GUIDE D'ADMINISTRATION

Cisco Small Business

Dispositifs de sécurité de la gamme SA500

Cisco et le logo Cisco sont des marques déposées de Cisco Systems, Inc. et/ou de ses sociétés affiliées aux États-Unis et dans d'autres pays. Vous trouverez une liste des marques commerciales de Cisco sur la page Web **www.cisco.com/go/trademarks**. Les autres marques commerciales mentionnées dans les présentes sont la propriété de leurs détenteurs respectifs. L'utilisation du terme « partenaire » n'implique pas de relation de partenariat entre Cisco et toute autre entreprise. (1005R)

© 2011 Cisco Systems, Inc. Tous droits réservés.
OL-24299-01

Chapitre 1 : Pour commencer 10

Présentation des caractéristiques 10
- Présentation du périphérique 11
- Panneau avant 11
- Panneau arrière 12

Installation 13
- Options d'installation 13
- Installation du matériel 16

Mise en route à l'aide de l'utilitaire de configuration 17
- Connexion au dispositif de configuration 18
- Utilisation des pages de la section Getting Started 19
- Naviguer à travers le dispositif de configuration 21
- Utilisation du système d'aide 22

À propos des paramètres par défaut 22

Tâches de base 23
- Modifier le nom d'utilisateur et le mot de passe par défaut 23
- Sauvegarde de la configuration 24
- Mise à jour du microprogramme 25

Scénarios communs de configuration 25

configuration de base du réseau avec accès Internet 26

configuration du système de communications Cisco Smart Business 29

pare-feu pour le contrôle du trafic entrant et sortant 30

DMZ pour sites Web et services publics 31

configuration de ProtectLink Web et de la sécurité de la messagerie 32

réseau de site à site et accès à distance 32

réseau sans fil 36

Chapitre 2 : Mise en réseau 37

Configuration de la connexion WAN 37
- Afficher l'état du WAN 41
- Création de profils PPPoE 42
- Configuration d'un alias IP 43

Configuration de la zone LAN 43
À propos des paramètres LAN par défaut 44
Configuration de la zone LAN 45
Afficher l'état du LAN 47
Configuration VLAN 48
IP DHCP réservées 53
Clients soumis au bail DHCP 54
Configuration d'un proxy IGMP 54
Configuration du port facultatif comme port LAN 55
Configuration du WAN facultatif 55
Configuration du renvoi automatique, de l'équilibrage de charge et de la détection des défaillances 59
Configuration des liaisons de protocole pour l'équilibrage de charge 62
Configuration d'un DMZ 64
Configuration des paramètres du DMZ 67
IP DMZ réservées 69
Clients soumis au bail DHCP DMZ 70
Routage 70
Routage 70
Routage statique 71
Routage dynamique 72
Gestion des ports 74
Configuration des ports 74
Configuration de SPAN (mise en miroir des ports) 74
Profils de bande passante QoS 75
Création des profils de bande passante QoS pour les interfaces WAN 75
Sélecteurs de trafic 77
QoS du LAN 78
Activation de QoS LAN 78
Mappage CoS de port 78
Mappage DSCP de port 78
Nouveau marquage DSCP 79

DNS dynamique 79
Configuration de l'adressage IPv6 80
Mode de routage IP 81
Configuration de la connexion WAN IPv6 82
Configuration du LAN IPv6 83
Pools d'adresses LAN IPv6 85
Multi-LAN IPv6 86
Routage statique IPv6 87
Routage (RIPng) 88
Tunnellisation 6to4 89
État des tunnels IPv6 89
Tunnels ISATAP 89
Tunnels MLD 90
RADVD (Router Advertisement Daemon) 91
Configuration des annonces du routeur 91
Ajouter des préfixes RADVD 92

Chapitre 3 : Configuration sans fil pour le SA520W 94

Configuration d'un point d'accès 94
Étape 1 : configuration des profils sans fil 95
Configuration avancée du profil 98
Configuration des paramètres de qualité de service pour un profil sans fil 99
Contrôle de l'accès sans fil par le biais des adresses MAC 100
Étape 2 : configuration des points d'accès 102
Configuration du réseau radio 103
Configuration radio de base 103
Page Advanced Radio Settings 105

Chapitre 4 : Configuration du pare-feu 107

Configuration des règles de pare-feu pour contrôler le trafic entrant et sortant 107
Tâches préliminaires pour les règles de pare-feu 108
Configuration de la stratégie sortante par défaut 111

Configuration d'une règle de pare-feu pour le trafic sortant 111
Configuration d'une règle de pare-feu pour le trafic entrant 114
Attribution de priorité aux règles de pare-feu 118
Exemples de configuration de règles de pare-feu 119
Utilisation d'autres outils pour éviter les attaques, limiter les accès et contrôler le trafic entrant 122
Configuration des contrôles d'attaque 123
Configuration du filtrage MAC pour autoriser ou bloquer le trafic 124
Fenêtre IP/MAC Binding 126
Déclenchement de port 127
Configuration d'une règle de déclenchement de port pour diriger le trafic vers les ports spécifiés 127
Affichage de l'état de déclenchement de port 128
Configuration des paramètres de session pour l'analyse des paquets entrants 129
Utilisation d'autres outils pour contrôler l'accès à Internet 130
Configuration du filtrage du contenu pour autoriser ou bloquer les composants Web 130
Configuration des URL approuvées pour autoriser l'accès aux sites Web 132
Configuration des URL bloquées pour empêcher l'accès aux sites Web 133
Configuration de l'association IP/MAC pour éviter l'usurpation d'adresse 134
SIP 135

Chapitre 5 : Système de prévention des intrusions 137

Configuration de la traduction d'adresses réseau (IPS) 138
Configuration de la politique IPS 139
Configuration des paramètres d'inspection de protocole 140
Configuration du blocage homologue-à-homologue et de la messagerie instantanée 141

Chapitre 6 : Utilisation des services Cisco ProtectLink Security 143

Chapitre 7 : La configuration VPN 144

À propos du VPN 144

Configuration d'un tunnel VPN de site à site 145
Configuration d'un tunnel VPN IPsec d'accès à distance avec un client VPN 148
Configuration de la base de données utilisateur pour l'accès à distance VPN IPsec 151
Configuration avancée du VPN IPsec 152
Affichage des valeurs par défaut des paramètres de base pour VPN IPsec 153
Configuration des stratégies IKE pour VPN IPsec 153
Configuration des stratégies VPN IPsec 157
Configuration d'un VPN SSL pour un accès à distance à partir d'un navigateur 164
Accédez aux options du VPN SSL 165
Conseils de sécurité pour le VPN SSL 166
Éléments du VPN SSL 166
Étape 1 du scénario : personnalisation de la présentation du portail 167
Étape 2 du scénario : ajouter des utilisateurs du VPN SSL. 170
Création de stratégies VPN SSL 171
Spécifier les ressources réseau pour le VPN SSL 174
Configuration du transfert de port VPN SSL 175
Configuration du client du tunnel VPN SSL 177
Afficher le portail du client VPN SSL 179
Configuration de la protection d'identité VeriSign™ 180
Configuration de la protection d'identité VeriSign 181
Gestion des informations d'identification des utilisateurs du service VeriSign 182

Chapitre 8 : Administration 183

Users 183
Fenêtre Domains 184
Fenêtre Groups 185
Ajouter ou modifier les paramètres utilisateur 186
Ajouter ou modifier les stratégies de connexion utilisateur 187
Microprogramme et configuration 189
Mettre à niveau le microprogramme et travailler avec des fichiers de configuration 189

Gérer le périphérique USB 191
Utiliser le microprogramme secondaire 193
Diagnostics 194
Mesurer et limiter le trafic avec l'utilitaire de contrôle du trafic 195
Configurer les paramètres de date/heure 197
Configurer les options de journalisation 198
Fenêtre Local Logging Config 198
Fenêtre IPV6 Logging 200
Fenêtre Remote Logging Config 201
Fenêtre Logs Facility and Severity 203
Gérer les certificats pour l'authentification 204
Configurer les enregistrements du serveur RADIUS 207
Gestion des licences 208

Chapitre 9 : Gestion du réseau 211

RMON (Gestion à distance) 211
CDP 213
SNMP 214
Fenêtre SNMP 214
Fenêtre SNMP System Info 215
UPnP 216
Bonjour 217
Fenêtre Bonjour Configuration 217
Fenêtre VLAN Association 217

Chapitre 10 : État 219

Page Device Status 219
Page Device Status 220
Page Resource Utilization 222
Page Interface Statistics 222
Page Port Statistics 223
Page Wireless Statistics for the SA520W 224

Page VPN Status 225
Page IPsec VPN Status 225
Page SSL VPN Status 226
Page Quick VPN Status 227
Page Active Users 228
Page View Logs 229
Page View All Logs 229
Page IPsec VPN Logs 231
Page ProtectLink Logs 231
Page CDP Neighbor 232
Page LAN Devices 232
Page Reports 232

Annexe A : Dépannage 234

Connexion Internet 234
Date et heure 237
Effectuer un test ping pour tester la connectivité LAN 237
Restauration des paramètres de la configuration d'usine par défaut 240

Annexe B : Services standard 241

Annexe C : Spécifications techniques et environnementales 244

Annexe D : Paramètres d'usine par défaut 246

Paramètres généraux 246
Paramètres du routeur 248
Paramètres sans fil 251
Stockage 254
Paramètres de sécurité 255

Annexe E : Pour en savoir plus 257

1

Pour commencer

Ce chapitre décrit le routeur SA500 et propose des scénarios pour vous aider à commencer à configurer votre dispositif de sécurité afin de répondre aux besoins de votre entreprise.

- **Présentation des caractéristiques**
- **Options d'installation**
- **Installation du matériel**
- **Mise en route à l'aide de l'utilitaire de configuration**
- **À propos des paramètres par défaut**
- **Tâches de base**
- **Scénarios communs de configuration**

Présentation des caractéristiques

Les fonctions des modèles SA520, SA520W et SA540 sont comparées dans le tableau suivant.

Tableau 1 Comparaison des modèles du dispositif de sécurité de la gamme SA500

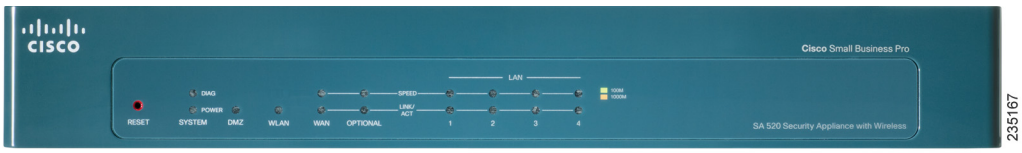
Fonctionnalité	SA520	SA520W	SA540
Performances du pare-feu	200 Mbit/s	200 Mbit/s	300 Mbits/s
UTM	200 Mbit/s	200 Mbit/s	300 Mbits/s

Fonctionnalité	SA520	SA520W	SA540
Performances VPN	65 Mbit/s	65 Mbit/s	85 Mbit/s
Connexions	15 000	15 000	40 000
Ports LAN	4	4	8
Sans fil (802.11n)	Non	Oui	Non
IPsec (nb postes)	Oui (50)	Oui (50)	Oui (100)
SSL (nb postes)	Comprend 2 postes. Avec licence, jusqu'à 25 postes.	Comprend 2 postes. Avec licence, jusqu'à 25 postes.	Compris (50)

Présentation du périphérique

Avant de commencer à utiliser le dispositif de sécurité, familiarisez-vous avec les voyants DEL situés sur le panneau avant et les ports du panneau arrière. Consultez les illustrations et les descriptions suivantes.

Panneau avant



- **Bouton RESET** : pour redémarrer le périphérique de sécurité, appuyez brièvement sur le bouton Reset. Pour restaurer les paramètres d'usine par défaut, maintenez le bouton Reset enfoncé pendant cinq secondes.
- **DEL DIAG** (orange) : lorsque ce voyant DEL est allumé, il indique que le dispositif est en train d'exécuter le diagnostic de mise sous tension. Lorsqu'il est éteint, cela signifie que le périphérique a démarré correctement.

- **DEL POWER** (vert) : lorsque ce voyant DEL est allumé, il indique que le dispositif est sous tension.
- **DEL DMZ** (vert) : lorsque ce voyant DEL est allumé, il indique que le port facultatif est configuré en tant que zone démilitarisée ou zone de démarcation (DMZ) qui autorise les services publics, tels que les serveurs Web, sans exposer votre réseau LAN.
- **DEL SPEED** (vert ou orange) : il indique le débit du trafic pour le port associé. Éteint = 10 Mbits/s, Verte = 100 Mbits/s, Orange = 1 000 Mbits/s.
- **DEL LINK/ACT** (vert) : lorsque ce voyant DEL est allumé, il indique qu'une connexion est établie via le port. Lorsqu'il clignote, cela signifie que le port est actif.
- **DEL WLAN** (vert) : lorsque ce voyant DEL est allumé, il indique que le mode sans fil est activé.
(SA520W).

Panneau arrière

- **Commutateur POWER** : permet d'éteindre ou d'allumer le périphérique de sécurité.
- **Connecteur POWER** : connecte le périphérique de sécurité à l'alimentation à l'aide du câble d'alimentation fourni.
- **Ports LAN** : connectent les ordinateurs et autres périphériques de réseau au dispositif de sécurité. Les modèles SA520 et SA520W ont 4 ports LAN. Le modèle SA540 en a 8.
- **Port OPTIONAL** : peut être configuré en tant que port WAN, LAN ou DMZ. Une DMZ (zone démilitarisée ou zone de démarcation) peut être configurée pour permettre l'accès public aux services tels que des serveurs Web sans exposer votre LAN.
- **Port WAN** : connecte le périphérique de sécurité au DSL, à un modem câble ou à un autre périphérique à connectivité WAN.

- **Port USB** : connecte le périphérique de sécurité à un périphérique USB. Vous pouvez utiliser un périphérique USB pour enregistrer les fichiers de configuration à des fins de sauvegarde et de restauration.

REMARQUE Le panneau arrière du modèle SA520W comprend trois connecteurs filetés pour les antennes

Installation

Cette section vous guide pas-à-pas dans l'installation de votre dispositif de sécurité. Reportez-vous aux rubriques suivantes :

- **Options d'installation, page 13**
- **Installation du matériel, page 16**

Options d'installation

Vous pouvez installer votre périphérique de sécurité sur un bureau, le monter sur un mur ou dans un bâti.

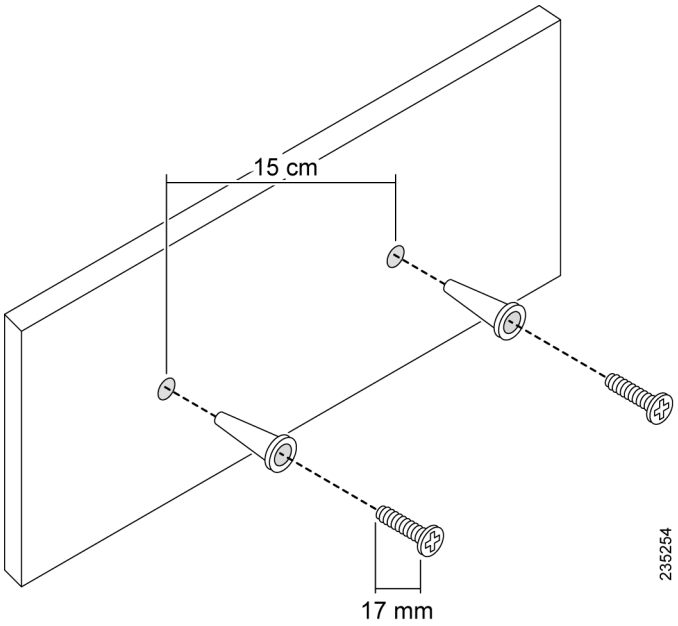
Choix de l'emplacement

- **Température ambiante :** pour éviter tout risque de surchauffe du périphérique de sécurité, ne l'utilisez pas dans les lieux où la température ambiante dépasse 40 °C (104 °F).
- **Circulation de l'air :** assurez-vous que la circulation de l'air est suffisante autour du périphérique.
- **Charge mécanique :** assurez-vous que le périphérique de sécurité est à bon niveau et stable, afin d'éviter tout danger.

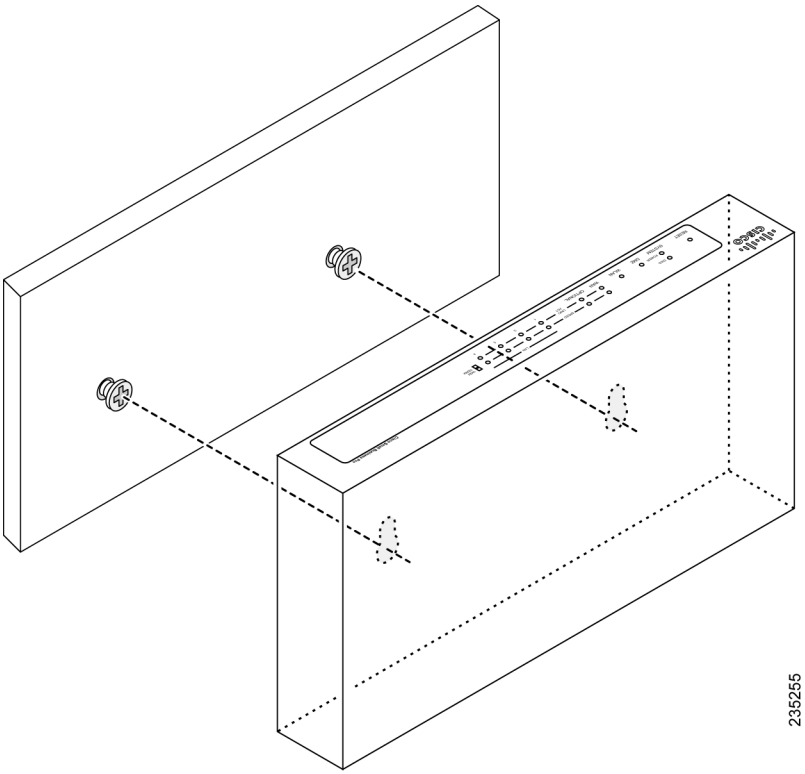
Pour monter le périphérique de sécurité sur un bureau, installez les quatre pieds en caoutchouc (fournis) sur la partie inférieure du périphérique de sécurité. Placez le périphérique sur une surface plane.

Montage mural

ÉTAPE 1 Insérez deux vis de 17 mm, avec les fixations, dans le mur en les plaçant à 15 cm (environ 5,9 pouces) l'une de l'autre. Laissez la tête exposée sur 3-4 mm (environ 1/8 pouce).



ÉTAPE 2 Positionnez l'unité de sorte que les orifices de montage mural recouvrent les deux vis. Faites glisser l'unité vers le bas jusqu'à ce que les vis s'ajustent parfaitement dans les orifices de montage mural.



Montage sur bâti

Vous pouvez monter le périphérique de sécurité dans un bâti de taille standard d'environ 48 cm (19 pouces) de largeur. Chaque périphérique de sécurité nécessite un espace de 1 RU (rack unit, unité de bâti), ce qui correspond à une hauteur de 44,45 mm (1,75 pouce).

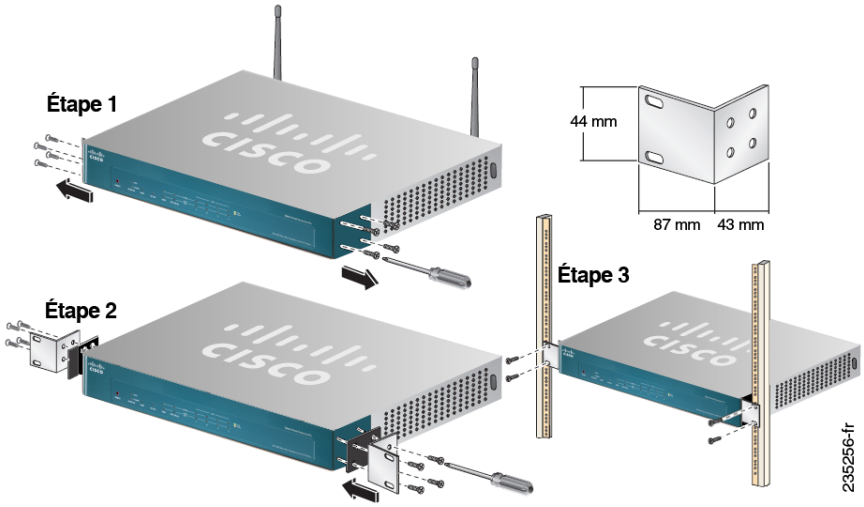
AVERTISSEMENT Lorsque vous installez plusieurs appareils dans un bâti, évitez de surcharger la prise ou le circuit électrique.

ÉTAPE 1 Retirez les quatre vis de chaque côté du périphérique de sécurité.

ÉTAPE 2 Placez l'une des entretoises fournies sur le côté du périphérique de sécurité en veillant à ce que les quatre orifices soient alignés sur les trous de vis. Placez ensuite une plaque de montage sur bâti à côté de l'entretoise et réinstallez les vis.

REMARQUE Si les vis sont trop courtes et que vous ne parvenez pas à fixer la plaque de montage avec l'entretoise, enlevez l'entretoise et fixez la plaque de montage directement sur le boîtier.

ÉTAPE 3 Installez le périphérique de sécurité dans un bâti standard comme illustré.



Installation du matériel

Pour connecter l'équipement, procédez comme suit :

ÉTAPE 1 Connectez le périphérique de sécurité à l'alimentation.

ÉTAPE 2 Pour installer le modèle SA520W, vissez chaque antenne sur un connecteur fileté situé sur le panneau arrière. Orientez chaque antenne vers le haut.

ÉTAPE 3 Pour le DSL, un modem câble ou tout autre périphérique à connectivité WAN, connectez un câble réseau Ethernet du périphérique au port WAN situé sur le panneau arrière. Cisco recommande vivement l'utilisation d'un câble Cat5e ou un cable de qualité supérieure.

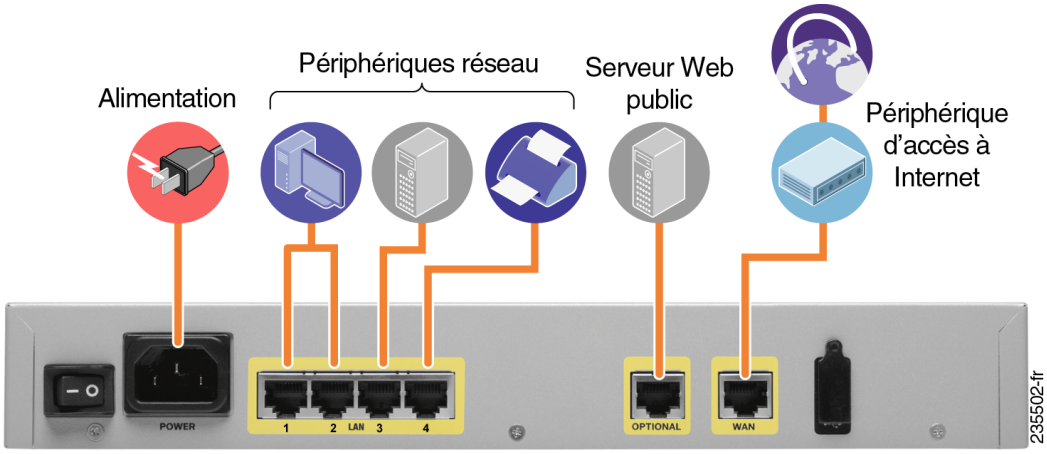
ÉTAPE 4 Pour les périphériques réseau, connectez un câble réseau Ethernet du périphérique réseau à l'un des ports LAN dédiés sur le panneau arrière.

ÉTAPE 5 Si vous utilisez une UC 500, reliez un câble réseau Ethernet du port WAN de l'UC 500 à un port LAN disponible sur le dispositif de sécurité.

ÉTAPE 6 Mettez le périphérique de sécurité sous tension.

ÉTAPE 7 Mettez sous tension les périphériques connectés. Chaque voyant DEL s'allume pour indiquer une connexion active.

Un exemple de configuration est illustré ci-dessous.



Félicitations ! L'installation du périphérique de sécurité est maintenant terminée.

Mise en route à l'aide de l'utilitaire de configuration

La page Web de l'utilitaire de configuration est un gestionnaire de périphériques basé sur le Web utilisé pour mettre en service les périphériques de sécurité de la gamme SA500. Pour utiliser le dispositif, vous devez pouvoir vous connecter aux périphériques de sécurité de la gamme SA500 de votre PC ou ordinateur portable d'administration. Vous pouvez accéder au dispositif de sécurité à l'aide de n'importe quel navigateur Web (tel que Microsoft Internet Explorer ou Mozilla Firefox).

Connexion au dispositif de configuration

ÉTAPE 1 Connectez votre ordinateur à un port LAN disponible sur le panneau arrière du dispositif de sécurité.

ÉTAPE 2 Lancez un navigateur Web, puis saisissez l'adresse suivante : **192.168.75.1**

Cette adresse est l'adresse LAN des paramètres d'usine du dispositif de sécurité. Si vous modifiez ce paramètre dans la configuration LAN, vous devez saisir la nouvelle adresse IP pour vous connecter à l'utilitaire de configuration.

ÉTAPE 3 Lorsque la boîte de dialogue Security Alert apparaît, acceptez ou installez le certificat :

- **Internet Explorer :** cliquez sur **Oui** pour continuer ou sur **Afficher le certificat** pour afficher les détails. Sur la page Certificat, cliquez sur **Installer le certificat**. Suivez les instructions fournies par l'assistant pour effectuer l'installation.
- **Firefox :** cliquez sur le lien pour ajouter une exception. Cliquez sur le bouton **Ajouter l'exception**. Cliquez sur **Obtenir le certificat** puis sur **Confirmer l'exception de sécurité**.
- **Safari :** cliquez sur **Continuer** pour continuer ou sur **Afficher le certificat**. Sur la page Certificat, cliquez sur **Installer le certificat**. Suivez les instructions fournies par l'assistant pour effectuer l'installation.

ÉTAPE 4 Saisissez le nom d'utilisateur par défaut et le mot de passe :

- Nom d'utilisateur : **cisco**
- Mot de passe : **cisco**

ÉTAPE 5 Cliquez sur **Log In**. La fenêtre Getting Started (Basic) s'ouvre. Pour plus d'informations, voir **Utilisation des pages de la section Getting Started, page 19**.

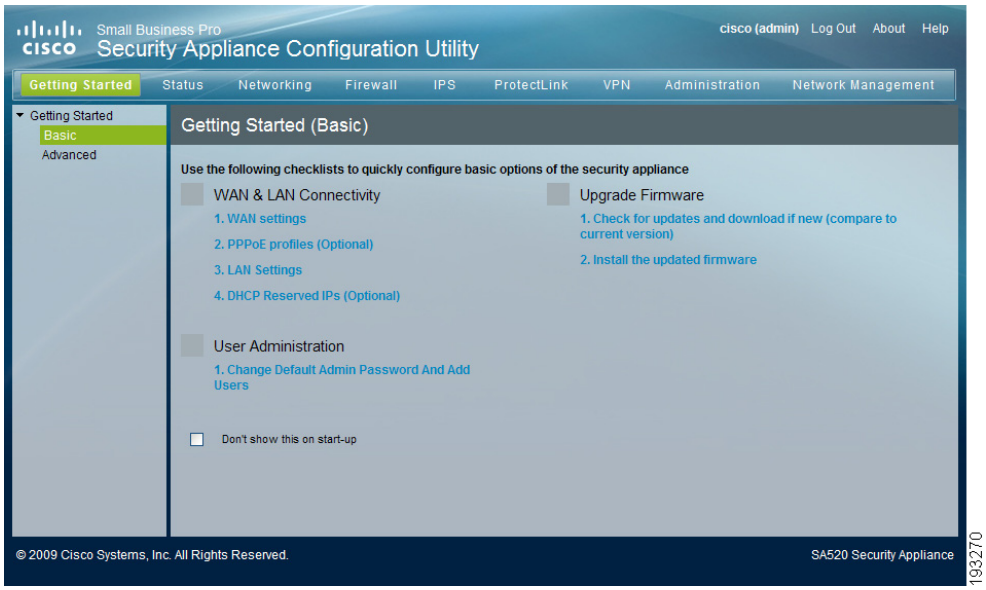
REMARQUE Si vous utilisez le dispositif de sécurité avec un périphérique prenant en charge le CCA (Cisco Configuration Assistant), comme l'UC 500, vous pouvez utiliser le CCA (Cisco Configuration Assistant) pour lancer l'utilitaire de configuration. Pour plus d'informations sur le CCA, voir : www.cisco.com/go/configassist.

Utilisation des pages de la section Getting Started

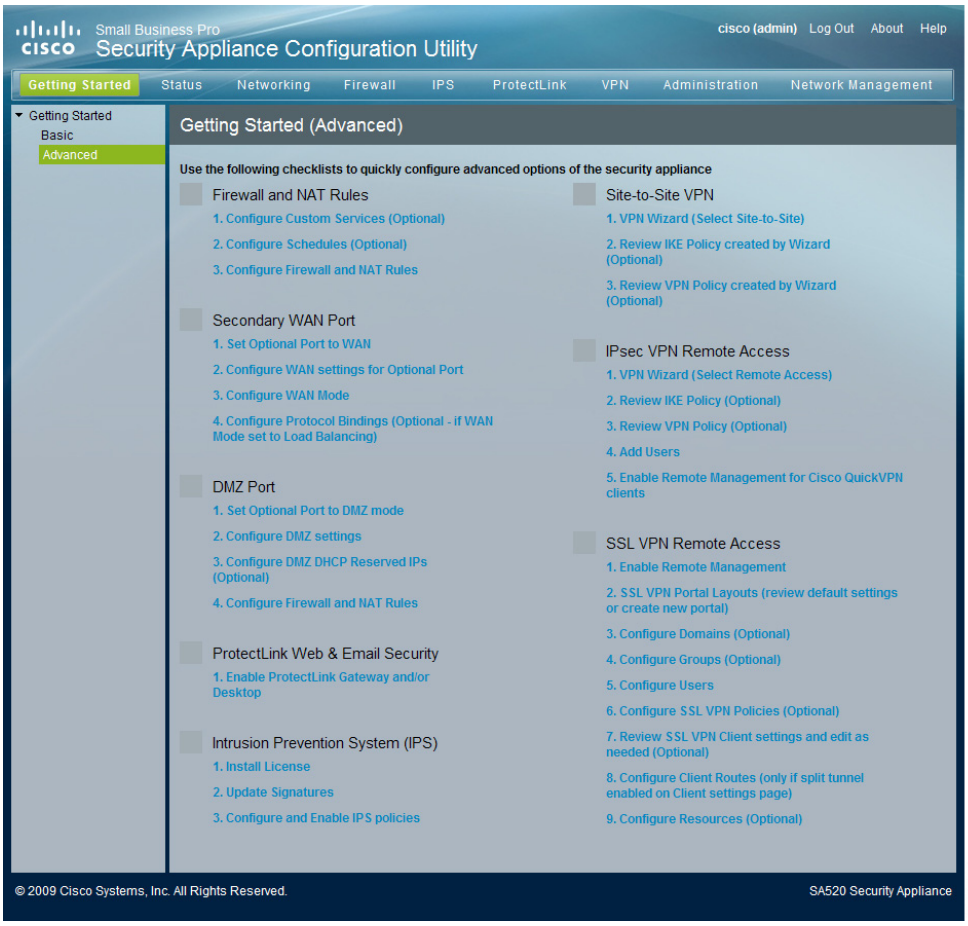
Les pages de mise en route proposent une aide pour l'utilisation des tâches de configuration courantes.

- Trouvez une tâche que vous devez effectuer, puis cliquez sur un lien pour commencer. Suivez les liens énumérés.
- Pour obtenir de l'aide sur les tâches de configuration avancée, telles que la configuration du pare-feu/NAT, la configuration WAN facultative, la configuration DMZ et la configuration VPN, cliquez sur le lien **Getting Started > Advanced** dans le volet de navigation, puis cliquez sur les liens correspondant aux tâches que vous voulez exécuter.
- Pour revenir sur la page Getting Started (Basic) à tout moment, cliquez sur le bouton **Getting Started** dans la barre de menu.
- Pour éviter l'affichage automatique de la page Getting Started (Basic) lorsque vous vous connectez, cochez la case **Don't show this on start-up**.

Page Getting Started (Basic)



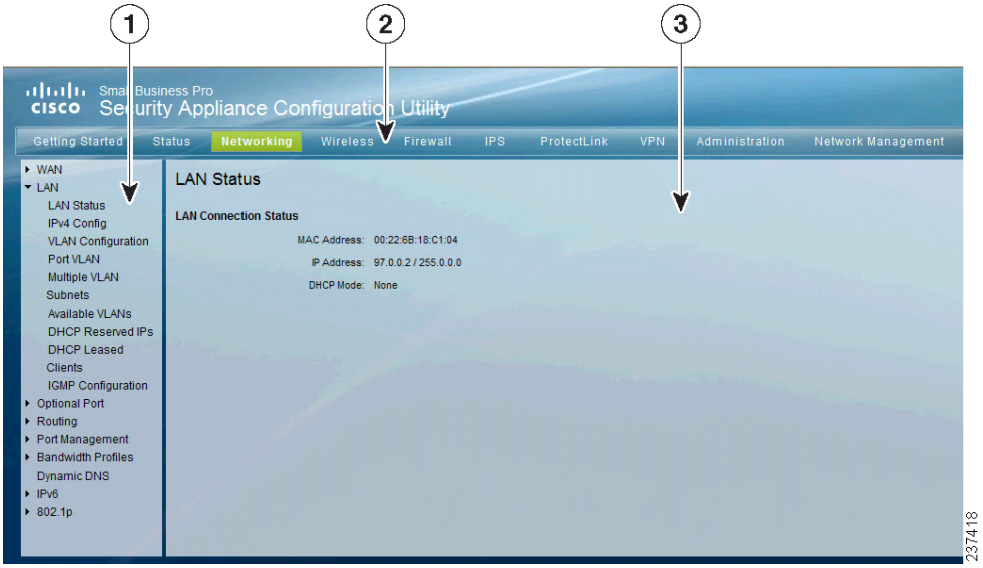
Page Getting Started (Advanced)



Naviguer à travers le dispositif de configuration

Utilisez la barre de menu et le volet de navigation pour effectuer des tâches dans l'utilitaire de configuration.

Barre de menu et volet de navigation



Numéro	Composant	Description
1	Barre de menu	Contient les principales catégories de fonctions. Cliquez sur un élément de menu pour passer à une autre catégorie.
2	Volet de navigation	Permet de passer facilement d'une fonctionnalité configurable du périphérique à une autre. Les branches principales se développent pour afficher les fonctionnalités secondaires. Cliquez sur le triangle en regard du titre de la branche principale pour développer ou réduire son contenu. Cliquez sur le titre d'une fonctionnalité ou d'une fonctionnalité secondaire pour l'ouvrir.
3	Contenu principal	Le contenu principal de la fonctionnalité apparaît dans cette zone.

Utilisation du système d'aide

L'utilitaire de configuration comporte des fichiers d'aide détaillant chaque tâche de configuration. Pour afficher une page d'aide, cliquez sur le lien **Help** (Aide) dans l'angle supérieur droit de la fenêtre. Une nouvelle fenêtre s'ouvre avec des informations sur la page que vous consultez actuellement.

À propos des paramètres par défaut

Les périphériques de sécurité de la gamme SA500 sont pré-configurés avec des paramètres qui vous permettent de commencer à utiliser le périphérique avec un minimum de modifications. Selon les exigences de votre fournisseur de services Internet (ISP) et les besoins de votre entreprise, vous serez peut-être amené à modifier certains paramètres. Vous pouvez utiliser l'utilitaire de configuration pour personnaliser tous les paramètres, si nécessaire.

Les paramètres d'intérêt particulier sont décrits ci-dessous. Pour obtenir une liste complète de tous les paramètres d'usine par défaut, voir **Annexe D, « Paramètres d'usine par défaut ».**

- **Adressage IPv4 :** par défaut, le dispositif de sécurité est en mode IPv4 uniquement. Si vous souhaitez utiliser l'adressage IPv6, activez le mode IPv6 et configurez ensuite votre WAN IPv6 et votre LAN IPv6. Voir **Configuration de l'adressage IPv6, page 80**
- **Configuration WAN :** par défaut, le dispositif de sécurité est configuré pour recevoir une adresse IP de votre ISP par l'intermédiaire du protocole DHCP (Dynamic Host Configuration Protocol). Si votre ISP a attribué une adresse IP statique, vous devrez la configurer. Par ailleurs, si votre ISP demande une connexion à chaque fois que vous vous connectez à Internet, vous devez saisir les informations de compte. Vous pouvez également modifier les autres paramètres WAN. Pour plus d'informations, voir **Scénario 1 : configuration de base du réseau avec accès Internet, page 26**
- **Configuration LAN :** par défaut, l'interface LAN agit en tant que serveur DHCP pour tous les périphériques connectés. Pour la plupart des scénarios de déploiement, les paramètres DHCP et TCP/IP du dispositif de sécurité doivent être satisfaisants. Vous pouvez toutefois modifier l'adresse de sous-réseau ou l'adresse IP par défaut du dispositif de sécurité. Vous pouvez attribuer des adresses IP statiques aux périphériques connectés plutôt que de permettre au dispositif de sécurité d'agir en tant que serveur DHCP. Pour plus d'informations, voir **Scénario 1 : configuration de base du réseau avec accès Internet, page 26**

- **Port facultatif :** ce port est prédéfini pour agir en tant que port WAN secondaire. Vous pouvez également configurer le port facultatif pour une utilisation en tant que port DMZ ou que port LAN supplémentaire. Voir **Scénario 1 : configuration de base du réseau avec accès Internet, page 26** ou **Scénario 7 : DMZ pour sites Web et services publics, page 31**.
- **Réseau sans fil (SA520W uniquement) :** le SA520W est configuré avec un point d'accès appelé AP1, dont le nom de réseau par défaut est Cisco_1. Le point d'accès est activé par défaut. Le profil de sécurité a la sécurité ouverte et s'identifie à tous les périphériques sans fil qui sont dans la plage. Ces paramètres facilitent l'utilisation de votre réseau sans fil. Cependant, pour des raisons de sécurité, nous vous recommandons vivement de configurer le profil avec les paramètres de sécurité appropriés. Voir **Scénario 10 : réseau sans fil, page 36**.
- **Accès administratif :** vous pouvez accéder à l'utilitaire de configuration à l'aide d'un navigateur Web et saisir l'adresse IP par défaut 192.168.75.1. Vous pouvez ouvrir une session en entrant *cisco* comme nom d'utilisateur et *cisco* comme mot de passe. Nous vous recommandons vivement de modifier le nom et le mot de passe par défaut. Vous pouvez également modifier le paramètre de délai d'inactivité par défaut. Le paramètre par défaut nécessite de se reconnecter après 10 minutes d'inactivité. Pour plus d'informations sur ces paramètres, voir **Modifier le nom d'utilisateur et le mot de passe par défaut, page 23**.

Tâches de base

Nous vous recommandons vivement de terminer les tâches de base suivantes avant de commencer à configurer votre dispositif de sécurité.

Modifier le nom d'utilisateur et le mot de passe par défaut

Pour empêcher tout accès non-autorisé, modifiez immédiatement le nom d'utilisateur et le mot de passe du compte administrateur par défaut.

ÉTAPE 1 Dans la section **User Administration** de la page Getting Started (Basic), cliquez sur **Change Default Admin Password And Add Users**.

La fenêtre Users s'ouvre.

ÉTAPE 2 Dans la première ligne du tableau, repérez le compte administrateur par défaut.

ÉTAPE 3 Cliquez sur le bouton dans la colonne **Edit**. La fenêtre User Configuration s'ouvre, affichant les informations par défaut.

ÉTAPE 4 Saisissez les informations suivantes :

- **User Name :** saisissez un identifiant unique pour l'utilisateur. Il peut inclure tous les caractères alphanumériques.
- **First Name :** saisissez le prénom de l'utilisateur.
- **Name :** entrez le nom de l'utilisateur.

  Vous ne pouvez pas modifier le **Type d'utilisateur** ni le **Groupe** pour ce compte.
- **Check to Edit Password :** cochez cette case pour activer les champs de mot de passe.
- **Enter Your Password :** saisissez le mot de passe actuel. Le mot de passe par défaut pour ce nouveau dispositif de sécurité est **cisco**.
- **New Password :** saisissez un mot de passe comportant des caractères alphanumériques, ainsi que les caractères '—' ou '_'.
- **Confirm Password :** saisissez à nouveau le mot de passe.
- **Idle Timeout :** saisissez la durée en minutes pendant laquelle l'utilisateur peut être inactif avant que la session n'expire. Vous pouvez saisir toute valeur comprise entre 0 et 999.

ÉTAPE 5 Cliquez sur **Apply** pour enregistrer les paramètres.

Sauvegarde de la configuration

Vous pouvez, à tout moment du processus, sauvegarder votre configuration. Si vous apportez ultérieurement des modifications que vous souhaitez abandonner, vous pouvez facilement revenir à une configuration sauvegardée. Pour plus d'informations, voir **Mettre à niveau le microprogramme et travailler avec des fichiers de configuration, page 189**.

Mise à jour du microprogramme

Avant d'exécuter une autre tâche, vous devez mettre le microprogramme à niveau afin de vous assurer d'utiliser la version la plus récente. Vous pouvez effectuer la mise à niveau à partir d'un fichier stocké sur votre ordinateur, du réseau ou d'une clé USB.

ÉTAPE 1 Dans la section **Upgrade Firmware** de la page Getting Started (Basic), cliquez sur le lien : **Check for updates and download if new**

ÉTAPE 2 Lous trouverez aussi le nouveau microprogramme pour leelle.

ÉTAPE 3 Dans la section **Upgrade Firmware** de la page Getting Started (Basic), cliquez sur le lien **Install the updated firmware**.

La fenêtre Firmware & Configuration (Network) s'ouvre.

ÉTAPE 4 Dans la zone **Firmware Upgrade**, cliquez sur **Browse**. Recherchez le fichier que vous avez téléchargé.

ÉTAPE 5 Cliquez sur **Upload**.

REMARQUE patientez pendant la mise à niveau du microprogramme.
1. Ne fermez PAS la fenêtre du navigateur.
2. N'allez PAS en ligne.
3. N'arrêtez ni ne redémarrez PAS le routeur.
4. N'arrêtez PAS l'ordinateur.

La mise à niveau du routeur peut prendre plusieurs minutes. Lorsque la mise à niveau est en cours, le voyant DEL de test, sur le panneau avant du routeur, est allumé. Lorsque la mise à niveau est terminée, le routeur redémarre automatiquement.

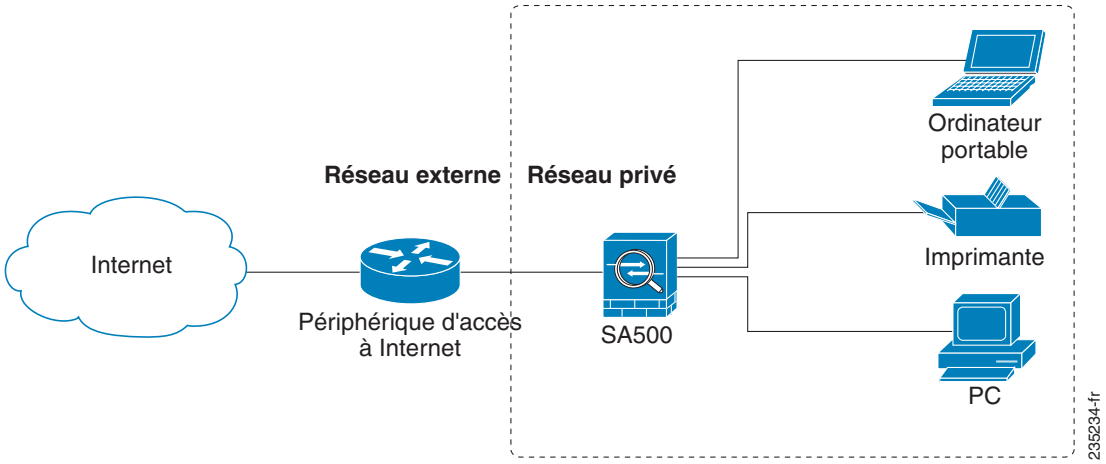
Scénarios communs de configuration

Vous pouvez déployer les périphériques de sécurité de la gamme SA500 pour résoudre les problèmes de sécurité de votre entreprise. Lorsque vous commencez à utiliser votre dispositif de sécurité, tenez compte des scénarios de configuration suivants :

- **Scénario 1 : configuration de base du réseau avec accès Internet, page 26**

- Scénario 8 : configuration du système de communications Cisco Smart Business, page 29
- Scénario 7 : DMZ pour sites Web et services publics, page 31
- Scénario 6 : pare-feu pour le contrôle du trafic entrant et sortant, page 30
- Scénario 9 : réseau de site à site et accès à distance, page 32
- Scénario 10 : réseau sans fil, page 36

Scénario 1 : configuration de base du réseau avec accès Internet



Dans un déploiement de base pour une petite entreprise, le dispositif de sécurité permet la communication entre les périphériques sur le réseau privé et permet également aux ordinateurs d'accéder à Internet. Avec les paramètres par défaut, le dispositif de sécurité obtient son adresse WAN de manière dynamique auprès de l'ISP. Tous les périphériques sur le LAN reçoivent leurs adresses IP de manière dynamique du dispositif de sécurité. Tous les périphériques disposent d'un accès Internet, mais aucun trafic entrant n'est autorisé entre Internet et les périphériques LAN.

Tâches de configuration pour ce scénario :

La configuration par défaut est suffisante pour la plupart des petites entreprises et vous pouvez ne pas avoir à modifier les paramètres WAN ou LAN. Cependant, selon les exigences de votre fournisseur d'accès Internet, ainsi vos préférences pour votre configuration LAN, vous pouvez apporter des modifications, si nécessaire.

REMARQUE Avant de configurer votre réseau, assurez-vous d'avoir mis le microprogramme à niveau (voir **Mise à jour du microprogramme, page 25**) et d'avoir modifié le mot de passe par défaut de l'administrateur (voir **Modifier le nom d'utilisateur et le mot de passe par défaut, page 23**).

Tenez compte des premières étapes suivantes :

1. Vérifiez la configuration WAN et apportez toutes les modifications nécessaires pour configurer votre connexion Internet.

   Dans la section **WAN & LAN Connectivity** de la page Getting Started (Basic), cliquez sur le lien **WAN settings**. Pour plus d'informations, voir **Configuration de la connexion WAN, page 37**.

2. Vérifiez la configuration LAN et apportez toutes les modifications nécessaires pour prendre en charge votre réseau. Les paramètres DHCP et TCP/IP par défaut sont, dans la plupart des cas, satisfaisants. Vous pouvez toutefois modifier l'adresse du sous-réseau ou l'adresse IP par défaut ou attribuer des adresses IP statiques à vos périphériques.

   Dans la section **WAN & LAN Connectivity** de la page Getting Started (Basic), cliquez sur le lien **WAN settings**. Pour plus d'informations, voir **Configuration de la zone LAN, page 43**.

3. Si vous pensez utiliser votre dispositif de sécurité avec le système de communications Cisco Smart Business (SBCS), installez et configurez votre UC 500.

   Voir **Scénario 8 : configuration du système de communications Cisco Smart Business, page 29**.

4. Envisagez votre utilisation du port facultatif :

   - Si vous devez héberger des services publics, comme des sites Web, vous avez besoin d'une DMZ. Pour plus d'informations, voir **Scénario 7 : DMZ pour sites Web et services publics, page 31**. Pour plus d'informations sur l'utilisation du port facultatif en tant que port LAN supplémentaire, voir **Configuration du port facultatif comme port LAN, page 55**.

   - Si vous disposez de deux liaisons ISP et n'avez pas besoin d'une DMZ, vous pouvez utiliser le port facultatif comme port WAN secondaire pour fournir

une connectivité de sauvegarde ou un équilibrage de charge. Pour configurer le port, utilisez les liens de la section **Secondary WAN Port** de la page Getting Started (Advanced). Pour plus d'informations, voir **Configuration du WAN facultatif, page 55**.

- Si vous n'avez pas besoin de DMZ ou de WAN secondaire, vous pouvez utiliser le port facultatif en tant que port LAN supplémentaire. Pour plus d'informations, voir **Configuration du port facultatif comme port LAN, page 55**.

5. Si vous souhaitez autoriser l'accès entrant depuis Internet ou restreindre certains types de trafic sortant vers Internet, configurez vos règles de pare-feu.

   Voir **Scénario 6 : pare-feu pour le contrôle du trafic entrant et sortant, page 30**.

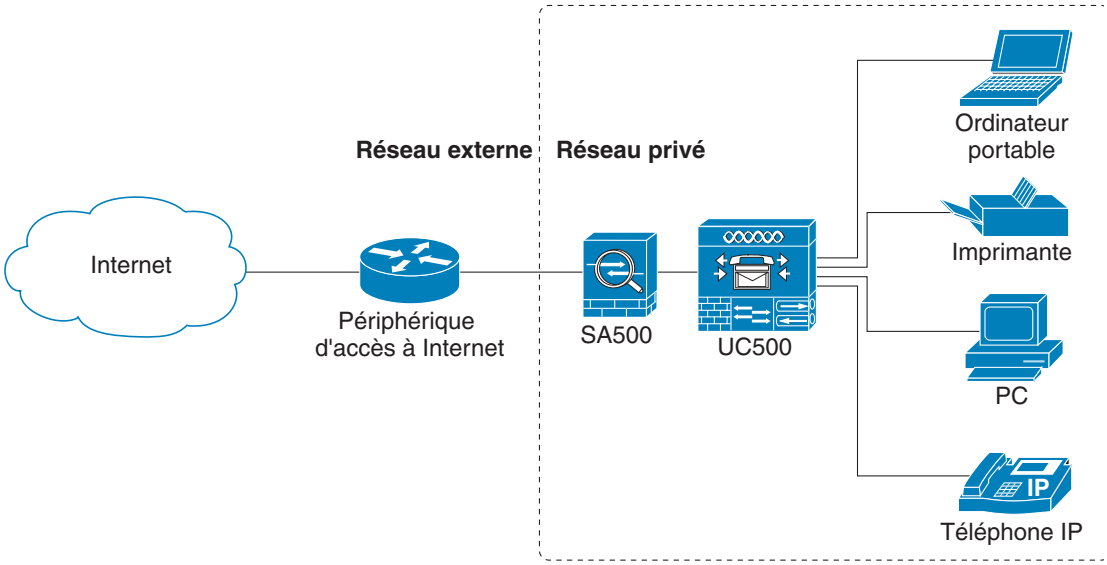
6. Demandez-vous si vous devez autoriser l'accès à votre réseau à partir de sites distants ou pour des télétravailleurs.

   Voir **Scénario 9 : réseau de site à site et accès à distance, page 32**.

7. Demandez-vous si vous devez activer des fonctionnalités telles que la journalisation ou l'accès à distance à l'utilitaire de configuration. Voir **Configurer les options de journalisation, page 198** et **RMON (Gestion à distance), page 211**.

Scénario 8 : configuration du système de communications Cisco Smart Business

Vous pouvez utiliser le dispositif de sécurité pour protéger votre réseau du système de communications Cisco Smart Business.



Tâches de configuration pour ce scénario :

1. Configurez les paramètres WAN et LAN pour votre dispositif de sécurité, comme nécessaire. Voir **Scénario 1 : configuration de base du réseau avec accès Internet, page 26**

2. Connectez un câble du port WAN de l'UC 500 à un port LAN disponible sur le dispositif de sécurité.

   Avec la configuration par défaut, le dispositif de sécurité fait office de serveur DCHP qui attribue les adresses IP de la plage 192.168.75.x. Les téléphones IP se voient attribuer des adresses IP sur une plage d'adresses 10.1.1.x/24.

3. Si vous voulez affecter une adresse IP statique à l'UC 500 ou à un autre périphérique LAN, cliquez sur le lien **DHCP Reserved IPs** sous **WAN & LAN Connectivity** sur la page Getting Started (Basic). Pour plus d'informations, voir **IP DHCP réservées, page 53**.

4. Configurez un routage IP statique entre le dispositif de sécurité et les données VLAN de l'UC 500 (192.168.10.x). Pour plus d'informations, voir **Routage statique, page 71**.

5. Le dispositif de sécurité fournissant le pare-feu, la traduction d'adresses de réseau (NAT), et la passerelle de couche applicative SIP (SIP-ALG) de votre réseau, désactivez ces fonctionnalités sur l'UC 500. Pour toute instruction, reportez-vous à la documentation ou l'aide en ligne du CCA (Cisco Configuration Assistant).

Scénario 6 : pare-feu pour le contrôle du trafic entrant et sortant

Par défaut, le trafic sortant est autorisé et tout trafic entrant est rejeté. Si vous souhaitez rejeter un trafic sortant ou autoriser un trafic entrant, vous devez configurer une règle de pare-feu. Pour empêcher tout trafic indésirable d'Internet et vous assurer que vos employés utilisent Internet à des fins professionnelles agréés, vous pouvez configurer différents niveaux de règles de pare-feu. Vous pouvez configurer des règles s'appliquant à une adresse IP spécifiée, une plage d'adresses IP ou à chacun de manière globale.

Prenons les exemples de règles de pare-feu suivants :

- Bloquer le trafic sortant vers certains sites Web
- Restreindre l'accès Internet pour certains utilisateurs
- Autoriser le trafic entrant de votre DMZ
- Configurer le routage avancé NAT

Pour ces scénarios et toutes les situations dans lesquelles vous avez besoin d'une exception à la stratégie de pare-feu par défaut, vous devez configurer des stratégies de pare-feu.

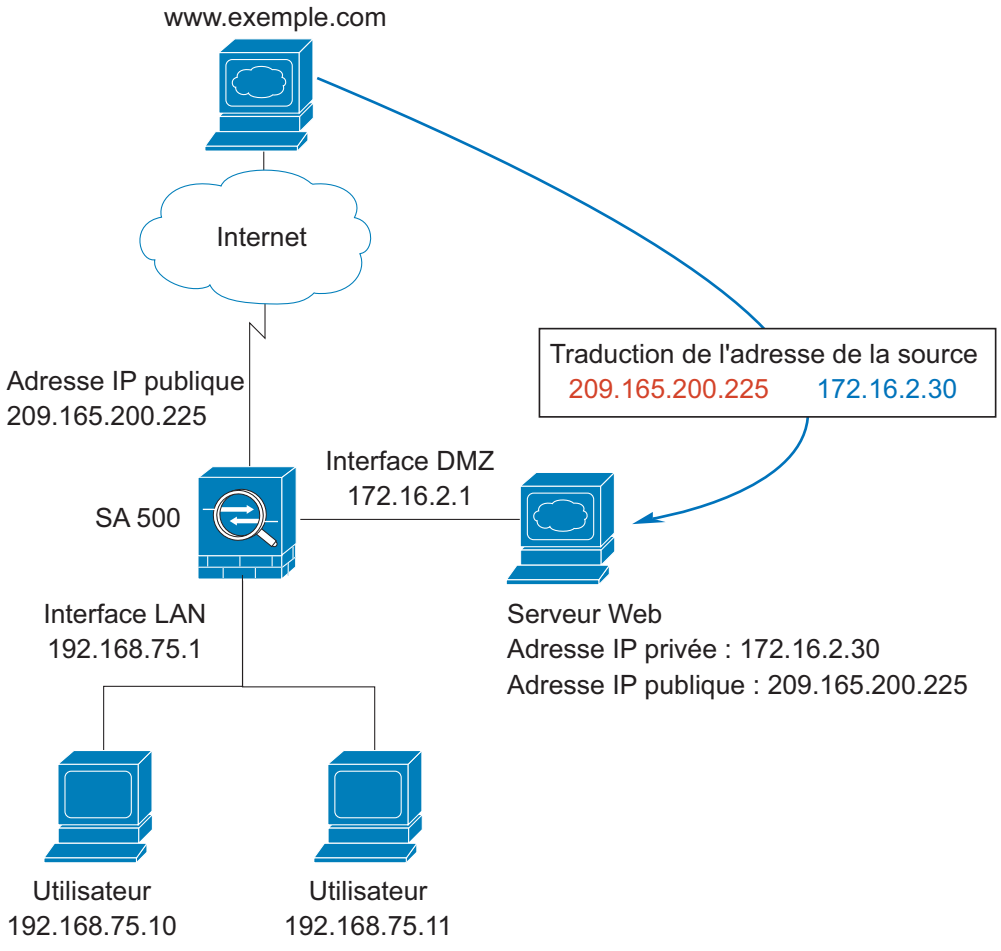
REMARQUE Les paramètres WAN et LAN par défaut peuvent être suffisants pour votre déploiement, mais vous devez tenir compte des étapes décrites dans le **Scénario 1 : configuration de base du réseau avec accès Internet, page 26**

Tâches de configuration pour ce scénario :

Pour commencer à configurer les règles de pare-feu, utilisez les liens **Firewall and NAT Rules** sur la page Getting Started (Advanced). Pour plus d'informations, voir **Configuration des règles de pare-feu pour contrôler le trafic entrant et sortant, page 107**.

Scénario 7 : DMZ pour sites Web et services publics

Si votre entreprise héberge des services publics tels que les sites Web, vous avez besoin d'un moyen d'autoriser l'accès à ces services sans exposer votre réseau LAN. Vous pouvez résoudre ce problème en configurant le port facultatif du dispositif de sécurité afin d'utiliser une DMZ (zone de démarcation ou zone démilitarisée). Cette zone agit comme un réseau distinct entre le réseau local privé et Internet. Après avoir configuré votre DMZ, vous pouvez configurer les règles de pare-feu autorisant le trafic à se connecter uniquement pour les services que vous spécifiez.



REMARQUE Les paramètres WAN et LAN par défaut peuvent être suffisants pour votre déploiement, mais vous devez tenir compte des étapes décrites dans le **Scénario 1 : configuration de base du réseau avec accès Internet, page 26**

Tâches de configuration pour ce scénario :

Pour commencer à configurer une DMZ, utilisez les liens dans la section **DMZ Port** de la page Getting Started (Advanced). Pour plus d'informations, voir **Configuration d'un DMZ, page 64**.

Scénario 8 : configuration de ProtectLink Web et de la sécurité de la messagerie

Pour une protection supplémentaire contre les menaces du Web et de messagerie électronique, le dispositif de sécurité prend en charge les services Cisco ProtectLink Security. À l'aide de ces services, votre réseau est protégé des menaces liées à l'utilisation de la messagerie électronique dans le « nuage » Internet et des menaces Web dans le dispositif de sécurité Cisco, proposant un accès uniquement à la messagerie électronique et aux sites Web appropriés pour votre entreprise.

Tâches de configuration pour ce scénario :

Dans la section **ProtectLink Web & Email Security** de la page Getting Started (Advanced), cliquez sur **Enable ProtectLink Gateway** et/ou **Endpoint**. La fenêtre ProtectLink s'ouvre. Pour plus d'informations, voir **Chapitre 6, « Utilisation des services Cisco ProtectLink Security ».**

Scénario 9 : réseau de site à site et accès à distance

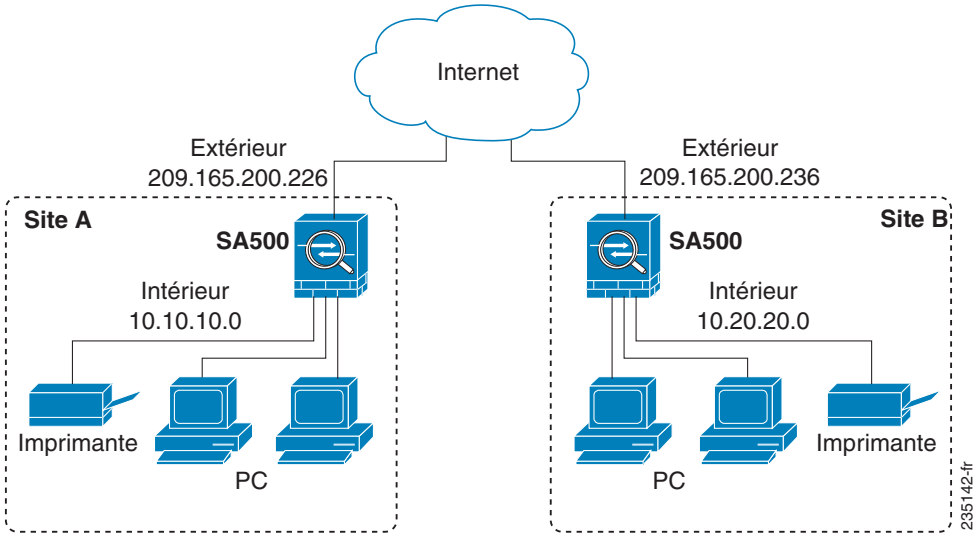
Vous pouvez configurer un réseau privé virtuel (VPN) pour étendre votre réseau à d'autres sites ou pour autoriser des partenaires commerciaux et des télétravailleurs à accéder aux applications et aux ressources du réseau.

Vous pouvez configurer les types de VPN suivants :

- VPN IPsec pour un tunnel de site à site
- VPN IPsec pour un accès à distance avec un client VPN
- VPN SSL pour un accès à distance à l'aide d'un navigateur Web

VPN IPsec pour un VPN de site à site

Pour un VPN de site à site, vous pouvez configurer un tunnel IPsec à l'aide du cryptage avancé afin de maintenir la sécurité réseau.

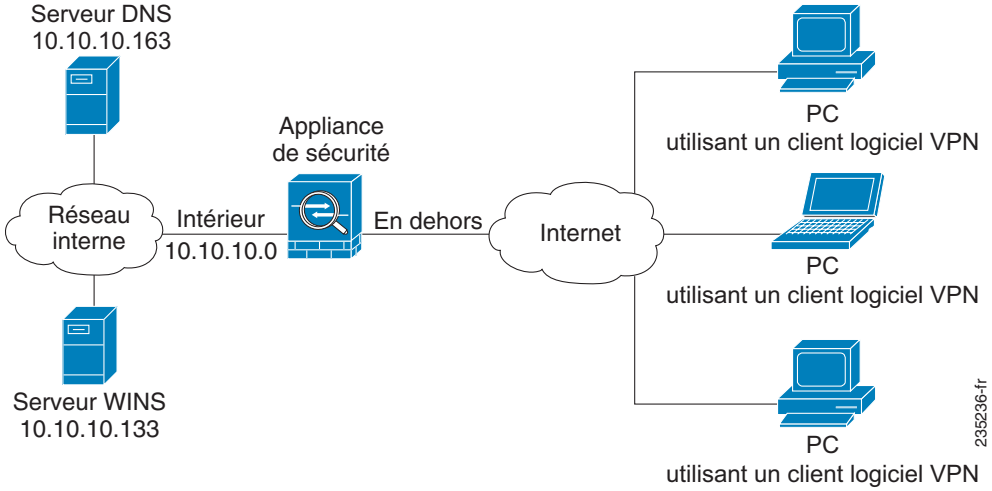


Tâches de configuration pour ce scénario :

Dans la section **Site-to-Site VPN** de la page Getting Started (Advanced), cliquez sur le lien **VPN Wizard**. Lorsque l'assistant VPN s'affiche, sélectionnez l'option **Site-to-Site** et saisissez les autres paramètres. Vous pouvez aussi utiliser les autres liens de la page Getting Started (Advanced) pour vérifier et modifier les stratégies créées par l'assistant. Pour plus d'informations, voir **Configuration d'un tunnel VPN IPsec d'accès à distance avec un client VPN, page 148**.

Accès à distance VPN IPsec avec un client VPN

Pour l'accès à distance par des utilisateurs ayant un client VPN IPsec sur leur PC, vous pouvez configurer un tunnel de client VPN IPsec pour un accès sécurisé. Cette option nécessite d'installer et de maintenir le logiciel client VPN pour ces sites et utilisateurs distants.

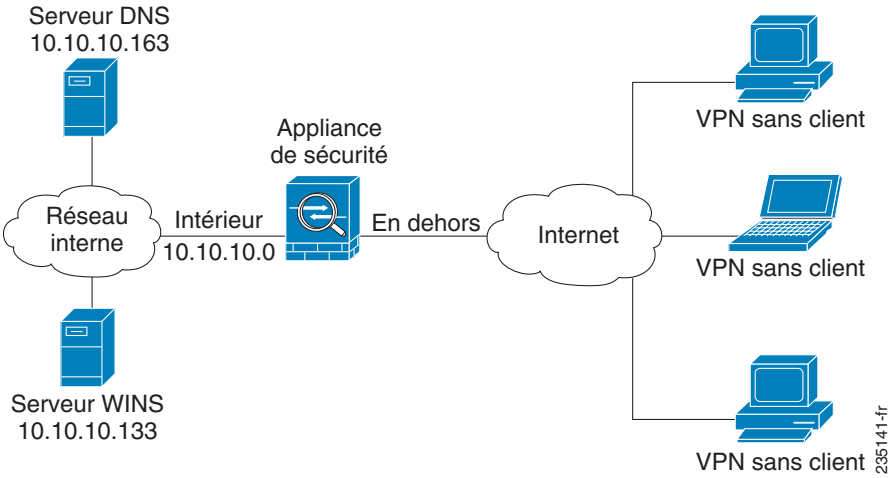


Tâches de configuration pour ce scénario :

Dans la section **IPsec VPN Remote Access** de la page Getting Started (Advanced), cliquez sur le lien **VPN Wizard**. Lorsque l'assistant VPN s'affiche, sélectionnez l'option **Remote Access** et renseignez les champs de la page. Revenez sur la page Getting Started (Advanced) et cliquez sur **Add Users** pour ajouter vos utilisateurs VPN. Vous pouvez aussi utiliser les autres liens de la page Getting Started (Advanced) pour vérifier et modifier les stratégies créées par l'assistant. Pour plus d'informations, voir **Configuration d'un tunnel VPN IPsec d'accès à distance avec un client VPN, page 148**.

Accès à distance VPN SSL avec un navigateur Web

Pour l'accès à distance par des utilisateurs n'ayant aucun logiciel particulier sur leur PC, tel que des sous-traitants ayant besoin d'un accès à certaines ou à toutes vos ressources réseau, le VPN SSL représente un moyen souple et sécurisé d'étendre vos ressources réseau. Vous n'êtes responsable d'aucun logiciel client VPN, le tunnel VPN étant accessible par tous avec un navigateur Web, un accès Internet et les informations d'identification de connexion appropriées.

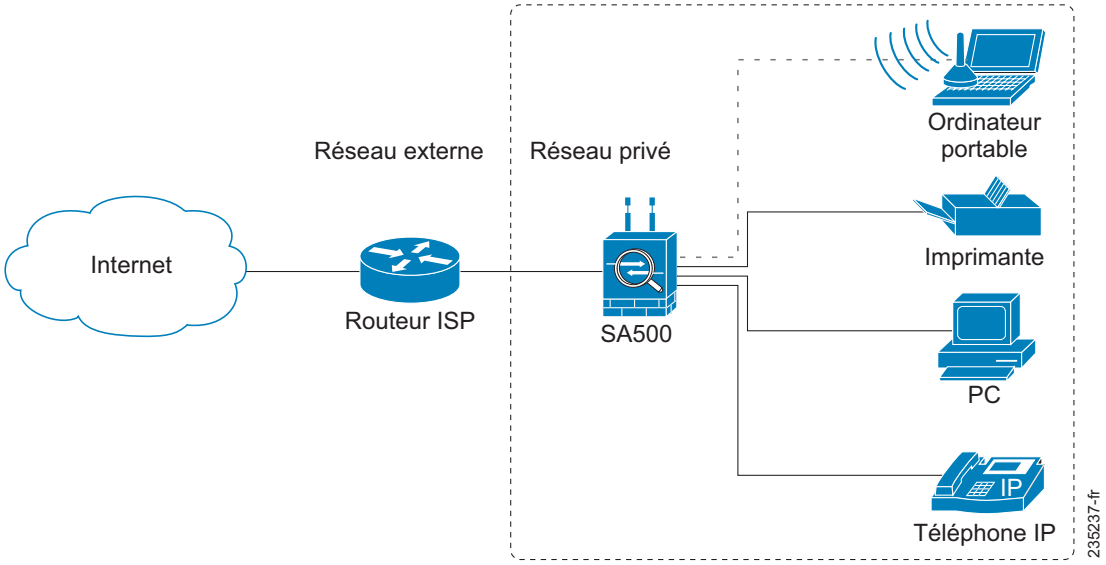


Tâches de configuration pour ce scénario :

Dans la section **SSL VPN Remote Access** de la page Getting Started (Advanced), cliquez sur le lien **SSL VPN Portal Layouts** afin de vérifier les paramètres par défaut pour le portail utilisateur. Créez des nouveaux portails pour les différents groupes d'utilisateurs, si nécessaire. Revenez sur la page Getting Started (Advanced) et cliquez sur le lien **Configure Users** pour ajouter vos utilisateurs VPN. Vous pouvez aussi utiliser les autres liens pour configurer les stratégies, les paramètres client, les routages et les ressources de votre VPN SSL. Pour plus d'informations, voir **Configuration d'un VPN SSL pour un accès à distance à partir d'un navigateur, page 164**.

Scénario 10 : réseau sans fil

Avec le SA520W, vous pouvez configurer votre réseau sans fil pour répondre aux exigences de votre environnement physique et de contrôler l'accès à vos ressources réseau.



Tâches de configuration pour ce scénario :

1. Les paramètres WAN et LAN par défaut peuvent être suffisants pour votre déploiement, mais vous devez tenir compte des étapes décrites dans le **Scénario 1 : configuration de base du réseau avec accès Internet, page 26**.
2. Bien que vous puissiez commencer à utiliser votre réseau sans fil immédiatement, vous devez configurer les paramètres de sécurité afin de protéger votre réseau et les données que vous transmettez. Pour configurer votre réseau sans fil, voir **Chapitre 3, « Configuration sans fil pour le SA520W ».**

2

Mise en réseau

Ce chapitre décrit la configuration des fonctionnalités de mise en réseau du routeur. Il comprend les sections suivantes :

- **Configuration de la connexion WAN**
- **Configuration de la zone LAN**
- **Configuration du WAN facultatif**
- **Configuration d'un DMZ**
- **Configuration VLAN**
- **Routage**
- **Gestion des ports**
- **Profils de bande passante QoS**
- **DNS dynamique**
- **Configuration de l'adressage IPv6**

Pour accéder aux pages Networking, cliquez sur **Networking** dans la barre de menu de l'utilitaire de configuration.

Configuration de la connexion WAN

Par défaut, votre appliance de sécurité est configurée pour recevoir une adresse IP publique de votre FAI automatiquement via DHCP. Selon les exigences de votre FAI, vous devrez peut-être modifier ces paramètres pour assurer la connectivité Internet. Par exemple, votre FAI peut avoir attribué une adresse IP statique ou nécessiter une connexion.

REMARQUE Si vous devez configurer l'adressage IPv6, consultez **Configuration de l'adressage IPv6, page 80.**

Utilisez les informations de compte fournies par votre FAI pour compléter les champs de cette page.

ÉTAPE 1 Cliquez sur **Networking** > **WAN > IPv4 Config** ou sur la page Getting Started (Basic), sous **WAN & LAN Connectivity**, cliquez sur **WAN settings**.

La fenêtre IPv4 WAN Configuration s'ouvre.

ÉTAPE 2 Dans la zone **ISP Configuration**, sélectionnez la case **Internet Connection Require a Login** si votre FAI nécessite une connexion à chaque fois que vous vous connectez à Internet.

- Si vous avez sélectionné la boîte de dialogue, passez à l'**Étape 3** pour compléter les champs de la zone ISP Connection Type.
- Si vous n'avez pas coché la case, passez à l'**Étape 4** pour renseigner les champs de la zone Internet (IP) Address et de la zone Dynamic Name System (DNS) Servers.

ÉTAPE 3 Si votre connexion internet nécessite une connexion, saisissez les paramètres dans la zone **ISP Connection Type** :

- **ISP Connection Type :** choisissez le type de connexion, tel que spécifié par votre fournisseur de service : PPTP, PPPoE ou L2TP. Puis renseignez également tous les champs signalés par un fond blanc.
- **PPPoE Profile Name :** sélectionnez un profil PPPoE. Pour gérer les profils de la liste déroulante, consultez **Création de profils PPPoE, page 42**.
- **User Name :** nom d'utilisateur nécessaire à la connexion
- **Password :** mot de passe nécessaire à la connexion
- **Secret :** entrez la phrase secrète pour vous connecter au serveur (le cas échéant).
- **Connectivity Type :** sélectionnez l'une des options suivantes :
  - **Keep Connected :** la connexion est toujours active, indépendamment du niveau de l'activité. Choisissez cette option si vous payez un abonnement fixe pour votre service Internet.
  - **Idle Time :** l'appliance de sécurité se déconnecte d'Internet après une période d'inactivité spécifiée (inactivité maximale). Si vous choisissez cette option, entrez également la durée d'inactivité en minutes. Choisissez cette option si votre connexion Internet est facturée au temps passé en ligne.

- **My IP Address :** saisissez l'adresse IP attribuée par votre FAI.
- **Server IP Address :** saisissez l'adresse IP du PPTP, PPPoE, ou d'un autre serveur.

ÉTAPE 4 Si votre FAI ne nécessite pas de connexion, saisissez les informations suivantes dans les zones **Internet (IP) Address** et **Dynamic Name System (DNS) Servers** :

- **IP Address Source :** votre FAI vous attribue une adresse IP qui peut être dynamique (générée à chaque connexion) ou statique (permanente).
  - **Get Dynamically from ISP** : choisissez cette option si votre FAI ne vous a pas attribué d'adresse IP.
  - **Use Static IP Address** : choisissez cette option si votre FAI vous a attribué une adresse IP. Saisissez également l'**adresse IP**, le **masque de sous-réseau IP** et l'**adresse IP de la passerelle** qui ont été fournis par le FAI.
- **DNS Server Source :** nom de domaine Internet de la carte de serveurs DNS (exemple : www.cisco.com) vers des adresses IP. Vous pouvez obtenir des adresses de serveur DNS automatiquement de votre FAI ou utiliser des adresses spécifiées par votre FAI.
  - **Get Dynamically from ISP** : choisissez cette option si vous n'avez pas reçu d'adresse IP DNS statique.
  - **Use These DNS Servers** : choisissez cette option si votre FAI vous a attribué une adresse IP DNS statique. Saisissez également les adresses du **serveur DNS principal** et du **serveur DNS secondaire**.

ÉTAPE 5 Si demandé par votre FAI, configurez les paramètres suivants dans la zone **MTU Size** :

- **Types MTU :** l'unité de transmission maximale est la taille, en octets, du plus grand paquet pouvant être transmis. Choisissez **Default** pour utiliser la taille MTU par défaut, 1 500 octets. Choisissez **Custom** si vous souhaitez spécifier une autre taille.
- **MTU Size :** si vous avez choisi **Customer** pour le type MTU, saisissez la taille MTU personnalisée en octets.

Le MTU (Maximum Transmit Unit) est la taille du plus grand paquet pouvant être envoyé sur le réseau. La valeur standard du MTU pour les réseaux Ethernet est généralement de 1 500 octets. Pour les connexions PPPoE, la taille est de 1 492 octets. Sauf indication contraire de votre FAI, il est recommandé de ne pas modifier les valeurs MTU.

ÉTAPE 6 Si votre FAI nécessite une source d'adresse MAC, saisissez les informations suivantes dans la zone **Router's MAC Address** :

- **MAC Address Source :** généralement, vous utilisez l'adresse Ethernet locale unique de 48 bits de l'appliance de sécurité comme source d'adresse MAC. Si votre FAI nécessite une authentification MAC et qu'une autre adresse MAC a déjà été enregistrée par votre FAI, vous pouvez saisir une adresse MAC différente à cet effet.
  - **Use Default Address :** choisissez cette option pour utiliser l'adresse MAC par défaut.
  - **Use this computer's MAC address :** choisissez cette option si vous souhaitez utiliser l'adresse MAC de votre ordinateur comme source d'adresse MAC.
  - **Use This MAC Address :** choisissez cette option si vous souhaitez saisir une adresse MAC nécessaire à votre FAI pour cette connexion (parfois appelée clonage d'adresse MAC). Saisissez l'**adresse MAC** au format XX:XX:XX:XX:XX:XX où X représente un nombre compris entre 0 et 9 (inclus) ou une lettre de l'alphabet entre A et F (inclus), comme dans l'exemple suivant : `01:23:45:67:89:ab`

ÉTAPE 7 Cliquez sur **Apply** pour enregistrer les paramètres.

REMARQUE Étapes suivantes :

- Si vous utilisez la page Getting Started (Basic), cliquez sur **Getting Started** dans la barre de menus, puis passez à la liste des tâches de configuration.
- Pour vérifier l'état du WAN, cliquez sur **WAN > WAN Status**. Pour obtenir plus d'informations, reportez-vous à la section **Afficher l'état du WAN, page 41**.
- Si vous devez créer des profils PPPoE, cliquez sur **WAN > PPPoE Profiles**. Pour obtenir plus d'informations, reportez-vous à la section **Création de profils PPPoE, page 42**.
- Si vous devez configurer une autre liaison FAI, cliquez sur **Optional Port > Optional Port Mode** et choisissez **WAN** pour le mode du port. Après avoir enregistré vos paramètres sur cette page, cliquez sur **Optional Port > WAN** pour configurer la connexion WAN. Pour obtenir plus d'informations, reportez-vous à la section **Configuration du WAN facultatif, page 55**.
- Si vous rencontrez des problèmes avec votre connexion WAN, consultez **Connexion Internet, page 234** dans **Annexe A, « Dépannage »**..

Afficher l'état du WAN

Vous pouvez vérifier l'état du WAN, renouveler la connexion ou libérer la connexion.

ÉTAPE 1 Cliquez sur **Networking** >**WAN > WAN Status**.

La fenêtre WAN Status s'ouvre. Cette page affiche les types d'informations suivants sur le WAN dédié et le WAN facultatif (le cas échéant) :

- Heure de connexion
- Type de connexion : IP dynamique (DHCP) ou IP statique
- État de la connexion : connecté ou déconnecté
- État de la liaison : actif ou inactif
- État du WAN : actif ou inactif
- DHCP Server
- Bail obtenu
- Durée du bail
- Adresse IP
- Masque de sous-réseau
- Passerelle
- Serveur DNS
- DNS secondaire
- Adresse MAC

ÉTAPE 2 Si le WAN est configuré à l'aide du protocole DHCP, vous pouvez utiliser les boutons de la page WAN Status pour renouveler ou libérer la connexion.

- Cliquez sur **Renew** pour renouveler la connexion.
- Cliquez sur **Release** pour libérer la connexion.
- Si le WAN est configuré avec une adresse IP statique, cliquez sur **Disable** pour désactiver la connexion.

REMARQUE Si vous rencontrez des problèmes avec votre connexion WAN, consultez **Connexion Internet, page 234** dans **Annexe A, « Dépannage »**..

Création de profils PPPoE

Si vous disposez de plusieurs comptes PPPoE, vous pouvez utiliser cette page pour gérer les informations. Vous pouvez alors associer un profil à l'interface WAN dans le cadre de la configuration WAN.

ÉTAPE 1 Cliquez sur **Networking** > **WAN > PPPoE Profiles** ou sur la page Getting Started (Basic), sous **WAN & LAN Connectivity**, cliquez sur**PPPoE profiles**.

La fenêtre PPPoE profiles s'ouvre.

ÉTAPE 2 Cliquez sur **Add** pour créer un profil.

Autres options : cliquez sur le bouton **Edit** pour modifier une entrée. Pour supprimer une entrée, sélectionnez la case correspondante, puis cliquez sur **Delete**. Pour sélectionner toutes les entrées du tableau, cochez la case située dans la ligne d'en-tête du côté gauche.

Lorsque vous cliquez sur Add ou Edit, la fenêtre PPPoE Profile Configuration s'ouvre.

ÉTAPE 3 Saisissez les informations suivantes :

- **Profile Name :** saisissez un nom pour le profil.
- **User Name :** saisissez le nom d'utilisateur qui est requis pour la connexion au compte FAI.
- **Password :** saisissez le mot de passe qui est requis pour la connexion au compte FAI.
- **Authentication Type :** choisissez le type d'authentification, tel que spécifié par votre FAI.
- **Connectivity Type :** sélectionnez l'une des options suivantes :
  - **Keep Connected :** la connexion est toujours active, indépendamment du niveau de l'activité. Ce choix est recommandé si vous payez un abonnement fixe pour votre service Internet.
  - **Idle :** l'appliance de sécurité se déconnecte d'Internet après une période d'inactivité spécifiée (inactivité maximale). Si vous choisissez cette option, entrez également la durée d'inactivité en minutes. Ce choix est recommandé si votre connexion Internet est facturée au temps passé en ligne.

ÉTAPE 4 Cliquez sur **Apply** pour enregistrer les paramètres.

Configuration d'un alias IP

Un seul port Ethernet WAN est accessible par plusieurs adresses IP en ajoutant un alias IP au port.

ÉTAPE 1 Cliquez sur **Networking** > **WAN > IP Alias**.

La fenêtre IP Aliases s'ouvre.

Tous les alias IP WAN actuellement configurés utilisés par le port WAN apparaissent dans le tableau List of IP Aliases.

ÉTAPE 2 Cliquez sur **Add** pour ajouter un nouvel alias.

Autres options : cliquez sur le bouton **Edit** pour modifier une entrée. Pour supprimer une entrée, sélectionnez la case correspondante, puis cliquez sur **Delete**. Pour sélectionner toutes les entrées du tableau, cochez la case située dans la ligne d'en-tête du côté gauche.

Lorsque vous cliquez sur Add ou Edit, la fenêtre IP Aliases s'ouvre.

ÉTAPE 3 Saisissez les informations suivantes :

- **Interface Name :** choisissez un nom d'interface sur lequel l'alias est créé.
- **IP Address :** alias d'adresse IP ajouté à ce port WAN du routeur.
- **Mask :** masque de sous-réseau IPv4.

ÉTAPE 4 Cliquez sur **Apply** pour enregistrer vos modifications.

Le nouvel alias apparaît dans le tableau List of IP Aliases.

Configuration de la zone LAN

Pour la plupart des applications, les paramètres DHCP et TCP/IP de l'appliance de sécurité sont satisfaisants. Toutefois, vous pouvez utiliser la page LAN Configuration pour modifier ces paramètres, entre autres.

- **À propos des paramètres LAN par défaut**
- **Configuration de la zone LAN**
- **Afficher l'état du LAN**
- **Configuration VLAN**
- **IP DHCP réservées**
- **Clients soumis au bail DHCP**
- **Configuration d'un proxy IGMP**
- **Configuration du port facultatif comme port LAN**

À propos des paramètres LAN par défaut

- Par défaut le LAN du routeur est configuré dans le sous-réseau **192.168.75.0** et l'adresse IP du LAN du routeur est **192.168.75.1**.
- Par défaut, l'appliance de sécurité agit comme un serveur DHCP (Dynamic Host Configuration Protocol) pour les hôtes du réseau WLAN ou LAN. Elle peut automatiquement attribuer des adresses IP et des adresses de serveur DNS aux ordinateurs et aux autres périphériques du LAN. Si DHCPest activé, l'adresse IP de l'appliance de sécurité est l'adresse de la passerelle vers votre LAN. Si vous souhaitez qu'un autre PC de votre réseau se trouve sur le serveur DHCP ou si vous configurez manuellement les paramètres réseau de tous vos ordinateurs, désactivez le DHCP et saisissez les paramètres appropriés.
- Au lieu d'utiliser un serveur DNS, vous pouvez utiliser un serveur WINS (Windows Internet Naming Service). Un serveur WINS est l'équivalent d'un serveur DNS mais il utilise le protocole NetBIOS pour résoudre les noms d'hôte. L'appliance de sécurité inclut l'adresse IP du serveur WINS dans la configuration DHCP lorsqu'elle reçoit une demande DHCP d'un client DHCP.
- Par défaut, votre LAN est configuré pour l'adressage IPv4. Si vous devez activer l'adressage IPv6, consultez **Configuration de l'adressage IPv6, page 80** et **Configuration du LAN IPv6, page 83**.

Configuration de la zone LAN

ÉTAPE 1 Cliquez sur **Networking** > **LAN > IPv4 Config** ou sur la page Getting Started (Basic), sous **WAN & LAN Connectivity**, cliquez sur **LAN Settings**.

La fenêtre IPv4 LAN Configuration s'ouvre.

ÉTAPE 2 Dans la zone **LAN TCP/IP Setup**, saisissez ces informations pour votre appliance de sécurité :

- **IP address :** saisissez l'adresse IP du LAN pour l'appliance de sécurité.

  REMARQUE Si vous modifiez l'adresse IP dans ce champ et que vous cliquez sur **Apply**, l'appliance de sécurité ne se trouvera plus à l'adresse IP que vous avez saisie dans votre navigateur Web pour lancer l'utilitaire de configuration et votre ordinateur ne se trouvera plus sur le même sous-réseau que l'appliance de sécurité (qui a reçu une adresse IP via DHCP basée sur l'ancienne adresse).

  Après avoir cliqué sur **Apply**, attendez quelques secondes pour permettre à votre ordinateur d'obtenir une nouvelle adresse IP du pool d'adresses IP récemment attribuées (ou débrancher et rebranchez le câble Ethernet pour libérer et renouveler votre adresse IP). Saisissez ensuite la nouvelle adresse IP de l'appliance de sécurité dans la barre d'adresse du navigateur, puis connectez-vous à nouveau.

- **Subnet mask :** saisissez le masque de sous-réseau pour cette adresse IP.

ÉTAPE 3 Dans la zone **DHCP**, configurez ces paramètres :

- **DHCP Mode :** sélectionnez l'une des options suivantes :
  - **None :** choisissez cette option si les ordinateurs du LAN sont configurés avec des adresses IP statiques ou sont configurés pour utiliser un autre serveur DHCP.
  - **DHCP Server :** choisissez cette option pour autoriser l'appliance de sécurité à jouer le rôle d'un serveur DHCP et à attribuer des adresses IP dans la plage spécifiée. Renseignez également les champs signalés par un fond blanc.

    Si vous souhaitez réserver certaines IP pour des périphériques particuliers, suivez la procédure puis configurez les adresses IP réservées. Voir aussi **IP DHCP réservées, page 53.**

- **DHCP Relay :** choisissez cette option pour autoriser l'appliance de sécurité à utiliser un relais DHCP. Si vous choisissez ce mode, saisissez également l'adresse IP de la passerelle relais.

- **Domain Name (optional) :** saisissez un nom pour le domaine.
- **Starting IP Address** et **Ending IP Address** : saisissez la plage d'adresses du pool d'adresses IP pour cette appliance de sécurité. Tout nouveau client DHCP qui se connecte au LAN se voit attribuer une adresse IP de cette plage. Par défaut, l'adresse de début est 192.168.75.2. L'adresse de fin par défaut est 192.168.75.100. Vous pouvez enregistrer une partie de la plage pour les PC disposant d'adresses fixes. Ces adresses doivent être dans le même sous-réseau d'adresses IP que l'adresse IP du LAN de l'appliance de sécurité.
- **Primary DNS Server** et **Secondary DNS Server (Optional)** : Éventuellement, saisissez l'adresse IP du serveur DNS principal et du serveur DNS secondaire pour votre prestataire de services.
- **Primary Tftp Server et Secondary Tftp Server (Optional) :** Éventuellement, saisissez l'adresse IP du serveur Tftp principal et du serveur Tftp secondaire pour votre prestataire de services.
- **WINS Server (Optional) :** saisissez l'adresse IP du serveur WINS ou, s'il se trouve dans votre réseau, le serveur NetBios Windows.
- **Lease Time :** saisissez la durée maximale de connexion en heures pendant laquelle une adresse IP dynamique fait « l'objet d'un bail » pour un utilisateur réseau. Lorsque le délai se termine, une nouvelle adresse IP dynamique est automatiquement attribuée à l'utilisateur. La valeur par défaut est de 24 heures.
- **Relay Gateway :** si vous avez choisi le relais DHCPcomme mode DHCP, saisissez l'adresse IP de la passerelle relais.

ÉTAPE 4 Dans la section **LAN Proxies**, spécifiez les paramètres de proxy :

- **Enable DNS Proxy :** cochez cette case pour permettre à l'appliance de sécurité d'agir comme proxy pour toutes les requêtes DNS et de communiquer avec les serveurs DNS du FAI. Lorsque cette fonction est désactivée, tous les clients DHCP reçoivent les adresses IP du serveur DNS du FAI.

ÉTAPE 5 Cliquez sur **Apply** pour enregistrer les paramètres.

REMARQUE Étapes suivantes :

- Si vous utilisez la page Getting Started (Basic), cliquez sur **Getting Started** dans la barre de menus, puis passez à la liste des tâches de configuration.
- Pour vérifier l'état de connexion du LAN, cliquez sur **LAN > LAN Status**. Pour obtenir plus d'informations, reportez-vous à la section **Afficher l'état du LAN, page 47**.
- Pour réserver certaines adresses IP de manière permanente pour des périphériques particuliers, cliquez sur **LAN > DHCP Reserved IPs**. Pour obtenir plus d'informations, reportez-vous à la section **IP DHCP réservées, page 53.**
- Pour afficher une liste des périphériques connectés, cliquez sur **LAN > DHCP Leased Clients**. Pour obtenir plus d'informations, reportez-vous à la section **Clients soumis au bail DHCP, page 54**.
- Si vous avez besoin d'un port LAN supplémentaire et que vous ne comptez pas configurer un WAN ou un DMZ facultatif, cliquez sur **Optional Port > Optional Port Mode** et choisissez **LAN** comme mode du port. Pour obtenir plus d'informations, reportez-vous à la section **Configuration du port facultatif comme port LAN, page 55.**
- Si vous rencontrez des problèmes avec votre connexion LAN, consultez **Effectuer un test ping pour tester la connectivité LAN, page 237** dans **Annexe A, « Dépannage ».**.

Afficher l'état du LAN

ÉTAPE 1 Cliquez sur **Networking > LAN > LAN Status**.

La fenêtre LAN Status s'ouvre. Cette page répertorie les types suivants d'informations :

- Adresse MAC de l'interface LAN.
- L'adresse IP et le masque de sous-réseau de l'interface
- Mode du serveur DHCP

ÉTAPE 2 Cliquez sur **Apply** pour enregistrer les paramètres.

Configuration VLAN

L'appliance de sécurité prend en charge les réseaux LAN virtuels (VLAN), qui vous permettent de répartir le réseau en LAN isolés les uns des autres. La configuration par défaut fournit un VLAN données et un VLAN voix, qui peuvent être traités comme deux réseaux distincts.

Vous pouvez modifier les paramètres des VLAN par défaut et vous pouvez ajouter de nouveaux VLAN, jusqu'à un total de 16 VLAN. Par exemple, si vous avez besoin d'un réseau invité pour les visiteurs sur votre site, vous pouvez créer un nouveau VLAN. Tous les PC connectés au port LAN spécifié sont sur un VLAN distinct et ne peut pas accéder aux autres VLAN, sauf si vous activez le routage inter-VLAN.

Cette section comprend les rubriques suivantes :

- **Paramètres VLAN par défaut**
- **Activation ou désactivation de la prise en charge VLAN**
- **Création des ID de VLAN**
- **Attribution de VLAN aux ports LAN**

Paramètres VLAN par défaut

Par défaut, le VLAN données et le VLAN voix sont activés avec les paramètres suivants :

- Data VLAN : le VLAN est activé avec l'ID de VLAN 1
  - VLAN - Data, VLAN Number (untagged packets) : 1
  - VLAN - Data, IP Address : soir l'onglet Product
  - VLAN - Data, IP Address Distribution : DHCP Server
  - VLAN - Data, Start IP Address : 192.168.75.50(en supposant que l'adresse IP LAN est 192.168.75.1)
  - VLAN - Data, End IP Address : 192.168.75.254(en supposant que l'adresse IP LAN est 192.168.75.1)
  - VLAN - Data, Subnet Mask : 255.255.255.0
  - VLAN - Data, Lease Time in Minutes : 1 440 (24 heures)
  - Lease Time in Minutes : 1 440 (24 heures)
  - HTTP Remote Access : disable

- HTTPS Remote Access : disable

- Voice VLAN : le VLAN est activé avec l'ID de VLAN 100.
  - IP Address : 10.1.1.1
  - IP Address Distribution : DHCP Server
  - Start IP Address : 10.1.1.50
  - End IP Address : 10.1.1.254
  - Subnet Mask : 255.255.255.0

Activation ou désactivation de la prise en charge VLAN

Par défaut, la prise en charge VLAN est activée. Si vous ne souhaitez pas de VLAN, vous pouvez désactiver la prise en charge VLAN.

ÉTAPE 1 Cliquez sur **Networking > VLAN > VLAN Configuration**.

La fenêtre Configuration VLAN s'ouvre.

ÉTAPE 2 Pour activer la prise en charge VLAN, cochez la case **Enable VLAN**. Pour désactiver la prise en charge VLAN, décochez la case.

ÉTAPE 3 Cliquez sur **Apply** pour enregistrer les paramètres.

REMARQUE Étapes suivantes :

Créer des ID de VLAN. Pour obtenir plus d'informations, reportez-vous à la section **Création des ID de VLAN, page 49**.

Création des ID de VLAN

Avant de pouvoir configurer un nouveau VLAN, vous devez créer des ID de VLAN. Ensuite vous attribuerez des ID de VLAN aux ports de la page Port VLANs.

ÉTAPE 1 Cliquez sur **Networking > VLAN > Available VLANs**.

La fenêtre Available VLANs s'ouvre. Le VLAN par défaut et tous les autres VLAN apparaissent dans le tableau List of available VLANs. L'ID de VLAN par défaut est 1.

ÉTAPE 2 Pour ajouter un VLAN, cliquez sur **Add**.

Autres options : pour supprimer une entrée, sélectionnez la case correspondante, puis cliquez sur **Delete**. Pour modifier une entrée, cochez la case puis cliquez sur le bouton **Edit**. Pour sélectionner toutes les entrées du tableau, cochez la case située dans la ligne d'en-tête du côté gauche.

Lorsque vous cliquez sur Add ou Edit, la fenêtre VLAN Configuration s'ouvre.

ÉTAPE 3 Saisissez les informations suivantes :

- **Name :** saisissez un nom descriptif, pour référence.
- **ID :** saisissez un numéro d'identification unique, qui peut être tous les numéros compris entre 2 et 4091.

  REMARQUE L'ID de VLAN 1 est réservé pour le VLAN par défaut, utilisé pour les trames non marquées reçues sur l'interface. L'ID de VLAN 4 092 est réservée et ne peut pas être utilisée.

- **Inter VLAN Routing Enable :** cochez la case si vous souhaitez autoriser le SA500 à router le trafic entre ce VLAN et un autre VLAN pour lequel le routage inter-VLAN est également activé. Décochez la case pour désactiver le routage inter-VLAN pour ce VLAN.

ÉTAPE 4 Cliquez sur **Apply** pour enregistrer les paramètres.

REMARQUE Étapes suivantes :

- Attribuez les VLAN aux ports LAN. Pour obtenir plus d'informations, reportez-vous à la section **Attribution de VLAN aux ports LAN, page 50.**
- Paramétrez des sous-réseaux VLAN. Pour obtenir plus d'informations, reportez-vous à la section **Sous-réseaux locaux virtuels (VLAN) multiples, page 52.**

Attribution de VLAN aux ports LAN

Pour attribuer un VLAN à un port LAN, choisissez le mode et attribuez une appartenance VLAN.

ÉTAPE 1 Cliquez sur **Networking > LAN > Port VLAN**.

La fenêtre Port VLANs s'ouvre. Les paramètres du port VLAN existants sont indiqués dans le tableau Port VLANs.

ÉTAPE 2 Pour mettre à jour les paramètres d'un port, cliquez sur le bouton **Edit**.

ÉTAPE 3 Dans la zone **VLAN Configuration**, saisissez les informations suivantes :

- **Mode :** sélectionnez l'une des options suivantes :
  - **Access :** le port d'accès est membre d'un VLAN unique. Aucune donnée dans et hors du port d'accès n'est marquée. Par défaut, tous les ports VLAN sont en mode Accès. Le mode Accès est recommandé si le port est connecté à un périphérique d'utilisateur final unique qui n'est pas compatible VLAN.
    Si vous choisissez cette option, saisissez également un ID de VLAN pour le port dans le champ **PVID**.
  - **General :** le port est membre d'un groupe spécifié de VLAN. Le port envoie et reçoit des données marquées et non marquées. Le PVID spécifié est affecté aux données non marquées arrivant dans le port. Les données envoyées hors du port à partir du même PVID ne sont pas marquées. Toutes les autres données sont marquées. Le mode Général est recommandé si le port est connecté à un commutateur non géré avec une combinaison de périphériques compatibles VLAN et non compatibles VLAN.
    Si vous choisissez cette option, saisissez également un numéro de **PVID** pour le port et configurez l'**appartenance VLAN** dans la moitié inférieure de la page.
  - **Trunk :** le port est membre d'un groupe spécifié de VLAN. Toutes les données dans et hors du port sont marquées. Les données non marquées arrivant dans le port ne sont pas transférées, à l'exception du VLAN par défaut avec le PVID= 1, qui n'est pas marqué. Le mode Liaison est recommandé si le port est connecté à un commutateur ou à un routeur compatible VLAN.
    Si vous choisissez cette option, configurez également l'**appartenance VLAN** dans la moitié inférieure de la page.
- **PVID** : si vous avez choisi le mode Accès ou Général, saisissez l'ID du port VLAN à utiliser pour le transfert ou le filtrage des paquets non marqués arrivant dans le port.

ÉTAPE 4 Dans la zone **VLAN Membership Configuration**, cochez la case pour chaque VLAN que vous souhaitez associer à ce port.

ÉTAPE 5 Cliquez sur **Apply** pour enregistrer les paramètres.

Sous-réseaux locaux virtuels (VLAN) multiples

En général, les VLAN sont isolés de telle sorte que le trafic généré par l'un de ces réseaux n'est pas vu par les autres. Toutefois, il existe des instances dans lesquelles vous souhaitez activer la communication entre les VLAN. Lorsque vous configurez des sous-réseaux VLAN, l'appliance de sécurité achemine le trafic entre les VLAN et fournit des services tels qu'un serveur DHCP pour les membres de chaque VLAN.

ÉTAPE 1 Cliquez sur **Networking > VLAN > Multiple VLAN Subnets**.

La fenêtre Multiple VLAN Subnets s'ouvre. Tous les VLAN de la page **Networking > LAN > Available VLANs** sont indiqués dans le tableau Multiple VLAN Subnets.

La fenêtre Multiple VLAN Subnet Configuration s'ouvre.

ÉTAPE 2 Dans la section **Multiple VLAN Subnet** de la page, saisissez les paramètres suivants :

- **IP Address :** saisissez l'adresse IP du sous-réseau VLAN.
- **Subnet Mask :** saisissez le masque de sous-réseau pour ce VLAN.

ÉTAPE 3 Dans la section **DHCP** de la page, choisissez le mode DHCP :

- **None :** choisissez cette option si vous ne souhaitez pas activer le serveur DHCP pour ce VLAN.
- **DHCP Server :** choisissez cette option pour autoriser l'appliance de sécurité à agir comme serveur DHCP pour ce VLAN. Si vous choisissez cette option, renseignez les autres champs de cette section de la page.
- **DHCP Relay :** choisissez cette option pour autoriser l'appliance de sécurité à utiliser un relais DHCP pour ce VLAN. Si vous choisissez ce mode, saisissez également l'adresse IP de la **Relay Gateway**.

ÉTAPE 4 Si vous avez choisi DHCP Server pour le mode DHCP, saisissez les informations suivantes :

- **Domain Name :** *(optional)* saisissez un nom de domaine pour ce VLAN.
- **Starting IP Address :** saisissez la première adresse IP de la plage DHCP. Une adresse IP entre cette adresse et l'adresse IP de fin est attribuée à tout nouveau client DHCP se connectant au VLAN.
- **Ending IP Address :** saisissez la dernière adresse IP de la plage DHCP. Une adresse IP entre l'adresse IP de début et l'adresse IP de fin est attribuée à tout nouveau client DHCP se connectant au LAN.

REMARQUE Les adresses DHCP de début et de fin doivent se trouver dans la même plage d'adresses IP que l'adresse TCP/IP du LAN (tel que configuré sur la page LAN > IPv4 LAN Configuration, à la section LAN TCP/IP Setup).

- **Primary DNS Server** et **Secondary DNS Server (Optional)** : saisissez l'adresse IP du serveur DNS principal pour le VLAN. Éventuellement, saisissez l'adresse IP d'un serveur DNS secondaire.
- **Primary Tftp Server** et **Secondary Tftp Server (Optional)** : saisissez l'adresse IP des serveurs Tftp principal et secondaire pour le VLAN
- **WINS Server (Optional) :** saisissez l'adresse IP du serveur WINS ou, s'il se trouve dans votre réseau, le serveur NetBios Windows.
- **Lease Time :** saisissez la durée maximale de connexion en heures pendant laquelle une adresse IP dynamique fait « l'objet d'un bail » pour un utilisateur réseau. Lorsque le délai se termine, une nouvelle adresse IP dynamique est automatiquement attribuée à l'utilisateur. La valeur par défaut est de 24 heures.

ÉTAPE 5 Dans la section **LAN Proxies**, cochez la case **Enable DNS Proxy** pour permettre au VLAN d'agir comme proxy pour toutes les requêtes DNS et pour communiquer avec les serveurs DNS du FAI. Lorsque cette fonction est désactivée, tous les clients DHCP du VLAN reçoivent les adresses IP du serveur DNS du FAI.

Cette fonctionnalité est particulièrement utile en mode Renvoi automatique. Par exemple, si les serveurs DNS de chaque connexion sont différents, une défaillance de liaison peut rendre les serveurs DNS inaccessibles. Toutefois, lorsque le proxy DNS est activé, les clients peuvent envoyer des requêtes au routeur et le routeur, en retour, envoie ces requêtes aux serveurs DNS de la connexion active. Vous pouvez également activer le proxy IGMP sur le LAN correspondant.

ÉTAPE 6 Cliquez sur **Apply** pour enregistrer les paramètres.

IP DHCP réservées

Même si l'appliance de sécurité est configurée pour agir comme serveur DHCP, vous pouvez réserver certaines adresses IP à attribuer à des périphériques spécifiés. Pour ce faire, ajouter l'adresse MAC du périphérique, ainsi que l'adresse IP souhaitée, à la liste des IP DHCP réservées. Dès que le serveur DHCP du LAN reçoit une demande d'un périphérique, l'adresse matérielle est comparée à la base de données. Si l'appareil est détecté, l'adresse IP réservée est utilisée. Sinon, une adresse IP est attribuée automatiquement depuis le pool DHCP.

REMARQUE Les IP réservées doivent être en dehors du pool d'adresses DHCP pour que le serveur DHCP les attribue de manière dynamique.

ÉTAPE 1 Cliquez sur **Networking > LAN > DHCP Reserved IPs** ou sur la page Getting Started (Basic), sous **WAN & LAN Connectivity**, cliquez sur **DHCP Reserved IPs (Optional)**.

La fenêtre DHCP Reserved IPs (LAN) s'ouvre. Tous les IP réservés existants sont répertoriés dans le tableau Available DHCP Assigned IPs (LAN).

ÉTAPE 2 Pour ajouter une adresse IP réservée, cliquez sur **Add**. La fenêtre DHCP Reserved IP for LAN s'ouvre.

Autres options : cliquez sur le bouton **Edit** pour modifier une entrée. Pour supprimer une entrée, sélectionnez la case correspondante puis cliquez sur **Delete**. Pour sélectionner toutes les entrées du tableau, cochez la case située dans la ligne d'en-tête du côté gauche.

ÉTAPE 3 Saisissez l'adresse IP et l'adresse MAC du périphérique que vous souhaitez ajouter.

Chaque adresse IP réservée doit être en dehors du pool d'adresses DHCP configuré.

ÉTAPE 4 Cliquez sur **Apply** pour enregistrer les paramètres.

Clients soumis au bail DHCP

Cette page affiche une liste des adresses IP attribuées par DHCP et des adresses matérielles des clients du LAN. Cliquez sur **Networking > LAN > DHCP Leased Clients**.

Configuration d'un proxy IGMP

Vous pouvez configurer le routeur pour agir comme un proxy pour toutes les demandes IGMP et pour communiquer avec les serveurs IGMP du FAI.

ÉTAPE 1 Cliquez sur **Networking > LAN > IGMP Configuration**.

La fenêtre IGMP Proxy s'ouvre.

ÉTAPE 2 Cochez la case correspondante pour activer un proxy IGMP.

ÉTAPE 3 Cliquez sur **Apply** pour enregistrer vos modifications.

Configuration du port facultatif comme port LAN

Si vous ne comptez pas configurer un WAN ou un DMZ facultatif, vous pouvez configurer le port facultatif comme port LAN.

ÉTAPE 1 Cliquez sur **Networking > Optional Port > Optional Port Mode**.

La fenêtre Optional Port Mode s'ouvre.

ÉTAPE 2 Choisissez **LAN**.

ÉTAPE 3 Cliquez sur **Apply** pour enregistrer les paramètres.

Configuration du WAN facultatif

Vous pouvez configurer le port facultatif comme WAN facultatif, ce qui vous permet de configurer deux liaisons FAI pour votre réseau. Vous pouvez utiliser une liaison en tant que liaison principale et l'autre comme liaison de secours ou vous pouvez configurer l'équilibrage de charge pour utiliser les deux liaisons en même temps.

ÉTAPE 1 Configurez d'abord le port facultatif en tant que port WAN :

a. Cliquez sur **Networking > Optional Port > Optional Port Mode**, ou sur la page Getting Started (Advanced), sous **Secondary WAN Port**, cliquez sur **Set Optional Port to WAN**.

   La fenêtre Optional Port Mode s'ouvre.

b. Choisissez **WAN**.

c. Cliquez sur **Apply** pour enregistrer les paramètres.

   Si vous êtes sur la page Getting Started (Advanced), cliquez sur **Getting Started > Advanced** pour retourner à la liste des tâches de configuration.

ÉTAPE 2 Cliquez sur **Networking > Optional Port > WAN** ou sur la page Getting Started (Advanced), sous **Secondary WAN Port**, cliquez sur **Configure WAN settings for Optional Port**.

ÉTAPE 3 La fenêtre WAN Configuration s'ouvre. Dans la zone **ISP Configuration**, sélectionnez la case **Internet Connection Require a Login** si votre FAI nécessite une connexion à chaque fois que vous vous connectez à Internet.

- Si vous avez coché la case, renseignez les champs de la zone ISP Connection Type.
- Si vous n'avez pas coché la case, poursuivez en renseignant les champs de la zone Internet (IP) Address et de la zone Dynamic Name System (DNS) Servers.

ÉTAPE 4 Si votre connexion internet nécessite une connexion, saisissez les paramètres dans la zone **ISP Connection Type** :

- **ISP Connection Type :** choisissez le type de connexion, tel que spécifié par votre fournisseur de service : PPTP, PPPoE ou L2TP. Puis renseignez également tous les champs signalés par un fond blanc.
- **PPPoE Profile Name :** sélectionnez un profil PPPoE. Pour gérer les profils de la liste déroulante, consultez **Création de profils PPPoE, page 42**.
- **User Name :** nom d'utilisateur nécessaire à la connexion
- **Password :** mot de passe nécessaire à la connexion
- **Secret :** entrez la phrase secrète pour vous connecter au serveur (le cas échéant).
- **Connectivity Type :** sélectionnez l'une des options suivantes :
  - **Keep Connected :** la connexion est toujours active, indépendamment du niveau de l'activité. Choisissez cette option si vous payez un abonnement fixe pour votre service Internet.
  - **Idle Time :** l'appliance de sécurité se déconnecte d'Internet après une période d'inactivité spécifiée (inactivité maximale). Si vous choisissez cette option, entrez également la durée d'inactivité en minutes. Choisissez cette option si votre connexion Internet est facturée au temps passé en ligne.
- **My IP Address :** saisissez l'adresse IP attribuée par votre FAI.
- **Server IP Address :** saisissez l'adresse IP du PPTP, PPPoE, ou d'un autre serveur.

ÉTAPE 5 Si votre FAI ne nécessite pas de connexion, saisissez les informations suivantes dans les zones **Internet (IP) Address** et **Dynamic Name System (DNS) Servers** :

- **IP Address Source :** votre FAI vous attribue une adresse IP qui peut être dynamique (générée à chaque connexion) ou statique (permanente).
  - **Get Dynamically from ISP** : choisissez cette option si votre FAI ne vous a pas attribué d'adresse IP.
  - **Use Static IP Address** : choisissez cette option si votre FAI vous a attribué une adresse IP. Saisissez également l'**adresse IP**, le **masque de sous-réseau IP** et l'**adresse IP de la passerelle** qui ont été fournis par le FAI.
- **DNS Server Source :** nom de domaine Internet de la carte de serveurs DNS (exemple : www.cisco.com) vers des adresses IP. Vous pouvez obtenir des adresses de serveur DNS automatiquement de votre FAI ou utiliser des adresses spécifiées par votre FAI.
  - **Get Dynamically from ISP** : choisissez cette option si vous n'avez pas reçu d'adresse IP DNS statique.
  - **Use These DNS Servers** : choisissez cette option si votre FAI vous a attribué une adresse IP DNS statique. Saisissez également les adresses du **serveur DNS principal** et du **serveur DNS secondaire**.

ÉTAPE 6 Si demandé par votre FAI, configurez les paramètres suivants dans la zone **MTU Size** :

- **MTU Type :** l'unité de transmission maximale est la taille, en octets, du plus grand paquet pouvant être transmis. Choisissez **Default** pour utiliser la taille MTU par défaut, 1 500 octets. Choisissez **Custom** si vous souhaitez spécifier une autre taille.
- **MTU Size :** si vous avez choisi **Customer** pour le type MTU, saisissez la taille MTU personnalisée en octets.

  Le MTU (Maximum Transmit Unit) est la taille du plus grand paquet pouvant être envoyé sur le réseau. La valeur standard du MTU pour les réseaux Ethernet est généralement de 1 500 octets. Pour les connexions PPPoE, la taille est de 1 492 octets. Sauf indication contraire de votre FAI, il est recommandé de ne pas modifier les valeurs MTU.

ÉTAPE 7 Si votre FAI nécessite une source d'adresse MAC, saisissez les informations suivantes dans la zone **Router's MAC Address** :

- **MAC Address Source :** généralement, vous utilisez l'adresse Ethernet locale unique de 48 bits de l'appliance de sécurité comme source d'adresse MAC. Si votre FAI nécessite une authentification MAC et qu'une autre adresse MAC a déjà été enregistrée par votre FAI, vous pouvez saisir une adresse MAC différente à cet effet.
  - **Use Default Address :** choisissez cette option pour utiliser l'adresse MAC par défaut.
  - **Use this computer's MAC address :** choisissez cette option si vous souhaitez utiliser l'adresse MAC de votre ordinateur comme source d'adresse MAC.
  - **Use This MAC Address :** choisissez cette option si vous souhaitez saisir une adresse MAC nécessaire à votre FAI pour cette connexion (parfois appelée clonage d'adresse MAC). Saisissez l'**adresse MAC** au format XX:XX:XX:XX:XX:XX où X représente un nombre compris entre 0 et 9 (inclus) ou une lettre de l'alphabet entre A et F (inclus), comme dans l'exemple suivant : `01:23:45:67:89:ab`

ÉTAPE 8 Cliquez sur **Apply** pour enregistrer les paramètres.

ÉTAPE 9 Étapes suivantes :

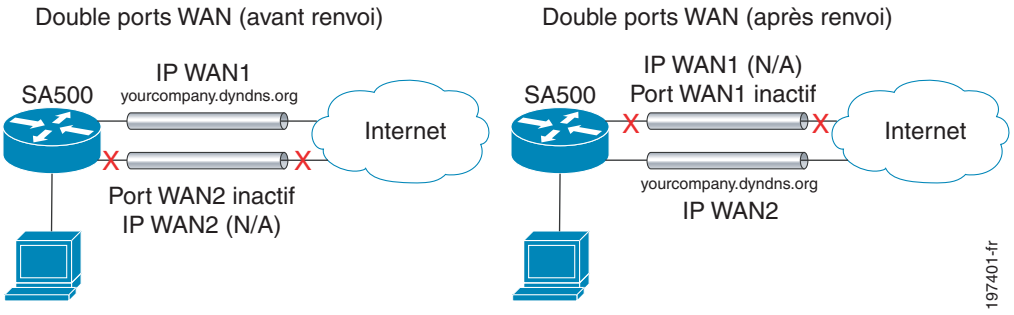
- Si vous êtes sur la page Getting Started (Advanced), cliquez sur **Getting Started > Advanced** pour poursuivre la liste des tâches de configuration.
- Pour vérifier l'état du WAN, cliquez sur **WAN > WAN Status**. Pour obtenir plus d'informations, reportez-vous à la section **Afficher l'état du WAN, page 41**.
- **Recommandé :** pour configurer le renvoi automatique, l'équilibrage de charge et la détection des défaillances pour vos liaison FAI, cliquez sur **Optional Port > WAN Mode**. Pour obtenir plus d'informations, reportez-vous à la section **Configuration du renvoi automatique, de l'équilibrage de charge et de la détection des défaillances, page 59.**
- Si vous rencontrez des problèmesavec votre connexion WAN, consultez **Connexion Internet, page 234** dans **Annexe A, « Dépannage »**..

Configuration du renvoi automatique, de l'équilibrage de charge et de la détection des défaillances

Si vous avez configuré deux liaisons FAI, une pour le WAN dédié et une pour le WAN facultatif, vous pouvez configurer le mode WAN pour définir le mode d'utilisation des deux liaisons FAI. Vous pouvez choisir parmi ces fonctions :

- **Auto-Rollover :** activez cette option si vous souhaitez utiliser une liaison FAI comme liaison de secours. Si une défaillance est détectée sur la liaison spécifiée en tant que liaison principale, l'appliance de sécurité dirige l'ensemble du trafic Internet vers la liaison de secours. Lorsque la liaison principale retrouve la connectivité, tout le trafic Internet est dirigé vers la liaison principale et la liaison de secours devient inactive. Vous pouvez désigner le port WAN dédié ou le port WAN facultatif comme liaison principale. **Figure 1** présente un exemple de double ports WAN configurés avec renvoi automatique.

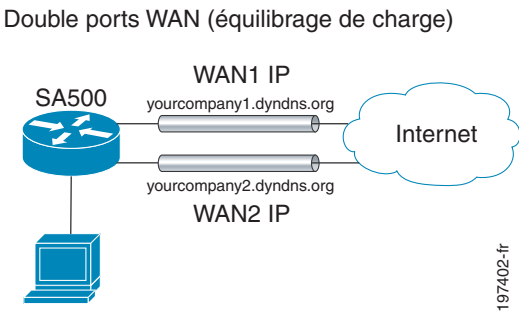
Figure 1 Exemple de double ports WAN avec renvoi automatique



- **Load Balancing :** activez cette option si vous souhaitez utiliser les deux liaisons FAI de manière simultanée. Les deux liaisons acheminent des données pour les protocoles qui leur sont rattachés. Vous pouvez utiliser cette fonctionnalité pour identifier le trafic entre les liaisons de vitesse différente. Par exemple, contraindre les services de haut volume sur le port connecté à la liaison haut-débit et contraindre les services de faible volume sur le port connecté à la liaison la plus lente.

  L'équilibrage de la charge est mis en œuvre pour le trafic sortant et non pour le trafic entrant. Pour garder un meilleur contrôle du trafic du port WAN, il est préférable de rendre publiques les adresses Internet du port WAN et de maintenir les autres privées. **Figure 2** présente un exemple de double ports WAN configurés avec équilibrage de charge.

Figure 2 Exemple de double ports WAN avec équilibrage de charge



REMARQUE Lors de la configuration de l'équilibrage de charge, vérifiez que vous configurez le type de connectivité des deux ports WAN sur Keep Connection. Si le WAN est configuré pour expirer après une période d'inactivité spécifiée, l'équilibrage de charge ne s'applique pas.

- **Failure Detection :** activez cette fonctionnalité pour autoriser l'appliance de sécurité à détecter la défaillance d'une liaison WAN. Vous pouvez spécifier la méthode de détection. En cas de défaillance, le trafic des liaisons indisponibles est dévié vers la liaison disponible.

  REMARQUE Avant de suivre cette procédure, vous devez configurer la connexion WAN facultative. Voir aussi **Configuration du WAN facultatif, page 55**.

ÉTAPE 1 Cliquez sur **Networking > Optional Port > WAN Mode** ou sur la page Getting Started (Advanced), sous **Secondary WAN Port**, cliquez sur **Configure WAN Mode**.

La fenêtre WAN Mode s'ouvre.

ÉTAPE 2 Dans la zone **Port Mode**, choisissez l'un des modes suivants :

- **Auto-Rollover with Primary port as :** choisissez cette option si vous disposez de deux liaisons FAI et que vous souhaitez en utiliser une comme liaison de secours. Dans la liste déroulante, choisissez le port WAN que vous souhaitez désigner en tant que liaison principale : **Dedicated WAN** ou **Optional WAN**.

  Lorsque le mode Basculement automatique est activé, l'état de la liaison du port WAN principal est vérifié à intervalles réguliers tel que défini par les paramètres de détection de défaillances.

- **Load Balancing :** choisissez cette option si vous disposez de deux liaisons FAI que vous souhaitez utiliser simultanément. Une fois cette procédure achevée en cliquant sur le bouton **Apply**, vous devez configurer les liaisons de protocole. Voir aussi **Configuration des liaisons de protocole pour l'équilibrage de charge, page 62.**

  Si l'appliance de sécurité est configurée en mode Équilibrage de charge, elle vérifie la connexion des deux liaisons à intervalles réguliers pour détecter l'état.

  REMARQUE Vous pouvez cliquer sur le lien **Protocol Bindings** pour afficher, ajouter ou modifier les liaisons de protocole, mais enregistrez d'abord vos paramètres sur cette page.

- **Use only single WAN port :** choisissez cette option si vous êtes connecté à un seul FAI. Sélectionnez également le port WAN connecté à votre FAI : **Dedicated WAN** ou **Optional WAN**. Cette option peut être utile pour résoudre les problèmes de connexion.

ÉTAPE 3 Si vous avez choisi les modes de port Renvoi automatique ou Équilibrage de charge, configurez **WAN Failure Detection Method** :

- **None :** sélectionnez cette option pour ne pas rechercher les défaillances du WAN. Cette option n'est valide que si le mode de port est configuré sur Équilibrage de charge.
- **DNS lookup using WAN DNS Servers :** sélectionnez cette option pour détecter une défaillance sur une liaison WAN à l'aide des serveurs DNS configurés pour port WAN dédié ou facultatif.
- **DNS lookup using these DNS Servers :** sélectionnez cette option pour détecter une défaillance sur une liaison WAN à l'aide des serveurs DNS spécifiés dans les champs ci-dessous.
  - **Dedicated WAN** : saisissez l'adresse IP des serveurs DNS pour le WAN dédié.
  - **Optional WAN** : saisissez l'adresse IP du serveur DNS pour l'interface WAN du port facultatif.
- **Ping these IP addresses :** sélectionnez cette option pour détecter une défaillance WAN à l'aide d'un test ping sur les adresses IP spécifiées dans les champs ci-dessous.
  - **Dedicated WAN** : saisissez une adresse IP valide pour effectuer un test ping à partir du WAN dédié.

- **Optional WAN** : saisissez une adresse IP valide pour effectuer un test ping à partir de l'interface WAN du port facultatif.

- **Retry Interval is :** indiquez la fréquence, en secondes, selon laquelle l'appliance de sécurité doit appliquer la méthode de détection de défaillances configurée ci-dessus.
- **Failover after :** indiquez le nombre de tentatives après lequel le basculement est initialisé.

ÉTAPE 4 Cliquez sur **Apply** pour enregistrer les paramètres.

REMARQUE Étapes suivantes :

- Si vous êtes sur la page Getting Started (Advanced), cliquez sur **Getting Started > Advanced** pour poursuivre la liste des tâches de configuration.
- **Obligatoire pour l'équilibrage de charge :** si vous avez choisi l'option d'équilibrage de charge, cliquez sur **Optional Port > Protocol Bindings** pour configurer vos liaisons de protocole. Pour obtenir plus d'informations, reportez-vous à la section **Configuration des liaisons de protocole pour l'équilibrage de charge, page 62.**

Configuration des liaisons de protocole pour l'équilibrage de charge

Si vous avez choisi le mode de port Équilibrage de charge pour votre WAN optionnel, configurez des liaisons de protocole pour déterminer la manière dont le trafic est équilibré entre les deux liaisons FAI. Cette fonctionnalité vous permet d'identifier le trafic entre les liaisons de vitesse différente. Le trafic de gros volume peut être routé via le port connecté vers une liaison à haut débit et le trafic de faible volume peut être acheminé via le port connecté vers la liaison lente.

Par exemple, vous pouvez contraindre le protocole HTTP au WAN dédié et contraindre le protocole FTP au WAN facultatif. Dans ce scénario, l'appliance de sécurité canalise automatiquement les données FTP via le WAN facultatif. Tout le trafic HTTP est acheminé via le WAN dédié.

REMARQUE Avant de pouvoir entrer les liaisons de protocole, vous devez configurer le port facultatif, la connexion WAN et le mode du port WAN. Pour obtenir plus d'informations, reportez-vous à la section **Configuration du renvoi automatique, de l'équilibrage de charge et de la détection des défaillances, page 59**.

Si vous souhaitez saisir une liaison de protocole pour un service personnalisé, vous devez d'abord ajouter le service personnalisé à la base de données. Voir aussi **Création de services personnalisés, page 108**.

ÉTAPE 1 Cliquez sur **Networking > Optional Port > Protocol Bindings**, ou sur la page Getting Started (Advanced), sous **Secondary WAN Port**, cliquez sur **Configure Protocol Bindings (facultatif - si le mode WAN est défini sur Équilibrage de charge)**.

La fenêtre Protocol Bindings s'ouvre. Toutes les liaisons de protocole existantes sont affichées dans le tableau List of Available Protocol Bindings.

ÉTAPE 2 Cliquez sur **Ajouter.**

Autres options : cliquez sur **Edit** pour modifier une entrée. Pour activer une liaison de protocole, cliquez sur **Enable**. Pour désactiver une liaison de protocole, cliquez sur **Disable**. Pour supprimer une entrée, sélectionnez la case correspondante, puis cliquez sur **Delete**. Pour sélectionner toutes les entrées du tableau, cochez la case située dans la ligne d'en-tête du côté gauche.

Lorsque vous cliquez sur Add ou Edit, la fenêtre Protocol Bindings Configuration s'ouvre.

ÉTAPE 3 Saisissez les informations suivantes :

- **Service :** choisissez un service de la liste.

  L'appliance de sécurité est configurée avec la liste des services standard. Pour obtenir des informations sur l'ajout de vos propres services personnalisés à la liste, consultez **Création de services personnalisés, page 108.**

- **Local Gateway :** choisissez l'interface que vous souhaitez utiliser : **Dedicated WAN** ou **Configured WAN**.

- **Source Network :** pour identifier le réseau source, choisissez **Any**, **Single Address**, or **Address Range**. Si vous choisissez **Single Address**, saisissez l'adresse dans le champ Start Address. Si vous choisissez **Address Range**, saisissez l'adresse de début et l'adresse de fin pour spécifier la plage.

- **Destination Network :** pour identifier le réseau de destination, choisissez **Any**, **Single Address**, or **Address Range**. Si vous choisissez **Single Address**, saisissez l'adresse dans le champ Start Address. Si vous choisissez **Address Range**, saisissez l'adresse de début et l'adresse de fin pour spécifier la plage.

ÉTAPE 4 Cliquez sur **Apply** pour enregistrer les paramètres.

ÉTAPE 5 Lorsque vous êtes prêt, activez les nouvelles liaisons de protocole ajoutées. Une nouvelle liaison de protocole est désactivée jusqu'à ce que vous l'activiez.

Configuration d'un DMZ

Un DMZ (zone de démarcation ou zone démilitarisée) est un sous-réseau qui se trouve derrière le pare-feu mais qui est ouvert au public. En plaçant vos services publics sur un DMZ, vous pouvez ajouter une couche de sécurité supplémentaire au LAN. Le public peut se connecter aux services du DMZ mais ne peut pas pénétrer le LAN. Vous devez configurer votre DMZ afin d'inclure tous les hôtes devant être exposés sur le WAN (tel que le Web ou les serveurs de messagerie).

La configuration DMZ est identique à la configuration LAN. Il n'existe aucune restriction à l'adresse IP ou au sous-réseau attribué au port DMZ, excepté qu'il ne peut pas être identique à l'adresse IP donnée à l'interface LAN de cette passerelle.

Dans ce scénario, l'entreprise dispose d'une adresse IP publique, 209.165.200.225, utilisée pour l'adresse IP publique du routeur et l'adresse IP publique du serveur Web. L'administrateur configure le port facultatif à utiliser comme port DMZ. Une règle de pare-feu autorise le trafic HTTP entrant sur le serveur Web à l'adresse 172.16.2.30. Les utilisateurs Internet peuvent saisir le nom de domaine associé à l'adresse IP 209.165.200.225 et ils sont connectés au serveur Web. La même adresse IP est utilisée pour l'interface WAN.

Figure 3 Exemple d'un DMZ avec une adresse IP publique pour le WAN et le DMZ

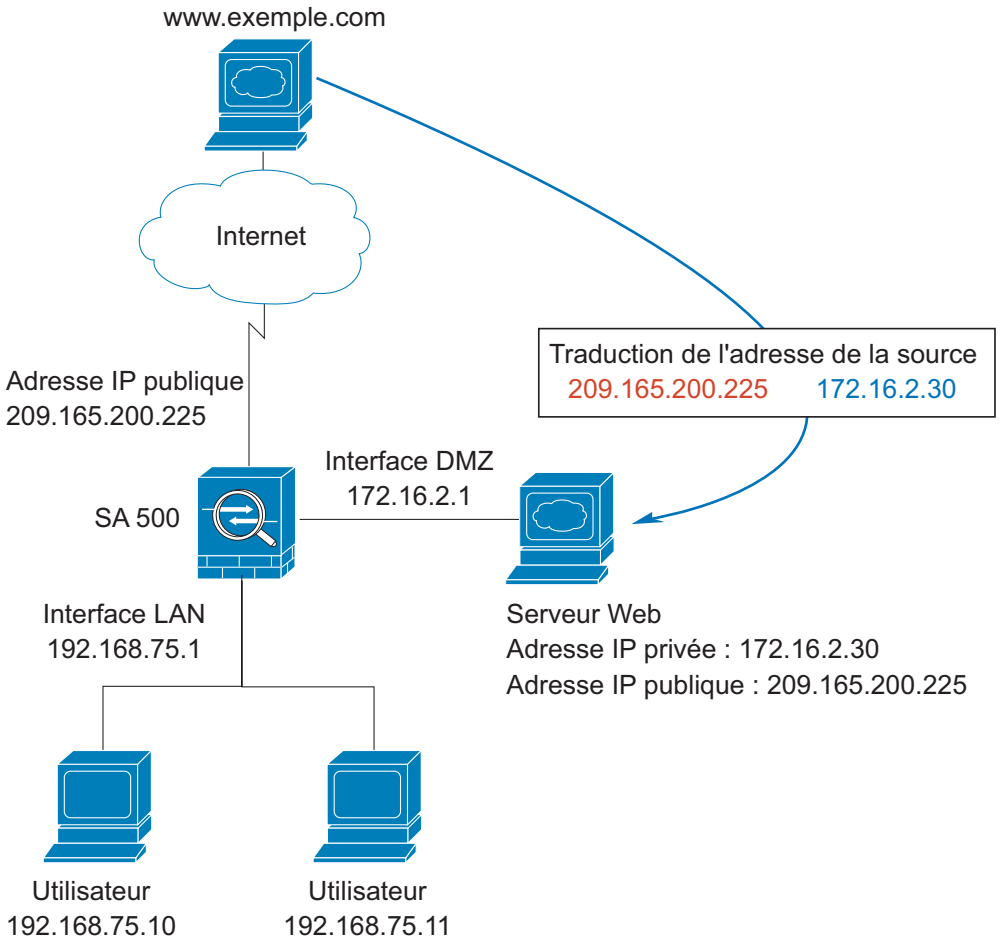
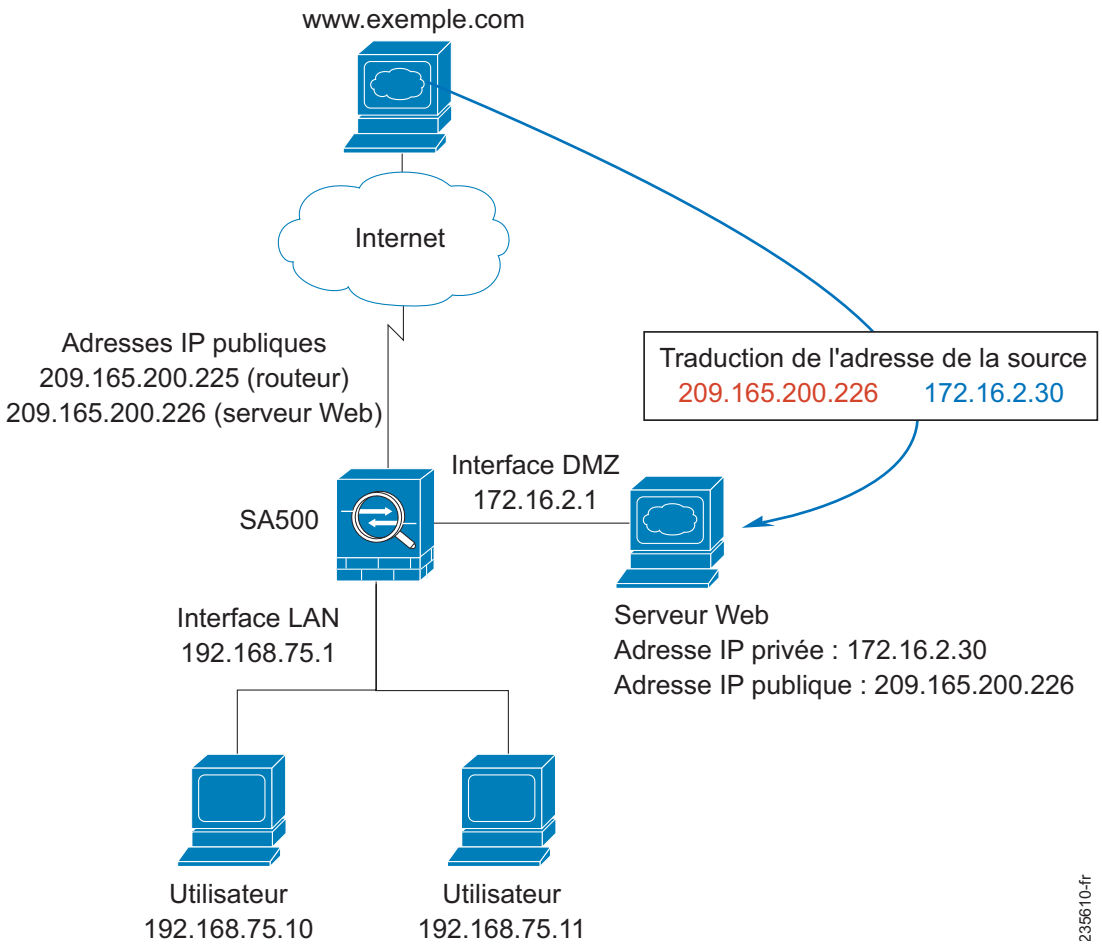


Figure 4 Exemple de DMZ avec deux adresses IP publiques



Dans ce scénario, le FAI a émis deux adresses IP statiques : 209.165.200.225 et 209.165.200.226. L'adresse 209.165.200.225est utilisée pour l'adresse IP publique du routeur. L'administrateur configure le port facultatif à utiliser comme port DMZ et crée une règle de pare-feu pour autoriser le trafic HTTP entrant sur le serveur Web à l'adresse 172.16.2.30. La règle de pare-feu spécifie l'adresse IP externe 209.165.200.226. Les utilisateurs Internet peuvent saisir le nom de domaine associé à l'adresse IP 209.165.200.226 et ils sont connectés au serveur Web.

Configuration des paramètres du DMZ

Suivez cette procédure pour configurer les paramètres de port DMZ, puis créez des règles de pare-feu pour permettre au trafic d'accéder aux services du DMZ.

ÉTAPE 1 Configurez d'abord le port facultatif en tant que DMZ :

a. Cliquez sur **Networking > Optional Port > Optional Port Mode**, ou sur la page Getting Started (Advanced), sous DMZ Port, cliquez sur **Set Optional Port to DMZ mode**.

La fenêtre Optional Port Mode s'ouvre.

b. Choisissez **DMZ**.

c. Cliquez sur **Apply** pour enregistrer les paramètres.

Si vous êtes sur la page Getting Started (Advanced), cliquez sur **Getting Started > Advanced** pour retourner à la liste des tâches de configuration.

ÉTAPE 2 Cliquez sur **Networking > Optional Port > DMZ Config** ou sur la page Getting Started (Advanced), sous **DMZ Port**, cliquez sur **Configure DMZ settings**.

La fenêtre DMZ Configuration s'ouvre.

ÉTAPE 3 Dans la zone **DMZ Port Setup**, saisissez une **adresse IP** et le **masque de sous-réseau** pour le port DMZ sur le réseau interne. Les périphériques sur le réseau DMZ communiquent avec le routeur à l'aide de cette adresse IP. L'adresse IP du DMZ par défaut 172.16.2.1 s'affiche à l'écran.

ÉTAPE 4 Dans la zone **DHCP for DMZ Connected Computers**, saisissez les informations suivantes :

- **DHCP Mode :** sélectionnez l'une des options suivantes :
  - **None :** choisissez cette option si les ordinateurs du DMZ sont configurés avec des adresses IP statiques ou sont configurés pour utiliser un autre serveur DHCP.
  - **DHCP Server :** choisissez cette option pour autoriser l'appliance de sécurité à jouer le rôle d'un serveur DHCP et à attribuer des adresses IP à tous les périphériques connectés au réseau DMZ. Renseignez également les champs signalés par un fond blanc.
  - **DHCP Relay :** choisissez cette option pour autoriser l'appliance de sécurité à utiliser un relais DHCP. Si vous choisissez ce mode, saisissez également l'adresse IP de la passerelle relais.

- **Domain Name (optional) :** saisissez un nom pour le domaine.
- **Starting IP Address** et **Ending IP Address** : saisissez la plage d'adresses du pool d'adresses IP pour cette appliance de sécurité. Tout nouveau client DHCP qui se connecte au DMZ se voit attribuer une adresse IP de cette plage.
- **Primary DNS Server** et **Secondary DNS Server (Optional)** : saisissez l'adresse IP du serveur DNS principal pour le DMZ. Éventuellement, saisissez l'adresse IP d'un serveur DNS secondaire.
- **Primary Tftp Server** et **Secondary Tftp Server (Optional)** : saisissez l'adresse IP des serveurs Tftp principal et secondaire pour le DMZ
- **WINS Server (Optional) :** saisissez l'adresse IP du serveur WINS ou, s'il se trouve dans votre réseau, le serveur NetBios Windows.
- **Lease Time :** saisissez la durée maximale de connexion en heures pendant laquelle une adresse IP dynamique fait « l'objet d'un bail » pour un utilisateur réseau. Lorsque le délai se termine, une nouvelle adresse IP dynamique est automatiquement attribuée à l'utilisateur. La valeur par défaut est de 24 heures.
- **Relay Gateway :** si vous avez choisi le relais DHCPcomme mode DHCP, saisissez l'adresse IP de la passerelle relais.

ÉTAPE 5 Dans la section **DMZ Proxies**, cochez la case pour permettre au DMZ d'agir comme proxy pour toutes les requêtes DNS et pour communiquer avec les serveurs DNS du FAI. Lorsque cette fonction est désactivée, tous les clients DHCP du DMZ reçoivent les adresses IP du serveur DNS du FAI.

ÉTAPE 6 Cliquez sur **Apply** pour enregistrer les paramètres.

REMARQUE Étapes suivantes :

- Si vous êtes sur la page Getting Started (Advanced), cliquez sur **Getting Started > Advanced** pour poursuivre la liste des tâches de configuration.
- **Obligatoire :** vous devez configurer une règle de pare-feu pour autoriser le trafic entrant à accéder à votre DMZ. Utilisez également la règle de pare-feu pour spécifier une adresse IP publique pour un serveur sur votre DMZ, le cas échéant. Pour commencer, cliquez sur **Firewall** dans la barre de menus. Pour obtenir plus d'informations, reportez-vous à la section **Configuration d'une règle de pare-feu pour le trafic entrant, page 114.**

- Si vous souhaitez réserver certaines adresses IP pour des périphériques spécifiés, cliquez sur **Optional port > DMZ Reserved IPs**. Pour obtenir plus d'informations, reportez-vous à la section **IP DMZ réservées, page 69.**
- Si vous souhaitez afficher une liste des clients DHCP DMZ, cliquez sur **Optional Port > DMZ DHCP Clients**. Pour obtenir plus d'informations, reportez-vous à la section **Clients soumis au bail DHCP DMZ, page 70.**

IP DMZ réservées

Si vous avez configuré votre DMZ pour agir en tant que serveur DHCP, vous pouvez réserver certaines adresses IP à attribuer aux périphériques spécifiés. Pour ce faire, ajouter l'adresse matérielle du périphérique, ainsi que l'adresse IP souhaitée, à la liste des IP DMZ réservées. Dès que le serveur DHCP du DMZ reçoit une demande d'un périphérique, l'adresse matérielle est comparée à la base de données. Si l'appareil est détecté, l'adresse IP réservée est utilisée. Sinon, une adresse IP est attribuée automatiquement depuis le pool DHCP.

REMARQUE Avant de pouvoir effectuer cette procédure, vous devez activer le mode de serveur DHCP ou de relais DHCP sur la page DMZ Configuration. Pour obtenir plus d'informations, reportez-vous à la section **Configuration d'un DMZ, page 64**.

ÉTAPE 1 Cliquez sur **Networking > Optional Port > DMZ Reserved IPs**, ou sur la page Getting Started (Advanced), sous **DMZ Port**, cliquez sur **Configure DMZ DHCP Reserved IPs (Optional)**.

La fenêtre DMZ Reserved IPs s'ouvre. Tous les adresses IP existantes réservées du DMZ apparaissent dans le tableau Available DHCP Assigned IPs (DMZ).

REMARQUE Les IP réservées doivent être en dehors du pool d'adresses DHCP pour que le serveur DHCP DMZ les attribue de manière dynamique.

ÉTAPE 2 Cliquez sur **Add.**

Autres options : cliquez sur **Edit** pour modifier une entrée. Pour supprimer une entrée, sélectionnez la case correspondante, puis cliquez sur **Delete**. Pour sélectionner toutes les entrées du tableau, cochez la case située dans la ligne d'en-tête du côté gauche.

Lorsque vous cliquez sur Add ou Edit, la fenêtre DMZ Reserved IPs Configuration s'ouvre.

ÉTAPE 3 Saisissez l'adresse IP et l'adresse MAC.

ÉTAPE 4 Cliquez sur **Apply** pour enregistrer les paramètres.

Clients soumis au bail DHCP DMZ

Cette page affiche une liste des adresses IP attribuées par DHCP et des adresses matérielles des clients du DMZ.

Cliquez sur **Networking > Optional Port > DMZ DHCP Clients**.

Routage

Selon vos besoins, vous pouvez modifier le mode de routage, configurer le routage statique ou configurer le routage dynamique sur votre appliance de sécurité.

- **Routage, page 70**
- **Routage statique, page 71**
- **Routage dynamique, page 72**

Routage

Selon les besoins de votre FAI, vous pouvez configurer l'appliance de sécurité en mode de routage NAT ou en mode de routage classique. Par défaut, le routage NAT est activé.

La traduction d'adresse réseau (NAT) est une technique qui permet à plusieurs ordinateurs sur un LAN de partagé une connexion Internet. Les ordinateurs sur le LAN utilisent une plage d'adresses IP privées alors que le port WAN du routeur est configuré avec une adresse IP publique unique. Outre le partage de connexion, le NAT masque également des adresses IP internes d'ordinateurs sur Internet.

ÉTAPE 1 Cliquez sur **Networking > Routing > Routing**.

La fenêtre Routing Mode s'ouvre.

ÉTAPE 2 Sélectionnez l'une des options suivantes :

- **NAT :** choisissez cette option si votre FAI vous a attribué une seule adresse IP ou si vous partagez des adresses IP sur plusieurs périphériques tels que votre LAN et si vous utilisez les autres périphériques dédiés pour le DMZ. L'option NAT est activée par défaut.
- **Classic Routing :** choisissez cette option si votre FAI a attribué une adresse IP pour chacun des ordinateurs que vous utilisez.

ÉTAPE 3 Cliquez sur **Apply** pour enregistrer les paramètres.

Routage statique

Pour configurer des routes statiques, saisissez un nom de routage et indiquez l'adresse IP et des informations relatives à la destination. Attribuez également une priorité, qui détermine la route à choisir lorsqu'il existe plusieurs routes vers la même destination.

Vous pouvez ajouter des routes statiques pour votre réseau IPv4 ou votre réseau IPv6, si le mode IPv6 est activé.

ÉTAPE 1 Cliquez sur **Networking > Routing > Static**.

La fenêtre Static Routing s'ouvre.

ÉTAPE 2 Cliquez sur **Add** pour ajouter une nouvelle route statique.

Autres options : cliquez sur le bouton **Edit** pour modifier une entrée. Pour supprimer une entrée, sélectionnez la case correspondante puis cliquez sur **Delete**. Pour sélectionner toutes les entrées du tableau, cochez la case située dans la ligne d'en-tête du côté gauche.

Lorsque vous cliquez sur Add ou Edit, la fenêtre Static Routing Configuration s'ouvre.

ÉTAPE 3 Saisissez les informations suivantes :

- **Name :** saisissez un nom à des fins d'identification et de gestion.
- **Active :** cochez cette case pour activer la route, ou décochez la case pour désactiver une route non utilisée mais que vous ne voulez pas supprimer. Une route inactive n'est pas diffusée si le protocole RIP (Routing Information Protocol) est activé.

- **Private :** détermine si la route peut être partagée avec d'autres routeurs si le protocole RIP est activé. Si cette option est sélectionnée, la route ne sera pas partagée dans une diffusion ou une multidiffusion RIP. Cela s'applique uniquement aux routes statiques IPv4.
- **Adresse IP de destination :** saisissez l'adresse IP de l'hôte ou du réseau auquel mène la route.
- **IP Subnet Mask :** saisissez le masque de sous-réseau pour le réseau de destination.
- **Interface :** choisissez dans la liste l'interface réseau physique (WAN dédié, WAN facultatif, DMZ ou LAN), par laquelle cette route est accessible.
- **Adresse IP de la passerelle :** saisissez l'adresse IP du routeur de la passerelle par lequel l'hôte de destination ou le réseau est accessible.
- **Metric :** saisissez un nombre entre 2 et 15 pour gérer la priorité de la route. S'il existe plusieurs routes pour la même destination, la route possédant la mesure la plus petite est choisie.

ÉTAPE 4 Cliquez sur **Apply** pour enregistrer les paramètres.

Routage dynamique

Le routage dynamique ou RIP est un protocole IGP (Interior Gateway Protocol) qui est généralement utilisé dans les réseaux internes. Il permet à un routeur d'échanger ses informations de routage automatiquement avec d'autres routeurs et lui permet de régler de manière dynamique les tables de routage et de s'adapter aux modifications du réseau.

REMARQUE Par défaut, RIP est désactivé.

ÉTAPE 1 Cliquez sur **Networking > Routing > Dynamic**.

La fenêtre Dynamic Routing (RIP) s'ouvre.

ÉTAPE 2 Dans la zone **RIP Configuration**, saisissez les informations suivantes :

- **RIP Direction :** détermine la manière dont le routeur envoie et reçoit des paquets RIP :
  - **Both :** le routeur diffuse sa table de routage et traite les informations RIP reçues des autres routeurs.

- **Out Only :** le routeur diffuse sa table de routage périodiquement mais n'accepte pas les informations RIP des autres routeurs.
- **In Only :** le routeur accepte les informations RIP des autres routeurs, mais ne diffuse pas sa table de routage.
- **None :** le routeur ne diffuse pas sa table de routage et n'accepte aucun paquet RIP des autres routeurs. Cela désactive efficacement le RIP.

▪ **Version RIP :** sélectionnez l'une des options suivantes :

- **Disabled :** si le RIP est désactivé, cette option est sélectionnée.
- **RIP-1** est une version de routage basée sur les classes qui n'inclut pas les informations de sous-réseau. C'est la version la plus souvent prise en charge.
- **RIP-2** comprend toutes les fonctionnalités de RIPv1 et prend en charge les informations de sous-réseau. Bien que les données soient envoyées en format RIP-2 pour RIP-2B et RIP-2M, le mode par lequel les paquets sont envoyés est différent.
- **RIP-2B** diffuse des données dans le sous-réseau entier.
- **RIP-2M** envoie des données aux adresses de multidiffusion.

ÉTAPE 3 Dans la zone **Authentication for RIP 2B/2M**, saisissez les informations suivantes :

▪ **Enabled Authentication for RIP 2B/2M :** cochez cette case pour activer l'authentification pour RIP-2B ou RIP-2M.

▪ **Paramètres de la première clé et paramètres de la deuxième clé**

- **MD5 Key ID :** saisissez l'ID unique de la clé MD-5
- **MD5 Auth Key :** saisissez la clé d'authentification pour cette clé MD5.
- **Not Valid Before :** date de début de la première clé pour l'authentification MD5 entre les routeurs.
- **Not Valid After :** date de fin de la première clé pour l'authentification MD5 entre les routeurs.

ÉTAPE 4 Cliquez sur **Apply** pour enregistrer les paramètres.

Gestion des ports

Vous pouvez activer ou désactiver des ports, définir le mode duplex et la vitesse et activer ou désactiver la mise en miroir des ports. Reportez-vous aux rubriques suivantes.

- **Configuration des ports, page 74**
- **Configuration de SPAN (mise en miroir des ports), page 74**

Configuration des ports

ÉTAPE 1 Cliquez sur **Networking > Port Management > Port Management**.

La fenêtre Port Management s'ouvre.

ÉTAPE 2 Choisissez les options suivantes pour chaque port :

- **Enable :** sélectionnez cette case pour activer le port. Décochez la case pour le désactiver. Par défaut, tous les ports sont activés.
- **Auto :** cochez cette case pour permettre à la passerelle et au réseau de déterminer les paramètres optimaux du port.
- **Duplex :** choisissez semi-duplex ou duplex intégral en fonction de la prise en charge du port. La valeur par défaut est duplex intégral pour tous les ports.
- **Speed :** choisissez la vitesse du port. La valeur par défaut est de 1 000 Mbit/s pour tous les ports.

ÉTAPE 3 Cliquez sur **Apply** pour enregistrer les paramètres.

Configuration de SPAN (mise en miroir des ports)

La mise en miroir des ports, parfois appelée SPAN (Switched Port Analyser), permet au trafic d'un port d'être visible sur un autre port. Cette fonctionnalité peut être utile pour le débogage ou pour la surveillance du trafic par une application externe. Vous pouvez choisir un port LAN pour surveiller le trafic sur tous les autres ports LAN.

ÉTAPE 1 Cliquez sur **Networking > Port Management > SPAN (Port Mirroring)**.

La fenêtre SPAN (Port Mirroring) s'ouvre.

ÉTAPE 2 Saisissez les informations suivantes :

- **Do you want to enable Port Mirroring :** cochez cette case pour activer la mise en miroir des ports.
- **Mirror all LAN Ports to :** choisissez le port LAN qui surveillera tous les autres ports LAN.

ÉTAPE 3 Cliquez sur **Apply** pour enregistrer les paramètres.

Profils de bande passante QoS

Vous pouvez configurer des profils de bande passante de qualité de service (QoS) pour le WAN et le LAN.

Pour le trafic de la zone sécurisée vers la zone non sécurisée, QoS est déterminé en limitant la vitesse et en attribuant une priorité. Pour ce faire, créez des profils de bande passante et attribuez-leur des classes de trafic. Le sélecteur du trafic identifie le flux du trafic qui est soumis au profil de gestion de la bande passante spécifié.

REMARQUE La limitation de bande passante ne s'applique pas à une interface DMZ.

Création des profils de bande passante QoS pour les interfaces WAN

ÉTAPE 1 Cliquez sur **Networking > QoS > WAN QoS**.

La fenêtre Bandwidth Management s'ouvre. Tous les profils existants sont affichés dans le tableau Bandwidth Profiles.

ÉTAPE 2 Pour activer cette fonctionnalité cochez la case qui se trouve au sommet de la page et cliquez sur **Apply**.

ÉTAPE 3 Dans la zone **WAN Configuration**, spécifiez la **Upstream Bandwidth in Kbps** et la **Downstream Bandwidth in Kbps** pour chaque interface WAN en saisissant les valeurs fournie par votre FAI. Cliquez ensuite sur **Apply**.

ÉTAPE 4 Dans la zone **Bandwidth Profiles Enable**, effectuez les opérations suivantes :

- Cochez la case pour activer les profils de bande passante.
- Cliquez sur **Apply** pour enregistrer les paramètres.

ÉTAPE 5 Cliquez sur **Add** pour ajouter un nouveau profil de bande passante.

Autres options : cliquez sur le bouton **Edit** pour modifier une entrée. Pour supprimer une entrée, sélectionnez la case correspondante, puis cliquez sur **Delete**. Pour sélectionner toutes les entrées du tableau, cochez la case située dans la ligne d'en-tête du côté gauche.

Lorsque vous cliquez sur Add ou Edit, la fenêtre Bandwidth Profile Configuration s'ouvre.

ÉTAPE 6 Saisissez les paramètres pour définir un profil de bande passante pour une interface WAN.

- **Profile Name :** saisissez un nom pour identifier ce profil.
- **Priority :** choisissez une priorité : Low, Medium, ou High, Urgent. Vous pouvez utiliser Urgent pour le trafic sensible à la latence tel que la voix. Il est recommandé de configurer un seul profil de bande passante avec la priorité Urgent.
- **Maximum Bandwidth :** saisissez la bande passante maximale à associer à ce profil.
- **Minimum Bandwidth :** saisissez la bande passante minimale à associer à ce profil.
- **WAN Interface :** choisissez l'interface à laquelle ce profil de bande passante s'applique.

ÉTAPE 7 Cliquez sur **Apply** pour enregistrer les paramètres.

ÉTAPE 8 Répétez aussi souvent que nécessaire pour créer des profils supplémentaires.

Sélecteurs de trafic

Une fois le profil de bande passante créé, vous pouvez l'associer au flux du trafic.

REMARQUE Avant de pouvoir créer des sélecteurs de trafic, vous devez activer les profils de bande passante et créer au moins un profil de bande passante. Pour obtenir plus d'informations, reportez-vous à la section **Création des profils de bande passante QoS pour les interfaces WAN, page 75.**

ÉTAPE 1 Cliquez sur **Networking > Bandwidth Profiles > Traffic Selectors**.

La fenêtre Traffic Selectors s'ouvre. Tous les sélecteurs de trafic existants sont répertoriés dans le tableau List of Traffic Selectors.

ÉTAPE 2 Cliquez sur **Add** pour ajouter un nouveau sélecteur de trafic.

Autres options : cliquez sur le bouton **Edit** pour modifier une entrée. Pour supprimer une entrée, sélectionnez la case correspondante puis cliquez sur **Delete**. Pour sélectionner toutes les entrées du tableau, cochez la case située dans la ligne d'en-tête du côté gauche.

Lorsque vous cliquez sur Add ou Edit, la fenêtre Traffic Selector Configuration s'ouvre.

ÉTAPE 3 Saisissez les informations suivantes :

- **Available Profiles :** sélectionnez le profil de bande passante qui doit s'appliquer à ce trafic.
- **Service :** choisissez un service dans la liste déroulante. Si aucun service ne convient, vous pouvez configurer un service personnalisé sur la page Firewall custom services.
- **Traffic Selector Match Type :** choisissez la méthode d'identification de l'hôte auquel doit s'appliquer le sélecteur de trafic. Saisissez ensuite **l'adresse IP**, **l'adresse MAC**, **le nom de port** ou**le VLAN** en fonction du type de correspondance choisie.

ÉTAPE 4 Cliquez sur **Apply** pour enregistrer les paramètres.

QoS du LAN

L'appliance de sécurité fournit des valeurs de classe de service (CoS) IEEE 802.1p basé sur QoS et des valeurs DSCP pour la mise en œuvre de la qualité de service au niveau du contrôle d'accès multimédia. Cette méthode QoS spécifie les valeurs de priorité pouvant être utilisées pour différencier le trafic et donner la préférence au trafic prioritaire, par exemple les appels téléphoniques.

Activation de QoS LAN

ÉTAPE 1 Cliquez sur **Networking > QoS > LAN QoS**.

ÉTAPE 2 Pour activer la qualité de service sur les ports LAN, cochez la case située en haut de la page. Décochez la case pour désactiver cette option.

ÉTAPE 3 Pour chaque port, choisissez le type de valeur à utiliser pour classer le trafic. Vous pouvez choisir DSCP, qui est un champ IP de couche 3, ou CoS, qui est un champ d'en-tête Ethernet de couche 2, selon vos besoins.

ÉTAPE 4 Cliquez sur **Apply** pour enregistrer les paramètres.

Mappage CoS de port

Utilisez la page Port CoS Mapping pour mapper chaque valeur CoS à une file d'attente hiérarchisée QoS.

ÉTAPE 1 Cliquez sur **Networking > Qos > Port CoS Mapping**.

La fenêtre Port CoS Mapping s'ouvre.

ÉTAPE 2 Pour chaque **valeur CoS**, utilisez la liste déroulante pour choisir la **file d'attente hiérarchisée** correspondante : **Lowest**, **Low**, **Medium** ou **High**.

ÉTAPE 3 Cliquez sur **Apply** pour enregistrer les paramètres.

Mappage DSCP de port

Utilisez la page Port DSCP Mapping pour mapper chaque valeur DSCP à une file d'attente hiérarchisée QoS.

ÉTAPE 1 Cliquez sur **Networking > Qos > Port DSCP Mapping**.

La fenêtre Port DSCP Mapping s'ouvre.

ÉTAPE 2 Pour chaque valeur DSCP, utilisez la liste déroulante pour choisir **la file d'attente** correspondante : **Lowest**, **Low**, **Medium** ou **High**.

ÉTAPE 3 Cliquez sur **Apply** pour enregistrer les paramètres.

Nouveau marquage DSCP

DSCP est un champ dans un paquet IP qui permet d'attribuer différents niveaux de service au trafic réseau. Utilisez la page Remark CoS to DSCP pour mapper les valeurs CoS aux valeurs DSCP.

ÉTAPE 1 Cliquez sur **Networking > Remark CoS to DSCP**.

La fenêtre Remark CoS to DSCP s'ouvre.

ÉTAPE 2 Pour chaque valeur CoS, utilisez la liste déroulante pour choisir la valeur DSCP correspondante :

ÉTAPE 3 Cliquez sur **Apply** pour enregistrer les paramètres.

DNS dynamique

Le DNS dynamique (DDNS) est un service Internet qui permet aux routeurs possédant des adresses IP publiques variables d'être localisés à l'aide de noms de domaine Internet. Si votre FAI ne vous a pas fourni d'adresse IP statique et que votre connexion WAN est configurée pour utiliser le protocole DHCP pour obtenir une adresse IP de manière dynamique, alors DDNS vous permet de disposer d'une adresse IP statique virtuelle pour votre site Web. Pour utiliser le DDNS, vous devez configurer un compte avec un fournisseur DDNS tel que DynDNS.com.

ÉTAPE 1 Cliquez sur **Networking > Dynamic DNS**.

La fenêtre Dynamic DNS s'ouvre.

ÉTAPE 2 Dans la zone **WAN Mode**, le mode WAN actuel est affiché.

ÉTAPE 3 Dans la zone **Dedicated WAN (DDNS Status)** ou **Optional WAN (DDN Status)**, saisissez les informations suivantes :

- **Select the Dynamic DNS Service :** choisissez None ou DynDNS.com.
- **Host and Domain Name :** indiquez le nom d'hôte et le nom de domaine complets pour le service DDNS.
- **User Name :** saisissez le nom d'utilisateur du compte DynDNS.
- **Password:** saisissez le mot de passe du compte DynDNS.
- **Use wildcards :** cochez cette case pour permettre à tous les sous-domaines de votre nom d'hôte DynDNS de partager la même IP publique en tant que nom d'hôte. Cette option peut être activée à cet endroit si elle ne l'a pas déjà été sur le site Web DynDNS.
- **Update every 30 days :** cochez cette case pour autoriser l'appliance de sécurité à mettre à jour les informations d'hôte sur DynDNS et à maintenir l'abonnement actif après la période d'évaluation de 30 jours.

ÉTAPE 4 Cliquez sur **Apply** pour enregistrer les paramètres.

Configuration de l'adressage IPv6

Internet Protocol Version 6 (IPv6) est un nouveau protocole IP conçu pour remplacer IPv4, le protocole Internet majoritairement déployé et intensivement utilisé dans le monde entier. IPv6 multiplie par quatre le nombre de bits des adresses réseau de 32 bits (IPv4) à 128 bits, permettant ainsi un espace d'adresse considérablement plus grand. Vous pouvez configurer l'appliance de sécurité pour la prise en charge de l'adressage IPv6 sur le LAN et le WAN dédié.

REMARQUE IPv6 n'est pas pris en charge sur le port facultatif.

Activez d'abord le mode IPv6 puis configurez la connexion WAN, la connexion LAN, le routage et la tunnellisation.

- **Mode de routage IP**
- **Configuration de la connexion WAN IPv6**
- **Configuration du LAN IPv6**
- **Pools d'adresses LAN IPv6**
- **Multi-LAN IPv6**

- **Routage statique IPv6**
- **Routage (RIPng)**
- **Tunnellisation 6to4**
- **État des tunnels IPv6**
- **Tunnels ISATAP**
- **Tunnels MLD**
- **Configuration des annonces du routeur**
- **Ajouter des préfixes RADVD**

Mode de routage IP

Pour la mise en route de la configuration IPv6, activez d'abord le mode IPv4 ou IPv6. Les adressages IPv4 et IPv6 sont pris en charge.

ÉTAPE 1 Cliquez sur **Networking > IPv6 > Routing Mode**.

La fenêtre Routing Mode s'ouvre.

ÉTAPE 2 Cliquez sur **IPv4/IPv6 mode** pour activer l'adressage IPv6 ou cliquez sur **IPv4 only mode** pour activer uniquement l'adressage IPv4.

ÉTAPE 3 Cliquez sur **Apply** pour enregistrer les paramètres.

ÉTAPE 4 Lorsque l'avertissement un « An IP Mode change will cause the device to reboot » s'affiche, cliquez sur **OK** pour continuer. Si vous ne souhaitez pas modifier le mode IP, cliquez sur **Cancel**.

REMARQUE Étapes suivantes :

- Pour configurer la connexion WAN, cliquez sur **IPv6 > IPv6 WAN Config**. Pour obtenir plus d'informations, reportez-vous à la section **Configuration de la connexion WAN IPv6, page 82**.
- Pour configurer le LAN, cliquez sur **IPv6 > IPv6 LAN Config**. Pour obtenir plus d'informations, reportez-vous à la section **Configuration du LAN IPv6, page 83**.

Configuration de la connexion WAN IPv6

Par défaut, lorsque vous activez le mode IPv6, votre appliance de sécurité est configurée pour être un client DHCPv6 du FAI, avec une configuration automatique sans état. Si votre FAI a attribué une adresse IPv6 statique, ou si vous devez modifier le mode de configuration automatique DHCP, configurez les paramètres sur cette page.

ÉTAPE 1 Cliquez sur **Networking > IPv6 > IPv6 WAN Config**.

La fenêtre IPv6 WAN Configuration s'ouvre.

ÉTAPE 2 Dans la zone **Internet(IPv6) Address**, choisissez **Static IPv6** si votre prestataire de service a attribué une adresse IP fixe (statique ou permanente). Si vous n'avez pas reçu d'adresse IP statique, choisissez **DHCPv6**.

ÉTAPE 3 Si vous configurez une adresse IP statique, saisissez les informations suivantes dans la zone **Static IP Address** de la page.

- **IPv6 Address :** saisissez l'adresse IP statique fournie par votre fournisseur d'accès.
- **IPv6 Prefix Length :** le réseau IPv6 (sous-réseau) est identifié par les bits initiaux de l'adresse, le préfixe. Tous les hôtes du réseau possèdent des bits initiaux identiques pour leur adresse IPv6. Saisissez le nombre de bits initiaux commun dans les adresses réseau. La longueur du préfixe par défaut est 64.
- **Default IPv6 Gateway :** saisissez l'adresse IPv6 de la passerelle pour votre FAI. Elle est généralement fournie par le FAI ou votre administrateur réseau.
- **Primary DNS Server** et **Secondary DNS Server** : saisissez l'adresse IP valide d'un serveur DNS principal et éventuellement d'un serveur DNS secondaire.

ÉTAPE 4 Si vous devez modifier le mode de configuration automatique DHCPv6, choisissez le mode dans la zone **DHCPv6** de la page **:**

- **Stateless Address Auto Configuration :** si vous choisissez cette option, l'appliance de sécurité peut générer ses propres adresses à l'aide d'une combinaison des informations disponibles localement et des informations annoncées par les routeurs.
- **Stateful Address Auto Configuration :** si vous choisissez cette option, l'appliance de sécurité se connecte au serveur DHCPv6 du FAI pour obtenir un bail d'adresse.

ÉTAPE 5 Cliquez sur **Apply** pour enregistrer les paramètres.

REMARQUE Étapes suivantes :

Pour configurer le LAN, cliquez sur **IPv6 > IPv6 LAN Config**. Pour obtenir plus d'informations, reportez-vous à la section **Configuration du LAN IPv6, page 83**.

Configuration du LAN IPv6

En mode IPv6, le serveur DHCP du LAN est activé par défaut (identique au mode IPv4). Le serveur DHCPv6 sert des adresses IPv6 à partir de pools d'adresses configurés avec la longueur du préfixe IPv6 attribuée au LAN. Pour obtenir plus d'informations, reportez-vous à la section **Pools d'adresses LAN IPv6, page 85.**

ÉTAPE 1 Cliquez sur **Networking > IPv6 > IPv6 LAN Config**.

La fenêtre IPv6 LAN Configuration s'ouvre.

ÉTAPE 2 Dans la section **LAN TCP/IP Settings**, saisissez les informations suivantes :

- **IPv6 Address :** saisissez l'adresse IPv6. L'adresse IPv6 par défaut pour la passerelle est fec0::1. Vous pouvez modifier cette adresse IPv6 de 128 bits en fonction des besoins de votre réseau.

  REMARQUE Si vous modifiez l'adresse IP et que vous cliquez sur **Apply**, la connexion du navigateur est perdue. Attendez quelques secondes que votre ordinateur d'administration obtienne une nouvelle adresse IP du pool d'adresses IP nouvellement attribué (ou qu'il libère et renouvelle son adresse si connecté via DHCP). Saisissez ensuite la nouvelle adresse IP de l'appliance de sécurité dans la barre d'adresse du navigateur, puis connectez-vous à nouveau.

- **IPv6 Prefix Length :** saisissez le nombre de caractères du préfixe IPv6.

  Le réseau IPv6 (sous-réseau) est identifié par le préfixe, constitué des bits initiaux de l'adresse. La longueur de préfixe par défaut est de 64 bits. Tous les hôtes du réseau possèdent des bits initiaux identiques pour l'adresse IPv6. Le nombre de bits initiaux communs dans les adresses est défini par le champ de longueur du préfixe.

ÉTAPE 3 Dans la zone **DHCPv6**, saisissez les informations suivantes :

- **DHCP Status :** si vous ne voulez pas que l'appliance de sécurité fasse office de serveur DHCP, cliquez sur **Disable DHCPv6 Server** (paramètre par défaut). Si vous souhaitez que l'appliance de sécurité fasse office de serveur DHCP qui attribue de manière dynamique des adresses IP à tous les périphériques connectés, cliquez sur **Enable DHCPv6 Server**, puis renseignez tous les champs signalés par un fond blanc.
- **DHCP Mode :** choisissez l'option appropriée à votre configuration :
  - **Stateless :** sélectionnez cette option pour autoriser l'appliance de sécurité à configurer automatiquement les hôtes LAN IPv6 à l'aide des messages de détection du routeur ICMPv6. Il n'y a aucune adresse gérée utilisée par les nœuds du LAN.

    REMARQUE Pour le mode sans état, vous devez également configurer le RADVD (Router Advertisement Daemon). Voir aussi **RADVD (Router Advertisement Daemon), page 91.**
  - **Stateful :** choisissez cette option pour autoriser l'hôte LAN IPv6 à compter sur un serveur DHCPv6 externe pour fournir des paramètres de configuration obligatoires.
- **Domain Name (optional) :** saisissez un nom de domaine pour le serveur DHCPv6.
- **Server Preference :** saisissez une valeur comprise entre 0 et 255 pour indiquer le niveau de préférence pour ce serveur DHCP. Les clients DHCPv6 choisiront le serveur DHCPv6 qui a la plus forte valeur de préférence. La valeur par défaut est 255.
- **DNS Servers :** sélectionnez l'une des options suivantes :
  - **Use DNS Proxy :** cochez cette case pour activer le proxy DNS sur ce LAN. L'appliance de sécurité fera office de proxy pour toutes les requêtes DNS et communiquera avec les serveurs DNS du FAI (tel que configuré dans la page WAN settings).
  - **Use DNS from ISP :** cochez cette case pour permettre au FAI de définir les serveurs DNS (principal et secondaire) pour le client DHCP du LAN.
  - **Use below :** cochez cette case pour utiliser le serveur DNS principal et le serveur DNS secondaire indiqués dans les champs ci-dessous.
- **Lease/Rebind Time :** saisissez le nombre de secondes pendant lesquelles les adresses IP sont louées aux clients. La valeur par défaut est 86 400, qui correspond à 24 heures.

ÉTAPE 4 Cliquez sur **Apply** pour enregistrer les paramètres.

REMARQUE Étapes suivantes :

- **Required for stateless autoconfiguration :** si vous choisissez le mode de configuration automatique sans état, cliquez sur **IPv6 > Router Advertisement** pour configurer le RADVD (Router Advertisement Daemon). Pour obtenir plus d'informations, reportez-vous à la section **RADVD (Router Advertisement Daemon), page 91**.
- Si vous voulez configurer les pools d'adresses LAN, cliquez sur **IPv6 > IPv6 Address Pools**. Pour obtenir plus d'informations, reportez-vous à la section **Pools d'adresses LAN IPv6, page 85**.
- Si vous devez configurer une adresse LAN alias, cliquez sur **IPv6 > IPv6 Multi LAN**. Pour obtenir plus d'informations, reportez-vous à la section **Multi-LAN IPv6, page 86**.
- Si vous devez configurer un routage statique, cliquez sur **IPv6 > IPv6 Multi LAN**. Pour obtenir plus d'informations, reportez-vous à la section **Routage statique IPv6, page 87**.

Pools d'adresses LAN IPv6

Vous pouvez définir le préfixe de délégation IPv6 pour une plage d'adresses IP à utiliser par le serveur DHCPv6. Le préfixe de délégation vous permet d'automatiser le processus de communication à d'autres équipements de mise en réseau sur le LAN des informations DHCP du préfixe attribué.

ÉTAPE 1 Cliquez sur **Networking > IPv6 > IPv6 Address Pools**.

La fenêtre IPv6 Address Pools s'ouvre. Tous les pools d'adresses existants sont répertoriés dans le tableau List of Available Pools.

ÉTAPE 2 Cliquez sur **Add** pour créer un nouveau pool d'adresses.

Autres options : cliquez sur le bouton **Edit** pour modifier une entrée. Pour supprimer une entrée, sélectionnez la case correspondante puis cliquez sur **Delete**. Pour sélectionner toutes les entrées du tableau, cochez la case située dans la ligne d'en-tête du côté gauche.

Lorsque vous cliquez sur Add ou Edit, la fenêtre IPv6 Address Prefix & Pools Configuration s'ouvre.

ÉTAPE 3 Saisissez les informations suivantes :

- **Start IPv6 Address :** saisissez la première adresse de la plage d'adresses pour ce pool.
- **End IPv6 Address :** saisissez la dernière adresse de la plage d'adresses pour ce pool.
- **IPv6 Prefix Length :** saisissez le nombre de caractères du préfixe IPv6.

  Le réseau IPv6 (sous-réseau) est identifié par le préfixe, constitué des bits initiaux de l'adresse. Tous les hôtes du réseau possèdent des bits initiaux identiques pour l'adresse IPv6. Le nombre de bits initiaux communs dans les adresses est défini par le champ de longueur du préfixe.

ÉTAPE 4 Cliquez sur **Apply** pour enregistrer les paramètres.

Multi-LAN IPv6

Cette page vous permet de configurer une adresse LAN IPv6 alias.

ÉTAPE 1 Cliquez sur **Networking > IPv6 > IPv6 Multi LAN**.

La fenêtre IPv6 Multi LAN s'ouvre. Toutes les adresses alias existantes sont répertoriées dans le tableau Available Multi IPv6 Addresses.

ÉTAPE 2 Cliquez sur **Add** pour ajouter une nouvelle adresse.

Autres options : cliquez sur le bouton **Edit** pour modifier une entrée. Pour supprimer une entrée, sélectionnez la case correspondante puis cliquez sur **Delete**. Pour sélectionner toutes les entrées du tableau, cochez la case située dans la ligne d'en-tête du côté gauche.

Lorsque vous cliquez sur Add ou Edit, la fenêtre IPv6 Multi LAN Configuration s'ouvre.

ÉTAPE 3 Saisissez les informations suivantes :

- **IPv6 Address :** saisissez l'adresse LAN IPv6 alias à ajouter.
- **Prefix Length :** saisissez la longueur du préfixe de l'adresse IPv6.

Le réseau IPv6 (sous-réseau) est identifié par le préfixe, constitué des bits initiaux de l'adresse. Tous les hôtes du réseau possèdent des bits initiaux identiques pour l'adresse IPv6. Le nombre de bits initiaux communs dans les adresses est défini par le champ de longueur du préfixe.

ÉTAPE 4 Cliquez sur **Apply** pour enregistrer les paramètres.

Routage statique IPv6

ÉTAPE 1 Cliquez sur **Networking > IPv6 > IPv6 Static Routing**.

La fenêtre IPv6 Static Routing s'ouvre. Toutes les routes statiques existantes sont répertoriées dans le tableau IPv6 Static Routes.

ÉTAPE 2 Cliquez sur **Add** pour ajouter une nouvelle route statique. **Autres options :** cliquez sur le bouton **Edit** pour modifier une entrée. Pour supprimer une entrée, sélectionnez la case correspondante puis cliquez sur **Delete**. Pour sélectionner toutes les entrées du tableau, cochez la case située dans la ligne d'en-tête du côté gauche.

Lorsque vous cliquez sur Add ou Edit, la fenêtre IPv6 Static Route Configuration s'ouvre.

ÉTAPE 3 Saisissez les informations suivantes :

- **Route Name :** saisissez le nom d'une route à des fins d'identification et de gestion.
- **Active :** cochez cette case pour activer la route ou décochez-la pour désactiver la route. Lorsqu'une route est ajoutée pendant l'état inactif, elle est répertoriée dans le tableau mais ne sera pas utilisée pour le routage. Cette fonctionnalité vous permet de configurer les routes avant même que le réseau de destination soit prêt à recevoir le trafic. Activez les routes si disponible.
- **IPv6 Destination :** saisissez l'adresse IPv6 de l'hôte de destination ou du réseau pour cette route.
- **IPv6 Prefix Length :** saisissez le nombre de bits du préfixe de l'adresse IPv6 pour définir le sous-réseau.
- **Interface :** choisissez l'interface réseau physique (WAN dédié, WAN facultatif, DMZ ou LAN), par laquelle cette route est accessible.

- **Gateway IP Address :** saisissez l'adresse IP de la passerelle par laquelle l'hôte de destination ou le réseau est accessible.
- **Metric :** spécifiez la priorité de cette route en saisissant une valeur comprise entre 2 et 15. S'il existe plusieurs routes vers la même destination, l'appliance de sécurité choisit la route avec la mesure la plus petite.

ÉTAPE 4 Cliquez sur **Apply** pour enregistrer les paramètres.

Routage (RIPng)

RIPng (Routing Information Protocol - nouvelle génération, RFC 2080) est un protocole de routage qui utilise des paquets UDP pour échanger des informations de routage via le port 521. La distance à une destination est mesurée par le nombre de sauts, de la façon suivante :

- Le nombre de sauts d'un routeur à un réseau directement connecté est 0.
- Le nombre de sauts entre deux routeurs directement connectés est 1.
- Lorsque le nombre de sauts est supérieur ou égal à 16, le réseau ou l'hôte de destination est injoignable.

Par défaut, la mise à jour du routage est envoyée toutes les 30 secondes. Si l'appliance de sécurité ne reçoit aucune mise à jour du routage d'un voisin au bout de 180 secondes, les routes apprises par le voisin sont considérées comme injoignables. Au bout de 240 secondes, si aucune mise à jour du routage n'est reçue, l'appliance de sécurité supprime ces routes de la table de routage.

REMARQUE RIPng est désactivé par défaut.

ÉTAPE 1 Cliquez sur **Networking > IPv6 > Routing (RIPng)**.

La fenêtre Routing (RIPng) s'ouvre.

ÉTAPE 2 Cochez la case **Enable RIPNG** pour activer RIPng. Décochez-la, pour désactiver ce protocole.

ÉTAPE 3 Cliquez sur **Apply** pour enregistrer les paramètres.

Tunnellisation 6to4

La tunnellisation automatique permet au trafic d'un réseau LAN IPv6 à être tunnellisé via un réseau WAN IPv4, et vice versa. Vous devez activer cette fonctionnalité si vous disposez d'un site ou un utilisateur terminal qui doit se connecter à Internet IPv6 à l'aide du réseau IPv4 existant.

ÉTAPE 1 Cliquez sur **Networking > IPv6 > 6to4 Tunneling**.

La fenêtre 6to4 Tunneling s'ouvre.

ÉTAPE 2 Cochez la case pour activer la tunnellisation automatique ou décochez-la pour la désactiver.

ÉTAPE 3 Cliquez sur **Apply** pour enregistrer les paramètres.

État des tunnels IPv6

Cette page vous permet d'afficher des informations sur le tunnel automatique configuré via l'interface WAN dédiée. Le tableau présente deux champs : le nom du tunnel et l'adresse IPv6 créée sur le périphérique.

Pour ouvrir cette page, cliquez sur **Networking > IPv6 > IPv6 Tunnels Status**.

Tunnels ISATAP

Le protocole ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) est utilisé pour transmettre des paquets IPv6 entre les nœuds dual-stack sur un réseau IPv4. L'appliance de sécurité est un point de terminaison (un nœud) pour le tunnel. Vous devez définir un point de terminaison local ainsi que le préfixe de sous-réseau ISATAP qui définit le sous-réseau ISATAP logique pour configurer un tunnel.

ÉTAPE 1 Cliquez sur **Networking > IPv6 > ISATAP Tunnels**.

La fenêtre **ISATAP Tunnels** s'ouvre. Tous les tunnels existants sont répertoriés dans le tableau List of Available ISATAP Tunnels.

ÉTAPE 2 Pour ajouter un tunnel ISATAP, cliquez sur **Add**.

Autres options : cliquez sur le bouton **Edit** pour modifier une entrée. Pour supprimer une entrée, sélectionnez la case correspondante puis cliquez sur **Delete**. Pour sélectionner toutes les entrées du tableau, cochez la case située dans la ligne d'en-tête du côté gauche.

Lorsque vous cliquez sur Add ou Edit, la fenêtre ISATAP Tunnel Configuration s'ouvre.

ÉTAPE 3 Saisissez les informations suivantes :

- **ISATAP Subnet Prefix :** saisissez le préfixe 64 bit de sous-réseau qui est attribué au sous-réseau ISATAP logique pour l'intranet. Vous pouvez obtenir le préfixe de votre FAI ou du registre Internet ou en le dérivant de RFC 4193.
- **Local End Point Address :** saisissez l'adresse du point de terminaison pour le tunnel qui démarre avec ce routeur. Le point de terminaison peut être l'interface LAN (en supposant que le LAN est un réseau IPv4) ou une adresse IPv4 LAN spécifique.
- **IPv4 Address :** saisissez l'adresse du point de terminaison local à défaut de l'adresse IPv4 LAN.

ÉTAPE 4 Cliquez sur **Apply** pour enregistrer les paramètres.

Tunnels MLD

Le MLD (Multicast Listener Discovery) est un protocole IPv6 qui détecte des écouteurs pour un groupe de multidiffusion spécifique. Ce protocole est similaire à IGMPdans IPv4.

ÉTAPE 1 Cliquez sur **Networking > IPv6 > MLD Tunnels**.

La fenêtre MLD Tunnels s'ouvre.

ÉTAPE 2 Cochez la case pour activer MLD lorsque ce routeur est en mode IPv6. Saisissez ensuite les informations suivantes :

- **Maximum query response time :** saisissez la durée maximale (en millisecondes) qui peut s'écouler entre le moment où le routeur envoie un message de requête à l'hôte et le moment où l'hôte répond à ce message. En variant l'intervalle de réponse aux requêtes, un administrateur peut contrôler les rafales de messages MLD sur la liaison ; des valeurs plus grandes diminuent les salves de trafic, car les réponses de l'hôte sont étendues sur un intervalle plus long. La valeur minimale de ce paramètre est de 5 000 ms (5 secondes) et la valeur maximale est de 1 800 000 ms (30 minutes).

- **Robustness Variable :** saisissez une valeur comprise entre 2 et 8 pour autoriser le réglage des pertes de paquets attendues sur une liaison. Saisissez une valeur supérieure si une liaison avec pertes est attendue. La valeur par défaut est 2. La valeur minimale de la variable Robustness est 2 et la valeur maximale est 8.
- **Query Interval :** saisissez le nombre de secondes écoulées entre les requêtes générales envoyées par le périphérique. La valeur par défaut est de 125 secondes. En variant l'intervalle entre les requêtes, un administrateur peut contrôler le nombre de messages MLD sur la liaison ; des valeurs plus grandes entraînent un ralentissement dans les envois de requêtes MLD. La valeur minimale de l'intervalle de requêtes est de 100 secondes et la valeur maximale est de 1 800 secondes.

ÉTAPE 3 Cliquez sur **Apply** pour enregistrer les paramètres.

RADVD (Router Advertisement Daemon)

Si vous avez configuré l'appliance de sécurité pour utiliser le mode IPv4/IPv6, vous pouvez configurer le RADVD (Router Advertisement Daemon) sur ce périphérique. Le RADVD écoute les sollicitations du routeur sur le LAN IPv6 et répond par des annonces au routeur selon les besoins. Il s'agit de la configuration automatique sans état IPv6 car elle distribue des préfixes IPv6 à tous les nœuds sur le réseau.

Configurez d'abord RADVD puis ajoutez vos préfixes RADVD comme décrit dans les sections suivantes :

- **Configuration des annonces du routeur**
- **Ajouter des préfixes RADVD**

Configuration des annonces du routeur

Cette page vous permet d'activer RADVD et de choisir le mode d'annonce.

ÉTAPE 1 Cliquez sur **Networking > IPv6 > Router Advertisement**.

La fenêtre RADVD s'ouvre.

ÉTAPE 2 Saisissez les informations suivantes :

- RADVD Status : active ou désactive le processus RADVD. Si vous activez RADVD, renseignez les champs signalés par un fond blanc.

- Advertise Mode : sélectionnez l'une des options suivantes :
  - Unsolicited Multicast : sélectionnez cette option pour envoyer des annonces du routeur à toutes les interfaces appartenant au groupe de multidiffusion. Saisissez également l'annonce interne.
  - Unicast only : sélectionnez cette option pour restreindre les annonces aux adresses IPv6 connues (les annonces sont envoyées uniquement à l'interface de l'adresse connue).
- Advertise Interval : si vous avez choisi le mode de multidiffusion non sollicitée, saisissez une valeur comprise entre les intervalles d'annonce du routeur minimal et maximal. MinRtrAdvInterval = 0,33 * MaxRtrAdvInterval. La valeur par défaut est 30 secondes.
- RA Flags : sélectionnez l'une des options suivantes :
  - **Managed :** choisissez cette option pour utiliser le protocole administré ou d'état intégral pour la configuration automatique des adresses.
  - **Other :** choisissez cette option pour permettre à l'hôte d'utiliser le protocole administré ou d'état intégral pour la configuration automatique d'autres informations (c.-à-d. différentes des adresses).
- Router Preference : choisissez **Low, Medium ou High** pour la préférence relative au processus RADVD de ce routeur. Ce paramètre est utile s'il existe d'autres périphériques compatibles RADVD sur le LAN. Le paramètre par défaut est High.
- MTU : si votre FAI le demande, vous pouvez modifier cette valeur, qui est utilisée dans les annonces pour vérifier que tous les nœuds sur le réseau utilisent la même valeur MTU dans les cas où le MTU LAN n'est pas connu. La valeur par défaut est 1500.
- Router Lifetime : saisissez la durée de vie en secondes de la route. La valeur par défaut est 3600 secondes.

ÉTAPE 3 Cliquez sur **Apply** pour enregistrer les paramètres.

Ajouter des préfixes RADVD

REMARQUE Avant de pouvoir suivre cette procédure, vous devez activer RADVD. Pour obtenir plus d'informations, reportez-vous à la section **Configuration des annonces du routeur, page 91**.

ÉTAPE 1 Cliquez sur **Networking > IPv6 > Advertisement Prefixes**.

La fenêtre Advertisement Prefixes s'ouvre. Tous les préfixes existants sont indiqués dans le tableau List of Prefixes to Advertise.

ÉTAPE 2 Pour ajouter un préfixe au tableau, cliquez sur **Add**.

Autres options : cliquez sur le bouton **Edit** pour modifier une entrée. Pour supprimer une entrée, sélectionnez la case correspondante puis cliquez sur **Delete**. Pour sélectionner toutes les entrées du tableau, cochez la case située dans la ligne d'en-tête du côté gauche.

Lorsque vous cliquez sur Add ou Edit, la fenêtre RADVD Prefixes s'ouvre.

ÉTAPE 3 Saisissez les informations suivantes :

- **IPv6 Prefix Type :** choisissez le type de préfixe **6to4** ou **Global/Local/ISATAP**. Renseignez également les champs signalés par un fond blanc.
- **ID de SLA** : l'ID de SLA (Site-Level Aggregation Identifier) du préfixe de l'adresse 6to4 est défini sur l'ID de l'interface sur laquelle les annonces sont envoyées.
- **IPv6 Prefix :** spécifiez l'adresse réseau IPv6.
- **IPv6 Prefix Length :** saisissez une valeur décimale qui indique le nombre de bits contigus d'ordre supérieur de l'adresse qui composent la partie de l'adresse relative au réseau.
- **Prefix Lifetime :** saisissez le nombre maximum de secondes pendant lesquelles le routeur demandeur peut utiliser le préfixe.

ÉTAPE 4 Cliquez sur **Apply** pour enregistrer les paramètres.

3

Configuration sans fil pour le SA520W

Ce chapitre décrit la procédure de configuration des points d'accès et du réseau radio pour le SA520W. Il comprend les sections suivantes :

- **Configuration d'un point d'accès**
- **Configuration du réseau radio**

REMARQUE Le routeur est configuré avec les paramètres par défaut d'un réseau sans fil simple. Toutefois, vous devez activer le point d'accès pour qu'un périphérique sans fil puisse se connecter.

Configuration d'un point d'accès

Par défaut, votre SA520W est configuré avec un point d'accès appelé AP1, dont le nom de réseau par défaut est Cisco_1. Le point d'accès est activé par défaut. Le profil de sécurité est défini sur Open et s'identifie à tous les périphériques sans fil qui sont à portée. Ces paramètres facilitent l'utilisation de votre réseau sans fil. Toutefois, pour des raisons de sécurité, nous vous recommandons vivement de configurer chaque profil avec le plus haut niveau de sécurité pris en charge par les périphériques sans fil que vous souhaitez autorisés dans votre réseau.

Vous pouvez créer plusieurs points d'accès pour segmenter le LAN sans fil dans plusieurs domaines de diffusion. Cette configuration vous permet de garder un meilleur contrôle sur le trafic de diffusion, qui affecte les performances réseau. Pour chaque point d'accès, vous pouvez personnaliser le mode de sécurité, les paramètres de qualité de service et les paramètres radio.

Étape 1 : configuration des profils sans fil

Un profil sans fil spécifie les paramètres de sécurité. Éventuellement, vous pouvez configurer des paramètres sans fil avancés, des paramètres de qualité de service et le filtrage MAC. Après avoir configuré un profil sans fil, vous pouvez l'attribuer à tout point d'accès.

REMARQUE Cisco recommande fortement WPA2 pour la sécurité sans fil. Les autres modes de sécurité sont vulnérables aux attaques.

ÉTAPE 1 Cliquez sur **Wireless > Profiles**.

La fenêtre Profiles s'ouvre. Les profils existants sont affichés dans le tableau List of Profiles.

ÉTAPE 2 Dans la première ligne du tableau, cliquez sur le bouton de la colonne **Edit** pour configurer le profil par défaut.

Autres options : cliquez sur **Add** pour ajouter une entrée. Cliquez sur le bouton de la colonne **Adv Config**, **QoS Config** ou **Configure MAC Filter** pour modifier d'autres paramètres (plus d'informations seront présentées ultérieurement dans ce chapitre). Pour supprimer un profil, cochez la case correspondante, puis cliquez sur **Delete**. Pour sélectionner toutes les entrées, sélectionnez la case de la première colonne de l'en-tête du tableau.

Lorsque vous cliquez sur Add ou Edit, la fenêtre Profile Configuration s'ouvre.

ÉTAPE 3 Saisissez les informations suivantes dans la zone **Profile Configuration** :

- **Profile Name :** s'il s'agit d'un nouveau profil, saisissez un identifiant (alphanumérique) unique pour ce profil sans fil. S'il s'agit du profil par défaut, le nom default1 ne peut pas être modifié.
- **Security :** choisissez le type de sécurité à configurer dans ce profil :
  - **OPEN :** aucune sécurité. Tous les périphériques sans fil peuvent se connecter (soumis à la stratégie de point d'accès ACL).
  - **WEP (Wired Equivalent Privacy) :** le cryptage WEP est une ancienne méthode de cryptage qui n'est pas considérée comme sûre et qui peut aisément être piratée. Ne sélectionnez cette option que si vous voulez autoriser l'accès aux périphériques ne prenant pas en charge WPA ou WPA2.
  - **WPA (Wi-Fi Protected Access) :** le cryptage WPA offre une meilleure sécurité que le protocole WEP grâce à un cryptage par clé dynamique. Cette norme a été mise en œuvre comme mesure intermédiaire pour

remplacer le WEP, en attendant la finalisation totale de la norme 802.11i pour le WPA2. WPA prend en charge le cryptage TKIP ou TKIP+CCMP (par défaut, TKIP) et l'authentification PSK/RADIUS. Choisissez cette option si vous devez autoriser l'accès à des périphériques ne prenant pas en charge WPA2.

- **WPA2 :** WPA2 fournit la meilleure sécurité en matière de transmissions sans fil. Cette méthode met en œuvre les normes de sécurité spécifiées dans la version finale de 802.11i. WPA2 prend en charge le cryptage CCMP ou CCMP+TKIP (par défaut, CCMP) et l'authentification PSK/RADIUS. WPA2 est recommandé, bien que certains périphériques ne prennent pas en charge ce mode de sécurité. Pour protéger vos informations à mesure de leur transmission sur les ondes, vous devez activer le plus haut niveau de cryptage pris en charge par votre équipement réseau.
- **WPA + WPA2 :** ce mode permet aux clients WPA et WPA2 de se connecter simultanément. Choisissez cette option pour activer un plus haut niveau de sécurité tout en autorisant l'accès aux périphériques qui ne prennent pas en charge WPA2.

- **Encryption :** sélectionnez la méthode de cryptage à utiliser. Pour WPA, les options disponibles sont TKIP ou TKIP+CCMP. Pour WPA2, les options disponibles sont CCMP ou CCMP+TKIP. CCMP est plus fort que TKIP et il est donc recommandé. Toutefois, certains périphériques sans fil peuvent ne prendre en charge que TKIP.
- **Authentication :** pour WPA/WPA2, sélectionnez la méthode d'authentification WPA/WPA2 à utiliser : RADIUS, PSK ou PSK + RADIUS.
- **WPA Password :** pour l'authentification PSK, saisissez une clé prépartagée. La clé peut comprendre jusqu'à 64 caractères ASCII. Les clients doivent aussi être configurés avec le même mot de passe.
- **Enable Pre-Authentication :** si vous choisissez RADIUS comme méthode d'authentification, vous pouvez cocher cette case pour activer la pré-authentification pour ce profil.
- **AP Isolation :** cochez cette case pour créer un réseau virtuel distinct pour les clients qui utilisent ce profil. Lorsque cette fonctionnalité est activée, chaque client se trouve dans son propre réseau virtuel et ne peut pas communiquer avec d'autres clients.

ÉTAPE 4 Si vous avez choisi WEP comme type de sécurité, saisissez les informations suivantes dans la zone **WEP Index and Keys** :

- **Authentication :** sélectionnez le schéma **Open System** ou **Shared Key**. Shared key est recommandé.
- **Encryption :** sélectionnez le type de cryptage (WEP 64 ou WEP 128). Les clés de plus grande taille fournissent un meilleur cryptage, la clé est plus difficile à pirater (c.-à-d. WEP 64 possède une clé de 40 bits qui est moins sûre que la clé de 104 bits de WEP 128).
- **WEP Passphrase :** choisissez une expression alphanumérique (de 8 caractères minimum pour une sécurité optimale) et cliquez sur **Generate key** pour générer 4 clés WEP uniques. Sélectionnez l'une des quatre comme clé statique que les périphériques doivent avoir afin d'utiliser le réseau sans fil.
- **WEP Key 1-4 :** si l'expression WEP n'est pas spécifiée, vous pouvez saisir une clé directement dans l'une des cases WEP Key. La longueur de la clé doit comprendre 5 caractères ASCII (ou 10 caractères hexadécimaux) pour une clé WEP de 64 bits et 13 caractères ASCII (ou 26 caractères hexadécimaux) pour une clé WEP de 128 bits.
- **WEP Key Index :** l'index de clé WEP dépend de la case de clé WEP utilisée. Le schéma de numérotation de l'index peut être différent en fonction des clients. Pour les clients dont l'indexation commence par 0, les clés WEP 1 à 4 correspondent aux index 0 à 3. Pour ceux dont l'indexation commence par 1, les clés WEB 1 à 4 correspondent aux index 1 à 4.

ÉTAPE 5 Cliquez sur **Apply** pour enregistrer les paramètres.

ÉTAPE 6 Répétez cette procédure autant que nécessaire pour ajouter d'autres profils sans fil.

REMARQUE Étapes suivantes :

- **Required for each access point :** configurez et activez le point d'accès. Voir aussi **Étape 2 : configuration des points d'accès, page 102**.
- Si vous devez configurer les paramètres avancés, cliquez sur le bouton **Advanced Config** dans le tableau List of Profiles. Pour obtenir plus d'informations, reportez-vous à la section **Configuration avancée du profil, page 98.**
- Si vous devez configurer les paramètres QoS, cliquez sur le bouton **QoS Config** dans le tableau List of Profiles. Pour obtenir plus d'informations,

reportez-vous à la section **Configuration des paramètres de qualité de service pour un profil sans fil, page 99.**

- Si vous voulez configurer le filtrage MAC, cliquez sur le bouton **MAC Filtering** dans le tableau List of Available Access Points. Pour obtenir plus d'informations, reportez-vous à la section **Contrôle de l'accès sans fil par le biais des adresses MAC, page 100.**
- Pour l'authentification RADIUS, configurez les paramètres RADIUS. Voir aussi **Configurer les enregistrements du serveur RADIUS, page 207**.

Configuration avancée du profil

ÉTAPE 1 Cliquez sur **Wireless > Profiles**.

La fenêtre Profiles s'ouvre. Les profils existants sont affichés dans le tableau List of Profiles.

ÉTAPE 2 Recherchez le profil que vous souhaitez modifier, puis cliquez sur le bouton de la colonne **Adv Config**.

La fenêtre Profile Advanced Configuration s'ouvre.

ÉTAPE 3 Selon vos besoins, modifiez les paramètres suivants :

- **Group Key Refresh Interval (Seconds) :** indique l'intervalle de temps après lequel les clés de groupe sont générées (utilisé uniquement si le profil est configuré avec une sécurité WPA ou WPA2).
- **PMKSA Life Time (Seconds) :** la norme de sécurité WPA2 propose l'option PMKSA caching qui permet de mettre en cache pendant un certain temps les clés principales dérivées d'une authentification RADIUS réussie afin d'éviter la répétition de cette authentification RADIUS longue à chaque connexion du client. Cet intervalle de temps d'expiration spécifie la durée de stockage de cette PMKSA dans le point d'accès. Si un client se reconnecte pendant cet intervalle (après une authentification RADIUS réussie), il peut ignorer l'authentification RADIUS.
- **802.1X Re-authentication Interval (Seconds) :** intervalle de temps après lequel le point d'accès doit authentifier à nouveau par le biais du serveur RADIUS.

ÉTAPE 4 Cliquez sur **Apply** pour enregistrer les paramètres.

Configuration des paramètres de qualité de service pour un profil sans fil

La qualité de service (QoS) est utilisée pour hiérarchiser les différents types de trafic. Elle permet d'accorder des priorités distinctes à des applications, des utilisateurs ou des flux de données distincts ou bien d'assurer un certain niveau de performances à un flux de données. Les paramètres de qualité de service par défaut sont généralement suffisants, mais les utilisateurs expérimentés peuvent mapper les valeurs DSCP/ToS aux classes de service, selon leurs besoins.

Vous avez le choix entre quatre files d'attente de classes de service pour hiérarchiser le trafic de données sur la liaison sans fil :

- **Voice :** file d'attente avec priorité supérieure, délai minimal. Généralement utilisé pour envoyer des données limitées dans le temps telles que la voix sur IP (VoIP).
- **Video :** file d'attente avec haute priorité, délai minimal. Généralement utilisé pour envoyer des données limitées dans le temps telles que la vidéo et d'autres flux de contenu multimédia.
- **Best Effort :** file d'attente avec priorité moyenne, débit et délai moyens. Les données IP les plus traditionnelles sont envoyées vers cette file d'attente.
- **Background :** file d'attente avec priorité inférieure, haut débit. Les données de masse qui nécessitent un débit maximal et ne dépendent pas du temps sont généralement envoyées vers cette file d'attente (données FTP, par exemple).

ÉTAPE 1 Cliquez sur **Wireless > Profiles**.

La fenêtre Profiles s'ouvre. Les profils existants sont affichés dans le tableau List of Profiles.

ÉTAPE 2 Recherchez le profil que vous souhaitez modifier, puis cliquez sur le bouton de la colonne **QoS Config**.

La fenêtre QoS Configuration s'ouvre.

ÉTAPE 3 Saisissez les paramètres suivants.

- **QoS Enable :** cochez cette case pour activer le QoS pour ce profil. Les paramètres de cette page s'appliquent uniquement si cette case est cochée.
- **Default Class Of Service :** utilisez ce paramètre pour spécifier la classe de service par défaut pour tout le trafic sur le point d'accès.

- **IP DSCP/TOS to Service Mapping :** pour chaque valeur IP DSCP/TOS, gardez le paramètre **Default** dans le champ pour appliquer la classe de service sélectionnée par défaut ou choisissez une classe de service particulière pour hiérarchiser le trafic.

ÉTAPE 4 Cliquez sur **Apply** pour enregistrer les paramètres.

Contrôle de l'accès sans fil par le biais des adresses MAC

Cette page vous permet de définir les adresses MAC spécifiques auxquelles accorder ou refuser l'accès au point d'accès sélectionné. La valeur par défaut est accès « ouvert », ce qui signifie que le filtrage MAC n'est pas activé. Tous les périphériques peuvent utiliser ce point d'accès.

Le filtrage MAC fournit une sécurité supplémentaire, mais il augmente également la complexité et la maintenance. Veillez à saisir chaque adresse MAC correctement pour que la stratégie soit appliquée comme prévu.

Avant d'effectuer cette procédure, décidez si vous souhaitez saisir une liste d'adresses auxquelles accorder ou refuser l'accès. Généralement il est plus facile et plus sûr d'utiliser cette fonctionnalité pour autoriser l'accès aux adresses MAC spécifiées, refusant de ce fait l'accès aux adresses MAC inconnues.

Saisissez d'abord les adresses MAC dans la table d'adresses MAC, puis définissez l'état de la stratégie ACL.

IMPORTANT : chaque fois que vous ajoutez ou supprimez des adresses de la table d'adresses MAC, cliquez sur le bouton **Apply** pour enregistrer vos paramètres. La stratégie s'applique uniquement aux adresses qui sont dans le tableau lorsque vous cliquez sur **Apply**.

ÉTAPE 1 Cliquez sur **Wireless > Access Point**.

La fenêtre Access Points s'ouvre. Les points d'accès existants sont répertoriés dans le tableau List of Available Access Points.

ÉTAPE 2 Recherchez le point d'accès que vous souhaitez modifier, puis cliquez sur le bouton de la colonne **Configure MAC Filter**.

La fenêtre MAC Filtering Configuration s'ouvre.

ÉTAPE 3 Pour ajouter une adresse à la table d'adresses MAC, effectuez les tâches suivantes :

a. Cliquez sur **Add.**

Cliquez sur le bouton **Edit** pour modifier une entrée. Pour supprimer une entrée, sélectionnez la case correspondante, puis cliquez sur **Delete**. Pour sélectionner toutes les entrées, sélectionnez la case de la première colonne de l'en-tête du tableau. Après avoir apporté des modifications dans le tableau, veillez à cliquez sur **Apply** pour appliquer la stratégie ACL à la nouvelle liste.

Lorsque vous cliquez sur Add ou Edit, la fenêtre New MAC Filter s'ouvre.

b. Saisissez l'**adresse MAC** du périphérique que vous souhaitez ajouter à la table.

c. Cliquez sur **Apply** pour enregistrer les paramètres.

ÉTAPE 4 Répétez l'étape précédente pour chaque adresse MAC que vous souhaitez ajouter à la table.

ÉTAPE 5 En haut de la page MAC Filtering, définissez la valeur de **ACL Policy Status**. Choisissez l'une des options suivantes dans la liste :

- **Open :** le filtrage MAC n'est pas activé. Tous les périphériques peuvent utiliser ce point d'accès.
- **Allow :** tous les périphériques de la table d'adresses MAC peuvent utiliser ce point d'accès. Les autres périphériques n'y ont pas accès.
- **Deny :** l'accès à ce point d'accès est refusé à tous les périphériques de la table d'adresses MAC. Tous les autres périphériques y ont accès.

ÉTAPE 6 Cliquez sur **Apply** pour enregistrer les paramètres.

Étape 2 : configuration des points d'accès

Utilisez la page Access Point pour configurer jusqu'à quatre points d'accès à votre réseau sans fil. Pour chaque point d'accès, attribuez un profil, spécifiez un SSID (Service Set Identifier) ou un nom de réseau, définissez le nombre maximum de clients et, éventuellement, spécifiez un planning.

ÉTAPE 1 Cliquez sur **Wireless > Access Point**.

La fenêtre Access Points s'ouvre. Les points d'accès existants sont répertoriés dans le tableau List of Available Access Points.

ÉTAPE 2 Dans la première ligne du tableau, cliquez sur le bouton de la colonne **Edit** pour configurer le point d'accès par défaut.

Autres options : cliquez sur **Add** pour ajouter une entrée. Pour afficher l'état, cliquez sur le bouton de la colonne **Status**. Pour activer un point d'accès, cochez la case puis cliquez sur **Enable**. Pour désactiver un point d'accès, cochez la case puis cliquez sur **Disable**. Pour supprimer un point d'accès, cochez la case puis cliquez sur **Delete**. Pour sélectionner tous les points d'accès, sélectionnez la case de la première colonne de l'en-tête du tableau.

Lorsque vous cliquez sur Add ou Edit, la fenêtre Access Point Configuration s'ouvre.

ÉTAPE 3 Saisissez les informations suivantes :

- **Profile Name :** choisissez un profil qui détermine la sécurité et les paramètres avancés facultatifs pour ce point d'accès. Pour obtenir plus d'informations, reportez-vous à la section **Étape 1 : configuration des profils sans fil, page 95.**
- **Active Time :** cochez cette case pour activer le point d'accès uniquement durant des heures déterminées de la journée. Puis saisissez l'heure de début et l'heure de fin.
  - **Start Time :** saisissez l'heure et les minutes de démarrage de la période active. choisissez AM ou PM dans la liste déroulante.
  - **Stop Time :** saisissez l'heure et les minutes de fin de la période active. choisissez AM ou PM dans la liste déroulante.
- **Max Associated Clients :** saisissez le nombre maximum de clients qui peuvent se connecter à ce point d'accès à tout moment. La valeur par défaut est de 8 clients.

- **SSID :** spécifiez le SSID (Service Set Identifier), ou le nom de réseau, que les clients utilisent pour se connecter au point d'accès. Il est conseillé de remplacer le SSID par défaut par un identifiant unique.
- **Broadcast SSID :** sélectionnez cette case pour autoriser l'appliance de sécurité à diffuser le SSID. Tous les périphériques sans fil à portée peuvent voir le SSID lorsqu'ils recherchent des réseaux disponibles. Décochez cette case pour empêcher la détection automatique du SSID. Dans ce cas, les utilisateurs doivent connaître le SSID pour paramétrer une connexion sans fil à ce point d'accès.

ÉTAPE 4 Cliquez sur **Apply** pour enregistrer les paramètres.

ÉTAPE 5 Répétez cette procédure autant que nécessaire pour ajouter ou modifier d'autres points d'accès dans votre SA520W.

REMARQUE Étapes suivantes :

Pour afficher l'état du point d'accès, cliquez sur le bouton du tableau List of Available Access Points. Pour obtenir plus d'informations, reportez-vous à la section **Page Wireless Statistics for the SA520W, page 224.**

Configuration du réseau radio

Configuration radio de base

La carte radio est préconfigurée avec des paramètres standard. Utilisez cette page pour modifier les paramètres, si nécessaire.

Par exemple, vous pouvez définir un canal manuel pour résoudre les problèmes d'interférences avec d'autres points d'accès de la zone. Vous pouvez également modifier le mode (g & b, g only, n only, ng) en fonction des périphériques de votre réseau.

ÉTAPE 1 Cliquez sur **Wireless > Radio Settings > Radio Settings**.

La fenêtre Radio Settings s'ouvre.

ÉTAPE 2 Saisissez les informations suivantes :

- **Region :** choisissez une zone géographique dans la liste déroulante des régions.
- **Country :** sélectionnez un pays dans la liste déroulante des pays. Cette liste s'adapte en fonction de la région sélectionnée. Cela détermine les canaux Wi-Fi™ disponibles comme spécifié par les autorités du réseau sans fil du pays ou de la région correspondante.
- **Mode :** choisissez la technique de modulation 802.11.
  - **g & b :** sélectionnez ce mode si certains périphériques du réseau sans fil utilisent 802.11g et que d'autres utilisent 802.11b.
  - **g only :** sélectionnez ce mode si tous les périphériques du réseau sans fil peuvent prendre en charge 802.11g.
  - **n only :** sélectionnez ce mode si tous les périphériques du réseau sans fil peuvent prendre en charge 802.11n.
  - **ng :** sélectionnez ce mode pour permettre aux clients 802.11n, 802.11g et 802.11b de se connecter à ce point d'accès.
- **Channel Spacing :** sélectionnez une agrégation (espacement) de canaux de 20 MHz ou 40 MHz ou choisissez « auto » pour laisser le système déterminer le meilleur espacement de canal à utiliser. Ce paramètre est propre au trafic 802.11n.
- **Control Side Band :** si vous avez choisi l'espacement de canal de 40 MHz, choisissez Lower Upper.
- **Current Channel :** affiche le canal actuellement utilisé par la radio.
- **Channel :** choisissez un canal dans la liste des canaux ou choisissez « auto » pour laisser le système déterminer le meilleur canal à utiliser en fonction des niveaux de bruit environnemental des canaux disponibles.
- **Default Transmit Power :** saisissez une valeur en dBm comme niveau de puissance transmis par défaut pour tous les points d'accès qui utilisent cette radio. La valeur par défaut est de 20 dBm.

ÉTAPE 3 Cliquez sur **Apply** pour enregistrer les paramètres.

Page Advanced Radio Settings

Cette page est utilisée pour définir les paramètres de configuration avancés pour la radio.

ÉTAPE 1 Cliquez sur **Wireless > Radio Settings > Advanced Settings**.

La fenêtre Advanced Radio Settings s'ouvre.

ÉTAPE 2 Saisissez les informations suivantes :

- **Beacon Interval :** les intervalles de trame sont transmis à intervalles réguliers par un point d'accès pour annoncer l'existence du réseau sans fil. Définissez l'intervalle en saisissant une valeur en millisecondes. La valeur par défaut est 100, ce qui signifie que les trames de balise sont envoyées toutes les 100 millisecondes (10 secondes).
- **Dtim Interval :** le message DTIM (Delivery Traffic Information Map) est un élément inclus dans certaines trames de balise. Il indique les stations client qui se trouvent actuellement en veille en mode bas-régime et qui ont stocké des données en attente d'utilisation dans la mémoire tampon sur le point d'accès. Définissez l'intervalle en saisissant une valeur en trames de balise. La valeur par défaut est 2, ce qui signifie que le message DTIM est inclus dans chaque deuxième trame de balise.
- **RTS Threshold :** détermine la taille de paquet qui nécessite l'établissement d'une liaison RTS (Request To Send) ou CTS (Clear To Send) avant envoi. Un paramètre de seuil bas peut être utile dans les zones où de nombreux périphériques client s'associent au périphérique sans fil ou dans les zones où les clients sont éloignés et qu'ils ne peuvent détecter que le point d'accès et non les autres clients. Bien qu'une valeur de seuil faible consomme davantage de bande passante et réduise le débit du paquet, les paquets RTS fréquents peuvent permettre un rétablissement du réseau suite à une interférence ou à des collisions. Définissez le seuil en saisissant la taille de paquet en octets. La valeur par défaut est 2346, ce qui désactive le RTS de manière efficace.
- **Fragmentation Threshold :** longueur des trames qui nécessitent que les paquets soient cassés (fragmentés) en deux ou trois trames. Une valeur minimale peut réduire les collisions car ces dernières se produisent plus fréquemment lors de la transmission de longues trames, lesquelles occupent le canal plus longtemps. Utilisez un paramètre bas dans les zones où la communication est médiocre ou dans les zones où il existe de nombreuses interférences radio. Définissez le seuil en saisissant la longueur de trame en octets. La valeur par défaut est 2346, ce qui désactive la fragmentation de manière efficace.

- **Preamble mode :** 802.11b nécessite qu'un préambule soit annexé à chaque trame avant sa transmission radio. Le préambule peut être le préambule long traditionnel, qui requiert 192 µs pour la transmission, ou un préambule court facultatif qui nécessite 96 µs seulement. Le préambule long est nécessaire pour la compatibilité avec les anciens systèmes 802.11 fonctionnant à 1 et 2 Mbits/s. La valeur par défaut est Long.
- **Protection Mode :** sélectionnez **RTS/CTS protection** si vous voulez que l'appliance de sécurité établisse une liaison RTS ou CTS avant d'émettre un paquet. Ce mode peut réduire les collisions entre les stations masquées.
- **U-APSD :** cochez cette case pour économiser la consommation électrique en activant la fonctionnalité Unscheduled Automatic Power Save Delivery (également appelée WMM Power Save).
- **Short Retry Limit**, **Long Retry Limit :** saisissez le nombre de fois qu'une appliance de sécurité doit retenter la transmission d'une trame qui échoue. Les nouvelles tentatives sont utilisées pour les trames longues et courtes, de taille inférieure ou égale au seuil RTS.

ÉTAPE 3 Cliquez sur **Apply** pour enregistrer les paramètres.

4

Configuration du pare-feu

Ce chapitre décrit comment configurer les règles de pare-feu qui contrôlent le trafic entrant et sortant, et comment définir d'autres paramètres pour protéger votre réseau. Il comprend les sections suivantes :

- **Configuration des règles de pare-feu pour contrôler le trafic entrant et sortant**
- **Attribution de priorité aux règles de pare-feu**
- **Exemples de configuration de règles de pare-feu**
- **Utilisation d'autres outils pour éviter les attaques, limiter les accès et contrôler le trafic entrant**
- **SIP**

Pour accéder aux pages relatives aux pare-feux, cliquez sur *Firewall* dans la barre de menu de l'utilitaire de configuration.

Configuration des règles de pare-feu pour contrôler le trafic entrant et sortant

Par défaut, le pare-feu bloque le trafic entrant et autorise le trafic sortant. Pour autoriser le trafic entrant ou bloquer le trafic sortant, vous devez configurer des règles de pare-feu. Vous pouvez choisir comment et à qui appliquer les règles, et définir les paramètres suivants :

- Services ou types de trafic (exemples : navigation Web, VoIP, autres services standard et services personnalisés que vous définissez)
- Sens du trafic
- Jours de la semaine et heures du jour
- Mots-clés dans un nom de domaine ou l'URL d'une page Web

- Adresses MAC des périphériques
- Déclenchement de port

Cette section inclut les sujets suivants :

- **Tâches préliminaires pour les règles de pare-feu**
- **Configuration de la stratégie sortante par défaut**
- **Configuration d'une règle de pare-feu pour le trafic sortant**
- **Configuration d'une règle de pare-feu pour le trafic entrant**

REMARQUE Pour des exemples détaillés, reportez-vous à la **Exemples de configuration de règles de pare-feu, page 119**.

Tâches préliminaires pour les règles de pare-feu

Selon les paramètres de pare-feu que vous souhaitez appliquer, vous devrez peut-être effectuer ces tâches avant de pouvoir configurer la règle de pare-feu :

- Si vous souhaitez créer des règles qui s'appliquent aux services personnalisés, commencez par créer les enregistrements pour les services. Voir aussi **Création de services personnalisés, page 108**.
- Si vous souhaitez créer des règles qui s'appliquent uniquement aux jours et aux heures spécifiés, commencez par créer les plannings. Voir aussi **Création des plannings pour les règles d'un pare-feu, page 109.**
- Pour les règles de pare-feu, vous souhaitez peut-être utiliser des adresses IP publiques supplémentaires (généralement attribuées par votre FAI) autres que l'adresse IP configurée sur l'interface WAN. Voir aussi **Configuration des alias IP pour les interfaces WAN, page 110.**

Création de services personnalisés

L'appliance de sécurité est configurée avec une longue liste de services standard qui vous permettent de configurer les règles de pare-feu et les règles de transfert de port. (Voir **Annexe B, « Services standard ».**) Si vous devez configurer une règle de pare-feu pour un service qui n'est pas dans la liste standard, commencez par identifier le service : entrez un nom, spécifiez son type et attribuez la plage de ports.

ÉTAPE 1 Cliquez sur **Firewall > Firewall > Services** ou sur la page Getting Started (Advanced), sous **Firewall and NAT Rules**, cliquez sur **Configure Custom Services**.

La fenêtre Custom Services s'ouvre. Tous les services personnalisés existants apparaissent dans le tableau List of Available Custom Services.

ÉTAPE 2 Pour ajouter un service personnalisé, cliquez sur **Add**.

Autres options : cliquez sur le bouton **Edit** pour modifier une entrée. Pour supprimer une entrée, sélectionnez la case correspondante, puis cliquez sur **Delete**. Pour sélectionner toutes les entrées, sélectionnez la case dans la première colonne de l'en-tête du tableau. Pour sélectionner toutes les entrées, sélectionnez la case dans la première colonne de l'en-tête du tableau.

Une fois que vous avez cliqué sur Add ou Edit, la fenêtre Custom Services s'ouvre.

ÉTAPE 3 Saisissez les informations suivantes :

- **Name :** saisissez un nom pour ce service.
- **Type :** spécifiez le protocole.
  - Si vous choisissez ICMP ou ICMPv6, entrez également le type ICMP.
  - Si vous choisissez TCP ou UDP, indiquez également la plage de ports en entrant les ports de départ et de fin.

ÉTAPE 4 Cliquez sur **Apply** pour enregistrer les paramètres.

Si vous utilisez la page Getting Started (Advanced), cliquez sur **Getting Started > Advanced** pour afficher la liste des tâches de configuration sous **Firewall and NAT Rules**.

Création des plannings pour les règles d'un pare-feu

Vous pouvez créer un planning et l'appliquer à une ou plusieurs règles de pare-feu. Par exemple, pour créer une règle de pare-feu qui s'applique uniquement le week-end, vous pouvez créer un planning appelé Week-end qui est actif les journées du samedi et dimanche.

Pour plus d'informations sur les paramètres horaires de votre appliance de sécurité, voir **Configurer les paramètres de date/heure, page 197**.

ÉTAPE 1 Cliquez sur **Firewall > Firewall > Schedules**, ou sur la page Getting Started (Advanced), sous Firewall and NAT Rules, cliquez sur **Configure Schedules (Optional)**.

La fenêtre Firewall Schedules s'ouvre. Tous les plannings existants apparaissent dans le tableau List of Available Schedules.

ÉTAPE 2 Pour créer un planning, cliquez sur **Add**.

Autres options : cliquez sur le bouton **Edit** pour modifier une entrée. Pour supprimer une entrée, sélectionnez la case correspondante, puis cliquez sur **Delete**. Pour sélectionner toutes les entrées, sélectionnez la case dans la première colonne de l'en-tête du tableau. Pour sélectionner toutes les entrées, sélectionnez la case dans la première colonne de l'en-tête du tableau.

Lorsque vous cliquez sur Add ou Edit, la fenêtre Schedules s'ouvre.

ÉTAPE 3 Saisissez les informations suivantes :

- **Schedule Name :** saisissez un nom pour le planning. Ce nom apparaît dans la liste déroulante Select Schedule de la page Firewall Rule Configuration.
- **Scheduled Days :** dans la liste déroulante, sélectionnez **All Days** ou **Specific Days**. Si vous sélectionnez **Specific Days**, indiquez également les jours pour ce planning.
- **Schedule Time of Day :** dans la liste déroulante, sélectionnez **All Day** ou **Specific Times**. Si vous choisissez **Specific Times**, indiquez également les valeurs **Start Time** et **End Time** en entrant les heures et les minutes.

ÉTAPE 4 Cliquez sur **Apply** pour enregistrer les paramètres.

Si vous utilisez la page Getting Started (Advanced), cliquez sur **Getting Started > Advanced** pour afficher la liste des tâches de configuration sous **Firewall and NAT Rules**.

Configuration des alias IP pour les interfaces WAN

Les alias IP sont utiles lorsque vous disposez d'adresses IP publiques supplémentaires fournies par votre fournisseur et souhaitez que ces adresses atteignent les périphériques de votre réseau local.

ÉTAPE 1 Cliquez sur **Networking > WAN > IP Alias**.

ÉTAPE 2 Pour ajouter des alias IP, cliquez sur **Add**.

ÉTAPE 3 Dans le menu déroulant Interface, choisissez l'interface **WAN**. Il s'agit de l'interface dans laquelle vous ajouterez l'adresse IP.

ÉTAPE 4 Cliquez sur **Apply** pour enregistrer les paramètres.

Configuration de la stratégie sortante par défaut

La stratégie sortante par défaut est utilisée lorsqu'aucune règle de pare-feu spécifique ne s'applique à la source, à la destination, au service ou à d'autres caractéristiques du trafic sortant. Cette stratégie s'applique à l'ensemble du trafic dirigé du LAN vers le WAN.

ÉTAPE 1 Cliquez sur **Firewall > Firewall > Default Outbound Policy**.

ÉTAPE 2 Sélectionnez **Allow Always** pour autoriser le trafic sortant ou **Block Always** pour le bloquer.

ÉTAPE 3 Cliquez sur **Apply** pour enregistrer les paramètres.

REMARQUE Étapes suivantes :

- Pour configurer une règle de pare-feu pour le trafic sortant, voir **Configuration d'une règle de pare-feu pour le trafic sortant, page 111.**
- Pour configurer une règle de pare-feu pour le trafic sortant, voir **Configuration d'une règle de pare-feu pour le trafic entrant, page 114.**

Configuration d'une règle de pare-feu pour le trafic sortant

Cette procédure explique comment configurer une règle de pare-feu pour les flux de trafic suivants :

- Du réseau LAN au réseau WAN
- Du réseau LAN au réseau DMZ
- Du réseau DMZ au réseau WAN

Pour des exemples, reportez-vous à la **Exemples de configuration de règles de pare-feu, page 119**.

REMARQUE Outre les règles de pare-feu, il existe deux autres méthodes pour contrôler l'accès à Internet :

- Vous pouvez autoriser l'accès aux sites Web approuvés. Pour obtenir plus d'informations, reportez-vous à la section **Configuration des URL approuvées pour autoriser l'accès aux sites Web, page 132**.
- Vous pouvez bloquer les URL qui contiennent des mots-clés spécifiés. Pour obtenir plus d'informations, reportez-vous à la section **Configuration des URL bloquées pour empêcher l'accès aux sites Web, page 133.**

ÉTAPE 1 Cliquez sur **Firewall > Firewall > IPv4 Rules** ou **IPv6 Rules** ; pour les règles IPv4, vous pouvez utiliser la page Getting Started (Advanced). Dans la section **Firewall and NAT Rules**, cliquez sur **Configure Firewall and NAT Rules**.

ÉTAPE 2 La fenêtre Firewall Rules s'ouvre. Toutes les règles existantes apparaissent dans le tableau List of Available Firewall Rules.

Pour les règles IPv4, vous pouvez afficher la liste des règles disponibles par zone. Choisissez la source et la destination dans les menus déroulants **From Zone** et **To Zone**, puis cliquez sur **Display Rules**.

ÉTAPE 3 Pour ajouter une règle, cliquez sur **Add**.

Autres options : cliquez sur le bouton **Edit** pour modifier une entrée. Pour supprimer une entrée, sélectionnez la case correspondante, puis cliquez sur **Delete**. Pour modifier l'état d'une règle, sélectionnez la case correspondante, puis cliquez sur **Enable** ou **Disable**. Pour sélectionner toutes les entrées, sélectionnez la case dans la première colonne de l'en-tête du tableau.

La page IPv4 Firewall Rules fournit une option permettant de déplacer une règle vers le haut ou vers le bas, ou de la déplacer vers un emplacement spécifié dans la liste des règles de pare-feu. Pour obtenir plus d'informations, reportez-vous à la section **Attribution de priorité aux règles de pare-feu, page 118**.

Si vous cliquez sur **Add** ou **Edit**, la fenêtre Firewall Rules Configuration s'ouvre.

ÉTAPE 4 Dans la zone **Firewall Rule Configuration**, saisissez les informations suivantes :

- **From Zone :** choisissez la source du trafic concernée par cette règle. Pour une règle sortante, choisissez **SECURE (LAN)** si le trafic vient de vos utilisateurs LAN ou **DMZ** s'il vient d'un serveur du réseau DMZ.
- **To Zone :** pour une règle sortante, choisissez **INSECURE (WAN)** si le trafic est à destination d'Internet ou **DMZ** s'il est à destination d'un serveur du réseau DMZ.

- Si la zone source est le réseau WAN, la zone de destination peut être le réseau DMZ public ou le réseau LAN sécurisé.
- Si la zone source est le réseau LAN, la zone de destination peut être le réseau DMZ public ou le réseau WAN sécurisé.

- **Service** : choisissez un service dans la liste des services communs ou un service personnalisé défini. Pour obtenir plus d'informations, reportez-vous à la section **Appendix B, "Services standard"** et à la section **Création de services personnalisés, page 108.**
- **Action :** choisissez comment et quand appliquer la règle.
- **Select Schedule :** si vous choisissez l'une des actions « par planning », sélectionnez un planning dans la liste.

  Pour plus d'informations sur les plannings, reportez-vous à la **Création des plannings pour les règles d'un pare-feu, page 109.**
- **Source Hosts** : vous pouvez appliquer la règle à tous les utilisateurs ou spécifier des utilisateurs en saisissant une adresse IP ou une plage d'adresses.
  - Si vous choisissez Single Address, entrez une adresse IP dans le champ **From**.
  - Si vous choisissez Address Range, saisissez la première adresse dans le champ **From** et la dernière adresse dans le champ **To**.
- **Destination Hosts** : vous pouvez appliquer la règle à tous les utilisateurs ou spécifier des utilisateurs en saisissant une adresse IP ou une plage d'adresses.
  - Si vous choisissez Single Address, entrez une adresse IP dans le champ **From**.
  - Si vous choisissez Address Range, saisissez la première adresse dans le champ **From** et la dernière adresse dans le champ **To**.
- **Log:** vous pouvez choisir de consigner ou non les paquets pour cette règle. Cliquez sur **Never** si vous ne souhaitez pas consigner les paquets ou sur **Always** dans le cas contraire.
- **QoS Priority :** vous pouvez utiliser cette règle pour hiérarchiser le trafic. Chaque niveau de priorité correspond à une valeur ToS (Term of Service).
  - **Normal-Service:** ToS=0 (QoS la plus basse)
  - **Minimize-Cost :** ToS=1

- **Maximize-Reliability :** ToS=2
- **Maximize-Throughput :** ToS=4
- **Minimize-Delay :** ToS=8 (QoS la plus élevée)

ÉTAPE 5 Pour une règle LAN to WAN uniquement, saisissez les informations suivantes dans la zone **Source NAT Settings** :

- **SNAT IP Type :** la traduction d'adresses réseau source (SNAT) nécessite la réécriture de l'adresse IP source ou de destination des paquets IP entrants lorsqu'ils transitent par le pare-feu. Sélectionnez l'une des options suivantes :
  - **WAN Interface Address :** sélectionnez cette option pour utiliser l'adresse IP de l'interface WAN.
  - **Single Address :** sélectionnez cette option pour associer le trafic sortant à une adresse IP externe (généralement fournie par votre FAI), puis sélectionnez l'alias IP configuré pour l'interface WAN. Si aucun alias IP n'est configuré, la liste est vide.

ÉTAPE 6 Cliquez sur **Apply** pour enregistrer les paramètres.

Configuration d'une règle de pare-feu pour le trafic entrant

Cette procédure explique comment configurer une règle de pare-feu pour les flux de trafic suivants :

- Du réseau WAN au réseau LAN
- Du réseau WAN au réseau DMZ
- Du réseau DMZ au réseau LAN

Si vous souhaitez autoriser le trafic entrant, vous devez rendre publique l'adresse IP du port WAN de l'appliance de sécurité. Il s'agit de l'« exposition de votre hôte ». Toutefois, cette adresse IP publique ne doit pas nécessairement être votre adresse WAN. L'appliance de sécurité prend en charge plusieurs adresses IP publiques sur une même interface WAN. Lorsque vous créez la règle de pare-feu, vous pouvez choisir d'associer le service public à l'adresse WAN dédiée, à l'adresse WAN facultative ou à une autre adresse IP fournie par votre FAI.

Pour des exemples, reportez-vous à la **Exemples de configuration de règles de pare-feu, page 119**.

REMARQUE Outre la configuration des règles de pare-feu, vous pouvez utiliser les méthodes suivantes pour contrôler le trafic entrant :

- Vous pouvez empêcher les types d'attaques communs. Pour obtenir plus d'informations, reportez-vous à la section **Configuration des contrôles d'attaque, page 123**.
- Vous pouvez autoriser ou bloquer le trafic provenant des adresses MAC spécifiées. Pour obtenir plus d'informations, reportez-vous au **Configuration du filtrage MAC pour autoriser ou bloquer le trafic, page 124**
- Vous pouvez associer les adresses IP aux adresses MAC pour éviter l'usurpation d'adresse. Pour obtenir plus d'informations, reportez-vous au **Configuration de l'association IP/MAC pour éviter l'usurpation d'adresse, page 134**

ÉTAPE 1 Cliquez sur **Firewall > Firewall > IPv4 Rules** ou **IPv6 Rules** ; pour les règles IPv4, vous pouvez utiliser la page Getting Started (Advanced). Dans la section **Firewall and NAT Rules**, cliquez sur **Configure Firewall and NAT Rules**.

La fenêtre Firewall Rules s'ouvre. Toutes les règles existantes apparaissent dans le tableau List of Available Firewall Rules.

Pour les règles IPv4, vous pouvez afficher la liste des règles disponibles par zone. Choisissez la source et la destination dans les menus déroulants **From Zone** et **To Zone**, puis cliquez sur **Display Rules**.

ÉTAPE 2 Pour ajouter une règle, cliquez sur **Add**.

Autres options : cliquez sur le bouton **Edit** pour modifier une entrée. Pour supprimer une entrée, sélectionnez la case correspondante, puis cliquez sur **Delete**. Pour modifier l'état d'une règle, sélectionnez la case correspondante, puis cliquez sur **Enable** ou **Disable**. Pour sélectionner toutes les entrées, sélectionnez la case dans la première colonne de l'en-tête du tableau.

La page IPv4 Firewall Rules fournit une option permettant de déplacer une règle vers le haut ou vers le bas, ou de la déplacer vers un emplacement spécifié dans la liste des règles de pare-feu. Pour obtenir plus d'informations, reportez-vous à la section **Attribution de priorité aux règles de pare-feu, page 118**.

Si vous cliquez sur **Add** ou **Edit**, la fenêtre Firewall Rules Configuration s'ouvre.

ÉTAPE 3 Dans la zone **Firewall Rule Configuration**, saisissez les informations suivantes :

- **From Zone :** choisissez la source du trafic concernée par cette règle. Pour une règle entrante, sélectionnez **INSECURE (WAN)** si le trafic provient d'Internet ou **DMZ** s'il provient d'un serveur sur le réseau DMZ.
- **To Zone :** pour une règle entrante, sélectionnez **SECURE (LAN)** si le trafic est à destination du LAN ou **DMZ** s'il est à destination d'un serveur sur le réseau DMZ.
  - Si la zone source est le réseau WAN, la zone de destination peut être le réseau DMZ public ou le réseau LAN sécurisé.
  - Si la zone source est le réseau LAN, la zone de destination peut être le réseau DMZ public ou le réseau WAN sécurisé.
- **Service** : choisissez un service dans la liste des services communs ou un service personnalisé défini. Pour obtenir plus d'informations, reportez-vous à la section **Appendix B, "Services standard"** et à la section **Création de services personnalisés, page 108.**
- **Action :** vous pouvez choisir de bloquer ou d'autoriser et d'appliquer la règle toujours ou selon un planning spécifié. Sélectionnez BLOCK always, ALLOW always, BLOCK by schedule ou ALLOW by schedule.
- **Select Schedule :** si vous choisissez l'une des actions « par planning », sélectionnez un planning dans la liste.

  Pour plus d'informations sur les plannings, reportez-vous à la **Création des plannings pour les règles d'un pare-feu, page 109.**
- **Source Hosts** : vous pouvez appliquer la règle à tous les utilisateurs ou spécifier des utilisateurs en saisissant une adresse IP ou une plage d'adresses.
  - Si vous choisissez Single Address, entrez une adresse IP dans le champ **From**.
  - Si vous choisissez Address Range, saisissez la première adresse dans le champ **From** et la dernière adresse dans le champ **To**.
- **Destination Hosts** (disponible uniquement si le flux de trafic va du DMZ au LAN) : vous pouvez appliquer la règle à tous les utilisateurs ou spécifier des utilisateurs en saisissant une adresse IP ou une plage d'adresses.
  - Si vous choisissez Single Address, entrez une adresse IP dans le champ **From**.

- Si vous choisissez Address Range, saisissez la première adresse dans le champ **From** et la dernière adresse dans le champ **To**.

- **Local Server :** vous pouvez afficher l'adresse IP du serveur local (s'applique uniquement aux règles IPv4 Firewall).
- **Log :** vous pouvez choisir de consigner ou non les paquets pour cette règle. Cliquez sur **Never** si vous ne souhaitez pas consigner les paquets ou sur **Always** dans le cas contraire.

ÉTAPE 4 Pour une règle WAN-to-LAN ou WAN-to-DMZ, saisissez les informations suivantes dans la zone **Destination NAT Settings** :

- **Internal IP Address :** saisissez l'adresse IP du serveur qui héberge le service.
- **Enable Port Forwarding :** sélectionnez cette case pour diriger le trafic jusqu'à un port spécifique.
- **Translate Port Number :** si vous avez activé le transfert de port, entrez le numéro de port qui correspondra à la destination du trafic transféré.
- **External IP Address :** sélectionnez l'une des options suivantes pour indiquer l'adresse IP rendue publique :
  - **Dedicated WAN :** les utilisateurs publics se connectent à ce service à l'aide de l'adresse IP associée à l'interface WAN.
  - **Optional WAN :** les utilisateurs publics se connectent à ce service à l'aide de l'adresse IP associée à l'interface WAN sur le port facultatif.
  - **Other :** les utilisateurs publics se connectent à ce service à l'aide d'une autre adresse IP fournie par votre FAI. Si vous choisissez cette option, saisissez l'adresse dans le champ **Other IP Address**.

ÉTAPE 5 Cliquez sur **Apply** pour enregistrer les paramètres.

La règle de pare-feu apparaît sur la page Firewall Rules.

Attribution de priorité aux règles de pare-feu

Si la stratégie de pare-feu contient plusieurs règles autorisant le trafic, vous pouvez les réorganiser par ordre de priorité. Vous pouvez déplacer une règle vers le haut ou vers le bas, ou la déplacer vers un emplacement spécifié dans la liste des règles de pare-feu.

REMARQUE Cette fonctionnalité ne s'applique qu'aux règles de pare-feu IPv4.

ÉTAPE 1 Cliquez sur **Firewall > Firewall > IPv4 Rules** ou utilisez la page Getting Started (Advanced). Dans la section **Firewall and NAT Rules**, cliquez sur **Configure Firewall and NAT Rules**.

La fenêtre IPv4 Firewall Rules s'ouvre.

Les règles de pare-feu apparaissent dans le tableau List of Available Firewall Rules. Cette liste contient toutes les règles de pare-feu pour le contrôle du trafic provenant d'une zone particulière ou vers une destination spécifique.

ÉTAPE 2 Pour afficher la liste des règles appartenant au même groupe, choisissez la source et la destination dans les menus déroulants **From Zone** et **To Zone**, puis cliquez sur **Display Rules**. Seules les règles pour les zones de sécurité indiquées s'affichent.

Par exemple : si vous choisissez WAN et LAN dans les menus déroulants de zone, seules les règles pour les zones de sécurité WAN à LAN s'affichent.

ÉTAPE 3 Pour réorganiser les règles, cliquez sur **Move**.

La fenêtre Move Firewall Rules s'ouvre.

ÉTAPE 4 Dans le tableau List of Available Firewall Rules, sélectionnez la case en regard de la règle à réorganiser et choisissez l'une des options suivantes :

- **MoveUp** : déplace la règle d'une place vers le haut.
- **MoveDown** : déplace la règle d'une place vers le bas.
- **Move To** : déplace la règle vers un emplacement spécifié. Entrez le numéro d'index cible vers lequel déplacer la règle sélectionnée.

  Par exemple : l'index cible 2 déplace la règle en position 2 et déplace les autres règles en position 3 dans la liste.

ÉTAPE 5 Ensuite, vous revenez à la page IPv4 Firewall Rules.

ÉTAPE 6 Vérifiez que les règles ont été réorganisées en choisissant la source et la destination appropriées dans les menus déroulants Zone, puis cliquez sur **Display Rules**.

Exemples de configuration de règles de pare-feu

Autorisation du trafic entrant sur un serveur Web à l'aide de l'adresse IP WAN

Situation : sous hébergez un serveur Web public sur le réseau DMZ. Vous souhaitez autoriser les requêtes HTTP entrantes depuis n'importe quelle adresse IP externe. Le trafic entrant est adressé à votre adresse IP WAN, mais est dirigé vers un serveur Web.

Solution : créez une règle entrante comme suit :

Paramètre	Valeur
From Zone	Insecure (WAN1)
To Zone	DMZ
Service	HTTP
Action	ALLOW always
Source Hosts	Toute
Internal IP Address	192.168.5.2
External IP Address	Dedicated WAN

Autorisation du trafic entrant vers un serveur Web à l'aide d'une adresse IP publique spécifiée

Situation : vous hébergez un serveur Web public sur votre réseau DMZ local. Vous souhaitez autoriser les requêtes HTTP entrantes depuis n'importe quelle adresse IP externe. Votre FAI vous a fourni une adresse IP statique que vous souhaitez exposer au public comme votre adresse de serveur Web.

Solution : ajoutez l'adresse IP statique (fournie par le FAI) à l'interface WAN comme un alias et créez une règle entrante. Pour plus d'informations sur la configuration des alias, voir **Configuration des alias IP pour les interfaces WAN, page 110**.

Paramètre	Valeur
From Zone	Insecure (WAN1)
To Zone	DMZ
Service	HTTP
Action	ALLOW always
Source Hosts	Any
Internal IP Address	192.168.5.2
External IP Address	Dedicated WAN-209.165.201.225

Autorisation du trafic entrant en provenance de l'intervalle spécifié des hôtes externes

Situation : sous souhaitez autoriser le lancement de vidéoconférence entrante à partir d'une plage limitée d'adresses IP externes (132.177.88.2 - 132.177.88.254).

Solution : créez une règle entrante, comme indiqué ci-dessous. Dans l'exemple, les connexions pour CU-SeeMe (client de vidéoconférence Internet) sont autorisées uniquement si elles proviennent d'une plage spécifiée d'adresses IP externes.

Paramètre	Valeur
From Zone	INSECURE (Dedicated WAN/Optional WAN)
To Zone	Secure (LAN)

Paramètre	Valeur
Service	CU-SEEME:UDP
Action	ALLOW always
Source Hosts	Address Range
From	132.177.88.2
To	134.177.88.254
Send to Local Server (DNAT IP)	192.168.75.11 (internal IP address)

Blocage du trafic sortant par planning et par plage d'adresses IP

Cas d'usage : bloquez toute utilisation d'Internet pendant le week-end si la requête provient d'une plage spécifiée d'adresses IP.

Solution : configurez un planning appelé « week-end » pour définir la période pendant laquelle la règle est appliquée. Configurez une règle sortante qui s'applique au trafic provenant du groupe marketing, avec une plage d'adresses IP de 10.1.1.1 à 10.1.1.100.

Paramètre	Valeur
From Zone	Secure (LAN)
To Zone	INSECURE (Dedicated WAN/Optional WAN)
Service	HTTP
Action	BLOCK by schedule
Programmation	Weekend
Source Hosts	Address Range
From	10.1.1.1
To	10.1.1.100
Destination Hosts	Any

Blocage du trafic sortant vers un serveur de messagerie hors site

La règle suivante bloque l'accès au service SMTP pour empêcher un utilisateur d'envoyer des e-mails via un serveur de messagerie hors site.

Paramètre	Valeur
From Zone	Secure (LAN)
To Zone	INSECURE (Dedicated WAN/Optional WAN)
Service	SMTP
Action	BLOCK Always
Source Hosts	Any

Utilisation d'autres outils pour éviter les attaques, limiter les accès et contrôler le trafic entrant

Outre les règles de pare-feu, l'appliance de sécurité fournit un certain nombre d'autres outils pour vous aider à protéger votre réseau du trafic entrant indésirable.

- **Configuration des contrôles d'attaque**
- **Configuration du filtrage MAC pour autoriser ou bloquer le trafic**
- **Configuration de l'association IP/MAC pour éviter l'usurpation d'adresse**
- **Configuration d'une règle de déclenchement de port pour diriger le trafic vers les ports spécifiés**

Configuration des contrôles d'attaque

Cette page permet de spécifier comment protéger votre réseau contre les types communs d'attaques, notamment la détection, l'inondation et les orages d'écho.

ÉTAPE 1 Cliquez sur **Firewall > Attacks**. La fenêtre *Attack Checks* s'ouvre.

ÉTAPE 2 Dans la zone **WAN Security Checks**, sélectionnez la case de chaque fonctionnalité à activer :

- **Block Ping to WAN interface :** sélectionnez cette case pour empêcher les agresseurs d'utiliser les demandes d'écho (ping) ICMP pour accéder à votre réseau. Cisco vous recommande de désélectionner cette case uniquement si vous devez autoriser l'appliance de sécurité à répondre aux demandes ping à des fins de diagnostic.

  Ce paramètre est remplacé dans les cas suivants :

  - Une règle de pare-feu qui dirige les demandes ping vers un ordinateur spécifique sur le LAN. Voir aussi **Configuration des règles de pare-feu pour contrôler le trafic entrant et sortant, page 107.**
  - Des paramètres du mode WAN qui exécutent une commande ping sur des adresses IP spécifiées à des fins de détection des défaillances. Voir aussi **Configuration du renvoi automatique, de l'équilibrage de charge et de la détection des défaillances, page 59.**

- **Enable Stealth Mode :** sélectionnez cette case pour empêcher l'appliance de sécurité de répondre aux analyses de ports du WAN. En mode furtif, votre réseau est moins exposé à la détection et aux attaques.
- **Block TCP Flood :** sélectionnez cette case pour abandonner tous les paquets TCP non valides. Cette fonction protège votre réseau contre une attaque de type inondation SYN, dans laquelle un pirate envoie une succession de requêtes SYN (synchronize) à un système cible.

ÉTAPE 3 Dans la section **LAN Security Checks**, sélectionnez la case **Block UDP Flood** pour empêcher l'appliance de sécurité d'accepter plus de 25 connexions UDP actives simultanées d'un même ordinateur sur le LAN.

ÉTAPE 4 Dans la zone **ICSA Settings**, saisissez les informations suivantes :

- **Block ICMP Notification :** sélectionnez cette case pour activer le blocage automatique sans envoyer de notification ICMP à l'expéditeur. Certains protocoles, tels que la découverte du MTU de chemin, nécessitent des notifications ICMP.

- **Block Fragmented Packets :** sélectionnez cette case pour bloquer les paquets fragmentés de ANY à ANY.
- **Block Multicast Packets :** sélectionnez cette case pour bloquer les paquets de multidiffusion.

ÉTAPE 5 Dans la zone **DoS Attacks**, saisissez les informations suivantes :

- **SYN Flood Detect Rate (max/sec) :** saisissez le nombre maximum de paquets SYN par seconde qui permettra à l'appliance de sécurité de déterminer qu'une intrusion de type inondation SYN est en train de se produire. Cette valeur est comprise entre 1 et 10 000 paquets par seconde. La valeur par défaut est 128 paquets SYN par seconde.
- **Echo Storm (ping pkts/sec) :** entrez le nombre de commandes Ping par seconde qui permettra à l'appliance de sécurité de déterminer qu'un événement d'intrusion de type orage d'écho est en train de se produire. Les événements d'intrusion de type orage d'écho ne sont pas mis sur la liste noire. Cette valeur est comprise entre 1 et 10 000 paquets Ping par seconde. La valeur par défaut est 15 paquets ping par seconde.
- **ICMP Flood [ICMP pkts./sec] :** saisissez le nombre de paquets ICMP par seconde, sans compter les paquets PING, qui permettra à l'appliance de sécurité de déterminer qu'un événement d'intrusion de type inondation ICMP est en train de se produire. Les événements d'inondation ICMP ne sont pas mis sur la liste noire. Cette valeur est comprise entre 1 et 10 000 paquets ICMP par seconde. La valeur par défaut est 100 paquets ICMP par seconde.

ÉTAPE 6 Cliquez sur **Apply** pour enregistrer les paramètres.

Configuration du filtrage MAC pour autoriser ou bloquer le trafic

Vous pouvez limiter (bloquer ou autoriser) le trafic vers les réseaux WAN et DMZ depuis le réseau LAN en fonction de l'adresse MAC du périphérique. La première étape consiste à renseigner la liste d'adresses MAC que la politique de filtrage doit couvrir. Vous pouvez configurer la politique pour bloquer toutes les adresses MAC dans la liste et autoriser les autres, ou pour autoriser uniquement les adresses MAC configurées et bloquer les autres.

ÉTAPE 1 Cliquez sur **Firewall > MAC Filtering > MAC Filtering**. La fenêtre Source MAC Filter s'ouvre.

Avant de pouvoir ajouter des adresses au tableau, vous devez sélectionner la case afin d'activer le filtrage MAC, puis cliquer sur **Apply**.

ÉTAPE 2 Dans la zone **MAC Filtering Enable**, saisissez les informations suivantes :

- **Enable MAC Address Filtering? :** sélectionnez cette case pour activer le filtrage des adresses MAC source.
- **Policy for MAC Addresses listed below :** sélectionnez l'une des options suivantes :
  - **Block and permit the rest :** toutes les adresses contenues dans le tableau MAC Addresses sont bloquées. Toutes les autres adresses sont autorisées.
  - **Permit and block the rest :** toutes les adresses contenues dans le tableau MAC Addresses sont autorisées. Toutes les autres adresses sont bloquées.
  - Cliquez sur **Apply** pour enregistrer les paramètres.

ÉTAPE 3 Pour ajouter une adresse MAC au tableau, cliquez sur **Add**.

Autres options : cliquez sur le bouton **Edit** pour modifier une entrée. Pour supprimer une entrée, sélectionnez la case correspondante, puis cliquez sur **Delete**. Pour sélectionner toutes les entrées, sélectionnez la case dans la première colonne de l'en-tête du tableau.

Une fois que vous avez cliqué sur Add ou Edit, la fenêtre MAC Filtering Configuration s'ouvre.

ÉTAPE 4 Saisissez l'adresse MAC.

ÉTAPE 5 Cliquez sur **Apply** pour enregistrer les paramètres.

Fenêtre IP/MAC Binding

L'association IP/MAC vous permet de lier les adresses IP à une adresse MAC, et vice-versa. Certains systèmes sont configurés avec des adresses statiques. Pour empêcher l'utilisateur de modifier les adresses IP statiques, le routeur doit autoriser l'association IP/MAC. Si le routeur détecte des paquets avec des adresses IP correspondantes, mais des adresses MAC incohérentes, ou vice-versa, il abandonne ces paquets.

ÉTAPE 1 Cliquez sur **Firewall > MAC Filtering > IP/MAC Binding**. La fenêtre IP/MAC Binding s'ouvre.

Toutes les règles actuellement définies apparaissent dans le tableau IP/MAC Binding.

ÉTAPE 2 Pour ajouter une règle IP/MAC, cliquez sur **Add**.

Autres options : cliquez sur le bouton **Edit** pour modifier une entrée. Pour supprimer une entrée, sélectionnez la case correspondante, puis cliquez sur **Delete**. Pour modifier l'état d'une règle, sélectionnez la case correspondante, puis cliquez sur **Enable** ou **Disable**. Pour sélectionner toutes les entrées, sélectionnez la case dans la première colonne de l'en-tête du tableau.

ÉTAPE 3 Si vous cliquez sur **Add** ou **Edit**, la fenêtre IP MAC Binding Configuration s'ouvre.

ÉTAPE 4 Saisissez les informations suivantes :

- **Name :** saisissez un nom unique pour cette règle.
- **MAC Address :** spécifiez l'adresse MAC pour cette règle.
- **IP Address** : spécifiez l'adresse IP pour cette règle.
- **Log Dropped Packets** : choisissez d'activer ou de désactiver les paquets abandonnés.

ÉTAPE 5 Cliquez sur **Apply** pour enregistrer vos modifications.

La nouvelle règle apparaît dans le tableau IP/MAC Binding.

Déclenchement de port

Le déclenchement de port ouvre un port entrant pour un type de trafic spécifié sur un port sortant défini. Lorsqu'un périphérique LAN établit une connexion sur l'un des ports sortants définis, l'appliance de sécurité ouvre le port entrant spécifié pour prendre en charge l'échange de données. Lorsque l'échange est terminé, les ports sont fermés.

Le déclenchement de port est plus flexible que le transfert de port statique, configurable dans une règle de pare-feu. Il n'est pas nécessaire que les règles du déclenchement de port référencent des plages d'adresse IP LAN ou d'adresses IP spécifiques. En outre, les ports ne restent pas ouverts lorsqu'ils ne sont pas utilisés, ce qui garantit un niveau de sécurité que le transfert de port statique ne fournit pas.

Le déclenchement de port est obligatoire pour certaines applications. Pour fonctionner correctement, ces applications nécessitent de recevoir, lorsque des périphériques externes se connectent à elles, des données sur un port ou une plage de ports spécifique. L'appliance de sécurité doit envoyer toutes les données entrantes pour cette application uniquement sur le port ou la plage de ports spécifié. La passerelle dispose d'une liste d'applications et de jeux courants avec les ports sortants et entrants associés à ouvrir. Vous pouvez également spécifier une règle de déclenchement de port en définissant le type de trafic (TCP ou UDP) et la plage des ports entrants et sortants à ouvrir en cas d'activation. Reportez-vous au **Annexe B, « Services standard ».**

REMARQUE Le déclenchement de port n'est pas adapté aux serveurs sur le LAN, puisque le périphérique LAN doit établir une connexion sortante avant qu'un port entrant soit ouvert.

Configuration d'une règle de déclenchement de port pour diriger le trafic vers les ports spécifiés

ÉTAPE 1 Cliquez sur **Firewall > Port Triggering > Port Triggering**. La fenêtre Port Triggering s'ouvre.

La fenêtre Port Triggering s'ouvre. Toutes les règles existantes sont répertoriées dans le tableau List of Available Port Triggering Rules.

ÉTAPE 2 Pour ajouter une nouvelle règle de déclenchement, cliquez sur **Add**.

Autres options : cliquez sur le bouton **Edit** pour modifier une entrée. Pour supprimer une entrée, sélectionnez la case correspondante, puis cliquez sur **Delete**. Pour sélectionner toutes les entrées, sélectionnez la case dans la première colonne de l'en-tête du tableau.

Une fois que vous avez cliqué sur Add ou Edit, la fenêtre Port Triggering Configuration s'ouvre.

ÉTAPE 3 Dans la zone **Port Triggering Rule**, saisissez les informations suivantes :

- **Name :** saisissez un nom pour cette règle.
- **Enable :** sélectionnez cette case pour activer la règle.
- **Protocol :** choisissez le protocole (TCP ou UDP).
- **Interface** : choisissez l'interface (LAN ou DMZ).

ÉTAPE 4 Dans la zone **Outgoing (Trigger) Port Range**, saisissez le port de début et le port de fin de manière à spécifier la plage de ports sortants pour cette règle.

ÉTAPE 5 Dans la zone Incoming (Response) Port Range, saisissez le port de début et le port de fin de manière à spécifier la plage de ports entrants pour cette règle.

ÉTAPE 6 Cliquez sur **Apply** pour enregistrer les paramètres.

Affichage de l'état de déclenchement de port

La page Port Triggering Status fournit des informations sur les ports qui ont été ouverts conformément aux règles de configuration du déclenchement de port. Les ports sont ouverts dynamiquement chaque fois que l'appliance de sécurité détecte du trafic correspondant à une règle de déclenchement.

Pour afficher cette page, cliquez sur **Firewall > Port Triggering > Port Triggering Status**. Les informations suivantes apparaissent :

- **LAN/DMZ IP Address :** affiche l'adresse IP LAN du périphérique à l'origine de l'ouverture des ports.
- **Open Ports :** affiche les ports ouverts pour que le trafic provenant de WAN et à destination de l'adresse IP LAN puisse circuler sur l'appliance de sécurité.
- **Time Remaining :** ce champ affiche la durée pendant laquelle le port reste ouvert lorsqu'il n'y a aucune activité sur celui-ci. Cette durée est réinitialisée lorsqu'une activité est détectée sur le port.

Configuration des paramètres de session pour l'analyse des paquets entrants

Cette page permet de configurer la manière dont les paquets entrants sont analysés.

ÉTAPE 1 Cliquez sur **Firewall > Session Setting**.

La fenêtre Session Settings s'ouvre.

ÉTAPE 2 Saisissez les informations suivantes :

- **Maximum Unidentified Sessions :** cette valeur définit le nombre maximum de sessions non identifiées pour le processus d'identification ALG (Application Layer Gateway, passerelle de couche d'applications). Elle est comprise entre 2 et 128. La valeur par défaut est 32 sessions.
- **Maximum Half Open Sessions :** la passerelle préserve les ressources en limitant le nombre de sessions semi-ouvertes à tout moment. Une session semi-ouverte correspond à l'état de session entre la réception d'un paquet SYN et du paquet SYN/ACK. Normalement, une session peut rester semi-ouverte pendant 10 secondes. La valeur maximale est comprise entre 0 et 3 000. La valeur par défaut est 1 024 sessions.
- **TCP Session Timeout Duration (seconds) :** les sessions TCP inactives sont supprimées de la table de session après cette période. La plupart des sessions TCP se terminent normalement lorsque les indicateurs RST ou FIN sont détectés. Cette valeur est comprise entre 0 et 4 294 967 secondes. La valeur par défaut est 1,800 secondes (30 minutes).
- **UDP Session Timeout Duration (seconds) :** les sessions UDP inactives sont supprimées de la table de session après cette période. Cette valeur est comprise entre 0 et 4 294 967 secondes. La valeur par défaut est 120 secondes (2 minutes).
- **Other Session Timeout Duration (seconds) :** les sessions non TCP/UDP inactives sont supprimées de la table de session après cette période. Cette valeur est comprise entre 0 et 4 294 967 secondes. La valeur par défaut est 60 secondes.
- **TCP Session Cleanup Latency (seconds) :** durée maximum pendant laquelle une session peut rester dans la table de session après la détection des indicateurs FIN. Cette valeur est comprise entre 0 et 4 294 967 secondes. La valeur par défaut est 10 secondes.

ÉTAPE 3 Cliquez sur **Apply** pour enregistrer les paramètres.

Utilisation d'autres outils pour contrôler l'accès à Internet

La passerelle offre des options de filtrage Web standard qui permettent à l'administrateur de créer facilement des stratégies d'accès à Internet entre le réseau LAN sécurisé et le réseau WAN non sécurisé. Au lieu de créer des stratégies basées sur le type de trafic (comme c'est le cas lorsque vous utilisez les règles de pare-feu), vous pouvez utiliser le contenu Web pour déterminer si le trafic est autorisé ou abandonné.

Reportez-vous aux rubriques suivantes :

- **Configuration du filtrage du contenu pour autoriser ou bloquer les composants Web**
- **Configuration des URL approuvées pour autoriser l'accès aux sites Web**
- **Configuration des URL bloquées pour empêcher l'accès aux sites Web**
- **Configuration de l'association IP/MAC pour éviter l'usurpation d'adresse**

Configuration du filtrage du contenu pour autoriser ou bloquer les composants Web

L'appliance de sécurité prend en charge une option de filtrage de contenu qui permet de bloquer l'accès à certains sites Internet. Vous pouvez spécifier jusqu'à 32 mots-clés pour le filtrage. Il peut s'agit d'URL de site Web, de noms de groupes de discussion, etc.

ÉTAPE 1 Cliquez sur **Firewall > Content Filtering > Content Filtering**.

La fenêtre Content Filtering s'ouvre.

ÉTAPE 2 Dans la zone **Content Filtering Enable**, activez ou désactivez les options suivantes :

- **Enable Content Filtering :** sélectionnez cette case pour activer le filtrage du contenu. Activez cette fonction si vous souhaitez configurer et utiliser des fonctionnalités telles qu'une liste de domaines approuvés, le filtrage par mot-clé, etc.

- **Enable Check Referrer :** sélectionnez cette case pour contrôler l'en-tête de référent HTTP lorsque vous autorisez l'accès aux URL qui correspondent à des mots-clés. Lorsqu'elle est activée, cette fonction permet d'accéder aux liens mentionnés sur un site Web, mais qui ne correspondent pas au nom du domaine de la page principale.
- **HTTP Ports :** saisissez les ports HTTP sur lesquels un filtrage du contenu aura lieu. Le port par défaut est 80. Si votre réseau utilise un serveur proxy HTTP externe qui écoute sur d'autres ports, vous pouvez les ajouter ici. Plusieurs ports peuvent être spécifiés dans une liste séparée par des virgules.

ÉTAPE 3 Dans la zone **Web Components**, cochez la case de tout composant à bloquer. Pour une sécurité accrue, vous pouvez bloquer certains composants Web couramment utilisés. Certains de ces composants peuvent être utilisés par des sites Web malveillants pour contaminer les ordinateurs qui les consultent.

- **Proxy** : sélectionnez cette case pour les serveurs proxy, qui peuvent être utilisés pour contourner certaines règles de pare-feu, et donc constituer une faille de sécurité potentielle.

  Par exemple, si les connexions à une adresse IP spécifique sont bloquées par une règle de pare-feu, les demandes peuvent être acheminées via un proxy qui n'est pas bloqué par la règle, ce qui rend la restriction inefficace.
- **Java** : sélectionnez cette case pour bloquer les applets Java pouvant être téléchargées à partir de pages qui les contiennent.

  Les applets Java sont de petits programmes inclus dans les pages Web, qui permettent la fonctionnalité dynamique de la page. Un applet malveillant peut être utilisé pour compromettre ou infecter l'ordinateur
- **ActiveX** : sélectionnez cette case pour empêcher le téléchargement d'applets ActiveX via Internet Explorer.

  À l'instar des applets Java, les contrôles ActiveX sont installés sur un ordinateur Windows lors de l'exécution d'Internet Explorer. Un contrôle ActiveX malveillant peut être utilisé pour compromettre ou infecter les ordinateurs.
- **Cookies :** pour une sécurité accrue, sélectionnez cette case afin de bloquer les cookies.

Les cookies permettent de stocker les informations de session des sites Web qui nécessitent généralement une connexion. Cependant, de nombreux sites Web utilisent les cookies pour stocker des informations de suivi et des habitudes de navigation. Si vous activez cette option, elle filtre les cookies créés par un site Web.

ÉTAPE 4 Cliquez sur **Apply** pour enregistrer les paramètres.

Configuration des URL approuvées pour autoriser l'accès aux sites Web

Cette page permet de créer une liste de sites Web auxquels les utilisateurs sont autorisés à accéder. Vous pouvez spécifier les noms de domaine exacts ou des mots-clés.

REMARQUE Cette page est disponible uniquement si vous avez activé le filtrage du contenu. Voir aussi **Configuration du filtrage du contenu pour autoriser ou bloquer les composants Web, page 130.**

ÉTAPE 1 Cliquez sur **Firewall > Content Filtering > Approved URLs**.

La fenêtre Approved URLs s'ouvre.

ÉTAPE 2 Dans la zone **Approved URLs List Enable**, activez ou désactivez cette fonctionnalité :

a. **Do you want to Enable Approved URLs List? :** sélectionnez cette case pour activer la liste des URL approuvées ou désélectionnez-la pour désactiver cette fonction.

b. Cliquez sur **Apply** pour enregistrer les paramètres.

ÉTAPE 3 Pour ajouter un nom de domaine ou un mot clé à la liste des URL approuvées, cliquez sur **Add**.

Autres options : cliquez sur le bouton **Edit** pour modifier une entrée. Pour supprimer une entrée, sélectionnez la case correspondante, puis cliquez sur **Delete**. Pour sélectionner toutes les entrées, sélectionnez la case dans la première colonne de l'en-tête du tableau.

Une fois que vous avez cliqué sur Add ou Edit, la fenêtre Approved URL Configuration s'ouvre.

ÉTAPE 4 Saisissez les informations suivantes :

- **URL :** entrez le nom de domaine ou les mots-clés d'un site Web à approuver. Séparez les entrées par des points-virgules (;).
- **Match Type :** spécifiez la méthode pour appliquer cette règle :
  - **Website :** sélectionnez cette option si vous voulez autoriser l'accès uniquement à l'URL exacte saisie dans le champ URL. Par exemple, si vous avez entré *www.yahoo.com*, les utilisateurs pourront accéder à www.yahoo.com, mais ils ne pourront pas aller sur www.yahoo.com.uk ou www.yahoo.co.jp.
  - **URL keyword :** sélectionnez cette option si vous voulez autoriser l'accès à toute URL qui contient le mot-clé saisi dans le champ URL. Par exemple, si vous avez entré *yahoo*, les utilisateurs pourront accéder à www.yahoo.com, tw.yahoo.com, www.yahoo.com.uk et www.yahoo.co.jp.

ÉTAPE 5 Cliquez sur **Apply** pour enregistrer les paramètres.

Configuration des URL bloquées pour empêcher l'accès aux sites Web

Cette page permet de créer une liste de sites Web auxquels les utilisateurs n'ont pas accès. Vous pouvez spécifier les noms de domaine exacts ou des mots-clés.

REMARQUE Cette page est disponible uniquement si vous avez activé le filtrage du contenu. Voir aussi **Configuration du filtrage du contenu pour autoriser ou bloquer les composants Web, page 130.**

ÉTAPE 1 Cliquez sur **Firewall > Content Filtering > Blocked URLs**.

La fenêtre Blocked URLs s'ouvre.

ÉTAPE 2 Pour ajouter un nom de domaine ou un mot-clé à la liste des URL bloquées, cliquez sur **Add**.

Autres options : cliquez sur le bouton **Edit** pour modifier une entrée. Pour supprimer une entrée, sélectionnez la case correspondante, puis cliquez sur **Delete**. Pour sélectionner toutes les entrées, sélectionnez la case dans la première colonne de l'en-tête du tableau.

Une fois que vous avez cliqué sur Add ou Edit, la fenêtre Blocked URLs Configuration s'ouvre.

ÉTAPE 3 Saisissez les informations suivantes :

- **URL :** entrez le nom de domaine ou les mots-clés d'un site Web à approuver. Séparez les entrées par des points-virgules (;).
- **Match Type :** spécifiez la méthode pour appliquer cette règle :
  - **Website :** sélectionnez cette option pour bloquer l'accès au nom de domaine exact. Par exemple, si vous entrez *www.yahoo.com* pour l'URL, les utilisateurs n'ont pas accès à www.yahoo.com, mais ils peuvent accéder à www.yahoo.com.uk ou www.yahoo.co.jp.
  - **URL Keyword :** sélectionnez cette option pour bloquer l'accès à n'importe quel site Web avec un nom de domaine contenant le mot-clé configuré. Par exemple, si vous entrez *yahoo* pour l'URL, les utilisateurs n'ont pas accès aux sites Web tels que www.yahoo.com, tw.yahoo.com, www.yahoo.com.uk et www.yahoo.co.jp.

ÉTAPE 4 Cliquez sur **Apply** pour enregistrer les paramètres.

Configuration de l'association IP/MAC pour éviter l'usurpation d'adresse

Vous pouvez utiliser l'association IP/MAC pour autoriser le trafic du LAN vers le WAN uniquement lorsque l'hôte possède une adresse IP correspondant à une adresse MAC indiquée. En demandant à la passerelle de valider l'adresse IP du trafic source avec l'adresse MAC unique du périphérique, l'administrateur peut garantir que le trafic de l'adresse IP spécifiée n'est pas frauduleux. En cas de violation (l'adresse IP source du trafic ne correspond pas à l'adresse MAC attendue avec la même adresse IP), les paquets sont abandonnés et peuvent être consignés à des fins le diagnostic.

ÉTAPE 1 Cliquez sur **Firewall > MAC Filtering > IP/MAC Binding**.

La fenêtre IP/MAC Binding s'ouvre.

ÉTAPE 2 Pour ajouter une association IP/MAC dans le tableau, cliquez sur **Add**.

Autres options : cliquez sur le bouton **Edit** pour modifier une entrée. Pour supprimer une entrée, sélectionnez la case correspondante, puis cliquez sur **Delete**. Pour sélectionner toutes les entrées, sélectionnez la case dans la première colonne de l'en-tête du tableau.

Une fois que vous avez cliqué sur Add ou Edit, la fenêtre IP MAC Binding Configuration s'ouvre.

ÉTAPE 3 Saisissez les informations suivantes :

- **Name :** saisissez un nom pour cette association IP/MAC.
- **MAC Address :** saisissez l'adresse MAC.
- **IP Address :** saisissez l'adresse IP.
- **Log Dropped Packets :** sélectionnez **Enable** pour conserver un journal de tous les paquets qui sont abandonnés en raison de cette fonctionnalité de sécurité. Sinon, sélectionnez **Disable**.

  REMARQUE Une fois que vous avez activé la consignation, vous pouvez afficher les journaux en cliquant sur **Status** dans la barre de menu, puis sur **View Log > View All Logs**.

ÉTAPE 4 Cliquez sur **Apply** pour enregistrer les paramètres.

SIP

La passerelle de couche Application SIP (Session Initiation Protocol) peut réécrire les informations dans les messages SIP (en-têtes SIP et corps SDP) pour permettre le trafic audio et la signalisation entre le client situé derrière le périphérique NAT et le point d'extrémité SIP.

REMARQUE La passerelle de couche Application SIP doit être activée lorsque des périphériques voix tels que les téléphones SIP ou UC500 sont connectés au réseau derrière l'appliance de sécurité.

ÉTAPE 1 Cliquez sur **Firewall > SIP**.

La fenêtre SIP ALG s'ouvre.

ÉTAPE 2 Sélectionnez ou désélectionnez cette case pour activer ou désactiver la prise en charge d'une passerelle de couche Application SIP (Session Initiation Protocol). Si cette fonctionnalité est désactivée, le routeur n'autorise pas les appels entrants vers l'UAC (User Agent Client) derrière le routeur.

ÉTAPE 3 Cliquez sur **Apply** pour enregistrer les paramètres.

5

Système de prévention des intrusions

La gamme SA500 utilise un système de prévention d'intrusion (IPS) pour protéger les zones de sécurité pour un ensemble désigné de catégories. L'IPS surveille le trafic réseau à la recherche de comportement malveillant ou indésirable sur le périphérique et peut répondre, en temps réel, pour bloquer ou empêcher ces activités.

Lorsqu'une attaque est détectée, les paquets incriminés sont abandonnés ou des alertes sont consignées selon les paramètres administratifs, mais le reste du trafic n'est pas affecté. Contrairement aux pare-feu traditionnels, un IPS prend des décisions de contrôle d'accès basées sur le contenu de l'application, et non sur l'adresse IP ou les ports.

Vous pouvez configurer l'IPS pour protéger les services réseau tels que le Web, les applications de messagerie instantanée, le courrier électronique, le transfert de fichiers, les services Windows et les DNS. Il protège également les applications contre les vulnérabilités telles que les virus et les vers, les applications homologue-à-homologue (P2P) et les opérations de détournement.

Ce chapitre décrit la procédure de configuration des fonctions IPS. Il comprend les sections suivantes :

- **Configuration de la traduction d'adresses réseau (IPS)**
- **Configuration de la politique IPS**
- **Configuration des paramètres d'inspection de protocole**
- **Configuration du blocage homologue-à-homologue et de la messagerie instantanée**

Pour accéder aux pages IPS, cliquez sur *IPS* dans la barre de menus de Configuration Utility.

Configuration de la traduction d'adresses réseau (IPS)

Vous configurez l'IPS depuis la page IPS Setup. Sur cette page vous pouvez activer l'IPS pour la zone de sécurité que vous souhaitez protéger (LAN ou DMZ), mettre à jour les signatures IPS et afficher le statut IPS.

ÉTAPE 1 Cliquez sur **IPS > IPS Setup** ou, sur la page Getting Started (Advanced), sous Intrusion Prevention System, cliquez sur **Update Signatures**.

La fenêtre IPS Configuration s'ouvre.

- **IPS Enable** : par défaut, l'IPS est désactivé. Pour activer l'IPS pour une zone particulière, sélectionnez LAN ou DMZ ou les deux pour la ou les zones que vous souhaitez protéger. Par exemple : l'activation de la protection IPS sur la zone LAN applique l'IPS sur tout le trafic LAN entrant et sortant.

  Cliquez sur **Apply** pour enregistrer les paramètres.

- **IPS Status** : affiche l'état des signatures IPS y compris la date d'expiration de la licence IPS, la version du fichier de signature et la dernière date à laquelle le dispositif de sécurité a recherché des mises à jour de signature.

  - Cliquez sur le lien **View IPS Logs** pour afficher les messages du journal IPS. Pour afficher les messages générés par l'IPS, vous devez choisir l'IPS en tant qu'installation. Pour obtenir plus d'informations, reportez-vous à **Page Active Users, page 228**.

- **Automatic Signature Updates :** l'IPS utilise des fichiers de signature pour identifier une attaque en cours. Vous pouvez également configurer l'appliance de sécurité pour mettre à jour automatiquement les signatures IPS lorsqu'elles sont disponibles.

  - Pour activer l'option de mise à jour automatique, sélectionnez la case **Automatically Update Signatures**.

    Entrez votre **nom d'utilisateur** et votre **mot de passe** Cisco.com pour vous authentifier sur le serveur de mise à jour de signature. Ces informations d'identification ne sont demandées qu'une fois. Cliquez sur **Apply** pour enregistrer les paramètres.

    REMARQUE Une fois appliqués, les détails du nom d'utilisateur et du mot de passe Cisco sont appliqués à tous les autres services sur le routeur qui les utilisent. Par exemple, le nom d'utilisateur et la connexion Cisco utilisés pour l'administration sont automatiquement mis à jour pour les téléchargements de signature IPS.

- Cliquez sur **Update Now** pour mettre à jour immédiatement les nouvelles signatures le cas échéant. Cette option est active uniquement si la case Automatically Update Signature est sélectionnée.
- Cliquez sur **Reset** pour rétablir les paramètres précédents.

▪ **Manual Signature Updates** : pour mettre à jour manuellement le dernier fichier de signature, cliquez sur le lien Cisco.com pour obtenir le fichier et le télécharger sur votre ordinateur. Accédez à l'emplacement du fichier de signature sur le PC local puis cliquez sur **Upload**.

Configuration de la politique IPS

Vous pouvez configurer les paramètres de stratégie IPS pour protéger le réseau contre les menaces telles que les attaques de déni de service, les programmes malveillants et les opérations de détournement.

ÉTAPE 1 Cliquez sur **IPS > IPS Policy** ou, sur la page Getting Started (Advanced), sous Intrusion Prevention System, cliquez sur **Configure and Enable IPS Policies.**

ÉTAPE 2 Choisissez la stratégie pour chaque catégorie ou pour chaque signature dans chaque catégorie.

▪ Pour sélectionner une stratégie pour une catégorie IPS, cliquez sur une option dans la ligne d'en-tête de la catégorie.

▪ Pour développer les signatures sous une catégorie, cliquez sur le bouton **+** en regard de l'en-tête de la catégorie. Pour masquer les signatures, cliquez sur le bouton **-**.

▪ Pour sélectionner une stratégie pour une signature individuelle, cliquez sur une option dans la ligne d'entrée de cette signature.

Options :

▪ **Disabled** : sélectionnez cette option pour désactiver la recherche dans cette catégorie.

▪ **Detect Only** : sélectionnez cette option pour rechercher des attaques sur cette catégorie et pour consigner un message après la détection. Cette option est principalement utilisée à des fins de dépannage.

- **Detect and Prevent** : sélectionnez cette option pour rechercher et empêcher des attaques sur cette catégorie. Après la détection, un message est consigné et une mesure préventive est prise.

  Pour que les messages IPS soient consignés, vous devez configurer l'IPS en tant qu'installation. Pour obtenir plus d'informations, reportez-vous à la section **Fenêtre Logs Facility and Severity, page 203**.

ÉTAPE 3 Cliquez sur **Apply** pour enregistrer les paramètres.

Configuration des paramètres d'inspection de protocole

Vous pouvez configurer les paramètres d'inspection de protocole pour détecter le comportement suspect et les attaques sur divers types de protocoles.

ÉTAPE 1 Cliquez sur **IPS> IPS Protocol Inspection**.

ÉTAPE 2 Sélectionnez les paramètres d'inspection pour chaque catégorie ou pour chaque signature dans chaque catégorie.

- Pour sélectionner une paramètre d'inspection pour une catégorie IPS, cliquez sur une option dans la ligne d'en-tête de la catégorie.
- Pour développer les signatures sous une catégorie, cliquez sur le bouton **+** en regard de l'en-tête de la catégorie. Pour masquer les signatures, cliquez sur le bouton **-**.
- Pour sélectionner un paramètre d'inspection pour une signature individuelle, cliquez sur une option dans la ligne d'entrée de cette signature.

Options :

- **Disabled** : sélectionnez cette option pour désactiver la vérification d'inspection pour ce protocole.
- **Detect Only** : sélectionnez cette option pour rechercher des attaques sur ce protocole et pour consigner un message après la détection. Cette option est principalement utilisée à des fins de dépannage.
- **Detect and Prevent** : sélectionnez cette option pour rechercher et empêcher des attaques sur ce protocole. Après la détection, un message est consigné et une mesure préventive est prise.

Pour que les messages IPS soient consignés, vous devez configurer l'IPS en tant qu'installation. Pour obtenir plus d'informations, reportez-vous au **Fenêtre Logs Facility and Severity, page 203**

ÉTAPE 3 Cliquez sur **Apply** pour enregistrer les paramètres.

Configuration du blocage homologue-à-homologue et de la messagerie instantanée

Vous pouvez configurer l'appliance pour bloquer le trafic homologue-à-homologue (P2P) et la messagerie instantanée (IM) sur l'appliance de sécurité. Sur la page d'IM et de blocage P2P, vous pouvez spécifier le type des applications P2P et IM (telles que Gnutella, BitTorrent, AOL ou Yahoo) à bloquer.

ÉTAPE 1 Cliquez sur **IPS > IM and P2P Blocking**.

ÉTAPE 2 Sélectionnez les paramètres d'inspection pour chaque catégorie ou pour chaque signature dans chaque catégorie.

- Pour sélectionner une paramètre d'inspection pour une catégorie IPS, cliquez sur une option dans la ligne d'en-tête de la catégorie.
- Pour développer les signatures sous une catégorie, cliquez sur le bouton **+** en regard de l'en-tête de la catégorie. Pour masquer les signatures, cliquez sur le bouton **-**.
- Pour sélectionner un paramètre d'inspection pour une signature individuelle, cliquez sur une option dans la ligne d'entrée de cette signature.

Options :

- **Disabled** : sélectionnez cette option pour désactiver la recherche dans ce service.
- **Detect Only** : sélectionnez cette option pour rechercher des attaques sur ce service et pour consigner un message après la détection. Cette option est principalement utilisée à des fins de dépannage.
- **Detect and Prevent** : sélectionnez cette option pour rechercher et empêcher des attaques pour ce service. Après la détection, un message est consigné et une mesure préventive est prise.

Pour que les messages IPS soient consignés, vous devez configurer l'IPS en tant qu'installation. Pour obtenir plus d'informations, reportez-vous au **Fenêtre Logs Facility and Severity, page 203**

ÉTAPE 3 Cliquez sur **Apply** pour enregistrer les paramètres.

6

Utilisation des services Cisco ProtectLink Security

La gamme SA500 prend en charge les services Cisco ProtectLink security. Ces services assurent des couches de protection contre différentes menaces de sécurité sur votre réseau.

- **Cisco ProtectLink Web** offre à tous les utilisateurs une protection contre les menaces Web afin d'éviter l'accès à des sites Web dangereux, ainsi qu'un filtrage des adresses URL destiné au contrôle de l'accès des employés à des sites Web considérés comme non liés à des sujets professionnels.
- **Cisco ProtectLink Gateway** fournit les fonctionnalités de sécurité Web de ProtectLink Web et les combine avec la sécurité de la messagerie électronique pour empêcher tout courrier indésirable, virus et tentatives de phishing dans la messagerie électronique.
- **Cisco ProtectLink Endpoint** protège les ordinateurs de bureau, les ordinateurs portables et les serveurs contre les virus, les logiciels espions et d'autres menaces Web sans exécuter de logiciel sur un serveur.

Pour obtenir des informations sur ces services, cliquez sur **ProtectLink** dans la barre de menus. Pour acheter, s'enregistrer ou activer le service, cliquez sur **Administration** sur la barre de menus, puis cliquez sur **License Management**.

Une fois votre service activé, utilisez les liens du volet de navigation pour configurer les services ProtectLink. Pour plus d'informations, reportez-vous à la documentation de Cisco ProtectLink Security à l'adresse : www.cisco.com/go/protectlink.

7

La configuration VPN

Ce chapitre décrit la procédure de configuration un réseau privé virtuel (VPN) pour permettre à d'autres sites et travailleurs distants d'accéder à vos ressources réseau. Il comprend les sections suivantes :

- **À propos du VPN**
- **Configuration d'un tunnel VPN de site à site**
- **Configuration d'un tunnel VPN IPsec d'accès à distance avec un client VPN**
- **Configuration d'un VPN SSL pour un accès à distance à partir d'un navigateur**
- **Configuration de la protection d'identité VeriSign™**

Pour accéder aux pages VPN, cliquez sur *VPN* dans la barre de menus de Configuration Utility.

À propos du VPN

Un VPN fournit un canal de communication sécurisé (« tunnel ») entre deux routeurs de passerelle ou entre un PC distant et un routeur de passerelle, comme dans les scénarios suivants :

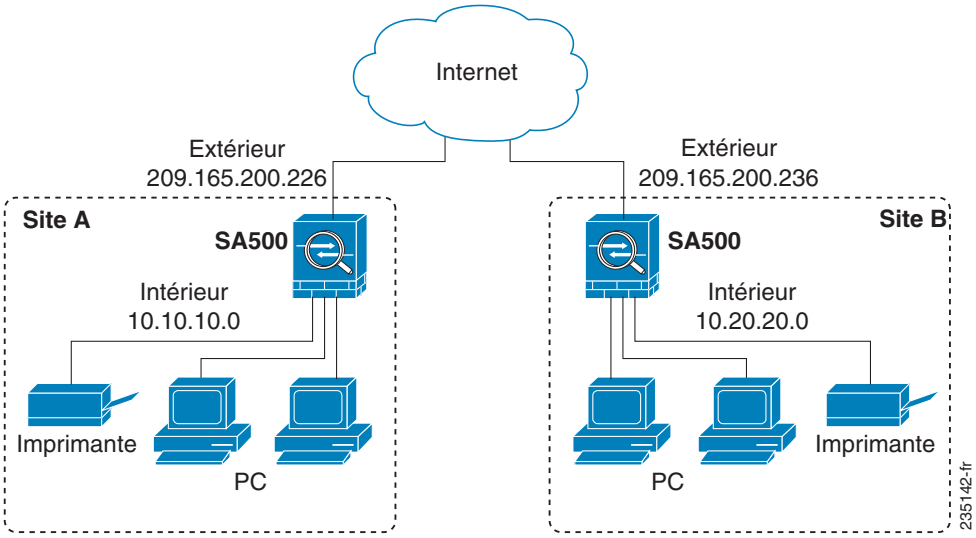
- **VPN de site à site :** le tunnel VPN connecte deux routeurs pour sécuriser le trafic entre deux sites physiquement séparés. Voir aussi **Configuration d'un tunnel VPN de site à site, page 145.**
- **Accès à distance avec un logiciel client VPN IPsec :** un travailleur distant utilise un logiciel client VPN sécurisé pour accéder au réseau d'entreprise. Voir aussi **Configuration d'un tunnel VPN de site à site, page 145**.
- **Accès à distance avec un navigateur Web :** un travailleur distant utilise un navigateur Web pour initier un tunnel VPN pour accéder aux services

disponibles sur le réseau d'entreprise. Voir aussi **Configuration d'un VPN SSL pour un accès à distance à partir d'un navigateur, page 164.**

Configuration d'un tunnel VPN de site à site

L'utilitaire de configuration comprend un assistant VPN qui vous permet de configurer facilement les paramètres VPN pour permettre à d'autres sites de se connecter à votre réseau.

Figure 5 VPN de site à site



L'assistant VPN vous aide à configurer un tunnel VPN IPsec. L'assistant définit la plupart des paramètres sur les valeurs par défaut comme suggéré par le consortium VPN (VPNC) et suppose une clé prépartagée, qui simplifie considérablement la configuration. Après avoir créé les stratégies via l'assistant VPN, vous pouvez mettre à jour tous les paramètres à l'aide des autres options du volet de navigation.

REMARQUE Pour obtenir des informations sur les recommandations du VPNC, rendez-vous sur le site Web suivant : www.vpnc.org/vpn-standards.html

ÉTAPE 1 Cliquez sur **VPN > IPsec > VPN Wizard** ou sur la page Getting Started (Advanced), sous **Site-to-Site VPN**, cliquez sur **VPN Wizard**.

La fenêtre VPN Wizard s'ouvre.

ÉTAPE 2 Dans la zone **About VPN Wizard**, choisissez **Site-to-Site** pour créer un tunnel VPN de site à site depuis l'appliance de sécurité vers une autre passerelle VPN.

ÉTAPE 3 Dans la zone **Connection Name and Remote IP Type**, saisissez les informations suivantes :

- **What is the new connection name? :** saisissez un nom pour la connexion. Le nom est utilisé à des fins de gestion et d'identification.
- **What is the pre-shared Key? :** saisissez la valeur souhaitée, que le périphérique homologue doit fournir pour établir une connexion. La longueur de la clé prépartagée est comprise entre 8 et 49 caractères et doit être saisie exactement de la même façon à cet endroit et sur la passerelle ou le client VPN distant.

  REMARQUE Si l'appliance de sécurité de l'autre site est configurée, la même clé prépartagée doit être saisie sur ce périphérique. N'utilisez pas de guillemet double (") dans la clé prépartagée.
- **Local WAN Interface :** choisissez l'interface WAN que vous souhaitez utiliser pour ce tunnel VPN : **Dedicated WAN** ou **Optional WAN**.

ÉTAPE 4 Dans la zone **Remote & Local WAN Addresses**, saisissez les informations suivantes relatives au serveur distant et au serveur local :

- **Remote Gateway Type :** choisissez **IP Address** si vous souhaitez saisir l'adresse IP du périphérique distant ou choisissez **Fully Qualified Domain Name (FQDN)** si vous souhaitez saisir le nom de domaine du réseau distant, par exemple vpn.company.com. Saisissez ensuite cette adresse ou ce nom dans champ **Remote WAN's IP Address or Internet Name**.

  Pour l'exemple illustré dans la **Figure 5**, le site distant, Site B, possède l'adresse IP publique 209.165.200.236. Vous choisissez le type IP Address et vous saisissez 209.165.200.236 dans le champ IP Address ou Internet Name.
- **Local Gateway Type :** ce champ peut rester vide si vous utilisez le même FQDN ou adresse IP que celle spécifiée dans la configuration du port WAN. Choisissez **IP Address** si vous souhaitez saisir une adresse IP ou choisissez **Fully Qualified Domain Name (FQDN)** si vous souhaitez saisir un nom de domaine, par exemple vpn.company.com. Saisissez ensuite cette adresse ou ce nom dans champ **Local WAN's IP Address or Internet Name**.

Pour l'exemple illustré dans la **Figure 5**, le site local, Site A, possède l'adresse IP publique 209.165.200.226. Vous choisissez le type IP Address et vous saisissez 209.165.200.226 dans le champ IP Address ou Internet Name.

ÉTAPE 5 Dans la zone **Secure Connection Remote Accessibility**, saisissez les informations suivantes relatives au LAN et au site distant :

- **Remote LAN IP Address :** saisissez l'adresse IP du LAN distant.

  Pour l'exemple illustré dans la **Figure 5**, le site distant, Site B, possède l'adresse IP du LAN 10.20.20.0.

- **Remote LAN Subnet Mask :** saisissez le masque de sous-réseau associé à l'adresse IP de sous-réseau entrée ci-dessus.

  Pour l'exemple illustré dans la **Figure 5**, le site distant, Site B, possède le masque de sous-réseau 255.0.0.0.

  REMARQUE La plage d'adresses IP utilisée sur le LAN distant doit être différente de la plage d'adresses IP utilisée sur le réseau LAN.

ÉTAPE 6 Cliquez sur **Apply** pour enregistrer les paramètres.

Les paramètres ne sont pas enregistrés sur la page Wizard. L'assistant crée une stratégie VPN et une stratégie IKE en fonction de vos entrées.

REMARQUE **Étapes suivantes** :

- Si vous êtes sur la page Getting Started (Advanced), cliquez sur **Getting Started > Advanced** pour retourner à la liste des tâches de configuration pour **Site-to-Site VPN**.
- Pour vérifier ou mettre à jour la stratégie VPN configurée, cliquez sur **IPsec > VPN Policies**. Pour obtenir plus d'informations, reportez-vous à la section **Configuration des stratégies VPN IPsec, page 157**.
- Pour vérifier ou mettre à jour la stratégie IKE configurée, cliquez sur **IPsec > IKE Policies**. Pour obtenir plus d'informations, reportez-vous à la section **Configuration des stratégies IKE pour VPN IPsec, page 153.**
- Pour configurer le transfert IPsec, cliquez sur **IPsec > Passthrough**. Pour obtenir plus d'informations, reportez-vous à la section **Configuration du transfert IPsec, page 162**.

Configuration d'un tunnel VPN IPsec d'accès à distance avec un client VPN

Cette section décrit la procédure de configuration d'un tunnel IPsec VPN pour l'accès à distance avec un client VPN ou à l'aide de Standard IPsec (Xauth). L'assistant VPN vous aide à configurer un tunnel pour permettre aux travailleurs de se connecter à votre réseau à partir d'emplacements distants à l'aide d'un client VPN IPsec. Après avoir créé les stratégies via l'assistant, vous pouvez mettre à jour tous les paramètres à l'aide des autres options du volet de navigation.

L'assistant définit la plupart des paramètres sur les valeurs par défaut comme suggéré par le consortium VPN (VPNC) et suppose une clé prépartagée, qui simplifie considérablement la configuration. Pour obtenir des informations sur les recommandations du VPNC, consultez : www.vpnc.org/vpn-standards.html.

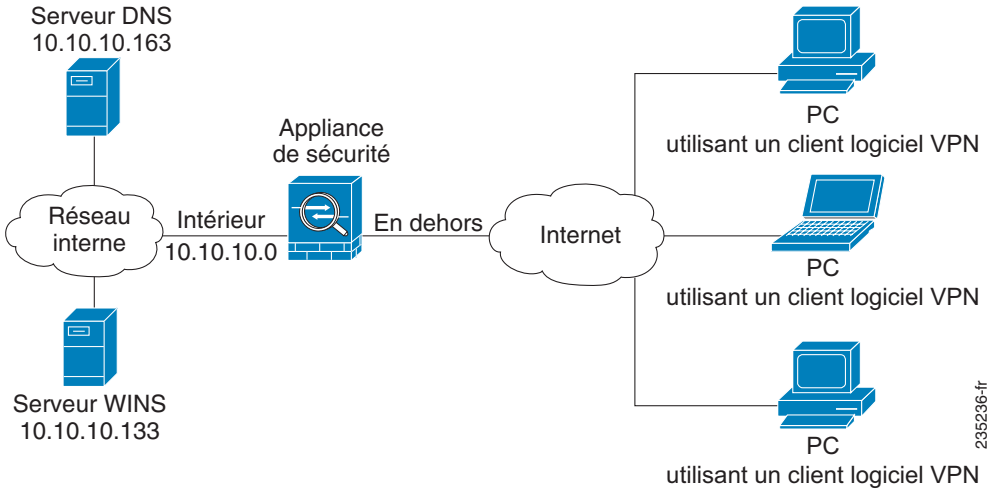
Avec les paramètres par défaut de l'assistant, vous devez ajouter des utilisateurs VPN via la page des utilisateurs VPN IPsec une fois l'assistant terminé. Vous pouvez également modifier la stratégie IKE pour permettre une authentification XAUTH (Extended Authentication) à partir des enregistrements utilisateur stockés sur un serveur d'authentification externe comme un serveur RADIUS.

Pour obtenir plus d'information sur la configuration d'un tunnel IPsec entre SA500 et un client VPN Cisco, reportez-vous à la note d'application dans la documentation technique : www.cisco.com/go/sa500resources.

Le logiciel client Cisco VPN est disponible au téléchargement à l'adresse suivante : www.cisco.com/go/ciscovpnclient. Pour Windows sélectionner Cisco VPN Client v5.x. Pour Mac OS sélectionner Cisco VPN Client v4.x.

REMARQUE Un contrat d'assistance de trois ans Cisco Small Business (CON-SBS-SVC2) est requis pour télécharger le logiciel client. Si vous n'en disposez pas, contactez votre partenaire ou revendeur, ou l'assistance Cisco pour plus d'informations.

Figure 6 Accès à distance VPN IPsec avec un client VPN



ÉTAPE 1 Cliquez sur **VPN > IPsec > VPN Wizard** ou, sur la page Getting Started (Advanced), sous **IPsec VPN Remote Access**, cliquez sur **VPN Wizard**.

La fenêtre VPN Wizard s'ouvre.

ÉTAPE 2 Dans la zone **About VPN Wizard**, choisissez **Remote Access** pour permettre à l'appliance de sécurité de donner accès aux PC distants qui exécutent le logiciel client VPN.

ÉTAPE 3 Dans la zone **Connection Name and Remote IP Type**, saisissez les informations suivantes :

- **What is the new connection name? :** saisissez un nom pour la connexion. Le nom est utilisé à des fins de gestion et d'identification.
- **What is the pre-shared Key? :** saisissez la valeur souhaitée, que le périphérique homologue doit fournir pour établir une connexion. La longueur de la clé prépartagée est comprise entre 8 et 49 caractères et doit être saisie exactement de la même façon à cet endroit et sur le client distant.

  REMARQUE N'utilisez pas de guillemet double (") dans la clé prépartagée.
- **Local WAN Interface :** si vous avez configuré deux WAN, choisissez l'interface que vous souhaitez utiliser pour ce tunnel VPN. Si vous avez configuré un seul WAN, choisissez Dedicated WAN.

ÉTAPE 4 Dans la zone **Remote & Local WAN Addresses**, saisissez les informations suivantes relatives au serveur distant et au serveur local :

- **Remote Gateway Type :** choisissez **Fully Qualified Domain Name (FQDN)** puis saisissez un nom dans le champ **Remote WAN's IP Address or Internet Name** pour identifier le client VPN sur la passerelle.
- **Local Gateway Type :** ce champ peut rester vide si vous utilisez le même FQDN ou adresse IP que celle spécifiée dans la configuration du port WAN. Choisissez **IP Address** si vous souhaitez saisir une adresse IP ou choisissez **Fully Qualified Domain Name (FQDN)** si vous souhaitez saisir un nom de domaine, par exemple vpn.company.com. Saisissez ensuite cette adresse ou ce nom dans champ **Local WAN's IP Address or Internet Name**.

ÉTAPE 5 Cliquez sur **Apply** pour enregistrer les paramètres.

REMARQUE **Étapes suivantes :**

- Si vous êtes sur la page Getting Started (Advanced), cliquez sur **Getting Started > Advanced** pour retourner à la liste des tâches de configuration pour **IPsec Remote Access VPN**.
- **Obligatoire :** configurez les utilisateurs du VPN.
  - Pour ajouter des utilisateurs à la base de données utilisateur, continuez avec la procédure **Configuration de la base de données utilisateur pour l'accès à distance VPN IPsec, page 151.**
  - Pour permettre l'authentification XAUTH à partir des enregistrements utilisateur stockés sur un serveur d'authentification externe comme RADIUS, consultez **Configuration des stratégies IKE pour VPN IPsec, page 153**.
- Pour vérifier ou mettre à jour la stratégie VPN configurée, cliquez sur **IPsec > VPN Policies**. Pour obtenir plus d'informations, reportez-vous à la section **Configuration des stratégies VPN IPsec, page 157**.
- Pour vérifier ou mettre à jour la stratégie IKE configurée, cliquez sur **IPsec > IKE Policies**. Pour obtenir plus d'informations, reportez-vous à la section **Configuration des stratégies IKE pour VPN IPsec, page 153.**
- Pour configurer le transfert IPsec, cliquez sur **IPsec > Passthrough**. Pour obtenir plus d'informations, reportez-vous à la section **Configuration du transfert IPsec, page 162**.

Configuration de la base de données utilisateur pour l'accès à distance VPN IPsec

Si vous utilisez VPN IPsec pour l'accès à distance par les travailleurs distants, cette page permet de gérer les utilisateurs (XAUTH et Cisco QuickVPN). La passerelle VPN authentifie les utilisateurs de cette liste lorsque XAUTH est utilisé dans une stratégie IKE.

Vous pouvez également activer l'authentification XAUTH à partir des enregistrements utilisateur stockés sur un serveur d'authentification externe comme un serveur RADIUS, consultez **Configuration des stratégies IKE pour VPN IPsec, page 153**.

Si vous utilisez le client VPN Cisco, reportez-vous à la note d'application dans la documentation technique : www.cisco.com/go/sa500resources.

ÉTAPE 1 Cliquez sur **VPN > IPsec > IPsec Users**.

La fenêtre IPsec Users s'ouvre. Tous les utilisateurs existants sont répertoriés dans le tableau List of IPsec Users.

ÉTAPE 2 Cliquez sur **Add** pour ajouter un utilisateur.

Autres options : cliquez sur le bouton **Edit** pour modifier une entrée. Pour supprimer une entrée, sélectionnez la case correspondante, puis cliquez sur **Delete**. Pour sélectionner toutes les entrées, sélectionnez la case dans la première colonne de l'en-tête du tableau.

Lorsque vous cliquez sur Add ou Edit, la fenêtre IPsec User Configuration s'ouvre.

ÉTAPE 3 Saisissez les informations suivantes :

- **User Name :** saisissez un identifiant unique pour l'utilisateur XAUTH.
- **Remote Peer Type :** sélectionnez l'une des options suivantes :
  - Standard IPsec (XAuth)
  - Cisco QuickVPN

    X-Auth est une norme IPsec qui étend l'authentification en IPsec natif pour fournir les informations d'identification des utilisateurs. XAUTH peut être utilisé si une sécurité supplémentaire du client est nécessaire avec les clients IPsec tels que Greenbow. QuickVPN est un client Cisco propriétaire/Linksys qui utilise l'authentification des utilisateurs mais la mise en œuvre est spécifique au QuickVPN uniquement. Cette option doit être sélectionnée lorsque les clients utilisent le client QuickVPN.

- **Allow user to change password? :** si vous choisissez Cisco QuickVPN en tant que type de l'homologue distant, vous pouvez cocher cette case pour autoriser l'utilisateur à modifier le mot de passe.
- **Password:** saisissez un mot de passe alphanumérique pour cet utilisateur.
- **Confirm Password :** confirmez les caractères que vous avez saisis dans le champ Password.
- **LAN IP address :** saisissez le sous-réseau IP LAN vers lequel l'utilisateur aura accès à distance. Le sous-réseau doit faire partie des adresses IP LAN ou VLAN.
- **Subnet Mask** : saisissez le masque de sous-réseau pour le sous-réseau local.

ÉTAPE 4 Cliquez sur **Apply** pour enregistrer les paramètres.

ÉTAPE 5 Répétez autant que nécessaire pour chaque utilisateur que vous devez ajouter.

REMARQUE **Étapes suivantes :**

- Si vous êtes sur la page Getting Started (Advanced), cliquez sur **Getting Started > Advanced** pour retourner à la liste des tâches de configuration pour **IPsec VPN Remote Access**.
- Éventuellement, vérifiez et modifiez les paramètres et les stratégies par défaut. Voir aussi **Configuration avancée du VPN IPsec, page 152**.
- Pour Cisco QuickVPN, vous devez également activer la gestion à distance. Voir aussi **RMON (Gestion à distance), page 211**.

Configuration avancée du VPN IPsec

Les rubriques suivantes sont utiles pour les utilisateurs souhaitant vérifier et modifier les paramètres créés par l'assistant VPN.

- **Affichage des valeurs par défaut des paramètres de base pour VPN IPsec**
- **Configuration des stratégies IKE pour VPN IPsec**
- **Configuration des stratégies VPN IPsec**

Affichage des valeurs par défaut des paramètres de base pour VPN IPsec

Pour afficher les valeurs par défaut des paramètres de base configurés par l'assistant, cliquez sur **VPN** dans la barre de menus, puis cliquez sur **IPsec > Basic Setting Defaults**.

Configuration des stratégies IKE pour VPN IPsec

Le protocole IKE (Internet Key Exchange) est un protocole de négociation comprenant une méthode de cryptage pour protéger les données et garantir la confidentialité. Il s'agit également d'une méthode d'authentification pour vérifier l'identité des périphériques qui tentent de se connecter au réseau. Vous pouvez créer des stratégies IKE pour définir les paramètres de sécurité comme l'authentification de l'homologue, les algorithmes de cryptage, etc. à utiliser dans ce processus.

Vous pouvez choisir d'authentifier des utilisateurs de la base de données utilisateur (consultez **Configuration de la base de données utilisateur pour l'accès à distance VPN IPsec**Configuration de la base de données utilisateur pour l'accès à distance VPN IPsec) ou d'un serveur d'authentification externe comme un serveur RADIUS (en choisissant l'option IPsec Host dans le champ XAUTH de cette page.

REMARQUE L'assistant VPN est la méthode recommandée pour créer les stratégies IKE et VPN correspondantes pour un tunnel VPN. Une fois que l'assistant a créé les stratégies IKE et VPN correspondantes, vous pouvez apporter des modifications selon vos besoins. Les utilisateurs avancés peuvent créer une stratégie IKE à partir de l'option **Add** mais ils doivent être certains d'utiliser les paramètres de cryptage, d'authentification et de groupes de clés compatibles avec la stratégie VPN.

ÉTAPE 1 Cliquez sur **VPN > IPsec > IKE Policies**. Les entrées existantes sont affichées dans le tableau List of IKE Policies.

La fenêtre IKE Policies s'ouvre. Toutes les politiques existantes sont répertoriées dans le tableau List of IKE Policies.

ÉTAPE 2 Cliquez sur **Edit** pour modifier une entrée.

Autres options : cliquez sur **Add** pour ajouter une entrée. Pour supprimer une entrée, sélectionnez la case correspondante, puis cliquez sur **Delete**. Pour sélectionner toutes les entrées, sélectionnez la case de la première colonne de l'en-tête du tableau.

Lorsque vous cliquez sur Add ou Edit, la fenêtre IKE Policy Configuration s'ouvre.

ÉTAPE 3 Dans la zone **General**, saisissez les informations suivantes :

- **Policy Name :** saisissez un nom unique à des fins d'identification et de gestion.
- **Direction/Type :** sélectionnez l'une des options suivantes :
  - **Initiator :** l'appliance de sécurité initie la connexion à la terminaison distante.
  - **Responder :** l'appliance de sécurité reste passive et répond aux requêtes IKE à distance.
  - **Both :** l'appliance de sécurité fonctionne en mode initiateur ou répondeur.
- **Exchange Mode :** sélectionnez l'une des options suivantes :
  - **Main Mode :** sélectionnez cette option pour une sécurité plus élevée, mais avec une connexion plus lente. Le mode principal dépend des échanges de clés bidirectionnels entre l'initiateur et le destinataire. Le processus d'échange de clés ralentit la connexion, mais augmente la sécurité.
  - **Aggressive Mode :** choisissez cette option si vous souhaitez une connexion plus rapide, mais avec une sécurité réduite. En mode agressif, les échanges de clés entre l'initiateur et le destinataire sont moins nombreux. Les deux côtés échangent des informations, même avant qu'un canal sécurisé n'existe. Cette fonctionnalité crée une connexion plus rapide mais avec moins de sécurité que le mode principal.

    REMARQUE Si vous sélectionnez **Main Mode**, vous devez utiliser une adresse IP comme type d'identifiant pour le périphérique local et le périphérique distant, dessous. Si le type d'identifiant est FQDN, User FQDN ou DER ASN1 DN, le mode principal est désactivé et le mode agressif est appliqué.

ÉTAPE 4 Dans la zone **Local**, saisissez les informations suivantes :

- **Identifier Type** et **Identifier :** choisissez le type d'identifiant pour le périphérique local, puis saisissez l'ID dans la zone de texte.
  - IP du WAN local
  - Internet Address/FQDN
  - User FQDN

- DER ASN1 DN.

REMARQUE Généralement, une adresse IP est utilisée pour les connexions de site à site, l'adresse IP ou FQDN étant des informations connues. Une adresse IP est obligatoire si vous souhaitez utiliser le mode principal. Pour les connexions de client distant, l'identifiant User FQDN n'est jamais résolu mais fournit un moyen d'identifier un client qui peut disposer de plusieurs adresses IP selon le réseau utilisé pour établir la connexion. Le DER ASN1 DN est utilisé comme identifiant lorsque des certificats sont utilisés pour l'authentification.

ÉTAPE 5 Dans la zone **Remote**, saisissez les informations suivantes :

- **Identifier Type** et **Identifier :** choisissez le type d'identifiant pour le périphérique local, puis saisissez l'ID dans la zone de texte.

  REMARQUE Une adresse IP est obligatoire si vous souhaitez utiliser le mode principal.

ÉTAPE 6 Dans la zone **IKE SA Parameters**, saisissez les informations relatives aux paramètres SA (Security Association), qui définissent la puissance et le mode de négociation du SA.

- **Encryption Algorithm :** algorithme utilisé pour négocier le SA. Il existe cinq algorithmes pris en charge par ce routeur : DES, 3DES, AES-128, AES-192 et AES-256.
- **Authentication Algorithm :** spécifiez l'algorithme d'authentification pour l'en-tête VPN. Il existe cinq algorithmes pris en charge par ce routeur : MD5, SHA-1, SHA2-256, SHA2-384 et SHA2-512.

  REMARQUE Vérifiez que l'algorithme d'authentification est configuré de manière identique des deux côtés.

- **Authentication Method :** sélectionnez une clé prépartagée pour une clé simple basée sur un mot de passe. La sélection de RSA-Signature désactive la zone de texte de clé prépartagée et utilise le certificat Active Self chargé sur la page Certificates. Dans ce cas, un certificat doit être configuré pour que la signature RSA fonctionne. Voir aussi **Gérer les certificats pour l'authentification, page 204**.

  REMARQUE Le guillemet double (") n'est pas autorisé pour la clé partagée.

- **Pre-shared key :** saisissez la clé alphanumérique à partager avec l'homologue IKE.

- **Diffie-Hellman (DH) Group :** choisissez l'algorithme Diffie-Hellman à utiliser lors de l'échange de clés. Le groupe DH définit la puissance de l'algorithme en bits.
- **SA Lifetime (seconds) :** saisissez le nombre de secondes pendant lesquelles l'association de sécurité reste valide.
- **Enable Dead Peer Detection :** cochez cette case pour autoriser l'appliance de sécurité à détecter si un homologue est actif ou non. Si un homologue est détecté comme mort, alors l'appliance de sécurité supprime l'association de sécurité entre IPsec et IKE.
- **Detection Period (seconds) :** la période de détection est l'intervalle entre des messages DPD R-U-THERE consécutifs. Les messages DPD R-U-THERE sont envoyés uniquement lorsque le trafic IPsec est inactif.
- **Reconnect after failure count :** nombre maximum d'échecs de DPD autorisés avant de couper la connexion.

ÉTAPE 7 Dans la zone **Extended Authentication (XAUTH)**, vous pouvez activer le routeur de passerelle VPN pour authentifier les utilisateurs de la base de données utilisateur (option par défaut) ou un serveur d'authentification externe comme RADIUS. Choisissez l'un des **types XAUTH** suivants :

- **None :** sélectionnez cette option pour désactiver XAUTH.
- **User Database :** sélectionnez cette option si vous voulez authentifier des utilisateurs d'après les comptes créés dans cet utilitaire de configuration. Si vous choisissez cette option, ajoutez les utilisateurs sur la page IPsec Users. Voir aussi **Configuration de la base de données utilisateur pour l'accès à distance VPN IPsec, page 151.**
- **IPsec Host :** sélectionnez cette option si vous voulez que l'appliance de sécurité soit authentifiée par une combinaison de nom d'utilisateur et mot de passe. Dans ce mode, l'appliance de sécurité agit en tant que client VPN de la passerelle distante. Si vous choisissez cette option, entrez également un nom d'utilisateur et un mot de passe.
  - **Username :** si vous avez choisi IPsec Host comme type de XAUTH, saisissez le nom d'utilisateur utilisé par l'appliance de sécurité lors de la connexion au serveur distant. Le nom d'utilisateur peut comprendre tous les caractères alphanumériques.
  - **Password :** saisissez le mot de passe utilisé par l'appliance de sécurité lors de la connexion au serveur distant.

ÉTAPE 8 Cliquez sur **Apply** pour enregistrer les paramètres.

REMARQUE **Étapes suivantes**

- Pour vérifier ou mettre à jour la stratégie VPN configurée, cliquez sur **IPsec > VPN Policies**. Pour obtenir plus d'informations, reportez-vous à la section **Configuration des stratégies VPN IPsec, page 157**.
- Pour vérifier ou mettre à jour la stratégie IKE configurée, cliquez sur **IPsec > IKE Policies**. Pour obtenir plus d'informations, reportez-vous à la section **Configuration des stratégies IKE pour VPN IPsec, page 153.**
- Pour configurer le transfert IPsec, cliquez sur **IPsec > Passthrough**. Pour obtenir plus d'informations, reportez-vous à la section **Configuration du transfert IPsec, page 162**.
- Pour configurer les utilisateurs VPN (pour le VPN d'accès à distance uniquement), cliquez sur **IPsec > IPsec Users**. Voir aussi **Configuration de la base de données utilisateur pour l'accès à distance VPN IPsec, page 151.**
- Pour configurer l'appliance de sécurité afin qu'elle fonctionne avec votre serveur RADIUS, consultez **Configurer les enregistrements du serveur RADIUS, page 207**.

Configuration des stratégies VPN IPsec

Cette page vous permet de gérer les stratégies VPN. Cette page contient les tableaux List of VPN Policies et List of back up Policies Ces tableaux répertorient les stratégies qui ont été ajoutées et permettent plusieurs opérations sur les stratégies.

REMARQUE Avant de créer une stratégie automatique, créez tout d'abord une stratégie IKE. Ensuite vous pouvez appliquer la stratégie IKE sur cette page. Pour obtenir plus d'informations, reportez-vous à la section **Configuration des stratégies IKE pour VPN IPsec, page 153.**

ÉTAPE 1 Cliquez sur **VPN > IPsec > VPN Policies**.

La fenêtre VPN Policies s'ouvre. Deux tableaux s'affichent :

- **List of VPN Policies :** répertorie les stratégies VPN à l'exception des stratégies de sauvegarde. Les stratégies automatiques et manuelles sont incluses.

- **List of back up Policies :** répertorie toutes les stratégies configurées en tant que stratégie de sauvegarde. Ces stratégies sont créées lorsque vous créez une stratégie IKE et que vous sélectionnez l'option **Enable Redundant Gateway**. La stratégie prend effet uniquement si la stratégie principale échoue. Vous ne pouvez pas activer, désactiver, modifier ou supprimer des stratégies de sauvegarde. Vous pouvez uniquement agir sur la stratégie principale, à l'aide des boutons du tableau List of VPN Policies.

ÉTAPE 2 Pour ajouter une stratégie VPN, cliquez sur **Add**.

Autres options : cliquez sur le bouton **Edit** pour modifier une entrée. Pour supprimer une entrée, sélectionnez la case correspondante, puis cliquez sur **Delete**. Pour sélectionner toutes les entrées, sélectionnez la case de la première colonne de l'en-tête du tableau.

Lorsque vous cliquez sur Add ou Edit, la fenêtre VPN Policy Configuration s'ouvre.

ÉTAPE 3 Dans la zone **General**, saisissez les informations suivantes :

- **Policy Name :** entrez un nom unique pour identifier la stratégie.
- **Policy Type :** choisissez l'un des types suivants :
  - **Auto :** certains paramètres du tunnel VPN sont générés automatiquement. Le protocole IKE (Internet Key Exchange) est utilisé pour effectuer des négociations entre les deux points de terminaison VPN. Pour créer une stratégie VPN automatique, vous devez d'abord créer une stratégie IKE puis ajouter la stratégie automatique correspondante.
  - **Manual :** tous les paramètres (y compris les clés) du tunnel VPN sont entrés manuellement pour chaque point de terminaison. Aucun serveur ou organisation tiers n'est impliquée.
- **Select Local Gateway :** si vous avez configuré le port facultatif pour qu'il soit utilisé en tant que port WAN, choisissez l'interface WAN qui agira comme l'une des extrémités du tunnel : **Dedicated WAN** ou **Optional WAN**.
- **Remote End Point :** choisissez d'identifier le point de terminaison distant par l'adresse IP ou le nom Internet/FQDN de la passerelle distante ou du PC client. Saisissez également l'adresse IP ou le nom Internet/FQDN dans le champ situé au-dessous de la liste déroulante.
- **Enable NetBIOS :** cochez cette case pour activer NetBIOS, un programme qui effectue la résolution de nom. Cette option permet aux diffusions NetBIOS de se déplacer via le tunnel VPN.

- **Enable RollOver :** cette option s'applique si vous disposez de deux liaisons FAI et si vous avez activé le renvoi automatique **Configuration du renvoi automatique, de l'équilibrage de charge et de la détection des défaillances, page 59).** Dans ce cas, vous pouvez cocher la case **Enable RollOver** pour vous assurer que le trafic VPN est renvoyé sur la liaison de secours chaque fois que la liaison principale échoue. L'appliance de sécurité met à jour automatiquement la passerelle WAN locale pour le tunnel en fonction de la configuration facultative de liaison WAN. Pour ce type de configuration, le DNS dynamique doit être configuré car l'adresse IP est modifiée par le basculement. Voir aussi **DNS dynamique, page 79.**

ÉTAPE 4 Dans les zones **Local Traffic Selection** et **Remote Traffic Selection**, saisissez les informations suivantes pour spécifier les adresses IP qui sont de part et d'autre du tunnel :

- **Local IP** ou **Remote IP :** sélectionnez l'une des options suivantes :
  - **Any :** autorise tout le trafic du point de terminaison spécifié. Notez que vous ne pouvez pas sélectionner **Any** pour les points de terminaison locaux et distants.
  - **Single :** permet à un seul hôte de se connecter au VPN. Si vous choisissez cette option, entrez également l'adresse IP de l'hôte dans le champ Start IP Address.
  - **Range :** permet à tous les ordinateurs dans une plage d'adresses IP de se connecter au VPN. Si vous choisissez cette option, indiquez également la plage en saisissant l'adresse IP de début et l'adresse IP de fin.
  - **Subnet :** permet à tous les ordinateurs sur un sous-réseau de se connecter au VPN. Si vous choisissez cette option, entrez également l'adresse réseau et le masque de sous-réseau.

ÉTAPE 5 Si vous avez choisi le type de stratégie Manual Policy, créez une SA (association de sécurité) en saisissant les entrées statiques suivantes dans la zone **Manual Policy Parameters** :

- **SPI-Incoming** ou **SPI-Outgoing :** saisissez une valeur hexadécimale comprise entre 3 et 8 caractères. Par exemple : 0a1234.
- **Encryption Algorithm :** choisissez l'algorithme utilisé pour crypter les données.
- **Key-In :** saisissez la clé de cryptage de la stratégie entrante.
- **Key-Out :** clé de cryptage de la stratégie sortante.

La longueur des clés dépend de l'algorithme choisi :

- **DES :** 8 caractères
- **3DES :** 24 caractères
- **AES-128 :** 16 caractères
- **AES-192 :** 24 caractères
- **AES-256 :** 32 caractères
- **AES-CCM :** 16 caractères

- **Integrity Algorithm :** choisissez l'algorithme utilisé pour vérifier l'intégrité des données.
- **Key-In :** saisissez la clé d'intégrité (pour ESP avec le mode intégrité) pour la politique entrante.
- **Key-Out :** saisissez la clé d'intégrité (pour ESP avec le mode intégrité) pour la politique entrante.

  La longueur de la clé dépend de l'algorithme choisi :

  - **MD5 :** 16 caractères
  - **SHA-1 :** 20 caractères
  - **SHA2-256 :** 32 caractères
  - **SHA2-384 :** 48 caractères
  - **SHA2-512 :** 64 caractères

ÉTAPE 6 Si vous avez le type de stratégie Auto Policy, saisissez les informations suivantes dans la zone **Auto Policy Parameters** :

- **SA Lifetime :** saisissez la durée de vie de l'association de sécurité et spécifiez s'il s'agit de secondes ou de kilooctets.
  - **Seconds :** si vous spécifiez la durée de vie SA en secondes, cette valeur représente l'intervalle après lequel l'association de sécurité n'est plus valide. Le SA est renégocié après cet intervalle. La valeur par défaut est de 3600 secondes.
  - **Kilobytes :** si vous spécifiez la durée de vie SA en kilooctets, le SA est renégocié après le transfert du nombre spécifié de kilooctets de données par le SA original. La valeur minimale est de 300 secondes ou de 1920000 Ko.

REMARQUE Pour chaque stratégie, deux SA sont créés, un pour le trafic entrant et un pour le trafic sortant. Lorsque vous utilisez une durée de vie configurée en kilooctets (dite lifebyte) avec une durée de vie en secondes, le SA expire de manière asymétrique. Par exemple, le lifebyte pour un flux de téléchargement descendant expire fréquemment si le trafic en aval est très élevé, mais le lifebyte du flux de téléchargement ascendant expire moins fréquemment ou uniquement lorsque son délai d'expiration touche à sa fin. Si vous paramétrez la durée de vie en secondes et en kilooctets, vous devez réduire la différence entre les fréquences d'expiration des SA, dans le cas contraire le système pourrait manquer de ressources suite à cette asymétrie. Les spécifications de lifebyte sont généralement recommandées pour les utilisateurs avancés uniquement.

- **Encryption Algorithm :** choisissez l'algorithme utilisé pour crypter les données.
- **Integrity Algorithm :** choisissez l'algorithme utilisé pour vérifier l'intégrité des données.
- **PFS Key Group :** cochez cette case pour activer le protocole PFS (Perfect Forward Secrecy) pour améliorer la sécurité. Bien que cette option soit plus lente, elle garantit qu'un échange Diffie-Hellman est effectué pour chaque négociation de phase 2.
- **Select IKE Policy :** choisissez la stratégie IKE pour définir les caractéristiques de la phase 1 de la négociation. **Configuration des stratégies IKE pour VPN IPsec, page 153.**

ÉTAPE 7 Dans la zone **Redundant VPN Gateway Parameters**, saisissez les informations suivantes pour créer une stratégie de secours pour cette stratégie :

- **Enable Redundant Gateway for this policy? :** cochez cette case pour définir une stratégie de secours pour cette stratégie. Lorsque le tunnel pour cette stratégie est inactif, le tunnel de secours devient automatiquement actif.
- **Select Back- up Policy :** choisissez une stratégie de secours pour cette stratégie. Cette liste contient uniquement les stratégies qui peuvent être configurées comme stratégies de secours.

REMARQUE Une stratégie de secours doit remplir les conditions suivantes :
1. Le type doit être défini sur Auto.
2. Le DPD doit être activé.
3. La direction doit être initiateur ou les deux.
4. La configuration de XAuth doit être Aucune ou Hôte IPsec.
5. La stratégie doit être une passerelle uniquement et non un client.

- **Failback time to switch from back-up to primary :** saisissez le nombre de secondes nécessaires avant de confirmer le rétablissement d'un tunnel principal après une défaillance. Si le tunnel principal est actif pendant le nombre de secondes spécifié, l'appliance de sécurité bascule sur le tunnel principal en désactivant le tunnel de secours.

ÉTAPE 8 Cliquez sur **Apply** pour enregistrer les paramètres.

REMARQUE **Étapes suivantes :**

- Pour afficher l'état des tunnels VPN, cliquez sur **Status > VPN Status > IPsec Status**. Pour obtenir plus d'informations, reportez-vous à la section **Page IPsec VPN Status, page 225**.
- Pour afficher les journaux VPN IPsec, cliquez sur **Status > View Logs > IPsec VPN Logs**. Pour obtenir plus d'informations, reportez-vous à la section **Page IPsec VPN Logs, page 231**.
- Pour configurer le transfert IPsec, cliquez sur **IPsec > Passthrough**. Pour obtenir plus d'informations, reportez-vous à la section **Configuration du transfert IPsec, page 162**.
- Pour configurer une plage d'adresses IP dynamiques, consultez **Configuration d'une plage IP dynamique, page 163.**
- Pour ajouter des utilisateurs au VPN d'accès à distance, consultez **Configuration de la base de données utilisateur pour l'accès à distance VPN IPsec, page 151.**
- Si vous avez activé le renvoi, veillez à configurer le DNS dynamique. Voir aussi **DNS dynamique, page 79.**

Configuration du transfert IPsec

Vous devez configurer le transfert IPsec si certains périphériques derrière l'appliance de sécurité nécessitent de configurer des tunnels IPsec indépendamment, par exemple, pour se connecter à un autre routeur sur le WAN.

ÉTAPE 1 Cliquez sur **VPN > IPsec > Passthrough**.

La fenêtre Passthrough s'ouvre.

ÉTAPE 2 Cochez la case pour chaque type de trafic que souhaitez autoriser à traverser le tunnel VPN.

ÉTAPE 3 Cliquez sur **Apply** pour enregistrer les paramètres.

Configuration d'une plage IP dynamique

L'adresse IP est définie par la plage IP dynamique et est automatiquement configurée par défaut. Toutefois, vous pouvez utiliser la page Dynamic IP Range pour spécifier manuellement une plage de début et de fin pour l'adresse IP.

La plage IP dynamique est utilisée par les clients VPN IPsec qui se connectent au routeur à l'aide de Mode- Config.

REMARQUE Si vous créez une stratégie VPN et que vous souhaitez modifier l'adresse IP dynamique, modifiez-la avant de créer la stratégie. Sinon, les modifications ne seront pas appliquées.

ÉTAPE 1 Cliquez sur **VPN > IPsec > Dynamic IP Range.**

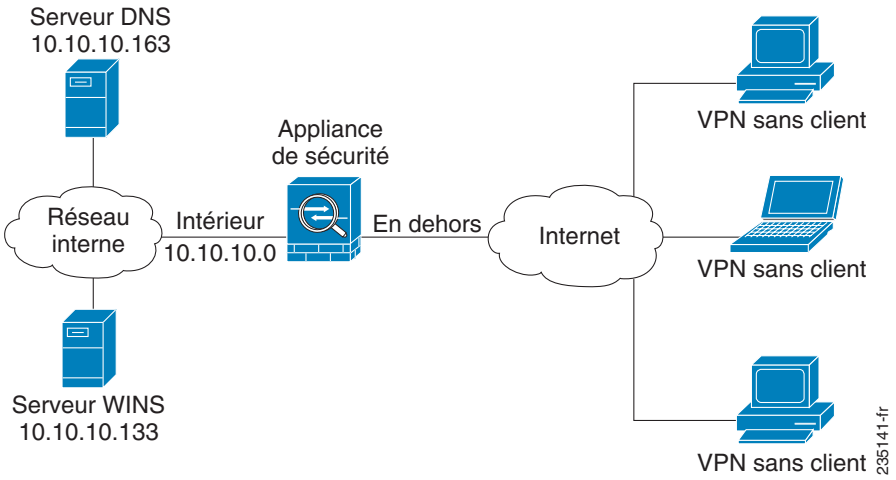
La fenêtre Dynamic IP Range s'ouvre.

ÉTAPE 2 Saisissez une plage IP de début et une plage IP de fin pour l'adresse IP.

Cliquez sur **Apply** pour enregistrer les paramètres.

Configuration d'un VPN SSL pour un accès à distance à partir d'un navigateur

La solution VPN SSL offre une méthode flexible et sécurisée permettant de déployer des ressources réseau à tous les utilisateurs distants ayant accès à Internet et à un navigateur Web. L'avantage est que vous n'avez pas à installer et à maintenir le logiciel client VPN sur les machines distantes.



Les utilisateurs peuvent accéder à distance au réseau à l'aide d'un navigateur Web. Lorsque le tunnel est établi, chaque utilisateur dispose d'une adresse IP sur le réseau interne, telle que 10.10.10.x, dans l'exemple ci-dessus.

Vous pouvez utiliser le VPN SSL pour donner accès aux types de services suivants sur votre réseau :

- Les sites Web internes
- Les applications Web
- Les partages de fichier FTP et NT/Active Directory
- Les proxy e-mail, y compris POP3S, IMAP4S et SMTPS
- MS Outlook Web Access
- MAPI
- Applications (c'est-à-dire, transfert de port pour l'accès à d'autres applications de type TCP)

L'appliance de sécurité prend en charge plusieurs sessions simultanées pour permettre aux utilisateurs distants d'accéder au LAN par une liaison cryptée via une interface personnalisable de portail utilisateur. Vous pouvez spécifier les privilèges utilisateur et vous pouvez contrôler chaque accès des utilisateurs aux ressources réseau. Vous pouvez rationaliser le processus de configuration en organisant les utilisateurs VPN en domaines et en groupes qui partagent les stratégies VPN.

REMARQUE La gestion à distance (RMON) doit être activée sinon l'accès VPN SSL sera bloqué. Pour obtenir plus d'informations, reportez-vous à la section **RMON (Gestion à distance), page 211**.

Accédez aux options du VPN SSL

L'utilisateur distant dispose de différentes options de service SSL :

- **VPN Tunnel** : le navigateur SSL de l'utilisateur distant est utilisé à la place d'un client VPN sur l'hôte distant pour établir un tunnel VPN sécurisé. Un client VPN SSL (basé sur Active-X ou Java) est installé sur l'hôte distant pour permettre au client de se connecter au réseau LAN d'entreprise avec des privilèges d'accès ou de stratégie préconfigurés. À ce stade, une interface réseau virtuelle est créée sur le PC de l'utilisateur à laquelle est attribué une adresse IP et une adresse de serveur DNS de l'appliance de sécurité.

  Pour créer un tunnel VPN, consultez **Éléments du VPN SSL, page 166**.

- **Port Forwarding** : le service de transfert de port prend en charge les connexions TCP entre l'utilisateur distant et l'appliance de sécurité. Un client Web (ActiveX ou Java) est installé sur la machine client. L'administrateur peut définir les services et les applications disponibles pour les utilisateurs de transfert de port distant. Les utilisateurs n'ont pas accès au LAN entier.

  Pour configurer le transfert de port, consultez **Configuration du transfert de port VPN SSL, page 175.**

Conseils de sécurité pour le VPN SSL

Pour réduire les risques induits par les certificats SSL :

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

Éléments du VPN SSL

Plusieurs éléments fonctionnent ensemble pour prendre en charge le VPN SSL.

- **Portal :** pour accéder au réseau, l'utilisateur démarre un navigateur Web et saisit l'URL du portail. L'appliance de sécurité est préconfigurée avec un portail que vous pouvez utiliser pour tous les utilisateurs. Vous pouvez modifier le titre, l'en-tête de la bannière, le message de la bannière, les paramètres de sécurité et le type d'accès (tunnel VPN, transfert de port, ou les deux). En outre, vous pouvez créer différentes présentations de portail selon les groupes d'utilisateurs. Par exemple, vous pouvez créer deux présentations de portail pour deux groupes qui ont accès à des ressources différentes. Sur chaque présentation de portail, vous pouvez personnaliser le message de la bannière pour fournir des informations personnalisées aux utilisateurs du portail.

  IMPORTANT : si vous comptez créer différentes présentations de portail pour différents domaines d'utilisateurs, vous devez d'abord créer les présentations de portail. Dans ce cas, commencez par l'**Étape 1 du scénario : personnalisation de la présentation du portail, page 167**. Si vous ne comptez pas créer plusieurs présentations de portail, vous pouvez démarrer le scénario par cette étape afin de pouvoir vérifier les paramètres par défaut et les modifier, selon vos besoins. En outre, la page Portal Layouts vous indique l'URL que vous devez fournir aux utilisateurs du portail.

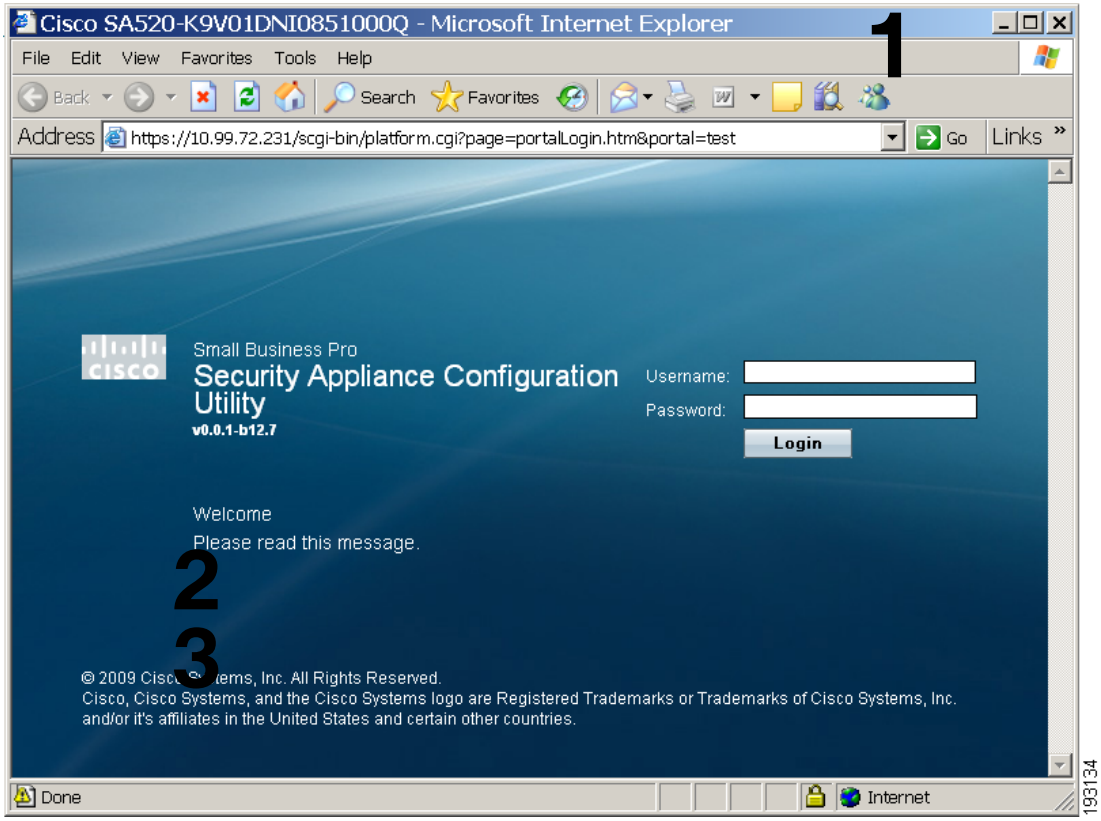
- **Users :** créez vos utilisateurs VPN. Vous pouvez utiliser le domaine et le groupe par défaut ou configurer vos propres domaines et groupes. Lorsque vous créez l'enregistrement de chaque utilisateur, sélectionnez SSL VPN User comme type d'utilisateur. Les instructions sont comprises dans le scénario mais pour plus d'informations sur les domaines, les groupes et les utilisateurs, reportez-vous au **Chapitre 8, « Administration »**..
- **VPN Policies :** les stratégies VPN par défaut doivent être suffisantes pour la plupart des objectifs. Selon les besoins, vous pouvez créer des stratégies plus complexes. Voir aussi **Création de stratégies VPN SSL, page 171.**
- **Port Forwarding :** vous pouvez configurer le transfert de port pour autoriser l'accès à un ensemble limité de ressources. Par exemple, si vous souhaitez que les utilisateurs de VPN SSL accèdent au service de messagerie électronique uniquement. Voir aussi **Configuration du transfert de port VPN SSL, page 175.**

Étape 1 du scénario : personnalisation de la présentation du portail

Lorsqu'un utilisateur distant souhaite accéder à votre réseau privé via un tunnel SSL, l'utilisateur lance un navigateur Web et saisit une URL. Le navigateur affiche une page de connexion avec plusieurs fonctionnalités que vous pouvez configurer :

1. Titre du site du portail : s'affiche en haut du navigateur
2. Titre de la bannière
3. Message de la bannière

Zones configurables de la présentation du portail VPN SSL



ÉTAPE 1 Cliquez sur **VPN > SSL VPN Server > Portal Layouts**.

La fenêtre Portal Layouts s'ouvre.

ÉTAPE 2 Pour modifier la présentation du portail par défaut, cliquez sur le bouton en forme de stylet de la colonne **Edit**.

Autres options : pour ajouter une présentation de portail, cliquez sur **Add**. Pour supprimer une présentation de portail, cochez la case puis cliquez sur **Delete**. Pour sélectionner toutes les entrées, sélectionnez la case de la première colonne de l'en-tête du tableau. Pour désigner une présentation comme présentation par défaut, cliquez sur le bouton étoile (*). Pour afficher une présentation de portail, cliquez sur le lien hypertexte de la colonne **Portal URL**.

Lorsque vous cliquez sur Add ou Edit, la fenêtre Portal Layout Configuration s'ouvre.

ÉTAPE 3 Dans la zone **Portal Layout and Theme Name**, saisissez les informations suivantes :

- **Portal Layout Name :** saisissez un nom descriptif pour le portail en cours de configuration. Le nom apparaîtra dans l'URL du portail. Ne saisissez pas les espaces ou les caractères spéciaux. Seuls les caractères alphanumériques, les tirets (« - ») et les traits de soulignement (« _ ») sont autorisés dans ce champ.
- **Portal Site Title :** saisissez le titre qui s'affiche au sommet de la fenêtre du navigateur Web pour le portail.
- **Banner Title :** saisissez un mot pour le titre de la bannière. Les espaces et les caractères spéciaux ne sont pas autorisés.
- **Banner Message :** saisissez le texte du message à afficher avec le titre de la bannière. Par exemple, saisissez les instructions ou les informations relatives aux ressources auxquelles les utilisateurs peuvent avoir accès une fois connectés. Les espaces et les caractères vides ne sont pas autorisés.
- **Display banner message on login page :** cochez la case pour afficher le titre et le message de la bannière sur la présentation de portail.
- **HTTP meta tags for cache control (recommended) :** sélectionnez ou désélectionnez cette case pour activer la fonctionnalité de sécurité, ce qui est fortement recommandé. Cette fonctionnalité garantit que les pages du portail VPN SSL et tout autre contenu Web ne peuvent pas être mis en cache. Les directives de contrôle du cache des balises méta HTTP empêchent le stockage des pages Web et des données obsolètes dans le cache du navigateur Web du client.
- **ActiveX web cache cleaner :** cochez cette case pour charger un contrôle de cache ActiveX à chaque connexion des utilisateurs à ce portail VPN SSL.

ÉTAPE 4 Dans la zone **SSL VPN Portal Pages to Display**, cochez la case pour chaque page SSL VPN Portal auxquelles les utilisateurs peuvent accéder via ce portail.

Les pages qui ne sont pas sélectionnée ne seront pas visibles dans le menu de navigation du portail VPN SSL. Toutefois, les utilisateurs peuvent encore accéder aux pages masquées, sauf si des stratégies d'accès VPN SSL sont créées pour empêcher l'accès à ces pages.

ÉTAPE 5 Cliquez sur **Apply** pour enregistrer les paramètres.

ÉTAPE 6 Pour afficher votre nouvelle page, cliquez sur le lien de la colonne Portal URL du tableau. Cette URL est celle que vous fournirez à vos utilisateurs.

ÉTAPE 7 Répétez cette opération autant que nécessaire pour ajouter plusieurs présentations de portail.

REMARQUE Étape suivante (obligatoire)

Configurez les utilisateurs du VPN SSL. Passez à la section suivante, **Étape 2 du scénario : ajouter des utilisateurs du VPN SSL.**

Étape 2 du scénario : ajouter des utilisateurs du VPN SSL.

L'authentification des utilisateurs distants du VPN SSL est réalisée par l'appliance de sécurité à l'aide d'une base de données locale sur l'appliance de sécurité ou de serveurs d'authentification externes. (c.-à-d. LDAP ou RADIUS). Le domaine d'utilisateur détermine la méthode d'authentification (base de données locale, serveur externe) à utiliser lors de la validation de la connexion de l'utilisateur distant.

Dans ce scénario, vous ajoutez tous les utilisateurs au domaine ou au groupe par défaut. Toutefois, vous pouvez créer différents domaines et groupes si vous souhaitez avoir différentes présentations de portail et différentes stratégies VPN SSL selon les utilisateurs. Pour des informations complètes sur les domaines, les groupes et les utilisateurs, ainsi que sur les stratégies utilisateur que vous pouvez configurer, reportez-vous au **Chapitre 8, « Administration ».** Pour obtenir des informations sur l'ajout des utilisateurs, consultez **Ajouter ou modifier les paramètres utilisateur, page 186.**

ÉTAPE 1 Cliquez sur **Administration > Users > Users**. Le tableau List of Users s'affiche.

La fenêtre User s'ouvre. L'administrateur et les utilisateurs invités par défaut sont affichés dans le tableau List of Users, ainsi que tous les nouveaux utilisateurs que vous ajoutez.

ÉTAPE 2 Pour ajouter un utilisateur, cliquez sur **Add**.

La fenêtre User Configuration s'ouvre.

ÉTAPE 3 Saisissez les informations suivantes :

- **User Name :** saisissez un identifiant unique pour l'utilisateur. Il peut inclure tous les caractères alphanumériques.
- **First Name :** saisissez le prénom de l'utilisateur.

- **Last Name** : entrez le nom de l'utilisateur.
- **TUser Type :** choisissez **SSL VPN User**.
- **Select Group :** choisissez **SSLVPN**.
- **Password :** saisissez un mot de passe comportant des caractères alphanumériques, ainsi que les caractères '—' ou '_'.
- **Confirm Password :** saisissez à nouveau le mot de passe.
- **Idle Timeout :** saisissez la durée, en minutes, pendant laquelle l'utilisateur peut être inactif avant la déconnexion de la session. Saisissez une valeur comprise entre 0 et 999. La valeur du délai d'expiration pour l'utilisateur est prioritaire sur le délai d'expiration pour le groupe. Si la valeur du délai d'expiration de l'utilisateur est définie sur 0, le paramètre de délai d'expiration du groupe s'applique.

  REMARQUE Chaque utilisateur est ajouté en tant qu'utilisateur local avec un mot de passe et, lorsque l'utilisateur est affecté à un mécanisme d'authentification externe en fonction du groupe, certains attributs, tels que le mot de passe local, sont ignorés.

ÉTAPE 4 Cliquez sur **Apply** pour enregistrer les paramètres.

Création de stratégies VPN SSL

Les stratégies VPN SSL donnent accès aux utilisateurs SSL configurés aux services et aux ressources réseau. Une stratégie s'applique à une ressource réseau, une adresses IP ou une plage d'adresses IP spécifiques sur le LAN ou à d'autres services VPN SSL pris en charge par l'appliance de sécurité.

Par défaut, une stratégie PERMIT globale (non affichée) est préconfigurée sur toutes les adresses et sur tous les services et les ports.

Vous pouvez créer des stratégies utilisateur, groupe et globales. Les stratégies sont appliquées en fonction des niveaux de priorité suivants :

- Les stratégies de niveau utilisateur sont prioritaires sur les stratégies de niveau groupe.
- Les stratégies de niveau groupe sont prioritaires sur les stratégies globales.
- Lorsque deux stratégies sont en conflit, une stratégie plus spécifique est prioritaire sur une stratégie générale. Par exemple, une stratégie pour une

adresse IP spécifique est prioritaire sur une stratégie pour une plage d'adresses IP comprenant cette adresse IP.

Une stratégie peut être proposée pour le tunnel VPN, le transfert de port, ou les deux.

Une stratégie entre en vigueur dès qu'elle est définie. Toutefois, si la gestion à distance (RMON) n'est pas activée, l'accès VPN SSL sera bloqué. Voir aussi **RMON (Gestion à distance), page 211.**

Si vous créez une stratégie qui s'applique à une ressource réseau, vous devez d'abord configurer un enregistrement pour la ressource réseau. Voir aussi **Spécifier les ressources réseau pour le VPN SSL, page 174.**

ÉTAPE 1 Cliquez **VPN > SSL VPN Server > SSL VPN Policies**.

La fenêtre SSL VPN Policies s'ouvre.

ÉTAPE 2 Dans la zone **Query**, choisissez les stratégies à afficher dans le tableau List of SSL VPN Policies.

- **View List of SSL VPN Policies for :** choisissez **Global** pour tous les utilisateurs, **Group** pour un groupe particulier ou **User** pour un utilisateur particulier.
- **Available Groups :** si vous avez choisi **Group** comme type de requête, sélectionnez le nom dans cette liste.
- **Available Users :** si vous avez choisi **User** comme type de requête, sélectionnez le nom dans cette liste.
- Cliquez sur **Display** pour exécuter la demande.

ÉTAPE 3 Pour ajouter une stratégie VPN SSL, cliquez sur **Add**.

Autres options : cliquez sur le bouton **Edit** pour modifier une entrée. Pour supprimer une entrée, sélectionnez la case correspondante, puis cliquez sur **Delete**. Pour sélectionner toutes les entrées, sélectionnez la case de la première colonne de l'en-tête du tableau.

Lorsque vous cliquez sur Add ou Edit, la fenêtre SSL VPN Policy Configuration s'ouvre.

ÉTAPE 4 Dans la zone **Policy For**, saisissez les informations suivantes :

- **Policy For :** sélectionnez le type de stratégie : Global, Group, ou User. Si vous choisissez Group, choisissez également le groupe dans la liste Available Groups. Si vous choisissez User, choisissez également l'utilisateur dans la liste Available Users.

ÉTAPE 5 Dans la zone **SSL VPN Policy**, saisissez les informations suivantes :

- **Apply Policy to :** choisissez d'appliquer une stratégie à une ressource réseau, une adresse IP, un réseau IP ou toutes les adresses gérées par le périphérique. Renseignez également les champs signalés par un fond blanc.
- **Policy Name :** entrez un nom pour identifier cette stratégie.

  REMARQUE Si vous créez une stratégie avec le même nom qu'une stratégie existante, la stratégie la plus récente remplace l'existante.
- **IP Address :** si vous choisissez IP Address ou Network Resource dans le champ Apply Policy, saisissez l'adresse IP du périphérique.
- **Mask Length :** si vous choisissez IP Network dans le champ Apply Policy, saisissez la longueur du masque de sous-réseau.
- **Port Range / Port Number (Begin & End) :** spécifiez un port ou une plage de ports pour appliquer la stratégie à tout le trafic TCP et UDP avec ces ports. Laissez les champs vides pour appliquer la stratégie à tout le trafic.
- **Service :** choisissez **VPN Tunnel**, **Port Forwarding** ou **All Services Defined**.
- **Defined Resources :** sélectionnez les services pour une stratégie donnée. Cette option est disponible uniquement pour les stratégies qui sont appliquées à une ressource réseau.
- **Permission :** choisissez Permit ou Deny pour cette stratégie.

ÉTAPE 6 Cliquez sur **Apply** pour enregistrer les paramètres.

REMARQUE Étapes suivantes :

Activez la gestion à distance (RMON), si vous ne l'avez pas encore fait. Si RMON est désactivé, l'accès VPN SSL est bloqué. Voir aussi **RMON (Gestion à distance), page 211.**

Spécifier les ressources réseau pour le VPN SSL

Les ressources réseau sont des services ou des groupes d'adresses IP LAN qui sont utilisés pour faciliter la création et la configuration des stratégies VPN SSL. Ce raccourci permet de gagner en efficacité lors de la création de stratégies similaires pour plusieurs utilisateurs de VPN SSL distants.

ÉTAPE 1 Cliquez sur **VPN > SSL VPN Server > Resources**.

La fenêtre Resources s'ouvre.

ÉTAPE 2 Pour ajouter une ressource réseau, cliquez sur **Add**.

Autres options : cliquez sur le bouton **Edit** pour modifier une entrée. Pour supprimer une entrée, sélectionnez la case correspondante, puis cliquez sur **Delete**. Pour sélectionner toutes les entrées, sélectionnez la case de la première colonne de l'en-tête du tableau.

ÉTAPE 3 Saisissez les informations suivantes :

- **Resource Name :** entrez un nom unique pour identifier cette ressource.
- **Service :** choisissez l'un des services VPN SSL pris en charge à associer à cette ressource.

ÉTAPE 4 Cliquez sur **Apply** pour enregistrer les paramètres.

Configuration du transfert de port VPN SSL

Le transfert de port est utilisé pour autoriser l'accès uniquement à un ensemble limité de ressources. Par exemple, si vous souhaitez que les utilisateurs de VPN SSL accèdent au service de messagerie électronique uniquement. Le transfert de port est différent des modes de tunnel partagé et plein qui autorisent l'accès à tous les ports pour un sous-réseau donné.

Le tableau suivant répertorie des applications courantes et leurs numéros de port TCP correspondant :

TCP Application	Port Number
Données FTP (généralement non obligatoires)	20
Protocole de contrôle FTP	21
SMTP (envoi de courrier électronique)	25
HTTP (Web)	80
POP3 (réception de courrier électronique)	110
Protocole NTP (Network Time Protocol)	123
Citrix	1494
Services Terminal Server	3389
VNC (Virtual Network Computing)	entrée 5900 ou 5800

Ajouter une configuration d'applications TCP pour le transfert de port

La configuration des applications TCP est obligatoire pour le transfert de port.

ÉTAPE 1 Cliquez sur **VPN > SSL VPN Server > Port Forwarding**.

La fenêtre Port Forwarding s'ouvre. Cette page comprend deux tableaux :

- Liste des applications configurées pour le transfert de port

- Liste des noms d'hôte configurés pour le transfert de port

ÉTAPE 2 Pour ajouter une application, cliquez sur **Add** dans le tableau List of Configured Applications for Port Forwarding.

Autres options : cliquez sur le bouton **Edit** pour modifier une entrée. Pour supprimer une entrée, sélectionnez la case correspondante, puis cliquez sur **Delete**. Pour sélectionner toutes les entrées, sélectionnez la case de la première colonne de l'en-tête du tableau.

ÉTAPE 3 Saisissez les informations suivantes :

- **Local Server IP Address :** saisissez l'adresse IP de l'ordinateur hôte interne ou du serveur local.
- **TCP Port Number :** saisissez le numéro de port de l'application TCP qui active le transfert de port.

ÉTAPE 4 Cliquez sur **Apply** pour enregistrer les paramètres.

Configuration de la résolution du nom de l'hôte pour le transfert de port

De manière facultative, vous pouvez configurer un nom d'hôte (FQDN) pour que le serveur réseau facilite la connexion des utilisateurs sans qu'ils doivent retenir et saisir une adresse IP.

REMARQUE L'adresse IP du serveur local du nom d'hôte configuré doit correspondre à l'adresse IP de l'application configurée pour le transfert de port.

ÉTAPE 1 Cliquez sur **VPN > SSL VPN Server > Port Forwarding**.

La fenêtre Port Forwarding s'ouvre. Cette page comprend deux tableaux :

- Liste des applications configurées pour le transfert de port
- Liste des noms d'hôte configurés pour le transfert de port

ÉTAPE 2 Pour ajouter un nom d'hôte configuré, cliquez sur **Add** dans le tableau List of Configured Host Names for Port Forwarding.

Autres options : cliquez sur le bouton **Edit** pour modifier une entrée. Pour supprimer une entrée, sélectionnez la case correspondante, puis cliquez sur **Delete**. Pour sélectionner toutes les entrées, sélectionnez la case de la première colonne de l'en-tête du tableau.

ÉTAPE 3 Saisissez les informations suivantes :

- **Local Server IP Address :** saisissez l'adresse IP de l'ordinateur hôte interne ou du serveur local.
- **TCP Port Number :** saisissez le nom de domaine complet pour l'application TCP.

ÉTAPE 4 Cliquez sur **Apply** pour enregistrer les paramètres.

Configuration du client du tunnel VPN SSL

Un client de tunnel VPN SSL fournit une connexion point à point entre la machine exécutant le navigateur et cette appliance de sécurité. Lorsqu'un client VPN SSL est lancé depuis le portail utilisateur, une « carte réseau » avec une adresse IP du sous-réseau d'entreprise et des paramètres DNS et WINS est créé automatiquement. Cette fonctionnalité autorise l'accès aux services sur le réseau privé sans aucune configuration réseau particulière de la machine du client VPN SSL distante.

Vérifiez que l'adresse de l'interface virtuelle (PPP) du client de tunnel VPN n'est pas en conflit avec l'adresse d'un périphérique physique sur le LAN. La plage d'adresses IP pour la carte réseau virtuelle VPN SSL doit se trouver dans un sous-réseau ou une plage sans chevauchement différente du LAN d'entreprise.

Si une adresse IP est attribuée au client VPN SSL dans un autre sous-réseau que le réseau d'entreprise, une route du client doit être ajoutée pour permettre l'accès au LAN privé via le tunnel VPN. En outre, une route statique sur le pare-feu du LAN privé (généralement cette appliance de sécurité) est nécessaire pour transférer le trafic privé à travers le pare-feu VPN au client VPN SSL distant.

REMARQUE Comme dans tout déploiement de tunnel IPsec, les deux réseaux qui sont reliés par le tunnel doivent utiliser des plages d'adresses IP différentes dans leurs sous-réseaux.

L'appliance de sécurité permet la prise en charge du plein tunnel et du tunnel partagé.

- **Full Tunnel Mode :** le tunnel VPN gère tout le trafic envoyé du client.
- **Split Tunnel Mode :** le tunnel VPN gère uniquement le trafic destiné aux adresses de destination spécifiées dans les routes du client configurées. Ces routes de client donnent accès au client SSL aux réseaux privés

spécifiques, permettant ainsi un contrôle de l'accès sur les services LAN spécifiques.

Configuration du client VPN SSL

ÉTAPE 1 Cliquez sur **VPN > SSL VPN Client > SSL VPN Client**.

La fenêtre SSL VPN Client s'ouvre.

ÉTAPE 2 Saisissez les informations suivantes :

- **Enable Split Tunnel Support :** cochez cette case pour activer l'option Split Tunnel Mode Support ou décochez-la pour activer Full Tunnel Mode Support. En mode plein tunnel, tout le trafic de l'hôte est dirigé via le tunnel. Par comparaison, en mode tunnel partagé, le tunnel est utilisé uniquement pour le trafic spécifié par les routes du client.

  REMARQUE Si vous activez Split Tunnel Support, vous devez également configurer SSL VPN Client Routes. Après avoir suivi cette procédure, consultez **Configuration des routes du client en mode tunnel partagé, page 179.**

- **DNS Suffix (Optional) :** saisissez le suffixe DNS pour ce client.
- **Primary DNS Server (Optional) :** saisissez l'adresse IP du serveur DNS principal pour ce client.
- **Secondary DNS Server (Optional) :** saisissez l'adresse IP du serveur DNS secondaire pour ce client.
- **Client Address Range Begin :** saisissez la première adresse IP attribuée aux clients VPN SSL.
- **Client Address Range End :** saisissez la dernière adresse IP attribuée aux clients VPN SSL.

  REMARQUE Configurez une plage d'adresses IP qui ne se superpose avec aucune adresse de votre réseau local. Par exemple, la plage par défaut est comprise entre 192.168.251.1 et 192.168.251.254.

ÉTAPE 3 Cliquez sur **Apply** pour enregistrer les paramètres.

REMARQUE **Étapes suivantes :**
Si vous activez Split Tunnel Support, vous devez également configurer SSL VPN Client Routes. Après avoir suivi cette procédure, consultez **Configuration des routes du client en mode tunnel partagé, page 179.**

Configuration des routes du client en mode tunnel partagé

Si la prise en charge du plein tunnel est désactivée sur la page SSL VPN Client, vous devez configurer les routes du client en mode tunnel partagé.

Les entrées Configured Client Routes sont ajoutées par le client VPN SSL de telle sorte que seul le trafic vers ces adresses de destination est redirigé via les tunnels VPN SSL et tout le reste du trafic est redirigé à l'aide de l'interface réseau native des hôtes (clients VPN SSL). Par exemple si les tentatives du client VPN SSL pour accéder au réseau local de ce périphérique en mode tunnel partagé, l'utilisateur doit ajouter le sous-réseau LAN comme réseau de destination à l'aide de cette page.

REMARQUE Vous pouvez configurer des routes de client uniquement si la prise en charge de tunnel partagé est activée sur la page SSL VPN Client. Voir aussi **Configuration du client VPN SSL, page 178**.

ÉTAPE 1 Cliquez sur **VPN > SSL VPN Client > Configured Client Routes**.

La fenêtre Configured Client Routes s'ouvre. Toutes les routes configurées sont répertoriées dans le tableau Configured Client Routes.

ÉTAPE 2 Pour ajouter une route configurée du client, cliquez sur **Add**.

Autres options : cliquez sur le bouton **Edit** pour modifier une entrée. Pour supprimer une entrée, sélectionnez la case correspondante, puis cliquez sur **Delete**. Pour sélectionner toutes les entrées, sélectionnez la case de la première colonne de l'en-tête du tableau.

La fenêtre SSL VPN Client Route Configuration s'ouvre.

ÉTAPE 3 Saisissez les informations suivantes :

- **Destination Network :** saisissez le sous-réseau de destination vers lequel une route est ajoutée sur le client VPN SSL.
- **Subnet Mask :** saisissez le masque de sous-réseau pour le réseau de destination.

ÉTAPE 4 Cliquez sur **Apply** pour enregistrer les paramètres.

Afficher le portail du client VPN SSL

Pour afficher le portail du client VPN SSL, cliquez sur **VPN> SSL VPN Client > SSL VPN Client Portal**.

REMARQUE Les utilisateurs distants utilisent l'URL du portail pour accéder au portail VPN.

Le portail du client permet d'accéder à distance au réseau d'entreprise grâce aux options suivantes du volet de navigation :

- **VPN Tunnel :** une fois que l'utilisateur a cliqué sur le lien du volet de navigation, la fenêtre d'information VPN Tunnel s'ouvre. L'utilisateur peut cliquer sur l'icône de l'utilitaire d'application pour se connecter au réseau distant.
- **Port Forwarding :** une fois que l'utilisateur a cliqué sur le lien du volet de navigation, la fenêtre d'informations Port Forwarding s'ouvre. L'utilisateur peut cliquer sur l'icône de l'utilitaire d'application pour se connecter aux serveurs distants.
- **Change Password :** l'utilisateur peut cliquez sur ce lien pour modifier son mot de passe.

REMARQUE

1. La section Change Password est disponible uniquement pour les utilisateurs appartenant à la base de données locale.
2. L'administrateur peut activer ou désactiver certaines fonctionnalités.
3. L'utilisateur doit s'assurer que les contrôles Java, Java script et Active-X sont activés ou autorisés dans les paramètres du navigateur Web.

Configuration de la protection d'identité VeriSign™

Cette page permet de configurer l'authentification à deux facteurs de protection d'identité VeriSign™ (VIP) facultative pour authentifier les utilisateurs VPN SSL, offrant un niveau de sécurité optimisé.

REMARQUE Pour plus d'informations ou pour commander le service de protection d'identité VeriSign, consultez la page : www.cisco.com/go/viptoken.

Configuration de la protection d'identité VeriSign

ÉTAPE 1 Cliquez sur **VPN > VeriSign ID Protection > VIP Configuration**.

La fenêtre VIP Configuration s'ouvre.

ÉTAPE 2 Pour activer ou désactiver votre service, effectuez les tâches suivantes dans la zone **VeriSign Identity Protection Configuration** :

a. **Enable VeriSign Identity Protection :** cochez cette case pour activer la fonctionnalité VIP ou décochez-la pour la désactiver.

b. **Service Type :** sélectionnez le type de service que vous avez acheté auprès de VeriSign :

- **VIP Pilot/Developer Test Drive :** choisissez cette option si les jetons pilotes vous ont été fournis pour tester et comprendre le service VIP lors des étapes initiales de déploiement.
- **VIP Production :** choisissez cette option si vous avez acheté le service VeriSign. Le service utilisera des serveurs de production VIP pour authentifier les utilisateurs.

c. Cliquez sur **Apply** pour enregistrer les paramètres.

ÉTAPE 3 Dans la zone **Upload Certificate**, effectuez les tâches suivantes :

a. **Certificate File :** cliquez sur **Browse**, puis recherchez votre fichier de certificat VeriSign (RA).

a. **Password for the certificate file :** saisissez le mot de passe qui vous a été fourni avec le fichier de certificat (RA). Le mot de passe crypte la clé privée fournie dans le certificat et est requis pour la décrypter et l'utiliser.

b. Cliquez sur **Upload** pour télécharger le certificat.

Gestion des informations d'identification des utilisateurs du service VeriSign

Cette page vous permet d'associer des jetons VeriSign à vos utilisateurs.

REMARQUE Vos utilisateurs doivent être tout d'abord configurés dans Administration. Voir aussi **Users, page 183**.

ÉTAPE 1 Cliquez sur **VPN > VeriSign ID Protection > Credential Management**.

La fenêtre VeriSign Credential Management s'ouvre.

ÉTAPE 2 Pour ajouter des informations d'identification, cliquez sur **Add**.

Autres options : cliquez sur le bouton **Edit** pour modifier une entrée. Pour supprimer une entrée, sélectionnez la case correspondante, puis cliquez sur **Delete**. Pour sélectionner toutes les entrées, sélectionnez la case de la première colonne de l'en-tête du tableau.

Lorsque vous cliquez sur Add ou Edit, la fenêtre VeriSign Credential Configuration s'ouvre.

ÉTAPE 3 Saisissez les informations suivantes :

- **Credential Id :** saisissez le nombre à 6 chiffres alphanumériques, généralement au dos du jeton physique. Chaque ID doit être unique et ne doit pas être ajouté s'il existe déjà dans le tableau de configuration des jetons.
- **User Name :** choisissez le nom à associer au numéro du jeton. Chaque ID peut être associé à un seul utilisateur. Une fois que l'utilisateur a été associé à des informations d'identification, le même utilisateur ne peut pas être associé à d'autres informations d'identification. Seuls les utilisateurs disponibles sont affichés dans la liste d'utilisateurs.

ÉTAPE 4 Cliquez sur **Apply** pour enregistrer les paramètres.

8

Administration

Ce chapitre décrit la gestion des utilisateurs, les opérations de maintenance, telles que la mise à niveau des microprogrammes et la sauvegarde de la configuration, et d'autres fonctionnalités relatives au routeur. Il comprend les sections suivantes :

- **Users**
- **Microprogramme et configuration**
- **Diagnostics**
- **Mesurer et limiter le trafic avec l'utilitaire de contrôle du trafic**
- **Configurer les paramètres de date/heure**
- **Configurer les options de journalisation**
- **Gérer les certificats pour l'authentification**
- **Configurer les enregistrements du serveur RADIUS**
- **Gestion des licences**

Pour accéder aux pages d'administration, cliquez sur **Administration** dans la barre de menu de l'utilitaire de configuration.

Users

Vous pouvez utiliser la page Users pour attribuer les noms d'utilisateur, les mots de passe et les stratégies d'accès.

Il existe deux comptes par défaut. Vous pouvez modifier le nom d'utilisateur et le mot de passe pour ces comptes, mais vous ne pouvez pas modifier les stratégies utilisateur.

- **admin :** compte administrateur, qui a un accès en lecture/écriture à tous les paramètres.

- **guest :** compte invité, qui a un accès en lecture seule. Par défaut, ce compte est désactivé. Pour activer le compte, modifiez les stratégies de connexion utilisateur. Voir aussi **Ajouter ou modifier les stratégies de connexion utilisateur, page 187**.
- **VPN SSL :** compte VPN SSL, qui permet l'accès aux services spécifiés dans la configuration VPN SSL.

Fenêtre Domains

Tous les utilisateurs VPN SSL sont membres d'un groupe et tous les groupes sont membres d'un domaine d'authentification. Le domaine doit être configuré avant que les différents groupes et utilisateurs ne puissent lui être affectés.

ÉTAPE 1 Cliquez sur **Administration > Users > Domains**.

La fenêtre Domains s'ouvre.

ÉTAPE 2 Pour ajouter un domaine, cliquez sur **Add** dans le tableau List of Domains.

Autres options : cliquez sur le bouton **Edit** pour modifier une entrée. Pour supprimer une entrée, sélectionnez la case correspondante, puis cliquez sur **Delete**. Pour sélectionner toutes les entrées, cochez la case dans la première colonne de l'en-tête du tableau.

Après avoir cliqué sur Add ou Edit, la fenêtre Domains Configuration s'ouvre.

ÉTAPE 3 Saisissez les informations suivantes :

- **Domain Name :** saisissez un identifiant unique pour le domaine.
- **Authentication Type :** sélectionnez le type d'authentification pour ce domaine.
- **Portal Layout Name :** sélectionnez une présentation de portail. Les présentations sont configurées via le menu du portail VPN SSL. Voir aussi **Étape 1 du scénario : personnalisation de la présentation du portail, page 167.**

ÉTAPE 4 Cliquez sur **Apply** pour enregistrer les paramètres.

Lorsque vous créez un domaine, un groupe est automatiquement créé. Il porte le même nom que le domaine et est associé à ce domaine. Pour modifier les paramètres du groupe, reportez-vous à la **Fenêtre Groups, page 185**.

Fenêtre Groups

Les groupes sont utilisés pour créer un regroupement logique d'utilisateurs VPN SSL qui partagent le même domaine d'authentification, les mêmes règles d'accès LAN et de service et les mêmes paramètres de délai d'inactivité. Ils sont associés aux domaines d'authentification.

ÉTAPE 1 Cliquez sur **Administration > Users > Groups**.

La fenêtre Groups s'ouvre.

ÉTAPE 2 Pour ajouter un groupe, cliquez sur **Add** dans le tableau List of Groups.

Autres options : cliquez sur le bouton **Edit** pour modifier une entrée. Pour supprimer une entrée, sélectionnez la case correspondante, puis cliquez sur **Delete**. Pour sélectionner toutes les entrées, cochez la case dans la première colonne de l'en-tête du tableau.

Après avoir cliqué sur Add ou Edit, la fenêtre Groups Configuration s'ouvre.

ÉTAPE 3 Saisissez les informations suivantes :

- **Group Name :** saisissez un identifiant unique pour le groupe. Vous pouvez utiliser tous les caractères alphanumériques.
- **Domain :** affectez un domaine de la liste déroulante des domaines d'authentification.
- **Idle Timeout :** entrez la durée, en minutes, pendant laquelle un périphérique peut demeurer inactif avant que la session ne soit déconnectée.

  REMARQUE Le paramètre d'expiration du groupe est utilisé comme paramètre d'expiration par défaut pour tous les utilisateurs du groupe. Vous pouvez affecter un délai d'inactivité différent à un utilisateur sur la page Users. Les paramètres utilisateur sont prioritaires sur les paramètres du groupe. Voir aussi **Ajouter ou modifier les paramètres utilisateur, page 186**.

ÉTAPE 4 Cliquez sur **Apply** pour enregistrer les paramètres.

Ajouter ou modifier les paramètres utilisateur

Les utilisateurs font partie d'un groupe, qui à son tour fait partie d'un domaine d'authentification.

REMARQUE Avant de configurer des utilisateurs, configurez les groupes. Voir aussi **Fenêtre Groups, page 185**.

REMARQUE Pour des raisons de sécurité, un mot de passe ne doit contenir aucun mot d'un dictionnaire d'une langue et doit inclure une combinaison de lettres majuscules et minuscules, de chiffres et de symboles. Le mot de passe peut comporter jusqu'à 30 caractères.

ÉTAPE 1 Cliquez sur **Administration > Users > Users**. Le tableau List of Users s'affiche.

La fenêtre Users s'ouvre.

ÉTAPE 2 Pour ajouter un utilisateur, cliquez sur **Add** ou, pour modifier les informations d'un utilisateur, cliquez sur le bouton dans la colonne **Edit**. La fenêtre User Configuration s'ouvre.

La fenêtre Users Configuration s'ouvre.

ÉTAPE 3 Saisissez les informations suivantes :

- **User Name :** saisissez un identifiant unique pour l'utilisateur. Il peut inclure tous les caractères alphanumériques.
- **First Name :** saisissez le prénom de l'utilisateur.
- **Last Name :** entrez le nom de l'utilisateur.
- **User Type :** identifiez le type de compte.
- **Select Group :** choisissez un groupe.
- Si vous ajoutez un nouvel utilisateur, renseignez les champs suivants :
  - **Password :** saisissez un mot de passe comportant des caractères alphanumériques, ainsi que les caractères '—' ou '_'.
  - **Confirm Password :** saisissez à nouveau le mot de passe.

- Si vous mettez à jour les paramètres d'un utilisateur, renseignez les champs suivants :
  - **Check to Edit Password :** cochez cette case pour activer les champs de mot de passe.
  - **Enter Your Password :** entrez votre mot de passe, comme vérification de sécurité avant que vous ne puissiez modifier un mot de passe.
  - **New Password :** saisissez un mot de passe comportant des caractères alphanumériques, ainsi que les caractères '—' ou '_'.
  - **Confirm Password :** saisissez à nouveau le mot de passe.
- **Idle Timeout :** saisissez la durée, en minutes, pendant laquelle l'utilisateur peut être inactif avant la déconnexion de la session. Saisissez une valeur comprise entre 0 et 999. La valeur du délai pour l'utilisateur est prioritaire sur le délai pour le groupe. Si vous souhaitez vous assurer que les paramètres de délai du groupe sont utilisés, définissez cette valeur sur 0.

  REMARQUE Chaque utilisateur est ajouté en tant qu'utilisateur local avec un mot de passe et, lorsque l'utilisateur est affecté à un mécanisme d'authentification externe basé sur le groupe, certains attributs, tels que le mot de passe local, sont ignorés.

ÉTAPE 4 Cliquez sur **Apply** pour enregistrer les paramètres.

Ajouter ou modifier les stratégies de connexion utilisateur

ÉTAPE 1 Pour ajouter ou modifier les stratégies de connexion utilisateur, cliquez sur **Administration > Users > Users**.

La fenêtre Users s'ouvre.

Vous ne pouvez pas configurer ces paramètres pour les utilisateurs par défaut du système, mais uniquement pour les utilisateurs que vous ajoutez.

ÉTAPE 2 Procédez comme requis, suivant le type de stratégie :

- **Stratégie de connexion utilisateur :** cliquez sur le premier bouton de la colonne Edit User Policies. Lorsque la fenêtre User Login Policies s'ouvre, entrez les informations suivantes :
  - **Disable Login :** cochez cette case pour désactiver le compte ou décochez cette case pour activer le compte. Ce paramètre ne peut pas être modifié pour le compte administrateur par défaut.
  - **Deny Login from WAN Interface :** cochez cette case pour empêcher l'utilisateur de se connecter à partir du WAN ou décochez cette case pour permettre à l'utilisateur de se connecter à partir du WAN. Ce paramètre ne peut pas être modifié pour le compte administrateur par défaut.
- **Stratégie de connexion utilisateur par navigateur :** cliquez sur le deuxième bouton de la colonne Edit User Policies. Lorsque la fenêtre User Policy By Client Browser, entrez les informations suivantes :
  - Dans la zone User Policy By Client Browser, sélectionnez **Deny Login from Defined Browsers** ou **Allow Login only from Defined Browsers**.
  - Pour ajouter un navigateur, cliquez sur **Add**, sélectionnez le navigateur, puis cliquez sur **Apply**.
  - Pour supprimer un navigateur, cochez la case correspondante, puis cliquez sur **Delete**.
- **Stratégie de connexion utilisateur par adresse IP :** cliquez sur le troisième bouton de la colonne Edit User Policies. Lorsque la fenêtre User Policy By Source IP Address s'ouvre, entrez les informations suivantes :
  - Dans la zone User Policy By Source IP Address, sélectionnez **Deny Login from Defined Addresses** ou **Allow Login only from Defined Addresses**.
  - Pour ajouter une adresse, cliquez sur **Add**, entrez le type et l'adresse, puis cliquez sur **Apply**.
  - Pour supprimer une adresse, cochez la case correspondante, puis cliquez sur **Delete**.

ÉTAPE 3 Cliquez sur **Apply** pour enregistrer les paramètres.

Microprogramme et configuration

Cette section décrit les tâches de maintenance suivantes :

- **Mettre à niveau le microprogramme et travailler avec des fichiers de configuration**
- **Gérer le périphérique USB**
- **Utiliser le microprogramme secondaire**

Mettre à niveau le microprogramme et travailler avec des fichiers de configuration

Vous pouvez utiliser la page Firmware & Configuration pour exécuter les tâches suivantes :

- Mettre à niveau la version du microprogramme et rechercher les nouvelles disponibilités.
- Sauvegarder les paramètres de configuration personnalisée pour une restauration ultérieure.
- Restaurer les paramètres sauvegardés à partir d'un fichier de sauvegarde ou restaurer les paramètres d'usine par défaut.
- Redémarrer le dispositif de sécurité.

  IMPORTANT ! Lors d'une opération de restauration ou une mise à niveau du microprogramme, ne tentez PAS d'accéder en ligne, d'arrêter le dispositif, d'arrêter le PC ou d'interrompre le processus de quelque manière que ce soit jusqu'à ce que l'opération soit terminée. Ce processus doit prendre approximativement deux minutes, en incluant le processus de redémarrage. L'interruption du processus de mise à niveau à des points spécifiques lorsque la mémoire flash est en cours d'écriture peut corrompre cette mémoire flash et rendre le routeur inutilisable. Vous devrez alors exécuter un processus de restauration du microprogramme flash de niveau inférieur (et non l'utilitaire de configuration).

ÉTAPE 1 Cliquez sur **Administration > Firmware & Configuration > Network**.

La fenêtre Firmware & Configuration (Network) s'ouvre.

ÉTAPE 2 Exécutez les tâches suivantes, comme requis :

- **Status**

  Affiche l'état du microprogramme. Inclut les versions principale et secondaire du microprogramme, la date/heure de la dernière exécution du contrôle du microprogramme, la dernière image disponible pour votre dispositif et un lien vers les notes de la dernière version du microprogramme sur Cisco.com. Reportez-vous aux Notes de version dans la documentation technique : www.cisco.com/go/sa500resource.

  Si une mise à niveau du microprogramme est disponible, sélectionnez une des options suivantes :

  - **Upload :** cochez cette option pour mettre à niveau le microprogramme.
  - **Upload & Factory Reset :** cochez cette option pour mettre à niveau le microprogramme et réinitialiser le dispositif de sécurité avec les paramètres par défaut.

    Si vous choisissez de ne pas mettre à niveau, un message de rappel qu'un nouveau microprogramme est disponible vous est envoyé toutes les 24 heures.

    Vous pouvez également consulter l'état du microprogramme dans les pages Status. Voir aussi **Page Device Status, page 219**.

- **Check for New Firmware & Download**

  - **Check Periodically** : cochez cette option pour rechercher automatiquement les mises à niveau du microprogramme sur une base journalière (toutes les 24 heures). Entrez votre **User name** Cisco et votre **Password** et cliquez sur **Apply** pour sauvegarder vos paramètres.

    REMARQUE Lorsqu'appliqués, les détails du nom d'utilisateur Cisco et du mot de passe Cisco sont appliqués à tous les autres services sur le routeur qui les utilise. Par exemple, le nom d'utilisateur Cisco et la connexion utilisés pour l'administration sont automatiquement mis à jour pour les téléchargements de signature IPS.

    Si un nouveau microprogramme est disponible, il est automatiquement téléchargé sur votre périphérique et vous êtes invité à l'installer. Cliquez sur **OK** pour fermer la fenêtre de notification, puis cliquez sur **Upgrade or Upgrade & Factory Reset.**

  - Pour vérifier si une version à niveau du microprogramme est immédiatement disponible, cliquez sur **Check Now**.

- **Firmware Upgrade**
  - Pour mettre manuellement à niveau le microprogramme, cliquez sur **Browse**, localisez et sélectionnez le fichier de configuration, puis cliquez sur **Upload**. Lorsque l'opération est terminée, le dispositif de sécurité redémarre automatiquement avec les nouveaux paramètres.
  - Pour mettre à niveau votre microprogramme et réinitialiser votre dispositif de sécurité avec les paramètres d'usine par défaut, cliquez sur **Browse**, localisez et sélectionnez le fichier de configuration, puis cliquez sur **Upload & Factory Reset**. Lorsque l'opération est terminée, le dispositif de sécurité redémarre automatiquement avec les nouveaux paramètres.
- **Backup/Restore Settings**
  - Pour sauvegarder une copie de vos paramètres actuels, cliquez sur **Backup**. Lisez l'avertissement qui s'affiche, puis cliquez sur **OK**. Lorsque la fenêtre Download s'ouvre, cliquez sur **Save**, puis sélectionnez un emplacement où sauvegarder le fichier.
  - Pour restaurer vos paramètres sauvegardés à partir d'un fichier de sauvegarde, cliquez sur **Browse**, localisez et sélectionnez le fichier, puis cliquez sur **Restore**. Lorsque l'opération est terminée, le dispositif de sécurité redémarre automatiquement avec les paramètres restaurés.
  - Pour effacer vos paramètres actuels et rétablir les paramètres d'usine par défaut, cliquez sur **Default**. Après la restauration, le dispositif de sécurité redémarre automatiquement avec les paramètres restaurés. Pour obtenir plus d'informations, reportez-vous au **Annexe D, « Paramètres d'usine par défaut ».**
- **Reboot :** pour redémarrer le dispositif de sécurité, cliquez sur **Reboot**.

Gérer le périphérique USB

Vous pouvez utiliser cette page pour effectuer les tâches de maintenance suivantes sur le périphérique USB :

- Monter ou démonter le périphérique USB sans risque.
- Mettre à niveau le microprogramme pour le dispositif de sécurité.

- Sauvegarder et restaurer les paramètres de configuration pour le périphérique USB.

IMPORTANT ! La restauration d'une configuration sauvegardée supprimera vos paramètres actuels. Les règles de pare-feu, les stratégies VPN, les paramètres LAN/WAN et tous les autres paramètres seront perdus. Sauvegardez vos paramètres pour vous assurer que vous pourrez les restaurer plus tard, si nécessaire.

Attendez que le processus soit terminé.

1. Ne fermez PAS la fenêtre du navigateur.
2. N'allez PAS en ligne.
3. N'arrêtez ni ne redémarrez PAS le routeur.
4. N'arrêtez PAS l'ordinateur.
5. Ne retirez ou ne débranchez PAS le périphérique USB.

ÉTAPE 1 Cliquez sur **Administration > Firmware & Configuration > USB**.

La fenêtre Firmware & Configuration (USB) s'ouvre.

ÉTAPE 2 Exécutez les tâches suivantes, comme requis :

- **Mount/Unmount**
  - Pour monter un périphérique USB, branchez le périphérique dans le port USB. Cliquez ensuite sur le bouton Refresh dans la barre d'outils du navigateur. Le bouton Mount est activé. Cliquez sur **Mount**.
  - Pour retirer sans risque un périphérique USB, cliquez sur **Unmount**.
- **Backup / Restore Settings / Software Upgrade**
  - Pour effectuer une copie de sauvegarde des paramètres actuels et des certificats numériques, cliquez sur **Backup**. Le fichier est enregistré sous le nom cisco.cfg.
  - Pour restaurer les paramètres d'un fichier de configuration précédemment sauvegardé, cliquez sur **Restore**. Localisez et sélectionnez le fichier de sauvegarde du périphérique de stockage USB connecté. Une barre de progression indiquant l'état de l'opération de restauration s'affiche. Le dispositif de sécurité redémarre automatiquement.

- Pour mettre à niveau le microprogramme, sélectionnez un fichier de mise à niveau, puis cliquez sur **Upload** pour télécharger le fichier ou sur **Upload & Factory Reset** pour télécharger le fichier et réinitialiser le dispositif de sécurité avec les paramètres d'usine par défaut. Une barre de progression affiche l'état de la mise à niveau.

  Pour toute information sur le téléchargement des fichiers de mise à niveau du microprogramme, reportez-vous à la **Mise à jour du microprogramme, page 25**.

  La mise à niveau du routeur peut prendre plusieurs minutes. Lorsque la mise à niveau est en cours, le DEL Test du panneau avant du routeur s'allume. Attendez que le voyant s'éteigne avant d'accéder à nouveau au routeur. Lorsque le téléchargement de l'image est terminé, le routeur redémarre automatiquement. Après une mise à niveau réussie, connectez-vous. Pour vérifier la version du microprogramme, accédez à **Status > Device Status**. La version du microprogramme (principal) doit être identique à la version que vous avez tenté d'installer. Si la mise à niveau a échoué, voir **Annexe A, « Dépannage ».**

- **Reboot :** cliquez sur **Reboot** s'il est nécessaire de redémarrer le routeur.

Utiliser le microprogramme secondaire

Vous pouvez utiliser cette fonctionnalité pour revenir à la version précédente du microprogramme qui était utilisée.

ÉTAPE 1 Cliquez sur **Administration > Firmware & Configuration > Swap Firmware**.

La fenêtre Swap Firmware s'ouvre.

ÉTAPE 2 Cliquez sur **Switch** pour redémarrer le dispositif de sécurité en utilisant l'image du microprogramme secondaire.

REMARQUE Si aucune image de microprogramme secondaire n'est présente, ne tentez pas de permuter les images. Cela peut empêcher le redémarrage du routeur.

Diagnostics

Vous pouvez utiliser la page Diagnostics pour évaluer la configuration du dispositif de sécurité et pour contrôler l'état général du réseau.

REMARQUE Ces fonctionnalités nécessitent une connexion WAN active.

ÉTAPE 1 Cliquez sur **Administration > Diagnostics**.

La fenêtre Diagnostics s'ouvre.

ÉTAPE 2 Exécutez les tâches suivantes, comme requis :

- **Ping or Trace an IP Address :** vous pouvez utiliser ces outils pour tester votre réseau.
  - **Ping through VPN tunnel :** cochez cette case pour activer le test Ping via le tunnel VPN. Sinon, décochez cette case.
  - Pour tester la connectivité entre le dispositif de sécurité et un périphérique connecté sur le réseau, entrez l'**adresse IP** du périphérique, puis cliquez sur **Ping**. Les résultats s'affichent dans la page Command Output. Cliquez sur **Back** pour revenir sur la page Diagnostics.
  - Pour afficher le chemin entre le dispositif de sécurité et une destination, entrez l'**adresse IP** de la destination, puis cliquez sur **Traceroute**. Les résultats s'affichent dans la page Command Output. Le rapport inclut jusqu'à 30 « sauts » (routeurs intermédiaires) entre ce dispositif de sécurité et la destination. Cliquez sur **Back** pour revenir sur la page Diagnostics.
- **DNS Lookup :** pour extraire l'adresse IP d'un serveur sur Internet, entrez le **nom Internet** dans la zone de texte, puis cliquez sur **Lookup**. Si l'entrée de l'hôte ou du domaine existe déjà, une réponse s'affiche avec l'adresse IP. Un message énonçant « Hôte inconnu » indique que le nom Internet spécifié n'existe pas.
- **Router Options :** vous avez le choix entre les options suivantes :
  - Pour afficher un tableau du routage IPv4 ou un tableau du routage IPv6, cliquez sur le bouton **Display**. Les résultats s'affichent dans la page Command Output. Cliquez sur **Back** pour revenir sur la page Diagnostics.

- Pour capturer tous les paquets qui transitent par une interface donnée, cliquez sur **Packet Trace**. Lorsque la fenêtre Capture Packets s'ouvre, choisissez l'interface : **LAN**, **Dedicated WAN** ou **Optional WAN**. Cliquez sur **Start** pour commencer la capture des paquets. Cliquez sur **Stop** pour arrêter la capture. Pour télécharger le rapport, cliquez sur **Download**.

Mesurer et limiter le trafic avec l'utilitaire de contrôle du trafic

L'utilitaire de contrôle du trafic vous permet de mesurer et de limiter le trafic acheminé par ce routeur. Vous pouvez configurer l'utilitaire de contrôle du trafic pour le WAN dédié et pour le WAN optionnel.

ÉTAPE 1 Cliquez sur **Administration > Traffic Meter > Dedicated WAN** pour configurer le WAN dédié ou sur **Traffic Meter > Optional WAN** pour configurer le WAN optionnel.

La fenêtre Traffic Meter s'ouvre.

ÉTAPE 2 Dans la zone **Enable Traffic Meter**, entrez les informations suivantes :

- **Enabled Traffic Metering :** cochez cette case pour activer l'utilitaire de contrôle du trafic sur le port. Le dispositif de sécurité conserve un enregistrement du volume du trafic acheminé à partir de cette interface. Vous pouvez également configurer le dispositif de sécurité pour appliquer une restriction au volume de données acheminées.
- **Traffic Limit Type :** sélectionnez l'une des options suivantes :
  - **No Limit :** option par défaut, aucune limite de transfert de données n'est imposée.
  - **Download Only :** limite la quantité de trafic de téléchargement. Entrez le volume de données maximum autorisé (en mégaoctets) pouvant être téléchargées pour un mois donné dans la zone de texte Monthly Limit. Une fois la limite atteint, aucun trafic n'est autorisé du côté WAN.
  - **Both Directions :** pour ce paramètre, le routeur calcule le trafic pour le chargement et le téléchargement. La limite de trafic saisie dans le champ Monthly Limit est partagée par le trafic de chargement et le trafic de téléchargement. Par exemple, pour une limite de 1 Go, si un fichier de

700 Mo est téléchargé, les 300 Mo restants doivent être partagés entre le trafic de chargement et le trafic de téléchargement. Le volume de trafic téléchargé réduira le volume du trafic pouvant être chargé et vice-versa.

- **Monthly Limit :** entrez la limite du volume dans le champ Monthly Limit s'appliquant à ce mois. Cette limite s'applique au type de direction (Download Only ou Both Directions) sélectionné ci-dessus.
- **Increase This Month's Limit :** si la limite de trafic mensuelle a été atteinte et vous devez augmenter temporairement la limite, cochez cette option et entrez le montant de l'augmentation.
- **This Month's Limit :** affiche la limite de transfert de données applicable pour ce mois, qui correspond à la somme des valeurs des champs Monthly Limit et Increase this Month's Limit.

ÉTAPE 3 Dans la zone **Traffic Counter**, entrez les informations suivantes.

- **Traffic Counter :** indiquez le type d'action à effectuer sur l'utilitaire de calcul du trafic.
  - **Restart Now :** sélectionnez cette option, puis cliquez sur **Apply** pour réinitialiser immédiatement le compteur.
  - **Specific Time :** sélectionnez cette option si vous voulez que le compteur redémarre à une date et heure spécifiées. Entrez ensuite l'heure (HH) et les minutes (MM), puis sélectionnez le jour du mois (du premier au dernier).
- **Send E-mail Report before restarting counter :** sélectionnez cette option pour envoyer un rapport par message électronique avant que l'utilitaire de calcul du trafic ne redémarre. Un message électronique est envoyé à l'adresse configurée dans la section Logging, si la journalisation est activée. Voir aussi **Fenêtre Remote Logging Config, page 201**.

ÉTAPE 4 Dans la zone **When Limit is Reached**, indiquez l'action se produisant lorsque la limite de l'utilitaire de calcul du trafic est atteinte.

- **Block All Traffic :** sélectionnez cette option pour bloquer tout trafic en provenance et à destination du WAN lorsque la limite du trafic est atteinte.
- **Block All Traffic Except E-mail :** sélectionnez cette option pour bloquer tout trafic en provenance et à destination du WAN, à l'exception du trafic de messagerie électronique.

ÉTAPE 5 Si l'utilitaire de contrôle du trafic est activé, la zone **Internet Traffic Statistics** affiche les informations suivantes :

Start Date/Time	Date à laquelle l'utilitaire de contrôle du trafic a démarré ou dernière date à laquelle le utilitaire de calcul du trafic a été réinitialisé.
Outgoing Traffic Volume	Volume du trafic, en mégaoctets, qui a été chargé via cette interface.
Incoming Traffic Volume	Volume du trafic, en mégaoctets, qui a été téléchargé via cette interface.
Total Traffic Volume	Volume du trafic, en mégaoctets, acheminé via cette interface dans les deux directions.
Average per day	Volume moyen du trafic acheminé via cette interface.
% of Standard Limit	Volume du trafic, en pourcentage, acheminé via cette interface par rapport à la limite mensuelle.
% of Monthly Limit	Volume du trafic, en pourcentage, acheminé via cette interface par rapport à la limite du mois (si la limite du mois a été augmentée).

Configurer les paramètres de date/heure

Vous pouvez configurer votre fuseau horaire, régler l'heure d'été et le serveur NTP (Network Time Protocol) utilisé pour synchroniser la date et l'heure. Le dispositif de sécurité obtient alors les informations de date et d'heure du serveur NTP. Suivez les étapes ci-dessous pour configurer le protocole NTP et les paramètres horaires :

ÉTAPE 1 Cliquez sur **Administration > Time Zone**.

La fenêtre Time Zone s'ouvre.

ÉTAPE 2 Saisissez les informations suivantes :

- **Date/Time :** sélectionnez le fuseau horaire par rapport au fuseau GMT (Greenwich Mean Time).

- **Automatically Adjust for Daylight Savings Time :** cochez cette case si vous voulez que l'heure d'été soit automatiquement réglée.
- **Use Default NTP Servers or Use Custom NTP Servers :** vous pouvez utiliser les serveurs NTP (Network Time Protocol) par défaut ou vous pouvez entrer les adresses IP de deux serveurs NTP personnalisés maximum.

ÉTAPE 3 Cliquez sur **Apply** pour enregistrer les paramètres.

Configurer les options de journalisation

Vous pouvez configurer les journaux pour différents événements se produisant sur votre réseau. Reportez-vous aux rubriques suivantes :

- **Fenêtre Local Logging Config**
- **Fenêtre IPV6 Logging**
- **Fenêtre Remote Logging Config**
- **Fenêtre Logs Facility and Severity**

Pour toute information sur la consultation des journaux des événements du système, des journaux VPN IPsec et des journaux d'application des stratégies, voir **Page Active Users, page 228**.

Fenêtre Local Logging Config

Vous pouvez configurer le routeur afin de consigner les événements comme le trafic monodiffusion ou de diffusion acheminé via le routeur, ou les paquets abandonnés suite au filtrage MAC d'origine.

REMARQUE L'activation des options de journalisation peut générer un volume significatif de messages de journalisation et est recommandée à des fins de débogage uniquement.

ÉTAPE 1 Cliquez sur **Administration > Logging > Logging Config**.

La fenêtre Local Logging Config s'ouvre.

ÉTAPE 2 Cochez la case pour chaque option de journalisation que vous voulez activer ou décochez la case pour désactiver l'option de journalisation spécifiée.

- **Routing Logs: :** pour chaque type de trafic, sélectionnez les types de paquet à consigner (paquets acceptés ou paquets abandonnés comme décrit dans le tableau **Journaux de routage**.
- **System Logs :** sélectionnez les types d'événement système à consigner.
  - **All Unicast Traffic :** tous les paquets de monodiffusion dirigés vers le routeur sont consignés.
  - **All Broadcast/Multicast Traffic :** tous les paquets de diffusion ou multidiffusion dirigés vers le routeur sont consignés.
- **Other Event Logs** : choisissez les autres types d'événement à consigner.
  - **Source MAC Filter :** si cette option est cochée, les paquets correspondants sont consignés suite au filtrage MAC d'origine. Décochez cette option pour désactiver les journaux du filtrage MAC d'origine.
  - **Output Blocking Event Log** : si cette option est cochée, le périphérique affiche les journaux pour les paquets bloqués par le service ProtectLink.
  - **Bandwidth Limit :** si cette option est cochée, les journaux relatifs aux paquets abandonnées en raison de la limite de la bande passante sont affichés.

ÉTAPE 3 Cliquez sur **Apply** pour enregistrer les paramètres.

Journaux de routage	
LAN to WAN	Activez la journalisation pour les règles de pare-feu correspondant à l'origine et la destination LAN-to-WAN. La journalisation pour les différentes règles de pare-feu doit être activée.
LAN to DMZ	Activez la journalisation pour les règles de pare-feu correspondant à l'origine et la destination LAN-to-DMZ. La journalisation pour les différentes règles de pare-feu doit être activée.
DMZ to WAN	Activez la journalisation pour les règles de pare-feu correspondant à l'origine et la destination DMZ-to-WAN. La journalisation pour les différentes règles de pare-feu doit être activée.

WAN to LAN	Activez la journalisation pour les règles de pare-feu correspondant à l'origine et la destination WAN-to-LAN. La journalisation pour les différentes règles de pare-feu doit être activée.
DMZ to LAN	Activez la journalisation pour les règles de pare-feu correspondant à l'origine et la destination DMZ-to-LAN. La journalisation pour les différentes règles de pare-feu doit être activée.
WAN to DMZ	Activez la journalisation pour les règles de pare-feu correspondant à l'origine et la destination WAN-to-DMZ. La journalisation pour les différentes règles de pare-feu doit être activée.

Fenêtre IPV6 Logging

Cette page permet activer les règles de journalisation pour la journalisation du trafic IPv6.

ÉTAPE 1 Cliquez sur **Administration > Logging > IPv6 Logging**.

La fenêtre IPV6 Logging s'ouvre.

ÉTAPE 2 Cochez la case pour chaque option de journalisation que vous voulez activer ou décochez la case pour désactiver l'option de journalisation spécifiée.

- **Accepted Packets :** consigne les paquets acheminés avec succès via le segment. Cette option est utile lorsque le champ Default Outbound Policy a la valeur « Block Always » (voir la page Firewall Rules, dans le menu Firewall).

  Par exemple, supposons que vous vouliez enregistrer chaque connexion SSH réussie du LAN vers le WAN. Vous cocheriez la case **LAN to WAN** sous **Accepted Packets**. À chaque fois qu'une machine LAN établit une connexion SSH vers le WAN, un message est consigné. (Cet exemple suppose que le champ Default Outbound Policy a la valeur « Block Always » et vous avez activé une règle de pare-feu pour autoriser le trafic SSH du LAN vers le WAN. La règle de pare-feu doit également autoriser la journalisation. Pour obtenir plus d'informations, reportez-vous à la **Configuration des règles de pare-feu pour contrôler le trafic entrant et sortant, page 107.)**

- **Dropped Packets :** les paquets dont le transfert via le segment a été bloqué sont consignés. Cette option est utile lorsque le champ Default Outbound Policy a la valeur « Allow Always » (voir la page Firewall Rules, dans le menu Firewall).

  Par exemple, supposons que vous vouliez enregistrer chaque connexion SSH bloquée du LAN vers le WAN. Vous cocheriez la case **LAN to WAN** sous **Dropped Packets**. À chaque fois qu'une machine sur le LAN tente d'établir une connexion SSH vers le WAN, un message est consigné Cet exemple suppose que le champ Default Outbound Policy a la valeur « Allow Always » et vous avez activé une règle de pare-feu pour bloquer le trafic SSH du LAN vers le WAN. La règle de pare-feu doit également autoriser la journalisation. Pour obtenir plus d'informations, reportez-vous à la section **Configuration des règles de pare-feu pour contrôler le trafic entrant et sortant, page 107.**

ÉTAPE 3 Cliquez sur **Apply** pour enregistrer les paramètres.

Fenêtre Remote Logging Config

Utilisez cette page pour activer et configurer la journalisation des messages électroniques pour différents types de journaux pour une adresse électronique donnée ou un serveur syslog.

ÉTAPE 1 Cliquez sur **Administration > Logging > Remote Logging**.

La fenêtre Remote Logging Config s'ouvre.

ÉTAPE 2 Dans la zone **Log Options**, entrez un nom permettant d'identifier le périphérique dans les journaux distants. Chaque message consigné inclura cet identifiant comme préfixe pour une identification plus facile de l'origine du message. L'identifiant du journal est ajouté au message électronique et au messages syslog.

ÉTAPE 3 Dans la zone **Enable E-Mail Logs**, entrez les informations suivantes :

- **Enable E-Mail Logs :** cochez cette case pour activer les journaux des messages électroniques.
- **E-mail Server Address :** entrez l'adresse IP ou le nom Internet d'un serveur de messagerie électronique. Le routeur se connecte à ce serveur pour envoyer les journaux des messages électroniques, lorsque requis.

- **Return E-mail Address :** entrez l'adresse électronique lorsque des réponses du serveur SMTP doivent être envoyées (requis pour les messages d'échec).
- **Send To E-mail Address :** entrez l'adresse électronique à laquelle les journaux et les alertes doivent être envoyés.
- **Authentication with SMTP server :** si le serveur SMTP requière une authentification avant d'accepter une connexion, sélectionnez l'authentification **Login Plain** ou **CRAM-MD5** dans le menu déroulant et entrez le nom et le mot de passe du compte utilisateur. Pour désactiver l'authentification, sélectionnez **None**.
- **Respond to Identd from SMTP Server :** cochez cette case pour configurer le routeur afin de répondre à une demande IDENT du serveur SMTP.

ÉTAPE 4 Dans la zone **Send E-mail logs by Schedule**, configurez les paramètres suivants afin de recevoir les journaux des messages électroniques suivant une planification :

- **Unit :** sélectionnez la fréquence à laquelle vous devez envoyer le journal : Hourly, Daily ou Weekly. Pour désactiver l'envoi des journaux, sélectionnez Never.

  Cette option est utile lorsque vous ne souhaitez pas recevoir les journaux par message électronique, mais voulez que les options de messagerie électronique soient configurées afin que vous puissiez utiliser la fonction d'envoi de journal des pages **Status > View Logs**.
- **Day :** si les journaux doivent être envoyés sur une base hebdomadaire, choisissez le jour de la semaine.
- **Time :** sélectionnez l'heure à laquelle les journaux doivent être envoyés.

ÉTAPE 5 Si vous souhaitez que le dispositif de sécurité envoie des journaux sur un serveur syslog, entrez l'adresse IP ou le nom Internet du serveur dans le champ **SysLog Server**.

ÉTAPE 6 Cliquez sur **Apply** pour enregistrer les paramètres.

Fenêtre Logs Facility and Severity

Différents événements peuvent être capturés et consignés pour vérification. Ces journaux peuvent être envoyés vers un serveur syslog ou envoyés par message électronique à une adresse spécifiée. Vous pouvez également spécifier les messages système devant être consignés suivant l'installation ayant généré le message et son niveau de gravité.

ÉTAPE 1 Cliquez sur **Administration> Logging > Logs Facility and Severity**.

La fenêtre Logs Facility and Severity s'ouvre.

ÉTAPE 2 Sélectionnez le niveau de gravité de la journalisation comme défini dans le tableau **Niveau de gravité du journal**.

ÉTAPE 3 Cochez la case pour chaque événement que vous souhaitez afficher dans le journal local ou pour l'envoyer au serveur syslog.

ÉTAPE 4 Cliquez sur **Apply** pour enregistrer les paramètres.

Niveau de gravité du journal	
Emergency (niveau 0)	Inutilisable par le système. La définition syslog est LOG_EMERG.
Alert (niveau 1)	Action immédiate requise. La définition syslog est LOG_ALERT.
Critical (niveau 2)	Conditions critiques. La définition syslog est LOG_CRIT.
Error (niveau 3)	Conditions d'erreur. La définition syslog est LOG_ERR.
Warning (niveau 4)	Conditions d'avertissement. La définition syslog est LOG_WARNING.
Notification (niveau 5)	Condition normale mais significative. La définition syslog est LOG_NOTICE.
Information (niveau 6)	Messages d'information uniquement. La définition syslog est LOG_INFO.

Debugging (niveau 7)	Messages de débogage. La définition syslog est LOG_DEBUG. Par exemple : si vous sélectionnez Critical, tous les messages listés sous les catégories Critical, Emergency et Alert sont consignés.

Gérer les certificats pour l'authentification

Des certificats numériques (également appelés certificats X509) sont utilisés pour authentifier l'identité des utilisateurs et des systèmes et sont délivrés par différentes autorités de certification de certification, comme VeriSign, Thawte ou d'autres organisations. Les certificats numériques sont utilisés par ce routeur lors de la phase d'authentification IKE (Internet Key Exchange) comme autre méthode d'authentification. Différentes autorités de certification vous émettent des certificats automatiques. Vous créez et gérez des certificats à partir de la page Authentication (Certificates).

Trusted Certificates (CA Certificate)	Utilisé pour vérifier la validité des certificats générés et signés par l'autorité de certification. Le tableau Trusted Certificates contient les certificats pour chaque autorité de certification et inclut les informations suivantes : **CA Identity (Subject Name)** : organisation ou personne pour laquelle le certificat est délivré. ▪ **Issuer Name** : nom de l'autorité de certification qui a délivré le certificat. ▪ **Expiry Time** : date après laquelle le certificat devient non valide.

Active Self Certificates	Liste les certificats que vous a délivré une autorité de certification fiable et qui sont disponibles pour être utilisés par les serveurs IKE distants. Le serveur IKE distant valide le routeur en utilisant ces certificats. Pour utiliser un certificat automatique, vous devez d'abord demander un certificat auprès de l'autorité de certification, puis télécharger et activer le certificat sur votre système. Pour chaque certificat, le tableau Active Self Certificates inclut les informations suivantes : ▪ **Name** : nom utilisé pour identifier ce certificat. ▪ **Subject Name** : nom du titulaire (propriétaire) de ce certificat affiché aux autres organisations. Entrez la raison sociale ou le nom officiel de la société. ▪ **Serial Number :** numéro de série géré par l'autorité de certification et utilisé à des fins d'identification. ▪ **Issuer Name** : nom de l'autorité de certification qui a délivré le certificat. ▪ **Expiry Time** : date d'expiration du certificat. Il est recommandé de renouveler le certificat avant qu'il n'arrive à expiration.
Certification Signing Request (CSR)	Contient toutes les informations requises pour la création de votre certificat numérique, dont les informations de contact, le nom pour lequel le certificat signé est délivré et la clé publique du serveur qui utilisera le certificat. Le tableau Certificate Signing Request liste les noms des certificats que vous demandez et le statut du certificat.

ÉTAPE 1 Cliquez sur **Administration > Authentication**.

La fenêtre Authentication (Certificates) s'ouvre.

ÉTAPE 2 Pour chaque type de certificat, exécutez les actions suivantes, comme requis :

- Pour ajouter un certificat, cliquez sur **Upload**. Vous pouvez charger le certificat de l'ordinateur ou du périphérique USB. Cliquez sur **Browse**, recherchez et sélectionnez le certificat, puis cliquez sur **Upload**.
- Pour supprimer un certificat, cochez la case pour sélectionner le certificat, puis cliquez sur **Delete**.

- Pour télécharger le certificat du routeur (fichier .pem), cliquez sur le bouton Download sous la zone Download Settings.

ÉTAPE 3 Pour demander un certificat auprès de l'autorité de certification, cliquez sur **Generate CSR**.

La fenêtre Generate Certification Signing Request s'ouvre.

a. Entrez les informations du nom unique dans les champs **Generate Self Certificate Request**.

- **Name** : nom unique utilisé pour identifier un certificat.
- **Subject** : nom du titulaire du certificat (propriétaire). L'entrée CN (Common Name) du certificat généré est renseignée par le champ Subject et peut comporter les champs suivants :
  - CN=Nom commun
  - O=Organisation
  - OU=Unité organisationnelle
  - L=Localité
  - ST=Région
  - C=Pays

    Par exemple : CN=routeur1, OU=mon_service, O=ma_société, L=Paris, C=France

  Quel que soit le nom que vous choisissez, il apparaîtra dans la ligne d'objet du CSR généré. Pour inclure plusieurs champs d'objet, entrez chaque objet séparé par une virgule. Par exemple : CN=nomhôte.domaine.com, ST=RhôneAlpes, C=France
- **Hash Algorithm** : algorithme utilisé par le certificat. Choisissez entre MD5 et SHA-1
- **Signature Algorithm** : algorithme (RSA) utilisé pour signer le certificat.
- **Signature Key Length** : longueur de la signature, 512 ou 1024.
- **(Facultatif)** Adresse IP, nom de domaine et adresse de messagerie électronique

b. Cliquez sur **Generate**.

Une nouvelle demande de certificat est créée et ajoutée au tableau Certification Signing Request (CSR). Pour afficher la demande, cliquez sur le bouton View en regard du certificat que vous venez de créer.

Configurer les enregistrements du serveur RADIUS

Cette page permet à l'utilisateur de configurer les détails des serveurs RADIUS utilisés pour l'authentification.

ÉTAPE 1 Cliquez sur **Administration> RADIUS Server**.

ÉTAPE 2 Pour ajouter un serveur, cliquez sur **Add**.

Autres options : cliquez sur le bouton **Edit** pour modifier une entrée. Pour supprimer une entrée, sélectionnez la case correspondante, puis cliquez sur **Delete**. Pour sélectionner toutes les entrées, cochez la case dans la première colonne de l'en-tête du tableau.

Après avoir cliqué sur Add ou Edit, la fenêtre Radius Server Configuration s'ouvre.

ÉTAPE 3 Saisissez les informations suivantes :

- **Authentication Server IP Address :** entrez l'adresse IP du serveur RADIUS d'authentification.
- **Authentication Port :** entrez le numéro de port du serveur RADIUS utilisé pour envoyer le trafic RADIUS.
- **Secret :** entrez la clé partagée configurée sur le serveur RADIUS. Le champ Secret peut contenir tous les caractères, à l'exception des apostrophes, guillemets et espaces.
- **Timeout :** entrez le nombre de secondes pendant lesquelles la connexion peut exister avant qu'une nouvelle authentification ne soit requise.
- **Retries :** entrez le nombre de nouvelles tentatives d'authentification par le dispositif avec le serveur RADIUS.

ÉTAPE 4 Cliquez sur **Apply** pour enregistrer les paramètres.

Gestion des licences

Vous installez et gérer des licences dans la page License Management. Selon le type, vous pouvez télécharger la licence, l'installer automatiquement à l'aide d'une clé d'autorisation de produit (Product Authorization Key - PAK) ou l'activer à partir de Cisco.com.

Licences prises en charge	
VPN par SSL	Fournit un accès à distance pour les employés, les partenaires et des consultants. Il s'agit d'une licence permanente, sans période d'utilisation ni renouvellement nécessaire. Le nombre de postes pris en charge par défaut est 2. ▪ Pour le modèle SA540, une mise à jour gratuite de 50 postes est disponible. Vous devez télécharger une clé de licence de Cisco pour activer ces postes. Pour obtenir la clé de licence, cliquez sur le lien **Upgrade to 50 Seats** sur la page License Management. ▪ Pour les modèles SA520 et SA520W, vous pouvez augmenter le nombre de postes de 2 à 25 utilisateurs. Pour ajouter des postes, vous devez acheter une licence VPN SSL de Cisco à l'adresse : www.cisco.com/go/license.
Services ProtectLink (Web/Gateway et Endpoint)	▪ **ProtectLink Web** propose à un nombre illimité d'utilisateurs une protection contre les menaces Web afin d'éviter tout accès à des sites Web dangereux, ainsi qu'un filtrage des adresses URL afin de contrôler l'accès des employés à des sites Web non liés à leur activité professionnelle. ▪ **ProtectLink Gateway** fournit les fonctionnalités de sécurité Web de ProtectLink Web et les combine avec la sécurité de la messagerie électronique pour empêcher tout courrier indésirable, virus et tentatives de phishing dans la messagerie électronique. Il est disponible dans une licence pour 25 ou 100 postes. Pour télécharger une licence gratuite ProtectLink (évaluation de 30 jours), cliquez sur le lien **Free Trial** sur la page License Management. ▪ **ProtectLink Endpoint** : protège les ordinateurs Windows et les serveurs de tout logiciel espion, virus et autres programmes malveillants.

IPS (Système de prévention des intrusions)	Fournit une protection contre les vers, attaques et programmes malveillants. Cette licence est valable un an. Pour obtenir plus d'informations sur les DN, reportez-vous à la **Configuration de la traduction d'adresses réseau (IPS), page 138**.

ÉTAPE 1 Cliquez sur **Administration > License Management,** ou, dans la page Getting Started (Advanced), sous Intrusion Prevention System (IPS), cliquez sur **Install License**.

La fenêtre License Management s'ouvre.

Le tableau License Status inclut les informations suivantes :

- **Feature** : affiche les licences disponibles. Cliquez sur le lien **Feature** pour afficher une description de la licence.
- **Status** : indique si la licence est installé. Une fois installée, les licences ne peuvent pas être transférés ni retirées.
- **Seats Available** : mombre actuel des licences installées.
- **Expiration** : date d'expiration de la licence sous le format MM/JJ/AAAAA. Par exemple : 04/23/2010.

  Pour les licences ProtectLink, le système met automatiquement à jour le nombre de postes et la date d'expiration toutes les 24 heures en fonction des modifications apportées au serveur de licence. Toutefois, si vous souhaitez récupérer immédiatement ces informations, cliquez sur le bouton **Update**.
- **Action** : pour effectuer une action d'étape suivante. Selon ce que vous souhaitez faire, cliquez sur l'un des liens suivants :
  - **Install** : installer et activer la licence.
  - **Free Trial** : télécharger une licence d'évaluation à partir de Cisco.com.
  - **Renew :** renouveler votre licence existante, si celle-ci est sur le point d'expirer ou a déjà expiré.
  - **Upgrade to 25 Seats :** mettre la licence à niveau pour activer les utilisateurs. (Ne s'applique qu'aux modèles SA520 et SA520W)
  - **Upgrade to 50 Seats :** mettre la licence à niveau pour activer les utilisateurs. (Ne s'applique qu'au modèle SA540)

- **Device Credentials** : champ en lecture seule. Cliquez sur ce bouton pour afficher l'ID produit et le numéro de série du périphérique, ainsi que les identifiants.

ÉTAPE 2 Pour installer une licence, sélectionnez la fonction et cliquez sur **Install**.

La fenêtre License Management Install License s'ouvre.

a. Pour une licence IPS, sélectionnez une des méthodes d'installation suivantes dans la page Install License :

- Type de licence d'installation
  - **License Code (PAK) from cisco.com** : récupère et installe automatiquement la licence sur le périphérique à partir du serveur Cisco. Pour utiliser cette option, entrez votre ID PAK, ainsi que votre nom d'utilisateur et votre mot de passe Cisco.com. Ces identifiants sont requis afin que le périphérique s'identifie sur le serveur Cisco.

    Assurez-vous que le dispositif de sécurité est défini avec l'heure actuelle, sinon la licence ne s'installera pas correctement. Voir aussi **Configurer les paramètres de date/heure, page 197.**
  - **License File downloaded from cisco.com** : installe une licence précédemment téléchargée sur votre PC.
- **Select Transfer File** : si le fichier de licence se trouve sur votre PC ou sur un périphérique USB, vous pouvez le télécharger sur le dispositif de sécurité. Cliquez sur **Browse** pour localiser et sélectionner le fichier de licence.

  Après avoir terminé la saisie des informations dans les champs obligatoires, cliquez sur **Validate License**. Cliquez sur **Back** pour revenir sur la page License Management.

b. Pour installer et activer une licence ProtectLink Web/Gateway ou Endpoint, cliquez sur **Install** et suivez les étapes décrites sur la page Install License.

9

Gestion du réseau

Ce chapitre décrit la configuration des fonctionnalités de gestion à distance du routeur. Il comprend les sections suivantes :

- **RMON (Gestion à distance)**
- **CDP**
- **SNMP**
- **UPnP**
- **Bonjour**

Pour accéder aux pages de gestion du réseau, cliquez sur *Network Management* dans la barre de menus de Configuration Utility.

RMON (Gestion à distance)

Méthode principale pour configurer cette passerelle via le GUI indépendant du navigateur. Il est possible d'accéder au GUI depuis le nœud LAN à l'aide de l'adresse IP LAN de la passerelle et HTTP ou depuis le WAN à l'aide de l'adresse IP WAN de la passerelle et du HTTPS (HTTP sur SSL).

La page de Remote Management permet d'accéder au routeur à partir d'un réseau WAN à distance. L'appliance de sécurité permet une gestion à distance sécurisée via HTTPS, c.-à-d. https://.

REMARQUE La désactivation de Remote Management empêche l'accès VPN SSL.

IMPORTANT : lorsque vous désactivez la gestion à distance, le routeur est accessible à tous ceux qui connaissent son adresse IP. Dans la mesure où un utilisateur de réseau WAN malveillant peut reconfigurer le routeur et en faire une mauvaise utilisation de plusieurs façons, nous vous *recommandons vivement* de modifier les mots de passe admin et invité avant de continuer.

ÉTAPE 1 Cliquez sur **Network Management > Remote Management**.

La fenêtre Remote Management (RMON) s'ouvre.

ÉTAPE 2 Saisissez les informations suivantes :

- **Enable Remote Management? :** par défaut, la gestion à distance est désactivée. Pour activer l'accès WAN au GUI de configuration, cochez la case.

  IMPORTANT : lorsque vous activez la gestion à distance, l'appliance de sécurité est accessible à tous ceux qui connaissent son adresse IP. Dans la mesure où un utilisateur de réseau WAN malveillant peut reconfigurer l'appliance de sécurité et en faire une mauvaise utilisation de plusieurs façons, nous vous recommandons vivement de modifier les mots de passe admin et invité avant de continuer.

- **Access Type :** choisissez le niveau d'autorisation pour la gestion à distance :
  - **All IP Addresses :** si cette option est sélectionnée, vérifiez que vous modifiez le mot de passe par défaut.
  - **IP Address Range :** si cette option est sélectionnée, renseignez le champ **From**: adresse IP de début pour la plage autorisée et le champ **To**: adresse IP de fin pour la plage autorisée.
- **Only this PC :** si cette option est sélectionnée, définissez ce qui suit :
  - **IP Address :** adresse IP du PC disposant des autorisations de gestion à distance
- **Port Number :** affiche le numéro de port utilisé pour la connexion à distance.
- **Remote SNMP Enable** : cochez la case pour activer SNMP pour la connexion à distance.

ÉTAPE 3 Cliquez sur **Apply** pour enregistrer les paramètres.

CDP

Cisco Discovery Protocol (CDP) est un protocole de détection de périphériques exécuté sur tous les équipements conçus par Cisco. Chaque périphérique compatible CDP envoie des messages périodiques à une adresse de multidiffusion et écoute également les messages périodiques envoyés par d'autres afin d'en savoir plus sur les périphériques voisins et déterminer l'état de ces périphériques. Cette page fournit des options de configuration pour contrôler le CDP.

REMARQUE L'activation du CDP n'est pas recommandée sur le port WAN dédié et les ports facultatifs car ils sont connectés à des réseaux non sécurisés.

ÉTAPE 1 Cliquez sur **Network Management > CDP**.

La fenêtre CDP s'ouvre.

ÉTAPE 2 Saisissez les informations suivantes :

- **CDP :** sélectionnez l'une des options suivantes :
  - **Enable All :** active le CDP sur tous les ports pris en charge par le périphérique.
  - **Disable All :** désactive le CDP
  - **Per Port :** configure le CDP sur des ports sélectifs, affichés dans le tableau d'informations des ports.
- **CDP Timer :** il s'agit de l'intervalle de temps entre les paquets CDP successifs envoyés par le routeur.
- **CDP Hold Timer :** le temporisateur de paquets est la durée pendant laquelle les informations envoyées dans le paquet CDP doivent être mises en cache par le périphérique qui reçoit le paquet CDP et après laquelle les informations expirent.

ÉTAPE 3 Cliquez sur **Apply** pour enregistrer les paramètres.

SNMP

Le protocole SNMP (Simple Network Management Protocol) vous permet de surveiller et de gérer votre routeur à partir d'un gestionnaire SNMP. Le SNMP permet de surveiller et de contrôler les périphériques réseau à distance et de gérer les configurations, la collecte des statistiques, les performances et la sécurité. Le routeur prend en charge la version v2c du protocole SNMP et peut envoyer des déroutements à une communauté spécifique.

Fenêtre SNMP

ÉTAPE 1 Cliquez sur **Network Management > SNMP > SNMP**.

La fenêtre SNMP s'ouvre.

ÉTAPE 2 Pour ajouter une entrée, cliquez sur **Add**.

REMARQUE Cliquez sur le bouton **Edit** pour modifier une entrée. Pour supprimer une entrée, sélectionnez la case correspondante, puis cliquez sur **Delete**. Pour sélectionner toutes les entrées, sélectionnez la case de la première colonne de l'en-tête du tableau.

La fenêtre Configuration SNMP s'ouvre.

ÉTAPE 3 Saisissez les informations suivantes :

- **IP Address :** saisissez l'adresse IP du gestionnaire ou de l'agent de déroutement SNMP.
- **Subnet Mask :** saisissez le masque de réseau utilisé pour déterminer la liste des gestionnaires SNMP autorisés.
- **Port :** saisissez le port de déroutement SNMP de l'adresse IP à laquelle les messages de déroutement seront envoyés.

ÉTAPE 4 Cliquez sur **Apply** pour enregistrer les paramètres.

Fenêtre SNMP System Info

Vous pouvez utiliser cette page pour configurer les champs MIB (Management Information Base).

ÉTAPE 1 Cliquez sur **Network Management > SNMP > SNMP System Info**.

La fenêtre SNMP System Info s'ouvre.

ÉTAPE 2 Saisissez les informations suivantes :

- **SysContact :** nom du contact pour cette appliance de sécurité.
- **SysLocation :** emplacement physique de l'appliance de sécurité.
- **SysName :** nom donné pour une identification aisée de l'appliance de sécurité.

ÉTAPE 3 Cliquez sur **Apply** pour enregistrer les paramètres.

UPnP

UPnP (Universal Plug and Play) est une fonction qui permet la détection automatique de périphériques pouvant communiquer avec cette appliance de sécurité.

Le tableau UPnP Portmap Table affiche les adresses IP et d'autres paramètres des périphériques UPnP qui ont accédé à l'appliance de sécurité.

ÉTAPE 1 Cliquez sur **Network Management > UPnP.**

La fenêtre UPnP s'ouvre.

ÉTAPE 2 Saisissez les informations suivantes :

- **Do you want to enable UPnP? :** cochez ou décochez cette case pour activer ou désactiver la prise en charge UPnP. Si elle est désactivée, le routeur ne permettra pas la configuration automatique du périphérique.
- **Advertisement Period :** il s'agit de la période (en secondes) pendant laquelle ce routeur diffuse ses informations UPnP à tous les périphériques à portée.
- **Advertisement Time to Live :** exprimé en sauts pour chaque paquet UPnP. Il s'agit du nombre d'étapes qu'un paquet est autorisé à propager avant d'être rejeté. Les petites valeurs limiteront la portée de diffusion UPnP.

ÉTAPE 3 Cliquez sur **Apply** pour enregistrer les paramètres.

Bonjour

Bonjour est un protocole de publicité de service et de détection. Bonjour annonce uniquement les services par défaut configurés sur le routeur lorsque Bonjour est activé.

Fenêtre Bonjour Configuration

ÉTAPE 1 Pour activer Bonjour, cliquez sur **Firewall > Attacks**. Désélectionnez la case **Block Multicast Packets** puis cliquez sur **Apply** pour enregistrer vos paramètres.

ÉTAPE 2 Cliquez sur **Network Management** dans la barre de menus, puis cliquez sur **Bonjour > Bonjour Configuration**.

La fenêtre Bonjour Configuration s'ouvre.

ÉTAPE 3 Sélectionnez la case **Enable Bonjour** pour activer les services par défaut. Les services disponibles sont csco-sb, http et https.

Sur un SA500, vous ne pouvez pas désactiver un service spécifique. Vous pouvez seulement activer ou désactiver Bonjour.

ÉTAPE 4 Cliquez sur **Apply** pour enregistrer les paramètres.

Fenêtre VLAN Association

Une fois le service Bonjour activé, vous devez sélectionner un VLAN disponible à lier avec les services par défaut.

ÉTAPE 1 Cliquez sur **Network Management > Bonjour > VLAN Association**.

La fenêtre VLAN Association s'ouvre.

ÉTAPE 2 Sélectionnez le VLAN dans le menu déroulant Available VLANs.

Les services par défaut sont visibles uniquement aux hôtes appartenant aux VLAN associés. Par défaut, le domaine de diffusion est LAN/Default-VLAN.

ÉTAPE 3 Cliquez sur **Apply** pour ajouter le VLAN.

Le VLAN associé au service apparaît dans le tableau List of VLANs.

Pour dissocier le VLAN du service, sélectionnez la case en regard du VLAN approprié et cliquez sur **Delete**.

.

10

État

Ce chapitre décrit la manière d'afficher l'état de votre routeur. Il comprend les sections suivantes :

- **Page Device Status**
- **Page VPN Status**
- **Page Active Users**
- **Page View Logs**
- **Page CDP Neighbor**
- **Page LAN Devices**
- **Page Reports**

Pour accéder aux pages Status, cliquez sur *Status* dans la barre de menus de l'utilitaire de configuration.

Page Device Status

La section Device Status comprend les pages suivantes :

- **Page Device Status**
- **Page Resource Utilization**
- **Page Interface Statistics**
- **Page Port Statistics**
- **Page Wireless Statistics for the SA520W**

Page Device Status

Utilisez la page Dashboard pour afficher les informations du système en temps réel.

Status > **Device Status**

Router Information	
System Name	Nom de l'unité du périphérique.
Firmware (Primary & Secondary)	Version du microprogramme que le routeur utilise actuellement (principal) et version que le routeur exécutait précédemment (secondaire). Par défaut, le routeur démarre avec les informations du routeur principal
Serial Number	Numéro de série de ce périphérique, unique par appliance de sécurité.
Users (Admin/Guest)	Nombre d'utilisateurs administrateurs et invités configurés dans le système
Utilisation des ressources	
CPU Utilization	Utilisation totale du processeur par le système
Memory Utilization	Utilisation totale de la mémoire par le système.
System Up Time	Durée d'exécution du périphérique.
Licences	
Affiche l'état de la licence de diverses fonctionnalités patentées du système. Ces fonctionnalités sont ProtectLink Gateway, ProtectLink Endpoint, VPN SSL et le système de prévention des intrusions.	
Syslog Summary	
Affiche le récapitulatif du journal d'événements du système. Les entrées Syslog peuvent avoir différents niveaux de gravité. Le nombre de journaux de chaque niveau est indiqué.	
Routing Mode	
Affiche le mode de routage du routeur (routage NAT ou classique),	
Mode WAN	

Affiche le mode de configuration WAN du routeur (port WAN unique, renvoi automatique ou équilibrage de charge).	
Interface LAN	
IP Address	Adresse IP LAN du routeur.
DHCP Mode	Affiche le mode du serveur DHCP du routeur. Le mode peut être Disabled, Server ou Relay.
Interface WAN	
IP Address	Adresse IP du port WAN principal (dédié).
State	Indique si la connexion WAN est UP (active) ou DOWN (inactive). L'état est défini sur UP si la liaison est active et que l'interface WAN dispose d'une adresse IP.
Optional Port (WAN/DMZ/LAN)	
IP Address	Adresse IP du port facultatif. Lorsque le port facultatif est en mode LAN, ce champ n'est pas affiché.
State	Indique si la connexion est UP (active) ou DOWN (inactive). Lorsque le port facultatif est en mode LAN ou DMZ, ce champ n'est pas affiché. En mode WAN, l'état est défini sur UP si la liaison est active et que l'interface WAN dispose d'une adresse IP.
Access Points	(s'applique uniquement à SA520W) Affiche le nombre de points d'accès configurés sur le SA520W et le nombre d'utilisateurs associés à chaque SSID.
Site to Site VPN	
All Tunnels	Nombre de tunnels VPN de site à site actifs et nombre total de tunnels VPN de site à site configurés.
Remote Access VPN	
SSL Users	Nombre d'utilisateurs SSL actifs.
IPsec Users	Nombre d'utilisateurs IPsec.

Page Resource Utilization

Utilisez cette page pour afficher les informations de ressources du routeur.

Device Status > Resource Utilization

CPU Utilization	Affiche les statistiques du processeur du système notamment l'utilisation du processeur par utilisateur et par noyau, l'inactivité du processeur et le processeur en attente d'IO.
Memory Utilization	Affiche l'état de la mémoire du système (totale, utilisée, libre, mise en cache et mémoire tampon).

Page Interface Statistics

Utilisez cette page pour afficher les statistiques du transfert de données pour les ports dédiés WAN, facultatif, LAN et WLAN. Cette page est mise à jour toutes les 10 secondes.

Device Status > Interface Statistics

Tx Packets	Nombre de paquets IP quittant le port.
Rx Packets	Nombre de paquets reçus par le port.
Collisions	Nombre de collisions de signal qui se sont produites sur cette interface. Une collision se produit lorsque l'interface tente d'envoyer des données en même temps qu'un port sur un autre routeur ou sur un ordinateur connecté à ce port.
Tx B/s	Nombre d'octets quittant le port par seconde.
Rx B/s	Nombre d'octets reçus par le port par seconde.
Up Time	Durée d'activité du port. La disponibilité est remise à zéro lorsque l'appliance de sécurité ou le port est redémarré.

Poll Interval	Saisissez une valeur en secondes pour l'intervalle entre deux interrogations. Pour modifier l'intervalle entre deux interrogations, cliquez sur le bouton **Stop** puis cliquez sur **Start** pour redémarrer l'actualisation automatique à l'aide de l'intervalle entre deux interrogations spécifié.
Start	Active l'actualisation automatique de page.
Stop	Désactive la fonction d'actualisation automatique de page.

Page Port Statistics

Utilisez cette page pour afficher les statistiques actuelles pour chaque port. Cette page est mise à jour toutes les 10 secondes.

Device Status > Port Statistics

Port Id	Indique les ID de port physique du périphérique (commutateur).
Tx Bytes	Nombre d'octets de données valides transmis par un port (y compris FCS). Le préambule est exclu.
Tx Drop Pkts	Ce compteur est incrémenté chaque fois qu'un paquet est rejeté par manque de ressources (par exemple le dépassement de transmission FIFO).
Rx Bytes	Nombre d'octets de données reçus par un port, y compris FCS et les paquets non valides. Le préambule est exclu.
Rx Drop Pkts	Affiche le nombre de paquets valides reçus par un port rejetés par manque de ressources (par exemple l'absence de mémoire tampon d'entrée).
Poll Interval	Saisissez une valeur en secondes pour l'intervalle entre deux interrogations. La page relit alors les statistiques de l'appliance de sécurité et s'actualise automatiquement. Pour modifier l'intervalle entre deux interrogations, cliquez sur le bouton Stop puis cliquez sur Start pour redémarrer l'actualisation automatique.

Start	Active l'actualisation automatique de page.
Stop	Désactive l'actualisation automatique de page.

Page Wireless Statistics for the SA520W

Cette page affiche le total cumulé des statistiques pertinentes pour le réseau sans fil et ses points d'accès configurés. Les compteurs sont réinitialisés lorsque le périphérique est redémarré.

Radio Statistics

Le réseau radio peut présenter plusieurs points d'accès virtuels configurés et actifs simultanément. Ce tableau indique les statistiques cumulatives pour le réseau radio.

Device Status > Radio Statistics

Radio	ID numérique du réseau radio.
Packets	Nombre de paquets sans fil transmis ou reçus (tx/rx) signalés au réseau radio, sur tous les points d'accès configurés.
Bytes	Nombre d'octets d'informations transmis ou reçus (tx/rx) signalés au réseau radio, sur tous les points d'accès configurés.
Errors	Nombre d'erreurs de paquets transmis ou reçus (tx/rx) signalées au réseau radio, sur tous les points d'accès configurés.
Dropped	Le nombre de paquets transmis ou reçus (tx/rx) rejetés par le réseau radio, sur tous les points d'accès configurés.
Multicast	Nombre de paquets de multidiffusion envoyés sur le réseau radio.

Access Point Statistics

Ce tableau affiche les données d'émission ou de réception d'un point d'accès donné.

Device Status > Access Point Statistics

Nom du SSID	Nom du point d'accès.
Radio	Numéro radio sur lequel est configuré le point d'accès.
Packets	Nombre de paquets sans fil transmis ou reçus (tx/rx) sur le point d'accès.
Bytes	Nombre d'octets d'informations transmis ou reçus (tx/rx) sur le point d'accès.
Errors	Nombre d'erreurs de paquets transmis ou reçus (tx/rx) signalées au point d'accès.
Dropped	Nombre de paquets transmis ou reçus (tx/rx) rejetés par le point d'accès.
Multicast	Nombre de paquets de multidiffusion envoyés sur ce point d'accès.
Poll Interval	Saisissez une valeur en secondes pour l'intervalle entre deux interrogations. Pour modifier l'intervalle entre deux interrogations, cliquez sur le bouton **Stop** puis cliquez sur **Start** pour redémarrer l'actualisation automatique à l'aide de l'intervalle entre deux interrogations spécifié.

Page VPN Status

Page IPsec VPN Status

Utilisez cette page pour afficher les statistiques actuelles des connexions IPsec. Vous pouvez utiliser les boutons de la page pour démarrer ou arrêter une connexion. La page s'actualise aussi automatiquement pour afficher le dernier état d'un SA.

Status > VPN Status > IPsec Status

Policy Name	Nom de la stratégie IKE ou VPN.
Endpoint	Affiche l'adresse IP de la passerelle ou du client VPN distant.
Tx (KB)	Données transmises en kilooctets.
Tx (Packets)	Nombre de paquets IP transmis.
State	Affiche l'état actuel des stratégies IKE. L'état peut être Not Connected ou IPsec SA Established.
Action	Cliquez sur **Connect** pour établir une connexion SA inactive ou **Drop** pour terminer une connexion SA active. Lorsqu'une stratégie VPN est en place et activée, tout trafic correspondant à la stratégie déclenche une connexion et le tunnel VPN est configuré automatiquement. Toutefois, vous pouvez utiliser le bouton Connect/Disconnect manuellement pour connecter ou déconnecter le tunnel VPN.

Page SSL VPN Status

Cette page affiche les statistiques actuelles des connexions du tunnel VPN SSL. Vous pouvez utiliser les boutons de la page pour démarrer ou arrêter les connexions.

Status > VPN Status > SSL VPN Status

User Name	Nom d'utilisateur de l'utilisateur connecté.
IP Address	Adresse IP Internet à partir de laquelle l'établissement du tunnel a été initialisé.
Tunnel Specific Fields	
Local ppp interface	Nom de l'interface PPP sur le routeur associé au tunnel sslvpn.
Peer PPP Interface IP	Adresse IP attribuée à l'interface PPP du côté du client distant à partir duquel le tunnel est établi.

Tx Packets	Nombre de paquets associés au tunnel transférés par le client distant.
Tx Dropped Packets	Nombre de paquets associés au tunnel rejetés au cours du transfert, par le client distant.
Tx Bytes (KB)	Volume total du trafic envoyé (en kilooctets) associé au tunnel.
Rx Packets	Nombre de paquets associés au tunnel reçus par le client distant.
Rx Dropped Packets	Nombre de paquets associés au tunnel rejetés au cours de la réception, par le client distant.
Rx Bytes (KB)	Volume total du trafic reçu (en kilooctets) associé au tunnel.
Connection Status	Cliquez sur **Disconnect** pour terminer une session d'utilisateur active et le tunnel SSLVPN associé (le cas échéant). **REMARQUE** Si le tunnel n'est pas établi par l'utilisateur, les champs spécifiques du tunnel ne contiendront aucune valeur.
Poll Interval	Saisissez une valeur en secondes pour l'intervalle entre deux interrogations. Pour modifier l'intervalle entre deux interrogations, cliquez sur le bouton **Stop** puis cliquez sur **Start** pour redémarrer l'actualisation automatique à l'aide de l'intervalle entre deux interrogations spécifié.
Start	Cliquez sur cette option pour activer la fonctionnalité d'actualisation automatique de page.
Stop	Cliquez sur **Stop** pour désactiver la fonctionnalité d'actualisation automatique de page.

Page Quick VPN Status

Cette page affiche l'état des connexions QuickVPN et vous permet de terminer (DROP) toutes les connexions actives (ONLINE) existantes.

Status > VPN Status > Quick VPN Status

User Name	Nom de l'utilisateur IPsec associé au tunnel QuickVPN.
Remote IP	Affiche l'adresse IP du client QuickVPN distant. Il peut s'agir d'une IP NAT ou publique si le client se trouve derrière le routeur NAT.
Status	Affiche l'état actuel du client QuickVPN. OFFLINE signifie que le tunnel QuickVPN n'est PAS initié ou établi par l'utilisateur IPsec. ONLINE signifie que ce tunnel QuickVPN, initié ou établi par l'utilisateur IPsec, est actif.
Action	Cliquez sur **Drop** pour terminer une connexion active ou ONLINE et changer l'état du client QuickVPN client en OFFLINE.
Poll Interval	Durée, en secondes, après laquelle la page se recharge automatiquement. Pour modifier l'intervalle entre deux interrogations, cliquez sur le bouton Stop et utilisez Start pour redémarrer l'actualisation automatique.
Start	Cliquez sur cette option pour activer la fonctionnalité d'actualisation automatique de page.
Stop	Cliquez sur Stop pour désactiver la fonctionnalité d'actualisation automatique de page.

Page Active Users

Cette page répertorie les utilisateurs administrateurs et VPN SSL actuellement connectés au périphérique. Un bouton sur la page permet de déconnecter tout utilisateur.

Status > Active Users

User Name	Identifiant unique pour l'utilisateur.
Group	Groupe auquel appartient l'utilisateur connecté.
IP address	Adresse IP de l'hôte à partir de laquelle l'utilisateur a accédé au routeur.
Login Time	Horodatage de la première connexion de l'utilisateur au routeur.
Disconnect	Termine une session d'utilisateur active et le tunnel SSLVPN associé (le cas échéant).

Page View Logs

Page View All Logs

Utilisez cette page pour afficher le contenu du journal des messages système générés par niveau de gravité et type d'installation.

Pour obtenir des informations sur la configuration des journaux, consultez **Configurer les options de journalisation, page 198.**

ÉTAPE 1 Cliquez sur **Status > View Logs > View All Logs**.

ÉTAPE 2 Sélectionnez les journaux à afficher.

Log Severity : choisissez un niveau de gravité pour le journal. Vous pouvez choisir parmi les niveaux suivants : Emergency, Alert, Critical, Error, Warning, Notification, Information ou Debugging. Pour obtenir une description de ces niveaux, consultez **Fenêtre Logs Facility and Severity, page 203.**

Par exemple : si vous sélectionnez Critical, tous les messages répertoriés sous Critical, Error Warning, Notification, Information et Debugging s'affichent. Les catégories Emergency et Alert ne sont pas affichées.

Log Facility : choisissez l'installation à partir de laquelle les journaux doivent être affichés.

All	Affiche tous les journaux d'installation.
Kernel logs	Affiche les journaux appartenant au code de noyau.

System logs	Affiche les journaux des applications de l'espace utilisateur tels que NTP, Session et DHCP.
Wireless	Affiche des journaux relatifs au réseau sans fil.
IPS	Affiche des journaux générés par le système IPS (Intrusion Prevention System).
ProtectLink	Affiche les journaux de la passerelle ProtectLink et des services de points de terminaison.
VPN	Affiche les journaux relatifs à IKE et VPN SSL.
Firewall	Affiche les journaux relatifs aux règles, aux attaques et au filtrage de contenu de pare-feu
Network	Affiche les journaux de routage DHCP, WAN, LAN et QoS.

ÉTAPE 3 Saisissez l'adresse IP source et de destination pour filtrer les journaux du pare-feu.

Les caractères génériques tels que l'astérisque (*) et le point (.) sont autorisés dans les champs d'adresse source et de destination

ÉTAPE 4 Cliquez sur **Apply** pour enregistrer les paramètres.

Les informations de journal sont affichées dans la zone Log Area. Elle comprend les informations suivantes :

Date	Date et heure du journal correspondant.
Severity	Gravité du journal correspondant.
Facility	Installation du journal correspondant.
Source IP	Adresse IP source du journal correspondant.
Destination IP	Adresse IP de destination du journal correspondant.
Log Data	Contenu de chaque journal.

- Cliquez sur **Refresh Logs** pour afficher les entrées ajoutées après l'ouverture de la page.
- Cliquez sur **Clear Logs** pour supprimer toutes les entrées de la fenêtre de journal.
- Cliquez sur **Send Logs** pour envoyer par courrier électronique des messages de journal actuellement affichés dans la fenêtre de journal. Les journaux sont envoyés aux adresses électroniques que vous avez configurées sur la page

Remote Logging Configuration. Pour obtenir plus d'informations, reportez-vous au **Fenêtre Remote Logging Config, page 201**

Page IPsec VPN Logs

Utilisez cette page pour afficher le contenu du journal généré par toutes les stratégies VPN IPsec. Les journaux sont générés automatiquement et n'ont pas besoin d'être explicitement activés. Cette page affiche l'état de l'activité récente du VPN IPsec.

Status > View Logs > IPsec VPN Logs

- Cliquez sur **Refresh Logs** pour afficher les entrées ajoutées après l'ouverture de la page.
- Cliquez sur **Clear Logs** pour supprimer toutes les entrées de la fenêtre de journal.

Page ProtectLink Logs

Utilisez cette page pour afficher les journaux des événements de services ProtectLink.

Status > View Logs > ProtectLink Logs

- Cliquez sur **Clear Logs** pour supprimer toutes les entrées de la fenêtre de journal
- Cliquez sur **Refresh Logs** pour afficher les entrées ajoutées après l'ouverture de la page.
- Cliquez sur **Send Logs** pour envoyer par courrier électronique des messages de journal actuellement affichés dans la fenêtre de journal. Vérifiez que l'adresse électronique et les informations de serveur sont configurées sur la page Firewall Logs & E-mail (sous le menu Administration) avant de cliquer sur Send Log.

Page CDP Neighbor

Le protocole CDP (Cisco Discovery Protocol) fournit des informations sur d'autres périphériques connectés à ce périphérique et qui prennent en charge le protocole CDP. La page affiche des informations spécifiques au périphérique et identifie l'interface réseau de ce périphérique sur lequel le voisin a été détecté. Pour obtenir plus d'informations sur la configuration globale du protocole CDP, consultez **CDP, page 213**.

Status* > *CDP Neighbor

Device Id	Affiche l'identifiant du périphérique annoncé par le voisin
Local Port	Interface sur laquelle le voisin a été détecté.
Duration	Nombre de minutes pendant lesquelles un périphérique a été connecté.
Function	Type de périphérique : R (routeur), T (pont de commutateur), S (commutateur), H (hôte), I-(IGMP), r (répéteur).
Platform	Nom de la plate-forme de l'équipement voisin.
Interface ID	Identifiant de l'interface du voisin.

Page LAN Devices

La page LAN Devices affiche tous les hôtes connectés au réseau LAN. Pour chaque périphérique, la page affiche l'adresse IP et l'adresse MAC associée. Le champ Name est également affiché pour les hôtes qui s'identifient à l'aide de NETBIOS. Pour tous les autres périphériques le nom est affiché en tant que « inconnu ».

Page Reports

Utilisez la page Reports pour afficher les 10 principaux sites Web visités ou les 10 principaux sites Web bloqués par des composants du filtrage de contenu ou du filtrage URL ProtectLink. La page est uniquement active lorsque les composants de filtrage de contenu ou de filtrage URL ProtectLink sont activés. Pour ouvrir cette page, cliquez sur **Status** > **Reports**.

Dans la liste déroulante **Report View**, choisissez le type de rapport à afficher, Website Hits ou Website Blocks. Puis cliquez sur **Apply** pour enregistrer vos modifications.

- Cliquez sur **Refresh Data** pour mettre à jour les données à l'écran.
- Cliquez sur **Reset Data** pour remettre les valeurs à 0.

REMARQUE *Elapsed Collection Time* indique la période de temps pendant laquelle les données ont été collectées.

A

Dépannage

Connexion Internet

Symptôme : sous ne pouvez pas accéder à l'utilitaire de configuration à partir d'un PC sur votre réseau LAN.

Action recommandée :

ÉTAPE 1 Vérifiez la connexion Ethernet entre le PC et l'appliance de sécurité.

ÉTAPE 2 Vérifiez que l'adresse IP de votre PC se trouve sur le même sous-réseau que l'appliance de sécurité. Si vous utilisez le schéma d'adressage recommandé, l'adresse de votre PC doit être comprise entre 192.168.75.2 et 192.168.75.254.

ÉTAPE 3 Vérifiez l'adresse IP de votre PC. Si le PC ne peut pas à joindre un serveur DHCP, certaines versions de Windows et de Mac OS génèrent et attribuent une adresse IP. Ces adresses sont générées automatiquement dans la plage 169.254.x.x. Si votre adresse IP se trouve dans cette plage, vérifiez la connexion du PC au pare-feu et redémarrez votre PC.

ÉTAPE 4 Si votre adresse IP a changé et que vous ne la connaissez pas, rétablissez les paramètres d'usine par défaut de l'appliance de sécurité (y compris l'adresse IP 192.168.75.1du pare-feu).

Si vous ne souhaitez pas rétablir les paramètres d'usine par défaut et perdre votre configuration, redémarrez l'appliance de sécurité et utilisez un outil de surveillance des paquets (par exemple Ethereal™) pour capturer les paquets envoyés au cours du redémarrage. Regardez les paquets du protocole de résolution d'adresse (ARP) pour localiser l'adresse de l'interface LAN.

ÉTAPE 5 Lancez le navigateur et vérifiez que java, Javascript ou ActiveX est activé. Si vous utilisez Internet Explorer, cliquez sur **Actualiser** pour vérifier que l'applet Java est chargé. Fermez le navigateur et relancez-le.

ÉTAPE 6 Vérifiez que vous utilisez les informations de connexion appropriées. Le nom de connexion par défaut est **cisco** et le mot de passe est **cisco**. Vérifiez que VERR. MAJ est désactivé lorsque vous saisissez ces informations.

Symptôme : l'appliance de sécurité n'enregistre pas mes modifications de configuration.

Action recommandée :

ÉTAPE 1 En saisissant les paramètres de configuration, cliquez sur **Apply** avant de passer à un autre menu ou onglet ; sinon vos modifications sont perdues.

ÉTAPE 2 Cliquez sur **Actualiser** ou **Recharger** dans le navigateur, ce qui effacera une copie de l'ancienne configuration dans le cache.

Symptôme : l'appliance de sécurité ne peut pas accéder à Internet.

Cause possible : si vous utilisez des adresses IP dynamiques, votre appliance de sécurité ne demande pas d'adresse IP au FAI.

Action recommandée :

ÉTAPE 1 Lancez le navigateur et vérifiez si vous pouvez vous connecter à un site externe tel que www.google.com.

ÉTAPE 2 Lancez l'utilitaire de configuration.

ÉTAPE 3 Cliquez sur **Status > Device Status > Device Status**.

ÉTAPE 4 Dans la zone **Dedicated WAN Info**, recherchez l'**adresse IPv4**. Si 0.0.0.0 est indiqué, votre pare-feu n'a pas obtenu d'adresse IP de votre FAI. Reportez-vous au prochain symptôme.

Symptôme : l'appliance de sécurité ne peut pas obtenir d'adresse IP du FAI.

Action recommandée :

ÉTAPE 1 Coupez l'alimentation du câble ou du modem DSL.

ÉTAPE 2 Désactivez l'appliance de sécurité.

ÉTAPE 3 Attendez 5 minutes, puis rebranchez le câble ou le modem DSL à l'alimentation.

ÉTAPE 4 Lorsque les voyants DEL du modem indiquent qu'il est resynchronisé avec le FAI, rebranchez l'appliance de sécurité à l'alimentation. Si l'appliance de sécurité ne peut toujours pas obtenir d'adresse du FAI, reportez-vous au prochain symptôme.

Symptôme : l'appliance de sécurité ne peut toujours pas obtenir d'adresse IP du FAI.

Action recommandée :

ÉTAPE 1 Cliquez sur **Networking > WAN > IPv4 Config**.

ÉTAPE 2 Posez à votre FAI les questions suivantes :

- Une connexion est-elle nécessaire pour votre connexion Internet ? Si oui, de quel type ? Sur la page IPv4 WAN Configuration, sélectionnez la case **Internet Connection Requires a Login**. Choisissez le type de connexion au FAI correct, puis saisissez les informations de compte comme spécifiées par le FAI (nom d'utilisateur, mot de passe et secret, le cas échéant).
- Votre FAI vérifie-t-il le nom d'hôte de votre PC ? Si oui, dans le champ **User Name**, saisissez le nom d'hôte du PC requis pour votre compte FAI.
- Votre FAI s'attend-il à ce que vous vous connectiez à partir d'une adresse MAC Ethernet particulière ? Si oui, dans la zone **Router's MAC Address**, choisissez **Use this MAC Address** pour la **MAC Address Source**, puis saisissez l'adresse MAC requise dans le champ prévu à cet effet.

Symptôme : l'appliance de sécurité peut obtenir une adresse IP, mais le PC ne peut pas charger les pages Internet.

Action recommandée :

ÉTAPE 1 Demandez à votre FAI les adresses de ses serveurs DNS (Domain Name System) désignés. Configurez votre PC pour qu'il identifie ces adresses. Pour plus de détails, reportez-vous à la documentation de votre système d'exploitation.

ÉTAPE 2 Sur votre PC, configurez l'appliance de sécurité en tant que passerelle TCP/IP.

Date et heure

Symptôme : la date affichée est le 1er janvier 2000.

Cause possible : l'appliance de sécurité n'a pas encore pu atteindre de serveur NTS (Network Time Server).

Action recommandée :

ÉTAPE 1 Si vous venez de configurer l'appliance de sécurité, attendez au moins 5 minutes, cliquez sur **Administration > Time Zone**.

ÉTAPE 2 Vérifiez les paramètres de date et heure.

ÉTAPE 3 Vérifiez vos paramètres d'accès à Internet.

Symptôme : l'heure de l'appliance retarde d'une heure.

Cause possible : l'appliance de sécurité ne se met pas automatiquement à l'heure d'été.

Action recommandée :

ÉTAPE 1 Cliquez sur **Administration > Time Zone**.

ÉTAPE 2 Vérifiez ou désélectionnez **Automatically adjust for Daylight Savings Time**.

ÉTAPE 3 Cliquez sur **Apply** pour enregistrer les paramètres.

Effectuer un test ping pour tester la connectivité LAN

La plupart des périphériques de terminal TCP/IP et des pare-feu contient un utilitaire de ping qui envoie un paquet de demande d'écho ICMP au périphérique désigné. Le périphérique répond par un écho. Le dépannage d'un réseau TCP/IP est grandement facilité par l'utilitaire de ping de votre PC ou station de travail.

Évaluation du chemin LAN de votre PC à votre appliance de sécurité

ÉTAPE 1 Sur votre PC, cliquez sur le bouton **Démarrer** de Windows, puis cliquez sur **Exécuter**.

ÉTAPE 2 Saisissez le ping <IP_address> où <IP_address> est l'adresse IP de l'appliance de sécurité. Exemple : ping 192.168.75.1.

ÉTAPE 3 Cliquez sur **OK**.

ÉTAPE 4 Observez le résultat qui s'affiche :

- Si le chemin fonctionne, cette séquence de message s'affiche :

```
Pinging <IP address> with 32 bytes of data
Reply from <IP address>: bytes=32 time=NN ms TTL=xxx
```

- Si le chemin ne fonctionne pas, cette séquence de message s'affiche :

```
Pinging <IP address> with 32 bytes of data
Request timed out
```

ÉTAPE 5 Si le chemin ne fonctionne pas, testez les connexions physiques entre le PC et l'appliance de sécurité :

- Si le voyant DEL du port LAN est éteinte, accédez à la section « Affichages des voyants DEL », page B-1 et suivez les instructions concernant « Les voyants DEL du port Internet ou LAN ne sont pas allumées ».
- Vérifiez que les voyants DEL de liaison correspondantes sont allumées pour votre carte d'interface réseau et pour tous les ports du concentrateur connectés à votre station de travail et à votre pare-feu.

ÉTAPE 6 Si le chemin n'est toujours pas actif, testez la configuration réseau :

- Vérifiez que le logiciel du pilote de la carte Ethernet et le logiciel TCP/IP sont installés et configurés sur le PC.
- Vérifiez que l'adresse IP de l'appliance de sécurité et du PC sont correctes et se trouvent sur le même sous-réseau.

Évaluation du chemin LAN de votre PC à un périphérique distant

ÉTAPE 1 Sur votre PC, cliquez sur le bouton **Démarrer** de Windows, puis cliquez sur **Exécuter**.

ÉTAPE 2 Saisissez le ping -n 10 <IP_address> où -n 10 spécifie un maximum de 10 essais et <IP address> est l'adresse IP du périphérique distant, par exemple le serveur DNS de votre prestataire de services. Exemple : ping -n 10 10.1.1.1.

ÉTAPE 3 Cliquez sur **OK** puis observez le résultat qui s'affiche (reportez-vous à la procédure précédente).

ÉTAPE 4 Si le chemin ne fonctionne pas, procédez comme suit :

- Vérifiez que l'adresse IP de votre pare-feu est répertoriée comme passerelle par défaut. (Si la configuration IP de votre PC est attribuée par DHCP, ces informations ne sont pas visibles dans l'application Réseau du Panneau de Configuration de votre PC.)
- Vérifiez que l'adresse réseau (sous-réseau) de votre PC est différente de l'adresse réseau du périphérique distant.
- Vérifiez que le câble ou le modem DSL est connecté et fonctionne.
- Contactez votre FAI et posez-lui les questions répertoriées dans **Symptôme : l'appliance de sécurité ne peut toujours pas obtenir d'adresse IP du FAI.**
- Demandez à votre FAI s'il rejette les adresses MAC Ethernet de tous vos ordinateurs sauf un. De nombreux FAI de haut débit limitent l'accès en acceptant le trafic uniquement de l'adresse MAC de votre modem haut débit. Certains FAI restreignent encore l'accès à l'adresse MAC d'un seul PC connecté à ce modem. Dans ce cas, configurez votre pare-feu pour cloner ou usurper l'adresse MAC du PC autorisé. Pour obtenir plus d'informations, reportez-vous à la section **Configuration de la connexion WAN, page 37.**

Restauration des paramètres de la configuration d'usine par défaut

Pour rétablir les paramètres de la configuration d'usine par défaut, effectuez l'une de ces opération :

- Lancez l'utilitaire de configuration et connectez-vous. Cliquez sur **Administration > Firmware & Configuration > Network**. Dans la zone **Backup/Restore Settings**, cliquez sur **Default**.

  OU

- Appuyez et maintenez enfoncé le bouton Reset de la façade avant de l'appliance de sécurité pendant environ 10 secondes, jusqu'à ce que le voyant DEL de test s'allume et clignote. Relâchez le bouton et attendez que l'appliance de sécurité redémarre. Si l'appliance de sécurité ne redémarre pas automatiquement, redémarrez-la manuellement pour appliquer les paramètres par défaut.

Après la restauration des valeurs d'usine par défaut, les paramètres suivants s'appliquent :

- LAN IP address : **192.168.75.1**
- Nom d'utilisateur : **cisco**
- Password: **cisco**
- DHCP server on LAN : **activé**
- WAN port configuration : **Get configuration via DHCP**

B

Services standard

L'appliance de sécurité est configurée avec la liste suivante de services standard disponibles pour le transfert de port et la configuration du pare-feu. Si vous voulez configurer une règle de transfert de port ou une règle de pare-feu pour un service qui n'est pas sur cette liste, vous pouvez créer un service personnalisé dans cet objectif. Voir aussi **Création de services personnalisés, page 108.**

TOUTE

AIM

BGP

BOOTP_CLIENT

BOOTP_SERVER

CU-SEEME:UDP

CU-SEEME:TCP

DNS:UDP

DNS:TCP

FINGER

FTP

HTTP

HTTPS

ICMP-TYPE-3

ICMP-TYPE-4

ICMP-TYPE-5

ICMP-TYPE-6

ICMP-TYPE-7

ICMP-TYPE-8

ICMP-TYPE-9

ICMP-TYPE-10

ICMP-TYPE-11

ICMP-TYPE-13

ICQ

IMAP2

IMAP3

IRC

NEWS

NFS

NNTP

PING

POP3

PPTP

RCMD

REAL-AUDIO

REXEC

RLOGIN

RTELNET

RTSP:TCP

RTSP:UDP

SFTP

SMTP

SNMP:TCP

SNMP:UDP

SNMP-TRAPS:TCP

SNMP-TRAPS:UDP

SQL-NET

SSH:TCP

SSH:UDP

STRMWORKS

TACACS

TELNET

TFTP

VDOLIVE

C

Spécifications techniques et environnementales

Fonctionnalité	SA520	SA520W	SA540
Normes	▪ IEEE 802.3 CSMA1CD ▪ IEEE 802.3i 10BASE-T ▪ IEEE 802.3U 100BASE-TX ▪ IEEE 802.3x (contrôle de flux en duplex intégral) ▪ IEEE 802.3ab (1000BASE-T) ▪ Auto MDI1MDIX ▪ IEEE 802.3Z (1000BASE-X)	▪ IEEE 802.3 CSMA1CD ▪ IEEE 802.3i 10BASE-T ▪ IEEE 802.3U 100BASE-TX ▪ IEEE 802.3x (contrôle de flux en duplex intégral) ▪ IEEE 802.3ab (1000BASE-T) ▪ Auto MDI1MDIX ▪ IEEE 802.3Z (1000BASE-X) ▪ IEEE 802.11n ▪ IEEE 802.1b, g et n	▪ IEEE 802.3 CSMA/CD ▪ IEEE 802.3 10BASE-T ▪ IEEE 802.3u 100BASE-TX ▪ IEEE 802.3ab 1000BASE-T ▪ IEEE 802.3x (contrôle de flux en duplex) ▪ Auto MDI/MDIX
Interfaces physiques	▪ 4 connecteurs RJ-45 pour le port LAN ▪ 1 connecteur RJ-45 pour le port WAN ▪ 1 connecteur RJ-45 pour le port LAN, WAN ou DMZ ▪ 1 connecteur USB pour USB 2.0 ▪ 1 commutateur d'alimentation	▪ 4 connecteurs RJ-45 pour le port LAN ▪ 1 connecteur RJ-45 pour le port WAN ▪ 1 connecteur RJ-45 pour le port LAN, WAN ou DMZ ▪ 1 connecteur USB pour USB 2.0 ▪ 1 commutateur d'alimentation ▪ 3 antennes externes	▪ 8 connecteurs RJ-45 pour 10BASE-T, 100BASE-TX, 1000BASE-T ▪ 1 connecteur RJ-45 pouvant être un port LAN, WAN ou DMZ ▪ 1 connecteur RJ-45 pour le port WAN ▪ 1 connecteur USB pour USB 2.0
Température de fonctionnement	De 0 à 40 ºC (de 32 à 104 ºF)	De 0 à 40 ºC (de 32 à 104 ºF)	De 0 à 40 ºC (de 32 à 104 ºF)

Fonctionnalité	SA520	SA520W	SA540
Température de stockage	-20 à 70°C (-4 à 158°F)	-20 à 70°C (-4 à 158°F)	-20 à 70°C (-4 à 158°F)
Humidité de fonctionnement	Humidité relative de 10 à 90 %, sans condensation	Humidité relative de 10 à 90 %, sans condensation	Humidité relative de 10 à 90 %, sans condensation
Humidité de stockage	Humidité relative de 5 à 95 %, sans condensation	Humidité relative de 5 à 95 %, sans condensation	Humidité relative de 5 à 95 %, sans condensation
Alimentation interne			
Plage de tension	90 à 264 VCA, MONOPHASÉ	90 à 264 VCA, MONOPHASÉ	90 à 264 VCA, MONOPHASÉ
Bande de fréquences en entrée	De 47 Hz à 63 Hz	De 47 Hz à 63 Hz	De 47 Hz à 63 Hz
Régulation de la tension de sortie	11.4 V ~ 12.6 V	11.4 V ~ 12.6 V	11.4 V ~ 12.6 V
Courant de sortie	MAX 2.5 A	MAX 2.5 A	MAX 2.5 A
Puissance d'émission (par défaut)	N/A	11 dBm	N/A
Spécifications physiques			
Format	Possibilité de montage sur bâti (rack) 1 RU, 19 pouces	Possibilité de montage sur bâti (rack) 1 RU, 19 pouces	Possiblité de montage sur bâti (rack) 1 RU, 19 pouces
Dimensions (H x W x D)	44 x 308 x 180 mm (1-3/4 x 12-1/8 x 7-1/8 pouces)	44 x 308 x 180 mm (1-3/4 x 12-1/8 x 7-1/8 pouces) L'antenne ajoute approximativement 171 mm (6-3/4 pouces) de hauteur et 30 mm (1-2/8 pouces) de profondeur.	44 x 308 x 180 mm (1-3/4 x 12-1/8 x 7-1/8 pouces)
Poids (avec alimentation)	4,91 lb	5.15	5,14 lb

D

Paramètres d'usine par défaut

Paramètres généraux

Fonctionnalité	Paramètre
Host Name	Numéro de modèle
Device Name	Numéro de modèle
Administrator Username	cisco
Administrator Password	cisco
Allow ICMP echo replies (good for validating connectivity)	désactiver
Date and Time - Automatic Time Update	activer
Date and Time - Daylight Savings Time	activer
Date and Time - Protocol	NTP
Date and Time - Time Zone	Heure du Pacifique (USA & Canada)
DDNS	désactiver
HTTP Remote Access	activer
HTTPS Remote Access	activer
SNMP - Trusted Peer	adresse IP
SNMP Agent	désactiver

Fonctionnalité	Paramètre
SNMP Version	SNMP V1 & V2c, SNMP V3
SNMP Read-Only Community String	public
SNMP Read-Write Community String	privé
SNMP Traps	désactiver
System Logging - Notify Level	À titre de information
System Logging	désactiver
System Logging - Log UnAuthorized Login Attempts	activer
System Logging - Log Authorized Login Attempts	activer
System Logging - Log System Errors	activer
System Logging - Configuration Changes	activer
Email Server Requires Authentication	désactiver
Cisco Discovery Protocol	activé sur le LAN / désactivé sur le port WAN
Bonjour	activé sur le LAN / désactivé sur le port WAN
UPnP	désactiver
Radius Server Port	1812

Paramètres du routeur

Fonctionnalité	Paramètre
VLAN - Voice, Name	Voice VLAN
VLAN - Voice, VLAN Number (802.1q tagged packets)	100
VLAN - Voice, IP Address	10.1.1.1
VLAN - Voice, IP Address Distribution	DHCP Server
VLAN - Voice, Start IP Address	10.1.1.50
VLAN - Voice, End IP Address	10.1.1.254
VLAN - Voice, Subnet Mask	255.255.255.0
VLAN - Data, Lease Time in Minutes	1440
HTTP Remote Access	désactiver
HTTPS Remote Access	désactiver
VLAN - Data, Name	Data VLAN
VLAN - Data, VLAN Number (untagged packets)	1
VLAN - Data, IP Address	Voir l'onglet Product
VLAN - Data, IP Address Distribution	DHCP Server
VLAN - Data, Start IP Address	192.168.x.50
VLAN - Data, End IP Address	192.168.x.254
VLAN - Data, Subnet Mask	255.255.255.0
VLAN - Data, Lease Time in Minutes	1440
HTTP Remote Access	activer

Fonctionnalité	Paramètre
HTTPS Remote Access	activer
WAN1 IP address assignment	DHCP Client
WAN1 - MTU	1500
WAN1- Outgoing Traffic Bandwidth Limit	désactiver
Allow ICMP echo replies (good for validating connectivity)	désactiver
HTTPS Remote Access	désactiver
WAN2 IP address assignment	DHCP Client
WAN2 - MTU	1500
WAN2- Outgoing Traffic Bandwidth Limit	désactiver
Allow ICMP echo replies (good for validating connectivity)	désactiver
HTTPS Remote Access	désactiver
Routing (RIP1/2)	désactiver
Inter-VLAN routing	activer / désactiver le VLAN DMS
Static Routing	désactiver
IPv4 and IPv6	IPv4 uniquement
IPSec - Signaling Authentication - Key Exchange Method	Automatique
IPSec - Signaling Authentication - Auto Reconnect	activer
IPSec - Signaling Authentication - Local Subnet (Data VLAN subnet)	192.168.10.0
IPSec - Signaling Authentication - Local Subnet (Data VLAN subnet mask)	255.255.255.0

Fonctionnalité	Paramètre
IPSec - Signaling Authentication - Keying Mode	IKE avec PSK
IPSec - Signaling Authentication - Phase 1 - Mode	Mode principal
IPSec - Signaling Authentication - Phase 1 - Encryption Algorithm	3DES-CBC, AES 256
IPSec - Signaling Authentication - Phase 1 - Hash Algorithm	SHA1
IPSec - Signaling Authentication - Phase 1 - Group Description Attribute	Groupe 2 DH (1024 bits)
IPSec - Signaling Authentication - Phase 1 - Lifetime in Seconds	28800
IPSec - Signaling Authentication - Phase 1 - Rekey Margin	540
IPSec - Signaling Authentication - Phase 1 - Rekey Fuzz Percent	100
IPSec - Signaling Authentication - Phase 1 - Negotiation Attempts	Infini
IPSec - Signaling Authentication - Phase 2 - Encryption Algorithm	3DES-CBC, AES 256
IPSec - Signaling Authentication - Phase 2 - Authentication Algorithm	SHA1
IPSec - Signaling Authentication - Phase 2 - Use PFS	désactiver
IPSec - Signaling Authentication - Phase 2 - Group Description Attribute	Groupe 2 DH (1024 bits)
IPSec - Signaling Authentication - Phase 2 - Hash Algorithm	SHA1

Fonctionnalité	Paramètre
IPSec - Signaling Authentication - Phase 2 - Lifetime in Seconds	3600
IPSec Pass through	activer
PPTP Pass through	activer
L2TP Pass through	activer

Paramètres sans fil

Fonctionnalité	Paramètre
VLAN - Voice, VLAN Number (802.1q tagged packets)	100
VLAN - Voice, Name (optional)	Voice VLAN
SSID Name	cisco-voice
SSID Broadcast	désactiver
Wireless Isolation (within SSID):	désactiver
802.1q Priority	5
802.11e Priority	6
VLAN - Data, VLAN Number (untagged packets)	1
VLAN - Data, IP Address Assignment (Management)	DHCP Client
VLAN - Data, IP Address (Failover when no DHCP Server Available)	Voir l'onglet Product
VLAN - Data, Subnet Mask (Failover when no DHCP Server Available)	255.255.255.0
VLAN - Data, Name (optional)	Data VLAN

Fonctionnalité	Paramètre
SSID Name	cisco-data
SSID Broadcast	désactiver
Wireless Isolation (within SSID):	désactiver
802.1q Priority	0
Radius Server Port	1812
Key Renewal Timeout	3600
Connection Control (MAC address filtering)	Désactivée
Wireless Isolation (between SSIDs):	activé
Wireless Network Mode	Mixte (802.11b, g, n)
Wireless Channel	Auto
CTS Protection Mode	désactivé
Basic Data Rates (Advertised)	Toutes
Beacon Interval	100 ms
DTIM Interval	2 ms
RTS Threshold	2347
Fragmentation Threshold	2346
Power Output	100%
Radio	désactivé
802.1x supplicant	désactivé
Clustering of Access Points - unique to AP54x	désactivé
Broadcast / Multicast Rate Limiting	désactivé
Broadcast / Multicast Rate Limit	50 pps
Multicast traffic rate per radio	auto

Fonctionnalité	Paramètre
MAC Authentication Default Action	Autoriser
Load Balancing Mode	désactivé
802.1d Spanning tree mode on wired / WDS link	désactivé
Country or Band code for Radio such as FCC, ETSI etc.	Dépend de SKU
Channel Bandwidth	40 Mhz
Maximum associations supported	200
Antenna Selection, automatically selects best antenna	Auto
WMM APSD Power mode setting	Allumé
AP Detection for neighbor AP - both rogue and known APs	activé
For a multiple-radio AP, which radio this WDS link is using	Radio 1
Arbitration Inter Frame Spacing (AIFS)	4 files d'attente = 1 ms, 1 ms, 3 ms, 7 ms
Minimum contention window	4 files d'attente = 3 ms, 7 ms, 15 ms, 15 ms
Maximum Burst	4 files d'attente - 1,5 ms, 3 ms, 0 ms, 0 ms
Maximum contention window	4 files d'attente = 7 ms, 15 ms, 15 ms, 15 ms

Stockage

Fonctionnalité	Paramètre
VLAN - Data, IP Address Assignment (Management)	DHCP Client
VLAN - Data, IP Address (Failover when no DHCP Server Available)	Voir l'onglet Product
VLAN - Data, Subnet Mask (Failover when no DHCP Server Available)	255.255.255.0
Windows workgroup name	WORKGROUP
HTTP Access Administration	80
HTTP File Access	8080
FTP File Access	21
HTTPS Administration Access	443
Dual Link Mode (802.3ad Link Aggregation, Active Backup)	Sauvegarde active
Idle Drive Spin Down (1-8 hours, 1 day)	8 heures
Public access to share	Lecture seule
Idle Disconnect Timeout	5 minutes
Banner	Welcome to the Cisco Small Business FTP Server
Allow Anonymous Access	désactiver
Allow Anonymous File Upload	désactiver
Allow Anonymous File Download	activer
Maximum Anonymous Transfer Rate (0 - unlimited) in KB/s	0
Disconnect Idle Sessions	5 minutes

Fonctionnalité	Paramètre
Disconnect Stalled Sessions	5 minutes
Maximum Connections per IP Address	5
Default File Creation Attributes (Group Read/Write, Everyone Read/Write	activer
Enable users to delete and rename other's files and folders	activer

Paramètres de sécurité

Fonctionnalité	Paramètre
UpNP	Désactivée
Remote Management	Désactivée
CDP. Enabled on LAN, disabled on WAN	Désactivé sur le WAN
Firewall	Entrant : rejeter / sortant : autoriser
Respond to Ping on internet	Désactivée
Enable Stealth Mode	Activer
Block TCP Flood	Activer
Block UDP Flood	Activer
Block ICMP Notification	Activer
Block Fragmented Packets	Activer
Block Multicast Packets	Activer
SYN Flood Detect Rate	128 max/sec
Echo Storm (ping packets/sec)	15 paquets/sec

Fonctionnalité	Paramètre
ICMP Flood (ICMP packets/sec)	100 paquets/sec

E

Pour en savoir plus

Cisco propose une vaste gamme de ressources pour vous aider à tirer pleinement parti du périphériques de sécurité de la gamme SA500.

Ressources sur les produits

Prise en charge	
Communauté d'assistance Cisco Small Business	www.cisco.com/go/smallbizsupport
Assistance technique et documentation en ligne	www.cisco.com/support (Identifiants de connexion requis)
Ressources et assistance Cisco Small Business	www.cisco.com/go/smallbizhelp
Coordonnées de l'assistance téléphonique	www.cisco.com/go/sbsc
Logiciels	
Logiciel QuickVPN	www.cisco.com/go/qvpn
Cisco VPN Client	www.cisco.com/go/ciscovpnclient
Téléchargement de microprogrammes SA500	www.cisco.com/go/sa500software
Documentation sur les produits	
Documentation technique SA500	www.cisco.com/go/sa500resources
Cisco Small Business	
Partenaires et revendeurs Cisco pour les PME (identification partenaire obligatoire)	www.cisco.com/web/partners/sell/smb
Accueil Cisco Small Business	www.cisco.com/smb