GUIDE D'ADMINISTRATION

Cisco Routeur VPN multifonction RV130

Cisco Routeur VPN multifonction sans fil RV130W

Version révisée décembre 2016

78-21401-01

Table des matières

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 par navigateur.

Vérification de l'installation matérielle

Configurez le périphérique à connecter aux réseaux filaires ou sans fil à l'aide du Guide de démarrage rapide du routeur VPN multifonction sans fil Cisco RV130/130W.

AVERTISSEMENT Utilisez l'alimentation de 12 V, 2 A fournie avec le périphérique. L'utilisation d'une autre alimentation est susceptible de dégrader les performances ou d'endommager l'appareil.

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

- Vérifiez l'état des voyants LED. Pour plus d'informations, reportez-vous au Guide de démarrage rapide du routeur VPN multifonction sans fil Cisco RV130/130W fourni avec le routeur.
- 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.

- 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 configuration

L'Assistant Installation et le Gestionnaire de périphérique sont pris en charge 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 configuration :

ÉTAPE 1 Démarrez l'ordinateur que vous avez connecté à un port LAN.

L'ordinateur devient un client DHCP de votre périphérique 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 de votre 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 **Se connecter**. L'Assistant configuration démarre.

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

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

Une fois que l'Assistant configuration a terminé de configurer le périphérique, vous devez modifier 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 configuration configure automatiquement le périphérique, il est recommandé de personnaliser certains des paramètres pour renforcer la sécurité et améliorer les performances.

- 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 de réseau local (LAN)**.
- Pour configurer votre réseau privé virtuel (VPN), reportez-vous à la section **Configuration de VPN**.
- Votre périphérique prend en charge jusqu'à quatre réseaux sans fil. Vous ne pouvez configurer qu'un seul réseau sans fil (ou SSID) avec l'Assistant configuration. Pour configurer des réseaux sans fil supplémentaires, utilisez le Gestionnaire de périphérique Web. Reportez-vous à la section **Configuration des réseaux sans fil**.

Mise en route

Utilisation de la page Mise en route

La page **Mise en route** affiche les tâches de configuration les plus courantes de votre périphérique. Cliquez sur les liens de la page Web pour accéder à la page de configuration appropriée.

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 configuration	Lance l'Assistant configuration. Suivez les instructions affichées à l'écran.

Configurer les paramètres WAN	Ouvre la page **Configuration Internet** pour modifier les paramètres. Par exemple, le nom d'hôte du périphérique. Reportez-vous à la section **Configuration des paramètres WAN**.
Configurer les paramètres LAN	Ouvre la page **Configuration LAN** pour modifier les paramètres du réseau local. Par exemple, l'adresse IP de gestion. Reportez-vous à la section **Configuration des paramètres de réseau local (LAN)**.
Configurer les paramètres sans fil	Ouvre la page **Paramètres de base** pour gérer la radio. Reportez-vous à la section **Configuration des réseaux sans fil**.

Accès rapide

Mettre à niveau le micrologiciel du routeur	Ouvre la page **Mise à niveau du micrologiciel/de la langue** pour mettre à jour le micrologiciel ou le module linguistique du périphérique. Reportez-vous à la section **Mise à niveau du micrologiciel ou changement de la langue**.
Ajouter des clients VPN	Ouvre la page **Serveur PPTP** pour configurer et gérer des tunnels VPN. Reportez-vous à la section **Configuration du protocole PPTP**.
Configurer l'accès pour la gestion à distance	Ouvre la page **Paramètres de base** pour activer les fonctionnalités de base du périphérique. Reportez-vous à la section **Configuration des paramètres de base du pare-feu**.

État du périphérique

Récapitulatif système	Affiche la page **Récapitulatif du système** qui indique l'état du micrologiciel, l'état de la configuration IPv4 et IPv6, ainsi que l'état de la connexion sans fil et du pare-feu sur le périphérique. Reportez-vous à la section **Affichage du récapitulatif du 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 **Serveur VPN IPSec** qui indique le VPN géré par ce périphérique. Reportez-vous à la section **Affichage de l'état des connexions VPN IPsec site-à-site**.

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.

Connexion au réseau sans fil

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

Les étapes suivantes sont indiquées à titre d'exemple ; vous pouvez choisir une autre configuration pour votre périphérique. Pour obtenir des instructions spécifiques, consultez la documentation de votre périphérique client.

ÉTAPE 1 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 de réseau (SSID) que vous avez choisi pour votre réseau dans l'Assistant configuration.

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

Si vous n'avez pas activé la sécurité (déconseillé), ne renseignez pas les champs de chiffrement 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 périphérique

Utilisez les pages du menu **État** pour consulter les statistiques en temps réel et les paramètres de configuration du VPN, de la connexion sans fil, des services TCP/IP actifs, des paramètres du portail captif et des journaux d'événements sur votre périphérique.

Pour vous assurer que les données et les statistiques seront fréquemment mises à jour sur les pages État, sélectionnez une fréquence d'actualisation dans la liste déroulante **Fréquence d'actualisation**.

Affichage du tableau de bord

Sélectionnez **État** > **Tableau de bord** pour afficher un instantané de la configuration de votre périphérique. La page Tableau de bord affiche des informations sur la version du micrologiciel, l'utilisation du processeur et de la mémoire, les paramètres de journalisation des erreurs, le LAN, le WAN, la connexion sans fil, le VPN IPsec site-à-site et les paramètres de serveur VPN PPTP de votre périphérique.

Pour modifier les informations affichées, cliquez sur le lien **détails** afin d'accéder à la page de configuration pour la section. Pour plus d'informations sur la gestion des paramètres affichés sur la page **Tableau de bord**, reportez-vous aux sections suivantes :

- **Configuration des paramètres de journal**
- **Configuration du VPN IPsec site-à-site de base**
- **Configuration des paramètres de réseau local (LAN)**
- **Configuration des connexions WAN filaires**
- **Configuration des paramètres sans fil de base**

Dans la liste déroulante **Fréquence d'actualisation**, choisissez la fréquence à laquelle les dernières statistiques et valeurs de paramètre seront actualisées sur le tableau de bord.

La page Tableau de bord affiche également une vue interactive du panneau arrière de votre périphérique lorsque vous cliquez sur **Afficher le panneau arrière du routeur**. Placez le curseur de votre souris sur chaque port pour lequel vous souhaitez consulter les informations de connexion.

Affichage du récapitulatif du système

Sélectionnez **État** > **Récapitulatif du système** pour afficher le détail des propriétés, des paramètres réseau pour les différents modes d'adresse IP, du pare-feu, de la connexion sans fil et des paramètres VPN de votre périphérique. Cliquez sur **Actualiser** pour afficher les informations les plus récentes.

Cliquez sur le lien souligne pour accéder à la fenêtre de configuration associée. Par exemple, pour modifier l'adresse IP du LAN, cliquez sur **IP du LAN**. La fenêtre Configuration LAN s'affiche.

La page **Récapitulatif du système** affiche des informations dans les sections suivantes :

Informations système

- **Version du micrologiciel** : version actuelle du logiciel exécutée par le périphérique.
- **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 langue** : somme de contrôle MD5 du module linguistique.
- **Modèle d'UC** : jeu de puces (chipset) du processeur actuellement utilisé.

- **Numéro de série** : numéro de série de l'appareil.
- **Temps de disponibilité du système** : durée de fonctionnement du système.
- **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.
- **IP du réseau WAN** : adresse IP WAN du périphérique. Pour libérer l'adresse IP actuelle et en obtenir une nouvelle, cliquez sur **Libérer** ou sur **Renouveler**.
- **Passerelle** : adresse IP de la passerelle à laquelle le périphérique est connecté (par exemple, le modem câble).
- **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.
- **IP du réseau WAN** : adresse IP WAN du périphérique.
- **Passerelle** : adresse IP de la passerelle à laquelle le périphérique est connecté (par exemple, le modem câble).
- **NTP** : serveur NTP (Network Time Protocol) (nom d'hôte ou adresse IPv6).
- **Longueur du préfixe** : préfixe transmis du périphérique au FAI et qui est attribué aux adresses IPv6 sur le périphérique.
- **DNS 1** : adresse IP du serveur DNS principal.
- **DNS 2** : adresse IP du serveur DNS secondaire.

Récapitulatif du réseau sans fil

Affiche le nom public et les paramètres de sécurité de vos réseaux sans fil configurés sur la page **Sans fil > Paramètres de base**. Pour plus d'informations, reportez-vous à la section **Configuration des paramètres sans fil de base**.

État des paramètres de pare-feu

Affiche les paramètres de DoS (Déni de service), de requête WAN et de gestion à distance configurés sur la page **Pare-feu > Paramètres de base**. Pour plus d'informations, reportez-vous à la section **Configuration des paramètres de base du pare-feu**.

État des paramètres VPN

Affiche les connexions VPN IPsec et PPTP disponibles, ainsi que les utilisateurs connectés pour chaque type de VPN.

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

Pour plus d'informations sur la configuration des connexions de serveur VPN et les comptes d'utilisateurs, reportez-vous aux sections **Configuration du VPN IPsec site-à-site de base** et **Configuration du protocole PPTP**.

Affichage des services TCP/IP actifs

Sélectionnez **État > Services TCP/IP actifs** pour afficher les connexions TCP/IP IPv4 et IPv6 qui sont actives sur votre périphérique. La section **Liste des services actifs** pour IPv4 et IPv6 affiche les protocoles et les services actifs sur le périphérique.

Affichage des statistiques sans fil

Choisissez **État > Statistiques sans fil** pour afficher les données statistiques sans fil de la radio du périphérique. Dans le champ **Fréquence d'actualisation**, choisissez la fréquence à laquelle vous souhaitez que les statistiques les plus à jour soient affichées.

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 réinitialisés au redémarrage de l'appareil.

Affichage de l'état du portail captif

Sélectionnez **État > Portail captif** pour afficher des informations sur les utilisateurs du portail captif qui sont connectés. Pour plus d'informations sur la configuration de portails captifs sur votre périphérique, reportez-vous à la section **Configuration du portail captif**.

Affichage de l'état des connexions VPN IPsec site-à-site

Sélectionnez **État > VPN IPSec site-à-site** pour afficher l'état de connexion des stratégies VPN IPsec site-à-site actives sur le périphérique. Pour obtenir des informations sur la configuration des stratégies VPN, reportez-vous à la section **Configuration du VPN IPsec site-à-site de base**.

Pour changer la fréquence à laquelle l'état de connexion en temps réel et actualisé s'affiche, sélectionnez une fréquence d'actualisation dans la liste déroulante **Fréquence d'actualisation**.

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** et cliquez sur **Enregistrer**.

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

Affichage de l'état du serveur VPN IPsec

Sélectionnez **État > Serveur VPN IPsec** pour afficher la liste de vos connexions VPN IPsec et la durée de la connexion. Pour plus d'informations sur la configuration des connexions VPN IPsec, reportez-vous à la section **Configuration du serveur VPN IPsec**.

Affichage du serveur PPTP

Sélectionnez **État > Serveur PPTP** pour afficher la liste de vos connexions VPN PPTP, la durée de la connexion et les actions que vous pouvez effectuer sur cette connexion. Pour plus d'informations sur la configuration des connexions VPN PPTP, reportez-vous à la section **Configuration du protocole PPTP**.

Affichage des journaux

Sélectionnez **État > Afficher les journaux**. Cliquez sur **Actualiser les journaux** pour afficher les entrées les plus récentes des 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, si vous cochez la case **Erreur**, vous incluez automatiquement les journaux Urgence, Alerte et Critique, en plus des journaux Erreur.

Les niveaux de sévérité des événements sont répertoriés du niveau le plus élevé au plus faible, 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.

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

Pour enregistrer tous les messages de journal depuis le périphérique vers le disque dur local, cliquez sur **Enregistrer les journaux**.

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

Pour parcourir les pages des journaux, utilisez les boutons de navigation.

Affichage des appareils connectés

La page **Appareils connectés** affiche des informations sur les périphériques client actifs connectés à votre routeur. 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.

La **Table ARP IPv4** affiche des informations émanant d'autres routeurs 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.

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 actualiser la page à intervalles réguliers, choisissez une fréquence d'actualisation 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.
Erreur	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 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 (Rx) et transmises (Tx) sur la liaison mobile.
- **Utilisation mensuelle** : données mensuelles téléchargées et utilisation de la bande passante.
- **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.
- **État de la carte** : état de la carte de données.

3

Configuration du réseau

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 (configuration automatique)

Si votre fournisseur d'accès à Internet (FAI) utilise le protocole DHCP (Dynamic Host Control Protocol) pour vous affecter une adresse IP, vous recevez 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 la liste déroulante **Type de connexion Internet**, sélectionnez **Configuration automatique - DHCP**.

ÉTAPE 3 Dans la liste déroulante **Source des serveurs DNS**, choisissez l'une des manières suivantes de définir l'adresse du serveur DNS :

- Si vous avez déjà reçu les adresses de serveur DNS de votre FAI, choisissez **Utiliser ces serveurs DNS**, puis entrez les adresses principale et secondaire.
- Si vous n'avez pas reçu les adresses de serveur DNS de votre FAI, choisissez **Obtention dynamique du FAI**.
- Pour utiliser les serveurs DNS fournis par OpenDNS (208.67.222.222, 208.67.220.220) pour résoudre vos adresses Web, choisissez **Utiliser OpenDNS**.

ÉTAPE 4 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 **IP statique**.

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.
Source des serveurs DNS	Adresse du serveur DNS. Si vous avez déjà reçu les adresses de serveur DNS de votre FAI, choisissez **Utiliser ces serveurs DNS**, puis entrez les adresses principale et secondaire dans les champs **DNS statique 1** et **DNS statique 2**. Pour utiliser les serveurs DNS fournis par OpenDNS (208.67.222.222, 208.67.220.220) pour résoudre vos adresses Web, choisissez **Utiliser OpenDNS**.
Passerelle par défaut	Adresse IP de la passerelle par défaut.

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 Sélectionnez un profil PPPoE ou cliquez sur **Configurer le profil** pour créer un nouveau profil.

ÉTAPE 4 Sur la page Profils PPPoE, saisissez les informations suivantes (contactez le cas échéant votre FAI pour obtenir vos informations de connexion PPPoE) :

Nom du profil	Nom unique pour le profil PPPoE.
Nom d'utilisateur	Nom d'utilisateur attribué par le FAI.
Mot de passe	Mot de passe attribué par le FAI.
Source des serveurs DNS	Adresse du serveur DNS. Si vous avez déjà reçu les adresses de serveur DNS de votre FAI, sélectionnez **Utiliser ces serveurs DNS**, puis entrez les adresses principale et secondaire. Sinon, choisissez **Obtention dynamique du FAI**. Pour utiliser les serveurs DNS fournis par OpenDNS (208.67.222.222, 208.67.220.220) pour résoudre vos adresses Web, choisissez **Utiliser OpenDNS**.
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**.
Maintenir actif	Lorsque vous cochez cette option, la connexion Internet est toujours active. Dans le champ de période de renumérotation, entrez le délai en secondes à l'issue duquel le périphérique, s'il est déconnecté, tente de se reconnecter.

Type d'authentification	**Négociation automatique** : le serveur envoie une demande de configuration spécifiant l'algorithme de sécurité paramétré. Le 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 du protocole CHAP, utilisée pour accéder aux services du FAI.

ÉTAPE 5 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**.
Maintenir actif	Lorsque vous cochez cette option, la connexion Internet est toujours active. Dans le champ **Période de renumérotation**, entrez le délai en secondes à l'issue duquel le périphérique, s'il est déconnecté, tente de se reconnecter.
Type d'authentification	Sélectionnez le type d'authentification : **Négociation automatique** : le serveur envoie une demande de configuration spécifiant l'algorithme de sécurité paramétré. Le périphérique renvoie alors les identifiants d'authentification avec le type de sécurité précédemment envoyé 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 MS-CHAP (Microsoft Challenge Handshake Authentication Protocol) lors de la connexion au FAI.
Nom du service	Entrez un nom pour le nouveau service PPTP.
Chiffrement MPPE	Cochez la case **Activer** de façon à activer le chiffrement MPPE pour la connexion PPTP.

Source des serveurs DNS	Adresse du serveur DNS. Si vous avez déjà reçu les adresses de serveur DNS de votre FAI, choisissez **Utiliser ces serveurs DNS**, puis entrez les adresses principale et secondaire dans les champs **DNS statique 1** et **DNS statique 2**. Pour recevoir les adresses de serveur DNS de votre FAI, choisissez **Obtention dynamique du FAI**. Pour utiliser les serveurs DNS fournis par OpenDNS (208.67.222.222, 208.67.220.220) pour résoudre vos adresses Web, choisissez **Utiliser OpenDNS**.

ÉTAPE 4 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	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 L2TP	Adresse IP du serveur L2TP.
Version	Version L2TP que vous souhaitez utiliser. Si vous sélectionnez la version 3, entrez l'ID de fournisseur et l'ID de circuit virtuel.
Longueur de cookie	Taille du cookie dans le paquet de données L2TP v3, qui identifie la session L2TP.

ID de fournisseur	ID de fournisseur contenu dans le format de codage AVP pour L2TP. Pour utiliser les valeurs d'attribut adoptées par l'IETF dans l'AVP, sélectionnez Standard. Pour implémenter les valeurs d'attribut privées et les extensions L2TP de Cisco, sélectionnez Cisco.
ID de circuit virtuel	Identifiant du circuit Layer 2 via lequel les paquets de données L2TP sont transmis. Ces informations sont requises si vous sélectionnez Cisco comme **ID de fournisseur** pour L2TP v3.
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**.
Maintenir actif	Lorsque vous cochez cette option, la connexion Internet est toujours active. Dans le champ de période de renumérotation, entrez le délai en secondes à l'issue duquel le périphérique, s'il est déconnecté, tente de se reconnecter.

Type d'authentification	**Négociation automatique** : le serveur envoie une demande de configuration spécifiant l'algorithme de sécurité paramétré. Le 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 MS-CHAP (Microsoft Challenge Handshake Authentication Protocol) utilisé lors de la connexion au FAI.
Nom du service	Entrez un nom pour le nouveau service L2TP.
Chiffrement MPPE	Cochez la case **Activer** de façon à activer le chiffrement MPPE pour la connexion L2TP.
Source des serveurs DNS	Adresse du serveur DNS. Si vous avez déjà reçu les adresses de serveur DNS de votre FAI, sélectionnez **Utiliser ces serveurs DNS**, puis entrez les adresses principale et secondaire dans les champs **Serveur DNS principal** et **Serveur DNS secondaire**. Pour recevoir les adresses de serveur DNS de votre FAI, sélectionnez **Obtention dynamique du FAI**. Pour utiliser les serveurs DNS fournis par OpenDNS (208.67.222.222, 208.67.220.220) pour résoudre vos adresses Web, sélectionnez **Utiliser OpenDNS**.

ÉTAPE 4 Cliquez sur **Enregistrer**.

Configuration des paramètres réseau facultatifs

Pour configurer les paramètres facultatifs :

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

MTU	L'unité maximale de transmission (Maximum Transmission Unit, MTU) correspond à la taille du plus gros paquet pouvant être transmis sur le réseau. 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 1 500 octets. Si votre FAI exige un réglage de MTU personnalisé, sélectionnez **Manuel** et modifiez la taille de MTU.
Taille	Taille de MTU personnalisée. La valeur de MTU standard sur les réseaux Ethernet est généralement de 1500 octets. Pour les connexions PPPoE, la valeur est de 1492 octets.
VLAN non balisé	Cochez la case pour activer le balisage de VLAN. Lorsque cette option est activée (paramètre par défaut), tout le trafic est balisé avec un ID de VLAN. Par défaut, la totalité du trafic sur le périphérique utilise le VLAN 1, à savoir le VLAN non balisé par défaut. L'ensemble du trafic est non balisé jusqu'à la désactivation du VLAN non balisé, la modification de l'ID de VLAN du trafic non balisé ou la modification de l'ID de VLAN.
ID VLAN non balisé	Nombre compris entre 1 et 4 094 pour l'ID de VLAN non balisé. La valeur par défaut est 1. Le trafic sur le VLAN que vous spécifiez dans ce champ n'est pas balisé avec un ID de VLAN lors de son transfert sur le réseau. VLAN 1 et le VLAN non balisé par défaut.

VLAN de gestion PA	VLAN associé à l'adresse IP que vous utilisez pour accéder au périphérique lorsqu'il est configuré en tant que point d'accès. Si vous créez des VLAN supplémentaires, pour des raisons de sécurité, sélectionnez une valeur correspondant au VLAN configuré sur les autres commutateurs du réseau. Il peut également être nécessaire de changer le VLAN de gestion pour limiter l'accès au Gestionnaire de périphérique.

ÉTAPE 2 Cliquez sur **Enregistrer**.

Configuration d'un réseau mobile

Sélectionnez **Mise en réseau > WAN > Réseau mobile** pour configurer le périphérique afin qu'il se connecte à un modem USB haut débit mobile, qui est lui-même connecté à son interface USB.

Configuration des paramètres de réseau mobile globaux

Pour configurer les paramètres globaux des périphériques USB pris en charge :

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 Auto, définissez une heure de **Connexion à la demande** ou sélectionnez **Maintenir actif**. L'option Connexion à la demande met fin à la connexion Internet à l'issue de la durée d'inactivité spécifiée dans le champ **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 d'accéder 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. Sélectionnez **Maintenir actif** pour maintenir la connexion active 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.

Configuration manuelle des paramètres de réseau mobile

Pour modifier les paramètres de réseau mobile dans la zone **Configuration du réseau mobile**, sélectionnez la case d'option **Manuel**. L'appareil détecte automatiquement les modems pris en charge et dresse la liste des paramètres de configuration appropriés. Pour remplacer les paramètres globaux, sélectionnez **Manuel**.

ÉTAPE 1 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.
SIM Check	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. Vous pouvez modifier le code PIN de la carte SIM en mode Auto ou Manuel.
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.
LTE Service	Paramètre de service LTE (Long-term Evolution). **Auto** choisit un signal basé sur le signal du service de la zone. **4G uniquement** recherche uniquement les signaux 4G. **3G uniquement** recherche uniquement les signaux 3G.

ÉTAPE 2 Cliquez sur **Enregistrer** pour enregistrer vos paramètres

Paramètre de limite de bande passante

Le périphérique 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 du destinataire, reportez-vous à la section **Configuration de l'envoi des journaux par 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 une connexion Ethernet et une liaison du réseau mobile sont disponibles, une seule connexion à la fois peut être utilisée pour établir une liaison WAN. Lorsqu'une connexion WAN échoue, le périphérique essaie d'établir une connexion sur une autre interface. Cette fonctionnalité est connue sous le nom de basculement. Lorsque la connexion WAN principale est restaurée, le chemin d'origine est rétabli et la connexion de secours est abandonnée. Cette fonctionnalité est connue sous le nom de récupération.

ÉTAPE 1 Sélectionnez **Mise en réseau > WAN > Basculement et récupération** pour afficher la fenêtre Basculement et récupération.

ÉTAPE 2 Sélectionnez **Basculement vers WAN 3G** pour activer la liaison du réseau mobile et la définir pour basculer à partir de la liaison Ethernet. Lorsque la liaison WAN Ethernet n'est pas active, le périphérique tente d'activer la liaison du réseau mobile sur l'interface USB. (Si le basculement n'est pas activé, la liaison du réseau mobile est toujours désactivée.)

ÉTAPE 3 Sélectionnez **Récupération sur WAN Ethernet** pour permettre à la liaison de revenir à la liaison Ethernet, et d'abandonner ainsi la liaison du réseau mobile. Le Mode de connexion **WAN > Réseau mobile** doit être défini sur Automatique pour pouvoir utiliser la récupération de la connexion Ethernet WAN.

ÉTAPE 4 Dans le champ **Intervalle de vérification du basculement**, entrez la fréquence (en secondes) à laquelle le périphérique doit tenter de détecter la connexion physique ou la présence de trafic sur la liaison du réseau mobile. Si la liaison est inactive, le périphérique tente d'envoyer une commande ping vers une destination selon cet intervalle. En l'absence de réponse au paquet ping, le périphérique part du principe que la liaison est inactive et retente l'interface Ethernet WAN.

ÉTAPE 5 Dans le champ **Intervalle de vérification de la récupération**, entrez la fréquence (en secondes) à laquelle le périphérique doit tenter de détecter la connexion physique ou la présence de trafic sur la liaison WAN Ethernet. Si la liaison est inactive, le périphérique tente d'envoyer une commande ping vers une destination selon cet intervalle. En cas de réponse au paquet ping, le périphérique part du principe que

la liaison est active et tente de désactiver la liaison du réseau mobile et d'activer la liaison Ethernet WAN.

ÉTAPE 6 Cliquez sur **Revenir à Ethernet immédiatement lorsque ce mode est disponible** ou cliquez sur **Revenir à Ethernet dans une plage horaire spécifique** et entrez l'heure de début et de fin de la plage.

ÉTAPE 7 Dans le champ **Site de validation de la connexion**, choisissez le site à partir duquel la validation du basculement doit avoir lieu. Utilisez la passerelle de saut suivant (par défaut, le périphérique envoie une commande ping à la passerelle par défaut) ou choisissez un site personnalisé et entrez l'adresse IPv4 ou IPv6 de ce site.

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

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.

Configuration des paramètres de réseau local (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 envoyée aux clients DHCP.

Si votre périphérique est connecté à un modem ou à un autre appareil ayant un réseau configuré sur le même sous-réseau (192.168.1.x), il remplace automatiquement le sous-réseau du LAN par un sous-réseau aléatoire basé sur 10.x.x.x, afin d'éviter tout conflit avec le sous-réseau sur la partie WAN du routeur.

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 du périphérique. Vérifiez que l'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**.

Une fois que vous avez modifié l'adresse IP de votre périphérique, votre ordinateur n'est plus en mesure d'afficher le Gestionnaire de périphérique.

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

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

Ouvrez une nouvelle fenêtre de navigateur et saisissez 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 autres 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 dans le groupe d'adresses IP, afin d'empêcher tout conflit 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 aux périphériques réseau.

Si vous avez activé le serveur DHCP du périphérique, entrez 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 VLAN**.

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

ÉTAPE 3 Saisissez les informations suivantes :

ID de réseau 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.
Port 1 **Port 2** **Port 3** **Port 4**	Vous pouvez associer les VLAN du périphérique aux ports LAN du périphérique. 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 votre routeur afin qu'il affecte une adresse IP spécifique à un périphérique client doté d'une adresse MAC spécifique.

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 que vous souhaitez affecter au périphérique client. 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 le périphérique client est connecté au réseau. Le serveur DHCP attribue l'adresse IP réservée lorsque le périphérique client doté de l'adresse MAC correspondante demande une adresse IP.
Adresse MAC	Adresse MAC du périphérique client. 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

Votre 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 Saisissez les informations suivantes :

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 4 096. Les valeurs autorisées sont 0, 4 096, 8 192, 12 288, 16 384, 20 480, 24 576, 28 672, 32 768, 40 960, 45 056, 49 152, 53 248, 57 344 et 61 440. Plus la priorité du système est basse, plus le périphérique est susceptible de devenir la racine dans l'arborescence STP. La valeur par défaut est **32 768**.
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 maximum	Le délai maximum correspond à la durée pendant laquelle le routeur doit attendre avant de recevoir un message de prise de contact. À l'expiration du délai maximum, 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 **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.
Trame Jumbo	Cochez cette case pour activer les trames Jumbo sur le périphérique et envoyer des trames sur le LAN contenant chacune jusqu'à 9 000 octets de données. Une trame Ethernet standard contient 1 500 octets de données.
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**.

Configuration de l'agrégation de liaisons

Utilisez la page Agrégation de liaisons pour regrouper plusieurs liaisons Ethernet en un seul canal logique. Les groupes d'agrégation de liaisons améliorent la rentabilité de votre périphérique en augmentant la bande passante cumulative sans nécessiter de mises à niveau matérielles, et permettent un reroutage facile lors de la défaillance d'un port ou d'un câble.

Pour attribuer des ports à un groupe d'agrégation de liaisons :

ÉTAPE 1 Sélectionnez **Mise en réseau > LAN > Agrégation de liaisons**. La section **État du port** affiche le mode associé à chaque port du périphérique, ainsi que son état.

ÉTAPE 2 Dans la section **Table des paramètres d'agrégation de liaison**, cochez la case de chaque port que vous souhaitez inclure dans le groupe.

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 ordinateur ou une autre adresse MAC. On appelle cela cloner l'adresse MAC.

Par exemple, certains FAI enregistrent l'adresse MAC de la carte 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.

Pour configurer votre périphérique afin qu'il soit reconnu par le FAI, vous devez alors cloner l'adresse MAC du port WAN pour qu'elle soit identique 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 l'adresse MAC du PC**.
- Pour spécifier une autre adresse MAC, entrez-la dans le champ **Adresse MAC**.

ÉTAPE 4 Cliquez sur **Enregistrer**.

Configuration du routage

Utilisez la page Routage pour configurer le mode de fonctionnement et d'autres options de routage pour votre périphérique.

Configuration du mode de fonctionnement

Pour configurer le mode de fonctionnement :

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

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

Passerelle	Pour configurer le périphérique afin qu'il fonctionne comme une passerelle (recommandé). Conservez ce paramètre par défaut si le périphérique héberge votre connexion réseau à Internet et s'il exécute les fonctions de routage.

Routeur	(Pour les utilisateurs expérimentés uniquement) Pour définir le périphérique afin qu'il fonctionne comme routeur. Sélectionnez cette option si le périphérique est sur un réseau avec d'autres routeurs. L'activation du mode Routeur désactive la traduction d'adresses réseau (Network Address Translation, 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.

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 inter VLAN

Pour permettre à une station finale dans un VLAN de communiquer avec une station finale dans un autre VLAN, cochez la case **Routage inter VLAN**.

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.

Une route statique est un chemin prédéfini devant être emprunté par un paquet afin d'atteindre un hôte ou un réseau particulier. 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.
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 la page **Mise en réseau** > **IPv6**.

Configuration du DNS dynamique

Le DDNS (Dynamic DNS) 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 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 Sélectionnez un **Intervalle de mise à jour** dans la liste déroulante.

ÉTAPE 3 La section **Table de service DDNS** répertorie les services DDNS que vous pouvez activer sur le périphérique.

ÉTAPE 4 Cochez la case en regard du service que vous souhaitez activer, puis cliquez sur **Modifier**.

ÉTAPE 5 Cochez la case **Activer** pour le service.

ÉTAPE 6 Précisez les informations suivantes :

Nom d'utilisateur/ adresse e-mail	Nom d'utilisateur du compte DDNS ou adresse e-mail que vous avez utilisé pour créer le compte DDNS.
Mot de passe	Mot de passe du compte DDNS.
Nom d'hôte/de domaine	Nom d'hôte du serveur DDNS ou nom du domaine qui est utilisé pour accéder au réseau.
Adresse IP Internet	(Lecture seule) Adresse IP Internet de votre 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 7 Cliquez sur **Tester la configuration** pour tester la configuration DDNS.

ÉTAPE 8 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	Pour utiliser IPv4 sur les ports LAN et WAN.
LAN : IPv6, WAN : IPv4	Pour utiliser IPv6 sur les ports LAN et IPv4 sur les ports WAN.
LAN : IPv6, WAN : IPv6	Pour utiliser IPv6 sur les ports LAN et WAN.
LAN : IPv4+IPv6, WAN : IPv4	Pour utiliser IPv4 et IPv6 sur les ports LAN et IPv4 sur les ports WAN.
LAN : IPv4+IPv6, WAN : IPv4+IPv6	Pour utiliser IPv4 et IPv6 sur les ports LAN et WAN.
LAN : IPv4, WAN : IPv6	Pour utiliser IPv4 sur le LAN et IPv6 sur les ports WAN.

ÉTAPE 3 (Facultatif) Si vous utilisez la tunnellisation 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 tunnellisation 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 votre 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 SLAAC

Pour attribuer automatiquement une adresse basée sur le préfixe IPv6, configurez le périphérique afin qu'il utilise SLAAC (Stateless Address Auto-Configuration) pour l'attribution d'adresse client IPv6.

Pour utiliser SLAAC :

ÉTAPE 1 Sélectionnez **Réseau** > **IPv6** > **Configuration WAN IPv6**.

ÉTAPE 2 Dans le champ **Type de connexion WAN**, sélectionnez SLAAC. En cas de DHCP sans état, il n'est pas nécessaire de disposer d'un serveur DHCPv6 du FAI. Un

message de détection ICMPv6 provenant de votre périphérique est utilisé pour la configuration automatique.

ÉTAPE 3 Cliquez sur **Enregistrer**.

Configuration de DHCPv6

Si votre FAI vous fournit une adresse affectée dynamiquement, configurez le périphérique pour qu'il fonctionne en tant que client DHCPv6.

Pour configurer le périphérique pour qu'il fonctionne en tant que client DHCPv6 :

ÉTAPE 1 Sélectionnez **Réseau** > **IPv6** > **Configuration WAN IPv6**.

ÉTAPE 2 Dans le champ **Type de connexion WAN**, sélectionnez **Configuration automatique - DHCPv6**. La passerelle se connecte au serveur DHCPv6 du FAI pour obtenir un bail d'adresse.

ÉTAPE 3 Pour automatiser l'attribution de préfixes à votre périphérique (le client DHCP), sélectionnez la case d'option **Longueur du préfixe**.

ÉTAPE 4 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 **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 IPv6 PPPoE

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

Pour configurer les paramètres IPv6 PPPoE :

ÉTAPE 1 Sélectionnez **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.
Maintenir actif	Garde la liaison WAN active en envoyant un message correspondant sur le port. Dans le champ de période de renumérotation, entrez le délai en secondes à l'issue duquel le périphérique, s'il est déconnecté, tente de se reconnecter.
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 incluant le type de sécurité envoyé 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 MS-CHAP (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	L'unité maximale de transmission (Maximum Transmission Unit, MTU) correspond à la taille du plus gros 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 définir 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 de 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 incluse dans la plage spécifiée et fournit des informations supplémentaires à tout point d'extrémité du LAN qui demande des adresses 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**.
Métrique	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 métrique la plus faible est utilisée.
Actif	Cochez cette option pour activer la route. Lorsque vous ajoutez une route dans un état inactif, elle apparaît dans la table de routage, mais 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, métrique 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 l'hôte de destination est inaccessible.

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 votre 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 de la tunnellisation

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

Tunnellisation 6 vers 4

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

Pour configurer la tunnellisation 6-to-4 :

ÉTAPE 1 Sélectionnez **Mise en réseau** > **IPv6** > **Tunnellisation**.

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

ÉTAPE 3 Sélectionnez le type de tunnellisation :

- **6to4**
- **6RD** (Rapid Deployment)
- **ISATAP** (Intra-Site Automatic Tunnel Addressing Protocol) : sélectionnez **Auto** ou **Manuel**.

ÉTAPE 4 Pour la tunnellisation 6RD, choisissez **Auto** ou **Manuelle**. Si vous sélectionnez **Manuel**, entrez les informations suivantes :

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

ÉTAPE 5 Pour la tunnellisation ISATAP, choisissez **Auto** ou **Manuel**. Si vous sélectionnez **Manuel**, entrez les informations suivantes :

- **Préfixe IPv6**
- **Longueur du préfixe IPv6**

ÉTAPE 6 Cliquez sur **Enregistrer**.

Tunnellisation 4 vers 6

Pour configurer la tunnellisation 4to6 :

ÉTAPE 1 Sélectionnez **Mise en réseau** > **IPv6** > **Tunnellisation**.

ÉTAPE 2 Dans le champ **Tunneling 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. 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. **Destination unique seulement** : 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 Transmission 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. Il 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 des réseaux sans fil

Sécurité sans fil

Les réseaux sans fil sont pratiques et simples à installer. 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 SSID par défaut du réseau sans fil.

  Les appareils sans fil sont dotés d'un nom ou 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, car elles seront accessibles à toute personne 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 périphérique 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 chiffrement.

  Le chiffrement 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 chiffrement par clé dynamique.

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

  WEP est une norme de chiffrement 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 complexes contenant au moins huit caractères. Combinez chiffres et lettres pour éviter l'utilisation de mots existants dans le dictionnaire.

Directives générales sur la sécurité réseau

Inutile de sécuriser le réseau sans fil si le réseau sous-jacent n'est pas sécurisé. Nous vous recommandons 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.

Réseaux sans fil sur votre périphérique

Votre 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 SSID	ciscosb1	ciscosb2	ciscosb3	ciscosb4
Activé	Oui	Non	Non	Non
Diffusion SSID	Activé	Désactivé	Désactivé	Désactivé
Mode de sécurité	Désactivé[1]	Désactivé	Désactivé	Désactivé
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 configuration, sélectionnez Sécurité optimale ou Meilleure sécurité pour protéger le périphérique de tout accès non autorisé.

Configuration des paramètres sans fil de base

Sélectionnez **Sans fil** > **Paramètres de base** pour configurer les paramètres sans fil de base.

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 :

Mixte B/G/N	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 **Mixte B/G/N**, **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 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** 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 la case des réseaux que vous souhaitez configurer.

ÉTAPE 2 Cliquez sur **Modifier**.

ÉTAPE 3 Configurez les paramètres suivants :

Activer SSID	Cliquez sur **Activé** pour activer le réseau.
Nom SSID	Nommez le 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.
Mode de sécurité	Reportez-vous à la section **Configuration du mode de sécurité**.
Filtre MAC	Reportez-vous à la section **Configuration du filtrage MAC**.
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.
Nombre max. de clients associés	Nombre maximal de clients pouvant se connecter au réseau sans fil sélectionné. Saisissez un nombre compris entre 1 et 64.
WPS	Cochez cette case pour associer le bouton WPS situé sur la façade du périphérique à ce réseau.
Profil du portail	Reportez-vous à la section **Configuration du portail captif**.

ÉTAPE 4 Cliquez sur **Enregistrer**.

Configuration du mode de sécurité

Vous pouvez configurer l'un des modes de sécurité suivants pour les réseaux sans fil :

-

Configuration de WEP

Le mode de sécurité WEP offre une sécurité faible en utilisant une méthode de chiffrement 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 Sélectionnez **Sans fil** > **Paramètres de base**. Dans la **Table sans fil**, 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 chiffrement :

- **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 chiffrement est plus difficile à décrypter. Nous recommandons le chiffrement 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 de WPA-Personal, WPA2-Personal et de WPA2-Personal mixte

Les modes de sécurité WPA Personnel, WPA2 Personnel et WPA2 Personnel mixte fournissent une sécurité forte pour remplacer 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 chiffrement 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 chiffrement 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 offre une meilleure sécurité.

ÉTAPE 6 Dans le champ **Clé de sécurité**, entrez une expression alphanumérique (8 à 63 caractères ASCII ou 64 chiffres hexadécimaux). L'échelle d'évaluation de la sécurité du mot de passe indique la robustesse de la clé : Inférieur au seuil

minimum, Faible, Fort, Très fort ou Sécurisé. Nous vous recommandons d'utiliser une clé de sécurité considérée comme sécurisée sur l'échelle d'évaluation.

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

Configuration des modes WPA-Enterprise, WPA2-Enterprise et WPA2-Enterprise 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 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 l'appareil 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 **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 d'arrêt**, spécifiez la plage horaire durant laquelle l'accès au réseau sera autorisé.

ÉTAPE 5 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	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. Par défaut, ce paramètre est désactivé.

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 sa vitesse de base aux autres périphériques sans fil de votre réseau, afin qu'ils connaissent les débits qui seront utilisés. La plateforme 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 Toutes lorsque le périphérique peut transmettre à toutes les vitesses sans fil. La vitesse de base ne correspond pas à la vitesse réelle de transmission des données. Si vous souhaitez spécifier la vitesse 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 votre sélection parmi une plage de vitesses de transmission ou vous pouvez sélectionner **Auto** pour que le périphérique utilise automatiquement le débit de données le plus rapide et activer la fonction 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 votre sélection parmi une plage de vitesses de transmission ou vous pouvez sélectionner **Auto** pour que le périphérique utilise automatiquement le débit de données le plus rapide et activer la fonction 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 importante des performances. La valeur par défaut est Automatique.
Intervalle de balise	La valeur d'intervalle de balise 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**.

Détection des points d'accès non autorisés

Un point d'accès non autorisé est un point d'accès qui a été installé sur un réseau sécurisé sans l'autorisation d'un administrateur système. Les points d'accès non autorisés constituent une menace en matière de sécurité car toute personne ayant accès aux locaux peut installer un point d'accès sans fil pouvant permettre à des personnes non autorisées d'accéder au réseau.

Utilisez la page Détection de point d'accès non autorisé pour permettre à votre périphérique d'afficher des informations sur tous les points d'accès détectés par le périphérique à proximité du réseau. Si le point d'accès identifié comme non autorisé est en réalité légitime, vous pouvez l'ajouter à la **Table des points d'accès autorisés**. Sélectionnez une fréquence d'actualisation pour vous assurer que la page Détection de point d'accès non autorisé affiche toujours les informations les plus à jour.

Pour activer la détection des points d'accès non autorisés :

ÉTAPE 1 Sélectionnez **Sans fil > Point d'accès non autorisé**.

ÉTAPE 2 Sélectionnez la case d'option **Détection de point d'accès non autorisé**.

ÉTAPE 3 Cliquez sur **Enregistrer**.

Pour autoriser les points d'accès détectés :

ÉTAPE 1 Dans la **Table des points d'accès non autorisés détectés**, cochez la case correspondant au point d'accès que vous souhaitez autoriser.

ÉTAPE 2 Cliquez sur **Autoriser**.

Pour ajouter un point d'accès à la Table des points d'accès autorisés :

ÉTAPE 1 Cliquez sur **Ajouter une ligne**.

ÉTAPE 2 Entrez l'adresse MAC du point d'accès que vous souhaitez autoriser.

ÉTAPE 3 Entrez le SSID ou le nom qui identifie le réseau sans fil.

ÉTAPE 4 Choisissez le mode de sécurité associé au point d'accès.

ÉTAPE 5 Choisissez le protocole TKIP (Temporal Key Integrity Protocol) ou CCMP (Counter Cipher Mode Protocol) comme algorithme de chiffrement associé au point d'accès.

ÉTAPE 6 Choisissez Serveur RADIUS ou PSK (Pre-Shared Key) pour authentifier le point d'accès.

ÉTAPE 7 Sélectionnez le mode de réseau sans fil utilisé par le point d'accès.

ÉTAPE 8 Choisissez la fréquence radio utilisée par le point d'accès.

ÉTAPE 9 Cliquez sur **Enregistrer**.

Importation des listes de points d'accès autorisés

Vous pouvez importer une liste de points d'accès autorisés à l'aide d'un fichier CSV. Utilisez les valeurs de référence suivantes pour créer le fichier CSV.

Champ	Valeurs
Sécurité	• 0 — Ouvert • 1 — WEP • 2 — WPA-Personal • 3 — WPA-Enterprise • 4 — WPA2-Personal • 5 — WPA2-Enterprise
Mode réseau	• 0 — B seulement • 1 — G seulement • 2 — N seulement • 3 — Mixte B/G • 4 — Mixte G/N • 5 — Mixte B/G/N

Champ	Valeurs
Canal	• 0 — Auto • 1 — 2,412 • 2 — 2,417 • 3 — 2,422 • 4 — 2,427 • 5 — 2,432 • 6 — 2,437 • 7 — 2,442 • 8 — 2,447 • 9 — 2,452 • 10 — 2,457 • 11 — 2,462
Cryptage	• 2 — TKIP • 4 — CCMP
Authentification	• 2 — PSK • 1 — RADIUS

Vérifiez que le contenu du fichier CSV correspond à l'exemple suivant :

BSSID	Sécurité	Cryptage	Authentification	Réseau sans fil	Canal	SSID
00:1C:10:CE:44:48	4	2	2	3	1	Auth_Guest

Pour importer une liste de points d'accès autorisés :

ÉTAPE 1 Cliquez sur **Fusionner** pour ajouter la liste de points d'accès à importer aux points d'accès affichés dans la **Table des points d'accès autorisés**. Cliquez sur **Remplacer** pour remplacer les points d'accès de la table par les points d'accès de la liste que vous souhaitez importer.

ÉTAPE 2 Cliquez sur **Parcourir** pour rechercher le fichier que vous souhaitez importer.

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 chiffrement (aucun ou WEP).

Vous pouvez configurer WDS en mode Pont dans lequel un point d'accès fonctionne en tant que liaison commune entre plusieurs points d'accès, ou en mode Répéteur dans lequel un point d'accès se connecte à deux points d'accès sans connexion filaire au réseau local, en répétant les signaux par l'intermédiaire de la connexion sans fil.

WDS est pris en charge sur un seul SSID.

Pour configurer WDS en mode Pont :

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

ÉTAPE 2 Pour activer WDS, cochez la case **Activer.**

ÉTAPE 3 Sélectionnez la case d'option **WDS Bridge**.

ÉTAPE 4 Dans la section **Adresse MAC du pont sans fil distant**, dans les champs **MAC 1**, **MAC 2**, **MAC 3** et **MAC 4**, entrez les adresses MAC de quatre points d'accès maximum à utiliser comme ponts.

ÉTAPE 5 Cliquez sur **Enregistrer**.

Pour configurer WDS en mode Répéteur :

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

ÉTAPE 2 Cochez la case **WDS**.

ÉTAPE 3 Sélectionnez le mode Répéteur. Si vous sélectionnez **Autoriser la répétition du signal sans fil à l'aide d'un répéteur**, dans les champs **MAC 1**, **MAC 2** et **MAC 3**, entrez les adresses MAC de trois points d'accès maximum que vous souhaitez utiliser comme répéteurs.

ÉTAPE 4 Si vous sélectionnez **Répéter le signal sans fil d'un point d'accès distant** :

- Entrez l'adresse MAC d'un point d'accès sans fil dans le champ **MAC**.
- Cliquez sur **Afficher les réseaux disponibles** pour afficher la **Table des réseaux disponibles.** Cliquez sur **Connexion** pour ajouter l'adresse MAC du point d'accès sélectionné au champ **MAC**.

ÉTAPE 5 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 apparaît.

ÉTAPE 2 Sélectionnez l'option SSID dans le menu déroulant.

ÉTAPE 3 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. Un appareil client nécessite un numéro PIN de ce routeur ; utilisez le numéro 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 du Wi-Fi Protected Setup, Nom du réseau (SSID) et Sécurité.

Configuration du portail captif

Utilisez la fonction Portail captif pour garantir un accès contrôlé et authentifié à Internet et à vos ressources réseau, sans compromettre la sécurité. Un portail captif affiche une page Web spéciale permettant d'authentifier les clients avant qu'ils ne puissent utiliser Internet. Vous pouvez configurer la vérification de portail captif de manière à autoriser l'accès à la fois pour les utilisateurs invités et les utilisateurs réseau authentifiés.

Configurez des instances de portail captif pour chaque réseau sans fil virtuel sur votre périphérique, en l'associant à un profil de portail.

Création de profils de portail captif

Pour créer un profil de portail captif :

ÉTAPE 1 Sélectionnez **Sans fil > Portail captif > Profil du portail.** Dans la section **Table de profil de portail**, cliquez sur **Ajouter une ligne**. Pour modifier le profil de portail fourni sur le périphérique, cochez la case **Profil_portail_par défaut** et cliquez sur **Modifier**.

ÉTAPE 2 Entrez un nom pour votre profil Portail captif.

ÉTAPE 3 Choisissez si vous souhaitez utiliser le profil pour authentifier les utilisateurs invités ou les utilisateurs de votre réseau.

ÉTAPE 4 Pour rediriger les utilisateurs vers une URL après l'authentification, activez **URL de redirection automatique**, puis entrez un nom de domaine complet ou une adresse IP dans le champ **URL de redirection**. Par exemple, incluez http:// dans l'URL.

ÉTAPE 5 Dans le champ **Délai d'expiration de session**, spécifiez le nombre de minutes pendant lequel le périphérique maintiendra une session d'authentification ouverte avec le client sans fil associé. Le délai d'expiration par défaut est de 60 minutes.

ÉTAPE 6 Sélectionnez une couleur de police pour le texte que vous souhaitez afficher sur la page.

ÉTAPE 7 Spécifiez le texte à afficher, comme le nom de votre organisation, le texte de l'étiquette des champs de nom d'utilisateur et de mot de passe, ainsi que l'étiquette du bouton Connexion.

ÉTAPE 8 Entrez un texte de copyright standard associé à votre entreprise.

ÉTAPE 9 Dans les champs **Erreur 1** et **Erreur 2**, entrez les messages d'erreur que les clients verront lorsque leur connexion échouera et qu'ils auront dépassé le nombre maximal de connexions.

ÉTAPE 10 Pour utiliser une case à cocher permettant aux utilisateurs d'accepter les conditions d'utilisation avant de continuer, activez **Accord**. Le texte contenu dans le champ **Texte d'accord** s'affichera comme étiquette de la case à cocher.

ÉTAPE 11 Entrez les conditions d'acceptation que les utilisateurs verront dans le champ **Politique d'utilisation acceptable**.

ÉTAPE 12 Dans la section **Transférer les fichiers**, sélectionnez les fichiers permettant de transférer le logo de votre entreprise et les fichiers d'arrière-plan, conformément aux directives de votre entreprise en termes de marque. Enregistrez votre profil.

Pour prévisualiser ce profil, sélectionnez **Portail captif > Aperçu de la page du portail**, puis sélectionnez le profil dans la liste déroulante **Profil du portail**.

Configuration des instances du portail captif

Pour configurer une instance du portail captif pour votre périphérique :

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

ÉTAPE 2 Dans la section **Table sans fil**, cochez la case **Activer** du SSID pour lequel vous souhaitez configurer un portail captif. Cliquez sur **Modifier**.

ÉTAPE 3 Sélectionnez un profil de portail pour le SSID.

Vous pouvez créer un maximum de quatre portails captifs à l'aide de SSID pour votre périphérique. Pour créer un nouveau profil de portail, sélectionnez **Créer un nouveau profil de portail** dans la liste déroulante. Choisissez Profil_portail_par défaut afin d'utiliser le profil de portail fourni sur votre périphérique.

ÉTAPE 4 Cochez la case **Activer** afin d'activer le portail captif pour le SSID.

ÉTAPE 5 Enregistrez vos instances de portail captif.

Création de comptes d'utilisateurs de portail captif

Pour créer un compte d'utilisateur de portail captif :

ÉTAPE 1 Sélectionnez **Sans fil > Portail captif > Comptes d'utilisateurs**.

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

ÉTAPE 3 Saisissez un nom d'utilisateur et un mot de passe. Saisissez à nouveau le mot de passe pour le confirmer.

Nous vous recommandons d'utiliser un mot de passe qui ne contienne aucun mot figurant dans un dictionnaire, quelle que soit la langue, et qui soit composé de lettres (majuscules et minuscules), de chiffres et de symboles. Le mot de passe peut comporter au maximum 64 caractères.

ÉTAPE 4 Dans le champ **Temps d'accès (minutes)**, spécifiez la durée à l'issue de laquelle la session d'authentification expirera.

ÉTAPE 5 Pour importer des noms d'utilisateur et des mots de passe à partir d'un fichier CSV, cliquez sur **Importer**. La page **Administration > Utilisateurs** s'affiche. Dans la section **Importer le nom de l'utilisateur et le mot de passe**, cliquez sur **Parcourir** pour rechercher le fichier, puis cliquez sur **Importer**. Pour plus d'informations, reportez-vous à la section **Importation de comptes d'utilisateurs**.

ÉTAPE 6 Enregistrez vos comptes d'utilisateurs.

Configuration du mode du périphérique

Vous pouvez configurer votre périphérique pour qu'il fonctionne dans les modes suivants :

- **Routeur :** pour fonctionner comme un routeur sans fil.
- **Point d'accès :** pour fournir des connexions sans fil aux clients et étendre la fonctionnalité Wi-Fi à un réseau filaire existant. Tous les ports LAN sont désactivés lorsque le périphérique fonctionne en tant que point d'accès.

  Veillez à configurer les informations VLAN de gestion PA sur la page **Mise en réseau > WAN > Configuration WAN**. Pour plus d'informations, reportez-vous à la section **Configuration des paramètres facultatifs**.

Pour configurer le mode du périphérique :

ÉTAPE 1 Sélectionnez **Sans fil > Mode de l'appareil**, puis sélectionnez le mode dans lequel vous souhaitez faire fonctionner votre périphérique.

ÉTAPE 2 Cliquez sur **Enregistrer**.

5

Configuration du pare-feu

Caractéristiques du pare-feu

Vous pouvez sécuriser votre réseau en créant et en appliquant des règles utilisées par le périphérique pour bloquer et autoriser sélectivement le trafic Internet entrant et sortant. Vous devez ensuite spécifier les périphériques concernés par ces règles et la façon dont elles s'appliquent. Pour ce faire, vous devez définir les éléments suivants :

- Types de services ou de trafic que le routeur doit autoriser ou bloquer. Par exemple, la navigation Web, la VoIP, d'autres services standard et des services personnalisés que vous définissez.
- 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).
- Horaires 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 horaire, 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 des groupes d'ordinateurs spécifiques sur 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 « exposer votre hôte ». La manière de rendre votre adresse publique dépend de la façon dont les ports WAN sont configurés. Sur le périphérique, vous pouvez utiliser l'adresse IP si une adresse statique est affectée au port WAN, ou un nom DDNS (Dynamic DNS) 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 :

Protection contre la mystification d'adresse IP	Pour protéger votre réseau contre la mystification d'adresse IP, cochez la case **Activer**.
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 LAN/VPN	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.
ALG SIP	Pour autoriser le trafic de protocole d'initiation de session (SIP) à traverser le pare-feu, cochez la case **ALG SIP**. Le périphérique prend en charge un maximum de 256 sessions.
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.

ÉTAPE 3 Cliquez sur **Enregistrer**.

Configuration de la gestion à distance

Vous pouvez activer la gestion à distance pour pouvoir accéder au périphérique 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 spécifiez une adresse IP spécifique dans le champ d'adresse.
Port de gestion à distance	Entrez le port sur lequel l'accès à distance 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. Par exemple : **https://<adresse_IP_distante>:<port_à_distance>** ou **https://168.10.1.11:443**

AVERTISSEMENT Lorsque la gestion à distance est activée, le routeur est accessible par tout utilisateur qui connaît l'adresse IP correspondante. Un utilisateur extérieur malveillant pouvant reconfigurer le périphérique, il est vivement conseillé 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 périphérique n'autorise pas l'application à ajouter la règle de redirection.
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 horaires afin d'appliquer les règles de pare-feu certains jours ou à certaines heures de la journée.

Ajout ou modification d'un horaire de pare-feu

Pour créer ou modifier un horaire :

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 l'horaire. Le nom est disponible dans la liste **Sélectionner un horaire** sur la page de configuration des règles de pare-feu. (Reportez-vous à la section **Configuration des règles d'accès**.)

ÉTAPE 4 Dans la section **Jours planifiés**, indiquez si vous souhaitez appliquer l'horaire à Tous les jours ou à Certains jours. Si vous sélectionnez **Certains jours**, cochez les cases en regard des jours que vous souhaitez inclure dans l'horaire.

ÉTAPE 5 Dans la section **Heures planifiées**, sélectionnez le moment où vous souhaitez appliquer l'horaire. 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 table 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.

REMARQUE Les stratégies d'accès à Internet remplacent les règles d'accès lorsqu'elles sont configurées ensemble sur le périphérique.

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 un récapitulatif de la zone source/cible, ainsi que les services et les 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** : bloque le type de trafic sélectionné en fonction d'un horaire.
- **Autoriser selon un horaire** : autorise le type de trafic sélectionné en fonction d'un horaire.

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 Dans le champ **IP source**, sélectionnez les utilisateurs auxquels appliquer la règle :

- **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 7 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 horaire 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 8 Cochez la case d'activation de l'**État de la règle** pour activer la nouvelle règle d'accès.

ÉTAPE 9 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 politique d'accès à Internet :

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

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

ÉTAPE 3 Cochez la case **État 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 l'horaire** : bloque le trafic Internet selon un horaire 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 l'horaire** : autorise le trafic Internet en fonction d'un horaire.

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

ÉTAPE 6 Sélectionnez un horaire 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 politique ;
- l'adresse IP de l'ordinateur ciblé 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 de **Nom de domaine du site Web et mot clé**, cliquez sur **Ajouter une ligne**.

b. Dans le menu déroulant **Type**, sélectionnez la manière de bloquer un site Web (en spécifiant le nom de domaine 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 du NAT (traduction d'adresses réseau) un-à-un

Utilisez la page NAT un-à-un pour mapper des adresses IP locales derrière votre pare-feu à des adresses IP globales. Le NAT un-à-un est un mécanisme permettant à des systèmes configurés avec des adresses IP privées et situés derrière un pare-feu d'apparaître comme disposant d'adresses IP publiques.

Pour ajouter une règle de NAT un-à-un :

ÉTAPE 1 Sélectionnez **Pare-feu > NAT un-à-un**.

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

ÉTAPE 3 Dans le champ **Début de la plage privée**, entrez la première adresse IP de la plage d'adresses IP (LAN) privées.

ÉTAPE 4 Dans le champ **Début de la plage publique**, entrez la première adresse IP de la plage d'adresses IP (WAN) publiques.

ÉTAPE 5 Dans **Longueur de la plage**, entrez le nombre d'adresses IP publiques devant être mappées aux adresses privées.

ÉTAPE 6 Dans le champ **Service**, sélectionnez le service auquel la règle s'applique. Les services de NAT un à un vous permettent de configurer le service que l'adresse IP privée (LAN) doit accepter lorsque du trafic est envoyé à l'adresse IP publique correspondante. Les services configurés sur les adresses IP de la plage sont acceptés lorsque du trafic est disponible sur l'adresse IP publique correspondante.

ÉTAPE 7 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 ports ne s'applique pas aux serveurs du LAN, en raison de la dépendance sur le périphérique 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 et 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 et 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 et 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

Types de tunnels VPN

Vous pouvez configurer un réseau privé virtuel (Virtual Private Network, VPN) sur votre périphérique pour disposer d'un tunnel ou d'un canal de communication sécurisé entre :

- deux routeurs-passerelles ;
- un périphérique client distant et un routeur-passerelle.

Configuration du VPN IPsec site-à-site de base

Votre périphérique prend en charge le VPN IPsec site-à-site pour un tunnel VPN passerelle-à-passerelle unique. Une fois que ces paramètres VPN de base ont été configurés, vous pouvez vous connecter en toute sécurité à un autre routeur VPN. Par exemple, vous pouvez configurer votre périphérique sur le site d'une filiale pour qu'il se connecte à un routeur, qui lui-même se connecte aux tunnels VPN site-à-site présents sur le site de l'entreprise, ceci afin que le site de la filiale puisse accéder en toute sécurité au réseau de l'entreprise.

Pour configurer les paramètres VPN de base d'une connexion IPsec site-à-site :

ÉTAPE 1 Sélectionnez **VPN > VPN IPSec site-à-site > Configuration VPN de base**.

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

ÉTAPE 3 Dans le champ **Clé prépartagée**, entrez la clé prépartagée, ou le mot de passe, qui sera échangée 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** : indiquez si le routeur auquel votre périphérique se connecte est identifié par son adresse IP ou par un nom de domaine complet. Par exemple, une adresse IP telle que 192.168.1.1 ou un nom de domaine complet tel que cisco.com.
- **Adresse IP de WAN (Internet) distant** : entrez l'adresse IP publique ou le nom de domaine du point d'extrémité distant.
- **Adresse IP de WAN (Internet) local** : entrez l'adresse IP publique ou le nom de domaine de votre périphérique.

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

- **Adresse IP du réseau local (LAN) distant** : 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** : masque de sous-réseau du réseau privé (LAN) du point d'extrémité distant.
- **Adresse IP du réseau local (LAN)** : 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)** : masque de sous-réseau du réseau privé (LAN) du réseau local.

Remarque : les adresses IP de WAN distant et de 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 créent 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

Cliquez sur **Afficher les paramètres par défaut** pour afficher les valeurs par défaut utilisées dans les paramètres VPN de base. Ces valeurs sont proposées par le VPN Consortium (VPNC) et supposent que vous utilisez une clé prépartagée ou un mot de passe connu de votre périphérique et du point d'extrémité distant.

Configuration des paramètres avancés VPN IPsec site-à-site

Les paramètres VPN avancés tels que les stratégies IKE et d'autres stratégies VPN contrôlent la façon dont le périphérique initie et reçoit des connexions VPN.

Pour configurer les paramètres VPN avancés, sélectionnez **VPN > VPN IPSec site-à-site > Configuration VPN avancée**.

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 afin de définir les paramètres de sécurité à utiliser pour l'échange de données avec le routeur distant via la connexion VPN IPsec. Par exemple, vous pouvez créer des stratégies IKE afin de définir des paramètres pour l'authentification d'homologue et les algorithmes de chiffrement. Assurez-vous que les paramètres de chiffrement, d'authentification et de clé-groupe de votre stratégie VPN sont compatibles avec les paramètres définis sur le routeur distant.

Pour ajouter une stratégie IKE **:**

ÉTAPE 1 Sur la page **Configuration VPN avancée**, cliquez sur **Ajouter une ligne**.

ÉTAPE 2 Saisissez un nom unique pour la stratégie IKE afin que vous puissiez l'identifier et la gérer facilement.

ÉTAPE 3 Dans le champ **Mode Exchange**, choisissez un des modes suivants pour la stratégie :

- **Principal** : négocie le tunnel avec une sécurité supérieure, mais est plus lent.
- **Agressif** : établit plus rapidement la connexion, mais la sécurité est moindre.

ÉTAPE 4 Dans les champs **Identifiant local** et **Identifiant distant**, indiquez si vous souhaitez identifier votre périphérique et le routeur distant par leur vraie adresse IP ou leur adresse IP publique. Si vous sélectionnez l'adresse IP, entrez la vraie adresse IP de votre périphérique et du routeur distant.

ÉTAPE 5 Dans la section **Paramètres de SA IKE**, configurez les paramètres afin de définir la robustesse et le mode de négociation de l'association de sécurité (Security Association, SA) entre votre périphérique et le routeur distant :

a. Dans le champ **Algorithme de chiffrement**, sélectionnez l'algorithme utilisé pour chiffrer les données.

b. Dans le champ **Algorithme d'authentification**, spécifiez l'algorithme d'authentification de l'en-tête VPN : Vérifiez que l'algorithme d'authentification est configuré de manière identique des deux côtés du tunnel VPN.

c. Dans le champ **Clé prépartagée**, entrez la clé ou le mot de passe. Vérifiez que le mot de passe ne contient pas de guillemets (“).

d. Dans le champ **Groupe Diffie-Hellman (DH)**, spécifiez l'algorithme de groupe DH qui est utilisé lors de l'échange d'une clé prépartagée. 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.

e. Dans le champ **Durée de vie SA**, saisissez l'intervalle en secondes au bout duquel l'association de sécurité devient non valide.

f. Pour activer la fonction **Détection d'homologue indisponible**, cochez la case **Activer**. La détection d'homologue indisponible (Dead Peer Detection, DPD) sert à détecter si l'homologue est actif. Si l'homologue est détecté comme étant indisponible, le périphérique supprime l'association de sécurité IPsec et IKE. Si vous activez cette fonction, entrez également les paramètres suivants :

- **Action DPD** : 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** : durée d'attente maximale du routeur pour recevoir une réponse au message DPD avant de considérer l'homologue comme inactif.

ÉTAPE 6 Cliquez sur **Enregistrer**.

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

Gestion des stratégies VPN

REMARQUE Avant de créer une stratégie VPN automatique, veillez à créer la stratégie IKE à partir de laquelle vous souhaitez créer la stratégie VPN automatique.

Pour gérer les stratégies VPN :

ÉTAPE 1 Sélectionnez **VPN > VPN IPSec site-à-site > Configuration VPN avancée**. Cliquez sur **Ajouter une ligne**.

ÉTAPE 2 Dans la section **Ajouter/modifier une configuration de stratégie VPN** :

a. Dans le champ **Nom de la stratégie**, entrez un nom unique permettant d'identifier la stratégie.

b. Dans le champ **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).

c. **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'adresse IP ou le nom de domaine complet.

ÉTAPE 3 Dans les sections **Sélection de trafic en local** et **Sélection de trafic distant** :

- **Dans les champs IP locale et IP distante**, indiquez le nombre de points d'extrémité inclus dans la stratégie VPN :
  - **Individuelle** : limite la stratégie à un seul hôte. Saisissez l'adresse IP de l'hôte qui fera partie du VPN dans le champ **Adresse IP**.
  - **Sous-réseau** : autorise l'ensemble d'un sous-réseau à se connecter au VPN. Saisissez l'adresse réseau dans le champ **Adresse IP** 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 IP**. Entrez le masque de sous-réseau, tel que 255.255.255.0, dans le champ **Masque de sous-réseau**. Le champ affiche automatiquement l'adresse de sous-réseau par défaut qui est basée sur l'adresse IP.

REMARQUE N'utilisez pas de sous-réseaux qui se chevauchent pour les sélecteurs de trafic local et distant. L'utilisation de ces sous-réseaux nécessite l'ajout de routes statiques sur le routeur et les hôtes à utiliser. Par exemple, évitez :

Sélecteur de trafic local : 192.168.1.0/24

Sélecteur de trafic distant : 192.168.0.0/16

ÉTAPE 4 Pour le type 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). L'index des paramètres de sécurité (Security Parameter Index, SPI) identifie l'association de sécurité des flux de trafic entrant et sortant.
- **Algorithme de chiffrement manuel** : sélectionnez l'algorithme utilisé pour chiffrer les données.
- **Clé entrante, Clé sortante** : saisissez la clé de chiffrement de la stratégie appliquée au trafic entrant et sortant. La longueur de la clé dépend de l'algorithme de chiffrement choisi :
  - DES : 8 caractères
  - 3DES : 24 caractères
  - AES-128 : 16 caractères
  - AES-192 : 24 caractères
  - AES-256 : 32 caractères
- **Algorithme d'intégrité manuel** : sélectionnez l'algorithme utilisé pour vérifier l'intégrité des données.
- **Clé entrante, Clé sortante** : saisissez la clé d'intégrité (pour l'ESP avec mode d'intégrité) de la stratégie appliquée au trafic entrant et sortant. La longueur de la clé dépend de l'algorithme choisi :
  - MD5 : 16 caractères
  - SHA-1 : 20 caractères
  - SHA2-256 : 32 caractères

ÉTAPE 5 Pour un type de stratégie **Auto**, 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.
- **Groupe DH :** spécifiez l'algorithme de groupe DH utilisé lors de l'échange d'une clé prépartagée. 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.
- **Sélectionner la stratégie IKE** : sélectionnez la stratégie IKE qui définira les caractéristiques de la négociation des associations de sécurité.

ÉTAPE 6 Cliquez sur **Enregistrer**.

Configuration du serveur VPN IPsec

L'utilisation du VPN IPsec permet de disposer d'un accès distant sécurisé aux ressources de l'entreprise en établissant un tunnel chiffré via Internet. Votre périphérique prend en charge les clients VPN IPsec suivants :

- TheGreenBow
- ShrewSoft

Configuration du serveur VPN IPsec

Pour configurer le serveur VPN IPsec :

ÉTAPE 1 Sélectionnez **VPN > Serveur VPN IPSec > Configuration**.

ÉTAPE 2 Cochez la case **Prise en charge serveur**.

ÉTAPE 3 Dans la section **Phase 1**, configurez les paramètres permettant aux deux points d'extrémité VPN de s'authentifier mutuellement et de négocier l'association de sécurité IKE, de façon à établir un canal sécurisé pour la négociation des associations de sécurité à la Phase 2.

a. Dans le champ **Clé prépartagée**, entrez la clé prépartagée, ou le mot de passe, qui sera échangée entre votre périphérique et le point d'extrémité distant. Le mot de passe doit comporter entre 8 et 49 caractères.

b. Dans le champ **Mode Exchange**, choisissez un des modes suivants pour la connexion VPN IPsec :

- **Principal** : négocie le tunnel avec une sécurité supérieure, mais est plus lent.
- **Agressif** : établit plus rapidement la connexion, mais la sécurité est moindre.

c. Choisissez l'**Algorithme de chiffrement** pour chiffrer les données et choisissez l'**Algorithme d'authentification** pour l'en-tête VPN. Vérifiez que l'algorithme d'authentification est configuré de manière identique sur votre périphérique et sur le point d'extrémité distant.

d. Dans le champ **Groupe Diffie-Hellman (DH)**, spécifiez l'algorithme de groupe Diffie-Hellman qui est utilisé lors de l'échange d'une clé prépartagée. Il définit la robustesse de l'algorithme en bits. Vérifiez que le groupe DH est configuré de manière identique sur votre périphérique et sur le point d'extrémité distant.

e. Dans le champ **Durée de vie SA IKE**, saisissez la durée en secondes à l'issue de laquelle l'association de sécurité de la connexion VPN est renégociée.

ÉTAPE 4 Dans la section **Configuration phase 2**, configurez les paramètres permettant de négocier l'association de sécurité IPsec pour le tunnel IPsec :

a. Dans le champ **IP locale**, indiquez le nombre de points d'extrémité inclus dans la stratégie VPN :

- **Individuelle** : limite la stratégie à un seul hôte. Saisissez l'adresse IP de l'hôte qui fera partie du VPN dans le champ **Adresse IP**.

- **Sous-réseau** : autorise l'ensemble d'un sous-réseau à se connecter au VPN. Saisissez l'adresse réseau dans le champ **Adresse IP** 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 IP**. Entrez le masque de sous-réseau, tel que 255.255.255.0, dans le champ **Masque de sous-réseau**. Le champ affiche automatiquement l'adresse de sous-réseau par défaut qui est basée sur l'adresse IP.

b. Dans le champ **Durée de vie SA IPSec**, saisissez la durée en secondes à l'issue de laquelle l'association de sécurité IPsec de la connexion VPN est renégociée.

c. Choisissez l'**Algorithme de chiffrement** pour chiffrer les données et choisissez l'**Algorithme d'authentification** pour l'en-tête VPN. Vérifiez que l'algorithme d'authentification est configuré de manière identique sur votre périphérique et sur le point d'extrémité distant.

d. Pour créer une connexion VPN IPsec plus sécurisée, cochez la case d'activation de **Groupe de clés PFS** garantissant un nouvel échange de clés Diffie-Hellman à la phase 2. Perfect Forward Secrecy (PFS) crée une couche de sécurité supplémentaire en protégeant vos données par une nouvelle clé, au cas où la clé DH générée à la phase1 serait compromise lors du transit. Vérifiez que PFS est activé sur les deux points d'extrémité IPsec.

ÉTAPE 5 Cliquez sur **Enregistrer**.

Configuration des comptes d'utilisateurs VPN IPsec

ÉTAPE 1 Sélectionnez **VPN > Serveur VPN IPSec > Utilisateur**.

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

ÉTAPE 3 Saisissez un nom d'utilisateur et un mot de passe.

Nous vous recommandons d'utiliser un mot de passe qui ne contienne aucun mot figurant dans un dictionnaire, quelle que soit la langue, et qui soit composé de lettres (majuscules et minuscules), de chiffres et de symboles. Le mot de passe peut comporter au maximum 64 caractères.

ÉTAPE 4 Pour importer des noms d'utilisateur et des mots de passe à partir d'un fichier .CSV, cliquez sur **Importer**. La page **Administration > Utilisateurs** s'affiche. Dans la section **Importer le nom de l'utilisateur et le mot de passe**, cliquez sur **Parcourir** pour rechercher le fichier, puis cliquez sur **Importer**.

ÉTAPE 5 Enregistrez vos comptes d'utilisateurs.

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.

Configuration du serveur PPTP

Pour configurer le serveur VPN PPTP :

ÉTAPE 1 Sélectionnez **VPN** > **Serveur PPTP**.

ÉTAPE 2 Dans la section **Configuration du serveur PPTP**, configurez les paramètres VPN PPTP :

a. Cochez la case d'activation de **Serveur PPTP**.

b. Saisissez l'adresse IP du serveur PPTP.

c. Saisissez la plage d'adresses IP des clients PPTP.

d. Pour chiffrer les données transitant par la connexion VPN PPTP, cochez la case d'activation de **Chiffrement MPPE**.

ÉTAPE 3 Cliquez sur **Enregistrer**.

Création et gestion des utilisateurs PPTP

Pour créer et activer les utilisateurs PPTP :

ÉTAPE 1 Sélectionnez **VPN > Serveur PPTP**. Dans la **Table des comptes d'utilisateurs PPTP**, cliquez sur **Ajouter une ligne**.

ÉTAPE 2 Saisissez le nom d'utilisateur et le mot de passe permettant d'authentifier l'utilisateur PPTP. Entrez des valeurs comprises entre 4 et 32 caractères.

ÉTAPE 3 Cochez la case **Activer** pour l'utilisateur.

ÉTAPE 4 Pour importer des noms d'utilisateur et des mots de passe à partir d'un fichier .CSV, cliquez sur **Importer**. La page **Administration > Utilisateurs** s'affiche. Dans la section **Importer le nom de l'utilisateur et le mot de passe**, cliquez sur **Parcourir** pour rechercher le fichier, puis cliquez sur **Importer**.

ÉTAPE 5 Enregistrez vos comptes d'utilisateurs.

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 Cochez la case **Activer** pour choisir le type de trafic autorisé à transiter par le périphérique.

ÉTAPE 3 Cliquez sur **Enregistrer**.

Certificat SSL

Le routeur Cisco RV130/RV130W prend en charge l'authentification par certificat pour les VPN IPsec. Le certificat SSL (Secure Socket Layer) permet le cryptage des données et l'authentification du serveur avant que la session SSL soit établie.

Pour gérer le certificat SSL, cliquez sur **VPN > Certificat SSL.**

- **Table des certificats de confiance et certificats CA**
  - Cliquez sur **Charger** pour vous rendre à la page des **certificats**. Cliquez sur **Parcourir** pour sélectionner un certificat de confiance sur votre disque, puis cliquez sur **Importer**.
- **Autocertificats actifs**
  - Cliquez sur **Charger** pour vous rendre à la page des **certificats**. Cliquez sur **Parcourir** pour sélectionner un autocertificat actif sur votre disque, puis cliquez sur **Importer**.

- **Demandes d'autocertificat**

  Les autocertificats sont émis par une autorité de certification (CA) identifiant votre appareil (ou sont autosignés si vous ne souhaitez pas bénéficier de la protection d'identité offerte par une CA). Pour demander la signature d'un autocertificat à une CA, vous pouvez générer une requête de signature de certificat à partir de la passerelle. Vous devez pour cela saisir les paramètres d'identification et les envoyer à la CA pour signature. Le certificat de confiance de la CA et le certificat signé par la CA seront alors chargés pour activer l'autocertificat permettant la validation de l'identité de cette passerelle. L'autocertificat est ensuite utilisé dans les connexions IPsec avec des homologues pour valider l'authenticité de la passerelle.

  - **Générer un certificat :** pour générer une demande de certificat SSL, cliquez sur **Générer un certificat**. Une nouvelle page de demande d'informations s'ouvre.

    Nom : saisissez le nom du nouveau certificat.

    Objet : veuillez respecter le format « CN=xxx », avec « CN » en lettres capitales

    Algorithme de hachage : sélectionnez l'algorithme approprié dans la liste déroulante.

    Algorithme de signature : sélectionnez l'algorithme approprié dans la liste déroulante.

    Longueur de clé de signature : sélectionnez la longueur appropriée dans la liste déroulante.

    Adresse IP (facultative) : saisissez l'adresse IP du routeur.

    Nom de domaine (facultatif) : saisissez le nom de domaine du routeur.

    Adresse e-mail (facultatif) : saisissez l'adresse e-mail des demandeurs.

  - **Exporter pour l'administrateur :** pour exporter les demandes de certificat sur le disque dur local.

- **Exporter le certificat** : pour télécharger le certificat du routeur, cliquez sur le bouton **Exporter pour le client**.

Cliquez sur **Enregistrer** pour enregistrer la configuration ou cliquez sur **Annuler** pour conserver les réglages précédents.

Assistant de configuration VPN

Pour utiliser l'assistant de configuration VPN :

ÉTAPE 1 Cliquez sur **VPN > Assistant de configuration VPN**.

ÉTAPE 2 La fenêtre de l'assistant s'ouvre. Suivez les instructions affichées à l'écran pour configurer le périphérique.

7

Configuration de la Qualité de service (QoS)

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. Ces garanties sont importantes lorsque la capacité du réseau est insuffisante, notamment pour les applications multimédias de diffusion en temps réel, telles que la voix sur IP, les jeux en ligne et la télévision IP. En effet, ces applications nécessitent 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.

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 :

Montant	La bande passante (Kbit/s) utilisée pour envoyer des données sur Internet.
Descendant	La bande passante (Kbit/s) utilisée pour recevoir des données d'Internet (applicable uniquement au VLAN par défaut).

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

ÉTAPE 2 Renseignez les champs suivants :

Activer	Cochez cette case pour activer la gestion de la bande passante pour ce service.
Direction	Choisissez si vous souhaitez définir la priorité pour le trafic entrant ou sortant.
Catégorie	Choisissez si vous souhaitez définir la priorité de bande passante pour un service, un VLAN/SSID, une IP source (trafic entrant) ou une IP de destination (trafic sortant).
Service	Sélectionnez le service auquel attribuer la priorité.
VLAN/SSID	Choisissez le VLAN ou le SSID pour lequel vous souhaitez définir la priorité.
Adresse IP	Si vous sélectionnez IP source ou IP de destination dans le champ **Catégorie**, entrez l'adresse IP et le masque de sous-réseau de la source ou de la destination.
Masque de sous-réseau	

Priorité	Définissez la priorité (**faible**, **moyenne** ou **élevée**) pour la catégorie sélectionnée.
Remarquage	Cochez cette option pour activer le remarquage sur le DSCP (Differentiated Services Code Point). 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**.
DSCP	Entrez la valeur de remarquage pour les paquets de ce réseau.

ÉTAPE 3 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 de la table, cochez la case correspondante, puis cliquez sur **Supprimer**. Cliquez 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**.

Configurer les paramètres de port QoS

Vous pouvez configurer les paramètres QoS pour chaque port de votre périphérique. Le périphérique prend en charge quatre files d'attente de priorité qui permet de définir la priorité du trafic pour chaque port.

Pour configurer les paramètres QoS des ports de votre périphérique :

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

ÉTAPE 2 Pour chaque port contenu dans la table **Paramètres de port QoS**, saisissez les informations suivantes :

Mode de confiance	Sélectionnez l'une des options suivantes dans le menu déroulant : • **Port** : active les paramètres de port 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 faible (1) et finit avec le niveau de priorité le plus élevé (3). • **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** : classe de service (Class of 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 3).

ÉTAPE 3 Cliquez sur **Enregistrer**.

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

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 transfert du trafic :

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

ÉTAPE 2 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 transfert du trafic**.

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

ÉTAPE 3 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 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 3 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 4 Cliquez sur **Enregistrer**.

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

8

Gestion de votre périphérique

Définition des propriétés du périphérique

Attribuez un nom et un nom de domaine à votre périphérique, afin qu'il soit facilement identifié par les autres périphériques.

Pour définir les propriétés du périphérique :

ÉTAPE 1 Sélectionnez **Administration > Propriétés de l'appareil**.

ÉTAPE 2 Dans le champ **Nom d'hôte**, entrez un nom qui identifie le périphérique de façon unique sur votre réseau. Par exemple, RTR141.

ÉTAPE 3 Dans le champ **Nom de domaine**, entrez le domaine dans lequel se trouve votre périphérique. Par exemple, abcbusiness.com. Si vous ne connaissez pas le nom de domaine de votre organisation, contactez votre administrateur réseau.

ÉTAPE 4 Enregistrez vos modifications.

Définition de la complexité des mots de passe

Vous pouvez 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** > **Complexité 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 (entre 0 et 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

Votre périphérique 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. Nous vous recommandons d'utiliser un mot de passe qui ne contienne aucun mot figurant dans un dictionnaire, quelle que soit la langue, et qui soit composé de lettres (majuscules et minuscules), de chiffres et de symboles. Le mot de passe peut comporter au maximum 64 caractères.
Confirmer le nouveau mot de passe	Saisissez une nouvelle fois le nouveau mot de passe.

ÉTAPE 4 Cliquez sur **Enregistrer**.

Importation de comptes d'utilisateurs

Vous pouvez importer simultanément plusieurs utilisateurs à l'aide d'un fichier CSV.

Assurez-vous que les données du fichier CSV apparaissent comme dans les tableaux suivants :

TYPE	NOM D'UTILISATEUR	MOT DE PASSE
Admin	Admin123	Admin123
Invité	Guest123	Guest123

TYPE	NOM D'UTILISATEUR	MOT DE PASSE	ACTIVER
PPTP	PPTP-user-1	12345678	activer
PPTP	PPTP-user-2	345123678	désactiver

TYPE	NOM D'UTILISATEUR	MOT DE PASSE
VPNServer	vpn-user-1	12345678
VPNServer	vpn-user-2	33245678

TYPE	NOM D'UTILISATEUR	MOT DE PASSE	TEMPS D'ACCÈS
guestnet	guestnet-user-1	12345678	1440
guestnet	guestnet-user-2	33245678	60

REMARQUE Les noms des colonnes respectent la casse. Ne changez pas l'ordre des noms des colonnes.

Pour importer des comptes d'utilisateurs à partir d'un fichier CSV :

ÉTAPE 1 Dans le champ **Importer le nom de l'utilisateur et le mot de passe**, cliquez sur **Parcourir**.

ÉTAPE 2 Trouvez le fichier et cliquez sur **Ouvrir**.

ÉTAPE 3 Cliquez sur **Importer**.

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

REMARQUE Avant de pouvoir utiliser SNMP, vous devez installer le logiciel SNMP sur votre ordinateur. Votre périphérique prend uniquement en charge SNMPv3 pour la gestion SNMP et SNNPv1/2/3 pour les messages de filtre SNMP.

Pour activer SNMP :

ÉTAPE 1 Sélectionnez **Administration** > **SNMP**.

ÉTAPE 2 Cochez la case **Activer** pour activer l'option SNMP.

ÉTAPE 3 Cochez la case **Activer** pour **autoriser l'accès aux utilisateurs via Internet** ou **autoriser l'accès aux utilisateurs via VPN**.

ÉTAPE 4 Saisissez les informations suivantes :

SysContact	Saisissez le nom de la personne à contacter pour ce périphérique. Par exemple, votre administrateur réseau.
SysLocation	Entrez l'emplacement physique du périphérique. Par exemple, Rack n° 2, 4e étage.
SysName	Saisissez un nom permettant d'identifier facilement votre périphérique. Par exemple, RTR 141.

ÉTAPE 5 Cliquez sur **Enregistrer**.

Modification des utilisateurs SNMPv3

Vous pouvez configurer les paramètres SNMPv3 pour les deux comptes d'utilisateurs par défaut (admin et invité) de votre périphérique.

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 et de confidentialité, ainsi que 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 SNMP** vous permettent de configurer un agent SNMP auquel le périphérique envoie les messages de filtre (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 de filtre 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**.
Niveau de gravité d'interruption SNMP	Sélectionnez le niveau de gravité auquel le périphérique doit envoyer des messages de filtre.

ÉTAPE 3 Cliquez sur **Enregistrer**.

ÉTAPE 4 Cliquez sur **Afficher les journaux** pour afficher la table des journaux système.

Utilisation des outils de diagnostic

Votre périphérique fournit 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** > **Diagnostic** > **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 accessible.

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** > **Diagnostic** > **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.

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 de tout autre serveur 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** > **Diagnostic** > **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.

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** > **Diagnostic** > **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 des paramètres de journal et d'e-mail

Configurez les journaux pour surveiller l'activité indiquant l'état de fonctionnement et de performance de votre périphérique.

Configuration des paramètres de journal

Pour configurer la journalisation :

ÉTAPE 1 Sélectionnez **Administration** > **Journalisation** > **Paramètres des journaux**.

ÉTAPE 2 Dans le champ **Mode de journalisation**, cochez la case **Activer**.

ÉTAPE 3 Cochez la case d'activation d'**Alerte e-mail** pour configurer le périphérique afin qu'il envoie des alertes par e-mail à une adresse e-mail spécifique lorsque des

événements ou des comportements sont susceptibles de nuire à la performance, au fonctionnement et à la sécurité du périphérique, ou à des fins de débogage. Cochez la case appropriée pour activer les alertes par e-mail pour les événements suivants :

WAN actif/inactif	Envoie un e-mail lorsque la liaison est inactive et envoie un autre e-mail dès que la liaison est rétablie.
Tunnel VPN IPsec site-à-site actif/inactif	Envoie un e-mail lorsque le tunnel VPN IPsec site-à-site est inactif et envoie un autre e-mail dès que le tunnel est de nouveau actif.
Surcharge du processeur	Envoie une alerte par e-mail si l'utilisation du processeur dépasse le seuil défini et envoie une autre alerte par e-mail dès que l'utilisation du processeur revient à un niveau normal.
Démarrage du système	Envoie une alerte par e-mail au démarrage du périphérique.
Nouveau micrologiciel disponible	Envoie une alerte par e-mail lorsqu'un nouveau micrologiciel est disponible pour le périphérique.

ÉTAPE 4 Cliquez sur **Ajouter une ligne**.

ÉTAPE 5 Configurez les paramètres suivants :

Serveur de journalisation distant	Saisissez l'adresse IP du serveur de journalisation qui enregistrera les journaux.

Indiquer la gravité pour le journal local et les e-mails	Sélectionnez la gravité des événements pour lesquels vous souhaitez enregistrer les journaux et les envoyer à une adresse e-mail spécifique. Tous les types de journaux dont la gravité est supérieure à celle du type de journal sélectionné sont automatiquement inclus et vous ne pouvez pas les exclure. Par exemple, si vous choisissez les journaux Erreur, alors Urgence, Alerte et Critique sont également sélectionnés. Les niveaux de gravité des événements sont répertoriés du niveau le plus élevé au plus faible, 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 du périphérique. • **Débogage** : informations détaillées sur un événement. La sélection de ce niveau de gravité des journaux 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 6 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 de l'envoi des journaux par e-mail

Vous pouvez configurer votre périphérique afin qu'il envoie les journaux par e-mail. Nous vous recommandons de configurer un compte de messagerie distinct pour l'envoi et la réception des journaux.

Vous devez commencer par configurer la sévérité des journaux à capturer ; voir la section **Configuration des paramètres de journal**.

Pour configurer l'envoi des journaux par e-mail :

ÉTAPE 1 Sélectionnez **Administration** > **Journalisation** > **Paramètres d'e-mail**.

ÉTAPE 2 Cochez la case **Activer** pour activer l'envoi des événements de journalisation par e-mail.

La gravité minimale des journaux à capturer s'affiche. Pour la modifier, cliquez sur **Configurer gravité**.

ÉTAPE 3 Configurez les paramètres suivants :

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	Entrez l'adresse e-mail de retour à laquelle le périphérique enverra les messages si les journaux provenant du routeur et acheminés à l'adresse e-mail de destination ne peuvent pas être remis.

Adresse e-mail de destination (1)	Saisissez une adresse e-mail à laquelle envoyer les journaux (par exemple, logging@nom_entreprise.com).
Adresse e-mail de destination (2) (facultatif)	
Adresse e-mail de destination (3) (facultatif)	
Chiffrement e-mail	Sélectionnez SSL ou TSL comme méthode de chiffrement e-mail. Choisissez Désactiver si vous ne voulez pas utiliser une méthode de chiffrement 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	Entrez le nom d'utilisateur d'authentification e-mail (par exemple, logging@nom_entreprise.com).
Mot de passe d'authentification e-mail	Entrez le mot de passe d'authentification e-mail (par exemple, le mot de passe utilisé pour accéder au compte de messagerie que vous avez configuré pour l'envoi des journaux).
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 planning**, 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 des journaux (quotidienne ou hebdomadaire), 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 votre périphérique, si Bonjour est activé, il annonce uniquement 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 de contrôle des interfaces 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 de l'heure**. L'heure actuelle s'affiche.

ÉTAPE 2 Renseignez les champs suivants :

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 case à cocher est estompée lorsque vous cliquez sur **Manuel** dans le champ **Définir la date et l'heure**.
Mode heure d'été	Si vous choisissez **Par date**, entrez la date à laquelle le mode heure d'été doit démarrer. Si vous choisissez **Récurrent**, entrez le mois, la semaine, le jour de la semaine et l'heure de démarrage du mode heure d'été. 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	Indiquez si vous souhaitez que la date et l'heure soient définies manuellement ou automatiquement sur le périphérique. Si vous sélectionnez **Manuel**, saisissez la date et l'heure dans les champs **Entrer la date et l'heure**.

Serveur NTP	Pour utiliser les serveurs NTP par défaut, cliquez sur le bouton **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.

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.

AVERTISSEMENT 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 devrait 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 de fonctionnement la plus couramment utilisée par le périphérique. En cas de perte de la configuration de démarrage du routeur, utilisez cette page pour copier la configuration de secours vers la configuration de démarrage et restaurer les informations de configuration antérieures. Vous pouvez télécharger la configuration de démarrage vers d'autres périphériques RV130/ RV130W pour un déploiement facile.
Configuration miroir	Sélectionnez cette option si le périphérique doit 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 un fichier de sauvegarde d'après l'option de configuration sélectionnée, 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\.

ÉTAPE 4 Pour effacer la configuration sélectionnée, cliquez sur **Effacer**.

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

ÉTAPE 4 Sélectionnez le fichier, puis cliquez sur **Ouvrir**.

ÉTAPE 5 Cliquez sur **Lancer le téléchargement**.

Le périphérique 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. Pour revenir au Gestionnaire de périphérique, rétablissez les valeurs par défaut du périphérique.

Le fichier de Configuration de secours reste en mémoire et permet de copier les informations de configuration sauvegardées vers 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 chiffrement

Le routeur vous permet de générer une clé de chiffrement pour protéger les fichiers de secours.

Pour générer une clé de chiffrement :

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**.

AVERTISSEMENT 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 du micrologiciel

Pour mettre à niveau le micrologiciel vers une version plus récente :

ÉTAPE 1 Sélectionnez **Administration** > **Mise à niveau du micrologiciel/de la langue**.

ÉTAPE 2 (Facultatif) Cliquez sur **Télécharger** pour télécharger la dernière version du micrologiciel.

ÉTAPE 3 Dans le champ **Type de fichier**, cliquez sur le bouton **Image du micrologiciel**.

ÉTAPE 4 Cliquez sur **Parcourir** pour trouver et sélectionner le micrologiciel téléchargé.

ÉTAPE 5 (Facultatif) Pour restaurer les paramètres par défaut du périphérique après une mise à niveau du micrologiciel, cochez la case **Rétablir tous les paramètres/ configurations d'usine**.

AVERTISSEMENT Si vous rétablissez les paramètres par défaut du routeur, tous les paramètres de configuration seront supprimés.

ÉTAPE 6 Cliquez sur **Démarrer la mise à niveau**.

Une fois validée, la nouvelle image du micrologiciel est enregistrée dans la mémoire flash et le routeur est automatiquement redémarré avec le nouveau micrologiciel.

ÉTAPE 7 Sélectionnez **État** > **Récapitulatif du système** pour vous assurer que le routeur a installé la nouvelle version du micrologiciel.

Modification de la langue

Pour changer la langue du périphérique :

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 (Facultatif) Pour rétablir les valeurs par défaut des paramètres de configuration du périphérique, sélectionnez **Rétablir tous les paramètres/configurations d'usine**.

ÉTAPE 5 Cliquez sur **Démarrer la mise à niveau**.

Redémarrage du périphérique

Pour redémarrer le routeur :

ÉTAPE 1 Sélectionnez **Administration** > **Redémarrer**.

ÉTAPE 2 Cliquez sur **Redémarrer**.

Restauration des paramètres d'usine

AVERTISSEMENT 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**.

9

Filtrage Web

La fonction de filtrage Web, disponible sur le routeur, vous permet de gérer l'accès aux sites Web inappropriés. Elle analyse les demandes d'accès à des sites Web sur le réseau du client et décide d'y autoriser ou non l'accès. Ainsi, elle permet de renforcer la sécurité de votre environnement et d'augmenter la productivité de vos collaborateurs.

Un administrateur peut définir des directives sur la sécurité du réseau en général, sur les objets connectés à l'IoT et/ou sur les règles à appliquer sur un réseau personnalisé pour un service spécifique au sein de l'entreprise. Ainsi, l'administrateur peut créer des règles planifiées personnalisées et les lier à des listes d'exceptions autorisant, par exemple, l'accès à des sites spécifiques uniquement à certains utilisateurs, à une heure définie.

Configuration du filtrage Web

Dans cette rubrique, vous apprendrez comment configurer le filtrage Web sur le routeur, ainsi que l'importance de cette fonction. Pour activer et configurer le filtrage Web sur le routeur, procédez de la façon suivante.

ÉTAPE 1 Cliquez sur **Filtrage Web.**

ÉTAPE 2 Dans la section Filtrage Web, sélectionnez l'une de ces options :

- **Toujours activé** : le filtrage Web est activé en permanence
- **Planifié** : un planning est défini pour l'application du filtrage Web
- **Toujours désactivé** : le filtrage Web est désactivé

REMARQUE Par défaut, le filtrage Web est toujours désactivé.

ÉTAPE 3 Dans la section Réputation Web, cochez la case **Activer** pour activer le filtrage en fonction des catégories de filtrage sélectionnées.

ÉTAPE 4 Cliquez sur Catégories et choisissez l'une de ces options pour la gestion et l'application des filtres.

- **Faible** : les catégories Contenu pour adultes et Sécurité sont activées. Pour personnaliser votre filtre, choisissez vos options parmi celles disponibles.
- **Moyen** : les catégories Contenu pour adultes, Contenu illicite/contestable et Sécurité sont activées. Pour personnaliser votre filtre, choisissez vos options parmi celles disponibles.
- **Élevé** : les catégories Contenu pour adultes, Économie/Investissement, Divertissement, Contenu illicite/contestable, Ressources IT, Art de vivre/ Culture et Sécurité sont activées. Pour personnaliser votre filtre, choisissez vos options parmi celles disponibles.
- **Personnalisé** : pas de catégorie activée par défaut. Vous pouvez ainsi personnaliser le filtrage Web.

ÉTAPE 5 Cliquez sur **Enregistrer** et **Retour** pour retourner à la page Filtre et poursuivre la configuration.

ÉTAPE 6 Cochez la case **Activer le filtrage HTTPS** pour filtrer le contenu Web en fonction de l'adresse IP et non de l'URL. Les sites S-HTTP ou HTTPS seront accessibles. Pour bloquer les sites Web sans tenir compte de l'URL, ne cochez pas la case **Activer le filtrage HTTPS**.

REMARQUE Le filtrage HTTPS filtre en fonction de l'adresse IP du serveur Web et non de l'URL, cette dernière étant cryptée. Il arrive souvent que plusieurs sites Web utilisent la même adresse IP de serveur Web. Dans ce cas, si plusieurs catégories de sites Web sont associées à une même adresse IP, le routeur ne bloque pas la page. Toutefois, elle sera bloquée si cette adresse IP héberge du contenu pour adultes ou si elle est connue pour héberger ou répandre des malwares.

ÉTAPE 7 Si vous avez sélectionné **Planifié** comme option de filtrage Web, la Table de planification apparaît. Sous la Table de planification, cliquez sur **Ajouter une ligne** pour créer une règle ou une politique planifiée à appliquer.

ÉTAPE 8 Dans la Table de planification, remplissez les champs Nom et Description.

ÉTAPE 9 Cochez ensuite la case du ou des jours de la semaine pour lesquels vous souhaitez activer le filtre.

ÉTAPE 10 Ensuite, à l'aide de l'horloge au format 24 heures, spécifiez l'heure à laquelle la règle prend effet.

ÉTAPE 11 Enfin, cochez la case **Active** pour activer la règle planifiée.

REMARQUE Vous pouvez appliquer autant de règles que vous le souhaitez.

ÉTAPE 12 Cliquez sur **Enregistrer**.

ÉTAPE 13 (Facultatif) Créez une liste de sites Web/contenus autorisés, interdits ou exclus du processus de filtrage. Choisissez le type de liste parmi ces options suivantes :

- **Liste blanche** : cliquez sur **Ajouter une ligne**, sélectionnez **Nom de domaine** ou **Mot-clé** dans la liste déroulante. Puis saisissez une valeur pour identifier cette politique.
- **Liste noire** : cliquez sur **Ajouter une ligne**, sélectionnez **Nom de domaine** ou **Mot-clé** dans la liste déroulante. Puis saisissez une valeur pour identifier cette politique.
- **Liste d'exclusion** : cliquez sur **Ajouter une ligne**, sélectionnez **Nom de domaine** ou **Mot-clé** dans la liste déroulante. Puis saisissez une valeur pour identifier cette politique.

ÉTAPE 14 Pour modifier ou supprimer une politique de filtrage Web, cochez la case correspondant à cette politique dans la liste et cliquez sur **Modifier** ou **Supprimer.**

ÉTAPE 15 Cliquez sur **Enregistrer.**

10

Pour en savoir plus

Assistance	
Communauté d'assistance Cisco	www.cisco.com/go/smallbizsupport
Assistance et ressources Cisco	www.cisco.com/go/smallbizhelp
Coordonnées de l'assistance téléphonique	www.cisco.com/en/US/support/tsd_cisco_small_business_support_center_contacts.html
Téléchargements de microprogrammes Cisco	www.cisco.com/cisco/software/navigator.html?i=!ch Sélectionnez un lien de téléchargement de microprogrammes. Aucune connexion n'est requise.
Demandes Open Source Cisco	www.cisco.com/go/smallbiz_opensource_request
Cisco Partner Central (connexion partenaire requise)	www.cisco.com/web/partners/sell/smb
Documentation sur les produits	
Routeur VPN multifonction sans fil Cisco RV130/RV130W	www.cisco.com/en/US/products/ps9923/tsd_products_support_series_home.html

Pour connaître les résultats des tests du lot EU 26, rendez-vous sur la page www.cisco.com/go/eu-lot26-results.