par l'identifiant de l'interface) :

```
interface <interface externe>
ip verify unicast reverse-path
```

Désactiver les messages ARP

Cisco SDM Express désactive les demandes ARP (Address Resolution Protocol) lorsque c'est possible. Une demande ARP gratuite est une diffusion ARP dans laquelle les adresses MAC source et cible sont identiques. Essentiellement, elle permet à un hôte d'informer le réseau sur son adresse IP. Un message ARP usurpé peut endommager le stockage des informations de mappage du réseau et générer des dysfonctionnements du réseau.

Pour désactiver les messages ARP, la configuration suivante est transmise au routeur :

```
no ip gratuitous-arps
```

Vous pouvez annuler ce correctif à l'aide de la fonction Audit de sécurité de Cisco SDM. Pour connaître la procédure, reportez-vous à l'aide en ligne de l'audit de sécurité dans Cisco SDM. Pour plus d'informations, cliquez sur Cisco Router and Security Device Manager.

Désactiver la redirection d'IP

Cisco SDM Express désactive les messages ICMP (Internet Message Control Protocol) lorsque c'est possible. ICMP prend en charge le trafic IP en relayant les informations sur les chemins, les routages et les conditions du réseau. Les messages de redirection ICMP ordonnent à un nœud d'extrémité d'utiliser un routeur particulier pour accéder à une destination donnée. Dans un réseau IP fonctionnant correctement, un routeur n'envoie des redirections qu'aux hôtes de ses propres sous-réseaux, aucun nœud d'extrémité n'envoie jamais de redirection et aucune redirection ne transite par plus d'un relais de réseau. Toutefois, un pirate peut contourner ces règles. D'ailleurs, certaines attaques sont basées sur cette méthode. La désactivation des redirections ICMP n'a aucun impact opérationnel sur le réseau et élimine le risque lié à ce type d'attaque.

La configuration transmise au routeur pour désactiver les messages de redirection ICMP est la suivante :

```
no ip redirects
```

Désactiver le Proxy IP ARP

Cisco SDM Express désactive le proxy ARP (Address Resolution Protocol) lorsque c'est possible. Le réseau utilise le protocole ARP pour convertir les adresses IP en adresses MAC. Normalement, ARP est confiné à un LAN, mais un routeur peut se comporter comme un proxy pour les demandes ARP, rendant ainsi ces dernières disponibles sur plusieurs segments du LAN. Dans la mesure où le proxy ARP franchit la barrière de sécurité du LAN, il est recommandé de ne l'utiliser qu'entre deux LAN ayant un niveau de sécurité égal, et uniquement lorsque la situation l'exige.

La configuration transmise au routeur pour désactiver le proxy ARP est la suivante :

```
no ip proxy-arp
```

Vous pouvez annuler ce correctif à l'aide de la fonction Audit de sécurité de Cisco SDM. Pour connaître la procédure, reportez-vous à l'aide en ligne de l'audit de sécurité dans Cisco SDM. Pour plus d'informations, cliquez sur Cisco Router and Security Device Manager.

Désactiver la diffusion d'IP dirigée

Cisco SDM Express désactive les diffusions d'IP dirigées lorsque c'est possible. Une diffusion d'IP dirigée est un datagramme qui est envoyé à l'adresse de diffusion d'un sous-réseau auquel la machine émettrice n'est pas directement liée. La diffusion dirigée est acheminée via le réseau en tant que paquet individuel, jusqu'au sous-réseau cible où il est converti en une diffusion de couche de liaison. De par la nature de l'architecture de l'adressage IP, seul le dernier routeur de la chaîne, celui qui est connecté directement au sous-réseau cible, peut identifier une diffusion dirigée de manière incontestable. Les diffusions dirigées sont parfois utilisées à des fins légitimes, mais rarement hors du secteur des services financiers.

Les diffusions d'IP dirigées sont utilisées notamment dans les attaques de déni de service, dites smurf, particulièrement répandues, mais également dans d'autres attaques. Dans une attaque de type smurf, le pirate envoie des demandes de réponse ICMP depuis une adresse source falsifiée à une adresse de diffusion dirigée, à quoi tous les hôtes du sous-réseau cible répondent en envoyant des réponses à la source falsifiée. En envoyant un flux continu de telles demandes, le pirate peut générer un flux bien plus important de réponses, et ainsi submerger totalement l'hôte dont l'adresse est falsifiée.

La désactivation des diffusions d'IP dirigées entraîne la suppression des diffusions dirigées qui seraient autrement décomposées en diffusions de couche de liaison sur cette interface.

La configuration transmise au routeur pour désactiver les diffusions d'IP dirigées est la suivante :

```
no ip directed-broadcast
```

Vous pouvez annuler ce correctif à l'aide de la fonction Audit de sécurité de Cisco SDM. Pour connaître la procédure, reportez-vous à l'aide en ligne de l'audit de sécurité dans Cisco SDM. Pour plus d'informations, cliquez sur Cisco Router and Security Device Manager.

Désactiver le service MOP

Cisco SDM Express désactive le protocole MOP (Maintenance Operations Protocol) sur toutes les interfaces Ethernet, lorsque c'est possible. Ce protocole permet de transmettre des informations de configuration au routeur lorsqu'il communique avec des réseaux DECNet. Il est vulnérable à diverses attaques.

La configuration transmise au routeur pour désactiver le service MOP sur les interfaces Ethernet est la suivante :

```
no mop enabled
```

Vous pouvez annuler ce correctif à l'aide de la fonction Audit de sécurité de Cisco SDM. Pour connaître la procédure, reportez-vous à l'aide en ligne de l'audit de sécurité dans Cisco SDM. Pour plus d'informations, cliquez sur Cisco Router and Security Device Manager.

Désactiver les IP injoignables

Cisco SDM Express désactive les messages d'hôte ICMP (Internet Message Control Protocol) injoignables lorsque c'est possible. ICMP prend en charge le trafic IP en relayant les informations sur les chemins, les routages et les conditions du réseau. Les messages d'hôte ICMP injoignable sont envoyés si un routeur reçoit un paquet de non-diffusion qui utilise un protocole inconnu ou un paquet ne pouvant pas atteindre sa destination finale car ne connaissant pas le routage à utiliser pour y accéder. Ces messages peuvent être utilisés par un pirate pour accéder aux informations de mappage d'un réseau.

La configuration transmise au routeur pour désactiver les messages d'hôte ICMP injoignable est la suivante :

```
int <toutes les interfaces>
no ip unreachables
```

Vous pouvez annuler ce correctif à l'aide de la fonction Audit de sécurité de Cisco SDM. Pour connaître la procédure, reportez-vous à l'aide en ligne de l'audit de sécurité dans Cisco SDM. Pour plus d'informations, cliquez sur Cisco Router and Security Device Manager.

Désactiver la réponse au masque IP

Cisco SDM Express désactive les messages de réponse au masque ICMP (Internet Message Control Protocol) lorsque c'est possible. ICMP prend en charge le trafic IP en relayant les informations sur les chemins, les routages et les conditions du réseau. Des messages de réponse au masque ICMP sont envoyés lorsqu'un périphérique réseau doit connaître le masque de sous-réseau d'un sous-réseau particulier dans un réseau interconnecté. Ces messages sont envoyés au périphérique qui demande des informations aux périphériques qui les détiennent. Ces messages peuvent être utilisés par un pirate pour accéder aux informations de mappage d'un réseau.

La configuration transmise au routeur pour désactiver les messages de réponse au masque ICMP est la suivante :

```
no ip mask-reply
```

Vous pouvez annuler ce correctif à l'aide de la fonction Audit de sécurité de Cisco SDM. Pour connaître la procédure, reportez-vous à l'aide en ligne de l'audit de sécurité dans Cisco SDM. Pour plus d'informations, cliquez sur Cisco Router and Security Device Manager.

Définir la longueur minimum du mot de passe pour qu'il ne dépasse pas 6 caractères

Cisco SDM Express configure votre routeur pour qu'il requière un mot de passe d'une longueur minimale de 6 caractères, lorsque c'est possible. L'une des méthodes utilisées par les pirates pour découvrir les mots de passe consiste à essayer toutes les combinaisons de caractères possibles. Plus les mots de passe sont longs, plus les combinaisons de caractères sont nombreuses, ce qui complique considérablement la tâche des pirates.

Cette modification de configuration requiert que chaque mot de passe sur le routeur (utilisateur, activation, secret, console, AUX, tty et vty) ait une longueur minimale de 6 caractères. Elle n'est effectuée que si la version de Cisco IOS exécutée sur le routeur prend en charge la fonction de longueur minimale des mots de passe.

La configuration transmise au routeur est la suivante :

```
security passwords min-length <6>
```

Définir le nombre d'échecs d'identification pour qu'il ne dépasse pas 3 tentatives de réidentification

Cisco SDM Express configure votre routeur pour qu'il verrouille l'accès après 3 tentatives infructueuses de connexion, lorsque c'est possible. L'une des méthodes permettant de découvrir des mots de passe, appelée attaque dictionnaire, consiste à utiliser un logiciel qui tente de se connecter en utilisant chaque mot d'un dictionnaire. Cette configuration entraîne le verrouillage du routeur pendant une durée de 15 secondes après 3 tentatives de connexion infructueuses, assurant ainsi une protection efficace contre les attaques de ce type. Outre le blocage de l'accès au routeur, cette configuration génère un message de journal après 3 tentatives de connexion infructueuses, avertissant l'administrateur qu'un utilisateur tente de se connecter sans y parvenir.

La configuration transmise au routeur pour verrouiller l'accès au routeur après 3 tentatives de connexion infructueuses est la suivante :

```
security authentication failure rate <3>
```

Définir la bannière

Cisco SDM Express configure une bannière de texte lorsque c'est possible. Dans certains pays, la procédure d'engagement de poursuites civiles ou pénales contre les utilisateurs qui s'introduisent dans vos systèmes a été simplifiée si vous affichez une bannière informant les intrus qu'ils ne sont pas autorisés à pénétrer dans vos systèmes. Dans d'autres, il est interdit de surveiller les activités des utilisateurs non autorisés sauf si vous les avez avertis de votre intention de les surveiller. La bannière est une des méthodes permettant d'officialiser cette notification.

La configuration transmise au routeur pour créer une bannière est la suivante (remplacez *<nom de société>*, *<adresse électronique de l'administrateur>* et *<numéro de téléphone de l'administrateur>* par les valeurs appropriées saisies dans Cisco SDM Express :

```
banner ~
Accès réservé
Ce système est la propriété de <nom de société>.
Déconnectez-vous IMMEDIATEMENT si vous n'êtes pas un utilisateur
autorisé.
Contactez <adresse électronique de l'administrateur> au <numéro de
téléphone de l'administrateur>.
~
```

Activer les paramètres Telnet

Cisco SDM Express sécurise les lignes console, AUX, vty et tty en mettant en œuvre les configurations suivantes, lorsque c'est possible :

- Il configure les commandes **transport input** et **transport output** pour définir les protocoles pouvant être utilisés pour se connecter à ces lignes.
- Il définit un délai d'attente EXEC de 10 minutes sur les lignes console et AUX, entraînant la déconnexion de l'administrateur de ces lignes après 10 minutes d'inactivité.

La configuration transmise au routeur pour définir une durée de TCP Synwait de 10 secondes est la suivante :

```
!
line console 0
transport output telnet
exec-timeout 10
login local
```

```
!
line AUX 0
transport output telnet
exec-timeout 10
login local
!
line vty ….
transport input telnet
login local
```

Activer SSH pour l'accès au routeur

Si la version de Cisco IOS exécutée sur le routeur est une crypto-image (une image utilisant le cryptage DES 56 bits et soumise à des restrictions d'exportation), Cisco SDM Express met en œuvre les configurations suivantes pour sécuriser l'accès Telnet, lorsque c'est possible :

- Il active Secure Shell (SSH) pour l'accès Telnet. SSH renforce considérablement l'accès Telnet.
- Il définit un délai d'attente SSH de 60 secondes, entraînant l'arrêt des connexions SSH incomplètes après 60 secondes.
- Il autorise jusqu'à deux tentatives de connexion SSH infructueuses avant de verrouiller l'accès au routeur.

La configuration transmise au routeur pour sécuriser l'accès et les fonctions de transfert de fichiers est la suivante :

```
ip ssh time-out 60
ip ssh authentication-retries 2
!
line vty 0 4
transport input ssh
```

Boutons Cisco SDM Express

Bouton Aide

Cliquez sur le bouton Aide pour ouvrir une nouvelle fenêtre de navigation et afficher des informations sur la fenêtre Cisco SDM Express affichée.

Bouton À propos de

Cliquez sur **À propos de** pour afficher une fenêtre contenant les informations de version de Cisco SDM Express. Cliquez sur **Informations sur le logiciel/matériel** dans cette fenêtre pour afficher les informations suivantes.

Informations sur le matériel :

- Type du modèle de routeur
- Mémoire totale du routeur
- Capacité totale de la mémoire Flash du routeur
- Source du démarrage du routeur, (par exemple : flash)

Un schéma de la configuration matérielle est également fourni.

Informations sur le logiciel :

- Nom du logiciel Cisco IOS que le routeur exécute
- Version du logiciel Cisco IOS
- Les jeux de fonctions, tels que Pare-feu et VPN, pris en charge par le logiciel Cisco IOS
- Version de Cisco SDM Express

Bouton Quitter

Après avoir terminé la configuration initiale, cliquez sur le bouton **Quitter** pour fermer Cisco SDM Express.

Bouton Actualiser

Ces boutons sont visibles si vous modifiez une configuration initiale. Cliquez sur le bouton **Actualiser** pour actualiser les données du routeur dans Cisco SDM Express.

Bouton Appliquer les modifications

Ces boutons sont visibles si vous modifiez une configuration initiale. Cliquez sur le bouton **Appliquer les modifications** pour valider les modifications que vous avez apportées au routeur.

Bouton Annuler les modifications

Ces boutons sont visibles si vous modifiez une configuration initiale. Cliquez sur le bouton **Annuler les modifications** pour annuler toutes les modifications effectuées.

Reconnexion au routeur à l'issue de la configuration initiale

Si vous avez donné à l'interface LAN une nouvelle adresse IP comme recommandé, vous allez perdre la connexion au routeur une fois que vous validerez la configuration.

Suivez cette procédure pour vous reconnecter au routeur après avoir effectué la configuration initiale avec Cisco SDM Express.

Étape 1 Placez le PC sur le même sous-réseau que l'interface LAN du routeur.

- Si vous avez configuré le routeur comme serveur DHCP, vous devez configurer le PC pour qu'il obtienne une adresse IP automatiquement, puis ouvrir une fenêtre de commande dans laquelle vous saisissez la commande **ipconfig /release** suivie de la commande **ipconfig /renew**.
- Si le routeur n'est pas configuré comme serveur DHCP, vous devez attribuer au PC une adresse IP statique appartenant au même sous-réseau que le routeur. Par exemple, si vous avez changé l'adresse IP du réseau local en 10.20.20.1 avec un masque de sous-réseau 255.255.255.224, vous devez donner à votre PC une adresse IP entre 10.20.20.2 et 10.20.20.30 et utiliser la même valeur de sous-réseau.

Étape 2 Si vous avez configuré une autre interface LAN que l'interface par défaut, veillez à connecter votre PC à l'interface LAN configurée. Par exemple, si vous avez configuré FE 0/1 et non pas FE 0/0 comme interface LAN, connectez votre PC à FE 0/1.

Étape 3 Après avoir configuré le PC, reconnectez-le au routeur en saisissant la nouvelle adresse IP que vous avez attribuée à l'interface LAN du routeur dans le navigateur (http://*nouvelle adresse IP)*. Par exemple, si vous avez remplacé l'adresse IP du réseau local par 10.20.20.1, vous devez saisir http://10.20.20.1 dans le navigateur Web pour vous reconnecter au routeur.

Étape 4 Après la reconnexion, vous devez tester votre connexion WAN pour vérifier que vous pouvez vous connecter à Internet.

Pour plus d'informations, reportez-vous à Test de votre connexion WAN (Internet).

Test de votre connexion WAN (Internet)

Vous pouvez tester votre connexion Internet en allant sur un site Web distant, tel que www.cisco.com, avec votre navigateur. Si vous pouvez vous connecter au site Web distant, votre configuration WAN fonctionne correctement.

Si vous n'arrivez pas à vous connecter à un site Web distant, vous pouvez utiliser Cisco SDM pour réparer la connexion en procédant comme suit :

Étape 1 Dans le menu Outils, cliquez sur **Cisco SDM** pour lancer Cisco SDM.

Étape 2 Connectez-vous à Cisco SDM et cliquez sur **Interfaces et connexions**.

Étape 3 Cliquez sur l'onglet Modifier et sélectionnez la connexion WAN à tester.

Étape 4 Cliquez sur **Tester la connexion** et suivez les instructions à l'écran. Cisco SDM établit un rapport sur les problèmes éventuels et actions recommandées.

Conseils de dépannage pour SDP

Utilisez ces informations avant de procéder à une inscription à l'aide de Secure Device Provisioning (SDP) pour préparer la connexion entre le routeur et le serveur de certificats. Si vous rencontrez des problèmes lors de l'inscription, suivez les conseils fournis dans cette section pour en déterminer l'origine.

Lorsque vous lancez SDP, vous devez minimiser la fenêtre du navigateur affichant cette rubrique d'aide pour visualiser l'application Web SDP.

Conseils de dépannage

Ces recommandations impliquent des opérations préalables sur le routeur local et l'autorité de certification (AC) du serveur. Vous devez signaler ces prérequis à l'administrateur du serveur AC. Vérifiez les points suivants :

- Le routeur local et le serveur AC sont reliés par une connexion IP. Le routeur local doit être capable de sonder le serveur de certificats avec succès et réciproquement.
- L'administrateur du serveur AC utilise un navigateur Web prenant en charge JavaScript.
- L'administrateur du serveur AC possède des privilèges d'activation sur le routeur local.
- Le pare-feu du routeur local autorise le trafic en provenance et à destination du serveur de certificats.
- Si un pare-feu est configuré sur le Petitionar (Pétitionnaire) et/ou sur le Registrar (Registraire), vous devez vous assurer qu'il autorise le trafic HTTP ou HTTPS sortant sur le PC à partir duquel l'application SDM/SDP est invoquée.

Pour plus d'informations sur SDP (en anglais), cliquez sur le lien suivant :

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a008028afbd.html#wp1043332

Mode Édition de Cisco SDM Express

Les écrans d'édition de SDM Express vous permettent d'apporter des modifications à vos configurations LAN et WAN et à vos divers paramètres (pare-feu, NAT, PAT, routage et sécurité).

Présentation

La fenêtre Présentation affiche des informations de base sur les configurations LAN, WAN et de pare-feu du routeur.

Icônes

	En service. L'interface est en service.
	Actif. Le pare-feu est actif.
	Hors service. L'interface est arrêtée.
	Inactif. Le pare-feu est inactif.

Champs LAN

Les champs LAN affichent des informations sur l'interface, l'adresse IP et le serveur DHCP concernant la connexion au réseau local (LAN).

- **Interface** : nom de l'interface du réseau local LAN. Par exemple, Fast Ethernet 0. Si SDM Express ne peut pas identifier les interfaces LAN du routeur, il affiche dans ce champ le nombre d'interfaces LAN configurées.
- **Masque/IP** : adresse IP suivie du nombre de bits de sous-réseau, qui représente le masque de sous-réseau. Les adresses IP du réseau LAN proviennent souvent de la plage d'adresses IP privées. Par exemple, une adresse IP 10.10.10.1 utilisant un masque de sous-réseau 255.255.255.0 sera représentée comme suit : 10.10.10.1/24.
- **Serveur DHCP** : soit **Configuré** soit **Non configuré**.
- **Pool DHCP** : si un serveur DHCP a été configuré, ce champ contient la plage d'adresses IP disponibles pour les clients DHCP. Par exemple, si l'interface LAN est configurée avec une adresse IP dans le réseau 10.10.10.0, le pool DHCP peut être configuré avec une plage d'adresses de 10.10.10.1 à 10.10.10.254.

Si SDM Express ne peut pas identifier les interfaces LAN sur le routeur, il affiche le nombre total d'interfaces LAN prises en charge et le nombre total d'interfaces LAN configurées.

Champs Internet (WAN)

Les champs Internet affichent des informations sur l'interface WAN, le type de connexion WAN configurée et les informations du masque de sous-réseau de l'adresse IP.

- **Interface** : nom de l'interface WAN, par exemple ATM 0/1. Si SDM Express ne peut pas identifier les interfaces WAN sur le routeur, il affiche dans ce champ le nombre d'interfaces WAN configurées.
- **Type de connexion** : type de connexion WAN, par exemple ADSL ou G.SHDSL.
- **Masque/IP** : adresse IP suivie du nombre de bits de sous-réseau, qui représente le masque de sous-réseau. Par exemple, une adresse IP 172.16.33.15 utilisant un masque de sous-réseau 255.255.255.0 sera représentée comme suit : 172.16.33.15/24.

Si SDM Express ne peut pas identifier les interfaces WAN sur le routeur, il affiche le nombre total d'interfaces WAN prises en charge et le nombre total d'interfaces WAN configurées.

Champs Pare-feu

- **Type de pare-feu** : Cisco SDM Express par défaut, Personnalisé ou Aucun.
- **Interne** : adresse IP de l'interface interne ou approuvée.
- **Externe** : type de connexion de l'interface Internet.

Configuration de base

Cette fenêtre affiche les comptes utilisateur configurés sur le routeur et vous permet de modifier le mot de passe secret d'activation. Le mot de passe secret d'activation doit être utilisé pour accéder au mode d'activation de l'interface de ligne de commande IOS.

Si vous souhaitez ajouter ou retirer des comptes utilisateur, vous pouvez le faire à l'aide de Cisco Router and Security Device Manager (SDM).

Boutons Modifier/Supprimer

Utilisez ces boutons pour gérer les comptes utilisateur sur le routeur. Vous pouvez modifier et supprimer des comptes utilisateur existants. Si vous devez créer un nouveau compte utilisateur, vous pouvez utiliser SDM. Pour plus d'informations, reportez-vous à la section Cisco Router and Security Device Manager.

Remarque Les boutons Modifier et Supprimer sont désactivés lorsqu'un compte utilisateur créé à l'aide de l'option Afficher est sélectionné.

Champs Nom d'utilisateur/Mot de passe de connexion/Le mot de passe est crypté

Cette zone répertorie les comptes utilisateur sur le routeur.

Champ Activer le mot de passe secret

Saisissez le nouveau mot de passe dans ces champs. Veillez à prendre note de ce mot de passe. Il est stocké sous forme cryptée sur le routeur et ne peut pas être lu.

Champ Nom d'hôte

Vous pouvez modifier le nom d'hôte du routeur si vous le souhaitez.

Champ Nom de domaine

Vous pouvez modifier le nom de domaine configuré du routeur.

Boutons Actualiser/Appliquer les modifications/Annuler les modifications

Ces boutons sont visibles si vous modifiez une configuration initiale. Pour plus d'informations, cliquez sur Boutons Cisco SDM Express**.**

Modification d'un nom d'utilisateur

Modifiez un compte utilisateur dans les champs affichés dans cette fenêtre.

Champ Nom d'utilisateur

Modifiez le nom d'utilisateur dans ce champ.

Champ Mot de passe

Entrez ou modifiez le mot de passe dans ce champ.

Retapez le mot de passe dans le champ **Confirmer le mot de passe**. Si les mots de passe saisis ne correspondent pas, un message d'erreur s'affiche lorsque vous cliquez sur **OK**.

Lorsque vous cliquez sur **OK**, les informations concernant le compte nouveau ou modifié s'affichent dans la fenêtre Configurer les comptes utilisateur pour Telnet/SSH.

Case à cocher Crypter le mot de passe avec un algorithme de hachage MD5

Il s'agit d'un champ en lecture seule qui affiche le paramètre en vigueur pour le cryptage de mot de passe MD5. Une coche indique que le mot de passe est crypté à l'aide de l'algorithme MD5 (Message Digest 5).

LAN

Case à cocher Raccorder/Ne pas raccorder l'interface LAN à l'interface sans fil

Si votre routeur possède une interface sans fil, vous pouvez acheminer le trafic du réseau sans fil vers votre réseau LAN Ethernet. Si vous souhaitez acheminer ainsi le trafic et partager l'espace des adresses entre le réseau LAN Ethernet sur votre routeur et le réseau sans fil, cliquez sur **Raccorder l'interface LAN à l'interface sans fil**.

Champs Configuration de l'interface LAN

Vous pouvez modifier dans ces champs l'adresse IP et le masque de sous-réseau de l'interface LAN. Pour plus d'informations sur les champs d'adresse IP et de masque de sous-réseau, reportez-vous à Champ Adresse IP.

Sans fil

La fenêtre Sans fil s'affiche lorsque votre routeur possède une interface sans fil. Si vous devez configurer des paramètres sans fil avancés, cliquez sur **Lancer application sans fil**.

Bouton Actualiser

Ce bouton est visible si vous modifiez une configuration initiale. Pour plus d'informations, cliquez sur Boutons Cisco SDM Express**.**

WAN : impossible de configurer l'interface WAN

Cette fenêtre s'affiche lorsque SDM Express ne parvient pas à configurer l'interface que vous avez choisie en tant qu'interface WAN. Cela peut se produire si l'interface que vous avez sélectionnée n'est pas prise en charge par SDM Express ou si elle possède une configuration partielle qui a été saisie via l'interface de la ligne de commande.

Vous pouvez sélectionner une autre interface à configurer ou vous connecter au routeur et supprimer les instructions de configuration relatifs à l'interface à configurer. Dans la section Outils, sélectionnez **Telnet**, connectez-vous au routeur et accédez au mode de configuration. Utilisez l'interface de la ligne de commande pour supprimer les instructions de configuration. Revenez ensuite à SDM Express et configurez l'interface WAN.

Aucun WAN disponible

Cette fenêtre s'affiche lorsque SDM Express ne parvient pas à détecter d'interface WAN sur votre routeur.

Supprimer la connexion

Lorsque vous supprimez une connexion, il est possible que des commandes de configuration associées soient conservées dans la configuration ou supprimées avec la connexion. Cliquez sur **Afficher détails** pour afficher ces associations. Cliquez sur **Masquer détails** pour masquer les informations d'association.

Cliquez sur **Suppression automatique de toutes les associations** si vous souhaitez que SDM Express supprime les associations parallèlement à la connexion.

Cliquez sur **Je supprimerai les associations plus tard** si vous souhaitez supprimer les associations vous-même.

Pour supprimer vous-même les associations, cliquez sur **Telnet** dans le menu Outils, connectez-vous au routeur et saisissez la commande **enable** pour accéder au mode d'activation. Ensuite, supprimez les commandes de configuration associées en entrant la forme **no** de la commande. Par exemple, si la commande **ip tcp adjust mss** est associée à la connexion, saisissez :

```
no ip tcp adjust mss
```

Pare-feu

Utilisez cette fenêtre pour activer un pare-feu si vous ne l'avez pas activé pendant la configuration initiale ou pour le désactiver dans le cas contraire. Si l'image Cisco IOS exécutée sur le routeur ne prend pas en charge la fonction du pare-feu, vous ne pourrez pas activer un pare-feu de base sur ce routeur. Vous ne pourrez pas utiliser SDM Express pour activer un pare-feu de base si votre routeur est un routeur modulaire avec plusieurs interfaces LAN ou WAN.

Pour obtenir une description des capacités d'un routeur de base, reportez-vous à Configuration du pare-feu.

Boutons Activer le pare-feu/Désactiver le pare-feu

Utilisez ces boutons pour ajouter ou supprimer la configuration de pare-feu de base.

Fenêtre Impossible de configurer le pare-feu

Si SDM Express ne parvient pas à vous laisser configurer un pare-feu, la fenêtre Impossible de configurer le pare-feu s'affiche. Les raisons possibles à cela sont les suivantes :

- Le routeur est un routeur à port fixe et il n'y a pas précisément une interface LAN et une interface WAN configurées.
- Le routeur est un routeur modulaire ou il existe plus de deux interfaces configurées.
- Un pare-feu et/ou des listes de contrôle d'accès ont été appliqués à votre routeur à l'aide d'autres outils.

Bouton Actualiser

Ce bouton est visible si vous modifiez une configuration initiale. Pour plus d'informations, cliquez sur Boutons Cisco SDM Express**.**

NAT

Si les périphériques du LAN possèdent des adresses privées, vous pouvez les autoriser à partager une même adresse IP publique en utilisant la conversion d'adresses réseau (NAT). La NAT utilise les numéros de port pour identifier les hôtes et les services d'hôte que vous souhaitez rendre disponibles.

Cliquez sur **Activer NAT** pour utiliser la conversion d'adresses réseau sur le routeur.

Impossible de configurer NAT

Si vous êtes en mode édition de SDM Express, cette fenêtre apparaît lorsque SDM Express ne peut pas vous aider à configurer NAT. SDM Express est incapable de vous aider à configurer NAT pour les raisons suivantes.

- Le routeur est un routeur à port fixe et il n'y a pas précisément une interface LAN et une interface WAN configurées.
- Le routeur est un routeur modulaire ou il existe plus de deux interfaces configurées.
- NAT est déjà configuré sur une interface.

Bouton Ajouter

Cliquez sur ce bouton pour ajouter une nouvelle règle NAT.

Bouton Modifier

Cliquez sur ce bouton pour modifier la règle NAT choisie.

Bouton Actualiser

Ce bouton est visible si vous modifiez une configuration initiale. Pour plus d'informations, cliquez sur Boutons Cisco SDM Express**.**

Ajouter ou modifier une règle de conversion d'adresse

Cette fenêtre vous permet d'entrer ou de modifier les informations concernant la conversion des adresses IP d'un serveur.

Adresse IP privée

Saisissez l'adresse IP utilisée par le serveur sur votre réseau interne. Cette adresse IP ne peut pas être utilisée de manière externe, sur Internet par exemple.

Adresse IP publique

Sélectionnez **Adresse IP de l'interface WAN** pour utiliser l'adresse IP de l'interface WAN du routeur. L'adresse IP configurée de l'interface WAN apparaît sur la droite. Vous pouvez également sélectionner **Nouvelle adresse IP** et entrer l'adresse IP du serveur.

Type de serveur

Dans le menu déroulant, sélectionnez l'un des types de serveurs suivants :

- Serveur Web

  Hôte HTTP utilisant HTML ou des pages WWW.

- Serveur de messagerie

  Serveur SMTP pour l'envoi de messages sur Internet.

- Autre

  Le serveur n'est pas un serveur Web ou de messagerie et nécessite une conversion de port pour fonctionner. Si vous sélectionnez cette option, le champ Port traduit et le menu déroulant Protocole deviennent accessibles.

Si vous ne sélectionnez pas de type de serveur, tout le trafic destiné à l'adresse IP publique choisie sera routé vers le serveur et aucune conversion de port ne sera effectuée.

Port d'origine

Entrez le numéro de port utilisé par le serveur pour accepter les requêtes de service en provenance du réseau interne.

Port traduit

Entrez le numéro de port utilisé par le serveur pour accepter les requêtes de service en provenance d'Internet.

Protocole

Sélectionnez TCP ou UDP comme protocole à utiliser par le serveur pour les ports convertis et d'origine.

Routage

La fenêtre Routage vous permet de modifier un routage par défaut existant lorsque des changements de configuration indiquent qu'il est recommandé de le modifier. Par exemple, si vous avez modifié une adresse IP statique d'une interface WAN, il est possible que vous deviez aussi changer l'adresse IP de la passerelle par défaut.

Case à cocher Activer

Cochez cette case pour activer un routage par défaut. Si un routage par défaut a déjà été défini, cette case sera cochée. Si vous la désactivez, le routage par défaut sera désactivé.

Champ Acheminement (relais suivant)

Vous pouvez préciser une interface de routeur ou une adresse IP comme relais suivant. Si vous cliquez sur **Interface**, sélectionnez l'interface dans la liste déroulante. Si vous cliquez sur **Adresse IP**, saisissez l'adresse IP.

Boutons Actualiser/Appliquer les modifications/Annuler les modifications

Ces boutons sont visibles si vous modifiez une configuration initiale. Pour plus d'informations, cliquez sur Boutons Cisco SDM Express**.**

Paramètres de sécurité

Cette fenêtre vous permet de désactiver les fonctions activées par défaut dans le logiciel Cisco IOS, mais qui peuvent générer des risques pour la sécurité ou qui forcent le routeur à envoyer des messages trop volumineux pour la mémoire disponible. Laissez ces cases non cochées sauf si vos besoins sont différents.

Si vous autorisez SDM Express à réaliser ces réglages et si vous souhaitez modifier ultérieurement l'un des paramètres décrits dans ces groupes de paramètres, vous pouvez le faire à l'aide de SDM. Pour plus d'informations, reportez-vous à la section Cisco Router and Security Device Manager.

Case à cocher Sélectionner tout (recommandé par Cisco)

En cliquant sur **Sélectionner tout**, vous pouvez mettre en œuvre tous les paramètres de sécurité dans cette fenêtre. Si vous souhaitez modifier ultérieurement les paramètres de sécurité, vous pouvez le faire à l'aide de Cisco SDM.

Case à cocher Désactiver les services entraînant des risques pour la sécurité

Cochez cette case pour désactiver les services suivants sur le routeur. Pour savoir pourquoi ces services doivent être désactivés, cliquez sur les liens ci-dessous :

- Désactiver le service Finger
- Désactiver le service PAD
- Désactiver le service TCP Small Servers
- Désactiver le service UDP Small Servers
- Désactiver le service IP Bootp Server
- Désactiver le service IP Ident
- Désactiver CDP
- Désactiver le routage d'IP source
- Désactiver les messages ARP
- Désactiver la redirection d'IP
- Désactiver le Proxy IP ARP
- Désactiver la diffusion d'IP dirigée
- Désactiver le service MOP
- Désactiver les IP injoignablesDésactiver la réponse au masque IP

Case à cocher Activer les services renforçant la sécurité sur le routeur/le réseau

Cochez cette case pour activer sur le routeur les fonctions et services améliorant la sécurité. Pour plus d'informations sur ces services et fonctions, cliquez sur les liens ci-dessous :

- Activer la commutation Netflow
- Activer le maintien des connexions TCP pour les sessions Telnet entrantes
- Activer le maintien des connexions TCP pour les sessions Telnet sortantes

- Activer les numéros de séquence et les horodatages sur les débogages
- Activer IP CEF
- Définir l'intervalle de planification
- Définir l'allocation de planification
- Définir la durée de TCP Synwait
- Activer la connexion

Case à cocher Crypter les mots de passe

Cochez cette case pour activer le cryptage des mots de passe. Pour plus d'informations, reportez-vous à Activer le service de cryptage des mots de passe.

Case à cocher Synchroniser avec l'horloge de mon PC local

Cliquez sur ce bouton pour synchroniser votre routeur avec l'horloge de votre PC local.

Boutons Actualiser/Appliquer les modifications/Annuler les modifications

Ces boutons sont visibles si vous modifiez une configuration initiale. Pour plus d'informations, cliquez sur Boutons Cisco SDM Express**.**

Outils

SDM Express dispose d'un certain nombre d'outils que vous pouvez utiliser.

Option de sondage

Cliquez dessus pour ouvrir une fenêtre dans laquelle vous pouvez indiquer la source et la destination du sondage. Pour plus d'informations, reportez-vous à Ping.

Option Telnet

Affiche la boîte de dialogue Telnet de Windows, qui vous permet de vous connecter au routeur et d'accéder à l'interface de ligne de commande de Cisco IOS à l'aide du protocole Telnet.

Option Cisco SDM

Permet de lancer Cisco Router and Security Device Manager (SDM). SDM vous permet de réaliser des configurations avancées.

Option Mise à jour du logiciel

SDM Express peut vous aider à mettre à jour le logiciel de configuration sur votre routeur. Vous pouvez effectuer la mise à jour à partir de Cisco.com ou, si vous avez téléchargé le fichier SDM.zip sur votre PC, à l'aide de ce dernier. Pour plus d'informations, cliquez sur l'un des liens suivants.

- Mettre à jour SDM depuis Cisco.com
- Mettre à jour SDM depuis un PC local
- Mettre à jour SDM depuis le CD

Ping

Cette fenêtre vous permet de sonder un périphérique homologue. Vous pouvez sélectionner la source et la destination de l'opération de sondage. Vous pouvez être amené à sonder un homologue distant après avoir reconfiguré une connexion WAN.

Champ Source

Sélectionnez ou entrez l'adresse IP source de la commande Sonder. Si l'adresse que vous souhaitez utiliser ne figure pas dans la liste, entrez-en une autre dans ce champ. La commande de sondage peut provenir de n'importe quelle interface du routeur. Par défaut, la commande **Ping** provient de l'interface externe connectée au périphérique distant.

Champ Destination

Sélectionnez l'adresse IP que vous souhaitez sonder. Si l'adresse que vous souhaitez utiliser ne figure pas dans la liste, entrez-en une autre dans ce champ.

Pour sonder un homologue distant :

Spécifiez la source et la destination, puis cliquez sur **Sonder**. Lisez le résultat de la commande **Ping** pour déterminer si elle a abouti.

Pour effacer le résultat de la commande Ping :

Cliquez sur **Effacer**.

Mettre à jour SDM depuis Cisco.com

Vous pouvez mettre à jour SDM Express et SDM directement à partir de Cisco.com. SDM vérifie les versions disponibles sur Cisco.com et vous informe si une version plus récente que celle utilisée sur le routeur est à disposition. Vous pouvez ensuite mettre à jour SDM à l'aide de l'assistant de mise à jour.

Pour mettre à jour SDM à partir de Cisco.com :

Étape 1 Sélectionnez Mettre à jour SDM depuis Cisco.com dans le menu Outils. Cette option démarre l'assistant de mise à jour.

Étape 2 Utilisez cet assistant pour récupérer les fichiers de SDM et les copier sur votre routeur.

Connexion CCO

Afin d'accéder à cette page Web, vous devez fournir une connexion CCO et un mot de passe. Donnez un nom d'utilisateur et un mot de passe, puis cliquez sur OK.

Si vous ne disposez pas d'une connexion CCO et d'un mot de passe, vous pouvez les obtenir en ouvrant un navigateur Web et en vous rendant sur le site Web de Cisco à l'adresse suivante :

http://www.cisco.com

Lors de l'ouverture de la page Web, cliquez sur S'inscrire et donnez les informations nécessaires à l'obtention d'un nom d'utilisateur et d'un mot de passe. Puis essayez à nouveau cette opération.

Mettre à jour SDM depuis un PC local

Vous pouvez mettre à jour SDM à l'aide du fichier SDM.zip que vous avez téléchargé depuis Cisco.com. SDM fournit un assistant de mise à jour qui va copier les fichiers nécessaires sur le routeur.

Pour mettre à jour SDM depuis le PC utilisé pour exécuter SDM, procédez comme suit :

Étape 1 Téléchargez le fichier sdm-v*nn*.zip à l'adresse suivante :

http://www.cisco.com/cgi-bin/tablebuild.pl/sdm

Si plusieurs fichiers zip SDM sont disponibles, choisissez celui dont le numéro de version est le plus élevé.

Étape 2 Utilisez l'assistant de mise à jour pour copier les fichiers de SDM depuis votre PC sur votre routeur.

Mettre à jour SDM depuis le CD

Si vous disposez du CD de SDM, vous pouvez l'utiliser pour mettre à jour SDM sur votre routeur. Pour ce faire, procédez comme suit :

Étape 1 Introduisez le CD de SDM dans le lecteur de CD du PC.

Étape 2 Sélectionnez **Mettre à jour SDM depuis le CD** et cliquez sur **Mettre à jour le logiciel** dans la fenêtre Instructions générales après avoir lu le texte.

Étape 3 SDM vous permet de repérer le fichier SDM-Updates.xml sur le CD. Une fois le fichier repéré, cliquez sur **Ouvrir**.

Étape 4 Suivez les instructions de l'assistant d'installation.

Propriétés de la date et de l'heure

Utilisez cette fenêtre pour définir la date et l'heure du routeur. Vous pouvez laisser SDM Express synchroniser ces paramètres sur ceux du PC ou les définir manuellement.

Case à cocher Synchroniser avec l'horloge de mon PC local

Cochez cette case pour que SDM Express synchronise la date et l'heure du routeur sur ceux du PC.

Case à cocher Synchroniser

Cliquez sur ce bouton pour laisser SDM Express effectuer la synchronisation. SDM Express n'ajuste la date et l'heure que lorsque vous cliquez sur **Synchroniser ; il ne les resynchronise pas automatiquement sur la date et l'heure du PC lors des sessions suivantes. Ce bouton est désactivé si vous n'avez pas coché Synchroniser avec l'horloge de mon PC local.**

Remarque Vous devez effectuer les réglages Fuseau horaire et Heure d'été sur le PC avant de lancer SDM Express pour que ce dernier reçoive les paramètres corrects lorsque vous cliquez sur **Synchroniser**.

Champs Modifier la date et l'heure

Utilisez cette zone pour définir la date et l'heure manuellement. Vous pouvez choisir le mois et l'année dans les listes déroulantes, et sélectionner le jour du mois dans le calendrier. Les champs de la zone Heure requièrent des valeurs au format 24 heures. Vous pouvez choisir le fuseau horaire GMT (Greenwich Mean Time) ou une des villes principales de votre fuseau horaire.

Si vous souhaitez que le routeur bascule automatiquement entre l'heure d'été et l'heure d'hiver, cochez la case **Ajuster automatiquement l'horloge en fonction du changement d'heure**.

Bouton Appliquer

Cliquez sur ce bouton pour appliquer la date et l'heure configurées dans les champs Date, Heure et Fuseau horaire.

Valeurs par défaut

Vous pouvez rétablir les réglages d'usine sur le routeur et enregistrer cette configuration dans un fichier réutilisable ultérieurement. Si vous avez modifié l'adresse IP du LAN du routeur (10.10.10.1), vous perdez la connexion entre le routeur et le PC car l'adresse IP 10.10.10.1 est rétablie lors de la réinitialisation.

Remarque La fonction Rétablir les réglages d'usine n'est pas prise en charge sur les routeurs Cisco 3620, 3640, 3640A et 7000.

Étape 1 : Enregistrez la configuration en cours sur le PC.

Enregistrez la configuration en cours du routeur sur le PC maintenant afin de pouvoir la restaurer sur votre routeur en cas de besoin. Utilisez le bouton **Parcourir** pour sélectionner le répertoire dans lequel stocker la configuration.

Étape 2 : Consignez ces étapes par écrit, puis réinitialisez le routeur.

Comme vous perdrez le contact avec le routeur lorsque vous cliquerez sur **Réinitialiser**, vous devez savoir comment vous allez vous reconnecter après la réinitialisation du routeur.

a) Affectez au PC une adresse IP sur le réseau 10.10.10.0.

Configurez votre PC pour le placer sur le sous-réseau 10.10.10.0. En fonction du routeur, vous devez configurer le PC de sorte qu'il obtienne une adresse IP automatiquement ou en lui attribuant une adresse IP statique sur le sous-réseau 10.10.10.0.

Si votre routeur figure dans le tableau suivant, configurez votre PC pour qu'il obtienne une adresse IP automatiquement. Pour savoir comment procéder, reportez-vous à Reconfiguration de votre PC avec une adresse IP statique ou dynamique.

Si vous possédez l'un de ces routeurs, configurez le PC afin qu'il obtienne une adresse IP automatiquement.
SB10x, Cisco 83x, 85x, 87x, 1701, 1710, 1711, 1712, 180x et 181x.

Si votre routeur est répertorié dans le tableau suivant, affectez à votre PC une adresse IP sur le sous-réseau 10.10.10.0, entre 10.10.10.2 et 10.10.10.6 et utilisant le masque de sous-réseau 255.255.255.248. Reportez-vous à la section Reconfiguration de votre PC avec une adresse IP statique ou dynamique pour connaître la procédure à suivre.

Si vous possédez l'un de ces routeurs, affectez à votre PC une adresse IP statique sur le sous-réseau 10.10.10.0.
Cisco 1721, 1751, 1760, 1841, 2600XM, 2691, 28xx, 36xx, 37xx et 38xx.

b) Pointez votre navigateur sur http(s)://10.10.10.1.

Après la réinitialisation, le routeur possède l'adresse IP par défaut d'origine de 10.10.10.1 : c'est donc celle-ci que vous devez utiliser pour vous reconnecter.

c) Connectez-vous de nouveau à SDM Express avec le nom d'utilisateur cisco et le mot de passe cisco.

Le nom d'utilisateur et le mot de passe ont également repris leur valeur initiale, que vous devez utiliser pour vous connecter à SDM Express.

Bouton Actualiser

Ce bouton est visible si vous modifiez une configuration initiale. Pour plus d'informations, cliquez sur Boutons Cisco SDM Express.

Reconfiguration de votre PC avec une adresse IP statique ou dynamique

Le processus d'attribution d'une adresse IP statique à un PC ou de configuration du PC pour qu'il obtienne automatiquement une adresse IP varie légèrement selon la version de Microsoft Windows installée sur le PC.

Remarque Ne reconfigurez pas le PC avant d'avoir réinitialisé le routeur.

Microsoft Windows NT

Dans le Panneau de configuration, double-cliquez sur l'icône **Réseau** pour afficher la fenêtre du même nom. Cliquez sur **Protocoles**, sélectionnez la première entrée Protocole TCP/IP puis cliquez sur **Propriétés**. Dans la fenêtre Propriétés, sélectionnez la carte Ethernet utilisée pour cette connexion. Cliquez sur **Obtenir une adresse IP automatiquement** pour obtenir une adresse IP dynamique.

Pour utiliser une adresse IP statique, cliquez sur **Utiliser l'adresse IP suivante**. Saisissez l'adresse IP 10.10.10.2 ou toute autre adresse supérieure à 10.10.10.1 dans le sous-réseau 10.10.10.0. Entrez le sous-réseau 255.255.255.248. Les autres champs peuvent être laissés vides. Cliquez sur **OK**.

Microsoft Windows ME

Dans le Panneau de configuration, double-cliquez sur l'icône **Réseau** pour afficher la fenêtre du même nom. Double-cliquez sur l'entrée Protocole TCP/IP associée à la carte Ethernet utilisée pour cette connexion, afin d'afficher les **Propriétés** de TCP/IP. Dans l'onglet Adresse IP, cliquez sur **Obtenir une adresse IP automatiquement** pour obtenir une adresse IP dynamique.

Pour utiliser une adresse IP statique, cliquez sur **Utiliser l'adresse IP suivante**. Saisissez l'adresse IP 10.10.10.2 ou toute autre adresse supérieure à 10.10.10.1 dans le sous-réseau 10.10.10.0. Entrez le sous-réseau 255.255.255.248. Les autres champs peuvent être laissés vides. Cliquez sur **OK**.

Microsoft Windows 2000

Dans le Panneau de configuration, sélectionnez **Connexions réseau et accès à distance/Connexion au réseau local**. Sélectionnez la carte Ethernet dans le champ Se connecter en utilisant. Sélectionnez Protocole Internet et cliquez sur Propriétés. Cliquez sur **Obtenir une adresse IP automatiquement** pour obtenir une adresse IP dynamique.

Pour utiliser une adresse IP statique, cliquez sur **Utiliser l'adresse IP suivante**. Saisissez l'adresse IP 10.10.10.2 ou toute autre adresse supérieure à 10.10.10.1 dans le sous-réseau 10.10.10.0. Entrez le sous-réseau 255.255.255.248. Les autres champs peuvent être laissés vides. Cliquez sur **OK**.

Microsoft Windows XP

Cliquez sur **Démarrer** et sélectionnez **Paramètres**, **Connexions réseau**, puis la connexion au réseau local que vous allez utiliser. Cliquez sur **Propriétés**, sélectionnez **Protocole Internet (TCP/IP)** et cliquez sur le bouton **Propriétés**. Cliquez sur **Obtenir une adresse IP automatiquement** pour obtenir une adresse IP dynamique.

Pour utiliser une adresse IP statique, cliquez sur **Utiliser l'adresse IP suivante**. Saisissez l'adresse IP 10.10.10.2 ou toute autre adresse supérieure à 10.10.10.1 dans le sous-réseau 10.10.10.0. Entrez le sous-réseau 255.255.255.248. Les autres champs peuvent être laissés vides. Cliquez sur **OK**.

Fonction non disponible

Cette fenêtre s'affiche lorsque la fonction que vous essayez de configurer n'est pas disponible. Cela peut se produire lorsque l'image IOS ou le matériel du routeur ne prend pas en charge la fonction concernée.

L

M

N

P

R

S

T

U