

GUIDE D'ADMINISTRATION

Cisco RV215W Pare-feu VPN Wireless-N

Version révisée de novembre 2013

78-20779-02

Cisco et le logo Cisco sont des marques commerciales ou des marques commerciales déposées de Cisco Systems, Inc. et/ou de ses filiales aux États-Unis et dans d'autres pays. Pour consulter la liste des marques commerciales de Cisco, rendez-vous sur : **www.cisco.com/go/trademarks**. Les autres marques commerciales mentionnées sont la propriété de leurs détenteurs respectifs. L'utilisation du terme « partenaire » n'implique pas de relation de partenariat entre Cisco et une autre société. (1110R)

Table des matieres

Chapitre 1 : Introduction 9

Vérification de l'installation matérielle 9
Utilisation de l'Assistant de configurations 10
Étapes suivantes de la configuration 11
Utilisation de la page Prise en main 11
Enregistrement des modifications 13
Connexion au réseau sans fil 14

Chapitre 2 : Affichage de l'état du routeur 15

Affichage du tableau de bord 15
Affichage du récapitulatif de la configuration système 17
Affichage des statistiques sans fil 20
Affichage de l'état du VPN 21
Affichage de l'état des connexions IPSec 22
Affichage des journaux 23
Affichage des appareils connectés 24
Affichage des statistiques des ports 25
Affichage de l'état du réseau invité 26
Affichage de l'état du réseau mobile 26

Chapitre 3 : Configuration des paramètres réseau 28

Configuration des paramètres WAN 29
Configuration des connexions WAN filaires 29
Configuration de DHCP 29
Configuration d'une adresse IP statique 29
Configuration du protocole PPPoE 30
Configuration du protocole PPTP 31
Configuration du protocole L2TP 33
Configuration des paramètres facultatifs 34
Configuration d'un réseau mobile 35
Paramètres globaux 35
Configuration du réseau mobile 37

Paramètre de limite de bande passante 38
Paramètre d'e-mail 39
Configuration du basculement et de la récupération 39
Mise à jour du périphérique WAN/USB 41
Configuration des paramètres LAN 41
Modification de l'adresse IP de gestion de périphérique 42
Configuration du serveur DHCP 43
Configuration des VLAN 44
Configuration de DHCP statique 46
Affichage des baux de clients DHCP 47
Configuration d'un hôte de DMZ 47
Configuration de RSTP 48
Gestion des ports 50
Clonage de l'adresse MAC 51
Configuration du routage 52
Configuration du mode de fonctionnement 52
Configuration du routage dynamique 53
Configuration du routage statique 54
Affichage de la table de routage 55
Configuration du DNS dynamique 55
Configuration du mode IP 57
Configuration d'IPv6 58
Configuration de la connexion WAN IPV6 58
Configuration des connexions LAN IPv6 62
Configuration du routage IPv6 statique 64
Configuration du routage (RIPng) 65
Configuration du tunneling 66
Affichage de l'état du tunnel IPv6 67
Configuration de l'annonce du routeur 68
Configuration des préfixes d'annonce 70

Chapitre 4 : Configuration du réseau sans fil 71

Sécurité sans fil 71
Conseils relatifs à la sécurité des réseaux sans fil 71
Directives générales sur la sécurité réseau 73
Cisco RV215W - Réseaux sans fil 73
Configuration des paramètres sans fil de base 74
Modification des paramètres de réseau sans fil 76
Configuration du mode de sécurité 77
Configuration du filtrage MAC 80
Configuration de l'accès par horaire 81
Configuration du réseau invité sans fil 82
Configuration des paramètres sans fil avancés 84
Configuration de WDS 87
Configuration de WPS 88

Chapitre 5 : Configuration du pare-feu 89

Fonctions de pare-feu du routeur Cisco RV215W 89
Configuration des paramètres de base du pare-feu 91
Configuration de la gestion à distance 94
Configuration de la fonction Universal Plug and Play 95
Gestion des plannings de pare-feu 95
Ajout ou modification d'un planning de pare-feu 95
Configuration de la gestion de services 96
Configuration des règles d’accès 97
Ajout de règles d'accès 98
Création d'une stratégie d'accès à Internet 101
Ajout ou modification d'une stratégie d'accès à Internet 101
Configuration de la redirection de ports 103
Configuration de la redirection de port individuel 103
Configuration de la redirection d'une plage de ports 104
Configuration du déclenchement de plage de ports 105

Chapitre 6 : Configuration de VPN 107

Types de tunnels VPN 107
Clients VPN 108
Configuration du protocole PPTP 108
Configuration de QuickVPN 109
Configuration de NetBIOS sur VPN 109
Création et gestion des utilisateurs PPTP 110
Création et gestion des utilisateurs QuickVPN 110
Importation des paramètres client VPN 111
Configuration de paramètres VPN site-à-site de base 112
Affichage des valeurs par défaut 113
Configuration des paramètres VPN avancés 114
Gestion des stratégies IKE 114
Ajout ou modification de stratégies IKE 115
Gestion des stratégies VPN 117
Ajout ou modification de stratégies VPN 117
Configuration de la gestion des certificats 120
Configuration de l'intercommunication VPN 122

Chapitre 7 : Configuration de la Qualité de service (QoS) 123

Configuration de la gestion de la bande passante 123
Configuration de la bande passante 124
Configuration des priorités de bande passante 124
Configuration des paramètres de port QoS 126
Configuration des paramètres CoS 127
Configuration des paramètres DSCP 128

Chapitre 8 : Administration du routeur 129

Définition de la complexité des mots de passe 130
Configuration des comptes d'utilisateurs 131
Définition du délai d'expiration de session 132

Configuration SNMP (Simple Network Management Protocol) 132
Configuration des informations système SNMP 133
Modification des utilisateurs SNMPv3 133
Configuration des filtres SNMP 135
Utilisation des outils de diagnostic 135
Outils réseau 136
Configuration de la mise en miroir des ports 137
Configuration de la journalisation 138
Configuration des paramètres de journalisation 138
Configuration des paramètres d'e-mail 140
Configuration de Bonjour 142
Configuration des paramètres de date et d'heure 143
Sauvegarde et restauration du système 144
Sauvegarde des paramètres de configuration 145
Restauration des paramètres de configuration 146
Copie des paramètres de configuration 146
Génération d'une clé de cryptage 147
Mise à niveau du micrologiciel ou changement de la langue 147
Mise à niveau automatique du micrologiciel 148
Mise à niveau manuelle du micrologiciel 149
Changement de la langue 150
Redémarrage du Cisco RV215W 150
Restauration des paramètres d'usine 150
Exécution de l'Assistant de configurations 151

Annexe A : Utilisation de Cisco QuickVPN 152

Présentation 152
Avant de commencer 152

Installation du logiciel Cisco QuickVPN 153
Installation à partir du CD-ROM 153
Téléchargement et installation à partir d'Internet 155
Utilisation du logiciel Cisco QuickVPN 155

Annexe B : Pour en savoir plus 159

1

Introduction

Ce chapitre contient des informations destinées à vous guider tout au long du processus d'installation et à vous permettre de commencer à utiliser le Gestionnaire de périphérique basé sur navigateur.

- **Vérification de l'installation matérielle**
- **Utilisation de l'Assistant de configurations**
- **Utilisation de la page Prise en main**
- **Connexion au réseau sans fil**

Vérification de l'installation matérielle

Configurez le routeur à connecter aux réseaux filaire ou sans fil à l'aide du Guide de démarrage rapide du pare-feu VPN Wireless-N Cisco RV215W.



ATTENTION Utilisez la source d'alimentation de 12 V, 1,67 A fournie avec le périphérique. L'utilisation d'une autre source d'alimentation risque de dégrader les performances ou d'endommager l'appareil.

Pour vérifier l'installation matérielle et la connexion à Internet, procédez comme suit :

ÉTAPE1 Vérifiez l'état des voyants LED. Pour plus d'informations, reportez-vous au Guide de démarrage rapide du pare-feu VPN Wireless-N Cisco RV215W fourni avec le routeur.

ÉTAPE 2 Connectez un ordinateur à un port LAN libre et vérifiez que vous pouvez vous connecter à un site Web sur Internet, par exemple www.cisco.com.

ÉTAPE 3 Depuis un ordinateur équipé d'une fonctionnalité sans fil, connectez-vous à un site Web sur Internet (www.cisco.com, par exemple). Pour configurer votre radio, reportez-vous à la section **Connexion au réseau sans fil**.

Utilisation de l'Assistant de configurations

L'Assistant de configurations et le Gestionnaire de périphérique fonctionnent sur Microsoft Internet Explorer 6.0 ou version ultérieure, Mozilla Firefox 3.0 ou version ultérieure et Apple Safari 3.0 ou version ultérieure.

Pour utiliser l'Assistant de configurations :

ÉTAPE1 Démarrez l'ordinateur que vous avez connecté à un port LAN.

L'ordinateur prend le rôle de client DHCP de l'appareil et se voit attribuer une adresse IP située dans la plage 192.168.1.xxx.

ÉTAPE 2 Ouvrez une page Web et saisissez **192.168.1.1** dans la barre d'adresse. Il s'agit de l'adresse IP par défaut du périphérique.

Un message s'affiche concernant le certificat de sécurité du site. Le périphérique utilise un certificat de sécurité auto-signé et ce message s'affiche parce que l'ordinateur ne reconnaît pas le périphérique.

ÉTAPE 3 Cliquez sur **Poursuivre sur ce site Web** (ou l'option affichée sur votre navigateur Web spécifique) pour accéder au site Web. La page de connexion s'affiche.

ÉTAPE 4 Saisissez le nom d'utilisateur et le mot de passe.

Le nom d'utilisateur par défaut est **cisco**. Le mot de passe par défaut est **cisco**. Les mots de passe sont sensibles à la casse.

ÉTAPE 5 Cliquez sur **Connexion**. L'Assistant de configurations démarre.

ÉTAPE 6 Suivez les instructions affichées à l'écran pour configurer le périphérique.

L'Assistant de configurations tente de détecter et de configurer votre connexion. S'il n'y parvient pas, l'Assistant de configurations peut vous demander de fournir certaines informations sur votre connexion Internet. Vous pouvez être amené à contacter votre fournisseur d'accès à Internet (FAI) pour obtenir ces informations.

Lorsque l'Assistant de configurations a fini de configurer le périphérique, il vous demande de changer le mot de passe par défaut. Suivez les instructions affichées à l'écran. Après avoir changé le mot de passe par défaut, la page **Prise en main** s'affiche.

Étapes suivantes de la configuration

Bien que l'Assistant de configurations configure automatiquement le périphérique, nous vous conseillons de personnaliser certains des paramètres pour renforcer la sécurité et obtenir des performances optimales :

- Si vous avez déjà un serveur DHCP sur votre réseau et que vous ne souhaitez pas que le périphérique fasse office de serveur DHCP du réseau, désactivez le serveur. Reportez-vous à la section **Configuration des paramètres LAN**.
- Configurez votre réseau privé virtuel (VPN) à l'aide de QuickVPN. QuickVPN est fourni sur le CD distribué avec votre pare-feu. Reportez-vous à la section **Annexe A, ? Utilisation du logiciel Cisco QuickVPN ?**
- Bien que le périphérique prenne en charge jusqu'à quatre réseaux sans fil, vous ne pouvez configurer qu'un seul réseau sans fil (ou SSID) avec l'Assistant de configurations. Pour configurer d'autres réseaux sans fil avec le Gestionnaire de périphérique, reportez-vous à la section **Configuration du réseau sans fil**.

Utilisation de la page Prise en main

La page **Prise en main** affiche les tâches de configuration du périphérique les plus courantes. Utilisez les liens de cette page pour passer directement à la page de configuration pertinente.

Cette page s'affiche chaque fois que vous démarrez le Gestionnaire de périphérique. Pour modifier ce comportement, cochez la case **Ne pas afficher au démarrage**.

Paramètres d'origine

Modifier le mot de passe d'administrateur par défaut	Affiche la page **Utilisateurs**, où vous pouvez modifier le mot de passe administrateur et configurer un compte invité. Reportez-vous à la section **Configuration des comptes d'utilisateurs**.
Lancer l'Assistant de configurations	Lance l'Assistant de configurations. Suivez les instructions affichées à l'écran.

Configurer les paramètres WAN	Ouvre la page **Configuration Internet** qui permet de modifier les paramètres tels que le nom de l'hôte du routeur. Reportez-vous à la section **Configuration des paramètres WAN**.
Configurer les paramètres LAN	Ouvre la page **Configuration LAN** pour modifier les paramètres du réseau LAN, notamment l'adresse IP de gestion. Reportez-vous à la section **Configuration des paramètres LAN**.
Configurer les paramètres sans fil	Ouvrez la page **Paramètres de base** afin de gérer la radio. Reportez-vous à la section **Configuration du réseau sans fil**.

Accès rapide

Mettre à niveau le micrologiciel du routeur	Ouvrez la page **Mise à niveau du micrologiciel/de la langue** afin de mettre à jour le micrologiciel ou le module linguistique du routeur. Reportez-vous à la section **Mise à niveau du micrologiciel ou changement de la langue**.
Ajouter des clients VPN	Ouvre la page **Clients VPN** pour gérer les réseaux privés virtuels. Reportez-vous à la section **Clients VPN**.
Configurer l'accès pour la gestion à distance	Ouvre la page **Paramètres de base** afin d'activer les fonctionnalités de base du routeur. Reportez-vous à la section **Configuration des paramètres de base du pare-feu**.

État de l'appareil

Récapitulatif du système	Affiche la page **Récapitulatif du système** qui indique l'état du routeur. Reportez-vous à la section **Affichage du récapitulatif de la configuration système**.
État du réseau sans fil	Affiche la page **Statistiques sans fil** qui indique l'état de la radio. Reportez-vous à la section **Affichage des statistiques sans fil**.
État du VPN	Affiche la page **État du VPN** qui décrit le VPN géré par ce routeur. Reportez-vous à la section **Affichage de l'état du VPN**.

Autres ressources

Assistance	Cliquez sur ce lien pour ouvrir la page d'assistance Cisco.
Forums	Cliquez sur ce lien pour visiter les forums d'assistance en ligne de Cisco.

Enregistrement des modifications

Lorsque vous avez fini d'apporter des modifications dans une page de configuration, cliquez sur **Enregistrer** pour enregistrer les modifications dans la mémoire Flash ou cliquez sur **Annuler** pour annuler les modifications.

Connexion au réseau sans fil

Pour connecter un périphérique (tel qu'un ordinateur) à votre réseau sans fil, vous devez configurer la connexion sans fil sur le périphérique avec les informations de sécurité sans fil que vous avez configurées pour le périphérique à l'aide de l'Assistant de configurations.

Les étapes suivantes sont indiquées à titre d'exemple ; vous devrez peut-être configurer différemment votre périphérique client. Pour des instructions spécifiques à votre périphérique client, consultez la documentation du périphérique.

ÉTAPE1 Ouvrez la fenêtre ou le programme de paramétrage de la connexion sans fil de votre périphérique.

Votre ordinateur peut comporter un logiciel spécial pour gérer les connexions sans fil. Vous pouvez également afficher les connexions sans fil dans la fenêtre **Connexions réseau** ou **Réseau et Internet** du Panneau de configuration. (L'emplacement varie selon le système d'exploitation.)

ÉTAPE 2 Saisissez le nom (SSID) que vous avez attribué à votre réseau dans l'Assistant de configurations.

ÉTAPE 3 Choisissez le type de cryptage et saisissez la clé de sécurité que vous avez spécifiée dans l'Assistant de configurations.

Si vous n'avez pas activé la sécurité (déconseillé), ne renseignez pas les champs de cryptage sans fil configurés avec le type de sécurité et le mot de passe.

ÉTAPE 4 Vérifiez votre connexion sans fil et enregistrez vos paramètres.

2

Affichage de l'état du routeur

Ce chapitre indique comment consulter des statistiques en temps réel et d'autres informations sur le périphérique.

- **Affichage du tableau de bord**
- **Affichage du récapitulatif de la configuration système**
- **Affichage des statistiques sans fil**
- **Affichage de l'état du VPN**
- **Affichage des journaux**
- **Affichage des appareils connectés**
- **Affichage des statistiques des ports**

Affichage du tableau de bord

La page **Tableau de bord** affiche des informations importantes sur le routeur.

Pour afficher le tableau de bord, choisissez **État** > **Tableau de bord**.

Pour modifier la fréquence d'actualisation des valeurs de paramètre et des statistiques affichées, sélectionnez la fréquence dans le menu déroulant **Fréquence d'actualisation**.

Pour afficher une vue interactive du panneau arrière du routeur, cliquez sur **Afficher le panneau arrière du routeur**.

Le panneau arrière montre les ports qui sont connectés à un périphérique (voyant vert).

- Pour afficher les informations de connexion d'un port, survolez-le à l'aide du curseur de la souris.
- Pour actualiser les informations sur le port, cliquez sur **Actualiser**.
- Pour fermer la fenêtre d'informations sur le port, cliquez sur **Fermer**.

La page **Tableau de bord** affiche les éléments suivants :

Informations concernant l'appareil

- **Nom du système** : nom de l'appareil.
- **Version du micrologiciel** : version du micrologiciel actuellement exécuté par l'appareil.
- **Numéro de série** : numéro de série de l'appareil.

Utilisation des ressources

- **UC** : utilisation du processeur.
- **Mémoire** : utilisation de la mémoire.
- **Heure actuelle** : heure du jour.
- **Durée de disponibilité du système** : durée de fonctionnement du système.

Récapitulatif Syslog

Indique si la journalisation est activée pour ces catégories d'événement :

- **Urgence**
- **Alerte**
- **Critique**
- **Erreurs**
- **Avertissement**

Pour afficher les journaux, cliquez sur **détails**. Pour plus d'informations, reportez-vous à la section **Affichage des journaux**.

Pour gérer les journaux, cliquez sur **gérer la journalisation**. Pour plus d'informations, reportez-vous à la section **Configuration des paramètres de journalisation**.

Interface LAN (réseau local)

- **Adresse MAC** : adresse MAC du périphérique.
- **Adresse IPv4** : adresse IP de gestion de l'appareil.
- **Adresse IPv6** : adresse IP de gestion de l'appareil (si IPv6 est activé).
- **Serveur DHCP** : état du serveur DHCP IPv4 de l'appareil (activé ou désactivé).

- **Serveur DHCPv6** : état du serveur DHCP IPv6 du routeur (activé ou désactivé).

Pour afficher les paramètres LAN, cliquez sur **détails**. Pour plus d'informations, reportez-vous à la section **Configuration des paramètres LAN**.

Informations WAN (réseau mobile)

- **Adresse IPv4** : adresse IPv4 du port USB.
- **État** : état de la connexion WAN du réseau mobile (montante ou descendante).

Pour afficher les paramètres WAN, cliquez sur les détails. Pour plus d'informations, reportez-vous à la section **Configuration des connexions WAN filaires**.

Informations WAN (Internet)

- **Adresse IPv4** : adresse IPv4 du port WAN du routeur.
- **Adresse IPv6** : adresse IPv6 du port WAN du routeur, si IPv6 est activé.
- **État** : état de la connexion WAN filaire (montante ou descendante).

Pour afficher les paramètres WAN, cliquez sur **détails**. Pour plus d'informations, reportez-vous à la section **Configuration des connexions WAN filaires**.

Réseaux sans fil

Répertorie l'état des quatre SSID de réseau sans fil.

Pour afficher les paramètres sans fil du routeur, cliquez sur **détails**. Pour plus d'informations, reportez-vous à la section **Affichage des statistiques sans fil**.

VPN

Utilisateurs QuickVPN : nombre d'utilisateurs QuickVPN.

PPTP : nombre d'utilisateurs PPTP (Point-to-Point Tunneling Protocol).

Affichage du récapitulatif de la configuration système

La page **Récapitulatif du système** affiche un récapitulatif des valeurs de l'appareil, notamment la version du micrologiciel et le numéro de série.

Pour afficher un récapitulatif des paramètres système, sélectionnez **État** > **Récapitulatif du système**.

Pour accéder à la fenêtre associée, cliquez sur le paramètre souligné. Par exemple, pour modifier l'adresse IP du LAN, cliquez sur **IP du LAN**. La fenêtre de configuration du LAN s'affiche.

Cliquez sur **Actualiser** pour obtenir les informations les plus récentes.

La page **Récapitulatif du système** affiche les informations suivantes :

Informations système

- **Version du micrologiciel** : version actuelle du logiciel exécutée par l'appareil.
- **Somme de contrôle MD5 du micrologiciel** : algorithme Message-Digest utilisé pour vérifier l'intégrité des fichiers.
- **Paramètres régionaux** : langue installée sur le routeur.
- **Version de langue** : version du module linguistique installé. La version du module linguistique doit être compatible avec le micrologiciel actuellement installé. Dans certains cas, un module linguistique plus ancien peut être utilisé avec une image plus récente du micrologiciel. Le routeur vérifie la version du module linguistique pour voir si elle est compatible avec la version actuelle du micrologiciel.
- **Somme de contrôle MD5 de la langue** : somme de contrôle MD5 du module linguistique.
- **Modèle de processeur** : jeu de puces (chipset) du processeur actuellement utilisé.
- **Numéro de série** : numéro de série de l'appareil.
- **Durée de fonctionnement du système** : durée depuis laquelle le système fonctionne.
- **Heure actuelle** : heure du jour.
- **PID VID** : ID de produit et ID de version de l'appareil.

Configuration IPv4

- **IP du LAN** : adresse IP LAN du périphérique.
- **Adresse IP du WAN** : adresse IP WAN du périphérique. Vous pouvez libérer l'adresse IP actuelle et en obtenir une nouvelle en cliquant sur **Libérer** ou sur **Renouveler**.
- **Passerelle** : adresse IP de la passerelle à laquelle le périphérique est connecté (le modem câble, par exemple).

- **Mode** : affiche **Passerelle** si la fonctionnalité NAT est activée, sinon **Routeur**.
- **DNS 1** : adresse IP du serveur DNS principal du port WAN.
- **DNS 2** : adresse IP du serveur DNS secondaire du port WAN.
- **DDNS** : indique si DNS dynamique est activé ou désactivé.

Configuration IPv6

- **IP du LAN** : adresse IP LAN du périphérique.
- **Adresse IP du WAN** : adresse IP WAN du périphérique.
- **Passerelle** : adresse IP de la passerelle à laquelle le périphérique est connecté (le modem câble, par exemple).
- **NTP** : serveur NTP (Network Time Protocol) (nom d'hôte ou adresse IPv6).
- **Longueur du préfixe** : préfixe IPv6 transmis du périphérique au FAI et qui est attribué aux adresses IP sur le périphérique.
- **DNS 1** : adresse IP du serveur DNS principal.
- **DNS 2** : adresse IP du serveur DNS secondaire.

Récapitulatif du réseau sans fil

- **SSID 1** : nom public du premier réseau sans fil.
  - **Sécurité** : paramètre de sécurité pour SSID 1.
- **SSID 2** : nom public du second réseau sans fil.
  - **Sécurité** : paramètre de sécurité pour SSID 2.
- **SSID 3** : nom public du troisième réseau sans fil.
  - **Sécurité** : paramètre de sécurité pour SSID 3.
- **SSID 4** : nom public du quatrième réseau sans fil.
  - **Sécurité** : paramètre de sécurité pour SSID 4.

État des paramètres du pare-feu

- **DoS (Déni de service)** : indique si la prévention DoS est active ou non.
- **Bloquer la requête WAN** : indique si le blocage de la requête WAN est actif ou non.
- **Gestion à distance** : indique s'il est possible d'accéder au Gestionnaire de périphérique à distance.

État des paramètres VPN

- **Connexions QuickVPN disponibles** : nombre de connexions QuickVPN disponibles.
- **Connexions VPN PPTP disponibles** : nombre de connexions VPN PPTP disponibles.
- **Utilisateurs connectés au QuickVPN** : nombre d'utilisateurs connectés au QuickVPN.
- **Utilisateurs connectés au VPN PPTP** : nombre d'utilisateurs connectés au VPN PPTP.

Affichage des statistiques sans fil

La page **Statistiques sans fil** indique les statistiques relatives au réseau sans fil de la radio.

Pour afficher les statistiques relatives au réseau sans fil, choisissez **État** > **Statistiques sans fil**.

Pour modifier la fréquence d'actualisation, sélectionnez une valeur dans le menu déroulant **Fréquence d'actualisation**.

Pour afficher les octets en kilo-octets (Ko) et les données numériques sous forme de valeurs arrondies, cochez la case **Afficher les données statistiques simplifiées** et cliquez sur **Enregistrer**. Par défaut, les données d'octets sont affichées en octets et les autres données numériques sont exprimées sous forme développée.

Pour réinitialiser les compteurs de statistiques sans fil, cliquez sur **Réinitialiser les compteurs**. Les compteurs sont également réinitialisés au redémarrage de l'appareil.

La page **Statistiques sans fil** affiche les informations suivantes :

Nom SSID	Le nom du réseau sans fil.
Paquet	Nombre de paquets sans fil reçus et envoyés signalés à la radio sur tous les SSID configurés et actifs.
Octet	Nombre d'octets d'informations reçus et envoyés signalés à la radio sur tous les SSID configurés.
Erreurs	Nombre d'erreurs de paquets reçus et envoyés signalées à la radio sur tous les SSID configurés.
Abandonné	Nombre de paquets reçus et envoyés abandonnés par la radio sur tous les SSID configurés.
Multidiffusion	Nombre de paquets en multidiffusion envoyés sur cette radio.
Collisions	Nombre de collisions de paquets signalées au routeur.

Affichage de l'état du VPN

La page **VPN** affiche l'état des connexions VPN.

Pour voir l'état des connexions utilisateurs au VPN, sélectionnez **État** > **État du VPN**.

La page **VPN** affiche les informations suivantes :

Nom d'utilisateur	Nom de l'utilisateur VPN associé au tunnel QuickVPN PPTP.
IP distante	Affiche l'adresse IP du client QuickVPN distant. Il peut s'agir d'une IP NAT/publique si le client se trouve derrière le routeur NAT.
État	Affiche l'état actuel du client QuickVPN. HORS LIGNE signifie que le tunnel QuickVPN n'est pas initié ou établi par l'utilisateur VPN. EN LIGNE signifie que le tunnel QuickVPN initié ou établi par l'utilisateur VPN est actif.

Heure de début	Heure à laquelle l'utilisateur VPN a établi une connexion.
Heure de fin	Heure à laquelle l'utilisateur VPN a interrompu une connexion.
Durée (secondes)	Durée entre l'établissement et la fin d'une connexion par l'utilisateur VPN.
Protocole	Protocole sélectionné par l'utilisateur.

Vous pouvez modifier l'état d'une connexion pour établir ou déconnecter le client VPN configuré.

Pour mettre fin à une connexion VPN active, cliquez sur **Déconnexion**.

Affichage de l'état des connexions IPSec

L'état des connexions IPSec indique l'état des stratégies VPN actives sur le périphérique. (Ces stratégies sont configurées sur la page **VPN** > **Configuration VPN avancée**.) Pour afficher l'état des connexions IPSec :

ÉTAPE1 Sélectionnez **État** > **État de la connexion IPSec**. Le tableau contient les informations suivantes :

- **Fréquence d'actualisation** : choisissez la fréquence à laquelle vous souhaitez que l'affichage des données soit actualisé.
- **Afficher les données statistiques simplifiées** : par défaut, les données d'octets sont affichées en octets et les autres données numériques sont exprimées sous forme développée. Pour afficher les octets en kilo-octets (Ko) et les données numériques sous forme de valeurs arrondies, cochez la case **Afficher les données statistiques simplifiées**.
- **Nom de la stratégie** : nom de la stratégie VPN pour laquelle les données sont affichées.
- **Local ou Distant** : affiche les adresses IP locales et distantes.
- **Heure de début et Heure de fin** : affiche les heures de début et de fin des connexions IPSec.
- **Durée** : indique la durée d'activation de la connexion.

- **Paquet** : affiche les paquets reçus et transmis via la connexion.
- **Octet** : affiche les octets reçus et transmis via la connexion.
- **État** : affiche l'état de la connexion (par exemple, active ou non connectée).
- **Action** : affiche les actions que vous pouvez effectuer sur la connexion (par exemple, déconnecter).
- **Action ext.** : indique s'il est possible de basculer entre les connexions VPN principale et secondaire. Si la case **Activer la restauration** sur la page **Advanced VPN Parameters** est cochée, le bouton **Commutateur** est estompé.

ÉTAPE 2 Si vous avez effectué des modifications, cliquez sur **Enregistrer**.

Affichage des journaux

La page **Afficher les journaux** affiche les journaux du périphérique.

Pour consulter les journaux, choisissez **État** > **Afficher les journaux**.

Pour afficher les entrées de journal les plus récentes, cliquez sur **Actualiser les journaux**.

Pour filtrer les journaux ou spécifier la gravité des journaux à afficher, cochez les cases en regard du type de journal correspondant et cliquez sur **OK**. Notez que tous les types de journaux au-delà d'un type sélectionné sont automatiquement inclus et qu'il n'est pas possible de les désélectionner. Par exemple, le fait de choisir les journaux d'erreurs inclut automatiquement les journaux d'urgence, d'alerte et critiques, en plus des journaux d'erreurs.

Les niveaux de sévérité des événements sont répertoriés du niveau le plus élevé au plus bas, comme suit :

- **Urgence** : le système n'est pas utilisable.
- **Alerte** : une action est requise.
- **Critique** : le système est dans un état critique.
- **Erreur** : le système subit une condition d'erreur.
- **Avertissement** : un avertissement système a été généré.

- **Notification** : le système fonctionne correctement, mais une notification système a été générée.
- **Information** : informations concernent l'appareil.
- **Débogage** : fournit des informations détaillées sur un événement.

Pour supprimer toutes les entrées de la fenêtre des journaux, cliquez sur **Effacer les journaux**.

Pour enregistrer tous les messages de journal du pare-feu sur le disque dur local, cliquez sur **Enregistrer les journaux**.

Pour enregistrer les messages du journal sur un lecteur USB externe, cliquez sur **Enregistrer le journal sur USB**.

Pour spécifier le nombre d'entrées à afficher par page, sélectionnez un nombre dans le menu déroulant.

Utilisez les boutons de navigation pour parcourir les pages des journaux.

Affichage des appareils connectés

La page **Appareils connectés** affiche des informations sur les appareils actifs connectés au périphérique.

La table ARP IPv4 affiche des informations émanant d'appareils qui ont répondu à la demande ARP (Address Resolution Protocol, protocole de résolution d'adresse) du périphérique. Si un appareil ne répond pas à la demande, il est supprimé de la liste.

La table NDP IPv6 affiche tous les appareils NDP (Neighbor Discover Protocol) IPv6 connectés à la liaison locale du périphérique.

Pour afficher les appareils connectés, choisissez **État** > **Appareils connectés**.

Pour spécifier les types d'interfaces à afficher, sélectionnez une valeur dans le menu déroulant **Filtre**.

Tous : tous les appareils connectés au routeur.

Sans fil : tous les appareils connectés à l'interface sans fil.

Filaire : tous les appareils connectés via les ports Ethernet sur le routeur.

WDS : tous les appareils WDS (système de distribution sans fil) connectés au routeur.

Affichage des statistiques des ports

La page **Statistiques des ports** affiche l'activité détaillée des ports.

Pour afficher les statistiques relatives aux ports, choisissez **État** > **Statistiques des ports**.

Pour recharger les statistiques du routeur et actualiser la page, sélectionnez une fréquence dans le menu déroulant **Fréquence d'actualisation**.

Pour afficher les octets en kilo-octets (Ko) et les données numériques sous forme de valeurs arrondies, cochez la case **Afficher les données statistiques simplifiées** et cliquez sur **Enregistrer**. Par défaut, les données d'octets sont affichées en octets et les autres données numériques sont exprimées sous forme développée.

Pour réinitialiser les compteurs de statistiques des ports, cliquez sur **Réinitialiser les compteurs**.

La page **Statistiques des ports** affiche les informations suivantes :

Interface	Nom de l'interface réseau.
Paquet	Nombre de paquets reçus/envoyés.
Octet	Nombre d'octets d'informations reçus/envoyés par seconde.
Erreurs	Nombre d'erreurs de paquets reçus/envoyés.
Abandonné	Nombre de paquets reçus/envoyés abandonnés.
Multidiffusion	Nombre de paquets en multidiffusion envoyés sur cette radio.
Collisions	Nombre de collisions de signal survenues sur ce port. Une collision survient lorsque le port essaie d'envoyer des données en même temps qu'un port sur un autre routeur ou ordinateur connecté à ce port.

Affichage de l'état du réseau invité

Les statistiques du réseau invité fournissent des informations sur le réseau invité sans fil configuré sur le périphérique.

Pour voir l'état du réseau invité, sélectionnez **État** > **État du réseau invité**. Les informations suivantes sont indiquées :

- **Nom d'hôte** : périphérique connecté au réseau invité.
- **Adresse IP** : adresse IP attribuée au périphérique connecté.
- **Adresse MAC** : adresse MAC ou matérielle du périphérique connecté.
- **Temps restant** : temps de connexion restant du périphérique au réseau invité. (Les limites de temps sont configurées dans la page **Sans fil** > **Paramètres de base** > **Paramètres du réseau invité**.)
- **Action** : actions que vous pouvez effectuer sur le périphérique connecté (par exemple, déconnecter).

Affichage de l'état du réseau mobile

Statistiques relatives au réseau mobile 3G/4G et à l'appareil de communication (dongle) configuré sur le périphérique.

Pour voir l'état du réseau mobile, sélectionnez **État** > **Réseau mobile**. Les informations suivantes sont indiquées :

- **Connexion** : périphérique connecté au réseau invité.
- **Adresse IP Internet** : adresse IP attribuée au périphérique USB.
- **Masque de sous-réseau** : masque de sous-réseau du périphérique USB.
- **Passerelle par défaut** : adresse IP de la passerelle par défaut.
- **Temps de disponibilité de la connexion** : durée de fonctionnement de la liaison.
- **Utilisation de la session actuelle** : volume des données reçues et transmises via la liaison mobile.
- **Fabricant** : nom du fabricant de la carte.
- **Modèle de carte** : numéro du modèle de la carte.

- **Micrologiciel de la carte** : version du micrologiciel de la carte.
- **État de la carte SIM** : état du module SIM.
- **IMS** : identification unique associée aux utilisateurs de téléphone mobile des réseaux GSM, UMTS ou LTE.
- **Porteuse** : porteuse du réseau mobile.
- **Type de service** : type de service auquel vous accédez.
- **Force du signal** : intensité du signal du réseau mobile sans fil.

3

Configuration des paramètres réseau

Ce chapitre indique la marche à suivre pour configurer les paramètres réseau du périphérique.

- **Configuration des paramètres WAN**
- **Configuration des paramètres LAN**
- **Clonage de l'adresse MAC**
- **Configuration du routage**
- **Gestion des ports**
- **Configuration du DNS dynamique**
- **Configuration du mode IP**
- **Configuration d'IPv6**

Configuration des paramètres WAN

Il est possible d'établir une connexion Internet via le port WAN ou un modem sans fil installé sur le port USB. Cette section décrit la configuration du réseau WAN, du réseau mobile, ainsi que les procédures de basculement et de récupération.

Configuration des connexions WAN filaires

La configuration des propriétés WAN d'un réseau IPv4 dépend du type de connexion Internet que vous utilisez.

Configuration de DHCP

Si votre fournisseur d'accès à Internet (FAI) utilise le protocole DHCP (Dynamic Host Control Protocol) pour vous affecter une adresse IP, vous recevrez une adresse IP générée de façon dynamique à chaque fois que vous vous connectez.

Pour configurer les paramètres WAN DHCP :

ÉTAPE 1 Sélectionnez **Mise en réseau** > **WAN**.

ÉTAPE 2 Dans le menu déroulant **Type de connexion Internet**, sélectionnez **Configuration automatique - DHCP**.

ÉTAPE 3 Cliquez sur **Enregistrer**.

Configuration d'une adresse IP statique

Si votre FAI vous a affecté une adresse IP permanente, effectuez les opérations suivantes pour configurer vos paramètres WAN :

ÉTAPE 1 Sélectionnez **Mise en réseau** > **WAN**.

ÉTAPE 2 Dans le menu déroulant **Type de connexion Internet**, sélectionnez **Adresse IP statique**.

ÉTAPE 3 Saisissez les informations suivantes :

Adresse IP Internet	Adresse IP du port WAN du pare-feu.
Masque de sous-réseau	Masque de sous-réseau du port WAN du pare-feu.

Passerelle par défaut	Adresse IP de la passerelle par défaut.
DNS statique 1	Adresse IP du serveur DNS principal.
DNS statique 2	Adresse IP du serveur DNS secondaire.

ÉTAPE 4 Cliquez sur **Enregistrer**.

Configuration du protocole PPPoE

Pour configurer les paramètres du protocole PPPoE (Point-to-Point Protocol over Ethernet) :

ÉTAPE 1 Sélectionnez **Mise en réseau** > **WAN**.

ÉTAPE 2 Dans le menu déroulant **Type de connexion Internet**, sélectionnez **PPPoE**.

ÉTAPE 3 Saisissez les informations suivantes (contactez le cas échéant votre FAI pour obtenir les informations de connexion PPPoE) :

Nom d'utilisateur	Nom d'utilisateur attribué par le FAI.
Mot de passe	Mot de passe attribué par le FAI.
Connexion à la demande	Sélectionnez cette option si votre FAI vous facture en fonction de la durée de connexion. Lorsque vous sélectionnez cette option, la connexion Internet n'est activée qu'en cas de présence de trafic. Si la connexion est en attente (sans trafic en transit), la connexion est fermée. Si vous cochez **Connexion à la demande**, entrez le délai (en minutes) avant déconnexion dans le champ **Durée d'inactivité max**.
Garder actif	Lorsque vous cochez cette option, la connexion Internet est toujours active. Dans le champ de délai de renumérotation, spécifiez le délai (en secondes) avant que le périphérique ne tente de se reconnecter après déconnexion.

Type d'authentification	**Négociation automatique** : le serveur envoie une demande de configuration spécifiant l'algorithme de sécurité paramétré. Le routeur périphérique renvoie alors les identifiants d'authentification avec le type de sécurité envoyé par le serveur. **PAP** : protocole PAP (Password Authentication Protocol) utilisé par le protocole PPTP lors de la connexion au FAI. **CHAP** : le protocole CHAP (Challenge Handshake Authentication Protocol) demande à ce qu'à la fois le client et le serveur connaissent le texte clair du secret pour pouvoir utiliser les services du FAI. **MS-CHAP ou MS-CHAPv2** : version Microsoft de CHAP, utilisée pour accéder aux services du FAI.

ÉTAPE 4 Cliquez sur **Enregistrer**.

Configuration du protocole PPTP

Pour configurer les paramètres PPTP :

ÉTAPE 1 Sélectionnez **Mise en réseau** > **WAN**.

ÉTAPE 2 Dans le menu déroulant **Type de connexion Internet**, sélectionnez **PPTP**.

ÉTAPE 3 Saisissez les informations suivantes :

Adresse IP Internet	Adresse IP du port WAN.
Masque de sous-réseau	Masque de sous-réseau du port WAN.
Passerelle par défaut	Adresse IP de la passerelle par défaut.
Serveur PPTP	Adresse IP du serveur PPTP (Point-To-Point Tunneling Protocol).
Nom d'utilisateur	Nom d'utilisateur qui vous est attribué par le FAI.
Mot de passe	Mot de passe qui vous est attribué par le FAI.

Connexion à la demande	Sélectionnez cette option si votre FAI vous facture en fonction de la durée de connexion. Lorsque vous sélectionnez cette option, la connexion Internet n'est activée qu'en cas de présence de trafic. Si la connexion est en attente (sans trafic en transit), la connexion est fermée. Si vous cochez **Connexion à la demande**, entrez le délai (en minutes) avant déconnexion dans le champ **Durée d'inactivité max**.
Garder actif	Lorsque vous cochez cette option, la connexion Internet est toujours active. Dans le champ de délai de renumérotation, spécifiez le délai (en secondes) avant que le périphérique ne tente de se reconnecter après déconnexion.
Type d'authentification	Sélectionnez le type d'authentification : **Négociation automatique** : le serveur envoie une demande de configuration spécifiant l'algorithme de sécurité paramétré. Le routeur périphérique renvoie alors les identifiants d'authentification en utilisant le type de sécurité envoyé précédemment par le serveur. **PAP** : le périphérique utilise le protocole PAP (Password Authentication Protocol) lors de la connexion au FAI. **CHAP** : le périphérique utilise le protocole CHAP (Challenge Handshake Authentication Protocol) lors de la connexion au FAI. **MS-CHAP ou MS-CHAPv2** : le périphérique utilise le protocole Microsoft Challenge Handshake Authentication Protocol lors de la connexion au FAI.

ÉTAPE 4 (Facultatif) Pour configurer les paramètres facultatifs, voir la section **Configuration des paramètres facultatifs**.

ÉTAPE 5 Cliquez sur **Enregistrer**.

Configuration du protocole L2TP

Pour configurer les paramètres L2TP :

ÉTAPE 1 Sélectionnez **Mise en réseau** > **WAN**.

ÉTAPE 2 Dans le menu déroulant **Type de connexion Internet**, sélectionnez **L2TP**.

ÉTAPE 3 Saisissez les informations suivantes :

Adresse IP Internet	Entrez l'adresse IP du port WAN.
Masque de sous-réseau	Entrez le masque de sous-réseau du port WAN.
Passerelle par défaut	Entrez l'adresse IP de la passerelle par défaut.
Serveur L2TP	Entrez l'adresse IP du serveur L2TP.
Nom d'utilisateur	Entrez le nom d'utilisateur fourni par le FAI.
Mot de passe	Entrez le mot de passe fourni par le FAI.
Connexion à la demande	Sélectionnez cette option si votre FAI vous facture en fonction de la durée de connexion. Lorsque vous sélectionnez cette option, la connexion Internet n'est activée qu'en cas de présence de trafic. Si la connexion est en attente (sans trafic en transit), la connexion est fermée. Si vous cochez **Connexion à la demande**, entrez le délai (en minutes) avant déconnexion dans le champ **Durée d'inactivité max**.
Garder actif	Lorsque vous cochez cette option, la connexion Internet est toujours active. Dans le champ de délai de renumérotation, spécifiez le délai (en secondes) avant que le périphérique ne tente de se reconnecter après déconnexion.

Type d'authentification	**Négociation automatique** : le serveur envoie une demande de configuration spécifiant l'algorithme de sécurité paramétré. Le routeur périphérique renvoie alors les identifiants d'authentification avec le type de sécurité envoyé par le serveur. **PAP** : protocole PAP (Password Authentication Protocol) utilisé lors de la connexion au FAI. **CHAP** : protocole CHAP (Challenge Handshake Authentication Protocol) utilisé pour la connexion au FAI. **MS-CHAP ou MS-CHAPv2** : protocole Microsoft Challenge Handshake Authentication Protocol utilisé lors de la connexion au FAI.

ÉTAPE 4 Cliquez sur **Enregistrer**.

Configuration des paramètres facultatifs

Pour configurer les paramètres facultatifs :

ÉTAPE 1 Dans la section **Paramètres facultatifs**, configurez les paramètres suivants :

Nom d'hôte	Nom d'hôte du périphérique.
Nom de domaine	Nom de domaine de votre réseau.

MTU	Le MTU (Maximum Transmission Unit) correspond à la taille maximale de paquet pouvant être transmis sur le réseau. La valeur de MTU standard sur les réseaux Ethernet est généralement de 1500 octets. Pour les connexions PPPoE, la valeur est de 1492 octets. À moins que votre FAI impose une modification, nous vous conseillons la sélection de l'option **Automatique**. Par défaut, la taille de MTU est de 1500 octets. Si votre FAI exige un réglage de MTU personnalisé, sélectionnez **Manuel** et modifiez la taille de MTU.
Taille	Taille MTU.

ÉTAPE 2 Cliquez sur **Enregistrer**.

Configuration d'un réseau mobile

Utilisez la page Réseau mobile pour configurer le périphérique en vue de sa connexion à un modem USB mobile à large bande connecté à son interface USB.

Pour afficher la fenêtre **Réseau mobile**, choisissez **Mise en réseau** > **WAN** > **Réseau mobile**.

Paramètres globaux

Pour installer un modem USB :

ÉTAPE 1 Connectez le modem USB. Si le modem est pris en charge, il est détecté automatiquement et apparaît sur la page Réseau mobile.

ÉTAPE 2 Sélectionnez le mode de connexion **automatique** ou **manuel**. La récupération de la connexion Ethernet fonctionne uniquement si Mode de connexion est défini sur Automatique.

- Pour permettre à votre modem d'établir une connexion automatiquement, sélectionnez le mode **Automatique**. Si vous sélectionnez Automatique, vous devez également définir une durée pour Connexion à la demande ou choisir Garder actif. L'option Connexion à la demande met fin à la connexion Internet après la durée d'inactivité spécifiée (Durée d'inactivité max.).

  Si votre connexion Internet est interrompue après une période d'inactivité, le modem établit automatiquement une nouvelle connexion lorsqu'un utilisateur tente de se connecter à Internet. Dans le champ **Durée d'inactivité max.**, entrez le nombre de minutes d'inactivité pouvant s'écouler avant que votre connexion Internet ne soit interrompue. Si vous choisissez **Garder actif** la connexion est maintenue en permanence.

- Pour connecter ou déconnecter votre connexion modem manuellement, sélectionnez le mode **Manuel**.

L'appareil affiche l'état actuel de la connexion modem, à savoir Initialisation en cours, Connexion, Déconnexion en cours ou Déconnecté.

ÉTAPE 3 Vérifiez que le champ **État de la carte** indique **Connecté** pour votre carte mobile.

Ces messages peuvent également s'afficher :

- Définissez le nom du point d'accès (APN) manuellement (car l'appareil n'est pas en mesure de le déterminer)
- Recherche du service en cours...
- Absence de carte SIM
- SIM verrouillée
- SIM occupée
- SIM prête
- Code PIN obligatoire
- Erreur de code PIN
- La carte est verrouillée
- La carte n'est pas activée
- Erreur d'initialisation de la carte
- erreur

Configuration du réseau mobile

S'il est nécessaire de modifier l'un des paramètres du réseau mobile dans la zone **Configuration du réseau mobile**, cliquez sur la case d'option **Manuel** dans le champ Mode de configuration. L'appareil détecte automatiquement les modems pris en charge et dresse la liste des paramètres de configuration appropriés. Le code PIN de la carte SIM peut être défini en mode Automatique ou Manuel.

Le Modèle de carte indique le modèle du modem sur le port USB. Les cartes non prises en charge sont signalées comme étant **non reconnues**.

Pour modifier d'autres paramètres, sélectionnez **Manuel** et renseignez les champs suivants :

Champ	Description
Nom du point d'accès (APN)	Réseau Internet auquel l'appareil mobile a établi une connexion. Entrez le nom du point d'accès spécifié par votre prestataire de services de réseau mobile. Si vous ne connaissez pas le nom du point d'accès, contactez votre prestataire de services.
Composer un numéro	Composez le numéro fourni par votre prestataire de services de réseau mobile pour accéder à Internet.
Nom d'utilisateur Mot de passe	Nom d'utilisateur et mot de passe spécifiés par votre prestataire de services de réseau mobile.
Contrôle SIM	Activer ou désactiver la vérification de la carte SIM.
Code PIN de la carte SIM	Code PIN associé à votre carte SIM. Ce champ s'affiche uniquement pour les cartes SIM GSM.
Nom du serveur	Nom du serveur pour la connexion à Internet (s'il est fourni par votre prestataire de services).
Authentification	Authentification utilisée par votre prestataire de services. Cette valeur peut être changée en sélectionnant le type d'authentification dans la liste déroulante. La valeur par défaut est Automatique. Si vous ne connaissez pas le type d'authentification à utiliser, sélectionnez Automatique.

Champ	Description
Type de service	Type de connexion de service de données mobile le plus communément disponible en fonction du signal du service de votre zone. Si votre emplacement prend en charge un seul service de données mobile, vous pouvez limiter l'option de votre choix, en réduisant les durées de configuration de connexion. La première sélection recherche toujours le service HSPDA/3G/UMTS, puis bascule automatiquement vers GPRS, si cette option est disponible.
Service LTE	Paramètre de service LTE (Long-term Evolution). Sélectionnez **Automatique** pour un signal basé sur le signal du service de la zone. Sélectionnez **4G uniquement** pour les signaux 4G. Sélectionnez **3G uniquement** pour les signaux 3G.

ÉTAPE 4 Cliquez sur **Enregistrer** pour enregistrer vos paramètres

Paramètre de limite de bande passante

Le routeur surveille l'activité des données sur la liaison du réseau mobile et lorsqu'il atteint un seuil donné, il envoie une notification.

Pour activer ou désactiver Suivi de la limite de bande passante et définir des limites :

ÉTAPE 1 Cliquez sur **Activé** ou **Désactivé**.

ÉTAPE 2 Sélectionnez **Date de renouvellement mensuel** dans la liste déroulante afin d'indiquer le jour du mois auquel la limite de bande passante est réinitialisée.

ÉTAPE 3 Dans le champ **Limite mensuelle de bande passante**, entrez la quantité maximale de données, en méga-octets, pouvant être transmise avant que le routeur ne réagisse, en envoyant, par exemple, un courrier électronique à un administrateur.

Paramètre d'e-mail

Lorsque la limite de données de bande passante est atteinte, un message électronique peut être envoyé à l'administrateur. Pour configurer l'adresse électronique de destination, cochez la case **Envoyer par e-mail à** et cliquez sur **Adresse e-mail**. Pour plus d'informations, reportez-vous à la section **Configuration des paramètres d'e-mail**.

Lorsque cette case à cocher est activée, un courrier électronique est envoyé dans les cas suivants :

- L'utilisation du réseau mobile a dépassé un pourcentage donné.
- Le périphérique bascule sur le mode de secours et une récupération a lieu.
- À chaque intervalle spécifié lorsqu'une liaison du réseau mobile est active.

Configuration du basculement et de la récupération

Si des connexions Ethernet et de liaison du réseau mobile sont disponibles, une seule connexion peut être utilisée à la fois pour établir une liaison WAN. Lorsqu'une connexion WAN échoue, le routeur essaie d'établir une autre connexion sur une autre interface. Cette fonctionnalité est connue sous le nom de basculement. Lorsque la connexion WAN principale est restaurée, la connexion secondaire est abandonnée. Cette fonctionnalité est connue sous le nom de récupération.

ÉTAPE 1 Choisissez **Mise en réseau > WAN > Basculement et récupération**.

ÉTAPE 2 Choisissez votre connexion réseau principale, à savoir une connexion WAN Ethernet ou une connexion réseau mobile utilisant un dongle USB 3G.

ÉTAPE 3 Cliquez sur la case d'option **Basculement sur l'interface secondaire** pour que le routeur bascule de la connexion réseau principale à la connexion secondaire pour restaurer la connectivité.

Par exemple, votre connexion principale est une connexion WAN Ethernet et la liaison WAN est interrompue. Le routeur tente de restaurer la connexion avec une liaison du réseau mobile 3G sur l'interface USB. Si la case d'option **Basculement sur l'interface secondaire** n'est pas activée, la connexion secondaire est désactivée.

ÉTAPE 4 Cliquez sur la case d'option **Récupération sur la connexion principale** pour que le routeur rétablisse automatiquement la connexion principale et abandonne la connexion secondaire. Le mode de connexion **WAN > Réseau mobile** doit être défini sur Automatique pour que la connexion principale soit automatiquement rétablie.

ÉTAPE 5 Dans le champ **Intervalle de vérification du basculement**, indiquez le délai (en secondes) après lequel le routeur doit tenter de détecter la présence de trafic sur la connexion secondaire.

ÉTAPE 6 Dans le champ **Intervalle de vérification de la récupération**, indiquez le délai (en secondes) après lequel le routeur doit tenter de détecter la présence de trafic sur la connexion principale. Si la liaison est inactive, le routeur envoie une commande ping à une destination selon cet intervalle. En cas de réponse au paquet ping, le routeur suppose que la liaison est active et tente de rétablir la connexion réseau principale.

ÉTAPE 7 Cliquez sur la case d'option **Revenir à Ethernet immédiatement lorsque ce mode est disponible** ou définissez une durée dans le champ **Revenir à Ethernet dans une plage horaire spécifique**. Si vous choisissez une plage horaire spécifique, définissez les heures de début et de fin.

ÉTAPE 8 Dans le champ **Ping de récupération**, indiquez le nombre de fois que le routeur doit envoyer une commande ping au site de validation de la connexion après la récupération de la connectivité. Vous pouvez spécifier l'envoi de 5 pings au site. Par défaut, le routeur envoie une commande ping au site de validation une seule fois.

ÉTAPE 9 Dans le champ **Site de validation de la connexion**, choisissez le site auquel envoyer une commande ping au cours du basculement et de la validation de la récupération. Vous pouvez choisir la passerelle du routeur, un DNS ou une adresse IP personnalisée valide comme site de validation. Si vous choisissez une adresse de site personnalisée, entrez l'adresse IPv4 ou IPv6 du site. Par défaut, le routeur envoie une commande ping à la passerelle par défaut pour valider le basculement.

ÉTAPE 10 Pour dépanner la connexion réseau mobile 3G, cliquez sur la case d'option **Diagnostic 3G**. Indiquez l'heure à laquelle le routeur doit tester la connexion 3G chaque jour.

ÉTAPE 11 Cliquez sur **Enregistrer**.

Le tableau d'interface WAN montre l'état de la liaison Ethernet WAN et de la liaison du réseau mobile sur Internet. Cliquez sur le lien hypertexte **État** pour afficher les informations relatives au port.

Mise à jour du périphérique WAN/USB

Cette page vous indique la marche à suivre pour charger les fichiers de module USB qui prennent en charge les dongles USB. Contactez l'assistance Cisco pour vous procurer les fichiers de module USB. La liste des modems USB à chargement dynamique montre les fichiers de module de dongle USB 3G et 4G pris en charge sur le routeur.

Pour supprimer un fichier de module, sélectionnez le module dans la liste des modems USB à chargement dynamique et cliquez sur **Supprimer**.

Pour télécharger le micrologiciel (module) d'un dongle USB depuis le PC :

ÉTAPE 1 Vérifiez que le dongle USB n'est pas connecté au routeur.

ÉTAPE 2 Recherchez et sélectionnez le fichier du module du dongle USB.

ÉTAPE 3 Cliquez sur **Importer**.

ÉTAPE 4 Connectez le dongle USB au routeur.

Configuration des paramètres LAN

Les paramètres DHCP et TCP/IP par défaut sont adaptés à la plupart des applications. Si vous souhaitez qu'un autre ordinateur de votre réseau soit le serveur DHCP, ou si vous souhaitez configurer manuellement les paramètres réseau de tous vos périphériques, désactivez DHCP.

Par ailleurs, au lieu d'utiliser un serveur DNS, qui associe les noms de domaines Internet (comme www.cisco.com) à des adresses IP, vous pouvez utiliser un serveur WINS (Windows Internet Naming Service). Un serveur WINS est similaire à un serveur DNS, mais utilise le protocole NetBIOS pour résoudre les noms d'hôte. Le périphérique inclut l'adresse IP du serveur WINS dans la configuration DHCP que le périphérique envoie aux clients DHCP.

Si le périphérique est connecté à un modem ou appareil disposant d'un réseau configuré sur le même sous-réseau (192.168.1.x), le périphérique modifie automatiquement le sous-réseau du LAN en choisissant une valeur aléatoire basée sur 10.x.x.x, afin d'éviter tout conflit de sous-réseau du côté WAN du périphérique.

Modification de l’adresse IP de gestion de périphérique

L'adresse IP de gestion de périphérique local du périphérique est statique ; il s'agit de 192.168.1.1 par défaut.

Pour modifier l’adresse IP de gestion de périphérique local :

ÉTAPE 1 Sélectionnez **Mise en réseau** > **LAN** > **Configuration LAN**.

ÉTAPE 2 Dans la section **IPv4**, saisissez les informations suivantes :

VLAN	Numéro du réseau VLAN.
Adresse IP locale	Adresse IP LAN locale de périphérique. Assurez-vous que cette adresse IP n'est pas utilisée par un autre appareil.
Masque de sous-réseau	Masque de sous-réseau de l'adresse IP locale. La valeur du masque de sous-réseau par défaut est 255.255.255.0.

ÉTAPE 3 Cliquez sur **Enregistrer**.

Lorsque vous modifiez l'adresse IP du périphérique, votre PC n'est plus en mesure d'afficher le Gestionnaire de périphérique.

Pour afficher le Gestionnaire de périphérique, effectuez l'une des opérations suivantes :

- Si le périphérique est configuré en DHCP, libérez et renouvelez l'adresse IP de votre PC.
- Affectez manuellement une adresse IP à votre PC. L'adresse doit appartenir au même sous-réseau que le périphérique. Par exemple, si vous définissez l'adresse IP du périphérique sur 10.0.0.1, affectez à votre PC une adresse IP appartenant à la plage 10.0.0.2 à 10.0.0.255.

Ouvrez une fenêtre de navigateur et entrez la nouvelle adresse IP du périphérique pour vous reconnecter.

Configuration du serveur DHCP

Par défaut, le périphérique tient lieu de serveur DHCP pour les hôtes du réseau LAN sans fil (WLAN) ou du LAN filaire. Il attribue les adresses IP et fournit les adresses du serveur DNS.

Lorsque DHCP est activé, le périphérique affecte des adresses IP aux périphériques réseau sur le LAN à partir d'un groupe d'adresses IPv4. Le périphérique teste chaque adresse avant de l'affecter, afin d'éviter la duplication d'adresses sur le LAN.

Le groupe d'adresses IP par défaut va de 192.168.1.100 à 192.168.1.149. Pour définir une adresse IP statique sur un périphérique réseau, utilisez une adresse IP ne faisant pas partie du groupe. Par exemple, si le groupe DHCP utilise les paramètres par défaut, il est possible d'utiliser les adresses IP statiques allant de 192.168.1.2 à 192.168.1.99. Vous évitez ainsi les conflits avec le groupe d'adresses IP DHCP.

Pour configurer les paramètres DHCP :

ÉTAPE 1 Sélectionnez **Mise en réseau** > **LAN** > **Configuration LAN**.

ÉTAPE 2 (Facultatif) Sélectionnez un VLAN à modifier dans la liste déroulante.

ÉTAPE 3 Dans le champ **Serveur DHCP**, sélectionnez l'une des options suivantes :

Activer	Permet au périphérique de faire office de serveur DHCP sur le réseau.
Désactiver	Désactive DHCP sur le périphérique lorsque vous souhaitez configurer manuellement les adresses IP de l'ensemble de vos périphériques réseau.
Relais DHCP	Relaie les adresses IP attribuées par un autre serveur DHCP vers les périphériques réseau.

Si vous avez activé le serveur DHCP du périphérique, précisez les informations suivantes :

Adresse IP de début	Première adresse du groupe d'adresses IP. Une adresse IP de cette plage est attribuée à chaque client DHCP rejoignant le LAN.

Nombre maximal d'utilisateurs DHCP	Nombre maximal de clients DHCP.
Plage d'adresses IP	(Lecture seule) Plage des adresses IP disponibles pour les clients DHCP.
Durée de bail du client	Durée (en heures) des baux des adresses IP affectés aux clients.
DNS statique 1	Adresse IP du serveur DNS principal.
DNS statique 2	Adresse IP du serveur DNS secondaire.
DNS statique 3	Adresse IP du serveur DNS tertiaire.
WINS	Adresse IP du serveur WINS principal.

ÉTAPE 4 Si vous avez sélectionné **Relais DHCP**, entrez l'adresse de la passerelle relais dans le champ **Serveur DHCP distant**. La passerelle relais transmet les messages DHCP aux périphériques réseau, y compris à ceux se trouvant sur d'autres sous-réseaux.

ÉTAPE 5 Cliquez sur **Enregistrer**.

Configuration des VLAN

Un LAN virtuel ou VLAN est un groupe de points d'extrémité d'un réseau, associés par fonction ou selon d'autres caractéristiques communes. Contrairement aux LAN, qui se trouvent généralement sur un même site géographique, les VLAN peuvent regrouper des points d'extrémité indépendamment de l'emplacement physique des appareils et des utilisateurs.

Le périphérique comporte un VLAN par défaut (VLAN 1), qui ne peut pas être supprimé. Vous pouvez créer jusqu'à quatre autres VLAN sur le périphérique.

Pour créer un VLAN :

ÉTAPE 1 Sélectionnez **Mise en réseau** > **LAN** > **Membres du réseau VLAN**.

ÉTAPE 2 Cliquez sur **Ajouter une ligne**.

ÉTAPE 3 Saisissez les informations suivantes :

ID de VLAN	Identifiant numérique du VLAN à affecter aux points d'extrémité des membres du VLAN. La valeur doit être comprise entre 3 et 4 094. L'ID de VLAN 1 est réservé au VLAN par défaut et est utilisé pour les trames non balisées reçues par l'interface.
Description	Description qui identifie le VLAN.
Routage inter VLAN	Permet à une station finale dans un VLAN de communiquer avec une station finale dans un autre VLAN.
Port 1 **Port 2** **Port 3** **Port 4**	Vous pouvez associer les VLAN du périphérique aux ports LAN de l'appareil. Par défaut, tous les ports LAN appartiennent au VLAN1. Vous pouvez modifier les ports pour les associer à d'autres VLAN. Choisissez le type de trame sortante pour chaque port : **Non balisé** : l'interface est un membre non balisé du VLAN. Les trames du VLAN sont envoyées non balisées au port VLAN. **Balisé** : l'interface est un membre balisé du VLAN. Les trames du VLAN sont envoyées balisées au port VLAN. **Exclu** : le port n'est pas actuellement membre du VLAN. Il s'agit du paramètre par défaut de tous les ports à la création du VLAN.

ÉTAPE 4 Cliquez sur **Enregistrer**.

Pour modifier les paramètres d'un VLAN, sélectionnez le VLAN et cliquez sur **Modifier**. Pour supprimer un VLAN sélectionné, cliquez sur **Supprimer**. Cliquez sur **Enregistrer** pour appliquer les modifications.

Configuration de DHCP statique

Vous pouvez configurer le périphérique afin qu'il affecte une adresse IP particulière à un appareil doté d'une adresse MAC particulière.

Pour configurer le DHCP statique :

ÉTAPE 1 Sélectionnez **Mise en réseau** > **LAN** > **DHCP statique**.

ÉTAPE 2 Dans le menu déroulant **VLAN**, sélectionnez un numéro de VLAN.

ÉTAPE 3 Cliquez sur **Ajouter une ligne**.

ÉTAPE 4 Saisissez les informations suivantes :

Description	Description du client.
Adresse IP	Adresse IP du périphérique. L'adresse IP affectée ne doit pas faire partie du groupe d'adresses DHCP. L'affectation DHCP statique signifie que le serveur DHCP attribue la même adresse IP à une adresse MAC définie chaque fois que l'appareil est connecté au réseau. Le serveur DHCP attribue l'adresse IP réservée lorsque l'appareil doté de l'adresse MAC correspondante demande une adresse IP.
Adresse MAC	Adresse MAC du périphérique. Le format d'une adresse MAC est XX:XX:XX:XX:XX:XX où X est un chiffre compris entre 0 et 9 (inclus) ou une lettre comprise entre A et F (inclus).

Pour modifier les paramètres d'un client DHCP statique, sélectionnez le client et cliquez sur **Modifier**. Pour supprimer un client DHCP sélectionné, cliquez sur **Supprimer**. Cliquez sur **Enregistrer** pour appliquer les modifications.

Affichage des baux de clients DHCP

Vous pouvez afficher une liste de points d'extrémité sur le réseau (identifiés par nom d'hôte, adresse IP ou adresse MAC), et voir les adresses IP qui leur sont affectées par le serveur DHCP. Le VLAN des points d'extrémité est également affiché.

Pour voir les clients DHCP, sélectionnez **Mise en réseau** > **LAN** > **Baux de clients DHCP**.

Pour chaque VLAN défini sur le périphérique, une table présente une liste de clients associés au VLAN.

Pour attribuer une adresse IP statique à l'un des périphériques connectés :

ÉTAPE 1 Sur la ligne du périphérique connecté, cochez la case **Ajouter au DHCP statique**.

ÉTAPE 2 Cliquez sur **Enregistrer**.

Le serveur DHCP sur le périphérique attribue toujours l'adresse IP affichée lorsque le périphérique demande une adresse IP.

Configuration d'un hôte de DMZ

Le périphérique prend en charge les zones démilitarisées ou DMZ. Une DMZ est un sous-réseau ouvert au public, bien que derrière le pare-feu. Une DMZ permet de rediriger des paquets qui arrivent sur l'adresse IP de votre port WAN vers une adresse IP particulière sur votre LAN.

Nous vous conseillons de placer les hôtes devant être exposés au WAN (comme les serveurs Web ou de messagerie) sur le réseau DMZ. Vous pouvez configurer des règles de pare-feu pour autoriser l'accès à des services et ports particuliers sur la DMZ, depuis le LAN et depuis le WAN. En cas d'attaque d'un nœud de la DMZ, le réseau local n'est pas forcément vulnérable.

Vous devez configurer une adresse IP fixe (statique) pour le point d'extrémité qui doit servir d'hôte de la DMZ. Affectez à l'hôte de la DMZ une adresse IP sur le même sous-réseau que l'adresse IP LAN du périphérique, mais distincte de l'adresse IP donnée à l'interface LAN de cette passerelle.

Pour configurer la DMZ :

ÉTAPE 1 Sélectionnez **Mise en réseau** > **LAN** > **Hôte DMZ**.

ÉTAPE 2 Cochez la case **Activer** pour activer la DMZ sur le réseau.

ÉTAPE 3 Dans le menu déroulant VLAN, sélectionnez l'ID du VLAN sur lequel la DMZ est activée.

ÉTAPE 4 Dans le champ **Adresse IP de l'hôte**, entrez l'adresse IP de l'hôte DMZ. L'hôte DMZ est le point d'extrémité qui reçoit les paquets redirigés.

ÉTAPE 5 Cliquez sur **Enregistrer**.

Configuration de RSTP

Le protocole réseau RSTP (Rapid Spanning Tree Protocol) empêche la formation de boucles dans le réseau et reconfigure de manière dynamique les liaisons physiques qui doivent transférer les trames. Pour configurer le protocole RSTP (Rapid Spanning Tree Protocol) :

ÉTAPE 1 Sélectionnez **Mise en réseau** > **LAN** > **RSTP**.

ÉTAPE 2 Configurez les paramètres suivants :

Priorité du système	Sélectionnez la priorité système dans le menu déroulant. Vous pouvez choisir une priorité système comprise entre 0 et 61440 en incréments de 4096. Les valeurs autorisées sont 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 40960, 45056, 49152, 53248, 57344 et 61440. Plus la priorité du système est basse, plus le périphérique a de chance de devenir la racine dans l'arborescence STP. La valeur par défaut est **327688**.

Délai Hello	Le délai Hello correspond à la durée pendant laquelle la racine de l'arborescence STP doit attendre avant d'envoyer des messages de prise de contact. Entrez un nombre entre 1 et 10. La valeur par défaut est **2**.
Âge maximal	Le délai maximal correspond à la durée pendant laquelle le routeur doit attendre avant de recevoir un message de prise de contact. À l'expiration du délai maximal, le routeur essaie de changer l'arborescence STP. Entrez un nombre entre 6 et 40. La valeur par défaut est **20**.
Délai de transfert	Le délai de transfert correspond à l'intervalle au bout duquel une interface passe de l'état de blocage à l'état de réacheminement. Entrez un nombre entre 4 et 30. La valeur par défaut est **15**.
Forcer la version	Sélectionnez la version par défaut du protocole à utiliser. Sélectionnez **Normal** (utiliser RSTP) ou **Compatible** (compatible avec l'ancien STP). La valeur par défaut est **Normal**.

ÉTAPE 3 Dans **Table des paramètres**, configurez les paramètres suivants :

Activer le protocole	Cochez pour activer le RSTP sur le port concerné. RSTP est désactivé par défaut.
Bordure	Cochez pour spécifier que le port concerné est un port de bordure (station terminale). Décochez pour spécifier que le port concerné est un lien (pont) vers un autre appareil STP. L'option Bordure est activée par défaut.
Coût du chemin	Indiquez le coût du chemin RSTP pour les ports concernés. Utilisez 0 pour la valeur par défaut (le périphérique détermine automatiquement la valeur du chemin). Vous pouvez également entrer une valeur comprise entre 2 et 200 000 000.

ÉTAPE 4 Cliquez sur **Enregistrer**.

Gestion des ports

Vous pouvez configurer les paramètres de vitesse et de contrôle de flux des ports LAN du périphérique.

Pour configurer la vitesse des ports et le contrôle de flux :

ÉTAPE 1 Sélectionnez **Mise en réseau** > **Gestion des ports**.

ÉTAPE 2 Précisez les informations suivantes :

Port	Le numéro du port.
Lien	La vitesse du port. Lorsqu'aucun appareil n'est branché sur le port, ce champ affiche la mention **Désactivé**.
Mode	Sélectionnez une des vitesses de port suivantes dans le menu déroulant : • **Négociation automatique** : le périphérique et l'appareil connecté sélectionnent une vitesse commune. • **10 Mbit/s semi** : 10 Mbit/s dans chaque direction, mais dans une seule direction à la fois. • **10 Mbit/s intégral** : 10 Mbit/s dans chaque direction, simultanément. • **100 Mbit/s semi** : 100 Mbit/s dans chaque direction, mais dans une seule direction à la fois. • **100 Mbit/s intégral** : 100 Mbit/s dans chaque direction, simultanément.

Contrôle de flux	Cochez cette case pour activer le contrôle de flux sur le port. Le contrôle de flux consiste à gérer le débit des transmissions de données entre deux nœuds, afin d'empêcher un expéditeur trop rapide de submerger un récepteur trop lent. Il fournit un mécanisme qui permet au récepteur de contrôler la vitesse de transmission, afin que le nœud de réception ne soit pas submergé par les données provenant du nœud de transmission.

ÉTAPE 3 Cliquez sur **Enregistrer**.

Clonage de l'adresse MAC

Parfois, il peut être utile de définir l'adresse MAC du port WAN du périphérique afin qu'il ait la même adresse MAC que votre PC ou une autre adresse MAC particulière. On appelle cela cloner l'adresse MAC.

Par exemple, certains FAI enregistrent l'adresse MAC de la carte réseau de votre ordinateur lors de l'installation du service. Si vous installez ensuite un routeur derrière le modem câble ou DSL, l'adresse MAC du port WAN du périphérique n'est pas reconnue par le FAI.

Dans ce cas, pour configurer le périphérique afin qu'il soit reconnu par le FAI, vous devez cloner l'adresse MAC du port WAN afin qu'elle corresponde à l'adresse MAC de votre ordinateur.

Pour configurer un clone d'adresse MAC :

ÉTAPE 1 Sélectionnez **Mise en réseau** > **Clone d'adresse MAC**.

ÉTAPE 2 Dans le champ **Clone d'adresse MAC**, cochez la case **Activer**.

ÉTAPE 3 Pour définir l'adresse MAC du port WAN du périphérique, utilisez l'une des méthodes suivantes :

- Pour régler l'adresse MAC du port WAN sur l'adresse MAC de votre PC, cliquez sur **Cloner MAC du PC**.
- Pour spécifier une autre adresse MAC, entrez-la dans le champ **Adresse MAC**.

ÉTAPE 4 Cliquez sur **Enregistrer**.

Configuration du routage

Configurez les options de routage.

Configuration du mode de fonctionnement

Pour configurer le mode de fonctionnement du périphérique :

ÉTAPE 1 Sélectionnez **Mise en réseau** > **Routage**.

ÉTAPE 2 Dans le champ **Mode de fonctionnement**, sélectionnez l'une des options suivantes :

Passerelle	(Recommandé) Cliquez sur ce bouton pour que le périphérique fasse office de passerelle. Conservez ce paramètre par défaut si le périphérique héberge la connexion Internet de votre réseau et s'il effectue les fonctions de routage.
Routeur	(Pour les utilisateurs expérimentés uniquement) Cliquez sur ce bouton pour que le périphérique joue le rôle de routeur. Sélectionnez cette option si le périphérique se trouve sur un réseau doté d'autres routeurs. L'activation du mode Routeur désactive la Traduction d'adresses réseau (ou NAT) sur le périphérique.

ÉTAPE 3 Cliquez sur **Enregistrer**.

Configuration du routage dynamique

Le protocole RIP (Routing Information Protocol) est un protocole IGP (Interior Gateway Protocol) couramment utilisé sur les réseaux internes. Il permet au routeur d'échanger ses données de routage automatiquement avec d'autres routeurs, et d'ajuster dynamiquement ses tables de routage et de s'adapter aux changements sur le réseau.

Le routage dynamique (RIP) permet au périphérique de s'adapter automatiquement aux modifications physiques de la topologie du réseau et d'échanger des tables de routage avec d'autres routeurs.

Le routeur détermine le chemin suivi par les paquets réseau, en visant le nombre le plus faible possible de sauts entre la source et la destination. RIP est désactivé par défaut.

REMARQUE Le protocole RIP est désactivé par défaut sur le périphérique.

Pour configurer le routage dynamique :

ÉTAPE 1 Sélectionnez **Mise en réseau** > **Routage**.

ÉTAPE 2 Configurez les paramètres suivants :

RIP	Cochez la case **Activer** pour activer l'option RIP. Le périphérique peut alors utiliser le protocole RIP pour acheminer le trafic.
Version de paquet RIP envoyé	Sélectionnez la version de paquet RIP envoyé (**RIPv1** ou **RIPv2**). La version de RIP utilisée pour envoyer des mises à jour de routage aux autres routeurs présents sur le réseau dépend de la configuration de ces autres routeurs. RIPv2 est compatible avec RIPv1.
Version de paquet RIP reçu	Sélectionnez la version de paquet RIP reçu.

ÉTAPE 3 Cliquez sur **Enregistrer**.

Configuration du routage statique

Vous pouvez configurer des routes statiques pour diriger des paquets vers un réseau de destination. Une route statique est un chemin prédéfini devant être emprunté par un paquet afin d'atteindre un hôte ou réseau particulier.

Certains FAI exigent des routes statiques plutôt que des protocoles de routage dynamiques pour la création de tables de routage. Les routes statiques ne requièrent pas de ressources de processeur pour l'échange des informations de routage avec un routeur homologue.

Vous pouvez également utiliser des routes statiques pour atteindre des routeurs homologues qui ne prennent pas en charge les protocoles de routage dynamique. Les routes statiques peuvent être utilisées avec des routes dynamiques.
Le périphérique peut prendre en charge jusqu'à 30 routes statiques.

Prenez garde à ne pas introduire de boucles de routage dans votre réseau.

Pour configurer le routage statique :

ÉTAPE 1 Sélectionnez **Mise en réseau** > **Routage**.

ÉTAPE 2 Dans le menu déroulant **Entrées de route**, sélectionnez une entrée de route.

Pour supprimer une entrée de route, cliquez sur **Supprimer cette entrée**.

ÉTAPE 3 Configurez les paramètres suivants pour l'entrée de route sélectionnée :

Entrer le nom de route	Entrez le nom de la route.
Adresse IP du LAN de destination	Entrez l'adresse IP du réseau local de destination.
Masque de sous-réseau	Entrez le masque de sous-réseau du réseau de destination.
Passerelle	Entrez l'adresse IP de la passerelle utilisée pour ce chemin.

Interface	Sélectionnez l'interface vers laquelle les paquets de cette route sont envoyés : • **LAN et sans fil** : cliquez sur ce bouton pour diriger les paquets vers le réseau local et sans fil. • **Internet (WAN)** : cliquez sur ce bouton pour diriger les paquets vers le réseau étendu ou Internet.

ÉTAPE 4 Cliquez sur **Enregistrer**.

Affichage de la table de routage

La table de routage contient des informations sur la topologie du réseau dans l'environnement proche de celui-ci.

Pour afficher les informations de routage sur votre réseau, choisissez **Mise en réseau** > **Table de routage** et sélectionnez l'une des options suivantes :

- **Afficher la table de routage IPv4** : la table de routage est affichée avec les champs configurés sur la page **Mise en réseau** > **Routage**.
- **Afficher la table de routage IPv6** : la table de routage est affichée avec les champs configurés sur les pages **Mise en réseau** > **IPv6**.

Configuration du DNS dynamique

Le DDNS (DNS dynamique) est un service Internet qui permet de localiser les routeurs dotés d'adresses IP publiques variables à l'aide de noms de domaine Internet. Pour utiliser le DDNS, vous devez créer un compte auprès d'un fournisseur DDNS comme DynDNS.com, TZO.com, 3322.org ou noip.com.

Le routeur notifie des serveurs DNS dynamiques de modifications d'adresses IP du WAN, afin que tout service public sur votre réseau puisse être contacté par le biais du nom de domaine.

Pour configurer le DDNS :

ÉTAPE 1 Sélectionnez **Mise en réseau** > **DNS dynamique**.

ÉTAPE 2 Dans le menu déroulant **Service DDNS**, sélectionnez **Désactiver** pour désactiver le service ou sélectionnez le service DDNS à utiliser.

ÉTAPE 3 Si vous n'avez pas de compte DDNS, cliquez sur l'URL du fournisseur DDNS pour visiter son site web et y créer un compte.

ÉTAPE 4 Précisez les informations suivantes :

Adresse e-mail	(TZO.com et noip.com) Adresse e-mail utilisée pour créer le compte DDNS.
Nom d'utilisateur	(DynDNS.com et 3322.org) Nom d'utilisateur du compte DDNS.
Mot de passe	Mot de passe du compte DDNS.
Vérifier le mot de passe	(TZO.com, DynDNS.com et noip.com) Confirmation du mot de passe du compte DDNS.
Nom d'hôte	(DynDNS.com, 3322.org et noip.com) Nom d'hôte du serveur DDNS.
Nom de domaine	(TZO.com) Nom du domaine utilisé pour accéder au réseau.
Intervalle de mise à jour	Choisissez l'une des options suivantes pour définir la fréquence d'actualisation de l'adresse IP et du nom de domaine sur le serveur DDNS : **Jamais** : ne jamais actualiser. **Toutes les semaines** : actualiser chaque semaine, le lundi à 00:MM. MM étant un nombre compris entre 0 et 59, sélectionné de façon aléatoire. L'option Toutes les semaines est choisie par défaut. **Deux fois par mois** : actualiser les premier et quinzième jours du mois à 00:MM. MM étant un nombre compris entre 0 et 59, sélectionné de façon aléatoire. **Chaque mois** : actualiser le premier jour du mois à 00:MM. MM étant un nombre compris entre 0 et 59, sélectionné de façon aléatoire.

Adresse IP Internet	(Lecture seule) Adresse IP Internet du périphérique.
État	(Lecture seule) Indique que la mise à jour DDNS s'est terminée correctement ou que l'envoi des informations de mise à jour du compte au serveur DDNS a échoué.

ÉTAPE 5 Pour tester la configuration DDNS, cliquez sur **Tester la configuration**.

ÉTAPE 6 Cliquez sur **Enregistrer**.

Configuration du mode IP

Les propriétés de réseau étendu peuvent être configurées pour les réseaux IPv4 et IPv6. Ces pages vous permettent de saisir des informations sur votre type de connexion Internet et d'autres paramètres.

Pour sélectionner un mode IP :

ÉTAPE 1 Sélectionnez **Mise en réseau** > **Mode IP**.

ÉTAPE 2 Dans le menu déroulant **Mode IP**, sélectionnez l'une des options suivantes :

LAN : IPv4, WAN : IPv4	Utilisez IPv4 sur les ports LAN et WAN.
LAN : IPv6, WAN : IPv4	Utilisez IPv6 sur les ports LAN et IPv4 sur les ports WAN.
LAN : IPv6, WAN : IPv6	Utilisez IPv6 sur les ports LAN et WAN.
LAN : IPv4+IPv6, WAN : IPv4	Utilisez IPv4 et IPv6 sur les ports LAN et IPv4 sur les ports WAN.
LAN : IPv4+IPV6, WAN : IPv4+IPv6	Utilisez IPv4 et IPv6 sur les ports LAN et WAN.
LAN : IPv4, WAN : IPv6	Utilisez IPv4 sur les ports LAN et IPv6 sur les ports WAN.

ÉTAPE 3 (Facultatif) Si vous utilisez le tunneling 6to4 qui permet la transmission de paquets IPv6 sur un réseau IPv4, procédez comme suit :

a. Cliquez sur **Afficher les champs d'entrée DNS 6to4 statique**.

b. Dans les champs **Domaine** et **IP**, saisissez jusqu'à cinq associations domaine/IP.

La fonction de tunneling 6to4 est généralement utilisée lorsqu'un site ou un utilisateur veut se connecter à l'Internet IPv6 à partir du réseau IPv4 existant.

ÉTAPE 4 Cliquez sur **Enregistrer**.

Configuration d'IPv6

Internet Protocol version 6 (IPv6) est une version du protocole Internet (IP) destinée à remplacer Internet Protocol version 4 (IPv4). La configuration des propriétés WAN d'un réseau IPv6 dépend du type de connexion Internet que vous utilisez.

Configuration de la connexion WAN IPV6

Vous pouvez configurer le périphérique en tant que client DHCPv6 du FAI pour ce WAN ou pour utiliser une adresse IPv6 statique fournie par le FAI.

Pour configurer les paramètres WAN IPv6 sur votre périphérique, vous devez d'abord définir le mode IP sur l'un des modes suivants :

- LAN : IPv6, WAN : IPv6
- LAN : IPv4+IPv6, WAN : IPv4
- LAN : IPv4 + IPv6, WAN : IPv4 + IPv6

Reportez-vous à la section **Configuration du mode IP** pour en savoir plus sur la définition du mode IP.

Configuration de DHCPv6

Si votre FAI vous fournit une adresse affectée dynamiquement, configurez le périphérique en tant que client DHCPv6.

Pour configurer le périphérique en tant que client DHCPv6 :

ÉTAPE 1 Sélectionnez **Mise en réseau** > **IPv6** > **Configuration WAN IPv6**.

ÉTAPE 2 Dans le champ **Type de connexion WAN**, sélectionnez **Configuration automatique - DHCPv6**.

ÉTAPE 3 Cliquez sur **Enregistrer**.

Configuration d'une adresse WAN IPv6 statique

Si votre FAI vous attribue une adresse fixe pour accéder au réseau WAN, configurez le périphérique afin qu'il utilise une adresse IPv6 statique.

Pour configurer une adresse WAN IPv6 statique :

ÉTAPE 1 Sélectionnez **Mise en réseau** > **IPv6** > **Configuration WAN IPv6**.

ÉTAPE 2 Dans le menu **Type de connexion WAN**, sélectionnez **IPv6 statique**.

ÉTAPE 3 Saisissez les informations suivantes :

Adresse IPv6	Adresse IPv6 du port WAN.
Longueur du préfixe IPv6	Longueur du préfixe IPv6 (généralement définie par le FAI). Le réseau (sous-réseau) IPv6 est identifié par les premiers bits de l'adresse, qui constituent le préfixe. Tous les hôtes du sous-réseau ont un préfixe identique. Par exemple, dans l'adresse IPv6 `2001:0DB8:AC10:FE01::` le préfixe est `2001`.
Passerelle IPv6 par défaut	Adresse IPv6 de la passerelle par défaut. Il s'agit généralement de l'adresse IP du serveur du FAI.
DNS statique 1	Adresse IP du serveur DNS IPv6 principal.
DNS statique 2	Adresse IP du serveur DNS IPv6 secondaire.

ÉTAPE 4 Cliquez sur **Enregistrer**.

Configuration des paramètres PPPoE IPv6

Vous pouvez exécuter PPPoE IPv4, PPPoE IPv6 ou les deux. Si vous exécutez les deux, les paramètres PPPoE WAN IPv6 doivent correspondre aux paramètres PPPoE WAN IPv4. S'ils ne correspondent pas, un message vous demande si vous voulez définir le protocole IPv6 afin qu'il corresponde au protocole IPv4. Pour plus d'informations, reportez-vous à **Configuration du protocole PPPoE**.

Pour configurer les paramètres PPPoE IPv6 :

ÉTAPE 1 Sélectionnez **Mise en réseau** > **IPv6** > **Configuration WAN IPv6**.

ÉTAPE 2 Dans le champ **Type de connexion WAN**, sélectionnez **PPPoE IPv6**.

ÉTAPE 3 Saisissez les informations suivantes (contactez le cas échéant votre FAI pour obtenir les informations de connexion PPPoE) :

Nom d'utilisateur	Nom d'utilisateur qui vous est attribué par le FAI.
Mot de passe	Mot de passe qui vous est attribué par le FAI.
Connexion à la demande	Si votre FAI vous facture en fonction de la durée de connexion, sélectionnez cette case d'option. Lorsque cette option est sélectionnée, la connexion Internet est active uniquement en présence de trafic. Si la connexion est en attente (sans trafic en transit), la connexion est fermée. Dans le champ **Durée d'inactivité max.**, entrez le nombre de minutes qui doivent s'écouler lorsqu'aucun trafic n'est détecté sur la liaison avant l'arrêt de cette dernière.
Garder actif	Garde la liaison WAN active en envoyant un message correspondant sur le port. Dans le champ de délai de renumérotation, spécifiez le délai (en secondes) avant que le périphérique ne tente de se reconnecter après déconnexion.

Type d'authentification	Types d'authentification : **Négociation automatique** : un serveur envoie une demande de configuration spécifiant l'algorithme de sécurité paramétré sur le serveur. Le périphérique répond avec ses identifiants d'authentification en utilisant le type de sécurité spécifié par le serveur. **PAP** : utilisez le protocole PAP (Password Authentication Protocol) lors de la connexion au FAI. **CHAP** : utilisez le protocole CHAP (Challenge Handshake Authentication Protocol) pour la connexion au FAI. **MS-CHAP ou MS-CHAPv2** : utilisez le protocole Microsoft Challenge Handshake Authentication Protocol lors de la connexion au FAI.
Nom du service	Nom que votre FAI peut demander lors de la connexion au serveur PPPoE.
MTU	Maximum Transmission Unit ou la taille maximale de paquet pouvant être transmis sur le réseau. À moins que votre FAI impose une modification, nous vous conseillons la sélection de l'option **Automatique**. La valeur de MTU standard sur les réseaux Ethernet est de 1500 octets. Pour les connexions PPPoE, la valeur est de 1492 octets. Si votre FAI exige un paramètre MTU personnalisé, sélectionnez **Manuel**.
Taille	Taille MTU. Si votre FAI exige un paramètre MTU personnalisé, entrez la taille de MTU.
Mode d'adresse	Mode d'adresse dynamique ou statique. Si vous choisissez statique, entrez l'adresse IPv6 dans le champ suivant.
Longueur du préfixe IPv6	Longueur du préfixe IPv6.
Passerelle IPv6 par défaut	Adresse IP de la passerelle IPv6 par défaut.

DNS statique 1	Adresse IP du serveur DNS principal.
DNS statique 2	Adresse IP du serveur DNS secondaire.

ÉTAPE 4 Cliquez sur **Enregistrer**.

Configuration des connexions LAN IPv6

En mode IPv6, le serveur DHCP du réseau local (LAN) est activé par défaut (comme en mode IPv4). Le serveur DHCPv6 affecte des adresses IPv6 à partir des groupes d'adresses qui utilisent la longueur de préfixe IPv6 affectée au LAN.

Pour configurer les paramètres LAN IPv6 sur votre périphérique, vous devez d'abord régler le mode IP sur l'un des modes suivants :

- LAN : IPv6, WAN : IPv4
- LAN : IPv6, WAN : IPv6
- LAN : IPv4+IPv6, WAN : IPv4
- LAN : IPv4 + IPv6, WAN : IPv4 + IPv6

Reportez-vous à la section **Configuration du mode IP** pour en savoir plus sur la définition du mode IP.

Pour configurer les paramètres de LAN IPv6 :

ÉTAPE 1 Sélectionnez **Mise en réseau** > **IPv6** > **Configuration LAN IPv6**.

ÉTAPE 2 Saisissez les informations suivantes pour configurer l'adresse IPv6 du LAN :

Adresse IPv6	Entrez l'adresse IPv6 du périphérique. L'adresse IPv6 par défaut de la passerelle est fec0::1 (ou FEC0:0000:0000:0000:0000:0000:0000:0001). Vous pouvez modifier cette adresse IPv6 de 128 bits en fonction de la configuration de votre réseau.

Longueur du préfixe IPv6	Entrez la longueur du préfixe IPv6. Le réseau (sous-réseau) IPv6 est identifié par les premiers bits de l'adresse, qui constituent le préfixe. Par défaut, le préfixe a une longueur de 64 bits. Tous les hôtes du réseau utilisent les mêmes premiers bits dans leur adresse IPv6. Vous réglez le nombre de bits initiaux communs des adresses du réseau dans ce champ.

ÉTAPE 3 Cliquez sur **Enregistrer** ou continuez pour configurer les paramètres LAN IPv6 DHCP.

ÉTAPE 4 Saisissez les informations suivantes pour configurer les paramètres DHCPv6 :

État du serveur DHCP	Cochez cette option pour activer le serveur DHCPv6. Lorsque cette option est activée, le périphérique attribue une adresse IP appartenant à la plage spécifiée et fournit des informations supplémentaires à tout point d'extrémité de LAN qui demande une adresse DHCP.
Nom de domaine	(Facultatif) Nom de domaine du serveur DHCPv6.
Préférence de serveur	Niveau de préférence serveur de ce serveur DHCP. Les messages d'annonce DHCP dotés de la valeur de préférence de serveur la plus élevée sont prioritaires sur les autres messages d'annonce DHCP. La valeur par défaut est 255.
DNS statique 1	Adresse IPv6 du serveur DNS principal du réseau IPv6 du FAI.
DNS statique 2	Adresse IPv6 du serveur DNS secondaire sur le réseau IPv6 du FAI.
Durée de bail du client	Durée (en secondes) du bail du client pour des baux d'adresses IPv6 destinés aux points d'extrémité du LAN.

ÉTAPE 5 Sélectionnez **Mise en réseau** > **IPv6** > **Configuration LAN IPv6**.

ÉTAPE 6 Dans la **Table des groupes d'adresses IPv6**, cliquez sur **Ajouter une ligne**.

ÉTAPE 7 Saisissez les informations suivantes :

Adresse de début	Adresse IPv6 de début du groupe.
Adresse de fin	Adresse IPv6 de fin du groupe.
Longueur du préfixe IPv6	Longueur de préfixe qui détermine le nombre de bits initiaux communs des adresses du réseau.

ÉTAPE 8 Cliquez sur **Enregistrer**.

Pour modifier les paramètres d'un groupe, sélectionnez le groupe et cliquez sur **Modifier**. Pour supprimer un groupe sélectionné, cliquez sur **Supprimer**. Cliquez sur **Enregistrer** pour appliquer les modifications.

Configuration du routage IPv6 statique

Vous pouvez configurer des routes statiques pour diriger des paquets vers un réseau de destination. Une route statique est un chemin prédéfini devant être emprunté par un paquet afin d'atteindre un hôte ou réseau particulier.

Certains FAI exigent une route statique pour établir une table de routage au lieu d'utiliser des protocoles de routage dynamique. Les routes statiques ne requièrent pas de ressources de processeur pour l'échange des informations de routage avec un routeur homologue.

Vous pouvez également utiliser des routes statiques pour atteindre des routeurs homologues qui ne prennent pas en charge les protocoles de routage dynamique. Les routes statiques peuvent être utilisées avec des routes dynamiques. Prenez garde à ne pas introduire de boucles de routage dans votre réseau.

Pour créer une route statique :

ÉTAPE 1 Sélectionnez **Mise en réseau** > **IPv6** > **IPv6 Routage statique**.

ÉTAPE 2 Dans la liste des routes statiques, cliquez sur **Ajouter une ligne**.

ÉTAPE 3 Saisissez les informations suivantes :

Nom	Nom de la route.
Destination	Adresse IPv6 de l'hôte ou réseau de destination pour cette route.
Longueur du préfixe	Nombre de bits de préfixe de l'adresse IPv6 qui définissent le sous-réseau de destination.
Passerelle	Adresse IPv6 de la passerelle par laquelle l'hôte ou réseau de destination est joignable.
Interface	Interface pour la route : **LAN**, **WAN** ou **6to4**.
Paramètre	Priorité de la route. Choisissez une valeur comprise entre 2 et 15. S'il existe plusieurs routes vers une même destination, la route avec la mesure la plus faible est utilisée.
Actif	Cochez cette option pour activer la route. Lorsque vous ajoutez une route dans un état inactif, elle est ajoutée à la table de routage, mais elle n'est pas utilisée par le périphérique. La saisie d'une route inactive peut être utile si la route n'est pas disponible au moment où vous l'ajoutez. Une fois le réseau disponible, vous pouvez activer la route.

ÉTAPE 4 Cliquez sur **Enregistrer**.

Pour modifier les paramètres d'une route, sélectionnez-la et cliquez sur **Modifier**. Pour supprimer une route sélectionnée, cliquez sur **Supprimer**. Cliquez sur **Enregistrer** pour appliquer les modifications.

Configuration du routage (RIPng)

RIP Next Generation (RIPng) est un protocole de routage basé sur l'algorithme D-V (Distance Vector). RIPng utilise des paquets UDP pour échanger des informations de routage par le port 521.

Le protocole RIPng utilise un nombre de sauts pour mesurer la distance jusqu'à la destination. Le nombre de sauts est appelé mesure ou coût. Le nombre de sauts d'un routeur vers un réseau auquel il est 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 hôte de destination est injoignable.

Par défaut, l'actualisation du routage est envoyée toutes les 30 secondes. Si le routeur ne reçoit pas de mise à jour de routage d'un voisin après 180 secondes, les routes obtenues du voisin sont considérées comme injoignables. Si aucune mise à jour de routage n'est reçue après 240 secondes de plus, le routeur supprime ces chemins de la table de routage.

Sur le périphérique, le protocole RIPng est désactivé par défaut.

Pour configurer RIPng :

ÉTAPE 1 Sélectionnez **Mise en réseau** > **IPv6** > **Routage (RIPng)**.

ÉTAPE 2 Cochez **Activer**.

ÉTAPE 3 Cliquez sur **Enregistrer**.

Configuration du tunneling

Le tunneling IPv6 vers IPv4 (tunneling 6to4) permet la transmission de paquets IPv6 sur un réseau IPv4. Le tunneling IPv4 vers IPv6 (tunneling 4to6) permet la transmission de paquets IPv4 sur un réseau IPv6.

Tunneling 6-to-4

Le tunneling 6-to-4 est généralement utilisé lorsqu'un site ou un utilisateur veut se connecter à l'Internet IPv6 à partir du réseau IPv4 existant.

Pour configurer le tunneling 6-to-4 :

ÉTAPE 1 Sélectionnez **Paramètres réseau** > **IPv6** > **Tunneling**.

ÉTAPE 2 Dans le champ **Tunnellisation 6to4**, cochez la case **Activer**.

ÉTAPE 3 Choisissez le type de tunneling (**6to4** ou **6RD** [déploiement rapide]).

ÉTAPE 4 Pour le tunneling 6RD, choisissez **Automatique** ou **Manuel**.

ÉTAPE 5 Saisissez les informations suivantes :

- **Préfixe IPv6**
- **Longueur du préfixe IPv6**
- **Border Relay**
- **Longueur du masque IPv4**

ÉTAPE 6 Cliquez sur **Enregistrer**.

Tunneling 4to6

Pour configurer le tunneling 4to6 :

ÉTAPE 1 Sélectionnez **Paramètres réseau** > **IPv6** > **Tunneling**.

ÉTAPE 2 Dans le champ **Tunnellisation 4to6**, cochez la case **Activer**.

ÉTAPE 3 Entrez l'adresse IPv6 du WAN local sur le périphérique.

ÉTAPE 4 Entrez l'adresse IPv6 distante ou l'adresse IP du point d'extrémité distant.

ÉTAPE 5 Cliquez sur **Enregistrer**.

Affichage de l'état du tunnel IPv6

Pour afficher l'état du tunnel IPv6 :

ÉTAPE 1 Sélectionnez **Mise en réseau** > **IPv6** > **État du tunnel IPv6**.

ÉTAPE 2 Cliquez sur **Actualiser** pour afficher les dernières informations.

Cette page affiche des informations sur le tunnel automatique établi sur l'interface WAN dédiée. La table indique le nom du tunnel et l'adresse IPv6 créée sur l'appareil.

Configuration de l'annonce du routeur

Le démon RADVD (Router Advertisement Daemon) sur le périphérique est à l'écoute des messages de sollicitation du routeur sur le LAN IPv6 et répond par des annonces de routeur selon les besoins. Il s'agit d'une configuration IPv6 automatique sans état et le périphérique distribue les préfixes IPv6 à tous les nœuds du réseau.

Pour configurer le RADVD :

ÉTAPE 1 Sélectionnez **Mise en réseau** > **IPv6** > **Annonce de routeur**.

ÉTAPE 2 Saisissez les informations suivantes :

État RADVD	Sélectionnez **Activer** pour activer le RADVD.
Mode d'annonce	Sélectionnez l'un des modes suivants : **Multidiffusion non demandée** : envoyez les annonces du routeur (RA) à toutes les interfaces appartenant au groupe de multidiffusion. **Monodiffusion uniquement** : limitez les annonces à des adresses IPv6 bien connues (les annonces du routeur ne sont envoyées qu'à l'interface appartenant à l'adresse connue).
Intervalle d'annonce	Intervalle d'annonce (4 à 1 800) pour la **Multidiffusion non demandée**. La valeur par défaut est 30. L'intervalle d'annonce est une valeur aléatoire comprise entre les valeurs minimales et maximales d'intervalle d'annonce (MinRtrAdvInterval et MaxRtrAdvInterval). MinRtrAdvInterval = 0,33 * MaxRtrAdvInterval
Indicateurs d'annonces	Cochez la case **Gérés** pour utiliser le protocole administré / avec état pour la configuration automatique des adresses. Cochez la case **Autre** pour utiliser le protocole administré / avec état pour la configuration automatique d'autres informations (autres que l'adresse).

Préférence de routeur	Sélectionnez **faible**, **moyen** ou **élevé** dans le menu déroulant. La valeur par défaut est moyen. La préférence de routeur fournit une mesure de préférence pour les routeurs par défaut. Les valeurs basse, moyenne et élevée sont signalées à l'aide de bits non utilisés dans les messages d'annonce du routeur. Cette extension est rétrocompatible, tant avec les routeurs (réglage de la valeur de préférence de routeur) qu'avec les hôtes (interprétation de la valeur de préférence de routeur). Ces valeurs sont ignorées par les hôtes qui ne mettent pas en œuvre la préférence de routeur. Cette fonctionnalité est pratique lorsque d'autres appareils utilisant le RADVD sont présents sur le réseau local.
MTU	Taille de MTU (0 ou de 1 280 à 1 500). La valeur par défaut est de 1 500 octets. Le MTU (Maximum Transmit Unit) correspond à la taille maximale de paquet pouvant être transmis sur le réseau. Le MTU est utilisé dans les annonces du routeur pour assurer que tous les nœuds du réseau utilisent la même valeur de MTU lorsque le MTU du réseau n'est pas connu.
Durée de vie du routeur	Valeur de durée de vie du routeur, ou durée en secondes d'existence des messages d'annonce sur la route. La valeur par défaut est 3600 secondes.

ÉTAPE 3 Cliquez sur **Enregistrer**.

Configuration des préfixes d'annonce

Pour configurer les préfixes RADVD disponibles :

ÉTAPE 1 Sélectionnez **Mise en réseau** > **IPv6** > **Préfixes d'annonce**.

ÉTAPE 2 Cliquez sur **Ajouter une ligne**.

ÉTAPE 3 Saisissez les informations suivantes :

Type de préfixe IPv6	Choisissez l'un des types suivants : **6to4** : permet la transmission des paquets IPv6 sur un réseau IPv4. Ce type est utilisé lorsqu'un utilisateur veut se connecter à l'Internet IPv6 en passant par son réseau IPv4 existant. **Global/local** : une adresse IPv6 locale unique que vous pouvez utiliser sur les réseaux IPv6 privés ou une adresse Internet IPv6 unique globale.
ID SLA	Si vous sélectionnez le type de préfixe IPv6 **6to4**, entrez l'ID SLA (identifiant Site-Level Aggregation). L'ID SLA du préfixe d'adresse 6to4 est réglé sur l'ID de l'interface sur laquelle les annonces sont envoyées.
Préfixe IPv6	Si vous sélectionnez le type de préfixe IPv6 **Global/local**, entrez le préfixe IPv6. Le préfixe IPv6 spécifie l'adresse réseau IPv6.
Longueur du préfixe IPv6	Si vous sélectionnez le type de préfixe IPv6 **Global/local**, entrez la longueur de préfixe. La variable de longueur de préfixe est une valeur décimale qui indique le nombre de bits contigus les plus significatifs de l'adresse qui composent la partie réseau de l'adresse.
Durée de vie du préfixe	Durée de vie du préfixe, ou durée durant laquelle le routeur à l'origine de la demande est autorisé à utiliser le préfixe.

ÉTAPE 4 Cliquez sur **Enregistrer**.

4

Configuration du réseau sans fil

Ce chapitre indique la marche à suivre pour configurer les paramètres de réseau sans fil du périphérique.

- **Sécurité sans fil**
- **Cisco RV215W - Réseaux sans fil**
- **Configuration des paramètres sans fil de base**
- **Configuration des paramètres sans fil avancés**
- **Configuration de WDS**
- **Configuration de WPS**

Sécurité sans fil

Les réseaux sans fil sont pratiques et faciles à créer, ce qui explique que les particuliers et les professionnels équipés d'un accès haut débit à Internet y ont de plus en plus recours.

Mais les réseaux sans fil fonctionnent en transmettant les informations par ondes radio, ce qui les rend potentiellement plus vulnérables que les réseaux traditionnels filaires.

Conseils relatifs à la sécurité des réseaux sans fil

Vous ne pouvez pas empêcher quelqu'un de se connecter à votre réseau sans fil, mais vous pouvez suivre les conseils suivants pour sécuriser votre réseau :

- Modifiez le nom ou le SSID par défaut du réseau sans fil.

  Les appareils sans fil sont dotés d'un nom ou le SSID de réseau sans fil par défaut. Il s'agit du nom de votre réseau sans fil, qui peut comporter jusqu'à 32 caractères.

Pour protéger votre réseau, changez le nom de réseau sans fil par défaut et donnez-lui un nom unique qui le distingue des autres réseaux sans fil qui vous entourent.

Lorsque vous choisissez un nom, n'utilisez pas d'informations personnelles (comme un numéro de carte bancaire), car cette information sera visible par tout individu qui parcourt les réseaux sans fil.

- Modifiez le mot de passe par défaut.

  Sur les appareils sans fil comme les points d'accès, routeurs et passerelles, vous devez saisir un mot de passe lorsque vous souhaitez modifier les paramètres. Ces appareils ont un mot de passe par défaut. Le mot de passe par défaut est souvent **cisco**.

  Les pirates connaissent ces valeurs par défaut et essaient de les exploiter pour accéder à vos appareils sans fil et modifier vos paramètres réseau. Pour empêcher les accès non autorisés, personnalisez le mot de passe du routeur afin qu'il soit difficile à deviner.

- Activez le filtrage des adresses MAC.

  Les routeurs et passerelles Cisco vous permettent d'activer le filtrage d'adresses MAC. L'adresse MAC est une série unique de chiffres et de lettres affectée à chaque appareil en réseau.

  Lorsque le filtrage des adresses MAC est activé, l'accès au réseau sans fil est réservé aux appareils sans fil dotés d'adresses MAC particulières. Vous pouvez par exemple spécifier l'adresse MAC de chaque ordinateur de votre réseau, afin que seuls ces ordinateurs puissent accéder à votre réseau sans fil.

- Activez le cryptage.

  Le cryptage protège les données transmises sur un réseau sans fil. Les normes WPA/WPA2 (Wi-Fi Protected Access) et WEP (Wired Equivalency Privacy) offrent différents niveaux de sécurité pour la communication sans fil. Actuellement, les appareils certifiés Wi-Fi sont tenus de prendre en charge le WPA2, mais ne sont pas obligés de prendre en charge le WEP.

  Un réseau chiffré par WPA/WPA2 est mieux sécurisé qu'un réseau chiffré en WEP, car le WPA/WPA2 utilise le cryptage par clé dynamique.

  Pour protéger les données qui transitent par les ondes, activez le niveau de cryptage le plus élevé pris en charge par vos équipements réseau.

  WEP est une norme de cryptage plus ancienne, mais certains appareils plus anciens n'offrent que cette option et ne prennent pas en charge le WPA.

- Ne placez pas les routeurs, points d'accès et passerelles sans fil près des murs extérieurs et des fenêtres.
- Éteignez les routeurs, points d'accès et passerelles sans fil lorsque vous ne les utilisez pas (la nuit, pendant les vacances).
- Utilisez des mots de passe forts contenant au moins huit caractères. Combinez chiffres et lettres pour éviter d'utiliser des mots du dictionnaire.

Directives générales sur la sécurité réseau

Inutile de sécuriser le réseau sans fil si le réseau sous-jacent n'est pas sécurisé. Cisco vous recommande de prendre les précautions suivantes :

- Protégez tous les ordinateurs sur le réseau et protégez individuellement les fichiers confidentiels par mot de passe.
- Changez les mots de passe à intervalles réguliers.
- Installez des logiciels antivirus et des logiciels de pare-feu individuels.
- Désactivez le partage de fichiers en point à point pour empêcher son utilisation par des applications sans votre accord.

Cisco RV215W - Réseaux sans fil

Le périphérique fournit quatre réseaux sans fil virtuels ou quatre SSID (Service Set Identifier) : ciscosb1, ciscosb2, ciscosb3 et ciscosb4. Il s'agit des noms ou SSID par défaut de ces réseaux, mais vous pouvez les renommer à votre guise.
Le tableau suivant décrit les paramètres par défaut de ces réseaux :

Nom du SSID	ciscosb1	ciscosb2	ciscosb3	ciscosb4
Activé	Oui	Non	Non	Non
Diffusion SSID	Activé	Désactivé	Désactivé	Désactivé
Mode de sécurité	Désactivé[1]	Désactivé	Désactivé	Désactivé

Nom du SSID	ciscosb1	ciscosb2	ciscosb3	ciscosb4
Filtre MAC	Désactivé	Désactivé	Désactivé	Désactivé
VLAN	1	1	1	1
Isolation sans fil avec SSID	Désactivé	Désactivé	Désactivé	Désactivé
WMM	Activé	Activé	Activé	Activé
Bouton matériel WPS	Activé	Désactivé	Désactivé	Désactivé

1. Lorsque vous utilisez l'Assistant d'installation, sélectionnez Sécurité optimale ou Meilleure sécurité pour protéger le périphérique contre les accès non autorisés.

Configuration des paramètres sans fil de base

Utilisez la page **Paramètres de base** (**Sans fil** > **Paramètres de base**) pour configurer les principaux paramètres sans fil.

Pour configurer les paramètres sans fil de base :

ÉTAPE 1 Sélectionnez **Sans fil** > **Paramètres de base**.

ÉTAPE 2 Dans le champ **Radio**, cochez la case **Activer** pour activer la radio sans fil. Par défaut, un seul réseau sans fil est activé, **ciscosb1**.

ÉTAPE 3 Dans le champ **Mode de réseau sans fil**, sélectionnez l'une des options suivantes dans le menu déroulant :

B/G/N mixte	Sélectionnez cette option si vous avez des appareils sans fil de type N, B et G sur votre réseau. Il s'agit de la valeur par défaut (recommandée).
B seulement	Sélectionnez cette option si vous n'avez que des appareils sans fil de type B sur votre réseau.

G seulement	Sélectionnez cette option si vous n'avez que des appareils sans fil de type G sur votre réseau.
N seulement	Sélectionnez cette option si vous n'avez que des appareils sans fil de type N sur votre réseau.
Mixte B/G	Sélectionnez cette option si vous n'avez que des appareils sans fil de type B et G sur votre réseau.
G/N mixte	Sélectionnez cette option si vous n'avez que des appareils sans fil de type G et N sur votre réseau.

ÉTAPE 4 Si vous choisissez **B/G/N mixte**, **N seulement** ou **Mixte G/N**, dans le champ **Sélection de bande sans fil**, sélectionnez la bande sans fil de votre réseau (**20 MHz** ou **20/40 MHz**). Si vous avez choisi N seulement, vous devez utiliser la sécurité WPA2 sur votre réseau. Reportez-vous à la section **Configuration du mode de sécurité**.

ÉTAPE 5 Dans le champ **Canal sans fil**, sélectionnez le canal sans fil dans le menu déroulant.

ÉTAPE 6 Dans le champ **VLAN de gestion PA**, sélectionnez **VLAN 1** si vous utilisez les paramètres par défaut.

Pour créer des VLAN supplémentaires, sélectionnez une valeur correspondant aux VLAN configurés sur d'autres commutateurs du réseau. Il s'agit d'une mesure de sécurité. Il peut également être nécessaire de changer le VLAN de gestion pour limiter l'accès au gestionnaire de dispositifs du périphérique.

ÉTAPE 7 (Facultatif) Dans le champ **U-APSD (économies d'énergie WMM)**, cochez la case **Activer** pour activer la fonction U-APSD (Unscheduled Automatic Power Save Delivery), également appelée WMM Power Save (économies d'énergie WMM), qui limite l'énergie consommée par les ondes radio.

U-APSD est un mécanisme d'économie d'énergie conçue pour les applications en temps réel, comme la VoIP, qui transfèrent les données en duplex intégral sur le réseau sans fil. En classifiant le trafic IP sortant en tant que données Voix, les applications de ce type peuvent améliorer l'autonomie d'environ 25 % tout en limitant les délais de transmission.

ÉTAPE 8 (Facultatif) Configurez les paramètres des quatre réseaux sans fil (voir la section **Modification des paramètres de réseau sans fil**).

ÉTAPE 9 Cliquez sur **Enregistrer**.

Modification des paramètres de réseau sans fil

La **Table sans fil** de la page **Paramètres de base** (**Sans fil** > **Paramètres de base**) présente les paramètres des quatre réseaux sans fil pris en charge par le périphérique.

Pour configurer ces paramètres de réseau sans fil :

ÉTAPE 1 Cochez les cases des réseaux que vous souhaitez configurer.

ÉTAPE 2 Cliquez sur le bouton **Modifier**.

ÉTAPE 3 Configurez les paramètres suivants :

Activer SSID	Cliquez sur **Activé** pour activer le réseau.
Nom SSID	Saisissez le nom du réseau.
Diffusion SSID	Cochez cette case pour activer la diffusion du SSID. Si la diffusion du SSID est activée, le routeur sans fil annonce sa disponibilité aux périphériques sans fil dans la plage du routeur.
VLAN	Sélectionnez le VLAN associé au réseau.
Isolation sans fil avec SSID	Cochez cette case pour activer l'isolation sans fil au sein du SSID.
WMM (Wi-Fi Multimedia)	Cochez cette case pour activer le WMM.
Bouton matériel WPS	Cochez cette case pour associer le bouton WPS de la façade du périphérique à ce réseau.

ÉTAPE 4 Cliquez sur **Enregistrer**.

Configuration du mode de sécurité

Vous pouvez configurer l'un des modes de sécurité suivant pour les réseaux sans fil.

Configuration de WEP

Le mode de sécurité WEP offre une sécurité faible en utilisant une méthode de cryptage simple et moins sûre que le WPA. La méthode WEP peut être nécessaire si vos appareils ne prennent pas en charge le WPA.

REMARQUE Si vous n'êtes pas obligé d'utiliser le WEP, nous vous conseillons d'utiliser le WPA2. Si vous utilisez le mode sans fil N seulement, vous devez activer WPA2.

Pour configurer le mode de sécurité WEP :

ÉTAPE 1 Dans la **Table sans fil** (**Sans fil** > **Paramètres de base**), cochez la case correspondant au réseau que vous souhaitez configurer.

ÉTAPE 2 Cliquez sur **Modifier le mode de sécurité**.

La page **Paramètres de sécurité** apparaît.

ÉTAPE 3 Dans le champ **Sélectionner un SSID**, sélectionnez le SSID dont vous souhaitez configurer les paramètres de sécurité.

ÉTAPE 4 Dans le menu **Mode de sécurité**, sélectionnez **WEP**.

ÉTAPE 5 Dans le champ **Type d'authentification**, sélectionnez l'une des options suivantes :

- **Système ouvert** : il s'agit de l'option par défaut.
- **Clé partagée** : sélectionnez cette option si votre administrateur réseau vous le demande. Dans le doute, sélectionnez l'option par défaut.

Dans les deux cas, les clients sans fil doivent fournir la bonne clé partagée (mot de passe) pour accéder au réseau sans fil.

ÉTAPE 6 Dans le champ **Chiffrement**, sélectionnez le type de cryptage :

- **10/64 bits (10 chiffres hexadécimaux) :** fournit une clé sur 40 bits.
- **26/128 bits (26 chiffres hexadécimaux)** : fournit une clé sur 104 bits dont le cryptage est plus difficile à décoder. Nous recommandons le cryptage sur 128 bits.

ÉTAPE 7 (Facultatif) Dans le champ **Mot de passe**, entrez une expression alphanumérique (de plus de huit caractères pour une sécurité optimale) et cliquez sur **Générer** pour créer quatre clés WEP uniques dans les champs Clé WEP.

Si vous préférez fournir votre propre clé, entrez-la directement dans le champ **Clé 1** (recommandé). La clé doit avoir une longueur de 5 caractères ASCII (ou 10 caractères hexadécimaux) pour le WEP 64 bits ou de 13 caractères ASCII (ou 26 caractères hexadécimaux) pour le WEP 128 bits. Les caractères hexadécimaux valables sont compris entre 0 et 9 et A et F.

ÉTAPE 8 Dans le champ **Clé transmise**, sélectionnez la clé que les appareils devront utiliser comme clé partagée pour accéder au réseau sans fil.

ÉTAPE 9 Cliquez sur **Enregistrer** pour enregistrer vos paramètres.

ÉTAPE 10 Cliquez sur **Retour** pour revenir à la page **Paramètres de base**.

Configuration des modes de sécurité WPA-Personnel, WPA2-Personnel et WPA2-Personnel mixte

Les modes de sécurité WPA Personnel, WPA2 Personnel et WPA2 Personnel mixte offrent un niveau de sécurité renforcé qui remplace le WEP.

- **WPA-Personnel** : WPA fait partie de la norme de sécurité sans fil (802.11i) homologuée par la Wi-Fi Alliance. Elle a été conçue en tant que standard intermédiaire pour remplacer le WEP pendant l'élaboration de la norme 802.11i. WPA-Personnel est compatible avec le cryptage TKIP (Temporal Key Integrity Protocol) et AES (Advanced Encryption Standard).
- **WPA2-Personnel** : (Recommandé) WPA2 est la norme de sécurité spécifiée par le standard 802.11i finalisé. WPA2 prend en charge le cryptage AES et utilise une clé prépartagée (PSK) pour l'authentification.
- **WPA2-Personnel mixte** : permet aux clients WPA et WPA2 de se connecter simultanément en utilisant l'authentification PSK.

L'authentification personnelle correspond à la clé prépartagée qui est un mot de passe alphanumérique partagé avec le poste sans fil.

Pour configurer le mode de sécurité WPA Personnel :

ÉTAPE 1 Dans la **Table sans fil** (**Sans fil** > **Paramètres de base**), cochez la case correspondant au réseau que vous souhaitez configurer.

ÉTAPE 2 Cliquez sur **Modifier le mode de sécurité**. La page **Paramètres de sécurité** apparaît.

ÉTAPE 3 Dans le champ **Sélectionner un SSID**, sélectionnez le SSID dont vous souhaitez configurer les paramètres de sécurité.

ÉTAPE 4 Dans le menu **Mode de sécurité**, sélectionnez l'une des trois options WPA Personnel.

ÉTAPE 5 (WPA-Personnel seulement) Dans le champ **chiffrement**, sélectionnez l'une des options suivantes :

- **TKIP/AES** : sélectionnez **TKIP/AES** pour assurer la compatibilité avec des appareils sans fil plus anciens qui ne prennent pas nécessairement en charge AES.
- **AES** : cette option est plus sûre.

ÉTAPE 6 Dans le champ **Clé de sécurité**, entrez une expression alphanumérique (comprenant entre 8 à 63 caractères ASCII ou 64 chiffres hexadécimaux). La jauge de sécurité des mots de passe indique la robustesse de la clé : Inférieur au seuil minimal, Faible, Robuste, Très robuste ou Sécurisé. Nous vous recommandons d'utiliser une clé de sécurité considérée comme sécurisée sur la jauge.

ÉTAPE 7 Pour afficher la clé de sécurité à mesure que vous la saisissez, cochez la case **Afficher le mot de passe**.

ÉTAPE 8 Dans le champ **Renouvellement de clé**, entrez l'intervalle de renouvellement de la clé (de 600 à 7 200 secondes). La valeur par défaut est 3600.

ÉTAPE 9 Cliquez sur **Enregistrer** pour enregistrer vos paramètres.

ÉTAPE 10 Cliquez sur **Retour** pour revenir à la page **Paramètres de base**.

Configuration des modes WPA-Entreprise, WPA2-Entreprise et WPA2-Entreprise mixte

Les modes de sécurité WPA-Entreprise, WPA2-Entreprise et WPA2-Entreprise mixte permettent d'utiliser l'authentification serveur RADIUS.

- **WPA-Entreprise** : permet d'utiliser le WPA avec authentification serveur RADIUS.
- **WPA2-Entreprise** : permet d'utiliser le WPA2 avec authentification serveur RADIUS.
- **WPA2-Entreprise mixte** : permet aux clients WPA et WPA2 de se connecter simultanément en utilisant l'authentification RADIUS.

Pour configurer le mode de sécurité WPA-Entreprise :

ÉTAPE 1 Dans la **Table sans fil** (**Sans fil** > **Paramètres de base**), cochez la case correspondant au réseau que vous souhaitez configurer.

ÉTAPE 2 Cliquez sur **Modifier le mode de sécurité**.

ÉTAPE 3 Dans le champ **Sélectionner un SSID**, sélectionnez le SSID dont vous souhaitez configurer les paramètres de sécurité.

ÉTAPE 4 Dans le menu **Mode de sécurité**, sélectionnez l'une des trois options WPA-Entreprise.

ÉTAPE 5 (WPA-Entreprise seulement) Dans le champ **Chiffrement**, sélectionnez l'une des options suivantes :

- **TKIP/AES** : sélectionnez **TKIP/AES** pour assurer la compatibilité avec des appareils sans fil plus anciens qui ne prennent pas nécessairement en charge AES.
- **AES** : cette option offre une meilleure sécurité.

ÉTAPE 6 Dans le champ **Serveur RADIUS**, entrez l'adresse IP du serveur RADIUS.

ÉTAPE 7 Dans le champ **Port RADIUS**, entrez le port utilisé pour accéder au serveur RADIUS.

ÉTAPE 8 Dans le champ **Clé partagée**, entrez une expression alphanumérique.

ÉTAPE 9 Dans le champ **Renouvellement de clé**, entrez l'intervalle de renouvellement de la clé (de 600 à 7 200 secondes). La valeur par défaut est 3600.

ÉTAPE 10 Cliquez sur **Enregistrer** pour enregistrer vos paramètres.

ÉTAPE 11 Cliquez sur **Retour** pour revenir à la page **Paramètres de base**.

Configuration du filtrage MAC

Vous pouvez utiliser le filtrage MAC pour accorder ou refuser l'accès au réseau sans fil en fonction de l'adresse MAC (matérielle) de l'appareil qui demande l'accès. Vous pouvez par exemple entrer les adresses MAC d'un ensemble d'ordinateurs et n'autoriser l'accès au réseau qu'à ces ordinateurs. Vous pouvez configurer le filtrage MAC pour chaque réseau ou SSID.

Pour configurer le filtrage MAC :

ÉTAPE 1 Dans la **Table sans fil** (**Sans fil** > **Paramètres de base**), cochez la case correspondant au réseau que vous souhaitez configurer.

ÉTAPE 2 Cliquez sur **Modifier le filtrage MAC**. La page **Filtre MAC sans fil** apparaît.

ÉTAPE 3 Dans le champ **Modifier le filtrage MAC**, cochez la case **Activer** pour activer le filtrage MAC pour le SSID actuel.

ÉTAPE 4 Dans le champ **Contrôle de la connexion**, sélectionnez le type d'accès au réseau sans fil :

- **Interdire** : sélectionnez cette option pour empêcher les appareils dont les adresses MAC sont incluses dans la **Table d'adresses MAC** d'accéder au réseau sans fil. Cette option est sélectionnée par défaut.
- **Autoriser** : sélectionnez cette option pour autoriser les appareils dont les adresses MAC sont incluses dans la **Table d'adresses MAC** à accéder au réseau sans fil.

ÉTAPE 5 Pour afficher les ordinateurs et autres appareils sur le réseau sans fil, cliquez sur **Afficher la liste des clients**.

ÉTAPE 6 Dans le champ **Enregistrer dans la liste de filtrage des adresses MAC**, cochez la case pour ajouter le routeur à la liste des appareils à ajouter à la **Table d'adresses MAC**.

ÉTAPE 7 Cliquez sur **Ajouter à l'adresse MAC** pour ajouter les appareils sélectionnés à la **Table de la liste des clients** de la **Table d'adresses MAC**.

ÉTAPE 8 Cliquez sur **Enregistrer** pour enregistrer vos paramètres.

ÉTAPE 9 Cliquez sur **Retour** pour revenir à la page **Paramètres de base**.

Configuration de l'accès par horaire

Pour renforcer la protection de votre réseau, vous pouvez restreindre l'accès en spécifiant les heures auxquelles les utilisateurs peuvent accéder au réseau.

Pour configurer l'accès par horaire :

ÉTAPE 1 Dans la **Table sans fil** (**Sans fil** > **Paramètres de base**), cochez la case correspondant au réseau que vous souhaitez configurer.

ÉTAPE 2 Cliquez sur **Accès par horaire**. La page Accès par horaire apparaît.

ÉTAPE 3 Dans le champ **Durée d'activité**, cochez la case **Activer** pour activer l'accès par horaire.

ÉTAPE 4 Dans les champs **Heure de début** et **Heure de fin**, spécifiez la plage horaire durant laquelle l'accès au réseau sera autorisé.

ÉTAPE 5 Cliquez sur **Enregistrer**.

Configuration du réseau invité sans fil

Le périphérique prend en charge un réseau invité sans fil qui est distinct des autres SSID, ou réseaux, sans fil sur le routeur. Ce routeur assure un accès invité sécurisé qui est isolé du reste du réseau et qui peut être configuré pour restreindre le temps d'accès et la bande passante utilisée. Les restrictions et les recommandations de configuration suivantes s'appliquent :

- Un réseau invité peut être configuré pour chaque périphérique.
- Le réseau invité est configuré en tant que l'un des quatre SSID disponibles sur le périphérique.
- Il n'est pas possible de configurer le réseau invité sur le VLAN de gestion PA (ID de VLAN 1).

Pour configurer le réseau invité :

Créer un VLAN

ÉTAPE 1 Dans l'interface de gestion, sélectionnez **Mise en réseau** > **LAN** > **Membres du réseau VLAN**.

ÉTAPE 2 Dans la table des paramètres de réseau VLAN, ajoutez un nouveau VLAN pour le réseau invité. Par exemple, cliquez sur **Ajouter une ligne** et entrez ce qui suit :

- **ID de VLAN** : entrez un numéro pour le VLAN (par exemple, **4**).
- **Description** : entrez le nom du VLAN (par exemple, **réseau-invité**).

ÉTAPE 3 Conservez les **balises** des ports et cliquez sur **Enregistrer**.

Configurer le réseau invité

ÉTAPE 1 Dans l'interface de gestion, choisissez **Sans fil** > **Paramètres de base**.

ÉTAPE 2 Dans la Table sans fil, choisissez le SSID ou le réseau que vous voulez désigner comme réseau invité.

ÉTAPE 3 Cliquez sur **Modifier**. Modifiez le nom du SSID pour qu'il reflète la désignation « invité » (par exemple, *réseau-invité*).

ÉTAPE 4 Cochez la case **Diffusion SSID** pour que le réseau apparaisse en tant que connexion sans fil pour les clients recherchant des réseaux.

ÉTAPE 5 Cochez la case **Réseau invité** pour configurer ce SSID en tant que réseau invité.

ÉTAPE 6 Choisissez le VLAN que vous avez créé pour le réseau invité (ou, si vous n'avez pas encore créé de réseau, sélectionnez **Ajouter un VLAN**).

ÉTAPE 7 Cliquez sur **Enregistrer**. Le système vous indique que les ports Ethernet physiques sur le périphérique sont exclus du VLAN que vous avez attribué au réseau invité. En outre, l'isolation sans fil avec SSID et WMM sont automatiquement activés.

Configurer le mot de passe et d'autres options

ÉTAPE 1 Dans l'interface de gestion, choisissez **Sans fil** > **Paramètres de base**.

ÉTAPE 2 Sous la Table sans fil, cliquez sur **Modifier le réseau invité**.

ÉTAPE 3 Entrez un mot de passe que les utilisateurs devront fournir pour se connecter au réseau invité.

ÉTAPE 4 Ressaisissez le mot de passe pour le confirmer.

ÉTAPE 5 Entrez la durée, en minutes, pendant laquelle la connexion invitée sera disponible pour les utilisateurs.

ÉTAPE 6 (Facultatif) Pour restreindre l'utilisation de la bande passante par le réseau invité, cochez **Activer la restriction de bande passante invité**. (La qualité de service (QoS) doit d'abord être activée. Cliquez sur le lien vers la page Gestion de la bande passante si vous devez configurer la qualité de service.) Dans le champ **Bande passante disponible**, entrez le pourcentage de bande passante à allouer au réseau invité.

ÉTAPE 7 Cliquez sur **Enregistrer**.

Configuration des paramètres sans fil avancés

Les paramètres sans fil avancés sont réservés à un administrateur expert, car un mauvais réglage peut diminuer les performances sans fil.

Pour configurer les paramètres sans fil avancés :

ÉTAPE 1 Sélectionnez **Sans fil** > **Paramètres avancés**. La page Paramètres avancés apparaît.

ÉTAPE 2 Configurez les paramètres suivants :

Rafale de trames	Activez cette option pour accélérer les performances de vos réseaux sans fil, en fonction du fabricant de vos appareils réseau. Si vous n'êtes pas sûr de la manière d'exploiter cette option, conservez l'état par défaut (activé).
Aucune validation WMM	Cliquez pour activer cette fonctionnalité. L'activation de l'option Aucune validation WMM peut entraîner une amélioration du débit, mais aussi du taux d'erreurs dans un environnement hautes fréquences (RF) saturé. Cette option est par défaut désactivée.
Vitesse de base	Le paramètre Vitesse de base ne correspond pas à la vitesse de transmission, mais à une série de débits de transmission de la plateforme Services Ready Platform. Le périphérique annonce son débit de base aux autres appareils sur le réseau, afin qu'ils connaissent les débits qui seront utilisés. La plate-forme Services Ready Platform annonce également qu'elle sélectionnera automatiquement le meilleur débit de transmission. Le paramètre par défaut est Par défaut, lorsque le périphérique peut transmettre à tous les débits sans fil standard (1 Mbit/s, 2 Mbit/s, 5,5 Mbit/s, 11 Mbit/s, 18 Mbit/s, 24 Mbit/s, 36 Mbit/s, 48 Mbit/s et 54 Mbit/s). Le périphérique prend en charge les débits N en plus des débits B et G. L'option 1-2 Mbit/s sert aux anciennes technologies sans fil et l'option Tout lorsque le périphérique peut transmettre à toutes les vitesses sans fil. Le débit de base ne correspond pas à la vitesse réelle de transmission des données. Si vous souhaitez spécifier le débit de transmission des données du périphérique, configurez le paramètre Vitesse de transmission.

Vitesse de transmission	Vous devez régler la vitesse de transmission en fonction de la vitesse de votre réseau sans fil. Vous pouvez effectuer une sélection dans une plage de vitesses de transmission ou sélectionner **Automatique** pour que le périphérique utilise automatiquement le débit de données le plus rapide et pour activer la fonctionnalité de négociation automatique. La fonction de négociation automatique négocie la meilleure vitesse de connexion possible entre le périphérique et un client sans fil. La valeur par défaut est Automatique.
Vitesse de transmission N	Vous devez régler la vitesse de transmission en fonction de la vitesse de votre réseau sans fil de type N. Vous pouvez effectuer une sélection dans une plage de vitesses de transmission ou sélectionner **Automatique** pour que le périphérique utilise automatiquement le débit de données le plus rapide et pour activer la fonctionnalité de négociation automatique. La fonction de négociation automatique négocie la meilleure vitesse de connexion possible entre le périphérique et un client sans fil. La valeur par défaut est Automatique.
Mode de protection CTS	Le périphérique utilise automatiquement le mode de protection CTS (Clear-To-Send) si vos appareils sans fil de type N et G rencontrent des problèmes et ne parviennent pas à transmettre vers le périphérique lorsque le trafic 802.11b environnant est très important. Cette fonction renforce la capacité du périphérique à capter les transmissions sans fil de type N et G, au prix d'une diminution considérable des performances. La valeur par défaut est Automatique.
Beacon Interval	Cette valeur indique la fréquence d'émission de la balise. Une balise est un paquet diffusé par le périphérique pour permettre la synchronisation du réseau sans fil. Entrez une valeur comprise entre 40 et 3500 millisecondes. La valeur par défaut est 100.

Intervalle DTIM	Cette valeur comprise entre 1 et 255 correspond à l'intervalle du message DTIM (Delivery Traffic Indication Message). Un champ DTIM est un champ de compte à rebours qui informe les clients de la prochaine fenêtre d'écoute des messages de diffusion et de multidiffusion. Lorsque les messages de diffusion ou de multidiffusion pour les clients associés sont stockés dans la mémoire tampon du périphérique, celui-ci envoie le message DTIM suivant avec une valeur d'intervalle DTIM. Les clients entendent les balises et sortent de veille pour recevoir les messages de diffusion ou de multidiffusion. La valeur par défaut est 1.
Seuil de fragmentation	Cette valeur spécifie la taille maximale d'un paquet au-delà de laquelle les données sont scindées en plusieurs paquets. Si vous rencontrez une quantité importante d'erreurs de paquets, essayez d'augmenter légèrement le seuil de fragmentation. Un réglage trop faible du seuil de fragmentation peut dégrader les performances du réseau. Seule une légère réduction de la valeur par défaut est recommandée. Dans la majorité des cas, conservez la valeur par défaut de 2346.
Seuil RTS	En cas de flux de données intermittent, essayez une réduction mineure. La valeur par défaut de 2347 est recommandée. Lorsque la taille d'un paquet réseau est inférieure au seuil RTS (Request to Send) prédéfini, le mécanisme RTS/CTS (Clear to Send) n'est pas enclenché. La plate-forme Services Ready Platform envoie des trames RTS à une station de réception et négocie l'envoi d'une trame de données. Après réception d'un RTS, la station sans fil répond par une trame CTS pour autoriser le début de la transmission.

ÉTAPE 3 Cliquez sur **Enregistrer**.

Configuration de WDS

Un WDS (Wireless Distribution System) est un système qui permet l'interconnexion sans fil de points d'accès sur un réseau. Il permet l'extension d'un réseau sans fil à l'aide de plusieurs points d'accès sans recours à un réseau filaire pour les relier.

Pour établir une liaison WDS, le périphérique ainsi que d'autres postes WDS distants doivent être configurés pour utiliser le même mode de réseau sans fil, canal sans fil, bande sans fil et types de cryptage (aucun ou WEP).

WDS est pris en charge sur un seul SSID.

Pour configurer un WDS :

ÉTAPE 1 Sélectionnez **Sans fil** > **WDS**.

ÉTAPE 2 Cochez la case **Autoriser la répétition du signal sans fil à l'aide d'un répéteur** pour activer le WDS.

ÉTAPE 3 Pour entrer manuellement l'adresse MAC d'un répéteur, cliquez sur **Manuel** ou choisissez **Automatique** pour que le routeur détecte automatiquement les points d'accès distants.

Pour sélectionner des répéteurs dans la table des réseaux disponibles, cliquez sur **Afficher l'analyse du site** afin d'afficher la **Table des réseaux disponibles**.

a. Cochez les cases afin de sélectionner jusqu'à trois points d'accès qui serviront de répéteurs.

b. Cliquez sur **Connexion** pour ajouter les adresses MAC des points d'accès sélectionnés au champ MAC.

Vous pouvez également entrer les adresses MAC pour trois points d'accès à utiliser comme répéteurs dans les champs **MAC 1**, **MAC 2** et **MAC 3**.

ÉTAPE 4 Cliquez sur **Enregistrer**.

Configuration de WPS

Configurez le WPS (Wi-Fi Protected Setup) pour permettre aux appareils compatibles WPS de se connecter aisément et en toute sécurité au réseau sans fil. Reportez-vous à la documentation de votre appareil client pour en savoir plus sur sa configuration WPS.

Pour configurer WPS :

ÉTAPE 1 Sélectionnez **Sans fil** > **WPS**. La page Configuration Wi-Fi protégée s'affiche.

ÉTAPE 2 Sélectionnez le réseau sans fil sur lequel vous souhaitez activer le WPS dans le menu déroulant **SSID**.

ÉTAPE 3 Cochez la case **Activer WPS** pour activer le WPS. Décochez la case pour désactiver le WPS.

ÉTAPE 4 Configurez le WPS sur les appareils clients de l'une des trois manières suivantes :

a. Cliquez ou appuyez sur le bouton WPS de l'appareil client, puis cliquez sur l'icône WPS de cette page.

b. Entrez le code PIN du WPS du client, puis cliquez sur **S'inscrire**.

c. Entrez le code PIN du routeur ; utilise le code PIN du routeur indiqué.

État du code PIN de l'appareil : état du numéro d'identification personnel (PIN) de l'appareil WPA.

Code PIN de l'appareil : identifie le code PIN d'un appareil essayant de se connecter.

Durée de vie du code PIN : durée de vie de la clé. À l'expiration de cette période, une nouvelle clé est négociée.

Une fois que vous avez configuré le WPS, les informations suivantes sont affichées au bas de la page **WPS** : État de la configuration Wi-Fi protégée, Nom du réseau (SSID) et Sécurité.

5

Configuration du pare-feu

Ce chapitre présente la procédure à suivre pour configurer les propriétés de pare-feu du périphérique.

- **Fonctions de pare-feu du routeur Cisco RV215W**
- **Configuration des paramètres de base du pare-feu**
- **Gestion des plannings de pare-feu**
- **Configuration de la gestion de services**
- **Configuration des règles d'accès**
- **Création d'une stratégie d'accès à Internet**
- **Configuration de la redirection de ports**

Fonctions de pare-feu du routeur Cisco RV215W

Vous pouvez sécuriser votre réseau en créant et en appliquant des règles utilisées par le routeur pour bloquer et autoriser du trafic Internet entrant et sortant. Vous spécifiez ensuite les appareils concernés par les règles. Pour ce faire, vous devez définir les éléments suivants :

- Services et types de trafic (exemples : navigation Web, VoIP, autres services standard et services personnalisés que vous définissez) que le routeur doit autoriser ou bloquer
- Direction du trafic en spécifiant la source et la destination du trafic, à savoir la Zone source (LAN/WAN/DMZ) et la Zone cible (LAN/WAN/DMZ).
- Plannings d'application des règles par le routeur
- Mots clés (d'un nom de domaine ou d'une adresse URL d'une page Web) que le routeur doit autoriser ou bloquer

- Règles autorisant ou bloquant le trafic Internet entrant et sortant pour certains services à certaines heures
- Adresses MAC des appareils dont les accès entrants doivent être bloqués par le routeur
- Déclencheurs de ports qui indiquent au routeur d'autoriser ou de bloquer l'accès à certains services définis par leur numéro de port
- Rapports et alertes que vous souhaitez recevoir du routeur

Vous pouvez par exemple définir des règles d'accès restreint en fonction d'un planning, d'une adresse Web ou de mots clés d'adresses Web. Vous pouvez bloquer l'accès Internet d'applications et de services sur le réseau local (LAN), comme les forums de discussion ou les jeux. Vous pouvez bloquer l'accès par le réseau étendu (WAN) ou la DMZ publique à certains groupes d'ordinateurs de votre réseau.

Les règles entrantes (WAN vers LAN/DMZ) limitent l'accès du trafic entrant sur votre réseau, n'autorisant l'accès à certaines ressources locales qu'à certains utilisateurs externes. Par défaut, tous les accès au réseau LAN sécurisé provenant du réseau WAN non sécurisé sont bloqués, à l'exception des réponses aux requêtes provenant du LAN ou de la DMZ. Pour autoriser des appareils externes à accéder à des services sur le LAN sécurisé, vous devez définir une règle de pare-feu pour chaque service.

Si vous souhaitez autoriser le trafic entrant, l'adresse IP du port WAN du routeur doit être rendue publique. Cela s'appelle « exposition de l'hôte ». La manière de rendre votre adresse publique dépend de la façon dont les ports WAN sont configurés. Sur le routeur, vous pouvez utiliser l'adresse IP si une adresse statique est affectée au port WAN, ou un nom DDNS (DNS dynamique) si l'adresse de votre WAN est dynamique.

Les règles sortantes (LAN/DMZ vers WAN) limitent l'accès du trafic sortant de votre réseau, n'autorisant l'accès à certaines ressources externes qu'à certains utilisateurs locaux. La règle sortante par défaut est d'autoriser l'accès depuis la zone sécurisée (LAN) à la DMZ publique ou au WAN non sécurisé. Pour bloquer l'accès à Internet (WAN non sécurisé) par des hôtes du LAN sécurisé, vous devez créer une règle de pare-feu pour chaque service.

Configuration des paramètres de base du pare-feu

Pour configurer les paramètres de base du pare-feu :

ÉTAPE 1 Sélectionnez **Pare-feu** > **Paramètres de base**.

ÉTAPE 2 Configurez les paramètres de pare-feu suivants :

Pare-feu	Cochez la case **Activer** pour pouvoir configurer les paramètres du pare-feu.
Protection DoS	Cochez la case **Activer** pour activer la protection contre les attaques de déni de service (DoS ou Denial of Service).
Bloquer la requête WAN	Bloque les requêtes ping qui parviennent au routeur depuis le WAN.
Accès Web	Sélectionnez le type d'accès Web autorisé pour la connexion au pare-feu : HTTP ou HTTPS (HTTP sécurisé).
Gestion à distance **Accès à distance** **Mise à niveau à distance** **Adresse IP distante autorisée** **Port de gestion à distance**	Reportez-vous à la section **Configuration de la gestion à distance**.
Intercommunication de multidiffusion IPv4 (proxy IGMP)	Cochez la case **Activer** pour activer l'intercommunication de multidiffusion pour IPv4.
Intercommunication de multidiffusion IPv6 (proxy IGMP)	Cochez la case **Activer** pour activer l'intercommunication de multidiffusion pour IPv6.

UPnP **Autoriser la configuration par les utilisateurs** **Autoriser les utilisateurs à désactiver l'accès à Internet**	Reportez-vous à la section **Configuration de la fonction Universal Plug and Play**.
Bloquer Java	Cochez la case pour bloquer les applets Java. Les applets Java sont de petits programmes intégrés aux pages Web qui activent des fonctions dynamiques de la page. Un applet malveillant peut servir à compromettre ou infecter un ordinateur. Activez ce paramètre pour bloquer le téléchargement des applets Java. Cliquez sur **Automatique** pour bloquer Java automatiquement ou sur **Manuel** pour spécifier un port sur lequel Java doit être bloqué.
Bloquer les cookies	Cochez la case pour bloquer les cookies. Les sites Web utilisent les cookies pour stocker des informations de session. Toutefois, certains sites Web utilisent les cookies pour surveiller l'utilisateur et ses habitudes de navigation. Activez cette option pour empêcher la création de cookies par les sites Web. De nombreux sites Web ne sont pas accessibles lorsque les cookies sont refusés. Le blocage des cookies peut donc entraîner le dysfonctionnement de ces sites. Cliquez sur **Automatique** pour bloquer automatiquement les cookies ou sur **Manuel** pour spécifier un port sur lequel les cookies doivent être bloqués.

Bloquer ActiveX	Cochez la case pour bloquer le contenu ActiveX. Les contrôles ActiveX, similaires aux applets Java, sont installés sur les ordinateurs Windows qui utilisent Internet Explorer. Les contrôles ActiveX malveillants peuvent servir à compromettre ou infecter un ordinateur. Activez ce paramètre pour bloquer le téléchargement des contrôles ActiveX. Cliquez sur **Automatique** pour bloquer ActiveX automatiquement ou sur **Manuel** pour spécifier un port sur lequel ActiveX doit être bloqué.
Bloquer le proxy	Cochez la case pour bloquer les serveurs proxy. Un serveur mandataire ou proxy permet à un ordinateur d'acheminer les connexions aux autres ordinateurs par le biais du proxy, contournant ainsi certaines règles de pare-feu. Par exemple, lorsque les connexions à une adresse IP spécifique sont bloquées par une règle de pare-feu, ces requêtes peuvent être acheminées par le biais d'un proxy qui n'est pas bloqué par la règle, contournant ainsi la règle concernée. Activez cette option pour bloquer les serveurs proxy. Cliquez sur **Automatique** pour bloquer automatiquement les serveurs proxy ou sur **Manuel** pour spécifier un port sur lequel les serveurs proxy doivent être bloqués.
ALG FTP	Cliquez sur **Automatique** pour utiliser le port FTP 21 par défaut. Cliquez sur **Manuel** pour entrer le numéro de port vers lequel vous voulez diriger le trafic FTP sur le routeur.

ÉTAPE 3 Cliquez sur **Enregistrer**.

Configuration de la gestion à distance

Activez la gestion à distance pour pouvoir accéder au routeur à partir d'un réseau WAN distant.

Pour configurer la gestion à distance, configurez les règles suivantes sur la page **Paramètres de base** :

Gestion à distance	Cochez la case **Activer** pour activer la gestion à distance.
Accès à distance	Sélectionnez le type d'accès Web autorisé pour la connexion au pare-feu : HTTP ou HTTPS (HTTP sécurisé).
Mise à niveau à distance	Pour autoriser la mise à niveau à distance du routeur, cochez la case **Activer**.
Adresse IP distante autorisée	Cliquez sur le bouton **Toute adresse IP** pour autoriser la gestion à distance à partir de toute adresse IP ou indiquez une adresse IP spécifique dans le champ d'adresse.
Port de gestion à distance	Entrez le port sur lequel l'accès distant est autorisé. Le port par défaut est 443. Lorsque vous accédez au routeur à distance, vous devez entrer le port de gestion à distance dans le cadre de l'adresse IP. Exemple : **https://<ip-distante>:<port-distant>** ou **https://168.10.1.11:443**

ATTENTION Lorsque la gestion à distance est activée, le routeur est accessible par tout utilisateur qui connaît l'adresse IP correspondante. Étant donné qu'un utilisateur malveillant connecté au WAN peut reconfigurer le routeur et en faire un mauvais usage, nous vous conseillons vivement de modifier le mot de passe administrateur et le mot de passe invité avant de continuer.

Configuration de la fonction Universal Plug and Play

Universal Plug and Play (UPnP) permet la découverte automatique d'appareils capables de communiquer avec le routeur.

Pour configurer l'UPnP, configurez les règles suivantes sur la page **Paramètres de base** :

UPnP	Cochez la case **Activer** pour activer le protocole UPnP.
Autoriser la configuration par les utilisateurs	Cochez cette case pour autoriser la définition de règles de correspondances de ports UPnP par les utilisateurs utilisant des ordinateurs ou d'autres appareils compatibles UPnP. Lorsque la case est décochée, le routeur n'autorise pas les applications à ajouter des règles de transfert.
Autoriser les utilisateurs à désactiver l'accès à Internet	Cochez cette case pour autoriser les utilisateurs à désactiver l'accès à Internet.

Gestion des plannings de pare-feu

Vous pouvez créer des plannings afin d'appliquer les règles de pare-feu certains jours ou à certaines heures de la journée.

Ajout ou modification d'un planning de pare-feu

Pour créer ou modifier un planning :

ÉTAPE 1 Sélectionnez **Pare-feu** > **Gestion des horaires**.

ÉTAPE 2 Cliquez sur **Ajouter une ligne**.

ÉTAPE 3 Dans le champ **Nom**, entrez un nom unique pour identifier le planning. Le nom est disponible dans la liste **Sélectionner un planning** sur la page de configuration des règles de pare-feu. (Reportez-vous à la section **Configuration des règles d'accès**.)

ÉTAPE 4 Sous **Jours planifiés**, indiquez si vous souhaitez appliquer le planning à certains jours ou tous les jours. Si vous sélectionnez **Certains jours**, cochez les cases en regard des jours que vous souhaitez inclure dans le planning.

ÉTAPE 5 Sous **Heures planifiées**, sélectionnez la plage horaire à appliquer par le planning. Sélectionnez **Tout le temps** ou **À certaines heures**. Si vous choisissez **À certaines heures**, entrez l'heure de début et l'heure de fin.

ÉTAPE 6 Cliquez sur **Enregistrer**.

Configuration de la gestion de services

Lorsque vous créez une règle de pare-feu, vous pouvez spécifier un service contrôlé par la règle. Différents types de services courants sont disponibles et vous pouvez créer vos propres services.

La page **Gestion des services** permet de créer des services personnalisés auxquels les règles de pare-feu sont appliquées. Une fois défini, le nouveau service apparaît dans la **liste** des **services personnalisés disponibles**.

Pour créer un service personnalisé :

ÉTAPE 1 Sélectionnez **Pare-feu** > **Gestion des services**.

ÉTAPE 2 Cliquez sur **Ajouter une ligne**.

ÉTAPE 3 Dans le champ **Nom du service**, entrez le nom du service pour pouvoir l'identifier plus tard.

ÉTAPE 4 Dans le champ **Protocole**, sélectionnez le protocole Layer 4 utilisé par le service dans le menu déroulant :

- **TCP**
- **UDP**
- **TCP et UDP**
- **ICMP**

ÉTAPE 5 Dans le champ **Port de début**, entrez le premier port TCP ou UDP de la plage utilisée par le service.

ÉTAPE 6 Dans le champ **Port de fin**, entrez le dernier port TCP ou UDP de la plage utilisée par le service.

ÉTAPE 7 Cliquez sur **Enregistrer**.

Pour modifier une entrée, sélectionnez-la et cliquez sur **Modifier**. Apportez les modifications voulues, puis cliquez sur **Enregistrer**.

Configuration des règles d'accès

Configuration de la stratégie appliquée par défaut au trafic sortant

La page **Règles d'accès** permet de configurer la stratégie sortante par défaut pour le trafic acheminé du réseau sécurisé (LAN) vers le réseau non sécurisé (WAN dédié/facultatif).

La stratégie entrante par défaut pour le trafic provenant de la zone non sécurisée en direction de la zone sécurisée est toujours bloquée et ne peut pas être modifiée.

Pour configurer la stratégie sortante par défaut :

ÉTAPE 1 Sélectionnez **Pare-feu** > **Règles d'accès**.

ÉTAPE 2 Sélectionnez **Autoriser** ou **Refuser**.

Remarque : vérifiez que la prise en charge d'IPv6 est activée sur le routeur pour configurer un pare-feu IPv6. Reportez-vous à la section **Configuration d'IPv6**.

ÉTAPE 3 Cliquez sur **Enregistrer**.

Réorganisation des règles d'accès

L'ordre dans lequel les règles d'accès sont affichées dans la table des règles d'accès indique l'ordre dans lequel elles sont appliquées. Vous pouvez réorganiser la table pour que certaines règles s'appliquent avant d'autres. Par exemple, si vous voulez appliquer une règle qui autorise certains types de trafic avant de bloquer d'autres types de trafic.

Pour réorganiser les règles d'accès :

ÉTAPE 1 Sélectionnez **Pare-feu** > **Règles d'accès**.

ÉTAPE 2 Cliquez sur **Réorganiser**.

ÉTAPE 3 Cochez la case dans la ligne de la règle que vous souhaitez déplacer vers le haut ou le bas et cliquez sur la flèche vers le haut ou le bas pour déplacer la règle d'une ligne vers le haut ou vers le bas ou sélectionnez la position voulue de la règle dans la liste déroulante et cliquez sur **Déplacer vers**.

ÉTAPE 4 Cliquez sur **Enregistrer**.

Ajout de règles d'accès

Toutes les règles de pare-feu configurées sur le routeur sont affichées dans la **table des règles d'accès**. Cette liste indique également si la règle est activée et présente les zones « source/cible » ainsi que les services et utilisateurs concernés par la règle.

Pour créer une règle d'accès :

ÉTAPE 1 Sélectionnez **Pare-feu** > **Règles d'accès**.

ÉTAPE 2 Cliquez sur **Ajouter une ligne**.

ÉTAPE 3 Dans le champ **Type de connexion**, sélectionnez la direction du trafic :

- **Sortant (LAN > WAN)** : sélectionnez cette option pour créer une règle sortante.
- **Entrant (WAN > LAN)** : sélectionnez cette option pour créer une règle entrante.
- **Entrant (WAN > DMZ)** : sélectionnez cette option pour créer une règle entrante.

ÉTAPE 4 Sélectionnez une action dans le menu déroulant **Action** :

- **Toujours bloquer** : toujours bloquer le type de trafic sélectionné.
- **Toujours autoriser** : ne jamais bloquer le type de trafic sélectionné.
- **Bloquer selon un horaire, sinon autoriser** : bloque le type de trafic sélectionné en fonction d'un planning spécifique.
- **Autoriser selon un horaire, sinon bloquer** : autorise le type de trafic sélectionné en fonction d'un planning spécifique.

ÉTAPE 5 Dans le menu déroulant **Services**, sélectionnez le service à autoriser ou bloquer pour cette règle. Sélectionnez **Tout le trafic** pour appliquer la règle à tous les services et applications ou sélectionnez une application particulière à bloquer :

- DNS (Domain Name System), UDP ou TCP
- FTP (File Transfer Protocol)
- HTTP (Hypertext Transfer Protocol)
- HTTPS (Secure Hypertext Transfer Protocol)
- TFTP (Trivia File Transfer Protocol)
- IMAP (Internet Message Access Protocol)
- NNTP (Network News Transport Protocol)
- POP3 (Post Office Protocol)
- SNMP (Simple Network Management Protocol)
- SMTP (Simple Mail Transfer Protocol)
- Telnet
- STRMWORKS
- TACACS (Terminal Access Controller Access-Control System)
- Telnet (commande)
- Telnet secondaire
- Telnet SSL
- Voix (SIP)

ÉTAPE 6 (Facultatif) Cliquez sur **Configurer les services** pour aller sur la page **Gestion des services** afin de définir les services avant de leur appliquer des règles d'accès.

Pour plus d'informations, reportez-vous à la section **Configuration de la gestion de services**.

ÉTAPE 7 Dans le champ **Adresse IP source**, sélectionnez les utilisateurs auxquels appliquer la règle de pare-feu :

- **Tout** : la règle s'applique au trafic provenant de tout hôte du réseau local.
- **Adresse individuelle** : la règle s'applique au trafic provenant d'une adresse IP spécifique du réseau local. Saisissez l'adresse dans le champ **Début**.
- **Plage d'adresses** : la règle s'applique au trafic provenant d'une adresse IP appartenant à une plage d'adresses spécifique. Saisissez l'adresse IP de début dans le champ **Début** et l'adresse IP de fin dans le champ **Fin**.

ÉTAPE 8 Dans le champ **Journal**, spécifiez si les paquets correspondant à cette règle doivent être consignés dans un journal.

Pour consigner les détails de tous les paquets correspondants à la règle, sélectionnez **Toujours** dans le menu déroulant. Exemple : si une règle sortante pour un planning est réglée sur **Toujours bloquer**, à chaque fois qu'un paquet tente d'établir une connexion sortante pour le service concerné, un message contenant l'adresse source et de destination du paquet (ainsi que d'autres informations) est enregistré dans le journal.

L'activation de la journalisation peut engendrer un volume conséquent de messages de journal et n'est recommandée qu'à des fins de débogage.

Sélectionnez **Jamais** pour désactiver la journalisation.

REMARQUE lorsque le trafic va du LAN ou de la DMZ vers le WAN, le système exige la réécriture de l'adresse IP source ou de destination des paquets IP entrants lorsqu'ils transitent par le pare-feu.

ÉTAPE 9 Dans le champ **Priorité QoS**, affectez une priorité aux paquets IP du service. Les priorités sont définies par niveau de QoS : (**1 (minimum)**, **2**, **3**, **4 (maximum)**).

ÉTAPE 10 Dans le champ **État de la règle**, cochez la case pour activer la nouvelle règle d'accès.

ÉTAPE 11 Cliquez sur **Enregistrer**.

Création d'une stratégie d'accès à Internet

Le routeur prend en charge plusieurs options permettant de bloquer l'accès à Internet. Vous pouvez bloquer l'ensemble du trafic Internet, le bloquer au niveau de certains ordinateurs ou points de terminaison ou encore bloquer l'accès à des sites Internet en spécifiant des mots clés spécifiques. Si ces mots clés sont détectés dans le nom d'un site (URL du site, nom d'un newsgroup, etc.), le site est bloqué.

Ajout ou modification d'une stratégie d'accès à Internet

Pour créer une stratégie d'accès à Internet :

ÉTAPE 1 Sélectionnez **Pare-feu** > **Stratégie d'accès à Internet**.

ÉTAPE 2 Cliquez sur **Ajouter une ligne**.

ÉTAPE 3 Dans le champ **État**, cochez la case **Activer**.

ÉTAPE 4 Entrez un nom de stratégie pour pouvoir l'identifier plus tard.

ÉTAPE 5 Dans le menu déroulant **Action**, sélectionnez le type de restriction d'accès voulu :

- **Toujours bloquer** : toujours bloquer le trafic Internet. Cette option bloque le trafic Internet en provenance et en direction de tous les points de terminaison. Si vous souhaitez bloquer l'intégralité du trafic, mais autoriser certains points de terminaison à recevoir du trafic Internet, reportez-vous à l'étape 7.
- **Toujours autoriser** : toujours autoriser le trafic Internet. Vous pouvez affiner ce paramètre afin de bloquer certains points de terminaison spécifiés du trafic Internet. Pour cela, reportez-vous à l'étape 7. Vous pouvez également autoriser l'ensemble du trafic Internet à l'exception de certains sites Web ; reportez-vous à l'étape 8.
- **Bloquer selon un horaire** : bloque le trafic Internet selon un planning précis (par exemple, si vous souhaitez bloquer le trafic Internet pendant les heures de travail, mais l'autoriser après les heures de travail et pendant le week-end).
- **Autoriser selon un horaire** : autorise le trafic Internet en fonction d'un planning.

Si vous sélectionnez **Bloquer selon un horaire** ou **Autoriser selon un horaire**, cliquez sur **Configurer les horaires** pour créer un planning. Reportez-vous à la section **Gestion des plannings de pare-feu**.

ÉTAPE 6 Sélectionnez un planning dans le menu déroulant.

ÉTAPE 7 (Facultatif) Appliquez la stratégie d'accès à des ordinateurs particuliers afin d'autoriser ou de bloquer le trafic provenant de périphériques particuliers :

a. Dans la table **Appliquer la stratégie d'accès aux ordinateurs suivants**, cliquez sur **Ajouter une ligne**.

b. Dans le menu déroulant **Type**, sélectionnez la manière d'identifier l'ordinateur (adresse MAC, adresse IP ou plage d'adresses IP).

c. En fonction du choix effectué à l'étape précédente, entrez l'une des valeurs suivantes dans le champ **Valeur** :

- l'adresse MAC (xx:xx:xx:xx:xx:xx) de l'ordinateur ciblé par la stratégie ;
- l'adresse IP des ordinateurs ciblés par la stratégie ;
- les adresses IP de début et de fin de la plage d'adresses à bloquer (comme 192.168.1.2-192.168.1.253).

ÉTAPE 8 Pour bloquer le trafic de sites Web particuliers :

a. Dans la table **Blocage de site Web**, cliquez sur **Ajouter une ligne**.

b. Dans le menu déroulant **Type**, sélectionnez la manière de bloquer le site web (en spécifiant l'URL ou un mot clé qui est inclus dans l'URL).

c. Dans le champ **Valeur**, entrez l'URL ou mot clé de blocage du site Web.

Exemple : pour bloquer l'URL exemple.com, sélectionnez **Adresse URL** dans le menu déroulant, puis entrez **exemple.com** dans le champ **Valeur**. Pour bloquer une URL qui contient le mot clé « exemple », sélectionnez **Mot clé** dans le menu déroulant et entrez **exemple** dans le champ **Valeur**.

ÉTAPE 9 Cliquez sur **Enregistrer**.

Configuration de la redirection de ports

La redirection de ports sert à rediriger le trafic Internet d'un port du réseau WAN vers un autre port du réseau LAN. Des services courants sont disponibles, mais vous pouvez également définir un service personnalisé et les ports associés pour la redirection.

Les pages **Redirection de ports individuels** et **Redirection de plages de ports** présentent toutes les règles de redirection de ports de l'appareil et vous permettent de les configurer.

REMARQUE La redirection de port ne s'applique pas aux serveurs du LAN, en raison de la dépendance sur l'appareil LAN qui établit une connexion sortante avant l'ouverture des ports entrants.

Pour fonctionner correctement, certaines applications doivent recevoir des données sur un port particulier ou une plage de ports particulière lorsque des appareils externes s'y connectent. Le routeur doit envoyer toutes les données entrantes pour cette application uniquement au port ou à la plage de ports spécifiques.

La passerelle dispose d'une liste d'applications et de jeux avec des ports entrants et sortants associés à ouvrir. Vous pouvez également spécifier une règle de redirection de port en spécifiant le type de trafic (TCP ou UDP) et la plage de ports entrants et sortants à ouvrir.

Configuration de la redirection de port individuel

Pour ajouter une règle de redirection de port individuel :

ÉTAPE 1 Sélectionnez **Pare-feu** > **Redirection de port individuel**. Une liste préexistante d'applications s'affiche.

ÉTAPE 2 Dans le champ **Application**, entrez le nom de l'application pour laquelle vous souhaitez configurer la redirection de port.

ÉTAPE 3 Dans le champ **Port externe**, entrez le numéro de port qui déclenche la règle en cas de demande de connexion émise par le trafic sortant.

ÉTAPE 4 Dans le champ **Port interne**, entrez le numéro de port utilisé par l'appareil distant pour répondre à la demande qu'il reçoit.

ÉTAPE 5 Dans le menu déroulant Interface, choisissez **Les deux (Ethernet & 3G)**, **Ethernet** ou **3G**.

ÉTAPE 6 Dans le menu déroulant **Protocole**, sélectionnez un protocole (**TCP**, **UDP** ou **TCP** et **UDP**).

ÉTAPE 7 Dans le champ **Adresse IP**, entrez l'adresse IP de l'hôte, côté LAN, vers laquelle le trafic IP spécifique doit être redirigé. Par exemple, vous pouvez rediriger le trafic HTTP vers le port 80 de l'adresse IP d'un serveur Web côté LAN.

ÉTAPE 8 Cochez la case **Activer** dans le champ correspondant pour activer la règle.

ÉTAPE 9 Cliquez sur **Enregistrer**.

Configuration de la redirection d'une plage de ports

Pour ajouter une règle de redirection de plage de ports :

ÉTAPE 1 Sélectionnez **Pare-feu** > **Redirection de plage de ports**.

ÉTAPE 2 Dans le champ **Application**, entrez le nom de l'application pour laquelle vous souhaitez configurer la redirection de port.

ÉTAPE 3 Dans le champ **Port externe**, entrez le numéro de port qui déclenche la règle en cas de demande de connexion émise par le trafic sortant.

ÉTAPE 4 Dans le champ **Début**, indiquez le numéro de port de début de la plage de ports à rediriger.

ÉTAPE 5 Dans le champ **Fin**, indiquez le numéro de port de fin de la plage de ports à rediriger.

ÉTAPE 6 Dans le menu déroulant Interface, choisissez **Les deux (Ethernet & 3G)**, **Ethernet** ou **3G**.

ÉTAPE 7 Dans le menu déroulant **Protocole**, sélectionnez un protocole (**TCP**, **UDP** ou **TCP** et **UDP**).

ÉTAPE 8 Dans le champ **Adresse IP**, entrez l'adresse IP de l'hôte, côté LAN, vers laquelle le trafic IP spécifique doit être redirigé.

ÉTAPE 9 Cochez la case **Activer** dans le champ correspondant pour activer la règle.

ÉTAPE 10 Cliquez sur **Enregistrer**.

Configuration du déclenchement de plage de ports

Le déclenchement de plages de ports permet aux appareils du LAN ou de la DMZ de demander qu'un ou plusieurs ports soient redirigés vers eux. Le mécanisme de déclenchement de port attend une demande sortante du LAN/DMZ sur l'un des ports sortants définis, puis ouvre un port entrant pour le type de trafic concerné.

Le déclenchement des ports est une forme de redirection de ports dynamiques lorsqu'une application transmet des données sur les ports entrants et sortants ouverts. Il ouvre un port entrant pour un type de trafic particulier sur un port sortant défini. Cette option est plus souple que la redirection de port statique (disponible lors de la configuration de règles de pare-feu), car il n'est pas nécessaire que la règle cible une adresse IP ni une plage IP du réseau LAN. En outre, les ports sont fermés lorsqu'ils ne sont pas utilisés, offrant ainsi un niveau de sécurité supérieur à la redirection de ports.

REMARQUE La redirection de port ne s'applique pas aux serveurs du LAN, en raison de la dépendance sur l'appareil LAN qui établit une connexion sortante avant l'ouverture des ports entrants.

Pour fonctionner correctement, certaines applications doivent recevoir des données sur un port particulier ou une plage de ports particulière lorsque des appareils externes s'y connectent. Le routeur doit envoyer toutes les données entrantes pour cette application uniquement au port ou à la plage de ports spécifiques. La passerelle dispose d'une liste d'applications et de jeux avec des ports entrants et sortants associés à ouvrir. Vous pouvez également spécifier une règle de déclenchement de ports en spécifiant le type de trafic (TCP ou UDP) et la plage de ports entrants et sortants à ouvrir.

Pour ajouter une règle de déclenchement de port :

ÉTAPE 1 Sélectionnez **Pare-feu** > **Déclenchement de plage de ports**.

ÉTAPE 2 Dans le champ **Application**, entrez le nom de l'application pour laquelle vous souhaitez configurer la redirection de port.

ÉTAPE 3 Dans le champ **Plage déclenchée**, entrez le numéro de port ou la plage de numéros de ports qui déclenche la règle en cas de demande de connexion émise par le trafic sortant. Si la connexion sortante n'utilise qu'un seul port, entrez le même numéro de port dans les deux champs.

ÉTAPE 4 Dans les champs **Plage redirigée**, entrez le numéro de port ou les numéros de plage de ports utilisés par le système distant pour répondre à la demande qu'il reçoit. Si la connexion entrante n'utilise qu'un seul port, entrez le même numéro de port dans les deux champs.

ÉTAPE 5 Dans le menu déroulant Interface, choisissez **Les deux (Ethernet & 3G)**, **Ethernet** ou **3G**.

ÉTAPE 6 Cochez la case **Activer** dans le champ correspondant pour activer la règle.

ÉTAPE 7 Cliquez sur **Enregistrer**.

6

Configuration de VPN

Ce chapitre explique comment configurer le VPN et la sécurité pour le routeur.

- **Types de tunnels VPN, page 107**
- **Clients VPN, page 108**
- **Configuration de paramètres VPN site-à-site de base, page 112**
- **Configuration des paramètres VPN avancés, page 114**
- **Configuration de la gestion des certificats, page 120**
- **Configuration de l'intercommunication VPN, page 122**

Types de tunnels VPN

Les VPN offrent un canal de communication sécurisé (tunnel) entre deux routeurs-passerelles ou entre un télétravailleur et un routeur-passerelle Vous pouvez créer différents types de tunnels VPN en fonction des besoins de votre entreprise. Différents exemples sont proposés ci-dessous. Lisez ces descriptions afin de comprendre les diverses options et les procédures requises pour configurer votre VPN.

Accès distant via PPTP

Dans cet exemple, un utilisateur distant équipé d'un ordinateur Microsoft se connecte à un serveur PPTP de votre site, afin d'accéder aux ressources du réseau. Utilisez cette option pour simplifier la configuration VPN. Vous n'avez pas à configurer de stratégies VPN. Les utilisateurs distants peuvent se connecter à l'aide du client PPTP à partir d'un ordinateur Microsoft. Vous n'avez pas à installer de client VPN. Toutefois, tenez compte du fait que des vulnérabilités en matière de sécurité ont été détectées dans ce protocole.

Accès distant avec Cisco QuickVPN

Pour définir rapidement les paramètres de sécurité VPN de base, distribuez le logiciel Cisco QuickVPN à vos utilisateurs, qui pourront alors accéder à vos ressources réseau de manière sécurisée. Utilisez cette option si vous souhaitez simplifier le processus de configuration VPN. Vous n'avez pas à configurer de stratégies VPN. Les utilisateurs distants peuvent se connecter de manière sécurisée à l'aide du client Cisco QuickVPN et d'une connexion Internet.

VPN site-à-site

Le routeur prend en charge le VPN site-à-site pour un tunnel VPN passerelle-à-passerelle unique. Par exemple, vous pouvez configurer le routeur sur un site de filiale pour qu'il se connecte au routeur du site de l'entreprise, afin que le site de la filiale puisse accéder en toute sécurité au réseau de l'entreprise. La configuration du VPN site-à-site s'effectue sur la page **VPN** > **Configuration VPN de base**.

Clients VPN

Le logiciel client VPN est nécessaire pour établir un tunnel VPN entre le routeur et le point d'extrémité distant. Le routeur prend en charge les clients VPN Cisco QuickVPN et PPTP.

Configuration du protocole PPTP

Le protocole PPTP (Point to Point Tunneling Protocol) est un protocole réseau permettant de transférer en toute sécurité des données depuis un client distant vers un réseau d'entreprise en créant une connexion VPN sécurisée sur les réseaux publics, comme Internet.

REMARQUE Lors de l'activation du VPN sur le routeur, le sous-réseau LAN sur le routeur est automatiquement modifié pour éviter les conflits d'adresses IP entre le réseau distant et le réseau local.

Pour configurer le service VPN PPTP :

ÉTAPE 1 Sélectionnez **VPN** > **Clients VPN**.

ÉTAPE 2 Saisissez les informations suivantes :

Serveur PPTP	Cochez cette case pour activer le serveur PPTP.
Adresse IP du serveur PPTP	Saisissez l'adresse IP du serveur PPTP.

Adresses IP des clients PPTP	Saisissez la plage d'adresses IP des clients PPTP.
Chiffrement MPPE	Cochez la case **Activer** pour activer le cryptage MPPE. Le cryptage MPPE (Microsoft Point-to-Point Encryption) est utilisé lorsque les utilisateurs configurent et emploient un client VPN PPTP pour se connecter au routeur.

ÉTAPE 3 Cliquez sur **Enregistrer**.

Configuration de QuickVPN

ÉTAPE 1 Ajoutez les utilisateurs du QuickVPN sur la page **VPN > Clients VPN**. Reportez-vous aux sections **Importation des paramètres client VPN** et **Création et gestion des utilisateurs QuickVPN**.

ÉTAPE 2 Demandez aux utilisateurs de récupérer le logiciel gratuit Cisco QuickVPN sur le site Cisco.com et de l'installer sur leurs ordinateurs. Reportez-vous à la section **Utilisation du logiciel Cisco QuickVPN**

ÉTAPE 3 Pour activer l'accès via Cisco QuickVPN sur le routeur, vous devez activer la gestion à distance afin d'ouvrir le port 443 pour SSL. Reportez-vous à la section **Configuration des paramètres de base du pare-feu**.

Configuration de NetBIOS sur VPN

Pour activer NetBIOS sur VPN :

ÉTAPE 1 Dans le champ **NetBIOS sur VPN**, cochez la case pour permettre aux diffusions NetBIOS de traverser le tunnel VPN. Par défaut, la fonction NetBIOS est disponible pour les stratégies client.

ÉTAPE 2 Cliquez sur **Enregistrer**.

Création et gestion des utilisateurs PPTP

Pour créer des utilisateurs PPTP :

ÉTAPE 1 Dans la **Table des paramètres des clients VPN**, cliquez sur **Ajouter une ligne**.

ÉTAPE 2 Saisissez les informations suivantes :

Activer	Cochez cette case pour activer l'utilisateur.
Nom d'utilisateur	Saisissez le nom d'utilisateur de l'utilisateur PPTP (entre 4 et 32 caractères).
Mot de passe	Saisissez le mot de passe (entre 4 et 32 caractères).
Protocole	Choisissez l'utilisateur **PPTP** dans le menu déroulant.

ÉTAPE 3 Cliquez sur **Enregistrer**.

Pour modifier les paramètres d'un utilisateur PPTP, cochez la case correspondante, puis cliquez sur Modifier. Une fois que vous avez terminé, cliquez sur **Enregistrer**.

Pour supprimer un utilisateur PPTP, cochez la case correspondante, puis cliquez sur **Supprimer**.

Création et gestion des utilisateurs QuickVPN

Pour créer des utilisateurs QuickVPN :

ÉTAPE 1 Dans la **Table des paramètres des clients VPN**, cliquez sur **Ajouter une ligne**.

ÉTAPE 2 Saisissez les informations suivantes :

ÉTAPE 3 Cliquez sur **Enregistrer**.

Pour modifier les paramètres d'un utilisateur QuickVPN, cochez la case correspondant à cet utilisateur, puis cliquez sur **Modifier**. Apportez les modifications voulues et cliquez sur **Enregistrer**.

Pour supprimer un utilisateur QuickVPN, cochez la case correspondant à cet utilisateur, cliquez sur **Supprimer**, puis sur **Enregistrer**.

Pour plus d'informations sur QuickVPN, reportez-vous à **Annexe A, ? Utilisation du logiciel Cisco QuickVPN ?**

Importation des paramètres client VPN

Vous pouvez importer des fichiers de paramètres client VPN contenant le nom d'utilisateur et le mot de passe des clients dans un fichier CSV (Comma Separated Value).

Vous pouvez utiliser un programme tel que Microsoft Excel pour créer un fichier CSV contenant les paramètres client VPN. Ce fichier doit contenir une ligne pour les en-têtes et une ou plusieurs lignes pour les clients VPN.

L'exemple suivant montre les paramètres à importer de deux utilisateurs :

PROTOCOLE	NOM D'UTILISATEUR	MOT DE PASSE
PPTP	pptp-user-1	12345678
QuickVPN	qv-user-1	12345678

ATTENTION L'importation de paramètres client VPN entraîne la suppression des paramètres existants.

Pour importer des paramètres client VPN :

ÉTAPE 1 Cliquez sur **Parcourir** pour trouver le fichier.

ÉTAPE 2 Cliquez sur **Importer** pour charger le fichier.

ÉTAPE 3 À l'invite, pour supprimer les paramètres d'utilisateur VPN existants et importer les paramètres du fichier CSV, cliquez sur **Oui**.

Configuration de paramètres VPN site-à-site de base

Le routeur prend en charge le VPN site-à-site pour un tunnel VPN passerelle-à-passerelle unique. Dans cette configuration, le routeur crée une connexion sécurisée vers un autre routeur VPN. Par exemple, vous pouvez configurer le routeur sur un site de filiale pour qu'il se connecte au routeur du site de l'entreprise, afin que le site de la filiale puisse accéder en toute sécurité au réseau de l'entreprise.

Pour configurer les paramètres VPN de base pour une connexion site-à-site :

ÉTAPE 1 Sélectionnez **VPN** > **Configuration VPN de base**.

ÉTAPE 2 Dans le champ **Nom de la connexion**, entrez le nom du tunnel VPN.

ÉTAPE 3 Dans le champ **Clé pré-partagée**, entrez la clé prépartagée, ou le mot de passe, qui sera échangé entre les deux routeurs. La clé prépartagée doit comporter entre 8 et 49 caractères.

ÉTAPE 4 Dans les champs **Informations sur le point d'extrémité**, entrez les informations suivantes :

- **Point d'extrémité distant** : choisissez la façon d'identifier le point d'extrémité distant, ou le routeur auquel le routeur se connectera. Par exemple, au moyen d'une adresse IP telle que 192.168.1.1 ou d'un nom de domaine complet tel que cisco.com.
- **Adresse IP du WAN (Internet) distant** : entrez l'adresse IP publique ou le nom de domaine du point d'extrémité distant.
- **Point d'extrémité de redondance** : pour que le routeur bascule vers une autre passerelle lorsque la connexion VPN principale échoue, cochez la case **Activer**. Entrez l'adresse IP du WAN ou le nom de domaine complet (FQDN) du point d'extrémité de redondance.
- **Adresse IP du WAN (Internet) local** : entrez l'adresse IP publique ou le nom de domaine du point d'extrémité local (routeur).

ÉTAPE 5 Dans les champs **Accessibilité à distance par connexion sécurisée**, entrez les informations suivantes :

- **Adresse IP du réseau local (LAN) distant** : entrez l'adresse de réseau privé (LAN) du point d'extrémité distant. Il s'agit de l'adresse IP du réseau interne pour le site distant.
- **Masque de sous-réseau du réseau local (LAN) distant** : entrez le masque de sous-réseau du réseau privé (LAN) du point d'extrémité distant.
- **Adresse IP du réseau local (LAN)** : entrez l'adresse de réseau privé (LAN) du réseau local. Il s'agit de l'adresse IP du réseau interne sur le périphérique.
- **Masque de sous-réseau du réseau local (LAN)** : entrez le masque de sous-réseau du réseau privé du réseau local (routeur).

Remarque : les adresses IP du WAN distant et du LAN distant ne peuvent pas exister sur le même sous-réseau. Par exemple, l'adresse IP de LAN distant 192.168.1.100 et l'adresse IP de LAN local 192.168.1.115 risquent de créer un conflit lorsque le trafic est acheminé via le VPN. Le troisième octet doit être différent pour que les adresses IP soient sur des sous-réseaux différents. Par exemple, l'adresse IP de LAN distant 192.168.1.100 et l'adresse IP de LAN local 192.168.2.100 sont acceptées.

ÉTAPE 6 Cliquez sur **Enregistrer**.

Affichage des valeurs par défaut

Les valeurs par défaut utilisées dans les paramètres VPN de base sont celles proposées par le VPN Consortium et elles supposent que vous utilisez une clé prépartagée, ou un mot de passe, connu du routeur et du routeur à l'autre extrémité (par exemple, un Cisco RV220W). Pour afficher les valeurs par défaut :

ÉTAPE 1 Sélectionnez **VPN** > **Configuration VPN de base**.

ÉTAPE 2 Cliquez sur **Afficher les paramètres par défaut** pour afficher les valeurs par défaut.

Pour plus d'informations sur ces valeurs, reportez-vous à la section **Configuration des paramètres VPN avancés**.

Configuration des paramètres VPN avancés

La page Configuration VPN avancée vous permet de configurer les paramètres VPN avancés, tels que les stratégies IKE et d'autres stratégies VPN. Ces stratégies déterminent la façon dont le routeur initie et reçoit les connexions VPN avec d'autres points d'extrémité.

Gestion des stratégies IKE

Le protocole IKE (Internet Key Exchange) échange des clés entre deux hôtes IPsec de manière dynamique. Vous pouvez créer des stratégies IKE pour définir les paramètres de sécurité tels que l'authentification de l'homologue et les algorithmes de cryptage à utiliser dans ce processus. Veillez à utiliser des paramètres de cryptage, d'authentification et de clé-groupe compatibles dans la stratégie VPN.

ÉTAPE 1 Sélectionnez **VPN** > **IPsec** > **Configuration VPN avancée**.

ÉTAPE 2 Dans la **table des stratégies VPN**, cochez la case de la ligne de la connexion VPN pour effectuer les tâches suivantes :

- **Ajouter une ligne** ou **Modifier** : permet de modifier les propriétés de la stratégie IKE. Reportez-vous à la section **Ajout ou modification de stratégies IKE**.
- **Activer** : permet d'activer la stratégie.
- **Désactiver** : permet de désactiver la stratégie.
- **Supprimer** : permet de supprimer la stratégie.

REMARQUE Vous ne pouvez pas supprimer une stratégie IKE si elle est utilisée dans une stratégie VPN. Vous devez d'abord désactiver et supprimer la stratégie VPN dans la **table des stratégies VPN**.

- **Ajouter une ligne** : permet d'ajouter une stratégie IKE. Reportez-vous à la section **Ajout ou modification de stratégies IKE**.

REMARQUE Si une connexion VPN est déjà configurée, vous devez la supprimer pour ajouter une autre connexion.

ÉTAPE 3 Cliquez sur **Enregistrer**.

Ajout ou modification de stratégies IKE

ÉTAPE 1 Pour ajouter ou modifier des stratégies IKE, configurez les paramètres suivants :

- **Nom de la stratégie** : saisissez un nom unique à attribuer à la stratégie à des fins d'identification et de gestion.
- **Mode Exchange** : choisissez l'une des options suivantes :
  - **Principal** : négocie le tunnel avec une sécurité supérieure, mais est plus lent.
  - **Agressif** : établit plus rapidement la connexion, mais la sécurité est moindre.
- **Identifiant local** : identifiant IKE local.
- **Identifiant distant** : identifiant IKE distant.
- **Identifiant de redondance** : l'identifiant unique de l'autre point d'extrémité de secours utilisé pour rétablir la connexion si la connexion VPN d'origine échoue.

ÉTAPE 2 Dans la section **Paramètres de SA IKE**, les paramètres d'association de sécurité (SA) définissent la robustesse et le mode de négociation de l'association de sécurité. Vous pouvez configurer les paramètres suivants :

- **Algorithme de chiffrement** : choisissez l'algorithme utilisé pour négocier l'association de sécurité :
  - **DES**
  - **3DES**
  - **AES-128**
  - **AES-192**
  - **AES-256**
- **Algorithme d'authentification** : spécifiez l'algorithme d'authentification de l'en-tête VPN :
  - **MD5**
  - **SHA-1**

- **SHA2-256**

  Veillez à ce que l'algorithme d'authentification soit configuré de façon identique des deux côtés du tunnel VPN (par exemple, sur le routeur et sur le routeur auquel il se connecte).

- **Clé prépartagée** : entrez la clé dans l'espace prévu à cet effet. Veuillez noter que les guillemets anglais (") ne sont pas pris en charge dans la clé prépartagée.
- **Groupe Diffie-Hellman (DH)** : spécifiez l'algorithme de groupe DH qui est utilisé lors de l'échange de clés. Le groupe DH définit la robustesse de l'algorithme, en bits. Vérifiez que le groupe DH est configuré de manière identique des deux côtés de la stratégie IKE.
- **Durée de vie SA** : saisissez l'intervalle, en secondes, au bout duquel l'association de sécurité devient non valide.
- **Détection d'homologue indisponible** : cochez la case **Activer** pour activer cette fonction ou décochez la case pour la désactiver. La détection d'homologue indisponible sert à détecter si l'homologue est actif ou non. Si l'homologue est détecté comme étant indisponible, le routeur supprime l'association de sécurité IPsec et l'association de sécurité IKE Si vous activez cette fonction, entrez également les paramètres suivants :

  - **Délai DPD** : entrez l'intervalle, en secondes, entre les messages DPD R-U-THERE consécutifs. Les messages DPD R-U-THERE sont envoyés uniquement lorsque le trafic IPsec est inactif.
  - **Expiration DPD** : indiquez combien de temps le routeur doit attendre pour recevoir une réponse au message DPD avant de considérer l'homologue comme inactif.

ÉTAPE 3 Cochez la case activant l'option **Type de XAUTH** pour configurer l'authentification étendue pour votre stratégie VPN IPsec. Fournissez le nom d'utilisateur et le mot de passe d'authentification.

ÉTAPE 4 Cliquez sur **Enregistrer**.

Gestion des stratégies VPN

Pour gérer les stratégies VPN :

ÉTAPE 1 Sélectionnez **VPN** > **IPsec** > **Configuration VPN avancée**.

ÉTAPE 2 Dans la **table des stratégies VPN**, cochez la case dans la ligne de la connexion VPN pour effectuer les tâches suivantes :

- **Ajouter une ligne** ou **Modifier** : permet de modifier les propriétés de la stratégie VPN. Reportez-vous à la section **Ajout ou modification de stratégies VPN**.
- **Activer** : permet d'activer la stratégie.
- **Désactiver** : permet de désactiver la stratégie.
- **Supprimer** : permet de supprimer la stratégie.
- **Ajouter une ligne** : permet d'ajouter une stratégie VPN. Reportez-vous à la section **Ajout ou modification de stratégies VPN**.

REMARQUE Si une connexion VPN est déjà configurée, vous devez la supprimer pour ajouter une autre connexion.

ÉTAPE 3 Cliquez sur **Enregistrer**.

Ajout ou modification de stratégies VPN

Pour créer une stratégie VPN automatique, vous devez d'abord créer une stratégie IKE, puis ajouter la stratégie automatique correspondant à cette stratégie IKE.

Pour ajouter ou modifier des stratégies VPN, configurez les paramètres suivants :

- **Nom de la stratégie** : saisissez un nom unique permettant d'identifier la stratégie.
- **Type de stratégie** : choisissez l'une des options suivantes :
  - **Stratégie automatique** : certains paramètres du tunnel VPN sont générés automatiquement. Cette option nécessite l'utilisation du protocole IKE (Internet Key Exchange) pour les négociations entre les deux points d'extrémité VPN.
  - **Stratégie manuelle** : tous les paramètres (y compris les clés) du tunnel VPN sont saisis manuellement pour chaque point d'extrémité. Aucun serveur tiers ni aucune organisation tierce n'est impliqué(e).

- **Point d'extrémité distant** : sélectionnez le type d'identifiant de passerelle à fournir sur le point d'extrémité distant : **Adresse IP** ou **FQDN** (nom de domaine complet). Entrez l'identifiant dans l'espace prévu à cet effet.
- **Point d'extrémité de redondance** : pour que le routeur bascule vers une autre passerelle lorsque la connexion VPN principale échoue, cochez la case **Activer**. Entrez l'adresse IP du WAN ou le nom de domaine complet (FQDN) du point d'extrémité de redondance.

  Pour basculer automatiquement sur la connexion VPN principale lorsque la connexion est rétablie, cochez la case **Activer la restauration**.

Dans **Sélection de trafic en local** et **Sélection de trafic distant**, entrez ces paramètres :

- **Adresse IP locale/Adresse IP distante** : sélectionnez le type d'identifiant que vous souhaitez fournir pour le point d'extrémité :
  - **Individuelle** : limite la stratégie à un seul hôte. Dans le champ Adresse IP de début, saisissez l'adresse IP de l'hôte qui fera partie du VPN. Entrez l'adresse IP dans le champ **Adresse de début**.
  - **Sous-réseau** : autorise l'ensemble d'un sous-réseau à se connecter au VPN. Saisissez l'adresse de réseau dans le champ Adresse IP de début et saisissez le masque de sous-réseau dans le champ Masque de sous-réseau. Entrez l'adresse IP réseau du sous-réseau dans le champ **Adresse de début**. Entrez le masque de sous-réseau, tel que 255.255.255.0, dans le champ **Masque de sous-réseau**. Le champ affiche automatiquement une adresse de sous-réseau par défaut qui est basée sur l'adresse IP.

    IMPORTANT : évitez d'utiliser des sous-réseaux qui se chevauchent pour les sélecteurs de trafic distant et local. L'utilisation de ces sous-réseaux nécessite l'ajout de routes statiques sur le routeur et les hôtes à utiliser. Par exemple, évitez la combinaison suivante :

    Sélecteur de trafic local : 192.168.1.0/24

    Sélecteur de trafic distant : 192.168.0.0/16

Pour le type de stratégie **manuelle**, entrez les paramètres dans la section **Paramètres de stratégie manuelle**.

- **SPI-entrant, SPI-sortant** : saisissez une valeur hexadécimale composée de 3 à 8 caractères (0x1234, par exemple).
- **Algorithme de chiffrement** : sélectionnez l'algorithme utilisé pour chiffrer les données :

- DES
- 3DES
- AES-128
- AES-192
- AES-256

- **Clé entrante** : saisissez la clé de cryptage de la stratégie appliquée au trafic entrant. La longueur de la clé dépend de l'algorithme de cryptage choisi :
  - DES : 8 caractères
  - 3DES : 24 caractères
  - AES-128 : 16 caractères
  - AES-192 : 24 caractères
  - AES-256 : 32 caractères
- **Clé sortante** : saisissez la clé de cryptage de la stratégie appliquée au trafic sortant. La longueur de la clé dépend de l'algorithme de cryptage choisi, comme indiqué ci-dessus.
- **Algorithme d'intégrité** : sélectionnez l'algorithme utilisé pour vérifier l'intégrité des données.
  - MD5
  - SHA-1
  - SHA2-256
- **Clé entrante** : saisissez la clé d'intégrité (pour l'ESP avec mode d'intégrité) de la stratégie appliquée au trafic entrant. La longueur de la clé dépend de l'algorithme choisi :
  - MD5 : 16 caractères
  - SHA-1 : 20 caractères
  - SHA2-256 : 32 caractères
- **Clé sortante** : saisissez la clé d'intégrité (pour l'ESP avec mode d'intégrité) de la stratégie appliquée au trafic sortant. La longueur de la clé dépend de l'algorithme choisi, comme indiqué ci-dessus.

Pour le type de stratégie **automatique**, entrez les paramètres dans la section **Paramètres de stratégie automatique**.

- **Durée de vie SA** : entrez la durée de l'association de sécurité en secondes. À la fin de l'intervalle indiqué en secondes, l'association de sécurité est renégociée. La valeur par défaut est 3 600 secondes. La valeur minimale est de 300 secondes.
- **Algorithme de chiffrement** : sélectionnez l'algorithme utilisé pour chiffrer les données.
- **Algorithme d'intégrité** : sélectionnez l'algorithme utilisé pour vérifier l'intégrité des données.
- **Groupe de clés PFS** : cochez la case **Activer** pour activer PFS (Perfect Forward Secrecy), afin de renforcer la sécurité. Ce protocole est plus lent, mais contribue à empêcher l'écoute électronique en garantissant qu'un échange Diffie-Hellman a lieu pour chaque négociation de phase 2.
- **Sélectionner la stratégie IKE** : sélectionnez la stratégie IKE qui définira les caractéristiques de la phase 1 de négociation. Cliquez sur **Afficher** pour afficher ou modifier la stratégie IKE existante qui est configurée sur le routeur.

Configuration de la gestion des certificats

Le routeur a recours à des certificats numériques pour l'authentification VPN IPsec et la validation SSL (pour l'authentification HTTPS). Le routeur dispose d'une fonctionnalité qui vous permet de générer et de signer vos propres certificats.

Génération d'un nouveau certificat

Vous pouvez générer un nouveau certificat en remplacement du certificat existant sur le routeur.

Pour générer un certificat :

ÉTAPE 1 Choisissez **VPN** > **Gestion des certificats.**

ÉTAPE 2 Cliquez sur le bouton **Générer un nouveau certificat**.

ÉTAPE 3 Cliquez sur **Générer un certificat**.

Importation de certificats

Vous pouvez importer un certificat enregistré au préalable dans un fichier via le bouton **Exporter pour l'admin**.

Pour importer un certificat :

ÉTAPE 1 Choisissez **VPN** > **Gestion des certificats.**

ÉTAPE 2 Cliquez sur le bouton **Importer le certificat depuis un fichier**.

ÉTAPE 3 Cliquez sur **Parcourir** et recherchez le fichier de certificat.

ÉTAPE 4 Cliquez sur **Installer un certificat**.

Exportation de certificats pour l'administrateur

Vous pouvez exporter le certificat pour l'administrateur dans un dossier sur votre ordinateur ou à un emplacement externe sur un lecteur USB. Le certificat pour l'administrateur contient la clé privée et doit être stocké dans un endroit sûr à des fins de sauvegarde. Si les paramètres par défaut de la configuration du routeur sont rétablis, ce certificat peut ainsi être importé et restauré sur le routeur.

Pour exporter un certificat pour l'administrateur :

ÉTAPE 1 Choisissez **VPN** > **Gestion des certificats.**

ÉTAPE 2 Pour exporter le certificat sur votre ordinateur, cliquez sur **Exporter pour l'admin**. Le Gestionnaire de périphérique enregistre le fichier admin.pem dans le dossier C:\Documents and Settings\userid\My Documents\Downloads.

Pour exporter le certificat sur un lecteur USB externe, cliquez sur **Exporter vers USB pour l'admin**.

Exportation de certificats pour le client

Vous pouvez exporter les certificats pour les clients sur votre ordinateur ou à un emplacement externe sur un lecteur USB. Le certificat pour le client permet aux utilisateurs QuickVPN de se connecter en toute sécurité au routeur Cisco RV215W. Les utilisateurs QuickVPN doivent placer le certificat dans le répertoire d'installation du client QuickVPN.

Pour exporter un certificat pour le client :

ÉTAPE 1 Sélectionnez **VPN** > **Gestion des certificats**.

ÉTAPE 2 Pour exporter le certificat sur votre ordinateur, cliquez sur **Exporter pour le client**. Sur un PC, le Gestionnaire de périphérique enregistre le fichier client.pem dans le dossier C:\Documents and Settings\userid\My Documents\Downloads.

Pour exporter le certificat sur un lecteur USB externe, cliquez sur **Exporter vers USB pour le client**.

Configuration de l'intercommunication VPN

L'intercommunication VPN permet au trafic VPN provenant des clients VPN de transiter par le routeur.

Pour configurer l'intercommunication VPN :

ÉTAPE 1 Sélectionnez **VPN** > **Intercommunication VPN**.

ÉTAPE 2 Sélectionnez le type de trafic que le pare-feu autorise à transiter :

Intercommunication IPsec	Cochez **Activer** pour permettre aux tunnels de sécurité IP de transiter par le routeur.
PPTP	Cochez **Activer** pour permettre aux tunnels PPTP de transiter par le routeur.
L2TP	Cochez **Activer** pour permettre aux tunnels L2TP (Layer 2 Tunneling Protocol) de transiter par le routeur.

ÉTAPE 3 Cliquez sur **Enregistrer**.

7

Configuration de la Qualité de service (QoS)

Le routeur Cisco RV215W vous permet de configurer les fonctions QoS (Qualité de service) suivantes :

- **Configuration de la gestion de la bande passante, page 123**
- **Configuration des paramètres de port QoS, page 126**
- **Configuration des paramètres CoS, page 127**
- **Configuration des paramètres DSCP, page 128**

Les paramètres de qualité de service (QoS) attribuent une priorité aux différents utilisateurs, applications ou flux de données ou garantissent un certain niveau de performances sur un flux de données. Cette garantie est important lorsque la capacité réseau est insuffisante, notamment pour les applications multimédias de diffusion en temps réel (téléphonie VoIP (voix sur IP), jeux en ligne et télévision IP). En effet, ces applications ont souvent besoin d'un débit fixe et sont sensibles aux retards. Il en va de même sur les réseaux dont la capacité est assurée par une ressource limitée, dans la communication de données cellulaires par exemple.

Configuration de la gestion de la bande passante

Vous pouvez utiliser la fonction de gestion de la bande passante du routeur pour gérer la bande passante du trafic entre le réseau sécurisé (LAN) et le réseau non sécurisé (WAN).

Configuration de la bande passante

Vous pouvez limiter la bande passante afin de réduire le débit de transmission de données du routeur. Vous pouvez également utiliser un profil de bande passante pour limiter le trafic sortant afin d'empêcher les utilisateurs du réseau LAN de consommer toute la bande passante de la liaison Internet.

Pour définir la bande passante montante et descendante :

ÉTAPE 1 Sélectionnez **QoS** > **Gestion de la bande passante**.

ÉTAPE 2 Dans le champ **Gestion de la bande passante**, cochez la case **Activer**. La bande passante maximale fournie par votre FAI s'affiche dans la section **Bande passante**.

ÉTAPE 3 Dans la **Table des bandes passantes**, saisissez les informations suivantes pour l'interface WAN :

Flux montant	La bande passante (kbit/s) utilisée pour envoyer des données sur Internet.
Flux descendant	La bande passante (kbit/s) utilisée pour recevoir des données d'Internet.

ÉTAPE 4 Cliquez sur **Enregistrer**.

Configuration des priorités de bande passante

Dans la **Table des priorités de bande passante**, vous pouvez affecter des priorités aux services pour gérer l'utilisation de la bande passante.

Pour configurer les priorités de bande passante :

ÉTAPE 1 Sélectionnez **QoS** > **Gestion de la bande passante**.

ÉTAPE 2 Dans le champ **Gestion de la bande passante**, cochez la case **Activer**. La bande passante maximale fournie par votre FAI s'affiche dans la section **Bande passante**.

ÉTAPE 3 Dans la **Table des priorités de bande passante**, cliquez sur **Ajouter une ligne**.

ÉTAPE 4 Saisissez les informations suivantes :

Activer	Cochez cette case pour activer la gestion de la bande passante pour ce service.
Service	Sélectionnez le service auquel attribuer la priorité.
Direction	Sélectionnez la direction du trafic que vous souhaitez privilégier (**Flux descendant** ou **Flux montant**).
Priorité	Sélectionnez le niveau de priorité du service (**Faible**, **Normal**, **Moyen** ou **Élevé**).

ÉTAPE 5 Cliquez sur **Enregistrer**.

Pour modifier les paramètres d'une entrée de la table, cochez la case correspondante, puis cliquez sur **Modifier**. Une fois les modifications terminées, cliquez sur **Enregistrer**.

Pour supprimer une entrée dans la table, cochez la case correspondant à cette entrée, cliquez sur **Supprimer**, puis sur **Enregistrer**.

Pour ajouter une nouvelle définition de service, cliquez sur le bouton **Gestion des services**. Vous pouvez définir un nouveau service à utiliser pour toutes les définitions de pare-feu et de QoS. Reportez-vous à la section **Configuration de la gestion de services**.

Configuration des paramètres de port QoS

Vous pouvez configurer les paramètres QoS pour chaque port LAN sur le Cisco RV215W. Le routeur prend en charge 4 files d'attente de priorité pour la hiérarchisation du trafic par port commuté physique.

Pour configurer les paramètres QoS des ports LAN du routeur :

ÉTAPE 1 Sélectionnez **QoS** > **Paramètres de port QoS**.

ÉTAPE 2 Pour chaque port de la table des **paramètres de port QoS Ethernet,** saisissez les informations suivantes :

Mode de confiance	Sélectionnez l'une des options suivantes dans le menu déroulant : • **Port** : ce paramètre active le port d'après le QoS. Vous pouvez alors définir la priorité du trafic pour un port particulier. La priorité de la file d'attente de trafic commence avec le niveau de priorité le plus bas (1) et finit avec le niveau de priorité le plus élevé (4). • **DSCP** : DSCP (Differentiated Services Code Point, point de code de services différenciés). L'activation de cette fonctionnalité privilégie le trafic réseau sur le LAN d'après le mappage de file d'attente DSCP sur la page **Paramètres DSCP**. • **CoS** : CoS (Class of Service, classe de service).
File d'attente de transfert du trafic par défaut pour les appareils non validés	Sélectionnez un niveau de priorité pour le trafic sortant (de 1 à 4).

ÉTAPE 3 Pour chaque port de la table des **paramètres de port QoS 3G**, saisissez les informations suivantes :

Mode de confiance	Sélectionnez l'une des options suivantes dans le menu déroulant : • **Port** : ce paramètre active le port d'après le QoS. Vous pouvez alors définir la priorité du trafic pour un port particulier. La priorité de la file d'attente de trafic commence avec le niveau de priorité le plus bas (1) et finit avec le niveau de priorité le plus élevé (4). • **DSCP** : DSCP (Differentiated Services Code Point, point de code de services différenciés). L'activation de cette fonctionnalité privilégie le trafic réseau sur le LAN d'après le mappage de file d'attente DSCP sur la page **Paramètres DSCP**. • **CoS** : CoS (Class of Service, classe de service).
File d'attente de redirection du trafic par défaut pour les appareils non validés	Sélectionnez un niveau de priorité pour le trafic sortant (de 1 à 4).

ÉTAPE 4 Cliquez sur **Enregistrer**.

Pour restaurer les paramètres de port QoS par défaut, cliquez sur **Restaurer les valeurs par défaut**, puis sur **Enregistrer**.

Configuration des paramètres CoS

Utilisez le lien vers la page Paramètres de port QoS pour associer le paramètre de priorité CoS à la file d'attente QoS.

Pour mettre en correspondance les paramètres de priorité CoS avec la file d'attente de redirection du trafic :

ÉTAPE 1 Sélectionnez **QoS** > **Paramètres CoS**.

ÉTAPE 2 Sélectionnez la case d'option **Ethernet** ou **3G**.

ÉTAPE 3 Pour chaque niveau de priorité CoS dans la **Table des paramètres CoS**, sélectionnez une valeur de priorité dans le menu déroulant **File d'attente de redirection du trafic**.

Ces valeurs associent aux différents types de trafic des niveaux de priorité plus ou moins élevés.

ÉTAPE 4 Cliquez sur **Enregistrer**.

Pour restaurer les paramètres de port QoS par défaut, cliquez sur **Restaurer les valeurs par défaut**, puis sur **Enregistrer**.

Configuration des paramètres DSCP

Vous pouvez configurer le mappage DSCP à file d'attente QoS depuis la page **Paramètres DSCP**.

Pour configurer le mappage DSCP à file d'attente QoS :

ÉTAPE 1 Sélectionnez **QoS** > **Paramètres DSCP**.

ÉTAPE 2 Sélectionnez la case d'option **Ethernet** ou **3G**.

ÉTAPE 3 Choisissez de répertorier uniquement les valeurs RFC ou toutes les valeurs DSCP dans la **Table des paramètres DSCP** en cliquant sur le bouton correspondant.

ÉTAPE 4 Pour chaque valeur DSCP dans la **Table des paramètres DSCP**, sélectionnez un niveau de priorité dans le menu déroulant **File d'attente**.

Cela associe la valeur DSCP avec la file d'attente QoS sélectionnée.

ÉTAPE 5 Cliquez sur **Enregistrer**.

Pour restaurer les paramètres DSCP par défaut, cliquez sur **Restaurer les valeurs par défaut** et **Enregistrer**.

8

Administration du routeur

Ce chapitre décrit les fonctionnalités d'administration du routeur, notamment la création d'utilisateurs, la gestion réseau, l'établissement de diagnostics système et la journalisation, la configuration de la date et de l'heure ainsi que d'autres paramètres.

- **Définition de la complexité des mots de passe, page 130**
- **Configuration des comptes d'utilisateurs, page 131**
- **Définition du délai d'expiration de session, page 132**
- **Configuration SNMP (Simple Network Management Protocol), page 132**
- **Utilisation des outils de diagnostic, page 135**
- **Configuration de la journalisation, page 138**
- **Configuration de Bonjour, page 142**
- **Configuration des paramètres de date et d'heure, page 143**
- **Sauvegarde et restauration du système, page 144**
- **Mise à niveau du micrologiciel ou changement de la langue, page 147**
- **Redémarrage du Cisco RV215W, page 150**
- **Restauration des paramètres d'usine, page 150**

Définition de la complexité des mots de passe

Le routeur peut exiger une complexité minimale du mot de passe lors des changements de mot de passe.

Pour configurer les paramètres de complexité du mot de passe :

ÉTAPE 1 Sélectionnez **Administration** > **Sécurité du mot de passe**.

ÉTAPE 2 Dans le champ **Paramètres de complexité du mot de passe**, cochez la case **Activer**.

ÉTAPE 3 Configurez les paramètres de complexité du mot de passe :

Longueur minimale du mot de passe	Saisissez la longueur minimale du mot de passe (de 0 à 64 caractères).
Nombre minimal de classes de caractères	Saisissez un nombre correspondant à l'une des classes de caractères suivantes : • Lettres majuscules • Lettres minuscules • Chiffres • Caractères spéciaux disponibles sur un clavier standard Par défaut, les mots de passe doivent contenir des caractères d'au moins trois de ces classes.
Le nouveau mot de passe doit être différent de l'actuel	Cochez la case **Activer** pour exiger que les nouveaux mots de passe soient différents du mot de passe actuel.
Âge du mot de passe	Cochez la case **Activer** pour que les mots de passe expirent après un délai donné.
Délai d'expiration du mot de passe	Saisissez le nombre de jours au bout duquel le mot de passe expire (1–365). La valeur par défaut est de 180 jours.

ÉTAPE 4 Cliquez sur **Enregistrer**.

Configuration des comptes d'utilisateurs

Le routeur prend en charge deux comptes d'utilisateurs pour l'administration et l'affichage des paramètres : un administrateur (nom d'utilisateur et mot de passe par défaut : cisco) et un invité (nom d'utilisateur par défaut : guest).

Le compte invité (guest) est en lecture seule. Vous pouvez définir et modifier le nom d'utilisateur et le mot de passe des comptes administrateur et invité.

Pour configurer les comptes d'utilisateurs :

ÉTAPE 1 Sélectionnez **Administration** > **Utilisateurs**.

ÉTAPE 2 Dans le champ **Activation du compte**, cochez les cases des comptes que vous souhaitez activer. Le compte administrateur doit être actif.

ÉTAPE 3 (Facultatif) Pour modifier le compte administrateur, sous **Paramètre du compte administrateur**, cochez **Modifier les paramètres administrateur**. Pour modifier le compte invité, sous **Paramètres d'invité**, cochez **Modifier les paramètres d'invité**. Saisissez les informations suivantes :

Nouveau nom d'utilisateur	Saisissez un nouveau nom d'utilisateur.
Ancien mot de passe	Saisissez le mot de passe actuel.
Nouveau mot de passe	Saisissez le nouveau mot de passe. Veillez à ce que le mot de passe ne contienne aucun mot du dictionnaire quelle que soit la langue et à ce qu'il contienne des lettres (majuscules et minuscules), des chiffres et des symboles. Le mot de passe peut comporter au maximum 64 caractères.
Confirmer le nouveau mot de passe	Ressaisissez le nouveau mot de passe.

ÉTAPE 4 Pour importer des noms d'utilisateurs et des mots de passe d'un fichier CSV :

a. Dans le champ **Importer le nom de l'utilisateur et le mot de passe**, cliquez sur **Parcourir**.

b. Trouvez le fichier et cliquez sur **Ouvrir**.

c. Cliquez sur **Importer**.

ÉTAPE 5 Saisissez l'ancien mot de passe.

ÉTAPE 6 Cliquez sur **Enregistrer**.

Définition du délai d'expiration de session

Le délai d'expiration est le nombre de minutes d'inactivité autorisées avant la fermeture de la session du Gestionnaire de périphérique. Vous pouvez configurer le délai d'expiration pour les comptes administrateur et invité.

Pour configurer le délai d'expiration de la session :

ÉTAPE 1 Sélectionnez **Administration** > **Délai d'expiration de session**.

ÉTAPE 2 Dans le champ **Délai d'expiration d'inactivité d'administrateur**, saisissez le nombre de minutes avant l'expiration d'une session pour cause d'inactivité. Choisissez **jamais** pour permettre à l'administrateur de rester connecté en permanence.

ÉTAPE 3 Dans le champ **Délai d'expiration d'inactivité d'invité**, saisissez le nombre de minutes avant l'expiration d'une session pour cause d'inactivité. Choisissez **jamais** pour permettre à l'administrateur de rester connecté en permanence.

ÉTAPE 4 Cliquez sur **Enregistrer**.

Configuration SNMP (Simple Network Management Protocol)

Le protocole SNMP (Simple Network Management Protocol) vous permet de surveiller et de gérer le routeur depuis un gestionnaire SNMP. Le protocole SNMP est une solution de surveillance et de contrôle des appareils réseau à distance, qui permet également la gestion des configurations, la collecte de statistiques, des performances et de la sécurité.

Configuration des informations système SNMP

Dans la section **Informations système SNMP** de la page **SNMP**, vous pouvez activer SNMP.

Avant de pouvoir utiliser SNMP, vous devez installer le logiciel SNMP sur l'ordinateur. Le routeur prend uniquement en charge SNMPv3 pour la gestion SNMP et SNNPv1/2/3 pour les messages « trap » SNMP.

Pour activer SNMP :

ÉTAPE 1 Sélectionnez **Administration** > **SNMP**.

ÉTAPE 2 Cochez la case **Activer** pour activer l'option SNMP.

ÉTAPE 3 Saisissez les informations suivantes :

SysContact	Saisissez le nom de la personne à contacter pour ce pare-feu (par exemple, **admin** ou **Jean Durand**).
SysLocation	Saisissez l'emplacement physique du pare-feu (par exemple, **Rack n° 2, 4e étage**).
SysName	Saisissez un nom pour une identification facile du pare-feu.

ÉTAPE 4 Cliquez sur **Enregistrer**.

Modification des utilisateurs SNMPv3

Vous pouvez configurer les paramètres SNMPv3 pour les deux comptes d'utilisateurs par défaut du routeur (admin et invité).

Pour configurer les paramètres SNMPv3 :

ÉTAPE 1 Sélectionnez **Administration** > **SNMP**.

ÉTAPE 2 Sous **Configuration utilisateur SNMPv3**, configurez les paramètres suivants :

Nom d'utilisateur	Sélectionnez le compte à configurer (**admin** ou **invité**).
Autorisation d'accès	Affiche les privilèges d'accès du compte d'utilisateur sélectionné.
Niveau de sécurité	Choisissez le niveau de sécurité SNMPv3 : **Aucune authentification et aucun privilège** : authentification et confidentialité non exigées. **Authentification et aucun privilège** : soumettez uniquement l'algorithme d'authentification et le mot de passe. **Authentification et privilège** : soumettez l'algorithme d'authentification/de confidentialité et le mot de passe.
Serveur d'algorithmes d'authentification	Sélectionnez le type d'algorithme d'authentification (**MD5** ou **SHA**).
Mot de passe d'authentification	Saisissez le mot de passe d'authentification.
Algorithme de confidentialité	Sélectionnez le type d'algorithme de confidentialité (**DES** ou **AES**)
Mot de passe de confidentialité	Saisissez le mot de passe de confidentialité.

ÉTAPE 3 Cliquez sur **Enregistrer**.

Configuration des filtres SNMP

Les champs de la section **Configuration de filtre** de **SNMP** vous permettent de configurer un agent SNMP auquel le pare-feu envoie les messages d'interception (notifications).

Pour configurer les filtres :

ÉTAPE 1 Sélectionnez **Administration** > **SNMP**.

ÉTAPE 2 Sous **Configuration de filtre**, configurez les paramètres suivants :

Adresse IP	Saisissez l'adresse IP du gestionnaire SNMP ou de l'agent de filtre.
Port	Saisissez le port du filtre SNMP de l'adresse IP à laquelle les messages « trap » seront envoyés.
Communauté	Saisissez la chaîne de communauté à laquelle appartient l'agent. La plupart des agents sont configurés pour écouter les filtres dans la communauté publique.
Version SNMP	Sélectionnez la version SNMP : **v1**, **v2c** ou **v3**.

ÉTAPE 3 Cliquez sur **Enregistrer**.

Utilisation des outils de diagnostic

Le routeur comporte plusieurs outils de diagnostic destinés à la résolution des problèmes réseau.

- **Outils réseau**
- **Configuration de la mise en miroir des ports**

Outils réseau

Utilisez les outils réseau pour résoudre les problèmes réseau.

Utilisation de l'outil PING

Vous pouvez utiliser l'utilitaire PING pour tester la connectivité entre ce routeur et un autre périphérique du réseau. Vous pouvez également utiliser l'outil PING pour tester la connectivité à Internet en envoyant une requête Ping à un nom de domaine complet (par exemple, www.cisco.com).

Pour utiliser l'outil PING :

ÉTAPE 1 Sélectionnez **Administration** > **Diagnostics** > **Outils réseau**.

ÉTAPE 2 Dans le champ **Adresse IP/nom de domaine**, saisissez l'adresse IP du périphérique ou un nom de domaine complet, tel que www.cisco.com, où envoyer la requête Ping.

ÉTAPE 3 Cliquez sur **Ping**. Les résultats de la requête Ping s'affichent. Ces résultats indiquent si le périphérique est joignable.

ÉTAPE 4 Cliquez sur **Fermer** lorsque vous avez terminé.

Utilisation de Traceroute

L'utilitaire Traceroute affiche tous les routeurs présents entre l'adresse IP de destination et ce routeur. Le routeur affiche jusqu'à 30 sauts (routeurs intermédiaires) entre ce routeur et la destination.

Pour utiliser Traceroute :

ÉTAPE 1 Sélectionnez **Administration** > **Diagnostics** > **Outils réseau**.

ÉTAPE 2 Dans le champ **Adresse IP/nom de domaine**, saisissez l'adresse IP à suivre.

ÉTAPE 3 Cliquez sur **Traceroute**. Les résultats Traceroute s'affichent.

ÉTAPE 4 Cliquez sur **Fermer** lorsque vous avez terminé.

Recherche DNS

Vous pouvez utiliser l'outil de recherche pour trouver l'adresse IP d'un hôte (par exemple, un serveur Web, FTP ou de messagerie) sur Internet.

Pour récupérer l'adresse IP d'un serveur Web, FTP, de messagerie ou autre sur Internet, saisissez le Nom Internet dans la zone de texte correspondante, puis cliquez sur **Rechercher**. Si l'hôte ou le domaine saisi existe, vous obtenez une réponse contenant l'adresse IP. Un message Hôte inconnu indique que le Nom Internet spécifié n'existe pas.

Pour utiliser l'outil de recherche :

ÉTAPE 1 Sélectionnez **Administration** > **Diagnostics** > **Outils réseau**.

ÉTAPE 2 Dans le champ **Nom Internet**, saisissez le nom Internet de l'hôte.

ÉTAPE 3 Cliquez sur **Rechercher**. Les résultats de la recherche s'affichent.

ÉTAPE 4 Cliquez sur **Fermer** lorsque vous avez terminé.

Configuration de la mise en miroir des ports

La mise en miroir des ports surveille le trafic réseau en envoyant des copies de tous les paquets entrants et sortants d'un port à un port de surveillance. La mise en miroir des ports peut servir d'outil de diagnostic ou de débogage, en particulier pour repousser une attaque ou pour surveiller le trafic utilisateur de LAN à WAN afin de voir si les utilisateurs accèdent à des informations ou à des sites Web inappropriés.

L'hôte LAN (PC) doit utiliser une adresse IP statique pour éviter tout problème avec la mise en miroir des ports. Les baux DHCP d'un hôte LAN peuvent expirer et entraîner l'échec de la mise en miroir des ports si une adresse IP statique n'est pas configurée pour l'hôte LAN.

Pour configurer la mise en miroir des ports :

ÉTAPE 1 Sélectionnez **Administration** > **Diagnostics** > **Mise en miroir de ports**.

ÉTAPE 2 Dans le champ **Source miroir**, sélectionnez les ports à mettre en miroir.

ÉTAPE 3 Dans le menu déroulant **Mettre le port en miroir**, sélectionnez un port miroir. Si vous utilisez un port pour la mise en miroir, ne l'utilisez pas pour d'autres types de trafic.

ÉTAPE 4 Cliquez sur **Enregistrer**.

Configuration de la journalisation

Le Cisco RV215W vous permet de configurer les options de journalisation.

Configuration des paramètres de journalisation

Pour configurer la journalisation :

ÉTAPE 1 Sélectionnez **Administration** > **Journalisation** > **Paramètres de journal**.

ÉTAPE 2 Dans le champ **Mode journalisation**, cochez la case **Activer**.

ÉTAPE 3 Cliquez sur **Ajouter une ligne**.

ÉTAPE 4 Configurez les paramètres suivants :

Serveur de journalisation distant	Saisissez l'adresse IP du serveur de journalisation qui recueille les journaux.
Indiquer la gravité pour le journal local et e-mail	Cliquez pour choisir la sévérité des journaux que vous souhaitez configurer. Notez que tous les types de journaux au-delà d'un type sélectionné sont automatiquement inclus et qu'il n'est pas possible de les désélectionner. Par exemple, le fait de choisir les journaux d'erreurs inclut automatiquement les journaux d'urgence, d'alerte et d'événement critique, en plus des journaux d'erreurs. Les niveaux de sévérité des événements sont répertoriés du niveau le plus élevé au plus bas, comme suit : • **Urgence** : le système n'est pas utilisable. • **Alerte** : une action est requise. • **Critique** : le système est dans un état critique. • **Erreur** : le système subit une condition d'erreur. • **Avertissement** : un avertissement système a été généré. • **Notification** : le système fonctionne correctement, mais une notification système a été générée. • **Information** : informations concernant l'appareil. • **Débogage** : fournit des informations détaillées sur un événement. La sélection de cette option de sévérité entraîne la génération de grandes quantités de journaux et n'est pas recommandée dans le cadre d'un fonctionnement normal du routeur.
Activer	Cochez cette case pour activer ces paramètres de journalisation.

ÉTAPE 5 Cliquez sur **Enregistrer**.

Pour modifier une entrée dans la **Table des paramètres de journalisation**, sélectionnez l'entrée en question, puis cliquez sur **Modifier**. Apportez les modifications voulues, puis cliquez sur **Enregistrer**.

Configuration des paramètres d'e-mail

Vous pouvez configurer le routeur Cisco RV215W pour envoyer des journaux, des alertes de micrologiciel et des alertes 3G par e-mail. Nous vous conseillons de configurer un compte d'e-mail pour envoyer et recevoir des alertes électroniques.

Pour configurer les paramètres d'e-mail :

ÉTAPE 1 Sélectionnez **Administration** > **Journalisation** > **Paramètres d'e-mail**.

ÉTAPE 2 Dans la section **Configuration d'alertes électroniques** :

- Pour activer l'envoi d'alertes 3G par e-mail, cochez la case **Alerte e-mail 3G**.
- Pour activer l'envoi de journaux par e-mail, cochez la case **Journaux par e-mail**. Veillez à définir la gravité des événements que vous voulez consigner. Pour plus d'informations, reportez-vous à la section **Configuration des paramètres de journalisation**. Le champ **Gravité minimale du journal e-mail** indique la gravité des journaux à prendre en compte. Pour changer le niveau de gravité des journaux, cliquez sur **Configurer gravité**.

  Dans la section **Envoyer les journaux par e-mail selon un horaire**, choisissez les options **Toutes les heures**, **Tous les jours** ou **Toutes les semaines**. Si vous sélectionnez **Jamais**, les journaux ne sont pas envoyés. Si vous avez choisi d'envoyer les journaux toutes les semaines, choisissez un jour dans la semaine pour envoyer les journaux. Si vous avez choisi d'envoyer les journaux tous les jours ou toutes les semaines, sélectionnez l'heure de la journée à laquelle le routeur doit envoyer les journaux.

ÉTAPE 3 Dans la section **Paramètres d'e-mail**, saisissez les informations suivantes pour configurer les paramètres d'envoi des alertes par e-mail :

Adresse du serveur de messagerie	Saisissez l'adresse IP du serveur SMTP. Il s'agit du serveur de messagerie associé au compte de messagerie que vous avez configuré (par exemple, mail.nom_entreprise.com).
Port du serveur de messagerie	Saisissez le port du serveur SMTP. Si votre fournisseur de messagerie demande un port spécial pour le courrier électronique, entrez-le à cet emplacement. Dans le cas contraire, utilisez la valeur par défaut (25).
Adresse e-mail de l'expéditeur	Saisissez l'adresse e-mail de l'expéditeur à laquelle le routeur devra Cisco RV215W envoyer les messages si les alertes envoyées du routeur ne sont pas livrées à l'adresse e-mail de destination.
Adresse e-mail de destination (1)	Saisissez l'adresse e-mail à laquelle envoyer les alertes (par exemple, logging@nom_entreprise.com).
Adresse e-mail de destination (2) (facultatif)	Saisissez une autre adresse e-mail à laquelle envoyer les alertes.
Adresse e-mail de destination (3) (facultatif)	Saisissez une autre adresse e-mail à laquelle envoyer les alertes.
Chiffrement e-mail (SSL)	Cochez la case **Activer** pour activer le cryptage e-mail.
Authentification avec serveur SMTP	Si le serveur (de messagerie) SMTP exige une authentification avant d'accepter les connexions, sélectionnez le type d'authentification dans le menu déroulant : **Aucun**, **CONNEXION**, **SIMPLE** et **CRAM-MD5**.
Nom d'utilisateur d'authentification e-mail	Saisissez le nom d'utilisateur pour l'authentification e-mail (par exemple, logging@nom_entreprise.com).

Mot de passe d'authentification e-mail	Saisissez le mot de passe d'authentification e-mail (par exemple, le mot de passe utilisé pour accéder au compte d'e-mail que vous avez configuré pour recevoir les alertes).
Test d'authentification e-mail	Cliquez sur **Test** pour tester l'authentification e-mail.

ÉTAPE 4 Dans la section **Envoyer les journaux par e-mail selon un horaire**, configurez les paramètres suivants :

Unité	Sélectionnez l'unité de temps pour les journaux (**Jamais**, **Toutes les heures**, **Tous les jours** ou **Toutes les semaines**). Si vous sélectionnez **Jamais**, les journaux ne sont pas envoyés.
Jour	Si vous choisissez une fréquence d'envoi hebdomadaire des journaux, sélectionnez le jour de la semaine auquel envoyer les journaux.
Heure	Si vous choisissez une fréquence d'envoi quotidienne ou hebdomadaire des journaux, sélectionnez l'heure de la journée à laquelle envoyer les journaux.

ÉTAPE 5 Cliquez sur **Enregistrer**.

Configuration de Bonjour

Bonjour est un protocole de découverte et d'annonce de service. Sur le Cisco RV215W, Bonjour doit être activé pour annoncer les services par défaut configurés sur le périphérique.

Pour activer Bonjour :

ÉTAPE 1 Sélectionnez **Administration** > **Bonjour**.

ÉTAPE 2 Cochez la case **Activer** pour activer le protocole Bonjour.

ÉTAPE 3 Pour activer Bonjour pour un réseau VLAN répertorié dans la **Table des commandes d'interface Bonjour**, cochez la case **Activer Bonjour** correspondante.

Vous pouvez activer Bonjour sur des réseaux VLAN spécifiques. L'activation de Bonjour sur un réseau VLAN permet aux périphériques présents sur le réseau VLAN de détecter les services Bonjour disponibles sur le routeur (tels que HTTP/HTTPS).

Par exemple, si un réseau VLAN est configuré avec un ID de 2, les périphériques et les hôtes présents sur un réseau VLAN 2 ne peuvent pas découvrir les services Bonjour exécutés sur le routeur à moins que Bonjour soit activé pour VLAN 2.

ÉTAPE 4 Cliquez sur **Enregistrer**.

Configuration des paramètres de date et d'heure

Vous pouvez configurer votre fuseau horaire, indiquer s'il faut ou non prendre en compte l'heure d'été et définir le serveur NTP (Network Time Protocol) avec lequel synchroniser la date et l'heure. Le routeur obtient alors ses informations de date et d'heure du serveur NTP.

Pour configurer les paramètres NTP et d'heure :

ÉTAPE 1 Sélectionnez **Administration** > **Paramètres horaires**. L'heure actuelle s'affiche.

ÉTAPE 2 Précisez les informations suivantes :

Fuseau horaire	Sélectionnez votre fuseau horaire par rapport à l'heure de Greenwich (GMT).
Prendre en compte l'heure d'été	Si cela est pertinent pour votre zone géographique, cochez la case **Prendre en compte l'heure d'été**. Cette option est disponible lorsque vous cliquez sur **Automatique** dans le champ **Définir la date et l'heure** plus bas.

Mode heure d'été	Choisissez **Par date** (vous devez alors indiquer la date à laquelle le mode heure d'été commence) ou **Récurrent** (vous devez alors indiquer le mois, la semaine, le jour de la semaine et l'heure à laquelle l'heure d'été commence). Saisissez les informations appropriées dans les champs « de » et « à ».
Décalage dû à l'heure d'été	Dans le menu déroulant, sélectionnez le décalage par rapport au temps universel coordonné (UTC).
Définir la date et l'heure	Sélectionnez le mode de définition de la date et de l'heure.
Serveur NTP	Pour utiliser les serveurs NTP par défaut, cliquez sur le bouton **Utiliser les valeurs par défaut**. Pour utiliser un serveur NTP spécifique, cliquez sur **Serveur NTP défini par l'utilisateur** et saisissez le nom de domaine complet ou l'adresse IP du serveur NTP dans les deux champs disponibles.
Entrer la date et l'heure	Saisissez la date et l'heure.

ÉTAPE 3 Cliquez sur **Enregistrer**.

Sauvegarde et restauration du système

Vous pouvez sauvegarder les paramètres de configuration personnalisés pour une restauration ultérieure ou restaurer depuis une précédente sauvegarde à partir de la page **Administration** > **Paramètres de sauvegarde/restauration**.

Lorsque le pare-feu fonctionne tel que configuré, vous pouvez sauvegarder la configuration pour une restauration ultérieure. Lors de la sauvegarde, vos paramètres sont enregistrés sous la forme d'un fichier sur votre ordinateur. Vous pouvez restaurer les paramètres du pare-feu à partir de ce fichier.



ATTENTION Lors d'une restauration, n'essayez pas de naviguer en ligne, ne désactivez pas le pare-feu, n'arrêtez pas l'ordinateur et n'utilisez pas le pare-feu jusqu'au terme de l'opération. Celle-ci doit prendre environ une minute. Lorsque le voyant de test s'éteint, patientez encore quelques secondes avant d'utiliser le pare-feu.

Sauvegarde des paramètres de configuration

Pour sauvegarder ou restaurer la configuration :

ÉTAPE 1 Sélectionnez **Administration** > **Paramètres de sauvegarde/restauration**.

ÉTAPE 2 Sélectionnez la configuration à sauvegarder ou à effacer :

Configuration de démarrage	Sélectionnez cette option pour télécharger la configuration de démarrage. La configuration de démarrage est la configuration d'exécution la plus couramment utilisée par le routeur. En cas de perte de la configuration de démarrage, utilisez cette page pour copier les informations de la configuration de secours dans la configuration de démarrage et conserver toutes les informations de configuration antérieures. Vous pouvez télécharger la configuration de démarrage sur d'autres routeurs Cisco RV215W pour faciliter le déploiement.
Configuration miroir	Sélectionnez cette option pour commander au routeur de sauvegarder la configuration de démarrage après 24 heures de fonctionnement sans aucune modification dans la configuration de démarrage.
Configuration de secours	Sélectionnez cette option pour sauvegarder les paramètres de configuration actuels.

ÉTAPE 3 Pour télécharger le fichier de sauvegarde sur votre ordinateur, cliquez sur **Télécharger**.

Par défaut, le fichier (startup.cfg, mirror.cfg ou backup.cfg) est téléchargé dans le dossier Téléchargements par défaut ; par exemple, C:\Documents and Settings\admin\Mes documents\Téléchargements\.

Pour enregistrer un fichier de sauvegarde à un emplacement donné sur un lecteur USB, cliquez sur **Enregistrer sur USB.**

ÉTAPE 4 Pour effacer la configuration sélectionnée, cliquez sur **Supprimer**.

Restauration des paramètres de configuration

Pour restaurer un fichier de configuration préalablement enregistré :

ÉTAPE 1 Sélectionnez **Administration** > **Paramètres de sauvegarde/restauration**.

ÉTAPE 2 Dans le champ Téléchargement de la configuration, sélectionnez la configuration à charger (**Configuration de démarrage** ou **Configuration de secours**).

ÉTAPE 3 Vous pouvez charger le fichier de configuration depuis votre PC ou un lecteur USB externe.

Pour télécharger le fichier de configuration depuis votre ordinateur, cliquez sur la case d'option **PC**. Cliquez sur **Parcourir** pour trouver le fichier. Sélectionnez le fichier, puis cliquez sur **Ouvrir**.

Pour télécharger le fichier de configuration depuis un emplacement sur un lecteur USB, cliquez sur la case d'option **USB**. Cliquez sur **Afficher USB** pour afficher tous les lecteurs USB connectés. Recherchez le fichier sur le lecteur USB et cliquez sur **Ouvrir**.

REMARQUE Le routeur prend en charge le format de fichier NTFS en mode lecture seule et les formats de fichier FAT et FAT32 en mode lecture/écriture sur les lecteurs USB.

ÉTAPE 4 Cliquez sur **Lancer le téléchargement**.

Le routeur charge le fichier de configuration et utilise les paramètres qu'il contient pour mettre à jour la configuration de démarrage. Puis il redémarre et utilise la nouvelle configuration.

Copie des paramètres de configuration

Copiez la configuration de démarrage dans la configuration de secours pour être sûr de disposer d'une copie de secours si vous oubliez votre nom d'utilisateur et votre mot de passe et si vous ne parvenez plus à accéder au Gestionnaire de périphérique. Dans ce cas, le seul moyen d'accéder au Gestionnaire de périphérique est de rétablir les paramètres par défaut du routeur.

Le fichier de la configuration de secours reste en mémoire et permet de copier les informations de configuration sauvegardées dans la configuration de démarrage, qui restaure l'ensemble des paramètres.

Pour copier une configuration (par exemple, pour copier une configuration de démarrage vers la configuration de secours) :

ÉTAPE 1 Sélectionnez **Administration** > **Paramètres de sauvegarde/restauration**.

ÉTAPE 2 Dans le champ **Copier**, sélectionnez les configurations source et destination dans les menus déroulants.

ÉTAPE 3 Cliquez sur **Lancer la copie**.

Génération d'une clé de cryptage

Le routeur vous permet de générer une clé de cryptage pour protéger les fichiers de secours.

Pour générer une clé de cryptage :

ÉTAPE 1 Sélectionnez **Administration** > **Paramètres de sauvegarde/restauration**.

ÉTAPE 2 Cliquez sur **Afficher les paramètres avancés**.

ÉTAPE 3 Dans la case, saisissez la valeur de départ utilisée pour générer la clé.

ÉTAPE 4 Cliquez sur **Enregistrer**.

Mise à niveau du micrologiciel ou changement de la langue

Vous pouvez mettre à niveau le micrologiciel vers une version plus récente ou modifier la langue du routeur depuis la page **Administration** > **Mise à niveau du micrologiciel/de la langue**.



ATTENTION Lors d'une mise à niveau du micrologiciel, n'essayez pas de naviguer en ligne, ne désactivez pas l'appareil, n'arrêtez pas l'ordinateur et n'interrompez surtout pas le processus jusqu'au terme de l'opération. Ce processus prend environ une minute, redémarrage inclus. L'interruption du processus de mise à niveau à certains moments de l'écriture de la mémoire flash peut la corrompre et rendre le routeur inutilisable.

Mise à niveau automatique du micrologiciel

ÉTAPE 1 Choisissez **Administration** > **Mise à niveau du micrologiciel/de la langue**.

ÉTAPE 2 Dans la section **Mise à niveau automatique du micrologiciel**, sélectionnez la fréquence à laquelle vous souhaitez que le routeur recherche des mises à jour du micrologiciel dans le champ **Intervalle - Vérifier tous les**.

ÉTAPE 3 Dans le champ **Mettre à niveau automatiquement**, choisissez si vous souhaitez procéder à la mise à niveau immédiatement une fois qu'une nouvelle version du micrologiciel est détectée ou à un moment spécifié.

ÉTAPE 4 Pour être notifié lorsqu'une nouvelle version du micrologiciel est disponible ou après la mise à niveau vers la dernière version, cochez une des cases suivantes :

- **Notifier via Interface d'administration** : recevez des notifications sur l'interface d'administration du routeur RV215W lorsque vous ouvrez une nouvelle session.
- **Envoyer par e-mail à** : recevez des notifications via des e-mails d'alerte. Cliquez sur **Adresse e-mail** pour configurer les paramètres d'e-mail. Cette case à cocher est estompée si l'option **Alerte par e-mail en cas de nouveau micrologiciel** n'est pas activée. Pour plus d'informations, reportez-vous à la section **Configuration des paramètres d'e-mail**.

ÉTAPE 5 Cliquez sur **Enregistrer**.

Mise à niveau automatique du micrologiciel et de la configuration depuis un lecteur USB

Pour mettre à niveau automatiquement le micrologiciel et la configuration depuis un lecteur USB :

ÉTAPE 1 Choisissez **Activer** dans le champ **Mettre à niveau à partir du périphérique USB au démarrage de l'appareil**.

Avec ce paramètre de déploiement automatique, si le lecteur USB est inséré :

- le micrologiciel du routeur est mis à niveau automatiquement dès qu'il est mis sous tension ;
- le fichier de configuration est mis à jour automatiquement lorsque le routeur est mis sous tension et dès que ses paramètres par défaut sont rétablis.

ÉTAPE 2 Cliquez sur **Enregistrer**.

Mise à niveau manuelle du micrologiciel

ÉTAPE 1 Choisissez **Administration** > **Mise à niveau manuelle du micrologiciel/de la langue**.

ÉTAPE 2 Dans la section **Mise à niveau du micrologiciel/de la langue**, cliquez sur la case d'option **Image du micrologiciel** dans le champ **Type de fichier**.

ÉTAPE 3 Téléchargez la dernière version du micrologiciel sur votre PC ou un lecteur USB. Pour télécharger la dernière version du micrologiciel depuis cisco.com sur un lecteur USB, cliquez sur **Démarrer le téléchargement** dans **Enregistrer sur USB à partir de cisco.com**.

ÉTAPE 4 Pour procéder à la mise à niveau vers la dernière version du micrologiciel, choisissez l'une des options suivantes :

- **cisco.com** : téléchargez le micrologiciel depuis le site Web cisco.com.
- **PC** : cliquez sur **Parcourir** pour rechercher et sélectionner le micrologiciel téléchargé sur votre ordinateur.
- **USB** : cliquez sur **Afficher USB** pour afficher tous les fichiers sur le lecteur USB dans la **table de contenus du lecteur USB**. Recherchez et sélectionnez le fichier du micrologiciel.

REMARQUE Le routeur prend en charge le format de fichier NTFS en mode lecture seule et les formats de fichier FAT et FAT32 en mode lecture/écriture sur les lecteurs USB.



ATTENTION Si vous rétablissez les paramètres par défaut du routeur, tous les paramètres de configuration seront supprimés.

ÉTAPE 5 Cliquez sur **Démarrer la mise à niveau**.

Une fois validée, la nouvelle image du micrologiciel est enregistrée dans la mémoire flash et le routeur redémarre automatiquement avec le nouveau micrologiciel. La section **Informations système** indique la dernière version installée du micrologiciel.

Changement de la langue

Pour changer la langue :

ÉTAPE 1 Sélectionnez **Administration** > **Mise à niveau du micrologiciel/de la langue**.

ÉTAPE 2 Dans le champ **Type de fichier**, cliquez sur le bouton **Fichier de langue**.

ÉTAPE 3 Cliquez sur **Parcourir** pour rechercher et sélectionner le fichier de langue.

ÉTAPE 4 Le cas échéant, pour rétablir les valeurs par défaut des paramètres de configuration du routeur, sélectionnez **Rétablir tous les paramètres/ configurations d'usine**.

ÉTAPE 5 Cliquez sur **Démarrer la mise à niveau**.

Redémarrage du Cisco RV215W

Pour redémarrer le routeur :

ÉTAPE 1 Sélectionnez **Administration** > **Redémarrer**.

ÉTAPE 2 Cliquez sur **Redémarrer**.

Restauration des paramètres d'usine

ATTENTION Lors d'une restauration, n'essayez pas de naviguer en ligne, ne désactivez pas le routeur, n'arrêtez pas l'ordinateur et n'utilisez pas le routeur jusqu'au terme de l'opération. Celle-ci devrait prendre environ une minute. Lorsque le voyant de test s'éteint, patientez encore quelques secondes avant d'utiliser le routeur.

Pour rétablir les paramètres d'usine du routeur :

ÉTAPE 1 Sélectionnez **Administration** > **Rétablir les paramètres d'usine**.

ÉTAPE 2 Cliquez sur **Par défaut**.

Exécution de l'Assistant de configurations

Pour exécuter l'Assistant de configurations :

ÉTAPE 1 Sélectionnez **Administration** > **Assistant de configurations**.

ÉTAPE 2 Suivez les instructions en ligne.

A

Utilisation de Cisco QuickVPN

Présentation

Cette annexe explique comment installer et utiliser le logiciel Cisco QuickVPN, disponible en téléchargement depuis Cisco.com. QuickVPN est compatible avec les ordinateurs fonctionnant sous Windows 7, Windows XP, Windows Vista ou Windows 2000 (les ordinateurs fonctionnant avec d'autres systèmes d'exploitation devront utiliser un logiciel VPN tiers).

Cette annexe comprend les sections suivantes :

- **Avant de commencer**
- **Installation du logiciel Cisco QuickVPN**
- **Utilisation du logiciel Cisco QuickVPN**

Avant de commencer

Le programme QuickVPN fonctionne uniquement avec un routeur correctement configuré pour accepter une connexion QuickVPN. Procédez comme suit :

ÉTAPE 1 Activez la gestion à distance. Reportez-vous à la section **Configuration des paramètres de base du pare-feu**.

ÉTAPE 2 Créez des comptes d'utilisateur QuickVPN. Reportez-vous à la section **Configuration du protocole PPTP**. Une fois le compte d'utilisateur créé, les informations de connexion peuvent être utilisées par le client QuickVPN.

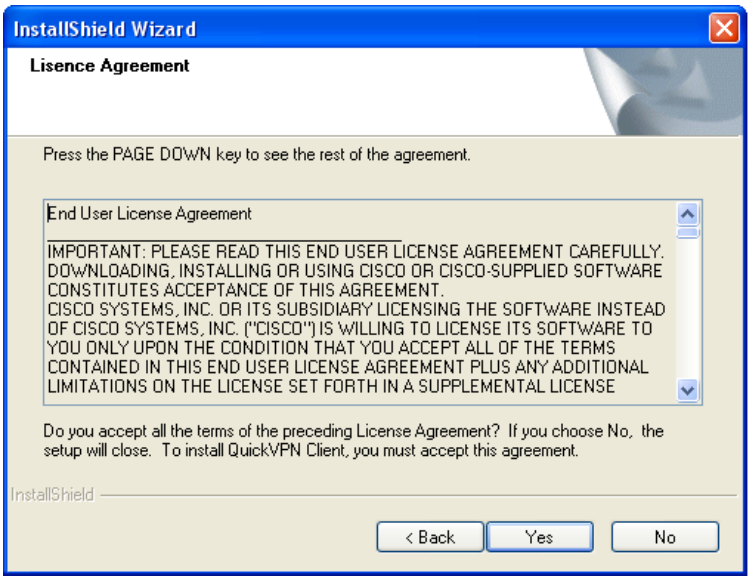
Installation du logiciel Cisco QuickVPN

Installation à partir du CD-ROM

ÉTAPE 1 Insérez le CD-ROM du Cisco RV215W dans le lecteur de CD-ROM. Lorsque l'Assistant de configurations démarre, cliquez sur le lien **Install QuickVPN** (installer QuickVPN).

La fenêtre License Agreement (contrat de licence) s'affiche.

Contrat de licence



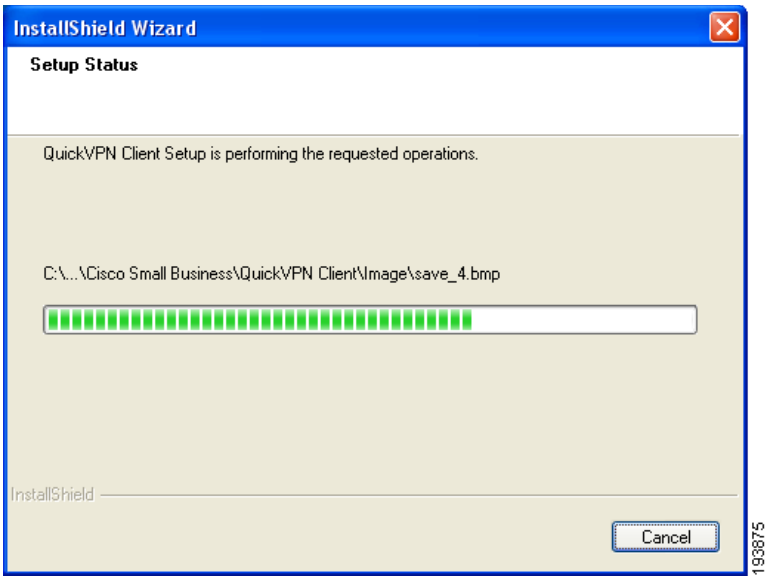
ÉTAPE 2 Cliquez sur **Yes** (oui) pour accepter le contrat.

ÉTAPE 3 Cliquez sur **Parcourir** et choisissez la destination de copie des fichiers (par exemple, C:\Cisco Small Business\QuickVPN Client).

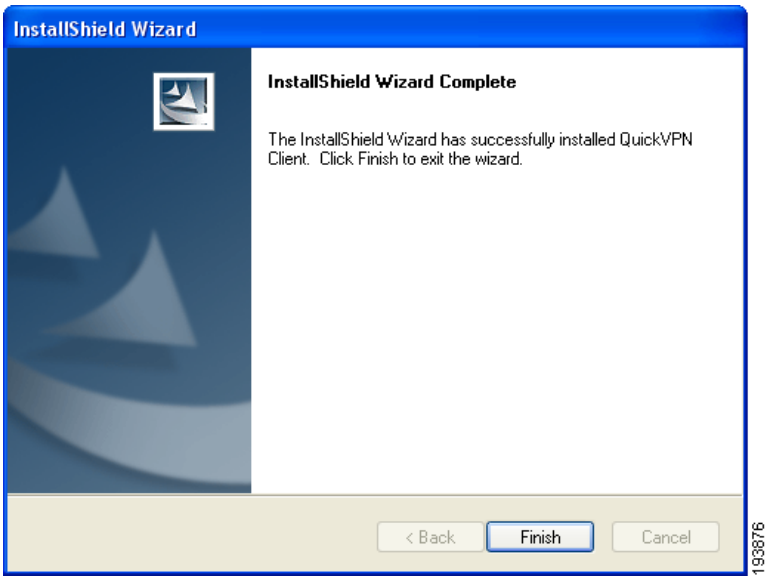
ÉTAPE 4 Cliquez sur **Next** (suivant).

L'Assistant de configurations copie les fichiers vers l'emplacement sélectionné.

Copie des fichiers



Installation des fichiers terminée



ÉTAPE 5 Cliquez sur **Finish** (terminer) pour terminer l'installation. Passez à la section **? Utilisation du logiciel Cisco QuickVPN ? page 155**.

Téléchargement et installation à partir d'Internet

ÉTAPE 1 Consultez la section Téléchargements de logiciel à l'**Annexe B, ? Pour en savoir plus ?**

ÉTAPE 2 Saisissez Cisco RV215W dans la zone de recherche et recherchez le logiciel **QuickVPN**.

ÉTAPE 3 Enregistrez le fichier .zip sur votre ordinateur avant d'extraire le fichier .exe.

ÉTAPE 4 Double-cliquez sur le fichier .exe, puis suivez les instructions affichées à l'écran.

Utilisation du logiciel Cisco QuickVPN

ÉTAPE 1 Double-cliquez sur l'icône Cisco QuickVPN située sur le Bureau ou dans la barre d'état système.

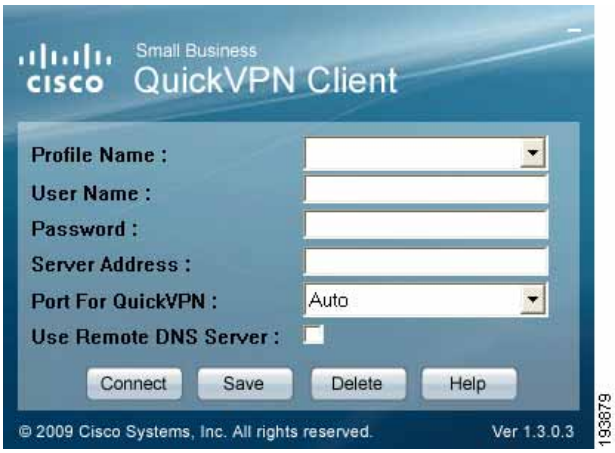


Icône QuickVPN du Bureau



Icône QuickVPN de la barre d'état système – Pas de connexion

La fenêtre QuickVPN Login (connexion à QuickVPN) s'affiche.



ÉTAPE 2 Dans le champ **Profile Name** (nom de profil), saisissez le nom à attribuer à votre profil.

ÉTAPE 3 Dans les champs **User Name** et **Password** (Nom d'utilisateur et Mot de passe), saisissez le nom d'utilisateur et le mot de passe.

ÉTAPE 4 Dans le champ **Server Address** (adresse de serveur), saisissez l'adresse IP ou le nom de domaine du Cisco RV215W.

ÉTAPE 5 Dans le champ **Port For QuickVPN** (port pour QuickVPN), saisissez le numéro de port qu'utilise le client QuickVPN pour communiquer avec le routeur VPN distant, ou laissez le paramètre par défaut, **Auto** (automatique).

ÉTAPE 6 Pour enregistrer ce profil, cliquez sur **Save** (enregistrer).

Pour supprimer ce profil, cliquez sur **Delete** (supprimer). Pour obtenir plus d'informations, cliquez sur **Help** (aide).

REMARQUE Si vous êtes amené à créer des tunnels vers plusieurs sites, vous pouvez créer plusieurs profils, mais un seul tunnel pourra être actif à la fois.

ÉTAPE 7 Pour lancer la connexion QuickVPN, cliquez sur **Connect** (se connecter).

L'évolution de la connexion s'affiche : Connecting (connexion), Provisioning (mise en service), Activating Policy (activation de la stratégie) et Verifying Network (vérification du réseau).

ÉTAPE 8 Une fois la connexion QuickVPN établie, l'icône QuickVPN dans la barre des tâches devient verte et la fenêtre QuickVPN Status (état QuickVPN) s'affiche.

La fenêtre affiche l'adresse IP de l'extrémité distante du tunnel VPN, la date et l'heure d'ouverture du tunnel VPN et la durée totale d'activité du tunnel VPN.



Icône QuickVPN de la barre d'état système – Connexion



Pour désactiver le tunnel VPN, cliquez sur **Disconnect** (déconnecter). Pour modifier le mot de passe, cliquez sur **Change Password** (modifier le mot de passe). Pour obtenir plus d'informations, cliquez sur **Help** (aide).

ÉTAPE 9 Si vous avez cliqué sur **Change Password** (modifier le mot de passe) et que vous êtes autorisé à modifier votre propre mot de passe, la fenêtre **Connect Virtual Private Connection** (connexion privée virtuelle) s'affiche.



ÉTAPE 10 Saisissez votre mot de passe dans le champ **Old Password** (ancien mot de passe). Saisissez votre nouveau mot de passe dans le champ **New Password** (nouveau mot de passe). Saisissez-le à nouveau dans le champ **Confirm New Password** (confirmer le nouveau mot de passe).

ÉTAPE 11 Cliquez sur **OK** pour enregistrer votre nouveau mot de passe.

REMARQUE Vous pouvez modifier votre mot de passe seulement si la case **Allow User to Change Password** (autoriser l'utilisateur à modifier le mot de passe) a été cochée pour votre nom d'utilisateur.

B

Pour en savoir plus

Assistance	
Communauté d'assistance Cisco	www.cisco.com/go/smallbizsupport
Assistance et documentation techniques en ligne (identification requise)	www.cisco.com/support
Assistance téléphonique	www.cisco.com/en/US/support/tsd_cisco_small_ business_support_ center_contacts.html
Téléchargements de logiciel (identification requise)	Rendez-vous sur le site tools.cisco.com/support/downloads, puis saisissez le numéro du modèle dans la zone de recherche de logiciels Software Download Search.

Documentation sur les produits	
Pare-feu VPN Wireless-N	www.cisco.com/en/US/products/ps9923/tsd_products_support_series_home.html
Cisco Partner Central (connexion partenaire requise)	www.cisco.com/web/partners/sell/smb
Marketplace	www.cisco.com/go/marketplace