Guide d'administration du routeur RV160x

Première publication : 2018-03-07

Dernière modification : 2019-10-13

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

LES SPÉCIFICATIONS ET INFORMATIONS SUR LES PRODUITS PRÉSENTÉS DANS CE MANUEL PEUVENT ÊTRE MODIFIÉES SANS PRÉAVIS. TOUTES LES DÉCLARATIONS, INFORMATIONS ET RECOMMANDATIONS PRÉSENTÉES DANS CE MANUEL SONT PRÉSUMÉES EXACTES, MAIS SONT OFFERTES SANS GARANTIE D'AUCUNE SORTE, EXPRESSE OU IMPLICITE. LES UTILISATEURS SONT ENTIÈREMENT RESPONSABLES DE L'UTILISATION QU'ILS FONT DES PRODUITS.

LA LICENCE LOGICIELLE ET LA GARANTIE LIMITÉE DU PRODUIT SE TROUVENT DANS LA DOCUMENTATION ENVOYÉE AVEC LE PRODUIT ET SONT INTÉGRÉES À LA PRÉSENTE DOCUMENTATION, PAR RÉFÉRENCE. SI VOUS NE TROUVEZ PAS LA LICENCE LOGICIELLE NI LA GARANTIE LIMITÉE, CONTACTEZ VOTRE CONSEILLER CISCO POUR EN OBTENIR UNE COPIE.

Les informations suivantes concernent la conformité FCC des périphériques de classe A : Cet équipement a été testé et déclaré conforme aux spécifications pour un périphérique numérique de classe A, établies dans la partie 15 des réglementations FCC. L'objectif de ces normes est de fournir une protection raisonnable contre toute interférence nuisible lorsque l'équipement est utilisé dans un environnement commercial. Cet équipement génère, utilise et peut émettre de l'énergie à hautes fréquences nuisible et, s'il n'est pas installé et utilisé selon le manuel d'instruction, peut provoquer des interférences gênantes pour les communications radio. L'utilisation de cet équipement dans une zone résidentielle est susceptible de provoquer des interférences nuisibles. Dans ce cas, il incombe aux utilisateurs de corriger les interférences à leurs frais.

Les informations suivantes concernent la conformité FCC des périphériques de classe B : Cet équipement a été testé et déclaré conforme aux spécifications pour un périphérique numérique de classe B, établies dans la partie 15 des réglementations FCC. L'objectif de ces normes est de fournir une protection raisonnable contre toute interférence nuisible dans une installation résidentielle. Cet équipement génère, utilise et peut émettre de l'énergie à hautes fréquences nuisible et, s'il n'est pas installé et utilisé selon les instructions, peut provoquer des interférences gênantes pour les communications radio. Il ne peut toutefois être garanti qu'une installation spécifique ne causera aucune interférence. Si cet équipement provoque des interférences gênantes pour la réception des ondes de radio ou de télévision, détectables en mettant l'équipement hors tension et sous tension, les utilisateurs peuvent tenter de remédier à ces interférences des façons suivantes :

- Réorienter ou déplacer l'antenne de réception
- Éloigner l'équipement du récepteur
- Raccorder l'équipement à une prise électrique située sur un circuit différent de celui auquel le récepteur est connecté
- Demander de l'aide à un revendeur ou technicien radio/télévision expérimenté

Toute modification apportée à ce produit sans l'autorisation de Cisco peut annuler l'agrément FCC et vous retirer l'autorisation d'utiliser ce produit.

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

PAR DÉROGATION À TOUTE AUTRE GARANTIE, TOUS LES FICHIERS DE DOCUMENT ET LOGICIELS DE CES FOURNISSEURS SONT FOURNIS « EN L'ÉTAT » AVEC TOUTES LEURS IMPERFECTIONS. CISCO ET LES FOURNISSEURS MENTIONNÉS CI-DESSUS DÉCLINENT TOUTE GARANTIE EXPLICITE OU IMPLICITE Y COMPRIS, MAIS SANS S'Y LIMITER, TOUTE GARANTIE DE QUALITÉ MARCHANDE, D'ADÉQUATION À UN USAGE PARTICULIER, D'ABSENCE DE CONTREFAÇON OU TOUTE AUTRE GARANTIE DÉCOULANT DE PRATIQUES OU DE RÈGLES COMMERCIALES.

EN AUCUN CAS CISCO OU SES FOURNISSEURS NE PEUVENT ÊTRE TENUS RESPONSABLES DES DOMMAGES INDIRECTS, SPÉCIAUX, CONSÉCUTIFS OU ACCESSOIRES, Y COMPRIS, MAIS SANS S'Y LIMITER, LA PERTE DE PROFITS ET LES PERTES OU DOMMAGES DE DONNÉES DÉCOULANT DE L'UTILISATION OU DE L'INCAPACITÉ D'UTILISER CE MANUEL, MÊME SI CISCO OU SES FOURNISSEURS ONT ÉTÉ AVISÉS DE LA POSSIBILITÉ DE TELS DOMMAGES.

Toutes les adresses de protocole Internet (IP) et les numéros de téléphone utilisés dans ce document ne prétendent pas représenter des adresses et numéros de téléphone réels. Tous les exemples, résultats d'affichage de commandes, schémas de topologie de réseau et autres figures compris dans ce document sont donnés à titre indicatif uniquement. Toute utilisation d'adresses IP ou de numéros de téléphone réels dans un contenu illustratif est involontaire et fortuite.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com go trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2018 Cisco Systems, Inc. Tous droits réservés.

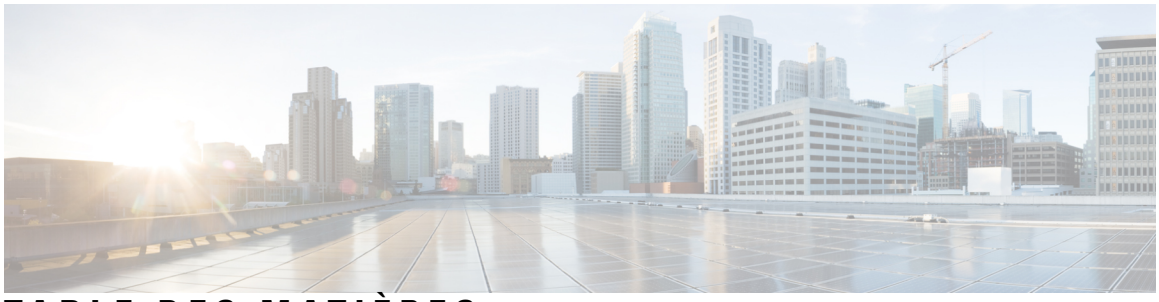
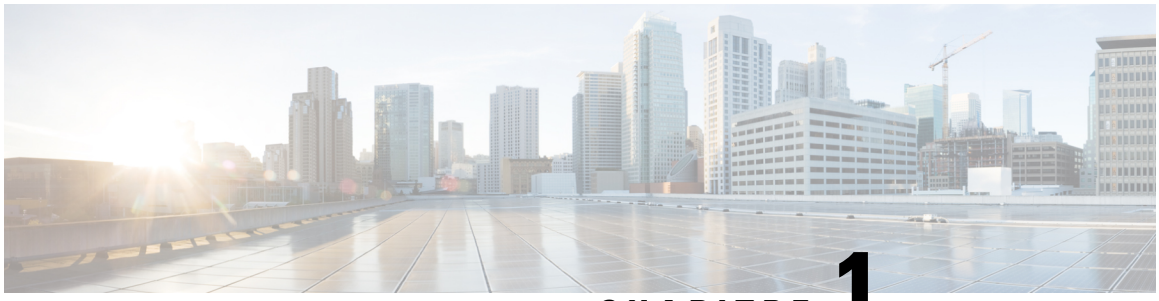


TABLE DES MATIÈRES



CHAPITRE 1

Mise en route

Cette section explique comment commencer à utiliser l'appareil ; elle comprend les rubriques suivantes :

Fonctionnalités des routeurs RV160X

Merci d'avoir choisi les routeurs VPN Cisco RV160/RV160W. Ultraperformants, les routeurs VPN Cisco RV160 et RV160W allient des fonctionnalités professionnelles et des niveaux élevés de sécurité et de fiabilité. Ces deux modèles sont parfaitement adaptés aux réseaux des petites entreprises et des bureaux à domicile.

- **Caractéristiques et avantages**
  - Le routeur VPN RV160 offre une connectivité filaire
  - Le routeur RV160W est un routeur VPN sans fil : 2x2 11ac
  - Ports WAN SFP/RJ45
  - Commutateur natif à 4 ports
  - Ports Gigabit Ethernet hautes performances qui permettent de transférer des fichiers volumineux entre plusieurs utilisateurs
  - Sécurité IP, PPTP et serveur OpenVPN pour assurer la connectivité sécurisée des employés distants et des différents bureaux
  - Sécurité renforcée : pare-feu SPI (inspection dynamique de paquets) éprouvé et cryptage du matériel
  - Configuration et utilisation faciles grâce à un Assistant de configuration
  - Nouvelle interface utilisateur pour faciliter la configuration et la gestion des appareils
  - Conception matérielle actualisée

Spécifications techniques

Description	Spécification
Ethernet WAN	Port Gigabit RJ45/SFP
Ethernet LAN	4 Gigabit Ethernet RJ45
Port console	1 RJ45
Commutateur	Marche/Arrêt
Type de câble	CAT5 ou plus récent
Voyants	Alimentation, VPN, WAN, LAN
Système d'exploitation	Linux
Réseau local	
VLAN	16
Sécurité des ports	Oui, 802.1X
IPv6	6rd/6in4 à double pile
Réseau WAN	Client DHCP (Dynamic Host Configuration Protocol), IP statique, PPPoE (Point-to-Point Protocol over Ethernet), PPTP, L2TP, pont transparent
WLAN	2x2, 11ac sans fil
Sécurité	
Pare-feu	Pare-feu SPI (inspection dynamique de paquets)
	Redirection et déclenchement de ports
	Prévention du déni de service (DoS)
Contrôle d'accès	Listes de contrôle d'accès IP
Gestion sécurisée	HTTPS, complexité nom d'utilisateur/mot de passe
Privilèges des utilisateurs	Deux niveaux d'accès : Administrateur et Invité
Réseau	

Description	Spécification
Protocoles réseau	• Serveur DHCP (Dynamic Host Configuration Protocol) • PPPoE (Point-to-Point Protocol over Ethernet) • PPTP (Point-to-Point Tunneling Protocol) • L2TP (Layer 2 Tunneling Protocol) • Proxy DNS • Agent de relais DHCP • Proxy IGMP et transfert de multidiffusion • RSTP (Rapid Spanning Tree Protocol) • Système de noms de domaine (DNS) dynamique (TZO, DynDNS, 3322.org, NOIP) • Traduction d'adresses réseau (NAT), traduction d'adresses de port (PAT) • NAT un à un • Gestion des ports • Mise en miroir des ports • DMZ configurable par logiciel sur toutes les adresses IP LAN • Passerelles de la couche application (ALG) de protocole d'initiation de session (SIP)
Protocoles de routage	• Routage statique, proxy IGMP • Routage dynamique • RIP v1 et v2 • RIP pour IPv6 (RIPng) • Routage inter-VLAN
Traduction d'adresses réseau (protocole NAT)	Traduction d'adresses de port (PAT), traduction d'adresses de port réseau (NPAT) Redirection de ports, NAT un à un, NAT VPN transversal, Initiation de session (SIP), Passerelle du niveau application (ALG), FTP ALG
VPN	
VPN IPsec passerelle à passerelle	10 tunnels IPSec
VPN IPsec client à passerelle	10 tunnels IPSec

Description	Spécification
VPN IPsec	Prise en charge de IKEv2, GRE, Hub et Spoke
VPN PPTP	10 tunnels VPN PPTP
OpenVPN	Prise en charge du serveur OpenVPN
Cryptage	3DES, AES avec clés 128, 192 et 256 bits
Intercommunication VPN	Intercommunication IPsec/PPTP/L2TP (protocole de tunneling de couche 2)
Qualité de service	
QoS	• Priorité basée sur les ports 802.1p sur le port LAN, priorité basée sur les applications sur le port WAN • 3 files d'attente • DSCP (Differentiated Services Code Point, point de code de services différenciés) • CoS (Class of Service, classe de service) • Gestion de la bande passante pour la hiérarchisation des services
Prise en charge des trames Jumbo	Prise en charge des trames Jumbo sur les ports Gigabit d'au moins 1 536 Go
Performances	
Débit NAT	600 Mbit/s
Sessions simultanées	15 000
Débit du VPN IPsec	50 Mbit/s
Configuration	
Interface utilisateur Web	Configuration basée sur le navigateur (HTTP/HTTPS)
Gestion	Interface utilisateur Web, SNMP v3, Bonjour, Universal Plugand Play (UPnP)
	Prise en charge de FindIT pour la surveillance et la gestion
Comptes rendus d'événements	Local, Syslog, alertes par courriel
Diagnostics du réseau	Ping, Traceroute, recherche DNS
Mises à niveau	Possibilité de mettre à niveau le microprogramme via l'interface utilisateur du navigateur, un fichier importé ou exporté, une clé USB ou Cisco FindIT
Heure système	NTP, heure d'été, réglage manuel
Spécifications environnementales	

Description	Spécification
Alimentation	RV160 : 12 V CC/1,5 A RV160W : 12 V CC/2 A
Température de fonctionnement	0 °C to 40 °C (32 °F à 104 °F)
Température de stockage	-20 c to 70 °C (-4 °f à 158 °F)
Humidité de fonctionnement	De 10 à 85 % sans condensation
Humidité - stockage	De 5 à 90 % sans condensation
Certifications	**Sécurité :** • UL 60950-1 • CAN/CSA-C22.2 No. 60950-1 • IEC 60950-1 • EN 60950-1 **Certifications radio** : • FCC Parties 15.247, 15.407 • RSS-210 (Canada) • EN 300.328, EN 301.893 (Europe) • AS/NZS 4268.2003 (Australie et Nouvelle-Zélande) **EMI et sensibilité (Classe B)** : • FCC Part 15.107 et 15.109 • ICES-003 (Canada) • EN 301.489-1 et -17 (Europe)

Mise en route

Votre périphérique a été configuré en usine avec des paramètres par défaut optimisés pour de nombreuses PME. En fonction de vos exigences réseau ou de votre fournisseur d'accès à Internet (FAI), il est néanmoins possible que vous deviez modifier ces paramètres. Vous pouvez pour cela utiliser l'interface Web, c'est-à-dire Internet Explorer, Firefox ou Safari (pour Mac) sur un ordinateur.

Pour lancer l'interface Web, procédez comme suit :

Étape 1 Raccordez un ordinateur à l'un des ports LAN numérotés sur le périphérique. Si l'ordinateur est configuré pour être utilisé comme client DHCP, une adresse IP comprise dans la plage 192.168.1.x est attribuée à l'ordinateur. DHCP automatise le processus d'affectation d'adresses IP, de masques de sous-réseau, de passerelles par défaut et d'autres

paramètres. Il est nécessaire de configurer les ordinateurs afin qu'ils participent au processus DHCP et obtiennent une adresse. Pour cela, sélectionnez l'option d'obtention automatique d'une adresse IP dans les propriétés TCP/IP de l'ordinateur.

Étape 2 Ouvrez une fenêtre de navigateur Web.

Étape 3 Dans la barre d'adresses, saisissez l'adresse IP par défaut du périphérique, à savoir **192.168.1.1**. Il est possible qu'un avertissement s'affiche sur le navigateur indiquant que le site Web n'est pas approuvé. Accédez quand même au site Web.

Étape 4 Lorsque la page de connexion s'affiche, saisissez le nom d'utilisateur et le mot de passe Cisco par défaut (en minuscules).

Étape 5 Cliquez sur **Connexion**. La page Mise en route s'affiche. Vous pouvez utiliser les liens disponibles sur cette page et suivre les instructions à l'écran pour configurer rapidement votre appareil réseau.

Remarque Si vous rencontrez des difficultés lors de la connexion à Internet ou à l'interface Web :

- Vérifiez que votre navigateur Web n'est pas configuré pour fonctionner hors connexion.
- Vérifiez les paramètres de connexion au réseau local de votre adaptateur Ethernet. L'ordinateur doit obtenir une adresse IP via DHCP. L'ordinateur peut en outre disposer d'une adresse IP statique dans la plage 192.168.1.x avec la passerelle par défaut définie sur 192.168.1.1 (adresse IP par défaut du périphérique).
- Vérifiez que vous avez saisi les bons paramètres de configuration Internet dans l'Assistant.
- Réinitialisez le modem et le périphérique en les mettant hors tension. Mettez sous tension le modem sans l'utiliser pendant environ 2 minutes, puis mettez sous tension l'appareil. Vous devriez maintenant recevoir une adresse IP WAN.
- Si vous possédez un modem ADSL, demandez à votre fournisseur d'accès à Internet de le placer en mode pont.

Vous pouvez également utiliser un ordinateur sans fil pour configurer les modèles de routeur RV160W et RV260W. Lorsque le routeur démarre avec les paramètres par défaut définis en usine, un SSID temporaire est activé. Vous pouvez vous connecter à ce SSID pour configurer le routeur.

Étape 6 Sur un ordinateur, recherchez le SSID et configurez-le comme décrit ci-après. La connexion sans fil est activée et l'ordinateur obtient l'adresse dans la plage 192.168.1.x.

- CiscoSB-Setup
- Sécurité : WPA2-PSK
- Clé prépartagée : cisco123
- Canal : Automatique

Étape 7 Accédez à la page Lancer l'Assistant de configuration en suivant les étapes 2 à 5. Une fois sur cette page, suivez les instructions qui s'affichent. Après avoir transmis la configuration à l'Assistant, le SSID est supprimé et la nouvelle configuration est appliquée.

Remarque Le SSID temporaire (CiscoSB-Setup) est utilisé uniquement pour l'Assistant de configuration initial. Ne l'utilisez pas pour transférer le trafic. Pour identifier votre SSID, accédez aux paramètres Wi-Fi de l'ordinateur et recherchez les réseaux Wi-Fi disponibles dans votre plage.

Lancer l'Assistant de configuration

Suivez les instructions de la page Lancer l'Assistant de configuration pour connaître la procédure de configuration de l'appareil.

Pour ouvrir cette page, sélectionnez **Lancer l'Assistant de configuration** dans le volet de navigation et suivez les instructions à l'écran pour continuer. Contactez votre fournisseur d'accès à Internet (FAI) pour obtenir les informations nécessaires à la configuration de votre connexion Internet.

Lancer l'Assistant de configuration

Configuration initiale du routeur	Lien vers la page **Configuration initiale du routeur**.
Assistant de configuration du VPN	Lien vers la page **Assistant d'état du VPN**.

Configuration initiale

Modifier le mot de passe de l'administrateur	Lien vers la page **Comptes d'utilisateur**, où vous pouvez modifier le mot de passe de l'administrateur et configurer un compte invité.
Configurer les paramètres WAN	Lien vers la page **Paramètres WAN**, où vous pouvez modifier les paramètres WAN.
Configurer les paramètres LAN	Lien vers la page **Appartenance VLAN**, où vous pouvez configurer le réseau VLAN.

Accès rapide

Mettre à niveau le microprogramme du routeur	Lien vers la page **Gestion de fichiers**, où vous pouvez mettre à jour le microprogramme de l'appareil.
Configurer l'accès pour la gestion à distance	Lien vers la page **Pare-feu > Paramètres de base**, où vous pouvez activer les fonctions de base de l'appareil.
Sauvegarder la configuration des appareils	Lien vers la page **Gestion de la configuration**, où vous pouvez gérer la configuration du routeur.

État du périphérique

Récapitulatif du système	Lien vers la page **Récapitulatif du système**, qui fournit des informations sur la configuration IPv4 et IPv6, ainsi que sur l'état du pare-feu de l'appareil.
État du réseau VPN	Lien vers la page **État du VPN**, qui indique l'état des VPN gérés par cet appareil.
Statistiques des ports	Lien vers la page **Trafic sur les ports**, qui indique l'état des ports de l'appareil et le trafic sur les ports.
Statistiques de trafic	Lien vers la page **Services TCP/IP**, qui indique l'état d'écoute des ports de l'appareil et l'état de la connexion établie.
Afficher le journal système	Lien vers la page **Afficher les journaux**, qui répertorie les journaux sur l'appareil.

Interface utilisateur

L'interface utilisateur est conçue pour faciliter la configuration et la gestion des appareils.

Les icônes de la barre d'outils En-tête sont décrites dans le tableau ci-dessous.

Tableau 1 : Options de la barre d'outils En-tête

Icône	Description
	**Bouton bascule** : situé en haut à gauche de l'en-tête, ce bouton vous permet d'afficher ou de réduire le volet de navigation.
	**Sélection de la langue** : cette liste déroulante permet de sélectionner la langue de l'interface utilisateur.
	**Aide** : aide en ligne du routeur.
	**À propos de** : version du microprogramme du routeur.
	**Déconnexion** : cliquez sur ce bouton pour vous déconnecter du routeur.

Légende de l'icône

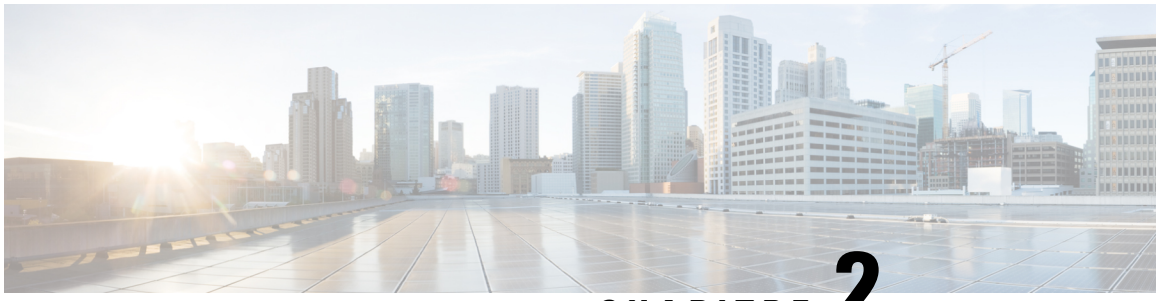
Ce tableau répertorie les icônes les plus courantes de l'interface utilisateur graphique du routeur et leur signification.

	**Ajouter** : cliquez sur cette icône pour ajouter une entrée.
	**Modifier** : cliquez sur cette icône pour modifier une entrée.
	**Supprimer** : cliquez sur cette icône pour supprimer une entrée.
	**Actualiser** : cliquez sur cette icône pour actualiser les données.

	**Réinitialiser les compteurs** : cliquez sur cette icône pour remettre les compteurs à zéro.
	**Cloner** : cliquez sur cette icône pour cloner les paramètres.
	**Exporter** : cliquez sur cette icône pour exporter les configurations.
	**Importer** : cliquez sur cette icône pour importer les configurations.

Fenêtres contextuelles

Certains liens et boutons ouvrent des fenêtres contextuelles contenant des informations détaillées ou les pages de configuration associées. Si un message d'avertissement concernant la fenêtre contextuelle s'affiche sur votre navigateur Web, autorisez le contenu bloqué.



CHAPITRE 2

État et statistiques

Cette section décrit l'état et les statistiques de l'appareil. Elle comprend les rubriques suivantes :

Récapitulatif du système

La section Récapitulatif du système vous permet d'obtenir une vue instantanée des paramètres définis sur votre périphérique. Elle fournit des informations sur le microprogramme du périphérique, le numéro de série, le trafic sur les ports, l'état du routage, les paramètres du serveur VPN et les réseaux mobiles. Pour afficher la section Récapitulatif du système, cliquez sur **État et statistiques > Récapitulatif du système**.

Informations système

- **Numéro de série** : numéro de série de l'appareil.
- **Temps de disponibilité du système** : durée active (au format aa-mm-jj, heures et minutes) durant laquelle le périphérique est resté disponible.
- **Heure actuelle** : date et heure actuelles.
- **VID PID** : numéro de version du matériel.
- **MAC LAN** : adresse MAC du réseau LAN.
- **MAC WAN** : adresse MAC du réseau WAN.

Informations sur le microprogramme

- **Version du microprogramme** : numéro de version du microprogramme installé sur le routeur.
- **Somme de contrôle MD5 du microprogramme** : valeur utilisée à des fins de validation des fichiers.
- **Paramètres régionaux** : localisation définie.
- **Version linguistique** : version linguistique.
- **Somme de contrôle MD5 de la langue** : valeur utilisée à des fins de validation du fichier de langue.

État des ports

- **ID du port** : nom défini et numéro de port.
- **Interface** : nom de l'interface utilisée pour la connexion.
- **État** : état de la connexion.
- **Vitesse** : vitesse de la connexion.

IPv4 et IPv6

Les protocoles IPv4 (Internet Protocol version 4) et IPv6 (Internet Protocol version 6) sont des adresses IP numériques nécessaires pour assurer la communication entre des appareils Internet. Sans adresses IP, les ordinateurs ne pourraient pas communiquer ni envoyer de données entre eux. Elles sont donc essentielles à l'infrastructure Web.

Cette section comprend les options suivantes :

- **Adresse IP** : adresse IP attribuée à l'interface.
- **Passerelle par défaut** : passerelle par défaut de l'interface.
- **DNS** : adresse IP du serveur DNS. Un serveur DNS est un serveur informatique contenant une base de données d'adresses IP publiques et des noms d'hôte associés.
- **DNS dynamique** : le système de noms de domaine (DNS) dynamique permet de mettre à jour automatiquement un serveur de noms dans le DNS, souvent en temps réel, avec la configuration DDNS active des noms d'hôte ou adresses configurés, ou d'autres informations. Cette option permet d'afficher l'adresse IP du DDNS correspondant à l'interface et d'indiquer si celle-ci est **désactivée** ou **activée**.
- **Déconnexion** : cliquez sur ce bouton pour vous déconnecter.
- **Renouveler** : cliquez sur cette option pour renouveler l'adresse IP.

Remarque

- Les boutons Connexion et Déconnexion sont disponibles lorsque le type de connexion WAN est PPTP, L2TP et PPPoE.
- Le réseau WAN est connecté uniquement si vous reconnectez ou modifiez la configuration WAN après avoir déconnecté la connexion WAN existante.

Statut du réseau sans fil

Cette section affiche l'état du réseau sans fil.

- **Radio 1 (2,4 G), Radio 2 (5 G)** et **Activé** : bandes indiquant l'adresse MAC, le mode, le canal et la bande passante, ainsi que les informations correspondantes.

État du réseau VPN

Cette section affiche l'état des tunnels VPN.

- **Type** : type de tunnel VPN.
- **Actif** : indique si le VPN est activé (actif) ou pas.
- **Configuré** : état du tunnel VPN, que ce dernier soit ou pas configuré.
- **Nombre maximal pris en charge** : nombre maximal de tunnels pris en charge sur l'appareil.
- **Connecté** : état du tunnel.

État des paramètres du pare-feu

Cette section affiche l'état du pare-feu.

- **Inspection dynamique de paquets (SPI)** : état du filtre SPI, à savoir Activé ou Désactivé. Les paquets légitimes sont uniquement autorisés via le pare-feu. Cette fonction est également appelée « filtrage dynamique des paquets ».
- **DoS (Déni de service)** : état du filtre DoS, à savoir Activé ou Désactivé. Une attaque DoS est une tentative de rendre indisponible une ressource d'ordinateur ou de réseau aux utilisateurs concernés.
- **Bloquer la requête WAN** : cette fonction permet de compliquer l'accès au réseau pour les utilisateurs extérieurs en masquant les ports réseau des équipements Internet ; elle permet également d'éviter que d'autres utilisateurs Internet puissent détecter le réseau ou le tester à l'aide de requêtes Ping.
- **Gestion à distance** : cette fonction indique si une connexion à distance pour gérer l'appareil est autorisée ou refusée.
- **Règle d'accès** : cette fonction indique le nombre de règles d'accès ayant été définies.

État des paramètres du journal

Les journaux permettent d'effectuer le suivi de l'activité du routeur, des échecs de processus, des événements de pare-feu, des connexions et déconnexions aux appareils WAN, des mises à jour DDNS (DNS dynamique), des états de connexion du réseau VPN, et de nombreux autres événements se produisant sur le routeur. Les journaux sont très utiles pour surveiller l'état du routeur et résoudre les problèmes d'intégrité à des moments particuliers.

- **Syslog Server** : état des journaux système.
- **Journaux par e-mail** : état des journaux à envoyer par e-mail.

Services TCP/IP

La page Services TCP/IP fournit des statistiques sur le protocole, les ports et les adresses IP. Pour afficher la page Services TCP/IP, cliquez sur **État et statistiques > Services TCP/IP**.

État d'écoute des ports

Cette section affiche l'état des ports ouverts pour recevoir (écouter) les données.

- **Protocole** : type de protocole utilisé pour la communication.
- **Adresse IP d'écoute** : l'adresse IP d'écoute indique l'interface sur laquelle elle écoute.
- **Port d'écoute** : le port d'écoute fait office de terminal dans un système d'exploitation pour divers types de communications.

État de la connexion établie

Cette section affiche l'état des ports disposant d'une connexion établie.

- **Protocole** : type de protocole utilisé pour la communication.
- **Adresse IP locale** : adresse IP du système.
- **Port local** : ports d'écoute sur les différents services.
- **Adresse externe** : adresse IP de l'appareil connecté.
- **Port externe** : port de l'appareil connecté.
- **État** : état de connexion de la session.

Trafic sur les ports

La page Trafic sur les ports fournit des statistiques et des renseignements sur l'état des interfaces du périphérique. Pour afficher la page Trafic sur les ports du périphérique, cliquez sur **État et statistiques > Trafic sur les ports**.

Trafic sur les ports

- **ID du port** : identifiant du port.
- **Libellé de port** : libellé du port.
- **État de la liaison** : état de l'interface.
- **Paquets reçus** : nombre de paquets reçus sur le port.
- **Octets reçus** : nombre de paquets reçus, mesurés en octets.
- **Paquets émis** : nombre de paquets envoyés sur le port.
- **Octets émis** : nombre de paquets envoyés, mesurés en octets.

- **Erreur de paquet** : informations concernant les paquets d'erreurs.

Trafic sans fil

- **Nom SSID** : détails du nom SSID.
- **Nom de la radio** : nom de la radio.
- **État** : état du port (p. ex : port activé, désactivé ou déconnecté).
- **Nombre de clients associés** : nombre de clients associés sur le réseau sans fil.
- **Paquets reçus** : nombre de paquets reçus.
- **Octets reçus** : nombre d'octets reçus.
- **Paquets émis** : nombre de paquets envoyés.
- **Octets émis** : nombre d'octets envoyés.
- **Paquets de multidiffusion** : nombre de paquets de multidiffusion.
- **Erreur de paquet** : nombre d'erreurs de paquets.
- **Paquet rejeté** : nombre de paquets rejetés.
- **Collisions** : nombre de collisions.

Cliquez sur le bouton Actualiser pour actualiser les données, ou sur **Réinitialiser** pour remettre les compteurs à zéro.

État des ports

- **ID du port** : nom défini et numéro de port.
- **État de la liaison** : état de l'interface.
- **Activité du port** : état du port (p. ex : port activé, désactivé ou déconnecté).
- **État du débit** : débit (en Mbit/s) de l'appareil après la négociation automatique.
- **État du duplex** : mode duplex, à savoir Semi-duplex ou Duplex intégral.
- **Négociation automatique** : état du paramètre de négociation automatique. Lorsque ce paramètre est activé (**Activé**), le mode duplex est détecté. Si la connexion nécessite une détection automatique, la configuration MDI ou MDIX correspondant à l'autre extrémité de la liaison est automatiquement choisie.

Statistiques de QoS WAN

La page Statistiques de QoS WAN contient des statistiques sur la qualité de service (QoS) WAN sortante et entrante. Pour afficher la page Statistiques de QoS WAN du périphérique, cliquez sur **État et statistiques > Statistiques de QoS WAN**.

- **Interface** : sélectionnez le nom de l'interface dans la liste déroulante.
- **Nom de la stratégie** : nom de la stratégie.

- **Description** : description des statistiques de QoS WAN.
- **Effacer les compteurs** : option permettant d'effacer les compteurs.

Statistiques de QoS sortante

- **File d'attente** : nombre de files d'attente sortantes.
- **Classe de trafic** : nom de la classe de trafic affectée à la file d'attente.
- **Paquets envoyés** : nombre de paquets sortants de la classe de trafic envoyés.
- **Paquets rejetés** : nombre de paquets sortants rejetés.

Statistiques de QoS entrante

- **File d'attente** : nombre de files d'attente entrantes.
- **Classe de trafic** : nom de la classe de trafic affectée à la file d'attente.
- **Paquets transmis** : nombre de paquets entrants de la classe de trafic transmis.
- **Paquets rejetés** : nombre de paquets entrants rejetés.

Afficher les statistiques de QoS de commutation

La page Afficher les statistiques de QoS de commutation présente des statistiques sur le débit d'envoi des paquets depuis une file d'attente, et sur le débit de rejet des paquets alloués, conformes ou dépassés. Pour afficher la page Afficher les statistiques de QoS de commutation, cliquez sur **État et statistiques > Afficher les statistiques de QoS de commutation**.

- **Effacer les compteurs** : toutes les statistiques de la table sont réinitialisées.

Réseau local

- **File d'attente** : nombre de files d'attente sortantes.
- **Port** : numéro du port.
- **Paquets envoyés** : nombre de paquets sortants de la classe de trafic envoyés.

Appareils connectés

La page Appareils connectés répertorie tous les appareils connectés sur le routeur. Pour afficher la page Appareils connectés, cliquez sur **État et statistiques > Appareils connectés**.

IPv4

- **Nom d'hôte** : nom de l'appareil connecté.
- **Adresse IPv4** : adresse IP de l'appareil connecté.

- **Adresse MAC** : adresse MAC de l'appareil connecté.
- **Type** : type d'adresse IP de l'appareil connecté.
- **Interface** : interface à laquelle l'appareil est connecté.
- **SSID** : nom principal attribué à un réseau sans fil.

IPv6

- **Nom d'hôte** : nom de l'appareil connecté.
- **Adresse IPv6** : adresse IPv6 de l'appareil connecté.
- **Adresse MAC** : adresse MAC de l'appareil connecté.
- **Type** : type d'adresse IP de l'appareil connecté.
- **Interface** : interface à laquelle l'appareil est connecté.
- **SSID** : nom principal attribué à un réseau sans fil.

Table de routage

Le routage est un processus consistant à déplacer les paquets sur un réseau d'un hôte à un autre. L'état de routage de ce processus s'affiche dans une table de routage. La table de routage contient des informations sur la topologie du réseau le plus proche. Pour afficher l'état de routage de l'appareil pour IPv4 et IPv6, cliquez sur **État et statistiques > Table de routage**.

Routes IPv4 et IPv6

- **Destination** : adresse IP et masque de sous-réseau de la connexion.
- **Saut suivant** : adresse IP du saut suivant.
- **Nombre de sauts** : nombre d'appareils intermédiaires (tels que des routeurs) par lesquels doivent passer les données entre la source et la destination.
- **Interface** : nom de l'interface à laquelle la route est liée.
- **Source** : source de la route.

Liaisons DHCP

La page Liaisons DHCP fournit des renseignements sur l'adresse IP et l'adresse MAC, la durée d'expiration du bail et le type de liaison (statique ou dynamique). Pour afficher la page Liaisons DHCP du périphérique, cliquez sur **État et statistiques > Liaisons DHCP**. Sélectionnez un nom d'hôte dans la liste et cliquez sur **Ajouter au DHCP statique** pour ajouter la liaison à la table de liaisons. Cliquez sur l'icône d'actualisation pour actualiser les données de la table de liaisons.

La table de liaisons DHCP fournit les renseignements suivants :

- **Nom d'hôte** : nom de l'hôte.

- **Adresse IPv4/IPv6** : adresse IP attribuée à IPv4 ou IPv6.
- **Adresse MAC** : adresse MAC de l'adresse IP attribuée au client.
- **Expiration du bail** : durée du bail du système du client.
- **Type** : état de connexion (**Statique** ou **Dynamique**).
- **Action** : état d'action des liaisons DHCP.

État du réseau VPN

La page État du VPN indique l'état du tunnel des clients site à site, client à site, OpenVPN et PPTP. Pour afficher la page État du VPN de l'appareil, cliquez sur **État et statistiques > État du VPN**.

État du tunnel site à site

- **Tunnel(s) utilisé(s)** : tunnels VPN en cours d'utilisation.
- **Tunnel(s) disponible(s)** : tunnels VPN disponibles.
- **Tunnel(s) activé(s)** : tunnels VPN activés.
- **Tunnel(s) défini(s)** : tunnels VPN définis.

La table des connexions vous permet d'ajouter, de modifier, de supprimer ou d'actualiser un tunnel Vous pouvez également cliquer sur **Sélection des colonnes affichées** pour sélectionner les en-têtes de colonne affichés dans la table des connexions.

État du tunnel GRE

La Table des connexions fournit les informations suivantes :

- **Nom de l'interface** : nom de l'interface.
- **Adresse IP** : adresse IP du tunnel GRE.
- **Source** : source du tunnel GRE.
- **Destination** : destination du tunnel GRE.
- **Activer** : option permettant d'activer le tunnel GRE.
- **État** : état du tunnel GRE.

État du VPN client à site

Dans ce mode, le client Internet se connecte au serveur pour accéder au réseau d'entreprise ou au réseau LAN derrière le serveur. Pour une connexion sécurisée, vous pouvez implémenter un VPN client à site. Vous pouvez afficher toutes les connexions client à tunnel, et ajouter, modifier ou supprimer les connexions dans la table des connexions

La Table des connexions fournit les informations suivantes :

- **Nom du groupe/tunnel** : nom du tunnel VPN. Cette information sert uniquement de référence et ne correspond pas au nom utilisé à l'autre extrémité du tunnel.

- **Connexions** : état de la connexion.
- **Cryptage/authentification/groupe de phase 2** : type de cryptage (NULL/DES/3DES/AES-128/AES-192/AES-256), méthode d'authentification (NULL/MD5/SHA1) et numéro de groupe DH (1/2/5) de phase 2.
- **Groupe local** : adresse IP et masque de sous-réseau du groupe local.
- **Action** : état d'action.

État du client OpenVPN

OpenVPN est une application logicielle ouverte qui met en œuvre des techniques VPN et qui permet de créer des connexions point à point ou site à site sécurisées dans les configurations routées ou pontées, et dans les environnements d'accès à distance. Vous pouvez afficher l'état du client OpenVPN.

La Table des connexions indique l'état du client OpenVPN. Vous pouvez également ajouter, modifier ou supprimer les connexions.

- **ID de session** : identifiant de la session.
- **Utilisateur** : nom de l'utilisateur.
- **IP du client (actuel)** : adresse IP du client actuel.
- **IP du client (VPN)** : adresse IP du client VPN.
- **Octets émis** : nombre d'octets envoyés.
- **Octets reçus** : nombre d'octets reçus.
- **Durée de connexion** : durée de la connexion.
- **Action** : état d'action.

État du tunnel PPTP

Le protocole PPTP (Point-to-Point Tunneling Protocol - protocole de tunneling point à point) permet de crypter les données sur 128 bits. Il permet d'assurer la sécurisation des messages envoyés d'un nœud VPN à un autre.

- **Tunnel(s) utilisé(s)** : tunnels PPTP utilisés pour la connexion VPN.
- **Tunnel(s) disponible(s)** : tunnels disponibles pour la connexion PPTP.

La Table des connexions indique l'état des tunnels établis. Vous pouvez également connecter ou déconnecter les connexions.

- **ID de session** : ID de session de la connexion proposée ou en cours.
- **Nom d'utilisateur** : nom de l'utilisateur connecté.
- **Adresse distante** : adresse IP de la connexion distante.
- **Adresse IP PPTP** : adresse IP du client PPTP.
- **Durée de connexion** : durée du tunneling.
- **Action** : connexion ou déconnexion du tunnel.

Affichage des journaux

La page Afficher les journaux affiche tous les journaux du périphérique. Vous pouvez filtrer ces journaux en fonction de la catégorie, de la gravité ou d'un mot-clé. Vous pouvez en outre actualiser, effacer et exporter ces journaux vers un ordinateur ou une clé USB. Pour afficher les journaux du périphérique, procédez comme suit :

Étape 1 Cliquez sur **État et statistiques > Afficher les journaux**.

Étape 2 Sous Journaux filtrés par, sélectionnez l'option appropriée.

Catégorie	Cliquez sur l'une des options d'affichage suivantes : • **Tous** : tous les journaux s'affichent. • **Catégorie** : les journaux de la catégorie sélectionnée s'affichent.
Gravité	Sélectionnez l'une des options disponibles pour afficher les journaux en fonction de leur gravité.
Mot-clé	Saisissez un mot-clé pour afficher les journaux correspondants.

Étape 3 Cliquez sur **Afficher les journaux**.

Remarque Pour configurer les paramètres de journal, reportez-vous à la section Journal, à la page 34.

Étape 4 Cliquez sur l'une des options suivantes :

- **Actualiser** : cliquez sur cette option pour actualiser les journaux.
- **Effacer les journaux** : cliquez sur cette option pour effacer les journaux.
- **Exporter les journaux vers un ordinateur** : cliquez sur cette option pour exporter les journaux vers un ordinateur.
- **Exporter les journaux vers une clé USB** : cliquez sur cette option pour exporter les journaux vers un périphérique de stockage USB.

État du portail captif

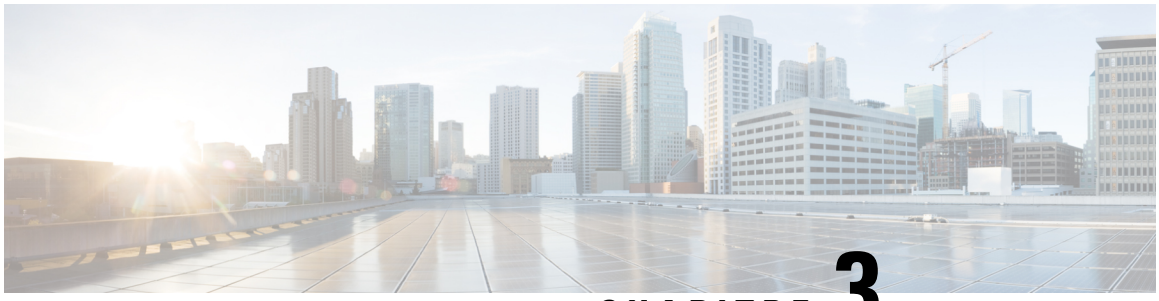
Pour utiliser le portail captif, les utilisateurs doivent accepter les conditions générales avant de se connecter à un réseau d'accès Internet public. Les portails captifs sont généralement destinés aux centres d'affaires, aéroports, hôtels, cafés et autres sites qui offrent des points d'accès Wi-Fi à leurs utilisateurs.

Vous pouvez afficher l'état du portail captif en sélectionnant **État et statistiques > État du portail captif**. Sélectionnez ensuite le SSID dans la liste déroulante ; l'état de connexion de l'utilisateur du portail captif correspondant au SSID sélectionné s'affiche.

- **Nom d'utilisateur** : nom de l'utilisateur connecté.
- **SSID** : nom du réseau.
- **Adresse IP** : adresse IP fournie par le fournisseur d'accès.

- **Adresse MAC** : masque fourni par le fournisseur d'accès.
- **Auth.** : passerelle par défaut fournie par le fournisseur d'accès.
- **Octets émis** : nombre de paquets envoyés, mesurés en octets.
- **Octets reçus** : nombre de paquets reçus, mesurés en octets.
- **Temps restant** : durée d'utilisation de l'appareil connecté.
- **Arrêter les utilisateurs** : passerelle par défaut de l'interface.

Vous pouvez cliquer sur **Actualiser** pour actualiser les données.



CHAPITRE 3

Administration

Cette section décrit les fonctions d'administration du périphérique. Elle contient les rubriques suivantes :

Gestion des fichiers

La section Gestion de fichiers vous permet d'obtenir une vue instantanée des paramètres définis sur votre périphérique. Pour afficher les informations de gestion de fichiers, procédez comme suit :

Étape 1 Cliquez sur **Administration> Gestion des fichiers** pour afficher les informations suivantes :

Informations système

- **Modèle de périphérique** : numéro de modèle du périphérique.
- **VID PID** : PID et numéro VID du routeur.
- **Version actuelle du microprogramme** : version actuelle du microprogramme.
- **Dernière version du microprogramme** : dernière version du microprogramme.
- **Dernière mise à jour du microprogramme** : date de la dernière mise à jour du microprogramme.

Fichier de langue

- **Version actuelle** : version actuelle du fichier de langue sur le périphérique.

Mise à niveau manuelle

La section Mise à niveau manuelle permet de charger et d'effectuer des mises à niveau vers une version plus récente de l'image du microprogramme ou du fichier de langue.

Mise en garde Lors d'une mise à niveau du microprogramme, n'essayez pas de vous connecter à Internet, n'éteignez 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 l'endommager et rendre le routeur inutilisable.

Étape 2 Si vous choisissez d'appliquer la mise à niveau à partir de la clé USB, le routeur recherche dans la clé USB le fichier image du microprogramme dont le nom comporte un ou plusieurs des éléments suivants : PID, adresse MAC et numéro de série. Si la clé USB contient plusieurs fichiers de microprogramme, le routeur sélectionne celui portant le nom le plus spécifique, notamment en classant les fichiers par ordre de priorité, du nom le plus détaillé au nom le plus simple.

Mise à niveau manuelle

Pour mettre à niveau le routeur vers une version plus récente du microprogramme :

Étape 1 Cliquez sur **Administration> Gestion de fichiers**.

Étape 2 Dans la section Mise à niveau manuelle, sélectionnez le type de fichier.

Étape 3 Dans la section Mise à niveau depuis, sélectionnez une option (**Cisco.com, PC ou USB**).

a) Si vous sélectionnez Cisco.com, cliquez sur **Mettre à niveau** pour mettre à niveau le microprogramme ou sur **Télécharger sur USB** pour enregistrer le fichier image du microprogramme.

b) Si vous sélectionnez PC ou USB, cliquez sur **Parcourir** pour rechercher le fichier du microprogramme sur votre ordinateur, puis cliquez sur **Mettre à niveau**.

Étape 4 Activez l'option **Rétablir tous les paramètres/la configuration d'usine** pour réinitialiser la configuration et appliquer les paramètres d'usine.

Étape 5 Cliquez sur **Mettre à niveau** pour charger l'image sélectionnée sur le routeur.

Mise à jour automatique

Le routeur prend en charge le chargement d'un microprogramme à partir d'une clé USB si celle-ci est raccordée avant le démarrage du système. Le routeur recherche dans la clé USB le fichier image du microprogramme dont le nom comporte un ou plusieurs des éléments suivants : PID, adresse MAC et numéro de série. Si la clé USB contient plusieurs fichiers de microprogramme, le routeur sélectionne celui portant le nom le plus spécifique, notamment en classant les fichiers par ordre de priorité, du nom le plus détaillé au nom le plus simple.

- PID-MAC-SN.IMG
- PID-SN.IMG
- PID-MAC.IMG
- PID.IMG

Les fichiers portant d'autres noms sont ignorés. Si la version est ultérieure à la version actuelle, elle est mise à niveau vers ce fichier image et le système redémarre. Après quoi, le processus de mise à niveau recommence.

Si le routeur ne trouve pas de fichier image plus récent dans l'interface USB1, il effectue une recherche dans l'interface USB2 en suivant la même logique.

Le routeur peut également charger un fichier de configuration à partir d'une clé USB lors du démarrage du système.

- Cette fonctionnalité est disponible uniquement lorsque le routeur utilise sa configuration d'origine et qu'il est mis sous tension après le raccordement d'une

  clé USB.

- Le routeur recherche dans la clé USB un fichier de configuration dont le nom comporte un ou plusieurs des éléments suivants : PID,

  adresse MAC et numéro de série. Si la clé USB contient plusieurs fichiers de microprogramme, le routeur sélectionne

  celui portant le nom le plus spécifique, notamment en classant les fichiers par ordre de priorité, du nom le plus détaillé au nom le plus simple.

  - PID-MAC-SN.xml
  - PID-SN.xml
  - PID-MAC.xml
  - PID.xml

Les fichiers portant d'autres noms sont ignorés.

*Mécanisme de reprise automatique du microprogramme

Un mécanisme de reprise est disponible pour que le routeur puisse surmonter les pannes lors d'une recherche directe dans le système de fichiers racine, ou lorsqu'il est tout simplement impossible d'installer le microprogramme sur le système de fichiers racine pour des raisons pratiques. Le routeur dispose de deux images de microprogramme dans la mémoire flash, qui fournissent un mécanisme de reprise automatique afin que le périphérique puisse basculer automatiquement sur le microprogramme secondaire lorsque le microprogramme actif est endommagé ou ne démarre pas après cinq tentatives.

Le mécanisme de reprise automatique fonctionne de la façon suivante :

Étape 1 L'appareil démarre avec le microprogramme actif.

Étape 2 Si le microprogramme est endommagé, il bascule automatiquement sur le microprogramme secondaire après cinq échecs de démarrage.

Étape 3 Si le routeur se bloque et ne démarre pas automatiquement, mettez-le hors tension puis de nouveau sous tension, attendez 30 secondes, puis remettez-le hors tension. Répétez cette opération à 5 reprises pour basculer sur le microprogramme secondaire ou inactif.

Étape 4 Lorsque le routeur redémarre avec le microprogramme secondaire ou inactif, vérifiez les erreurs de fonctionnement avec le microprogramme actif.

Étape 5 Rechargez le nouveau microprogramme si nécessaire.

*Remarque - Cette fonctionnalité sera temporairement désactivée à partir du 1er janvier 2020.

Redémarrage

Le redémarrage permet aux utilisateurs de redémarrer le périphérique avec des images actives ou inactives.

Pour accéder à la page de redémarrage, procédez de la façon suivante :

Étape 1 Cliquez sur **Administration > Redémarrage**.

Étape 2 Dans la section Image active après redémarrage, sélectionnez une option (**Image active x.x.xx.xx**) dans la liste déroulante.

Étape 3 Sélectionnez l'une des options de redémarrage suivantes.

- Redémarrez l'appareil.
- Rétablissez les paramètres d'usine après le redémarrage.
- Rétablissez les paramètres d'usine (notamment les certificats) après le redémarrage.

Étape 4 Cliquez sur **Redémarrage** pour redémarrer le périphérique.

Diagnostic

Votre routeur comporte plusieurs outils de diagnostic destinés à la résolution des problèmes réseau. Utilisez les outils de diagnostic suivants pour vérifier l'intégrité globale de votre réseau.

Vous pouvez utiliser l'utilitaire Ping ou Traceroute pour tester la connectivité entre un routeur et un autre périphérique sur le réseau. Pour cela, procédez comme suit :

Étape 1 Sélectionnez **Administration > Diagnostic**.

Étape 2 Dans le champ Adresse IP/nom de domaine, saisissez l'adresse IP ou le nom de domaine.

Étape 3 Cliquez sur **Ping** pour afficher les résultats du test Ping. Ils vous indiquent si le périphérique est accessible. Cliquez sur **Traceroute** pour afficher les résultats du test Traceroute.

Étape 4 Pour lancer une recherche DNS, saisissez l'adresse IP ou le nom de domaine dans le champ Effectuer une recherche DNS, puis cliquez sur **Rechercher**.

Étape 5 Vous pouvez exporter le rapport de l'assistance technique ; pour cela, sélectionnez l'une des options suivantes :

- **Exporter vers un ordinateur** : pour exporter le rapport de l'assistance technique vers un ordinateur.
- **Exporter vers une clé USB** : pour exporter le rapport de l'assistance technique vers une clé USB.
- **Envoyer par e-mail à... :** pour envoyer le rapport à une adresse e-mail.

Certificat

Les certificats sont essentiels dans le processus de communication. Une autorité de certification (CA) approuvée permet de s'assurer que le détenteur du certificat est bien celui qu'il prétend être. Sans certificat signé approuvé, les données sont certes cryptées, mais la personne avec laquelle vous communiquez n'est peut-être pas celle que vous croyez.

Une liste des certificats contenant les détails de chaque certificat s'affiche sur cette page. Vous pouvez exporter un certificat autosigné, local et CSR.

Si un certificat de périphérique est importé, il remplace le certificat CSR correspondant.

Les certificats associés au routeur s'affichent dans la table de certificats. Vous pouvez supprimer, exporter, afficher les détails ou importer un certificat répertorié dans la table de certificats.

Importer le certificat

Pour importer un certificat, procédez comme suit.

Étape 1 Cliquez sur **Importer le certificat**.

Étape 2 Sélectionnez le type de certificat à importer dans la liste déroulante :

- Certificat CA
- Certificat de périphérique local
- Fichier codé au format PKCS#12

Étape 3 Saisissez le nom du certificat (pour PKCS#12, vous devez saisir un mot de passe).

Étape 4 Dans la section Charger le certificat, sélectionnez **Importer depuis un ordinateur**, puis cliquez sur **Parcourir** pour charger et importer le certificat à partir d'un emplacement spécifique.

Étape 5 Sélectionnez **Importer depuis un périphérique USB**, puis cliquez sur **Actualiser** pour charger et importer le certificat à partir d'une clé USB.

Étape 6 Cliquer sur **Charger**.

Générer un CSR/un certificat

Pour générer un CSR/certificat, procédez comme suit :

Étape 1 Cliquez sur **Générer un CSR/un certificat**.

Étape 2 Sélectionnez le type de certificat à générer en choisissant l'une des options suivantes de la liste déroulante :

a) **Certificat autosigné** : sélectionnez ce certificat et renseignez les champs requis. Vous devez indiquer une durée de validité, en jours.

b) **Certificat CA** : sélectionnez ce type de certificat et renseignez les champs requis pour configurer une signature automatique.

c) **Demande de signature de certificat** : sélectionnez ce type de certificat et renseignez les champs requis.

d) **Certificat signé par un certificat CA** : sélectionnez ce type de certificat et renseignez les champs requis pour faire signer ce certificat par une autorité de certification.

Étape 3 Saisissez les informations suivantes :

Nom du certificat	Donnez un nom au certificat. Le nom du certificat ne doit pas comporter d'espaces ni de caractères spéciaux.
Nom de sujet alternatif (facultatif)	Saisissez un nom et sélectionnez l'un des paramètres suivants : **Adresse IP, Nom de domaine complet ou E-mail**.
Nom du pays	Sélectionnez un pays dans la liste déroulante.
Nom du département/région	Saisissez le nom du département ou de la région.
Nom de la localité	Saisissez le nom de la localité.
Nom de l'organisation	Saisissez le nom de l'organisation.
Nom de l'unité d'organisation	Saisissez le nom de l'unité d'organisation.
Nom courant	Saisissez un nom courant.
Adresse e-mail	Saisissez l'adresse e-mail.
Longueur de clé de cryptage	Sélectionnez la longueur de la clé de cryptage dans le menu déroulant. Elle doit être de 512, de 1 024 ou de 2 048.
Durée de validité	Saisissez le nombre de jours (**Plage : 1-10 950, Valeur par défaut : 360**).

Étape 4 Cliquez sur **Générer**.

Afficher les certificats CA tiers intégrés

Dans la table de certificats tiers, vous pouvez vérifier les détails des certificats, et exporter ou supprimer un certificat. Pour afficher des certificats tiers intégrés, procédez comme suit :

Étape 1 Cliquez sur **Afficher les certificats CA tiers intégrés**.

Étape 2 Sélectionnez un certificat dans la table et cliquez sur **Exporter**.

Étape 3 Cliquez sur **Détails** pour afficher les détails du certificat.

Étape 4 Cliquez sur **Supprimer** pour supprimer le certificat.

Remarque Si vous souhaitez supprimer un certificat CA tiers, veillez à exporter et à enregistrer une copie avant la suppression au cas où vous souhaitiez récupérer le certificat ultérieurement.

Gestion de la configuration

La page Gestion de la configuration fournit des renseignements sur la configuration des fichiers du routeur.

- **Nom du fichier de configuration** : cette section indique l'heure de dernière modification.
- **Copier/enregistrer la configuration** : cette section fournit des renseignements sur la configuration par défaut de l'appareil utilisant le fichier de configuration de fonctionnement, qui est instable et ne conserve pas les paramètres entre les redémarrages. Vous pouvez enregistrer ce fichier de configuration de fonctionnement dans le fichier de configuration de démarrage Copier/enregistrer la configuration, à la page 29.
- **Source** : sélectionnez le nom du fichier source dans la liste déroulante.
- **Destination** : sélectionnez le nom du fichier de destination dans la liste déroulante.
- **Désactiver le clignotement de l'icône d'enregistrement** : cliquez sur cette option pour désactiver le clignotement de l'icône.

Copier/enregistrer la configuration

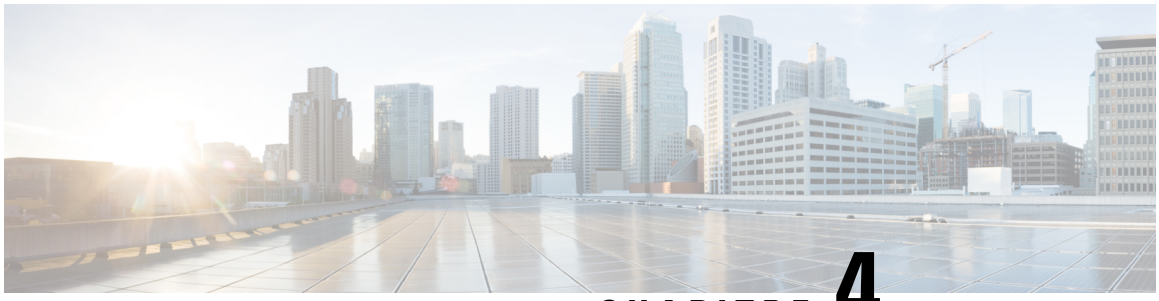
Toutes les configurations actuellement utilisées par le routeur sont contenues dans le fichier de configuration de fonctionnement. Ce fichier est volatile et il n'est pas conservé lors de redémarrages successifs. Pour conserver la configuration entre les redémarrages, copiez le fichier de configuration de fonctionnement dans le fichier de configuration de démarrage une fois toutes les modifications effectuées.

Pour copier le fichier de configuration de fonctionnement, procédez comme suit :

Étape 1 Dans la section Copier/enregistrer la configuration, sélectionnez la source dans la liste déroulante.

Étape 2 Dans la section Destination, sélectionnez l'emplacement de copie du fichier de configuration dans la liste déroulante.

Étape 3 Cliquez sur **Appliquer**.



CHAPITRE 4

Configuration du système

Cette section décrit la configuration système de l'appareil. Elle comprend les rubriques suivantes :

Configuration initiale du routeur

Vous pouvez vérifier la connexion et configurer les paramètres de base du routeur sur la page Assistant de configuration initiale. Suivez les instructions de la page **Exécuter l'Assistant de configuration** pour connaître la procédure de configuration du périphérique.

Étape 1 Cliquez sur **Configuration système> Configuration initiale du routeur** pour accéder à l'Assistant de configuration du routeur.

Étape 2 Cliquez sur **Suivant** pour passer à la page Vérification de la connexion. Si votre routeur a détecté une connexion, les détails de la connexion s'affichent sur cette page.

Étape 3 Cliquez sur **Suivant**.

Étape 4 La fenêtre contextuelle **Configurer le routeur – Sélectionner le type de connexion** s'affiche. Sélectionnez votre type de connexion Internet.

Étape 5 Si vous sélectionnez **IP dynamique** ou **DHCP** (recommandé), cliquez sur **Suivant**.

Étape 6 Si vous sélectionnez **Adresse IP statique**, cliquez sur **Suivant** et configurez les paramètres ci-dessous.

Adresse IP statique	Une adresse IP statique est un numéro (sous forme de notation décimale à points) qu'un fournisseur d'accès à Internet (FAI) attribue à un ordinateur en tant qu'adresse permanente sur Internet. Saisissez l'adresse IP statique.
Masque de sous-réseau	Masque utilisé pour déterminer le sous-réseau auquel appartient une adresse IP. Saisissez le masque de sous-réseau.
IP de passerelle	Interface de routeur connectée à un réseau local qui envoie des paquets. Saisissez l'adresse IP de la passerelle.
DNS	Un serveur DNS est un ordinateur permettant de résoudre les noms d'hôte en adresses IP. Saisissez l'adresse IP du DNS.
DNS secondaire (facultatif)	Saisissez l'adresse IP du serveur DNS secondaire.

Étape 7 Si vous sélectionnez **PPPoE**, cliquez sur **Suivant** et configurez les paramètres ci-dessous.

Nom de compte	Saisissez le nom du compte.
Mot de passe	Saisissez le mot de passe.
Confirmer le mot de passe	Confirmez le mot de passe.

Étape 8 Si vous sélectionnez **PPTP** ou **L2TP**, cliquez sur **Suivant** et configurez les paramètres ci-dessous.

Nom de compte	Saisissez le nom du compte.
Mot de passe	Saisissez le mot de passe.
Confirmer le mot de passe	Confirmez le mot de passe.
Adresse IP statique	Saisissez l'adresse IP statique.
Masque de sous-réseau	Saisissez le masque de sous-réseau.
IP de passerelle	Saisissez l'adresse IP de la passerelle.
DNS	Saisissez le DNS.

Étape 9 Sélectionnez le fuseau horaire du routeur dans le menu déroulant Fuseau horaire.

Étape 10 Sélectionnez l'une des options suivantes :

- **Activer la synchronisation du protocole de temps réseau (NTP)** pour configurer automatiquement la date et l'heure.
- **Définir la date et l'heure manuellement** pour configurer manuellement la date et l'heure ou les importer depuis votre ordinateur.

Étape 11 Cliquez sur **Suivant**.

Étape 12 Dans la section Choisir une adresse MAC, sélectionnez l'une des options suivantes :

- Utiliser l'adresse par défaut (recommandé)
- Utiliser l'adresse de cet ordinateur
- Utiliser cette adresse : saisissez une adresse MAC.

Étape 13 Cliquez sur **Suivant**.

Étape 14 Passez en revue les paramètres et cliquez sur **Suivant**.

Étape 15 Dans la section Activer la sécurité – Définir le mot de passe du routeur, saisissez le mot de passe du routeur, puis confirmez-le. Vous pouvez cocher la case Désactiver l'application de longueur du mot de passe pour désactiver cette option.

Étape 16 Cliquez sur **Suivant**, puis dans le champ Nom du réseau, saisissez le nom à attribuer au réseau.

Étape 17 Cliquez sur **Suivant**, puis dans la section Activer la sécurité – Sécuriser votre réseau sans fil, sélectionnez le type de sécurité du réseau parmi les options suivantes :

- **Sécurité optimale (WPA2 Personnel – AES)**
  - Recommandé pour les nouveaux ordinateurs et appareils sans fil. Les appareils sans fil plus anciens risquent de ne pas prendre en charge cette option. Saisissez une clé de sécurité de 8 à 63 caractères ou 64 chiffres hexadécimaux, ou utilisez la clé aléatoire proposée lorsque vous sélectionnez cette option.
- **Aucune sécurité (déconseillé)**
  - Aucun paramètre de sécurité supplémentaire n'est nécessaire. Ce mode signifie que toutes les données transférées de et vers l'appareil ne sont pas chiffrées.

Étape 18 Cliquez sur **Enregistrer les paramètres de sécurité** pour enregistrer les paramètres de sécurité.

Étape 19 Cliquez sur **Imprimer les paramètres de sécurité** pour imprimer une copie des paramètres de sécurité du routeur.

Étape 20 Cliquez sur **Appliquer**.

Système

Attribuez un nom d'hôte et un nom de domaine pour vous assurer que votre appareil est facilement identifiable par d'autres appareils.

Étape 1 Cliquez sur **Configuration système > Système**.

Étape 2 Dans le champ Nom d'hôte, saisissez un nom pour identifier l'appareil de façon unique sur le réseau. Par exemple, Routeur001.

Étape 3 Dans le champ Nom de domaine, indiquez le domaine dans lequel se trouve l'appareil. Par exemple, exemple.com. Si vous ne connaissez pas le nom du domaine de votre entreprise, contactez votre administrateur réseau.

Étape 4 Cliquez sur **Appliquer** pour appliquer vos modifications.

Heure

Il est essentiel de configurer l'heure sur un périphérique réseau afin d'horodater chaque journal système et message d'erreur de façon à contrôler et à synchroniser le transfert de données avec d'autres périphériques réseau.

Vous pouvez configurer le fuseau horaire, indiquer s'il faut ou non prendre en compte l'heure d'été et sélectionner le serveur NTP (Network Time Protocol) avec lequel synchroniser la date et l'heure.

Pour configurer l'heure et les paramètres du serveur NTP, procédez de la façon suivante :

Étape 1 Cliquez sur **Configuration système > Heure**.

Étape 2 Fuseau horaire : sélectionnez votre fuseau horaire par rapport au temps universel coordonné (UTC).

Étape 3 Définir la date et l'heure : sélectionnez **Auto** ou **Manuel**.

a) Pour Manuel : saisissez la date et l'heure.

Étape 4 Dans la section Serveur NTP : cochez la case **Par défaut** ou **Défini par l'utilisateur**, puis saisissez un nom de serveur NTP qualifié dans les champs Serveur NTP 1 à 4.

Étape 5 Heure d'été : cochez cette case pour activer l'heure d'été. Vous pouvez sélectionner le mode Heure d'été (**Par date** ou **Récurrent**) et saisir les dates de début et de fin. Vous pouvez également spécifier le Décalage dû à l'heure d'été, en minutes.

Étape 6 Cliquez sur **Appliquer**.

Journal

L'un des paramètres de base d'un périphérique réseau est son journal système (Syslog), qui permet de consigner les données propres au périphérique. Vous pouvez définir les instances que doit générer un journal. Dès qu'une instance définie se produit, un journal indiquant l'heure et l'événement est généré, puis transmis à un Syslog Server ou envoyé par e-mail. Il est ainsi possible d'utiliser le journal système pour analyser et dépanner un réseau, mais aussi pour augmenter sa sécurité.

Configuration des paramètres de journal

Pour configurer les paramètres de journal, procédez de la façon suivante :

Étape 1 Cliquez sur **Configuration système > Journal**.

Étape 2 Sous **Paramètre de journal**, cochez la case **Activer** dans la section Journal.

Étape 3 Dans le champ **Tampon du journal**, indiquez le nombre de Ko (plage : 1 Ko à 4 096 Ko, valeur par défaut : 1 024 Ko).

Étape 4 **Gravité** : sélectionnez le niveau de sécurité du journal approprié dans la liste déroulante. Ces niveaux sont classés du plus élevé au plus faible.

Urgence	Niveau 0, qui indique que le système est inutilisable.
Alerte	Niveau 1, qui indique qu'une action immédiate est nécessaire.
Critique	Niveau 2, qui indique que le système se trouve dans un état critique.
Erreur	Niveau 3, qui indique une erreur sur le routeur, notamment qu'un port unique est hors connexion.
Avertissement	Niveau 4, qui indique qu'un message d'avertissement est consigné lorsque le routeur fonctionne correctement, mais qu'un problème opérationnel est survenu.

Notification	Niveau 5, qui indique une condition normale, mais significative. Une notification est consignée lorsque le routeur fonctionne correctement, mais qu'une remarque système a été générée.
Informations	Niveau 6, qui indique une condition qui n'est pas une condition d'erreur, mais nécessite une gestion spéciale.
Débogage	Niveau 7, qui indique que les messages de débogage contiennent des informations à utiliser uniquement lors du débogage d'un programme.

Étape 5 **Catégorie** : sélectionnez **Toutes** les catégories ou certaines catégories d'événement requises que vous souhaitez consigner sur le routeur.

Noyau	Journaux impliquant le code du noyau.
Système	Journaux liés au système.
Pare-feu	Journaux liés aux règles de pare-feu, attaques et filtrage de contenu.
Réseau	Journaux liés au réseau.
VPN	Journaux liés au réseau VPN.
OpenVPN	Journaux liés à OpenVPN, y compris aux instances telles que l'échec de l'établissement du tunnel VPN, l'échec de la passerelle VPN, etc.
Filtrage Web	Journaux liés au filtrage Web.
Utilisateurs	Journaux liés aux utilisateurs du périphérique.
Sans fil RV160W	Journaux liés au réseau sans fil.
PnP	Journaux liés au PnP.

Étape 6 Dans **Enregistrer sur USB automatiquement**, cochez la case **Activer** pour enregistrer les journaux automatiquement.

Serveur de messagerie

Il est possible de configurer le serveur de messagerie sur votre compte de messagerie. Les journaux du serveur de messagerie sont envoyés régulièrement à l'adresse e-mail spécifiée afin que l'administrateur soit toujours à jour sur le réseau. Le routeur prend en charge la configuration d'un compte de messagerie SMTP, notamment les adresses e-mail, le mot de passe, l'algorithme Message-Digest, ainsi que des paramètres facultatifs tels que le numéro de port du serveur SMTP, SSL, TLS, etc.

Étape 1 Dans la section **Syslogs de messagerie**, cochez la case **Activer** pour activer les syslogs de messagerie.

Étape 2 Dans la section **Paramètres de messagerie**, cliquez sur **Lien vers la page de configuration de la messagerie** pour configurer les paramètres de votre messagerie.

Étape 3 Dans la section **Objet du courrier électronique**, saisissez l'objet.

Étape 4 Dans la section **Gravité**, sélectionnez le niveau de gravité dans la liste déroulante.

Étape 5 Dans la section **Consigner la longueur des files d'attente**, indiquez une valeur comprise entre 1 et 1000. La valeur par défaut est 50.

Étape 6 Dans la section **Consigner le seuil de temps**, sélectionnez le seuil de temps dans la liste déroulante.

Étape 7 Dans la section **Alertes électroniques en temps réel**, sélectionnez la totalité ou une partie des catégories d'alertes électroniques que vous souhaitez consigner sur le périphérique.

Étape 8 Cliquez sur **Appliquer**.

Syslog Servers distants

Un Syslog Server distant permet d'envoyer des messages d'événement à un serveur de journalisation. Il est possible de configurer les Syslog Servers en spécifiant le nom ou l'adresse IP.

Étape 1 Dans la section **Syslog Servers**, cochez la case **Activer** pour activer le Syslog Server.

Étape 2 Dans le champ **Syslog Server 1**, saisissez l'adresse IP d'un Syslog Server auquel envoyer les messages de journaux.

Étape 3 Dans le champ **Syslog Server 2**, saisissez l'adresse IP d'un Syslog Server auquel envoyer les messages de journaux.

Étape 4 Cliquez sur **Appliquer**.

E-mail

Vous pouvez configurer le serveur de messagerie de votre périphérique en fonction de vos besoins.

Configuration du serveur de messagerie

Pour configurer le serveur de messagerie, procédez de la façon suivante :

Étape 1 Sélectionnez **Configuration système > E-mail**.

Étape 2 Sous **Serveur de messagerie**, définissez les paramètres suivants :

Serveur SMTP	Saisissez l'adresse du serveur SMTP.
Port SMTP	Saisissez le port SMTP.
Cryptage de l'e-mail	Sélectionnez **Aucun** ou **TLS/SSL** comme méthode de cryptage.
Authentification	Sélectionnez le type d'authentification dans la liste déroulante : **Aucun, Texte en clair, MD5** ou **Connexion**.
Nom d'utilisateur	Saisissez un nom d'utilisateur.
Mot de passe	Saisissez un mot de passe.
Envoyer l'e-mail à 1	Saisissez l'adresse e-mail du destinataire.
Envoyer l'e-mail à 2	Saisissez l'adresse e-mail (facultative) du destinataire.

Adresse e-mail de l'expéditeur	Saisissez l'adresse e-mail de l'expéditeur.

Étape 3 Cliquez sur **Appliquer et tester la connectivité au serveur de messagerie** pour tester la connectivité.

Étape 4 Cliquez sur **Effacer** pour effacer les paramètres de messagerie actuels.

Étape 5 Cliquez sur **Appliquer**.

Comptes d'utilisateur

Vous pouvez créer, modifier et supprimer les utilisateurs locaux et les authentifier à l'aide de la base de données locale pour différents services tels que PPTP, le client VPN et la connexion à l'interface Web graphique (GUI). Les administrateurs sont ainsi en mesure de contrôler et d'autoriser uniquement les utilisateurs locaux à accéder au réseau. Vous pouvez en outre configurer le délai d'expiration de la session de connexion Web.

Pour cela, sélectionnez **Configuration système > Comptes d'utilisateur** et définissez les paramètres suivants dans la section Délai d'expiration de la session de connexion Web :

Délai d'expiration d'inactivité d'administrateur	Définissez le nombre de minutes du délai d'expiration d'inactivité. (Plage : 0 à 1 440, 0 indiquant que le délai n'expire jamais.)
Délai d'expiration d'inactivité d'invité	Définissez le nombre de minutes du délai d'expiration d'inactivité d'invité. (Plage : 0 à 1 440, 0 indiquant que le délai n'expire jamais.)
Délai d'expiration d'inactivité de l'ambassadeur de lobby	Définissez le nombre de minutes du délai d'expiration d'inactivité de l'ambassadeur de lobby. (Plage : 0 à 1 440, 0 indiquant que le délai n'expire jamais.)

Dans la section Complexité des mots de passe de l'utilisateur local, pour créer des utilisateurs locaux et déterminer la complexité des mots de passe, procédez comme suit :

Étape 1 Cliquez sur **Configuration système > Comptes d'utilisateur**.

Étape 2 Dans la section Paramètres de complexité des mots de passe, cochez la case **Activé** et définissez les paramètres suivants :

Longueur minimale du mot de passe	Saisissez la longueur minimale du mot de passe pour créer un nouveau mot de passe. La plage est comprise entre 0 et 64 et la valeur par défaut est 8.
Nombre minimum de classes de caractères	Saisissez le nombre minimum de caractères à utiliser lors de la création du nouveau mot de passe. La plage est comprise entre 0 et 4 et la valeur par défaut est 3. Les quatre classes de caractères sont les suivantes : majuscules, minuscules, chiffres et caractères spéciaux.
Le nouveau mot de passe doit être différent du mot de passe actuel	Cochez cette case pour demander à l'utilisateur de saisir un mot de passe différent lors de l'expiration du mot de passe actuel.
Délai d'expiration du mot de passe	Saisissez le nombre de jours avant l'expiration du mot de passe. (Plage : 0 à 365, 0 indiquant que le mot de passe n'expire jamais.)

Étape 3 Pour ajouter un utilisateur au routeur, cliquez sur **Ajouter** sous Utilisateurs locaux, puis définissez les paramètres suivants sur la page Ajouter/modifier le compte d'utilisateur :

Nom d'utilisateur	Saisissez un nom d'utilisateur.
Nouveau mot de passe	Saisissez un mot de passe.
Confirmer le mot de passe	Confirmez le mot de passe.
Groupe	Sélectionnez le groupe dans la liste déroulante. • **Administrateur** : un utilisateur administrateur dispose d'un accès en lecture et en écriture au gestionnaire de périphériques, et peut modifier les données de configuration. • **Invité** : un utilisateur invité dispose d'un accès en lecture au gestionnaire de périphériques.

Étape 4 Cliquez sur **Appliquer**.

Service d'authentification à distance

Le service d'authentification à distance est un système client-serveur distribué qui protège les réseaux contre tout accès non autorisé. Dans la mise en œuvre Cisco, les clients RADIUS s'exécutent sur des routeurs Cisco et envoient des demandes d'authentification à un serveur RADIUS central contenant toutes les informations sur l'authentification des utilisateurs et l'accès aux services réseau. Le serveur de sécurité RADIUS est identifié sur la base de son nom d'hôte ou adresse IP, du nom d'hôte et de numéros de port UDP spécifiques, ou de l'adresse IP et de numéros de port UDP spécifiques.

Pour activer l'authentification des utilisateurs externes à l'aide de RADIUS et LDAP, utilisez le service d'authentification à distance et sélectionnez Groupe par défaut dans la liste déroulante. Configurez ensuite les paramètres suivants :

Étape 1 Sous la **table des services d'authentification à distance**, cliquez sur **Ajouter** et configurez les paramètres suivants dans la fenêtre contextuelle Ajouter/modifier le domaine :

Nom	Donnez un nom au domaine.
Type d'authentification	Sélectionnez un type d'authentification dans la liste déroulante. • **LDAP** : protocole LDAP (Lightweight Directory Access Protocol). • **RADIUS** : protocole de mise en réseau qui fournit un service AAA (authentification, autorisation et comptabilité) centralisé aux utilisateurs qui utilisent et se connectent à un service réseau. • **Active Directory** : service d'annuaire Windows qui permet d'utiliser les ressources réseau interconnectées, complexes et différentes de manière unifiée.

Serveur principal	Saisissez l'adresse IP du serveur principal.
Port	Saisissez le port de secours du serveur.
Nom de domaine de base	Saisissez le nom de domaine de base pour lancer la recherche.

Étape 2 Cliquez sur **Appliquer** pour enregistrer les paramètres. Cliquez sur **Modifier** ou sur **Supprimer** pour modifier ou supprimer un domaine existant.

Remarque La priorité de la base de données externe est toujours RADIUS/LDAP/AD/Locale. Si vous ajoutez le serveur RADIUS sur le routeur, le service de connexion Web et d'autres services utilisent la base de données externe RADIUS pour authentifier l'utilisateur. Il est impossible d'activer la base de données externe uniquement pour le service de connexion Web et de configurer une autre base de données pour un autre service. Après avoir créé et activé RADIUS sur le routeur, ce dernier utilise le service RADIUS comme base de données externe pour la connexion Web, le VPN site à site, le VPN PPTP, OpenVPN, le VPN client à site et 802.1x.

Groupes d'utilisateurs

L'administrateur peut créer des groupes d'utilisateurs pour une série d'utilisateurs qui partagent le même ensemble de services. Ces groupes d'utilisateurs peuvent être autorisés à accéder à divers services tels que OpenVPN, VPN PPTP< 802.1x et Portail captif.

Pour créer des groupes d'utilisateurs, procédez comme suit :

Étape 1 Cliquez sur **Configuration système > Groupes d'utilisateurs**.

Étape 2 Sous Groupes d'utilisateurs, cliquez sur **Ajouter** pour créer un nouveau groupe d'utilisateurs.

Étape 3 Dans le champ Nom du groupe, saisissez le nom à attribuer à votre groupe.

Étape 4 Sous Liste d'appartenance de l'utilisateur local, cliquez sur **Ajouter**, puis cochez la case et sélectionnez le groupe d'utilisateurs souhaité auquel ajouter un nouvel utilisateur.

Étape 5 Sous Services, sélectionnez les services auxquels doivent avoir accès les groupes d'utilisateurs et saisissez les informations suivantes.

Connexion Web/NETCONF/RESTCONF	Spécifiez les autorisations de connexion Web accordées aux utilisateurs rattachés au groupe : • **Désactiver** : aucun membre du groupe d'utilisateurs ne peut se connecter à l'utilitaire de configuration à l'aide d'un navigateur Web. • **Lecture seule** : les membres du groupe d'utilisateurs peuvent uniquement lire l'état système après s'être connectés. Ils ne peuvent pas modifier les paramètres. • **Admin** : tous les membres du groupe d'utilisateurs disposent de privilèges complets pour configurer et lire l'état système.
VPN site à site	• Cliquez sur **Ajouter** pour ouvrir la fenêtre **Ajouter une liste de fonctions**. • Sélectionnez un profil dans la liste déroulante et cliquez sur **Ajouter**.

VPN client à site	• Cliquez sur **Ajouter** pour ouvrir la fenêtre **Ajouter une liste de fonctions**. • Sélectionnez un profil dans la liste déroulante et cliquez sur **Ajouter**.
OpenVPN	Cliquez sur **Activer** pour activer la fonction OpenVPN ou sur **Désactiver** pour la désactiver. Sélectionnez un profil dans la liste déroulante.
VPN PPTP	Cliquez sur **Activer** pour activer la fonction PPTP ou sur **Désactiver** pour la désactiver.
802.1x	Cochez la case **Autoriser** pour autoriser l'authentification 802.1x.
Ambassadeur de lobby	Cliquez sur **Activer** pour activer la fonction Ambassadeur de lobby ou sur **Désactiver** pour la désactiver.
Portail captif	Cliquez sur **Ajouter** pour ajouter un nouveau portail captif et configurer le SSID et la bande de fréquences de ce dernier.

Étape 6 Cliquez sur **Appliquer**.

Remarque 802.1x prend uniquement en charge l'authentification RADIUS. PPTP/L2TP prend en charge RADIUS et la base de données locale. Si vous choisissez la base de données locale, seul le protocole d'authentification des mots de passe (PAP) est pris en charge pour l'authentification locale.

Groupes d'adresses IP

Pour configurer et gérer les stratégies de contrôle d'application et le filtrage Web, vous devez configurer des groupes d'adresses IP. Pour configurer les groupes d'adresses IP, procédez de la façon suivante :

Étape 1 Cliquez sur **Configuration système > Groupes d'adresses IP**.

Étape 2 Dans Groupes d'adresses IP, cliquez sur **Ajouter** pour ajouter un groupe, puis saisissez un nom. Pour supprimer un groupe, cliquez sur **Supprimer**.

Étape 3 Cliquez sur **Ajouter**, puis saisissez les informations suivantes.

Type et détails de l'adresse	Sélectionnez le type de groupe dans la liste déroulante et saisissez les détails de l'adresse : • **IP unique** : saisissez une adresse IP dans le champ Détails de l'adresse. • **Sous-réseau de l'adresse IP** : saisissez une adresse IP dans le champ Détails de l'adresse. • **Plage d'adresses IP** : saisissez une adresse IP dans le champ Détails de l'adresse.

Étape 4 Cliquez sur **Appliquer**.

SNMP

Le protocole SNMP (Simple Network Management Protocol) est un protocole Internet permettant de collecter et d'organiser les données sur les appareils gérés connectés aux réseaux IP. Il permet par ailleurs aux administrateurs de gérer, de surveiller et de recevoir des notifications d'événements critiques lorsque ceux-ci se produisent sur le réseau. Cet appareil prend en charge v1, v2c et v3.

Il fait office d'agent SNMP qui répond aux commandes SNMP à partir de systèmes de gestion de réseaux SNMP. Il prend en charge les commandes SNMP standard get/next/set. Il génère également des messages de filtre pour informer le gestionnaire SNMP des conditions d'alarme qui se produisent, par exemple redémarrages, cycles d'alimentation et liaisons WAN.

Étape 1 Pour configurer le protocole SNMP du routeur, saisissez les informations suivantes.

SNMP activé	Cochez cette case pour activer le protocole SNMP.
Autoriser l'accès utilisateur via Internet	Cochez cette case pour autoriser l'utilisateur via Internet.
Autoriser l'accès utilisateur via le VPN	Cochez cette case pour autoriser l'accès utilisateur via le VPN.
Version	Sélectionnez la version dans la liste déroulante.
Nom du système	Saisissez le nom du système.
Contact système	Saisissez le nom du contact système.
Emplacement du système	Saisissez l'emplacement du système.
Obtenir une communauté	Saisissez le nom de la communauté.
Définir une communauté	Saisissez le nom de la communauté.

Configuration de filtre

L'utilisation des configurations de filtre vous permet de définir l'adresse source de chaque paquet de filtres SNMP envoyé par le routeur à une seule adresse, quelle que soit l'interface sortante.

Étape 2 Pour configurer les filtres SNMP, saisissez les informations suivantes.

Communauté de filtre	Saisissez le nom de la communauté de filtre.
Adresse IP du récepteur d'interruptions	Saisissez l'adresse IP.
Port du récepteur d'interruptions	Saisissez le numéro de port.

Étape 3 Cliquez sur **Appliquer**.

Détection Bonjour

Bonjour est un protocole de détection de services qui identifie les périphériques réseau, notamment les ordinateurs et les serveurs, sur votre réseau LAN. Lorsque cette fonction est activée, le routeur diffuse régulièrement des enregistrements du service Bonjour au réseau LAN pour faire connaître son existence.

Remarque Pour détecter des produits Cisco Small Business, Cisco fournit un utilitaire fonctionnant par le biais d'une simple barre d'outils dans le navigateur de l'utilisateur, appelé FindIt. L'utilitaire de détection FindIT détecte les appareils Cisco sur le réseau et fournit des informations de base telles que les numéros de série et les adresses IP. Pour obtenir plus d'informations et télécharger l'utilitaire de détection FindIT, rendez-vous sur www.cisco.com/go/findit.

Pour activer la fonction de détection Bonjour, procédez comme suit :

Étape 1 Sélectionnez **Configuration système > Détection Bonjour**.

Étape 2 Cochez la case **Activer** pour activer globalement la détection Bonjour (cette fonction est activée par défaut).

Étape 3 Sélectionnez **Appliquer**.

LLDP

Le protocole LLDP (Link Layer Discovery Protocol) est un protocole non lié à un fournisseur, qui est utilisé par des appareils réseau pour annoncer leur identité, leurs capacités et leurs voisins sur un réseau local IEEE 802. Les informations LLDP sont envoyées par l'interface du périphérique à intervalles fixes, sous la forme d'une trame Ethernet. Chaque trame contient une unité de données LLDP (LLDPDU). Chaque unité LLDPDU est une série de structures type-longueur-valeur (TLV).

Pour configurer LLDP, procédez de la façon suivante :

Étape 1 Sélectionnez **Configuration système > LLDP**.

Étape 2 Dans la section LLDP, sélectionnez l'option **Activer** (qui est activée par défaut).

Étape 3 Dans la **Table de paramètres de port LLDP**, cochez la case **Activer LLDP** pour activer le protocole LLDP sur une interface.

Étape 4 Cliquez sur **Appliquer**.

Étape 5 La **Table des voisins LLDP** fournit les renseignements suivants :

- **Port local** : identifiant du port.
- **Sous-type de l'ID du châssis** : type d'ID de châssis (adresse MAC, par exemple).
- **ID de châssis** : identifiant du châssis. Si vous avez choisi l'adresse MAC comme sous-type d'ID de châssis, l'adresse MAC du routeur s'affiche.
- **Sous-type de l'ID du port** : type de l'identifiant du port.

- **ID du port** : identifiant du port.
- **Nom du système** : nom du routeur.
- **Durée de vie** : fréquence (en secondes) d'envoi des mises à jour des annonces LLDP.

Étape 6 Cliquez sur **Actualiser** pour actualiser les données.

Mises à jour automatiques

La mise à niveau vers la dernière version du microprogramme peut vous aider à résoudre les erreurs et autres problèmes occasionnels sur le routeur. Il est possible que le routeur soit configuré pour vous envoyer des notifications par e-mail lorsque des mises à jour importantes du microprogramme sont disponibles. Ces informations peuvent être envoyées à des intervalles spécifiques et pour des types spécifiques d'événements réseau. Avant de configurer ces notifications, vous devez configurer le serveur de messagerie.

Pour configurer les mises à jour automatiques, procédez comme suit.

Étape 1 Sélectionnez **Configuration système > Mises à jour automatiques**.

Étape 2 Dans la liste déroulante Intervalle de recherche, sélectionnez la fréquence à laquelle le périphérique doit automatiquement rechercher des mises à jour du microprogramme. Cliquez sur **Rechercher maintenant** pour lancer une recherche.

Étape 3 Dans le champ Notifier par, activez l'option **Interface Admin** ou **Envoyer par e-mail à** et saisissez l'adresse e-mail. Les notifications sont envoyées à l'adresse e-mail configurée. Si vous n'avez pas configuré de serveur de messagerie, cliquez sur le lien dans la note en regard du champ E-mail et configurez le serveur de messagerie.

Étape 4 Sous Mise à jour automatique, vous pouvez sélectionner l'heure à laquelle le microprogramme du système et celui du modem USB sont automatiquement mis à jour. Vous pouvez en outre choisir de recevoir une notification pour chaque mise à jour.

Étape 5 Cliquez sur **Appliquer**.

Horaires

Les périphériques réseau doivent être protégés contre les attaques et virus intentionnels susceptibles de compromettre la confidentialité, ou d'entraîner l'altération des données ou un déni de service. Il est donc possible de planifier des horaires afin d'appliquer les règles de pare-feu ou de redirection de ports certains jours ou à certaines heures de la journée.

Pour configurer les horaires, procédez de la façon suivante :

Étape 1 Sélectionnez **Configuration système > Horaires**.

Étape 2 Dans Horaires, cliquez sur **Ajouter** pour créer un nouvel horaire. Vous pouvez modifier ou supprimer un horaire en le sélectionnant et en cliquant sur **Modifier ou Supprimer**.

Étape 3 Saisissez un nom pour identifier l'horaire dans la colonne Nom.

Étape 4 Saisissez l'heure de début et l'heure de fin souhaitées.

Étape 5 Dans la colonne Jours, cochez la case **Tous les jours** pour appliquer l'horaire tous les jours de la semaine. Désactivez cette option pour appliquer l'horaire certains jours uniquement. Sélectionnez ensuite les jours de la semaine auxquels appliquer l'horaire. Vous pouvez également sélectionner **Jours de la semaine** ou **Week-ends**.

Étape 6 Cliquez sur **Appliquer**.

Gestion des services

La section Gestion des services fournit des renseignements sur la configuration du système. Vous pouvez ajouter une nouvelle entrée à la liste Gestion des services ou modifier une entrée existante. Pour configurer la Gestion des services, procédez de la façon suivante :

Étape 1 Cliquez sur **Configuration système > Gestion des services**.

Étape 2 Dans la Table des services, cliquez sur **Ajouter**.

Étape 3 Dans le champ Nom, saisissez le nom à attribuer à la gestion des services.

Étape 4 Dans le champ Protocole, sélectionnez le protocole de couche 4 utilisé par le service dans la liste déroulante.

Étape 5 Dans le champ Port de début/Type ICMP/Protocole IP, saisissez le numéro de port, le type ICMP ou le protocole IP.

Étape 6 Dans le champ Port de fin/Code CMP, saisissez le numéro de port.

Étape 7 Cliquez sur **Appliquer**.

Étape 8 Pour modifier ou supprimer une entrée, sélectionnez l'entrée et cliquez sur **Modifier ou sur Supprimer**. Apportez les modifications souhaitées, puis cliquez sur **Appliquer**.

PnP (Plug and Play)

L'agent Cisco Open Plug-n-Play est une application logicielle exécutée sur un appareil Cisco SMB. Lors de la mise sous tension d'un appareil, le processus de détection de l'agent Open Plug-n-Play (intégré à l'appareil) tente de détecter l'adresse du serveur Open Plug-n-Play. L'agent Open Plug-n-Play utilise des méthodes telles que DHCP, DNS et la détection des services cloud Cisco pour récupérer l'adresse IP du serveur Open Plug-n-Play. Le processus de déploiement simplifié de l'appareil SMB automatise les tâches opérationnelles liées au déploiement suivantes :

- Établir la connectivité de réseau initiale de l'appareil.
- Fournir la configuration de l'appareil.
- Fournir les images du logiciel et du microprogramme.

Pour activer ou désactiver Plug and Play, procédez comme suit :

Étape 1 Cliquez sur **Configuration système > PnP**.

Étape 2 Dans le champ **PnP**, cochez la case **Activer**.

Étape 3 Dans la section **Transport PnP**, sélectionnez une option dans la liste déroulante.

- **Auto** : la détection du serveur PnP est téléchargée automatiquement par PnP.
- **Statique** : sélectionnez et saisissez l'adresse IP/le nom de domaine complet et le numéro de port, puis sélectionnez le certificat à importer dans la liste déroulante Certificat CA.

Étape 4 Cliquez sur **Appliquer**.

PnP Connect Service

Plug and Play Connect est un service fourni par Cisco qui est le dernier recours utilisé par un périphérique compatible Plug and Play réseau pour découvrir le serveur. Pour utiliser Plug and Play Connect pour la découverte du serveur, vous devez d'abord créer un profil de contrôleur représentant le gestionnaire, puis enregistrer chacun de vos appareils avec le service Plug and Play Connect.

Pour accéder au service Plug and Play Connect, procédez comme suit:

Étape 1 Dans votre navigateur Web, naviguez jusqu'à https://software.cisco.com.

Étape 2 Cliquez sur le bouton se connecter en haut à droite de l'écran. Connectez-vous avec un identifiant cisco.com associé à votre compte Cisco Smart Account.

Étape 3 Sélectionnez le lien **Plug and Play Connect** sous l'en-tête Plug and Play réseau. La page principale du service Plug and Play Connect s'affiche.

Création d'un profil de contrôleur

Pour créer un profil de contrôleur, procédez comme suit:

Étape 1 Ouvrez la page Web Plug and Play Connect https://software.cisco.com/#module/pnp dans votre navigateur. Si nécessaire, sélectionnez le compte virtuel correct à utiliser.

Étape 2 Sélectionnez le lien profils de contrôleurs, puis cliquez sur Ajouter un profil.

Étape 3 Sélectionnez un type de contrôleur de serveur PNP dans la liste déroulante. Puis cliquez sur **suivant**.

Étape 4 Spécifiez un nom, et éventuellement une description pour le profil.

Étape 5 Sous l'en-tête du contrôleur principal, utilisez la liste déroulante fournie pour sélectionner s'il faut spécifier le serveur par nom ou adresse IP. Renseignez le nom ou les adresses du serveur dans les champs fournis.

Étape 6 Sélectionnez le protocole à utiliser lors de la communication avec le serveur. Il est vivement recommandé d'utiliser le protocole HTTPS pour assurer l'intégrité du processus de provisionnement.

Étape 7 Si le protocole sélectionné est HTTPS et que le serveur est configuré avec un certificat auto-signé (par défaut) ou qu'il n'est pas signé par une autorité de certification connue, le certificat utilisé par le serveur doit être téléchargé à l'aide des contrôles fournis.

Étape 8 Cliquez sur suivant, puis examinez les paramètres avant de cliquer sur **Envoyer**.

Enregistrement des périphériques

Certains produits achetés directement auprès de Cisco peuvent être associés à votre compte Smart Cisco au moment de l'achat, et ceux-ci seront automatiquement ajoutés à Plug and Play Connect. Cependant, la majorité des produits compatibles Plug and Play de Cisco 100 de la série 500 devront être enregistrés manuellement. Pour enregistrer les périphériques avec Plug and Play Connect, procédez comme suit:

Étape 1 Ouvrez la page Web Plug-and-Play Connect https://software.cisco.com/#module/pnp dans votre navigateur. Si nécessaire, sélectionnez le compte virtuel correct à utiliser.

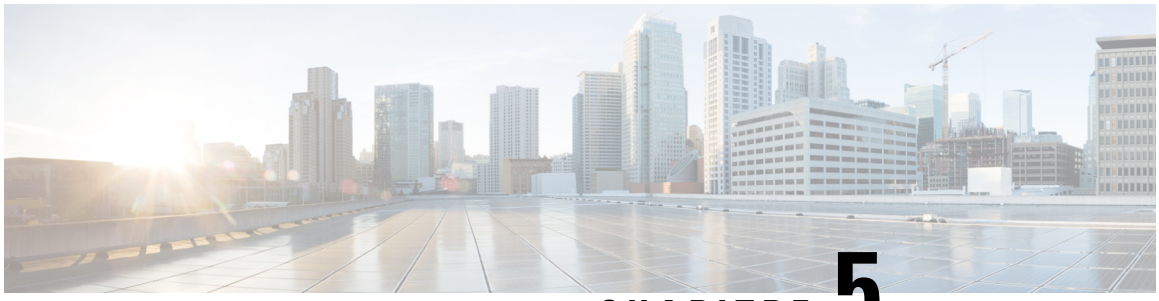
Étape 2 Sélectionnez le lien périphériques, puis cliquez sur Ajouter des périphériques. Vous devrez peut-être être approuvé pour ajouter manuellement des périphériques à votre compte. Il s'agit d'un processus unique et, si nécessaire, vous serez avisé par courriel une fois que l'approbation aura été accordée.

Étape 3 Choisissez d'ajouter des périphériques manuellement ou d'ajouter plusieurs périphériques en téléchargeant les détails au format CSV. Cliquez sur le lien fourni pour télécharger un exemple de fichier CSV. Si vous choisissez de télécharger un fichier CSV, cliquez sur le bouton Parcourir pour sélectionner le fichier. Puis cliquez sur suivant.

Étape 4 Si vous avez sélectionné pour ajouter des périphériques manuellement, cliquez sur identifier le périphérique. Spécifiez le numéro de série et l'ID de produit pour l'appareil à ajouter. Sélectionnez un profil de contrôleur dans la liste déroulante. Entrez éventuellement une description pour cet appareil.

Étape 5 Répétez l'étape 4 jusqu'à ce que vous ayez ajouté tous vos appareils, puis cliquez sur suivant.

Étape 6 Examinez les périphériques que vous avez ajoutés, puis cliquez sur Envoyer.



CHAPITRE 5

Réseau WAN

Un réseau étendu (WAN) est un ensemble de réseaux de télécommunications ou de réseaux informatiques distribués géographiquement. Ce terme fait la distinction entre un réseau local (LAN) et une structure de télécommunication plus vaste. Privé ou disponible en location, un réseau étendu permet à une entreprise d'exécuter efficacement ses tâches quotidiennes, quel que soit son emplacement.

Cette section décrit les fonctions WAN de l'appareil. Elle comprend les rubriques suivantes :

Paramètres WAN

Vous pouvez configurer deux interfaces physiques WAN et VLAN sur le routeur. Pour configurer les paramètres WAN, procédez de la façon suivante :

Étape 1 Sélectionnez **WAN > Paramètres WAN**.

Étape 2 Cliquez sur les onglets libellés et configurez les paramètres IPv4, IPv6 ou les Paramètres avancés.

Étape 3 Pour une connexion IPv4, cliquez sur l'onglet **IPv4** ; pour une connexion IPv6, cliquez sur **IPv6** et sélectionnez le type de connexion.

Étape 4 Si IPv4 ou IPv6 utilise DHCP pour la connexion, configurez les paramètres suivants :

Serveur DNS	Sélectionnez **Utiliser le serveur DNS fourni via DHCP** ou **Utiliser les valeurs DNS suivantes**.
DNS statique 1 et 2	Saisissez l'adresse IP du serveur DNS statique principal et du serveur DNS statique secondaire dans les champs correspondants.
DHCP-PD (IPv6 uniquement)	Sélectionnez cette option pour l'activer et saisissez un nom de préfixe.

Si IPv4 ou IPv6 utilise l'adresse IP statique pour la connexion, configurez les paramètres suivants :

Adresse IP	Saisissez l'adresse IP.
Masque de réseau	Saisissez l'adresse du masque de réseau.

Passerelle par défaut	Saisissez l'adresse IP de la passerelle par défaut. La passerelle par défaut est nécessaire sur cette interface pour participer à l'équilibrage de charge et au basculement (Multi-WAN).
DNS statique 1 et 2	Saisissez l'adresse IP du serveur DNS statique principal et du serveur DNS statique secondaire dans les champs correspondants.

Si IPv4 ou IPv6 utilise PPPoE pour la connexion, configurez les paramètres suivants :

Nom d'utilisateur	Nom d'utilisateur que votre FAI vous a attribué.
Mot de passe	Mot de passe que votre FAI vous a attribué.
Afficher le mot de passe	Cochez cette case pour afficher le mot de passe.
Serveur DNS	Sélectionnez **Utiliser le serveur DNS fourni via PPPoE** ou **Utiliser DNS**.
DNS statique 1 et 2	Saisissez l'adresse IP du serveur DNS statique principal et du serveur DNS statique secondaire dans les champs correspondants.
Connexion à la demande	Sélectionnez **Connexion à la demande** si votre FAI vous facture chaque connexion. Saisissez la période d'inactivité maximale, en secondes, avant la fin de la connexion suite à une période d'inactivité. La valeur par défaut est de 5 minutes.
Maintenir actif	Sélectionnez **Maintenir actif** pour vérifier régulièrement la connexion et la rétablir lorsque celle-ci est indisponible.
Type d'authentification	Sélectionnez le type d'authentification dans la liste déroulante (**Négociation auto, PAP, CHAP, MS-CHAP, MS-CHAPv2**).
Nom du service	Saisissez le nom du service.

Remarque Certains fournisseurs d'accès n'autorisent pas l'envoi de requêtes Ping sur la passerelle par défaut, notamment pour la connexion PPPoE. Accédez à la page Multi-WAN pour désactiver la fonction « Détection de services réseau » ou sélectionnez un hôte valide pour la détection. Dans le cas contraire, le trafic ne sera pas redirigé par le périphérique.

Si IPv4 utilise PPTP pour la connexion, configurez les paramètres suivants :

Affectation des adresses IP	Pour DCHP, sélectionnez cette option afin que DHCP fournisse une adresse IP. Pour IP statique, sélectionnez cette option et fournissez une adresse IP, un masque de réseau et l'adresse IP de la passerelle par défaut.
Adresse IP/Nom de domaine complet du serveur PPTP	Saisissez le nom du serveur.
Nom d'utilisateur	Nom d'utilisateur que votre FAI vous a attribué.
Mot de passe	Mot de passe que votre FAI vous a attribué.
Afficher le mot de passe	Cochez cette case pour afficher le mot de passe.
Serveur DNS	Sélectionnez **Utiliser le serveur DNS fourni via PPTP** ou **Utiliser DNS**.
DNS statique 1 et 2	Saisissez l'adresse IP du serveur DNS statique principal et du serveur DNS statique secondaire dans les champs correspondants.

Connexion à la demande	Sélectionnez **Connexion à la demande** si votre FAI vous facture chaque connexion. Saisissez la période d'inactivité maximale, en secondes, avant la fin de la connexion suite à une période d'inactivité. La valeur par défaut est de 5 minutes.
Maintenir actif	Sélectionnez **Maintenir actif** pour vérifier régulièrement la connexion et la rétablir lorsque celle-ci est indisponible.
Type d'authentification	Sélectionnez le type d'authentification dans la liste déroulante (**Négociation auto, PAP, CHAP, MS-CHAP, MS-CHAPv2**).
Cryptage MPPE	Cochez cette case pour activer le cryptage MPPE.

Si IPv4 utilise L2TP pour la connexion, configurez les paramètres suivants :

Affectation des adresses IP	Pour DCHP, sélectionnez cette option afin que DHCP fournisse une adresse IP. Pour IP statique, sélectionnez cette option et fournissez une adresse IP, un masque de réseau et l'adresse IP de la passerelle par défaut.
Adresse IP/Nom de domaine complet du serveur L2PT	Saisissez le nom du serveur.
Nom d'utilisateur	Nom d'utilisateur que votre FAI vous a attribué.
Mot de passe	Mot de passe que votre FAI vous a attribué.
Afficher le mot de passe	Cochez cette case pour afficher le mot de passe.
Serveur DNS	Sélectionnez **Utiliser le serveur DNS fourni via L2TP** ou **Utiliser DNS**.
DNS statique 1 et 2	Saisissez l'adresse IP du serveur DNS statique principal et du serveur DNS statique secondaire dans les champs correspondants.
Connexion à la demande	Sélectionnez **Connexion à la demande** si votre FAI vous facture chaque connexion. Saisissez la période d'inactivité maximale, en secondes, avant la fin de la connexion suite à une période d'inactivité. La valeur par défaut est de 5 minutes.
Maintenir actif	Sélectionnez **Maintenir actif** pour vérifier régulièrement la connexion et la rétablir lorsque celle-ci est indisponible.
Type d'authentification	Sélectionnez le type d'authentification dans la liste déroulante (**Négociation auto, PAP, CHAP, MS-CHAP, MS-CHAPv2**).

Si IPv6 utilise SLAAC pour la connexion

Dans la section Paramètres SLAAC, saisissez les informations suivantes :

DNS statique 1 et 2	Saisissez l'adresse IP du serveur DNS statique principal et du serveur DNS statique secondaire.
DHCP-PD (IPv6 uniquement)	Sélectionnez cette option pour l'activer et saisissez un nom de préfixe.

Étape 5 Cliquez sur **Appliquer**.

Pour les paramètres avancés

Étape 6 Cliquez sur l'onglet Paramètres avancés et configurez les paramètres suivants :

Balise VLAN WAN	Cochez cette option pour activer la balise VLAN WAN.
ID de VLAN	Saisissez l'ID du VLAN
Unité maximale de transmission (MTU)	Sélectionnez **Auto** pour définir la taille automatiquement. Pour définir manuellement la taille de la MTU, sélectionnez **Manuel** et saisissez la taille de la MTU. (Taille en octets de la plus grande unité de données de protocole que la couche peut transmettre.)
Clone de l'adresse MAC	Cochez la case **Clone d'adresse MAC** et saisissez l'adresse MAC. Cliquez sur **Cloner MAC du PC** pour utiliser l'adresse MAC de votre ordinateur comme adresse MAC clone du périphérique.

Remarque Lorsque vous activez l'option Clone d'adresse MAC, la mise en miroir des ports ne fonctionne pas.

Étape 7 Cliquez sur **Appliquer**.

DNS dynamique

DDNS (Dynamic Domain Name System) est une méthode permettant de maintenir la liaison entre un nom de domaine et une adresse IP changeante, dans la mesure où les ordinateurs n'utilisent pas tous des adresses IP statiques. Le DNS dynamique met automatiquement à jour un serveur dans le DNS avec la configuration active de ses noms d'hôte, adresses ou autres informations. DDNS permet d'attribuer un nom de domaine fixe à une adresse IP WAN dynamique.

Pour configurer les stratégies DNS dynamiques, procédez de la façon suivante :

Étape 1 Sélectionnez **WAN > DNS dynamique**.

Étape 2 Dans la Table de DNS dynamique, sélectionnez l'interface à ajouter à la stratégie DNS dynamique.

Étape 3 Cliquez sur **Modifier**.

Étape 4 Cochez la case **Activer cette stratégie DNS dynamique** pour activer la configuration de la stratégie.

Étape 5 Sélectionnez le nom du fournisseur d'accès dans la liste déroulante Fournisseur.

Étape 6 Saisissez le **Nom d'utilisateur** et le **Mot de passe** du compte DDNS. Pour afficher le mot de passe, cochez la case **Activer** en regard du champ Afficher le mot de passe.

Étape 7 Saisissez le nom complet du périphérique, y compris le nom de domaine dans le champ Nom de domaine complet.

Étape 8 Cochez la case **Activer** pour recevoir des mises à jour concernant le fournisseur de DNS dynamique, puis sélectionnez la périodicité.

Étape 9 Cliquez sur **Appliquer**.

Transition IPv6

Pour migrer d'IPv4 vers IPv6, vous pouvez utiliser un mécanisme de transition Internet appelé 6in4. 6in4 utilise le tunneling pour encapsuler le trafic IPv6 sur les liaisons IPv4 configurées. Le trafic 6in4 est envoyé sur la liaison IPv4, qui contient l'en-tête du paquet IPv4, suivi par le paquet IPv6 dont les en-têtes IP adoptent le protocole IP 41.

Pour configurer la transition IPv6, procédez de la façon suivante :

Étape 1 Sélectionnez **WAN > Transition IPv6**.

Étape 2 Cochez la case **Activer** pour activer l'interface du tunnel.

Étape 3 Saisissez une description.

Étape 4 L'interface locale et l'adresse IPv4 locale affichent l'interface sélectionnée.

Étape 5 Cliquez sur **Appliquer**.

Tunnel IPv6 en IPv4 (6in4)

Pour ajouter le tunnel IPv4 (6in4), saisissez les informations suivantes :

Étape 1 Cliquez sur l'onglet **Tunnel IPv6 en IPv4 (6in4)**.

Étape 2 Saisissez l'adresse IPv4 distante.

Étape 3 Saisissez l'adresse IPv6 locale et la longueur.

Étape 4 Saisissez l'adresse IPv6 distante et la longueur.

Étape 5 Cliquez sur **Appliquer**.

Déploiement IPv6 rapide (6rd)

Dans la section Déploiement IPv6 rapide (6rd), chaque FAI utilise l'un de ses propres préfixes IPv6 plutôt que le préfixe spécial 2002::/16 normalisé pour 6to4. Un fournisseur garantit ainsi la disponibilité de ses hôtes 6rd à partir de tous les hôtes IPv6 natifs pouvant joindre leur réseau IPv6.

Étape 1 Cochez la case **Déploiement IPv6 rapide (6rd)**, puis définissez les paramètres suivants.

Étape 2 Dans la section Mode de communication, cliquez sur **Automatiquement depuis DHCP** pour utiliser DHCP (option 212) en vue d'obtenir le préfixe 6rd, l'adresse IPv4 du relais et la longueur du masque IPv4.

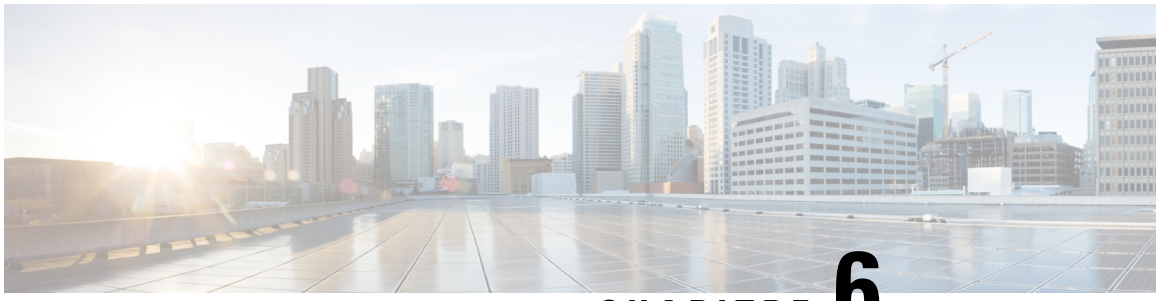
Étape 3 Vous pouvez également sélectionner **Manuel** et définir les paramètres 6rd suivants.

a) Saisissez l'adresse IPv4 du relais.

b) Saisissez la longueur du préfixe commun IPv4.

c) Saisissez la longueur du préfixe IPv6. Le réseau IPv6 (sous-réseau) est identifié par le préfixe. Tous les hôtes sur le réseau possèdent des bits initiaux identiques pour leurs adresses IPv6. Saisissez le nombre de bits initiaux communs dans les adresses réseau. La valeur par défaut est 64.

Étape 4 Cliquez sur **Appliquer**.



CHAPITRE 6

Réseau local

Un réseau local (LAN) est un réseau informatique couvrant une zone relativement restreinte, telle qu'un immeuble de bureaux, une école ou un logement. Les réseaux locaux se caractérisent par leur topologie, leurs protocoles et leurs appareils. La topologie correspond à la disposition géométrique des appareils dans un réseau. Les protocoles sont des règles et des spécifications de codage pour l'envoi de données. Ils déterminent par ailleurs si le réseau utilise une architecture P2P ou client/serveur. Le type de réseau LAN le plus courant est le réseau Ethernet.

Cette section décrit les fonctions LAN du périphérique. Elle comprend les rubriques suivantes :

Paramètres des ports

La page Paramètres des ports affiche les ports pour la technologie EEE, le contrôle de flux, le mode, la mise en miroir des ports, les trames Jumbo et l'agrégation de liaisons.

Pour configurer les paramètres des ports, procédez de la façon suivante :

Étape 1 Sélectionnez **LAN > Paramètres des ports**.

Étape 2 Dans la table Configuration de base par port, configurez les paramètres suivants :

Port	Liste des ports actuellement disponibles sur le routeur.
Libellé de port	Saisissez un libellé de port.
Activer	Cochez la case **Activer** pour activer les paramètres du port. Si cette option est désactivée, tous les paramètres définis sur le port sont perdus.
EEE (Energy-Efficient on Ethernet)	Cochez cette case pour que le port consomme moins d'énergie en période de faible activité des données.

Contrôle de flux	Cochez cette case pour activer le contrôle de flux symétrique. Le contrôle de flux permet d'envoyer et de respecter des trames de pause vers et depuis l'ordinateur LAN connecté au périphérique.
Mode	Sélectionnez le mode des paramètres de port dans la liste déroulante.
Trames géantes	Les trames Jumbo sont des trames Ethernet dont la charge utile est supérieure à 1 500 octets, ce qui correspond à la limite établie par le standard IEEE 802.3. Les trames Jumbo peuvent prendre en charge une charge utile de 9 000 octets maximum. Cochez la case **Activer** pour activer les trames Jumbo.

Étape 3 Dans la section Configuration de mise en miroir des ports, saisissez les informations suivantes :

Activer	Cochez la case **Activer** pour activer la configuration de mise en miroir des ports.
Port de destination	Port sur lequel le trafic mis en miroir peut être géré. Sélectionnez l'un des réseaux LAN **(LAN1 à LAN4)** dans la liste déroulante.
Port contrôlé	Sélectionnez les ports dont le trafic doit être contrôlé sur le port de destination.

Étape 4 Cliquez sur **Appliquer**.

Paramètres VLAN

La page Paramètres VLAN permet d'ajouter l'ID de VLAN pour différencier le trafic.

Pour créer de nouveaux VLAN, procédez comme suit :

Étape 1 Sélectionnez **LAN > Paramètres VLAN**.

Étape 2 Cliquez sur **Ajouter** pour créer un nouveau VLAN.

Étape 3 Saisissez l'ID de VLAN (plage comprise entre 1 et 4 093) et un nom.

Étape 4 Cochez la case Activé pour activer le routage inter-VLAN et la gestion des périphériques.

Étape 5 Renseignez le champ IPv4 ou IPv6.

Configuration du VLAN pour IPv4

Pour configurer le réseau VLAN pour IPv4, sélectionnez IPv4, puis définissez les paramètres suivants.

Adresse IP	Saisissez l'adresse IPv4.
Masque de sous-réseau	Saisissez le masque de sous-réseau.

Type DHCP	• **Désactivé** : le serveur DHCP IPv4 est désactivé sur le VLAN.
	• **Serveur**
	  • **Durée du bail** : saisissez une valeur comprise entre 5 et 43 200 minutes. La valeur par défaut est de 1 440 minutes, soit 24 heures.
	  • **Début de plage et Fin de plage** : saisissez le début de plage et fin de plage des adresses IP pouvant être attribuées de façon dynamique.
	  • **Serveur DNS** : sélectionnez cette option pour utiliser le serveur DNS en tant que proxy ou depuis le FAI dans la liste déroulante.
	  • **Serveur WINS** : saisissez le nom du serveur WINS.
	  • **Options DHCP**
	  • **Option 66** : saisissez l'adresse IP du serveur TFTP.
	  • **Option 150** : saisissez l'adresse IP d'une liste de serveurs TFTP.
	  • **Option 67** : saisissez le nom du fichier de configuration.
	• **Relais** : saisissez l'adresse IPv4 du serveur DHCP distant pour configurer l'agent de relais DHCP.

Configuration du type DHCP pour IPv6

Pour configurer le mode DHCP pour IPv6, saisissez les informations suivantes :

Préfixe	Saisissez le préfixe IPv6.
Longueur de préfixe	Saisissez la longueur du préfixe IPv6.
Aperçu	Affichez un aperçu de l'adresse IPv6.
Identifiant d'interface	Sélectionnez l'identifiant d'interface approprié.

Type DHCP	• **Désactivé** : le serveur DHCP IPv6 est désactivé sur le VLAN.
	• **Serveur**
	  • **Durée du bail** : saisissez une valeur comprise entre 5 et 43 200 minutes. La valeur par défaut est de 1 440 minutes, soit 24 heures.
	  • **Début de plage et Fin de plage** : saisissez les début de plage et fin de plage des adresses IP pouvant être attribuées de façon dynamique.
	  • **Serveur DNS** : sélectionnez cette option pour utiliser le serveur DNS en tant que proxy ou depuis le FAI dans la liste déroulante.

Étape 6 Cliquez sur **Appliquer**.

Affecter les VLAN aux ports

Le trafic sur le port peut être balisé en appliquant un réseau VLAN spécifique. Ce balisage peut vous aider à différencier le trafic et à le rediriger. Il n'existe que 16 réseaux VLAN dans le système, et seul un VLAN sur le réseau étendu du système peut être configuré.

Pour affecter un réseau VLAN à un port, saisissez les informations suivantes.

Étape 7 Sélectionnez l'ID de VLAN approprié.

Étape 8 Cliquez sur **Modifier** pour affecter un réseau VLAN à un port LAN et définissez les paramètres suivants :

- **Non balisé** : le port n'est pas balisé dans le réseau VLAN sélectionné. Si le port est en mode d'accès ou de liaison, le réseau VLAN par défaut est automatiquement exclu lorsque le port non balisé se connecte au VLAN. Sélectionnez **Non balisé** dans la liste déroulante pour ne pas baliser le port.
- **Balisé** : le port est inclus en tant que membre du réseau VLAN sélectionné, et les paquets envoyés à partir de ce port à destination du réseau VLAN sont balisés avec l'ID de VLAN. Sélectionnez **Balisé** dans la liste déroulante pour inclure le port en tant que membre du réseau VLAN sélectionné. Les paquets envoyés à partir de ce port à destination du réseau VLAN sélectionné sont balisés avec l'ID de VLAN. S'il n'existe aucun VLAN non balisé sur un port, l'interface se connecte automatiquement au réseau VLAN1.
- **Exclu** : sélectionnez cette option dans la liste déroulante pour exclure le port du réseau VLAN sélectionné.

Étape 9 Cliquez sur **Appliquer**.

Paramètres Option82

La configuration DHCP permet de configurer le serveur DHCP pour le relais ou le paramètre Option82 (option des informations sur l'agent de relais DHCP) pour les clients LAN en vue d'obtenir des adresses IP. Le serveur DHCP conserve les pools et les baux locaux. Il permet par ailleurs aux clients LAN de se connecter à un serveur distant en vue d'obtenir des adresses IP.

Le paramètre Option82 permet à un agent de relais DHCP d'inclure des informations sur lui-même lors de la redirection des paquets DHCP provenant du client vers le serveur DHCP. Le serveur DHCP peut utiliser ces informations pour implémenter l'adressage IP ou d'autres stratégies d'attribution des paramètres.

Pour configurer le paramètre Option82, procédez de la façon suivante :

Étape 1 Sélectionnez **LAN > Paramètres Option82**.

Étape 2 Cliquez sur **Ajouter** et configurez les options suivantes :

Étape 3 Saisissez les informations suivantes pour configurer le circuit Option82 :

Description	Saisissez la description du client de l'option 82.
ID de circuit	Améliore la sécurité de validation des informations fournies dans l'ID de circuit de l'option 82. Saisissez l'ID de circuit et son format.
Adresse IP et masque de sous-réseau	Saisissez l'adresse IP et le masque de sous-réseau du périphérique.
Durée de bail du client	Durée pendant laquelle un utilisateur du réseau est autorisé à se connecter au routeur avec l'adresse IP actuelle. Saisissez la durée en minutes. Les valeurs valides sont comprises entre 5 et 43 200 minutes. La valeur par défaut est de 1 440 minutes (24 heures).
Début de plage et **Fin de plage**	Début de plage et fin de plage des adresses IP pouvant être attribuées de façon dynamique. La plage peut correspondre au nombre maximal d'adresses IP que le serveur peut attribuer sans chevauchement avec le client PPTP et le client VPN SSL. Par exemple, si le routeur utilise l'adresse IP LAN par défaut, 192.168.1.1, la valeur de début doit être 192.168.1.2 ou supérieure.
Serveur DNS	Type de service DNS où l'adresse IP du serveur DNS est acquise.
DNS statique 1 et DNS statique 2	Adresse IP statique d'un serveur DNS. (Facultatif) Si vous saisissez un deuxième serveur DNS, le routeur utilise le premier serveur DNS pour répondre à une requête.
WINS	Adresse IP facultative d'un serveur WINS (Windows Internet Naming Service) qui résout les noms NetBIOS sur les adresses IP. Par défaut, ce champ est vide.
Options DHCP	• **Option 66** : saisissez l'adresse IP ou le nom d'hôte d'un serveur TFTP unique. • **Option 150** : saisissez les adresses IP d'une liste de serveurs TFTP. • **Option 67** : saisissez le nom du fichier de démarrage.

Étape 4 Cliquez sur **Finish**.

DHCP statique

La fonctionnalité DHCP statique permet au serveur DHCP sur votre routeur de toujours affecter la même adresse IP à un ordinateur spécifique sur votre réseau LAN. Cliquez sur **Afficher les appareils connectés** pour afficher les appareils déjà connectés au routeur.

Pour configurer la fonctionnalité DHCP statique, procédez de la façon suivante :

Étape 1 Cliquez sur **LAN > DHCP statique**.
Étape 2 Cliquez sur **Ajouter**.
Étape 3 Saisissez le nom de la description.
Étape 4 Saisissez l'adresse MAC et l'adresse IPv4 statique.
Étape 5 Cochez la case **Activé**.
Étape 6 Cliquez sur **Appliquer** pour ajouter les appareils à la liste des adresses IP statiques.
Étape 7 Cliquez sur **Importer** ou sur **Exporter** pour utiliser ces détails.

Configuration 802.1X

L'authentification IEEE 802.1X basée sur les ports empêche les périphériques (clients) non autorisés à accéder au réseau. Ce contrôle d'accès au réseau utilise les caractéristiques d'accès physique aux infrastructures LAN IEEE 802 pour authentifier et autoriser les appareils connectés à un port LAN prenant en charge une connexion point à point. Dans ce contexte, un port est un point de liaison unique vers l'infrastructure LAN.

Pour configurer l'authentification basée sur les ports :

Étape 1 Sélectionnez **LAN > Configuration 802.1X**.
Étape 2 Sélectionnez l'option **Activer l'authentification basée sur les ports** pour l'activer.
Étape 3 Sélectionnez l'état d'administration de chaque port dans la liste déroulante.

- **Auto** : cette option permet d'activer l'authentification basée sur les ports. L'interface bascule entre un état autorisé ou non autorisé en fonction de l'échange d'authentification entre le périphérique et le client.
- **Autorisation forcée** : aucune autorisation n'est requise. Au moins un port LAN doit être en mode d'autorisation forcée.

Étape 4 L'état du port indique l'état de la liaison, qu'elle soit active ou inactive, ainsi que l'état de l'authentification.
Étape 5 Cliquez sur **Appliquer**.

Annonce de routeur

Le démon RADVD (démon de notification de routeur) est utilisé pour la configuration des paramètres d'interface, des préfixes, des routes et des annonces. Les hôtes s'appuient sur les routeurs pour faciliter la communication vers tous les autres hôtes, à l'exception de ceux qui se trouvent sur le réseau local. Les routeurs envoient régulièrement des messages d'annonce de routeur et y répondent. Lorsque vous activez cette fonction, les messages sont envoyés régulièrement par le routeur en réponse aux sollicitations. Un hôte utilise ces informations pour obtenir les préfixes et paramètres du réseau local. La désactivation de cette fonction désactive

la configuration automatique, ce qui implique la configuration manuelle de l'adresse IPv6, du préfixe de sous-réseau et de la passerelle par défaut sur chaque périphérique.

Pour configurer l'annonce de routeur, procédez de la façon suivante :

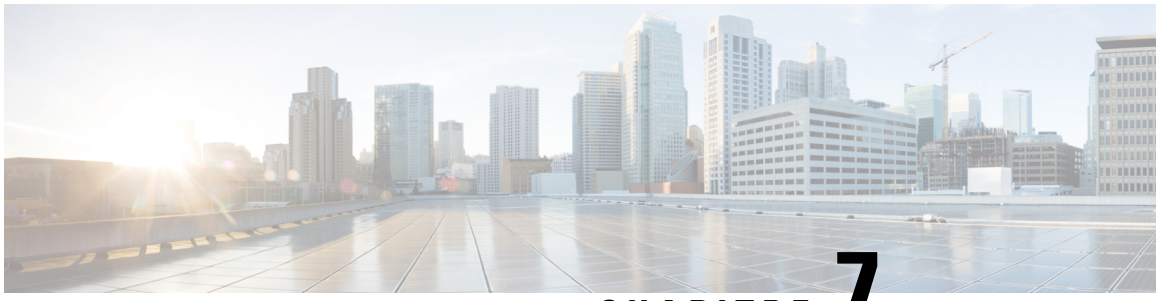
Étape 1 Sélectionnez **LAN > Annonce de routeur**.

Étape 2 Configurez ensuite les paramètres suivants :

Nom de l'interface	Sélectionnez une interface dans la liste déroulante.
Annonce de routeur	Cochez la case **Activer** pour activer l'annonce de routeur sur le réseau VLAN sélectionné.
Mode d'annonce	Sélectionnez le mode d'annonce dans la liste déroulante. • **Multidiffusion non sollicitée** : ce mode envoie les annonces du routeur à toutes les interfaces dans le groupe de multidiffusion. Saisissez l'intervalle d'annonce. Il s'agit du paramètre par défaut. • **Monodiffusion** : ce mode envoie les messages d'annonce de routeur uniquement aux adresses IPv6 connues.
Intervalle d'annonce	Saisissez l'intervalle d'envoi des messages d'annonce de routeur, sur une plage comprise entre 10 et 1 800 secondes (30 secondes étant la valeur par défaut).
Indicateurs d'annonces	Ce paramètre détermine si les hôtes peuvent utiliser DHCPv6 pour obtenir les adresses IP et les informations connexes. Sélectionnez l'une des options suivantes : • **Géré** : les hôtes utilisent un protocole de configuration administré et avec état (DHCPv6) pour obtenir des adresses avec état et d'autres informations via DHCPv6. • **Autre** : les hôtes utilisent un protocole de configuration administré et avec état (DHCPv6) pour obtenir d'autres informations non liées aux adresses, notamment des informations sur le serveur DNS.
Préférence de routeur	Cette mesure de préférence est utilisée dans une topologie de réseau dans laquelle des hôtes à plusieurs hébergements ont accès à plusieurs routeurs. La préférence de routeur permet à un hôte de choisir le routeur approprié. Il existe trois mesures de préférence : **Élevé, Moyen** et **Faible**. La valeur par défaut est Élevé. Sélectionnez la préférence dans la liste déroulante.
Unité maximale de transmission (MTU)	L'unité de transmission maximale (MTU) correspond à la taille maximale de paquet pouvant être transmis sur le réseau. Les MTU sont utilisées dans les messages d'annonce de routeur pour s'assurer que tous les nœuds du réseau utilisent la même valeur de MTU lorsque la MTU du réseau LAN n'est pas connue. Le paramètre par défaut est de 1 500 octets, qui correspond à la valeur standard pour les réseaux Ethernet. Pour les connexions PPPoE, la valeur standard est de 1 492 octets. Ce paramètre ne doit pas être modifié, à moins que votre FAI exige une autre valeur. Saisissez une valeur comprise entre 1 280 et 1 500.
Durée de vie du routeur	Durée d'existence des messages d'annonce de routeur sur la route, en secondes. Saisissez la durée en secondes. La valeur par défaut est de 3 600 secondes.

Étape 3 Dans la table des préfixes, cliquez sur **Ajouter** ou sur **Modifier** pour ajouter ou modifier un masque de sous-réseau et saisir l'adresse IPv6, la longueur de préfixe et la durée de vie.

Étape 4 Cliquez sur **Appliquer**.



CHAPITRE 7

Sans fil

Un réseau local sans fil (WLAN) est une méthode de distribution sans fil qui met en œuvre un système flexible de communication des données utilisant des ondes de radio haute fréquence ; il inclut souvent un point d'accès à Internet. Cette mise en œuvre se fait par l'optimisation, plutôt que le remplacement, d'un réseau LAN filaire au niveau d'un bâtiment ou d'un site. Étant donné que les réseaux WLAN utilisent une fréquence radio pour transmettre et recevoir les données, ils ne nécessitent pas de connexions filaires. Cela permet aux utilisateurs de se déplacer dans la zone de couverture tout en conservant une connexion au réseau.

Cette section décrit le réseau WLAN, qui est un type de réseau local utilisant des ondes radio haute fréquence plutôt que des câbles pour communiquer d'un nœud à l'autre. Elle contient les rubriques suivantes :

Paramètres de base

Le périphérique fournit un réseau LAN sans fil (WLAN) avec tous les ports (LAN et WLAN) sur un seul domaine de diffusion. Le routeur prend en charge 802.11ac et une sélection bibande simultanée (2,4 et 5 GHz). Selon la radio sélectionnée, vous pouvez sélectionner la fréquence ou le canal pour la transmission et la réception de données réseau WLAN. La sélection de la largeur de canal appropriée pour chaque radio peut améliorer le débit WLAN.

Sur la page Paramètres de base, vous pouvez ajouter, modifier ou supprimer les paramètres SSID sans fil, et sélectionner et configurer les canaux radios. Vous pouvez ajouter jusqu'à quatre réseaux sans fil virtuels distincts par radio. En d'autres termes, vous ne pouvez pas ajouter plus de huit SSID (c.-à-d., quatre SSID par radio) ; le bouton Ajouter est grisé lorsque vous atteignez cette limite.

Pour configurer les paramètres SSID sans fil, procédez de la façon suivante :

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

Étape 2 Sous la Table des services, cliquez sur **Ajouter** ou sur **Modifier** et configurez les paramètres suivants.

Nom SSID	Spécifiez le nom du réseau.
Activer	Cochez la case **Activer** pour activer le réseau.

Appliquer activement à la fréquence radio	Sélectionnez la bande **2,4 G** ou **5 G** pour une connexion à un réseau correspondant aux paramètres réseau et à la bande sélectionnée uniquement. Le SSID est créé sur la fréquence radio sélectionnée. Sélectionnez **Les deux** pour configurer le SSID sur les deux fréquences radio et connecter ce profil à un réseau disponible correspondant aux paramètres réseau sélectionnés.
Diffusion SSID	Cochez la case **Activer** pour activer la diffusion SSID si vous souhaitez autoriser les clients sans fil de la zone de couverture à détecter ce réseau sans fil lorsqu'ils recherchent les réseaux disponibles. Désactivez cette fonction si vous ne souhaitez pas faire connaître le SSID. Lorsque cette fonction est désactivée, le client sans fil peut se connecter à votre réseau sans fil uniquement s'il fournit le SSID et les informations de sécurité requises.
Mode de sécurité	Sélectionnez un mode de sécurité pour le réseau parmi les options suivantes : • **Aucun** : sélectionnez cette option pour un réseau non sécurisé. • **WEP-64** : sélectionnez le mode de sécurité WEP 64 bits et saisissez une clé WEP si vous utilisez un équipement ancien qui ne prend pas en charge la sécurité WPA ou WPA2. La clé WEP est une chaîne comportant 10 caractères hexadécimaux. • **WEP-128** : sélectionnez le mode de sécurité WEP 128 bits et saisissez une clé WEP si vous utilisez un équipement ancien qui ne prend pas en charge la sécurité WPA ou WPA2. La clé WEP est une chaîne comportant 26 caractères hexadécimaux. • **WPA2-Personnel** : Sélectionnez le protocole de sécurité Wi-Fi Protected Access II (WPA2) pour une meilleure sécurité. Si cette option est sélectionnée, saisissez une phrase de sécurité alphanumérique. • **WPA2-Personal Mixed** : Sélectionnez ce protocole de sécurité pour une meilleure sécurité lorsque vous autorisez des clients WPA et WPA2 à se connecter simultanément. Si cette option est sélectionnée, saisissez une phrase de sécurité alphanumérique. • **WPA2-Entreprise** : Sélectionnez ce protocole de sécurité pour utiliser l'authentification de serveur RADIUS. Si cette option est sélectionnée, spécifiez les paramètres suivants : • **Adresse IP du serveur RADIUS** (gère l'authentification client). • **Port du serveur RADIUS** (port utilisé pour accéder au serveur RADIUS). • **Secret RADIUS**(secret RADIUS partagé). • **WPA2-Enterprise Mixed** : Sélectionnez ce protocole de sécurité pour utiliser l'authentification de serveur RADIUS lorsque vous autorisez des clients WPA et WPA2 à se connecter simultanément. S'il est sélectionné, spécifiez l'adresse IP du serveur RADIUS, le port du serveur RADIUS et le secret RADIUS.
Phrase secrète	Saisissez la phrase secrète. **Remarque** Si vous utilisez une phrase secrète, cochez la case **Afficher la phrase secrète** pour la rendre visible.

PMF (trames de gestion protégées)	Wi-Fi certified WPA2 avec PMF fournit un niveau de protection WPA2 pour les trames d'action de gestion monodiffusion et multidiffusion. Sélectionnez l'une des options suivantes : • Non requis • Compatible • Obligatoire
Isolation sans fil avec SSID	Cochez la case **Activer** pour activer l'isolation sans fil au sein du SSID. Lorsque l'isolation sans fil est configurée, les clients sans fil ne peuvent pas se voir ou communiquer entre eux lorsqu'ils sont connectés au même SSID.
WMM	Pour hiérarchiser et placer le trafic en file d'attente en fonction de la catégorie d'accès, cochez la case **Activer** afin d'activer les extensions multimédias sans fil (WME). L'activation de WMM peut entraîner une amélioration du débit, mais aussi du taux d'erreurs dans un environnement hautes fréquences (RF) saturé.
WPS	Cochez cette case pour activer WPS. Cette option autorise jusqu'à deux modes d'utilisation : code PIN et bouton de commande. Si cette option est activée, cliquez sur **Configurer** et configurez les paramètres WPS dans la fenêtre contextuelle. Pour plus d'informations sur la configuration de WPS, reportez-vous à la section WPS, à la page 67.
VLAN	Spécifiez l'ID du VLAN auquel le SSID est mappé. Les appareils connectés à ce réseau obtiennent des adresses sur ce VLAN. L'ID du VLAN par défaut est 1 ; si tous les appareils se trouvent sur le même réseau, il est inutile de modifier cette valeur.
Accès par horaire	Spécifiez un horaire si le SSID n'est disponible qu'à certaines heures de la journée ou certains jours de la semaine. Vous pouvez protéger votre réseau en indiquant à quel moment les utilisateurs peuvent accéder au réseau, limitant de cette façon son accès.
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. Cochez cette case pour activer le filtrage MAC pour le SSID. Si cette option est activée, cliquez sur **Configurer** et spécifiez la liste noire (appareils qui n'auront pas le droit d'accéder) et la liste blanche (appareils autorisés à accéder) pour le réseau sans fil.
Portail captif	Cochez la case **Activer** pour activer la vérification du portail captif pour le SSID. Sélectionnez ensuite un profil de portail dans la liste déroulante. Si cette option est activée, vous pouvez aussi cliquer sur **Nouveau** et configurer un nouveau profil. Reportez-vous à la section Portail captif, à la page 67 pour plus d'informations sur l'ajout d'un profil de portail captif.

Étape 3 Cliquez sur **Appliquer**.

Sélection bibande simultanée

Vous pouvez activer ou désactiver les fréquences bibandes, 2,4 GHz et 5 GHz, qui sont prises en charge par le routeur. Vous pouvez spécifier manuellement le numéro de canal de chaque bande ou effectuer une sélection

automatique du canal en vue d'appliquer les paramètres correspondants à tous les réseaux sans fil virtuels. Selon la fréquence radio sélectionnée, le réseau WLAN transmet et reçoit les données sur cette fréquence ou le canal sélectionné. La sélection de la largeur de canal appropriée pour chaque fréquence peut améliorer le débit du réseau WLAN.

Configuration de la fréquence 2,4 GHz

Pour configurer la fréquence radio 2,4 GHz, procédez de la façon suivante :

Étape 1 Cliquez sur **Sans fil > Paramètres de base > 2,4G**.

Étape 2 Cochez la case **Radio** pour activer la bande 2,4 GHz.

Étape 3 Sélectionnez le mode de bande réseau dans la liste déroulante Mode de réseau sans fil.

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

Étape 4 Cliquez sur **20 MHz** ou **20/40 MHz** pour sélectionner la bande passante du canal.

Remarque Lorsque vous utilisez la radio de diffusion 2,4 GHz, vous devez généralement utiliser un bloc de bande passante de canal de 20 MHz. Ceci est dû au fait que davantage de canaux sans chevauchement sont disponibles lors de l'utilisation d'un bloc de 20 MHz (par rapport à un bloc de 40 MHz) ; il est donc peu probable que les canaux entrent en conflit et provoquent une congestion. Vous pouvez également utiliser le bloc 40 MHz sur la radio de diffusion 2,4 GHz. Notez toutefois que celui-ci risque d'entraîner une congestion du trafic Wi-Fi ; par conséquent, nous vous déconseillons son utilisation, notamment si vous vivez dans un immeuble, car il risque de provoquer des interférences avec d'autres utilisateurs 2,4 GHz. Dans ce cas, il est recommandé de sélectionner l'option 20/40 MHz.

Étape 5 Sélectionnez le canal principal en cliquant sur la case d'option **Inférieur** ou **Supérieur**.

Remarque Vous ne pouvez pas sélectionner de canal principal si vous avez sélectionné Bande passante 20 MHz à l'étape 4 ou Auto dans la liste déroulante.

Étape 6 Sélectionnez le canal sans fil approprié dans le menu déroulant. Vous pouvez choisir **Auto.** et permettre au système de sélectionner le canal.

Si vous avez sélectionné **Inférieur** comme canal principal, vous pouvez sélectionner les canaux 1 à 7. Si vous avez sélectionné **Supérieur**, vous pouvez sélectionner les canaux 5 à 11.

Étape 7 Pour activer le mode U-APSD (Unscheduled Automatic Power Save Delivery) et permettre aux clients connectés dotés de la fonctionnalité U-APSD d'économiser de l'énergie, cochez la case **U-APSD (économie d'énergie WMM)**. Ce mode utilise les mécanismes de 802.11e et de l'ancienne version 802.11 pour économiser de l'énergie et régler la consommation d'énergie.

Étape 8 Saisissez le nombre maximal de clients associés dans le champ prévu à cet effet.

Étape 9 Cliquez sur **Appliquer**.

Configuration de la fréquence 5 GHz

Pour configurer la fréquence radio 5 GHz, procédez de la façon suivante :

Étape 1 Cliquez sur **Sans fil > Paramètres de base > 5G**.

Étape 2 Dans la section Radio, cochez la case **Activer** pour activer la bande 5 GHz.

Étape 3 Sélectionnez le mode de bande réseau dans la liste déroulante Mode de réseau sans fil.

Option	Description
A uniquement	Sélectionnez cette option si vous n'avez que des appareils sans fil de type A sur votre réseau.
Mixte N/AC	Sélectionnez cette option si vous n'avez que des appareils sans fil de type N et AC sur votre réseau.
Mixte A/N/AC	Sélectionnez cette option si vous n'avez que des appareils sans fil de type A, N et AC sur votre réseau.

Étape 4 Cliquez sur la case d'option **20 MHz, 40 MHz** ou **80 MHz** pour sélectionner la bande passante du canal.

Remarque Néanmoins, lorsque vous sélectionnez 5 GHz, il est possible d'utiliser des bandes de canaux plus larges pour augmenter la bande passante. Ainsi, vous pouvez utiliser les bandes 20 MHz, 40 MHz (voire 80 MHz) sur le canal 5 GHz.

Dans un environnement moins congestionné nécessitant un débit de données plus élevé, il est recommandé d'utiliser le canal 40 MHz, car il offre 12 canaux sans chevauchement sur la bande 5 GHz.

Étape 5 Sélectionnez le canal principal en cliquant sur **Inférieur** ou **Supérieur**.

Remarque Vous pouvez sélectionner un canal principal, uniquement si vous avez sélectionné une bande passante de 40 MHz.

Étape 6 Sélectionnez le canal sans fil approprié dans le menu déroulant. Vous pouvez choisir **Auto.** et permettre au système de sélectionner le canal.

Étape 7 Si vous utilisez un équipement alimenté par batterie et souhaitez activer le mode U-APSD, cochez la case **U-APSD (économies d'énergie WMM)**.

Étape 8 Saisissez le nombre maximal de clients associés à associer simultanément.

Étape 9 Cliquez sur **Appliquer**.

Paramètres avancés

Pour chaque fréquence, vous pouvez spécifier des paramètres avancés : Rafale de trames, Aucune validation WMM, Vitesse de base, Vitesse de transmission, Intervalle DTIM, Seuil RTS, etc.

Pour configurer les paramètres avancés sous Sans fil, procédez de la façon suivante :

Étape 1 Cliquez sur **Sans fil > Paramètres avancés > 2,4 G ou 5 G**.

Étape 2 Configurez ensuite les paramètres suivants :

Rafale de trames	Cochez la case **Activer** pour activer l'envoi de plusieurs trames avec un écart minimal entre les trames, ce qui améliore l'efficacité du réseau et réduit la charge.
Aucune validation WMM	Cochez la case **Activer** pour améliorer le débit. Cette option peut entraîner un taux d'erreurs plus élevé dans un environnement hautes fréquences (RF) saturé.
Débit de données	Pour Débit de données, cliquez sur **Définissez ce paramètre sur la valeur par défaut** pour rétablir les valeurs par défaut des vitesses de base et de transmission.
Vitesse de base	Sélectionnez les paramètres de vitesse de base, c'est-à-dire les vitesses auxquelles la plate-forme prête pour les services peut transmettre les données. L'appareil annonce sa vitesse de base aux autres appareils sur le réseau afin qu'ils connaissent les vitesses qui seront utilisées. La plate-forme prête pour les services annonce également qu'elle sélectionnera automatiquement la meilleure vitesse de transmission.
Vitesse de transmission	Sélectionnez la vitesse de transmission des données en fonction du débit de votre réseau sans fil.
Index MCS HT	Sélectionnez les options correspondant au paramètre Index MCS HT pour les débits Module haute transmission et Index du modèle de codage. Vous pouvez utiliser les valeurs de l'index MCS en combinaison avec les valeurs de largeur de canal pour calculer instantanément le débit de données disponible du matériel sans fil.
Mode de protection CTS	Le mode de protection CTS est le mécanisme utilisé par le protocole réseau sans fil 802.11 pour réduire les collisions de trame causées par les problèmes de nœuds masqués. Par défaut, cette option est définie sur Auto. Pour la désactiver, cliquez sur **Désactivé**.
Intervalle de balise	Spécifiez le délai entre les transmissions de balise, en millisecondes. Une balise est une diffusion de paquets depuis l'appareil qui permet de synchroniser le réseau sans fil. L'heure à laquelle un nœud (un point d'accès, par exemple) doit envoyer une balise est appelée heure de transmission de balise (TBTT, Target Beacon Transmission Time), exprimée en unité de temps. La plage est comprise entre 40 et 3 500 millisecondes. La valeur par défaut est 100.
Intervalle DTIM	Spécifiez l'intervalle de carte DTIM (Delivery Traffic Indication Map). Ce paramètre informe les clients de la présence de données de multidiffusion/diffusion dans la mémoire tampon du point d'accès. Il est généré dans le cadre de la balise périodique à une fréquence définie par l'intervalle DTIM. La plage est comprise entre 1 et 255. La valeur par défaut est 1.

Seuil de fragmentation	Saisissez la valeur de fragmentation qui indique 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. La plage est comprise entre 256 et 2 346. La valeur par défaut est 2 346.
Seuil RTS	Dans le champ Seuil RTS, saisissez la taille du seuil RTS. Lorsque la taille d'un paquet réseau est inférieure au seuil spécifié, le mécanisme RTS/CTS n'est pas enclenché. La plage est comprise entre 0 et 2347. La valeur par défaut est 2347.
Puissance de transmission	Sélectionnez le volume de données à transmettre dans la liste déroulante.

Étape 3 Cliquez sur **Appliquer**.

WPS

La Configuration WPS (Wi-Fi Protected Setup) est une fonctionnalité de sécurité réseau qui permet aux clients sur lesquels WPS est activé de se connecter facilement et en toute sécurité au réseau sans fil. Trois méthodes de connexion au réseau sans fil sont prises en charge par WPS : bouton de commande WPS, code PIN WPS sur l'appareil client et code PIN d'appareil généré sur la page de configuration WPS.

Pour configurer WPS :

Étape 1 Cliquez sur **Sans fil > WPS**. La page Configuration Wi-Fi protégée apparaît.

Étape 2 Sélectionnez le SSID (pour lequel WPS doit être configuré) dans la liste déroulante WPS

Étape 3 Sélectionnez la bande de fréquences (**2,4 G, 5 G ou Les deux**) dans la liste déroulante des bandes de fréquences.

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

a) Cliquez sur **WPS** sur le client, puis cliquez sur **WPS** sur la page de configuration WPS.

b) Si votre appareil client a un code PIN WPS, saisissez ce code dans la zone de texte et cliquez sur **S'inscrire**.

c) Si l'appareil client requiert un code PIN depuis votre routeur, cliquez sur **Générer** et saisissez le code PIN.

Dans le champ Durée de vie du PIN, sélectionnez la durée de vie de la clé. À l'expiration de cette période, une nouvelle clé est négociée.

La configuration WPS est terminée.

Portail captif

La fonction Portail captif est disponible uniquement sur les modèles de routeur sans fil ; elle fournit aux clients un accès contrôlé et authentifié aux ressources réseau sans compromettre la sécurité. Un client se connectant aux interfaces WLAN est limité à un environnement cloisonné jusqu'à ce qu'il obtienne l'autorisation. Le portail captif affiche une page Web spéciale pour authentifier les clients avant qu'ils puissent utiliser Internet. Le client peut résoudre les noms DNS et sites de navigateur Web ajoutés à cet environnement cloisonné.

L'authentification utilise un portail captif qui initie l'authentification. Lorsqu'un client non authentifié tente de se connecter à une page Web (sur le port 80), la requête est interceptée par un démon et redirigée vers le portail captif (port UI).

Vous pouvez configurer le portail captif pour chaque réseau sans fil virtuel de votre appareil en l'associant à un profil de portail. Vous pouvez aussi afficher l'état du portail captif en sélectionnant **État et statistiques > Trafic du portail captif**. Reportez-vous à la section Paramètres de base, à la page 61 pour des instructions sur l'activation d'un profil de portail captif.

Pour créer un profil de portail captif :

Étape 1 Cliquez sur **Sans fil > Portail captif**.

Étape 2 Sur la page du portail captif, cliquez sur **Ajouter** sous la Table des profils du portail. Pour modifier un profil de portail existant, cochez la case correspondante et cliquez sur **Modifier**.

Étape 3 Sur la page Ajouter un profil pour le portail captif, configurez les paramètres suivants :

Nom du profil	Donnez un nom au profil de portail captif.
Authentification	Indiquez si vous souhaitez activer (**Auth.**) ou désactiver (**Pas d'auth.**) l'authentification.
Connexion utilisateur alternative, redirection	Sélectionnez **URL originale** ou **Une nouvelle URL** et saisissez l'URL dans la zone de texte pour rediriger les utilisateurs vers cette URL après l'authentification.
Délai d'expiration de session inactive	Définissez la durée de vie de l'authentification en secondes, de 0 à 1 440. 0 indique une durée indéfinie.

Étape 4 Dans la section Personnalisation de la page du portail, configurez les paramètres suivants :

Couleur de police	Dans la liste déroulante, sélectionnez la couleur de la police pour le texte qui s'affichera sur la page
Image d'arrière-plan	Cliquez sur **Parcourir** et sélectionnez l'image à afficher en arrière-plan de la page du portail.
Nom de la société	Spécifiez le nom de société qui sera affiché.
Logo de l'entreprise	Cliquez sur **Parcourir** et sélectionnez l'image du logo d'entreprise à afficher.
Message de bienvenue	Saisissez le message de bienvenue à afficher lors de la connexion.
Champ du nom d'utilisateur	Saisissez le texte à afficher pour le champ du nom d'utilisateur.
Champ du mot de passe	Saisissez le texte à afficher pour le champ du mot de passe.
Nom du bouton de connexion	Saisissez le texte affiché sur le bouton de connexion.
Message sur les droits d'auteur	Saisissez le texte standard sur le droit d'auteur associé à votre société.
Message d'erreur à afficher lorsque la connexion échoue	Saisissez le message d'erreur à afficher lorsque la connexion échoue.

Message à afficher lorsque le nombre maximal de connexions est dépassé.	Saisissez le message à afficher lorsque le nombre maximal de connexions est dépassé.
Afficher le contrat d'utilisation	Cochez la case **Activer** pour accepter les conditions d'utilisation.
Titre du contrat d'utilisation	Saisissez un titre pour le texte du contrat.
Message du contrat d'utilisation	Saisissez les termes du contrat qui seront affichés.

Étape 5 Cliquez sur **Aperçu** pour afficher un aperçu des nouveaux paramètres.

Étape 6 Cliquez sur **Appliquer**.

Ambassadeur de lobby

Un ambassadeur de lobby peut créer et gérer les comptes d'utilisateurs invités sur le routeur sans fil. L'ambassadeur de lobby dispose de privilèges de configuration limités ; il peut accéder uniquement aux pages Web utilisées pour gérer les comptes d'invités. L'ambassadeur de lobby peut spécifier le délai d'activité des comptes d'utilisateurs invités. Une fois ce délai écoulé, les comptes d'utilisateurs invités expirent automatiquement. Par défaut, la page Ambassadeur de lobby est masquée ou grisée. Pour utiliser cette fonction, procédez de la façon suivante :

Étape 1 Activez le service Ambassadeur de lobby pour des groupes d'utilisateurs spécifiques dans la page Configuration système > Groupes d'utilisateurs.

Étape 2 Activez le portail captif sur un SSID, puis sélectionnez le nom du groupe d'authentification.

Étape 3 Sélectionnez ensuite **Sans fil > Ambassadeur de lobby**.

Étape 4 Dans la section Ajouter un invité, saisissez un nom d'utilisateur dans le champ correspondant ou cliquez sur **Générer automatiquement** pour générer automatiquement un nom d'utilisateur.

Étape 5 Dans le champ Mot de passe, saisissez un mot de passe ou cliquez sur **Générer automatiquement** pour générer automatiquement un mot de passe.

Étape 6 Dans la section Date d'expiration, sélectionnez les **Jours, Heures** et **Minutes** dans le menu déroulant.

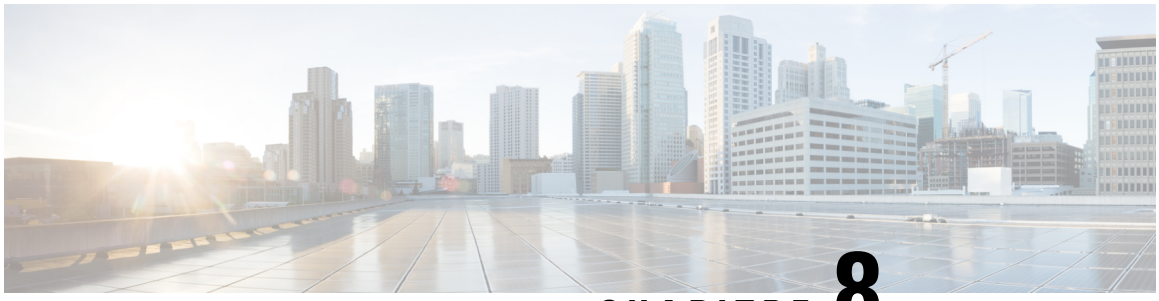
Étape 7 Cochez la case d'option **Supprimer le compte invité lorsqu'il expire** ou **Suspendre le compte invité lorsqu'il expire** pour supprimer ou suspendre le compte de l'ambassadeur de lobby.

Étape 8 Dans le champ SSID, saisissez le SSID en sélectionnant les options dans le menu déroulant.

Étape 9 Cliquez sur **Ajouter** pour ajouter de nouvelles configurations ou sur **Réinitialiser** pour recommencer.

Étape 10 Pour modifier ou supprimer un ambassadeur de lobby existant, cliquez sur **Modifier** ou **Supprimer** sous Invité.

Étape 11 Cliquez sur **Appliquer** pour enregistrer les paramètres.



CHAPITRE 8

Routage

Le routage est le processus de sélection des chemins d'accès les mieux adaptés dans un réseau. Le routage dynamique est une technologie de réseau permettant un routage optimal des données. Grâce au routage dynamique, les routeurs peuvent sélectionner les chemins d'accès en fonction des modifications apportées en temps réel au réseau logique. Le protocole de routage exécuté sur le routeur est chargé de la création, de la maintenance et de la mise à jour de la table de routage dynamique lors du routage dynamique.

Cette section décrit les fonctions de routage de l'appareil. Elle comprend les rubriques suivantes :

Routage statique

Le routage statique est un chemin d'accès fixe configuré manuellement par lequel doit transiter un paquet pour atteindre sa destination. En cas d'absence de communication entre les routeurs sur la topologie de réseau actuelle, le routage statique peut être configuré pour communiquer entre les routeurs. Le routage statique utilise moins de ressources réseau que le routage dynamique, car il ne calcule pas constamment la prochaine route à prendre.

Pour configurer le routage statique, procédez de la façon suivante :

Étape 1 Sélectionnez **Routage > Routage statique**.

Étape 2 Pour les routes IPv4, dans la table WAN, cliquez sur **Ajouter** et configurez les paramètres suivants : Vous pouvez modifier une route existante en cochant la case correspondante et en cliquant sur **Modifier**.

Réseau	Saisissez l'adresse IP du sous-réseau de destination auquel vous souhaitez attribuer une route statique.
Masque	Saisissez le masque de sous-réseau de l'adresse de destination.
Saut suivant	Saisissez l'adresse IP du routeur utilisé en dernier recours.
Nombre de sauts	Saisissez le nombre maximal de sauts (max. 255).
Interface	Sélectionnez l'interface à utiliser pour cette route statique dans le menu déroulant.

Étape 3 Pour les routes IPv6, dans la table WAN, cliquez sur **Ajouter** et configurez les paramètres suivants : Vous pouvez modifier une route existante en cochant la case correspondante et en cliquant sur **Modifier**.

Préfixe	Saisissez le préfixe IPv6.
Durée	Saisissez le nombre de bits de préfixe de l'adresse IP.
Saut suivant	Saisissez l'adresse IP du routeur utilisé en dernier recours.
Nombre de sauts	Saisissez le nombre maximal de sauts (max. 255).
Interface	Sélectionnez l'interface à utiliser pour cette route statique dans le menu déroulant.

Étape 4 Cliquez sur **Appliquer**.

RIP

Le protocole RIP (protocole d'informations de routage) est le protocole IGP standard utilisé sur les réseaux locaux (LAN). Le protocole RIP assure une grande stabilité du réseau en redirigeant rapidement les paquets réseau si l'une des connexions réseau est indisponible. Lorsque le protocole RIP est activé, les utilisateurs subissent peu, voire aucune interruption de service due à un routeur, commutateur ou serveur unique en panne si les ressources réseau disponibles sont suffisantes.

Pour configurer le protocole RIP, procédez de la façon suivante :

Étape 1 Sélectionnez **Routage > RIP**.

Étape 2 Pour activer le protocole RIP, activez l'option **pour IPv4** ou **pour IPv6**, ou les deux, et configurez les paramètres suivants :

Remarque La transmission de l'annonce RIP sur l'interface WAN est automatiquement désactivée si le protocole NAT est activé.

Interface	Cochez la case **Activer** dans l'interface correspondante pour recevoir les routes en amont. **Remarque** Cocher la case **Activer** pour une interface active automatiquement le protocole RIP version 1, le protocole RIP version 2, le protocole RIPng (IPv6) et l'authentification pour cette interface. De même, décocher la case **Activer** désactive toutes ces options.
RIP version 1	Ce protocole utilise le routage par classe et n'inclut pas les informations ou l'authentification du sous-réseau. • Cochez la case **Activer** pour activer l'envoi et la réception des informations de routage sur RIP version 1. • Cochez la case **Passif** pour désactiver l'envoi des informations de routage sur RIP version 1. **Remarque** La configuration passive est activée uniquement lorsque vous cochez la case **Activer**.

RIP version 2	Ce protocole sans classe utilise la multidiffusion et l'authentification par mot de passe. • Cochez la case **Activer** pour activer l'envoi et la réception des informations de routage sur RIP version 2. • Cochez la case **Passif** pour désactiver l'envoi des informations de routage sur RIP version 2. **Remarque** La configuration passive est activée uniquement lorsque vous cochez la case **Activer**.
RIPng (IPv6)	Le protocole RIP de nouvelle génération (RIPng) utilise les paquets UDP (User Datagram Packets) pour envoyer les informations de routage. Bien que basé sur le protocole RIP version 2, il est utilisé pour le routage IPv6. • Cochez la case **Activer** pour activer le routage RIP IPv6. • Cochez la case **Passif** pour désactiver l'envoi de la version RIPng. **Remarque** La configuration passive est activée uniquement lorsque vous cochez la case **Activer**.
Authentification (cette fonction n'est pas disponible pour RIPv1)	Cette fonction de sécurité force l'authentification des paquets RIP avant l'échange des routes avec les autres routeurs. Cette fonction n'est pas disponible pour RIPv1. • Cochez la case **Activer** pour activer l'authentification de façon à ce que l'échange des routes n'ait lieu qu'avec les routeurs de confiance sur le réseau. • **Mot de passe** : sélectionnez le type d'authentification, à savoir **Texte en clair** (méthode d'authentification courante) ou **MD5** (mécanisme d'authentification par stimulation/réponse), puis saisissez le mot de passe.

Étape 3 Cliquez sur **Appliquer**.

Proxy IGMP

IGMP (Internet Group Management Protocol) est un protocole utilisé pour la multidiffusion. Il est activé entre les routeurs et les hôtes qui appartiennent à des groupes de multidiffusion. Les adresses IP de multidiffusion sont une plage spéciale d'adresses IP permettant de réduire le trafic sur le réseau. Lorsqu'un groupe de multidiffusion est affecté à une adresse de multidiffusion, le trafic de multidiffusion de ce groupe est envoyé à cette adresse IP. Le protocole IGMP peut être utilisé pour les ressources Web et les applications associées telles que la diffusion en ligne de vidéos et de jeux. Le proxy IGMP permet au routeur d'émettre des messages IGMP au nom des clients qui se trouvent derrière lui.

Pour activer le proxy IGMP, procédez de la façon suivante :

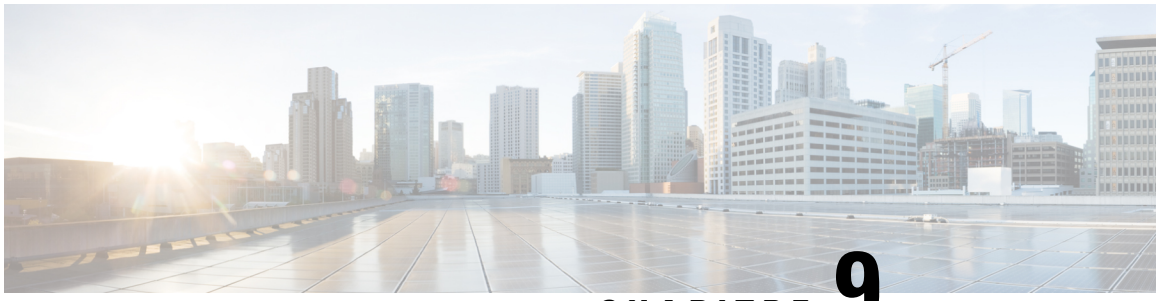
Étape 1 Sélectionnez **Routage > Proxy IGMP**.

Étape 2 Sélectionnez l'option **Activer le proxy IGMP** pour permettre au routeur et aux nœuds de communiquer entre eux.

Étape 3 Sélectionnez l'interface en amont dans la liste.

Étape 4 Sélectionnez l'interface en aval dans la liste afin que le proxy IGMP puisse recevoir des demandes d'adhésion IGMP.

Étape 5 Cliquez sur **Appliquer**.



CHAPITRE 9

Pare-feu

Un pare-feu est une fonction désignée permettant d'éviter tout accès non autorisé par le biais de l'analyse du trafic réseau entrant et sortant. Le pare-feu examine le trafic et filtre les transmissions qui ne respectent pas les critères de sécurité spécifiés. Le pare-feu décide du type de paquets autorisés ou rejetés. Cette section décrit le pare-feu de l'appareil. Elle comprend les rubriques suivantes :

Paramètres de base

La page Paramètres de base vous permet d'activer et de configurer les paramètres de base. Vous pouvez en outre ajouter des domaines approuvés à cette liste. Pour configurer les paramètres de base, procédez de la façon suivante :

Étape 1 Cliquez sur **Pare-feu > Paramètres de base**, puis définissez les paramètres suivants :

Pare-feu	Cochez la case **Activer** pour activer les paramètres de pare-feu ; décochez la case **Activer** pour désactiver cette fonction.
DoS (Déni de service)	Cochez la case **Activer** pour activer le DoS. Le déni de service permet de bloquer les attaques suivantes : Ping fatal, Débit de détection d'inondation SYN [max/sec], Mystification IP, Echo Storm, Saturation ICMP, Saturation UDP et Saturation TCP. **Remarque** Le débit de trafic pour les attaques Inondation SYN, Echo Storm et Saturation ICMP peut être configuré. Les valeurs par défaut sont les suivantes : 128, 15, et 100, respectivement.
Bloquer la requête WAN	Cochez la case **Activer** pour bloquer les demandes d'écho ICMP à destination du réseau WAN.

RESTCONF	RESTCONF normalise l'utilisation des techniques REST pour manipuler les données décrites dans les modèles de données YANG. YANG est un langage de modélisation destiné à prendre en charge les appareils netconf. Cochez les cases **Activer** et **LAN** et/ou **WAN** pour activer RESTCONF.
Port RESTCONF	Saisissez le numéro du port RESTCONF. La valeur par défaut est 443.
NETCONF	Le protocole NETCONF définit un mécanisme simple qui permet de gérer un appareil réseau, de récupérer des informations sur les données de configuration et de charger et manipuler de nouvelles données de configuration. Cochez les cases **Activer** et **LAN** et/ou **WAN** pour activer NETCONF.
Port NETCONF	Saisissez le numéro du port NETCONF.
Gestion Web LAN/VPN	Cochez la case **Activer** pour activer la gestion Web LAN/VPN. Sélectionnez ensuite HTTP ou HTTPS, puis saisissez le numéro de port dans le champ Port.
Gestion Web à distance	Cochez la case **Activer** pour activer la gestion Web à distance. • Sélectionnez **HTTP** ou **HTTPS**, puis saisissez le port (par défaut : 443, plage : 1025-65535).
Adresse IP distante autorisée	Cochez la case **Toutes les adresses IP** ou **Plage d'adresses IPv4 ou IPv6**, puis saisissez un expéditeur et des destinataires pour l'accès à distance.
ALG SIP (passerelle de la couche application de protocole d'initiation de session)	Cochez la case **Activer** pour autoriser l'ALG SIP. Cette fonction permet de traduire puis de coder une nouvelle fois dans le paquet les messages SIP qui transitent par un périphérique configuré avec le mode NAT (Network Address Translation, traduction des adresses réseau).
Port ALG FTP	Saisissez le numéro de port. La valeur par défaut est 21. Le port ALG FTP traduit les paquets FTP.
UPnP (Universal Plug and Play)	Cochez la case **Activer** pour activer le protocole UPnP. UPnP est un ensemble de protocoles réseau qui permet aux appareils sans fil (ordinateurs, imprimantes, passerelles Internet, points d'accès Wi-Fi et terminaux mobiles) de se détecter entre eux sur le réseau et d'établir des services réseau fonctionnels pour le partage de données et les communications.

Étape 2 Dans la section Restreindre les fonctionnalités Web, configurez les paramètres suivants :

Bloquer	Cochez cette case pour restreindre les fonctionnalités Web suivantes : • **Java** : bloque la fonctionnalité Web Java. • **Cookies** : bloque les cookies. • **ActiveX** : bloque ActiveX. • **Accès aux serveurs proxy HTTP** : bloque les serveurs proxy HTTP.
Exception	Cochez la case **Activer** pour autoriser uniquement les fonctionnalités Web sélectionnées, telles que Java, Cookies, ActiveX ou Accès aux serveurs proxy HTTP et restreindre toutes les autres.

Étape 3 Dans la **Table des domaines approuvés**, activez l'option **Nom du domaine** pour modifier les paramètres du domaine existant.

Étape 4 Cliquez sur **Ajouter, Modifier** ou **Supprimer** pour ajouter, modifier ou supprimer un domaine.

Étape 5 Cliquez sur **Appliquer**.

Règles d'accès

Il est possible de configurer des règles pour filtrer les paquets en fonction de paramètres spécifiques tels que l'adresse IP ou les ports. Pour configurer les règles d'accès, procédez de la façon suivante.

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

Étape 2 Dans la table des règles d'accès IPv4 ou IPv6, cliquez sur **Ajouter** (ou sélectionnez la ligne et cliquez sur **Modifier**) et configurez les paramètres suivants :

État de la règle	Sélectionnez **Activer** pour activer la règle d'accès spécifique. Désélectionnez cette option pour la désactiver.
Action	Sélectionnez **Autoriser** ou **Refuser** dans la liste déroulante.
Services	• **IPv4** : sélectionnez le service auquel appliquer la règle IPv4. • **IPv6** : sélectionnez le service auquel appliquer la règle IPv6. • **Services** : sélectionnez le service dans la liste déroulante.
Journal	Sélectionnez une option dans la liste déroulante. • **Toujours** : les journaux qui correspondent au paquet répondant aux règles s'affichent. • **Jamais** : aucun journal n'est requis.
Interface source	Sélectionnez l'interface source dans la liste déroulante.
Adresse source	Sélectionnez l'adresse IP source à laquelle la règle est appliquée, puis saisissez les informations suivantes : • **Toutes** : toutes les adresses IP sont sélectionnées. • **Unique** : saisissez une adresse IP. • **Sous-réseau** : indiquez le sous-réseau d'un réseau. • **Plage IP** : saisissez la plage d'adresses IP.
Interface de destination	Sélectionnez l'interface source dans la liste déroulante.

Adresse de destination	Sélectionnez l'adresse IP de destination à laquelle la règle est appliquée, puis saisissez les informations suivantes : • **Toutes** : toutes les adresses IP sont sélectionnées. • **Unique** : saisissez une adresse IP. • **Sous-réseau** : indiquez le sous-réseau d'un réseau. • **Plage IP** : saisissez la plage d'adresses IP.
Nom de l'horaire	Sélectionnez **Toujours, Bureau, Soirée, Marketing** ou **Heures de travail** dans la liste déroulante pour appliquer la règle de pare-feu. Cliquez ensuite **ici** pour configurer les horaires.

Étape 3 Cliquez sur **Appliquer**.

Étape 4 Cliquez sur **Restaurer les valeurs par défaut** pour restaurer les paramètres par défaut.

Étape 5 Cliquez sur **Gestion des services**.

Étape 6 Pour ajouter un service, cliquez sur **Ajouter** sous la Table des services.

Pour modifier un service, sélectionnez la ligne correspondante et cliquez sur **Modifier**.

Modifiez les champs correspondants.

Étape 7 La liste peut comporter de nombreux services :

- **Nom** : nom du service ou de l'application.
- **Protocole** : sélectionnez un protocole dans la liste déroulante.
- **Port de début/Type ICMP/Protocole IP** : plage des numéros de port réservés à ce service.
- **Port de fin/Code ICMP** : dernier numéro de port réservé à ce service.

Étape 8 Cliquez sur **Appliquer**.

Traduction des adresses réseau

La traduction des adresses réseau (NAT) permet aux réseaux IP privés dotés d'adresses IP non enregistrées de se connecter au réseau. Le protocole NAT traduit les adresses privées du réseau interne en adresses publiques avant la redirection des paquets vers le réseau public.

Pour configurer le protocole NAT, procédez de la façon suivante :

Étape 1 Cliquez sur **Pare-feu > Traduction des adresses réseau**.

Étape 2 Dans la Table NAT, cochez la case **Activer NAT** pour activer les interfaces dans la liste des interfaces.

Étape 3 Cliquez sur **Appliquer**.

NAT statique

La fonctionnalité NAT statique permet de protéger les périphériques LAN contre les détections et les attaques. La fonctionnalité NAT statique crée une relation qui met en correspondance une adresse IP de réseau WAN valide avec des adresses IP LAN masquées sur le WAN (Internet) par le mécanisme NAT.

Étape 1 Cliquez sur **Pare-feu > NAT statique**.

Étape 2 Dans la table NAT statique, cliquez sur **Ajouter** (ou sélectionnez la ligne et cliquez sur **Modifier**) et configurez les paramètres suivants :

Activer	Cochez cette case pour activer la fonctionnalité NAT statique.
Début de la plage IP privée	Saisissez l'adresse IP de début de la plage d'adresses IP interne à mettre en correspondance avec la plage publique.
Début de la plage IP publique	Saisissez l'adresse IP de début de la plage d'adresses IP interne fournie par le FAI. **Remarque** N'incluez pas l'adresse IP de réseau WAN du routeur dans cette plage.
Longueur de la plage	Saisissez le nombre d'adresses IP de la plage. **Remarque** La longueur de plage ne doit pas dépasser le nombre d'adresses IP valides. Pour mettre en correspondance une seule adresse, saisissez 1.
Services	Sélectionnez le nom du service dans la liste déroulante à appliquer à la fonctionnalité NAT statique.
Interfaces	Sélectionnez le nom de l'interface dans la liste déroulante.

Étape 3 Cliquez sur **Gestion des services**.

Étape 4 Pour ajouter un service, cliquez sur **Ajouter** sous la Table des services. Pour modifier ou supprimer un service, sélectionnez la ligne et cliquez sur **Modifier ou sur Supprimer**. Modifiez les champs correspondants.

Étape 5 Configurez les services suivants :

- **Nom** : nom du service ou de l'application.
- **Protocole** : saisissez le protocole.
- **Port de début/Type ICMP/Protocole IP** : saisissez la plage des numéros de port réservés à ce service.
- **Port de fin/Code CMP** : saisissez le dernier numéro de port réservé à ce service.

Étape 6 Cliquez sur **Appliquer**.

Redirection de ports

La redirection de ports permet un accès public aux services sur les appareils réseau sur le LAN en ouvrant un port spécifique ou une plage de ports pour un service tel que FTP. La redirection de ports ouvre une plage de

ports pour les services tels que les jeux Internet, qui utilise des ports alternatifs pour communiquer entre le serveur et l'hôte LAN.

Pour configurer la redirection de ports, procédez de la façon suivante :

Étape 1 Cliquez sur **Pare-feu > Redirection de ports**.

Étape 2 Dans la table Redirection de ports, cliquez sur **Ajouter** (ou sélectionnez la ligne et cliquez sur **Modifier**), puis configurez les paramètres suivants :

Activer	Cochez la case **Activer** pour activer la redirection de ports.
Service externe	Sélectionnez un service externe dans la liste déroulante. Si un service ne figure pas dans la liste, vous pouvez l'ajouter ou modifier la liste en suivant les instructions de la section Gestion des services.
Service interne	Sélectionnez un service interne dans la liste déroulante. Si un service ne figure pas dans la liste, vous pouvez l'ajouter ou modifier la liste en suivant les instructions de la section Gestion des services.
Adresse IP interne	Saisissez les adresses IP internes du serveur.
Interfaces	Sélectionnez l'interface dans la liste déroulante à laquelle appliquer la redirection de ports.

Pour ajouter ou modifier une entrée dans la liste des services, procédez comme suit :

Étape 3 Cliquez sur **Gestion des services**.

Étape 4 Dans la **Table des services**, cliquez sur **Ajouter** (ou sélectionnez la ligne et cliquez sur **Modifier**), puis configurez les paramètres suivants :

- **Nom de l'application** : nom du service ou de l'application.
- **Protocole** : protocole requis. Consultez la documentation du service que vous hébergez.
- **Port de début/Type ICMP/Protocole IP** : plage des numéros de port réservés à ce service.
- **Port de fin** : dernier numéro de port réservé à ce service.

Étape 5 Cliquez sur **Appliquer**.

Étape 6 Dans la table de redirection de ports UPnP, cliquez sur le bouton Actualiser pour actualiser les données. Les règles de redirection de ports pour UPnP sont ajoutées de façon dynamique à l'application UPnP.

Déclenchement de ports

Le déclenchement de ports permet à un port spécifique ou à une plage de ports de s'ouvrir pour recevoir le trafic entrant après que l'utilisateur a envoyé le trafic sortant via le port de déclenchement. Le déclenchement de ports permet au périphérique de contrôler les données sortantes pour des numéros de port spécifiques. Le périphérique rappelle l'adresse IP du client ayant envoyé les données correspondantes. Lorsque les données demandées transitent à nouveau par le périphérique, elles sont envoyées vers le client approprié grâce aux règles d'adressage IP et de mappage de ports.

Pour ajouter ou modifier un service dans la table de déclenchement de ports, configurez les paramètres suivants :

Étape 1 Cliquez sur **Ajouter** (ou sélectionnez la ligne et cliquez sur **Modifier**), puis saisissez les informations suivantes :

Activer	Cochez cette case pour activer le déclenchement de port.
Nom de l'application	Saisissez le nom de l'application.
Service de déclenchement	Sélectionnez un service dans la liste déroulante. Si un service ne figure pas dans la liste, vous pouvez l'ajouter ou modifier la liste en suivant les instructions de la section Gestion des services.
Service entrant	Sélectionnez un service dans la liste déroulante. Si un service ne figure pas dans la liste, vous pouvez l'ajouter ou modifier la liste en suivant les instructions de la section Gestion des services.
Interfaces	Sélectionnez l'interface dans la liste déroulante.

Étape 2 Cliquez sur **Gestion des services** pour ajouter ou modifier une entrée dans la liste des services.

Étape 3 Dans la **Table des services**, cliquez sur **Ajouter** ou sur **Modifier** et configurez les paramètres suivants :

- **Nom de l'application** : nom du service ou de l'application.
- **Protocole** : protocole requis. Consultez la documentation du service que vous hébergez.
- **Port de début/Type ICMP/Protocole IP** : plage des numéros de port réservés à ce service.
- **Port de fin/Code ICMP** : dernier numéro de port réservé à ce service.

Étape 4 Cliquez sur **Appliquer**.

NAT conditionnelle

La fonctionnalité NAT conditionnelle permet d'identifier l'adresse réelle à des fins de traduction des adresses en spécifiant l'adresse source et l'adresse de destination dans une liste d'accès étendue. Vous pouvez spécifier des ports source et de destination. La fonctionnalité NAT conditionnelle permet de créer des règles NAT flexibles pour les utilisateurs avancés. Avant de configurer ces règles, vous devez bien comprendre cette fonctionnalité et les cas d'utilisation qui sont les vôtres. Des paramètres non valides peuvent être acceptés, mais risquent de ne pas fonctionner. Pour la plupart des utilisateurs, il est recommandé d'utiliser la fonction Redirection de ports ou NAT statique.

Remarque La traduction d'adresses dynamique (DNAT) est une forme avancée de traduction d'adresses réseau qui demande au routeur de traduire l'adresse IP, mais pas le numéro de port. Cette approche dynamique permet de mapper les adresses d'un grand nombre d'ordinateurs internes sur des adresses IP routables. Pour DNAT, vous devez définir l'interface sur **toutes**.

Pour configurer la fonctionnalité NAT conditionnelle, procédez de la façon suivante :

Étape 1 Sélectionnez **Pare-feu > NAT conditionnelle**.

Étape 2 Cliquez sur **Ajouter** pour ajouter une nouvelle règle de NAT conditionnelle.

Étape 3 Saisissez un nom pour la nouvelle règle de NAT conditionnelle.

Étape 4 Cochez la case **Activer** pour activer la fonctionnalité NAT conditionnelle.

Étape 5 Dans la section Interface de début, sélectionnez l'interface dans la liste déroulante.

Étape 6 Dans la section Interface de fin, sélectionnez l'interface dans la liste déroulante.

Étape 7 Dans la section Adresse source, sélectionnez **Toutes** ou **Utiliser un nouveau groupe IP** pour créer une nouvelle adresse. Cochez ensuite la case Traduite, puis sélectionnez une option dans la liste déroulante.

Étape 8 Dans la section Adresse de destination, sélectionnez **Toutes** ou **Utiliser un nouveau groupe IP** pour créer une nouvelle adresse. Cochez ensuite la case Traduite, puis sélectionnez une option dans la liste déroulante.

Étape 9 Dans la section Service, sélectionnez une option dans la liste déroulante. Cochez la case, puis sélectionnez l'option Traduite dans la liste déroulante.

Remarque Vous pouvez créer ou sélectionner l'adresse source ou le groupe IP dans la page des adresses IP située sous la page Configuration système. S'il s'agit d'un enregistrement de gestion des services, vous êtes redirigé vers la page Gestion des services sous le groupe d'adresses IP.

Étape 10 Cliquez sur **Appliquer**.

Étape 11 Cliquez sur **Modifier** ou sur **Supprimer** pour modifier ou supprimer une NAT conditionnelle existante.

Étape 12 Cliquez sur **Appliquer**.

Exemples d'utilisation de la fonctionnalité NAT conditionnelle

La fonctionnalité NAT conditionnelle permet d'identifier les adresses réelles pour les traduire, en spécifiant les adresses sources et de destination dans une liste d'accès étendue. Vous pouvez spécifier des ports source et de destination. La fonctionnalité NAT standard prend uniquement en compte les adresses sources, pas l'adresse de destination. Par exemple, avec la fonctionnalité NAT conditionnelle, vous pouvez traduire l'adresse réelle en une adresse mappée lorsqu'elle accède à un serveur spécifique, mais aussi traduire l'adresse réelle en une adresse mappée lorsqu'elle accède un serveur désigné. Voici des exemples d'utilisation de la fonctionnalité NAT conditionnelle.

Exemple 1 : L'adresse source du trafic HTTP est traduite en une autre adresse publique pour le trafic initié par le même hôte LAN.

Topologie: PC1 — LAN[RV260W]WAN — (Internet) — PC2

- PC1: 192.168.1.111
- RV260W LAN : 192.168.1.1
- RV260W WAN : 172.16.1.1/24
- PC2: 172.16.1.100

Objectif : Le trafic HTTP est traduit par une nouvelle adresse publique (172.16.1.10), tandis que le trafic non HTTP est traduit par une adresse WAN pour PC1.

Objet de l'adresse : Configurez l'adresse sur PC1 comme une adresse IP simple de 192.168.1.111 et l'alias WAN comme la nouvelle adresse publique de 172.16.1.10.

Résultat : L'adresse source est traduite par 172.16.1.10 lors de l'activation du trafic HTTP depuis PC1. Lors de l'activation du trafic FTP depuis PC1, l'adresse source est traduite par l'adresse WAN d'origine de 172.16.1.1.

Exemple 2

Topologie PC1/PC10 — LAN[RV260W]WAN — (Internet) — PC2

- PC1 : 192.168.1.111
- PC10 : 192.168.1.10
- RV260W LAN : 192.168.1.1
- RV260W WAN : 172.16.1.1/24
- PC : 172.16.1.100

Objectif : Utilisez l'adresse source pour permettre au PC de la traduire en une adresse publique spécifique tandis que les autres se traduisent par une adresse WAN.

Objet de l'adresse: Configurez l'adresse sur PC1 en 192.168.1.111, sur PC10 en 192.168.1.10, l'alias WAN en 172.16.1.10 et l'alias 2 WAN en 172.16.1.11.

Résultat : Activez le trafic issu de PC1, PC10 et des autres PC. Le trafic venant de PC1 et PC10 est traduit par 172.16.1.10 et 172.16.1.11 respectivement. Le trafic provenant des autres PC est traduit par l'adresse WAN 172.16.1.1.

Exemple 3

Le sous-réseau VLAN2 exécute la fonctionnalité NAT tandis que VLAN1 et les autres sous-réseaux sont en mode de routage.

Topologie PC1/PC10 — LAN[RV260W]WAN — (Intranet) — PC2

- PC1 : 192.168.1.111, sur VLAN1
- PC10 : 192.168.2.10, sur VLAN2
- RV260W LAN : 192.168.1.1 (VLAN1), 192.168.2.1 (VLAN2)
- RV260W WAN : 172.16.1.1/24
- PC2 : 172.16.1.100

Remarque: Désactivez la fonctionnalité NAT globale sur WAN1.

Objet de l'adresse: Configurez le sous-réseau VLAN2 sur 192.168.2.0/24.

Résultat: Le trafic VLAN provenant du sous-réseau VLAN2 est traduit en trafic IP WAN. Le reste du trafic provenant de VLAN2 sort du WAN en mode routé (l'adresse source n'est pas traduite).

Exemple 4

Vous configurez VLAN1 avec le sous-réseau A et VLAN2 avec le sous-réseau B. Les deux sous-réseaux font l'objet d'une traduction NAT vers le WAN : le sous-réseau A vers une adresse IP publique 1 et le sous-réseau B vers une adresse IP publique 2.

Topologie PC1/PC10 — LAN[RV260W]WAN — (Internet) — PC2

- PC1 : 192.168.1.111, sur VLAN1
- PC10 : 192.168.2.10, sur VLAN2

- RV260W LAN : 192.168.1.1 (VLAN1), 192.168.2.1 (VLAN2)
- RV260W WAN : 172.16.1.1/24
- PC2 : 172.16.1.100

Résultat : PC1, sur VLAN1, est traduit en l'alias WAN 172.16.1.10, tandis que PC10, sur VLAN2, est traduit en l'alias 2 WAN 172.16.1.11.

Exemple 5

Les hôtes LAN généraux sont traduits en adresses IP WAN lorsqu'ils accèdent à Internet. Le client OpenVPN est traduit en une autre adresse publique lorsqu'il accède à Internet.

Objet de l'adresse: Configurez l'alias WAN sur 172.16.1.10 et OpenVPN sur 10.1.4.0/24.

Résultat: Le PC accède au serveur Internet et l'utilisateur LAN général est traduit par l'adresse IP WAN 172.16.1.1. Le client OpenVPN (PC2) se traduit par 172.16.1.10.

Exemple 6

Autorisez uniquement certains hôtes Internet à accéder au serveur côté LAN.

Topologie PC1/PC10 — LAN[RV260W]WAN — PC2

- PC1 : 192.168.1.111/24
- RV260W LAN : 192.168.1.1/24
- RV260W WAN : 172.16.1.1/24, GW 172.16.1.2
- PC2 : 172.16.1.110

Objet de l'adresse : Configurez les hôtes autorisés sur 172.16.1.100-110, l'IP WAN sur 172.16.1.1 et PC1 sur 192.168.1.111.

Remarque : Sélectionnez l'option **Any** (Tous) pour l'interface de destination du préroutage DNAT. Le périphérique transfère le trafic à l'interface appropriée en fonction de l'adresse de destination traduite. Vous ne pouvez pas configurer une interface VLAN spécifique.

Résultat : L'adresse de PC2 est 172.16.1.110, et il peut accéder à PC1 via http://172.16.1.1. Modifiez l'adresse du PC en utilisant une adresse hors de la plage 172.16.1.100-110 s'il ne peut pas accéder au serveur interne.

Exemple 7

Autorisez uniquement certains hôtes Internet à accéder au serveur LAN avec une règle de type 1:1.

Topologie PC1/PC10 — LAN[RV260W]WAN — PC2

- PC1 : 192.168.1.111/24.
- RV260W LAN : 192.168.1.1/24
- RV260W WAN : 172.16.1.1/24, GW 172.16.1.2.
- PC2 : 172.16.1.110

Objet de l'adresse: Configurez les hôtes autorisés sur 172.16.1.100-110, l'alias WAN sur 172.16.1.10 et PC1 sur 192.168.1.111.

Résultat: Seul les hôtes de la plage 172.16.1.100-110 peuvent accéder à PC1 via 172.16.1.10.

Délai d'expiration de session

Dans la section Délai d'expiration de session, vous pouvez configurer le délai d'expiration de la session et le nombre maximal de connexions simultanées pour les flux TCP/UDP/ICMP. Le délai d'expiration de session indique le délai d'expiration d'une session TCP ou UDP après une période d'inactivité.

Pour configurer le délai d'expiration de session, procédez de la façon suivante :

Étape 1 Cliquez sur **Pare-feu > Délai d'expiration de session**.

Étape 2 Configurez les paramètres suivants :

Délai d'expiration de session TCP	Saisissez la valeur du délai d'expiration des sessions TCP, en secondes. Les sessions TCP inactives sont supprimées de la table des sessions après ce délai (plage comprise entre 30 et 1 800, valeur par défaut 1 800).
Délai d'expiration de session UDP	Saisissez la valeur du délai d'expiration des sessions UDP, en secondes. Les sessions UDP inactives sont supprimées de la table des sessions après ce délai (plage comprise entre 30 et 86 400, valeur par défaut 30).
Délai d'expiration de session ICMP	Saisissez la valeur du délai d'expiration des sessions ICMP, en secondes. Les sessions ICMP inactives sont supprimées de la table des sessions après ce délai (plage comprise entre 15 et 60, valeur par défaut 30).
Nombre maximal de connexions simultanées	Saisissez le nombre maximal de connexions simultanées autorisées (plage comprise entre 10 000 et 15 000, valeur par défaut 15 000).
Connexions actives	Indiquez le nombre de connexions actives.
Supprimer les connexions	Cliquez sur ce bouton pour supprimer les connexions actives.

Étape 3 Cliquez sur **Appliquer**.

Hôte DMZ

Une DMZ est un sous-réseau ouvert au public, bien que derrière le pare-feu. Grâce à la DMZ, les paquets qui accèdent au port WAN peuvent être redirigés vers une adresse IP spécifique sur le réseau LAN.

L'hôte DMZ permet à un hôte sur le réseau local d'être visible sur Internet afin d'utiliser des services tels que les jeux ou la visioconférence sur Internet, le Web ou les serveurs de messagerie. L'accès à l'hôte DMZ à partir d'Internet peut être restreint à l'aide des règles d'accès du pare-feu. Activez l'hôte DMZ avec prudence, car tous les services de cet hôte seront exposés à Internet.

Pour configurer l'hôte DMZ, procédez de la façon suivante :

Étape 1 Sélectionnez **Pare-feu > Hôte DMZ**.

Étape 2 Dans **Hôte DMZ**, sélectionnez **Activer**.

Étape 3 Saisissez l'**Adresse IP de l'hôte DMZ**.

Étape 4 Cliquez sur **Appliquer**.

CHAPITRE 10

VPN

Un réseau privé virtuel (VPN) permet d'établir une connexion cryptée sur un réseau moins sécurisé. Le réseau VPN garantit un niveau de sécurité approprié pour les systèmes connectés lorsque l'infrastructure réseau sous-jacente n'a pas les capacités de le faire. Un tunnel est établi en tant que réseau privé pouvant envoyer des données de façon sécurisée à l'aide de méthodes de cryptage et d'authentification standard.

Une connexion de réseau privé virtuel (VPN) entre deux terminaux est appelée « tunnel IP ». Le tunnel est créé via une méthode d'encapsulation, qui encapsule les données dans un protocole connu (IP) approuvé par les deux terminaux. Le tunnel crée un circuit virtuel entre les deux terminaux et fait apparaître la connexion comme connexion dédiée, même si elle couvre l'infrastructure Internet.

Un VPN d'accès distant repose généralement sur le protocole IPSec ou SSL pour sécuriser la connexion. Les VPN fournissent un accès de couche 2 au réseau cible ; ils nécessitent l'exécution d'un protocole de tunneling tel que PPTP ou L2TP sur la connexion IPSec de base. Le VPN IPSec prend en charge le VPN site à site pour un tunnel passerelle à passerelle et le VPN client à serveur pour un tunnel hôte à passerelle. Par exemple, un utilisateur peut configurer un tunnel VPN sur un site distant pour le connecter au routeur du siège et pouvoir accéder en toute sécurité au réseau d'entreprise. Le VPN client à serveur permet de connecter un ordinateur portable ou de bureau à un réseau d'entreprise via un serveur VPN.

Cette section décrit les fonctions VPN de l'appareil. Elle comprend les rubriques suivantes :

Assistant de configuration du VPN

Un réseau privé virtuel (VPN) permet d'établir une connexion cryptée sur un réseau moins sécurisé. Le réseau VPN garantit un niveau de sécurité approprié pour les systèmes connectés lorsque l'infrastructure réseau sous-jacente n'a pas les capacités de le faire. Un tunnel est établi en tant que réseau privé pouvant envoyer des données de façon sécurisée à l'aide de méthodes de cryptage et d'authentification standard. Un VPN d'accès distant repose généralement sur le protocole IPSec ou SSL pour sécuriser la connexion. Les VPN fournissent un accès de couche 2 au réseau cible ; ils nécessitent l'exécution d'un protocole de tunneling tel que PPTP ou L2TP sur la connexion IPSec de base. Le VPN IPSec prend en charge le VPN site à site pour un tunnel

passerelle à passerelle et le VPN client à serveur pour un tunnel hôte à passerelle. Par exemple, un utilisateur peut configurer un tunnel VPN sur un site distant pour le connecter au routeur du siège et pouvoir accéder en toute sécurité au réseau d'entreprise. Le VPN client à serveur permet de connecter un ordinateur portable ou de bureau à un réseau d'entreprise via un serveur VPN.

Pour démarrer l'Assistant de configuration du VPN, procédez de la façon suivante :

Étape 1 Cliquez sur **VPN > Assistant de configuration du VPN**.

Étape 2 Dans la section Mise en route, saisissez un nom de connexion dans la zone **Attribuer un nom de connexion**.

Étape 3 Sélectionnez une interface dans la liste déroulante.

Étape 4 Cliquez sur **Suivant**.

Étape 5 Dans la section Paramètres du routeur distant, sélectionnez un type de connexion distante dans la liste déroulante. Si vous sélectionnez **IP statique ou Nom de domaine complet**, saisissez la connexion distante dans le champ Connexion distante.

Étape 6 Cliquez sur **Suivant** pour passer à l'écran suivant.

Étape 7 Dans la section Réseaux local et distant, sous Sélection de trafic en local, sélectionnez l'adresse IP locale (**Sous-réseau, Adresse individuelle ou Toutes**) dans la liste déroulante. Si vous sélectionnez **Sous-réseau**, saisissez l'adresse IP et le masque de sous-réseau. Si vous sélectionnez **Adresse individuelle**, saisissez l'adresse IP.

Étape 8 Sous Sélection de trafic distant, sélectionnez l'adresse IP distante (**Sous-réseau ou Adresse individuelle**) dans la liste déroulante. Si vous sélectionnez **Sous-réseau**, saisissez l'adresse IP et le masque de sous-réseau. Si vous sélectionnez **Adresse individuelle**, saisissez l'adresse IP.

Étape 9 Cliquez sur **Suivant**.

Étape 10 Dans la section Réseaux local et distant, attribuez un nom au profil IPSec dans la liste déroulante.

- Si le profil IPSec par défaut est sélectionné, définissez les paramètres suivants :

Clé prépartagée	Clé prépartagée à utiliser pour authentifier l'homologue IKE distant. Vous pouvez saisir jusqu'à 30 caractères clavier ou valeurs hexadécimales, tels que Mon_@123 ou 4d795f40313233. Les deux extrémités du tunnel VPN doivent utiliser la même clé prépartagée. Il est fortement recommandé de modifier régulièrement la clé prépartagée afin d'optimiser la sécurité du VPN. Vous pouvez afficher la clé prépartagée en sélectionnant Activer.

- Si vous sélectionnez un nouveau profil IPSec et la version IKE 1 et 2, définissez les paramètres suivants :

Options Phase 1

Groupe Diffie-Hellman (DH)	Sélectionnez un groupe DH (**Groupe 2 ou Groupe 5**) dans la liste déroulante. DH est un protocole d'échange de clés comportant deux groupes de différentes longueurs de clés principales : Le Groupe 2 comporte jusqu'à 1 024 bits, et le Groupe 5 jusqu'à 1 536 bits. Pour obtenir un débit plus rapide au détriment de la sécurité, sélectionnez le Groupe 2. Pour obtenir un débit moins rapide, mais une sécurité plus élevée, sélectionnez le Groupe 5. Le Groupe 2 est sélectionné par défaut.

Cryptage	Sélectionnez l'option de cryptage (**3DES, AES-128, AES-192 ou AES-256**) dans la liste déroulante. Cette méthode détermine l'algorithme utilisé pour crypter ou décrypter les paquets ESP/ISAKMP.
Authentification	La méthode d'authentification détermine le mode de validation des paquets d'en-têtes ESP (Encapsulating Security Payload). MD5 est un algorithme de hachage unidirectionnel produisant un prétraitement 128 bits. SHA1 est un algorithme de hachage unidirectionnel produisant un prétraitement 160 bits. L'algorithme SHA1 est recommandé, car il est plus sécurisé. Assurez-vous que les deux extrémités du tunnel VPN utilisent la même méthode d'authentification. Sélectionnez une méthode d'authentification (**MD5, SHA1 ou SHA2-256**).
Durée de vie SA (secondes)	Durée d'activité d'une association de sécurité (SA) IKE dans cette phase (plage comprise entre 120 et 86 400, 28 800 étant la valeur par défaut).
Clé prépartagée	Saisissez la clé prépartagée à utiliser pour authentifier l'homologue IKE distant. Vous pouvez saisir jusqu'à 30 caractères clavier ou valeurs hexadécimales, tels que Mon_@123 ou 4d795f40313233. Les deux extrémités du tunnel VPN doivent utiliser la même clé prépartagée. Nous vous recommandons de modifier régulièrement la clé prépartagée afin de maximiser la sécurité VPN.

Options Phase 2

Sélection du protocole	Sélectionnez un protocole dans la liste déroulante. • **AH** : sélectionnez AH pour assurer l'intégrité des données dans les cas où les données ne sont pas secrètes, mais doivent être authentifiées. • **ESP** : sélectionnez ESP pour crypter les données, puis indiquez la méthode de cryptage.
Cryptage	Sélectionnez le cryptage (**3DES, AES-128, AES-192 ou AES-256**) dans la liste déroulante. Cette méthode détermine l'algorithme utilisé pour crypter ou décrypter les paquets ESP/ISAKMP.
Authentification	Sélectionnez une méthode d'authentification (**MD5, SHA1 ou SHA2-256**).
Durée de vie SA (secondes)	Durée d'activité d'un tunnel VPN (SA IPSec) dans cette phase. La valeur par défaut pour la phase 2 est de 3600 secondes.
Enregistrer en tant que nouveau profil	Attribuez un nom au nouveau profil.
PFS (Perfect Forward Secrecy)	Si l'option PFS (Perfect Forward Secrecy) est activée, la phase 2 de la négociation IKE génère une nouvelle clé pour le cryptage et l'authentification du trafic IPSec. L'option PFS permet d'améliorer la sécurité des communications transmises sur Internet à l'aide de clés publiques chiffrées. Cochez cette case pour activer cette fonction ou décochez-la pour la désactiver. Il est recommandé d'activer cette fonction. Saisissez la durée en secondes.

Étape 11 Cliquez sur **Suivant** pour afficher un récapitulatif de toutes les configurations.

Étape 12 Cliquez sur **Soumettre**.

IPSec VPN

IPSec (Internet Protocol Security) est un ensemble de protocoles situé au sommet de la couche IP (Internet Protocol). Il permet à deux hôtes ou plus de communiquer de façon sécurisée grâce à l'authentification et au cryptage de chaque paquet IP de données.

Le protocole IPSec est principalement utilisé pour fournir un service VPN (Virtual Private Networking). Un VPN est un réseau virtuel qui sert de base aux réseaux physiques existants. Les réseaux VPN constituent un mécanisme de communication sécurisé pour les données et les informations IP transmises entre les réseaux. Il est également possible d'utiliser un réseau VPN sur un réseau existant (p. ex., Internet) pour assurer le transfert sécurisé des données sensibles via les réseaux publics.

Les réseaux VPN permettent par ailleurs de sécuriser les communications entre les entreprises et les télétravailleurs, quel que soit le lieu où se trouvent ces derniers. Il est de surcroît possible de créer un réseau VPN au sein d'un réseau unique en vue de protéger les communications sensibles d'autres parties sur le même réseau.

Dans les sections suivantes, nous aborderons les profils IPSec, ainsi que les réseaux VPN site à site et client à site.

Profils IPsec

Le profil IPSec est la configuration centrale dans IPSec qui définit la plupart des paramètres IPSec tels que le protocole (ESP [Encapsulation Security Payload], AH [Authentication Header]), le mode (tunnel, transport), les algorithmes (cryptage, intégrité, Diffie-Hellman), la confidentialité persistante (PFS), la durée de vie SA et le protocole de gestion des clés (IKEv1, IKEv2).

Les profils IPSec contiennent des informations liées aux algorithmes, notamment le cryptage, l'authentification et le groupe DH pour les négociations des phases I et II en mode auto. Ces profils contiennent par ailleurs des clés pour les algorithmes correspondants lorsque le mode de génération de clés est manuel.

Pour configurer les profils IPsec, procédez de la façon suivante :

Étape 1 Sélectionnez **VPN > VPN IPSec > Profils IPSec**.

Étape 2 Dans la Table des profils IPSec, cliquez sur **Ajouter**.

Étape 3 Donnez un nom au profil et sélectionnez le mode de génération de clés.

Étape 4 Pour le mode de génération de clés automatique, sélectionnez la version IKE.

Étape 5 Dans la section Options de la phase 1, configurez les paramètres suivants :

Groupe Diffie-Hellman (DH)	DH est un protocole d'échange de clés comportant deux groupes de différentes longueurs de clés principales : 1 024 bits et 1 536 bits. Sélectionnez une option dans la liste déroulante.
Cryptage	Sélectionnez l'option de cryptage (**3DES, AES-128, AES-192 ou AES-256**) dans la liste déroulante. Cette méthode détermine l'algorithme utilisé pour crypter ou décrypter les paquets ESP/ISAKMP.

Authentification	La méthode d'authentification détermine le mode de validation des paquets d'en-têtes ESP (Encapsulating Security Payload). MD5 est un algorithme de hachage unidirectionnel produisant un prétraitement 128 bits. SHA1 est un algorithme de hachage unidirectionnel produisant un prétraitement 160 bits. L'algorithme SHA1 est recommandé, car il est plus sécurisé. Assurez-vous que les deux extrémités du tunnel VPN utilisent la même méthode d'authentification. Sélectionnez une méthode d'authentification (**MD5, SHA1 ou SHA2-256**).
Durée de vie SA	Durée d'activité d'une association de sécurité (SA) IKE dans cette phase. (Plage de 120 à 86 400, 28 800 étant la valeur par défaut).

Étape 6 Dans la section Options de la phase 2, configurez les paramètres suivants :

Sélection du protocole	Sélectionnez un protocole dans la liste déroulante. • **ESP** : sélectionnez ESP pour crypter les données, puis indiquez la méthode de cryptage. • **AH** : sélectionnez AH pour assurer l'intégrité des données dans les cas où les données ne sont pas secrètes, mais doivent être authentifiées.
Cryptage	Sélectionnez l'option de cryptage (**3DES, AES-128, AES-192 ou AES-256**) dans la liste déroulante. Cette méthode détermine l'algorithme utilisé pour crypter ou décrypter les paquets ESP/ISAKMP.
Authentification	Sélectionnez une méthode d'authentification (**MD5, SHA1 ou SHA2-256**).
Durée de vie SA (secondes)	Durée d'activité d'un tunnel VPN (SA IPSec) dans cette phase. La valeur par défaut pour la phase 2 est de 3600 secondes.
PFS (Perfect Forward Secrecy, confidentialité persistante)	Cochez la case **Activer** pour activer la confidentialité persistante.
Groupe Diffie-Hellman (DH)	DH est un protocole d'échange de clés comportant deux groupes de différentes longueurs de clés principales : 1 024 et 1 536 bits. Sélectionnez une option dans la liste déroulante.

Étape 7 Pour le **Mode de génération de clés manuel**, configurez les paramètres suivants :

Configurations IPSec

SPI (Security Parameter Index) entrant	Saisissez une valeur (comprise entre 100 et FFFFFFFF). La valeur par défaut est 100. L'indice SPI est une balise d'identification ajoutée à un en-tête lors de l'utilisation du protocole IPSec pour le tunneling du trafic IP. Cette balise aide le noyau à faire la différence entre deux flux de trafic susceptibles d'utiliser des règles et des algorithmes de cryptage différents.
SPI sortant	Saisissez une valeur (comprise entre 100 et FFFFFFFF, la valeur par défaut étant 100).
Cryptage	Sélectionnez l'option de cryptage (**3DES, AES-128, AES-192 ou AES-256**) dans la liste déroulante. Cette méthode détermine l'algorithme utilisé pour crypter ou décrypter les paquets ESP/ISAKMP.

Clé entrante	Saisissez un numéro (hexadécimal à 48 caractères). Cette clé permet de décrypter les paquets ESP reçus au format hexadécimal.
Clé sortante	Saisissez un numéro (hexadécimal à 48 caractères). Cette clé permet de crypter les paquets standard au format hexadécimal.
Authentification	La méthode d'authentification détermine le mode de validation des paquets d'en-têtes ESP (Encapsulating Security Payload). MD5 est un algorithme de hachage unidirectionnel produisant un prétraitement 128 bits. SHA1 est un algorithme de hachage unidirectionnel produisant un prétraitement 160 bits. L'algorithme SHA1 est recommandé, car il est plus sécurisé. Assurez-vous que les deux extrémités du tunnel VPN utilisent la même méthode d'authentification. Sélectionnez une méthode d'authentification (**MD5, SHA1 ou SHA2-256**).
Clé entrante	Saisissez un numéro (hexadécimal à 32 caractères). Cette clé permet de décrypter les paquets ESP reçus au format hexadécimal.
Clé sortante	Saisissez un numéro (hexadécimal à 32 caractères). Cette clé permet de crypter les paquets standard au format hexadécimal.

Étape 8 Sélectionnez un profil IPSec et cliquez sur **Modifier** ou sur **Supprimer**.

Étape 9 Pour cloner un profil existant, sélectionnez un profil, puis cliquez sur **Cloner**.

Étape 10 Cliquez sur **Appliquer**.

Site à site

Dans un VPN site à site, le routeur local sur un site se connecte à un routeur distant via un tunnel VPN. Les périphériques clients peuvent accéder aux ressources du réseau comme s'ils se trouvaient sur le même site. Ce modèle peut être utilisé pour plusieurs utilisateurs sur un site distant.

Pour établir une connexion, au moins l'un des routeurs doit être identifiable à l'aide d'une adresse IP statique ou d'un nom d'hôte DNS dynamique. Si l'un des routeurs possède uniquement une adresse IP dynamique, vous pouvez utiliser une adresse e-mail (nom de domaine complet de l'utilisateur) ou un nom de domaine complet pour vous identifier afin d'établir la connexion.

Les deux sous-réseaux LAN aux deux extrémités du tunnel ne peuvent pas être connectés au même réseau. Par exemple, si le réseau LAN du site A utilise le sous-réseau 192.168.1.x/24, le site B peut utiliser 192.168.2.x/24.

Pour configurer un tunnel, saisissez les paramètres correspondants (en inversant le groupe local et le groupe distant) lors de la configuration des deux routeurs. Supposez que ce routeur est identifié comme le Routeur A. Saisissez ses paramètres dans la section Configuration du groupe local et saisissez les paramètres de l'autre routeur (Routeur B) dans la section Configuration du groupe distant. Lorsque vous configurez l'autre routeur (Routeur B), saisissez ses paramètres dans la section Configuration du groupe local, et saisissez les paramètres du Routeur A dans la section Configuration du groupe distant.

Pour configurer le VPN site à site, procédez de la façon suivante :

Étape 1 Cliquez sur **VPN > VPN IPSec > Site à site**.

Étape 2 Les informations suivantes s'affichent dans la table Site à site :

Nom de la connexion	Nom de la connexion au tunnel VPN créée à l'aide de l'Assistant de configuration VPN. Il n'est pas nécessaire que ce nom corresponde au nom utilisé à l'autre extrémité du tunnel.
Terminal distant	Adresse IP du point d'extrémité distant sur lequel la connexion VPN doit être établie. Il peut s'agir d'un nom de domaine complet ou d'une adresse IP.
Interface	Interface utilisée pour le tunnel.
Profil IPSec	Profil IPSec utilisé pour le tunnel VPN.
Sélection de trafic en local	Sélecteurs de trafic d'où provient le trafic.
Sélection de trafic distant	Sélecteurs de trafic auxquels le trafic est destiné.
État	État du tunnel.
Actions	• **Modifier** : cliquez sur ce bouton pour modifier la connexion ; la page Site à Site - Ajouter ou modifier une nouvelle connexion s'ouvre. • **Supprimer** : cliquez sur ce bouton pour supprimer la connexion. • **Connexion** : cliquez sur ce bouton pour vous connecter et établir le tunnel. • **Déconnexion** : cliquez sur ce bouton pour vous déconnecter.

Connexion VPN site à site

Pour créer une nouvelle connexion VPN site à site, cliquez sur **Ajouter** et configurez les paramètres suivants :

Étape 1 Sous l'onglet Paramètres de base, configurez les paramètres suivants :

Activer	Cliquez sur **Activer** pour activer la configuration.
Nom de la connexion	Attribuez un nom de connexion au tunnel VPN. Cette description sert uniquement de référence et ne doit pas nécessairement correspondre au nom utilisé à l'autre extrémité du tunnel.
Profil IPSec	**Par défaut** : le profil automatique est sélectionné.
Interface	Sélectionnez l'interface (**WAN1, WAN2, USB1 ou USB2**) dans la liste déroulante pour utiliser ce tunnel.
Terminal distant	Sélectionnez **IP statique** ou **Nom de domaine complet** dans la liste déroulante.

Méthode d'authentification IKE

Clé prépartagée	Les homologues IKE s'authentifient l'un l'autre en calculant et en envoyant un hachage de données indexé incluant la clé prépartagée. Si l'homologue de réception est capable de créer indépendamment le même hachage à l'aide de sa clé prépartagée, il sait que les deux homologues doivent partager le même secret et doivent donc s'authentifier l'un l'autre. Les clés prépartagées ne sont pas modulables, car chaque homologue IPSec doit être configuré avec la clé prépartagée de tous les autres homologues avec lesquels il établit une session. Saisissez la clé prépartagée, puis cliquez sur **Activer** pour activer la complexité de clé prépartagée minimale.
Afficher la clé prépartagée	Cochez la case **Activer** pour afficher la clé prépartagée.
Mesure de la fiabilité de la clé prépartagée	Cette mesure indique le niveau de sécurité de la clé prépartagée à l'aide de barres de couleur.
Complexité minimale de la clé prépartagée	Cochez la case **Activer** pour activer la complexité minimale de la clé prépartagée.
Certificat	Le certificat numérique est un paquet contenant des informations telles que l'identité d'un porteur de certificat : nom ou adresse IP, numéro de série du certificat, date d'expiration du certificat et copie de la clé publique du porteur du certificat. Le format du certificat numérique standard est défini dans la spécification X.509. La version 3 de la spécification X.509 définit la structure de données des certificats. Sélectionnez le certificat dans la liste déroulante.

Pour la configuration du groupe local

Type d'identifiant local	Sélectionnez l'option IP WAN locale, Nom de domaine complet local ou Nom de domaine complet de l'utilisateur local dans la liste déroulante.
Identifiant local	Saisissez le nom ou l'adresse IP de l'identifiant en fonction de votre sélection.
Type d'IP locale	Sélectionnez **Adresse IP** ou **Sous-réseau** dans la liste déroulante.
Adresse IP	Saisissez l'adresse IP du périphérique pouvant utiliser ce tunnel.
Masque de sous-réseau	Saisissez le masque de sous-réseau.

Configuration du groupe distant

Type d'identifiant distant	Sélectionnez l'option IP WAN distante, Nom de domaine complet distant ou Nom de domaine complet de l'utilisateur distant dans la liste déroulante.
Identifiant distant	Saisissez le nom ou l'adresse IP de l'identifiant en fonction de votre sélection.
Type d'IP distante	Sélectionnez **Adresse IP** ou **Sous-réseau** dans la liste déroulante.
Adresse IP	Saisissez l'adresse IP du périphérique pouvant utiliser ce tunnel.
Masque de sous-réseau	Saisissez le masque de sous-réseau.
Mode agressif	Cochez cette case pour activer le mode agressif.

Étape 2 Sous l'onglet Paramètres avancés, configurez les paramètres suivants :

Compresser (prend en charge le protocole de compression de la charge utile IP)	Ce protocole permet de réduire la taille des datagrammes IP. Cochez la case **Compresser** pour que le routeur puisse proposer une compression lorsqu'il démarre une connexion. Si le répondeur refuse cette proposition, le routeur ignore la compression. Si le routeur est le répondeur, il accepte la compression même si celle-ci n'est pas activée. Si vous activez cette fonction pour ce routeur, activez-la également sur le routeur à l'autre extrémité du tunnel.
Diffusion NetBIOS	Cette fonction envoie des messages de diffusion utilisés pour la résolution des noms dans la mise en réseau Windows en vue d'identifier les ressources, telles que les ordinateurs, les imprimantes et les serveurs de fichiers. Ces messages sont utilisés par certains logiciels et fonctions Windows, tels que le Voisinage réseau. En règle générale, le trafic de diffusion LAN n'est pas transmis sur un tunnel VPN. Il est néanmoins possible de sélectionner cette option pour activer les diffusions NetBIOS d'une extrémité du tunnel en vue de les rediffuser sur l'autre extrémité.
Maintenir actif	Cette fonction tente de rétablir la connexion VPN à intervalles réguliers.
Intervalle de surveillance de la fonction Maintenir actif	Saisissez le nombre de secondes pour définir l'intervalle de surveillance de la fonction Maintenir actif. La plage est comprise entre 10 et 300 secondes.
Activer DPD (détection d'homologue indisponible)	Cochez la case **Activer DPD** pour activer DPD. Cette fonction permet d'envoyer des messages HELLO/ACK (bonjour/accusé de réception) périodiques pour vérifier l'état du tunnel VPN. L'option DPD doit être activée sur les deux extrémités du tunnel VPN. Spécifiez l'intervalle entre les messages HELLO/ACK dans le champ Intervalle en définissant les paramètres suivants : • **Délai de retard** : saisissez le délai de retard entre chaque message Hello. • **Délai de détection dépassé** : saisissez le délai pour déclarer que l'homologue est indisponible. • **Action DPD** : action à prendre après le délai d'expiration de la détection d'homologue indisponible. Sélectionnez **Effacer** ou **Redémarrer** dans la liste déroulante.
Authentification étendue	Sélectionnez l'option **Authentification étendue** pour l'activer. Pour un utilisateur unique, sélectionnez **Utilisateur**, puis saisissez le nom d'utilisateur et le mot de passe. Pour un groupe, sélectionnez **Nom du groupe**, puis sélectionnez **admin** ou **invité** dans la liste déroulante.

DNS fractionné	Cochez l'option **DNS fractionné** pour l'activer. Cette option permet de fractionner les requêtes DNS au serveur DNS et les requêtes DNS à un autre serveur DNS en fonction des noms de domaine spécifiés. Lorsque le routeur reçoit une requête de résolution d'adresse, il inspecte le nom de domaine. Si le nom de domaine correspond à celui défini dans le paramètre DNS fractionné, il transmet la requête au serveur DNS spécifié. Dans le cas contraire, la requête est transmise au serveur DNS spécifié dans les paramètres d'interface WAN. **Serveur DNS 1 et Serveur DNS 2** : saisissez l'adresse IP du serveur DNS à utiliser pour les domaines spécifiques. Vous pouvez également spécifier un autre serveur DNS dans le champ Serveur DNS 2. **Nom de domaine 1 à 6** : saisissez les noms de domaine correspondant aux serveurs DNS. Les requêtes de domaines sont transmises au serveur DNS spécifié.

Étape 3 Pour activer le basculement site à site, la fonction Maintenir actif doit être activée sous l'onglet Paramètres avancés. Ensuite, sous l'onglet Basculement, configurez les paramètres suivants :

Sauvegarde du tunnel	Sélectionnez l'option **Sauvegarde du tunnel** pour l'activer. Lorsque le tunnel principal est indisponible, cette fonction permet au routeur de rétablir le tunnel VPN en utilisant une adresse IP alternative pour l'homologue distant ou une interface WAN locale alternative. Cette fonction n'est disponible que si vous avez activé l'option DPD.
Adresse IP de sauvegarde à distance	Saisissez l'adresse IP de l'homologue distant, ou saisissez de nouveau l'adresse IP WAN déjà définie pour la passerelle distante.
Interface locale	Sélectionnez l'interface locale (**WAN1, WAN2, USB1 ou USB2**) dans la liste déroulante.

Étape 4 Cliquez sur **Appliquer**.

Client à site

Les clients Internet peuvent se connecter au serveur pour accéder au réseau d'entreprise ou à un réseau LAN derrière le serveur. Cette fonction permet de créer un nouveau tunnel VPN permettant aux télétravailleurs et aux employés en déplacement d'accéder à votre réseau à l'aide d'un logiciel client VPN tiers.

Pour créer et configurer le tunnel client à site, procédez de la façon suivante :

Étape 1 Cliquez sur **VPN > VPN IPsec > Client à site**.

Étape 2 Dans la section Tunnels client à site IPSec, cliquez sur **Ajouter** pour ajouter un nouveau tunnel.

Étape 3 Cliquez sur l'onglet Paramètres avancés et configurez les paramètres suivants :

Activer	Cochez la case **Activer** pour activer le tunnel.
Nom du tunnel	Spécifiez le nom du tunnel.
Profil IPSec	Sélectionnez un profil dans la liste déroulante.
Interface	Sélectionnez l'interface dans la liste déroulante.

Méthode d'authentification IKE	Méthode d'authentification à utiliser lors des négociations IKE dans les tunnels IKE. • **Clé prépartagée** : les homologues IKE s'authentifient l'un l'autre en calculant et en envoyant un hachage de données indexé incluant la clé prépartagée. Si l'homologue de réception est capable de créer indépendamment le même hachage à l'aide de sa clé prépartagée, il sait que les deux homologues doivent partager le même secret et doivent donc s'authentifier l'un l'autre. Les clés prépartagées ne sont pas modulables, car chaque homologue IPSec doit être configuré avec la clé prépartagée de tous les autres homologues avec lesquels il établit une session. Saisissez la clé prépartagée, puis cliquez sur **Activer** pour l'afficher et pour activer la complexité de clé prépartagée minimale. • **Certificat** : Le certificat numérique est un paquet contenant des informations telles que l'identité d'un porteur de certificat : nom ou adresse IP, numéro de série du certificat, date d'expiration du certificat et copie de la clé publique du porteur du certificat. Le format du certificat numérique standard est défini dans la spécification X.509. La version 3 de la spécification X.509 définit la structure de données des certificats. Sélectionnez le certificat dans la liste déroulante.
Identifiant local	Sélectionnez l'identifiant local dans la liste déroulante (**IP WAN locale, Adresse IP, Nom de domaine complet ou Nom de domaine complet de l'utilisateur**). Saisissez ensuite l'adresse IP correspondant à l'identifiant local.
Identifiant distant	Sélectionnez l'identifiant distant dans la liste déroulante (**Adresse IP, Nom de domaine complet ou Nom de domaine complet de l'utilisateur**). Saisissez ensuite l'adresse IP correspondant à l'identifiant distant.
Authentification étendue	Cochez la case **Authentification étendue** pour activer cette option, puis sélectionnez les options existantes ou cliquez sur **Ajouter** pour ajouter un nouveau nom.
Plage de groupes pour le réseau LAN du client	Cochez la case **Plage de groupes pour le réseau LAN du client** pour activer cette option et définissez les paramètres suivants : • **IP de début** : saisissez la première adresse IP de la plage. • **IP de fin** : saisissez la dernière adresse IP de la plage.

Étape 4 Sous l'onglet Paramètres avancés, configurez les paramètres suivants :

Terminal distant	Sélectionnez le point d'extrémité distant (**IP statique, Nom de domaine complet ou IP dynamique**) dans la liste déroulante.
Type d'IP locale	Ressources LAN fournies avec un accès sécurisé utilisant le tunnel. Sélectionnez l'adresse IP ou le sous-réseau dans la liste déroulante.
Serveur DNS principal	Saisissez l'adresse IP principale du serveur DNS à utiliser dans le réseau distant.
Serveur DNS secondaire	Saisissez l'adresse IP secondaire du serveur DNS à utiliser dans le réseau distant.
Serveurs WINS principal et secondaire	Adresses IP principale et secondaire d'un serveur WINS (Windows Internet Naming Service).
Domaine par défaut	Saisissez le nom du domaine par défaut.

Tunnel fractionné	Cochez la case **Activé** pour activer le tunnel fractionné. Cliquez ensuite sur **Ajouter**, vérifiez le nom du domaine et saisissez un nom. Vous pouvez également ajouter, modifier ou supprimer un tunnel fractionné.
DNS fractionné	Cochez cette case pour activer le tunnel fractionné. Cliquez ensuite sur Ajouter pour saisir une adresse IP et un masque de réseau pour le tunnel fractionné. Vous pouvez également ajouter, modifier ou supprimer un tunnel fractionné.
Mode agressif	Sélectionnez l'option **Mode agressif** pour l'activer. La fonction Mode agressif permet de spécifier les attributs du tunnel RADIUS d'un homologue de sécurité IP (IPsec) et d'initier une négociation en mode agressif via le protocole IKE (Internet Key Exchange) avec le tunnel.
Compresser (prend en charge le protocole de compression de la capacité utile IP [IP Comp])	Si le répondeur refuse cette proposition, le routeur ignore la compression. Si le routeur est le répondeur, il accepte la compression même si celle-ci n'est pas activée. Si vous activez cette fonction pour ce routeur, activez-la également sur le routeur à l'autre extrémité du tunnel.

Remarque Si vous configurez le serveur VPN IKEv2 pour Windows 7, définissez une durée de vie supérieure à celle du client Windows pour éviter tout problème de génération de clés.

Étape 5 Cliquez sur **Appliquer**.

OpenVPN

OpenVPN utilise le protocole SSL/TLS et prend en charge des fonctions d'authentification de client flexibles pour les connexions point à point. OpenVPN fonctionne en mode client-serveur lorsqu'un serveur est connecté à Internet. Tous les clients ont un accès complet à Internet. Le client utilise le serveur pour terminer l'ensemble de son trafic Internet après la connexion au serveur. OpenVPN crée des ponts Ethernet sécurisés à l'aide d'appareils virtuels.

Pour configurer OpenVPN, procédez de la façon suivante :

Étape 1 Cliquez sur **VPN > OpenVPN**.

Étape 2 Cochez la case **Activer** pour activer le VPN, puis configurez les paramètres suivants :

Interface	Sélectionnez l'interface dans la liste déroulante.
Certificat CA	Sélectionnez le certificat CA dans la liste déroulante.
Certificat du serveur	Sélectionnez le certificat du serveur dans la liste déroulante.
Authentification du client	Sélectionnez le mode d'authentification du client dans la liste déroulante.
Pool d'adresses du client	Saisissez l'adresse IP du pool d'adresses du client.
Masque de réseau	Saisissez le masque de réseau.
Protocole	Sélectionnez le protocole dans la liste déroulante.

Port	Saisissez le numéro de port.
Cryptage	Sélectionnez le type de cryptage dans la liste déroulante.
Mode du tunnel	Sélectionnez **Full-Tunnel** ou **Tunnel fractionné**. Si vous sélectionnez l'option Tunnel fractionné, cliquez sur **Ajouter**, puis saisissez l'adresse IP et le masque de sous-réseau du tunnel fractionné.
Nom de domaine	Saisissez le nom de domaine.
DNS 1 et 2	Saisissez les adresses IP du DNS 1 et du DNS 2
Serveur WIN principal	Saisissez l'adresse IP du serveur WINS (Windows Internet Naming Service) principal.
Serveur WINS secondaire	Saisissez l'adresse IP du serveur WINS (Windows Internet Naming Service) secondaire.
Isolation du client	Cochez cette case pour activer l'**Isolation du client**.
Compression	Cochez cette case pour activer la **Compression**.

Étape 3 Cliquez sur **Appliquer**.

Prochaine étape

Pour générer les fichiers de configuration pour le client, procédez comme suit.

1. Dans la section Paramètre d'exportation, cochez la case **Inclure le certificat du client**. Sélectionnez une option pour inclure le certificat du client dans le fichier de configuration. Cette option s'applique uniquement au mode « Mot de passe + Certificat ».
2. Cochez la case **Exporter le modèle de configuration du client (.ovpn)** pour exporter le modèle de configuration du client.
3. Cochez la case **Envoyer un e-mail**. Choisissez ensuite d'envoyer le modèle de configuration du client par e-mail aux destinataires. Saisissez l'adresse e-mail et l'objet du courriel. Cliquez sur **Générer** une fois tous les champs renseignés.

Serveur PPTP

Le protocole PPTP (Point-to-Point Tunneling Protocol) permet d'implémenter des réseaux privés virtuels. Le protocole PPTP utilise un canal de contrôle sur TCP et un tunnel GRE pour encapsuler les paquets PPP. Il est possible d'activer jusqu'à 10 tunnels VPN PPTP pour les utilisateurs qui exécutent un logiciel client PPTP sur les routeurs RV160. Dans l'Assistant, l'utilisateur choisit l'option qui lui permet d'établir une connexion avec son lieu de travail via une connexion VPN. L'utilisateur doit connaître l'adresse IP du réseau étendu de l'appareil. Pour en savoir plus, consultez la documentation ou les fichiers d'aide de votre système d'exploitation.

Vous devez configurer le serveur VPN et vous assurer que le port 1723 est ouvert pour les clients Internet ; PPTP ne nécessite aucune configuration supplémentaire. PPTP est l'un des plus anciens protocoles VPN ; il présente donc un niveau de sécurité faible. Pour configurer le serveur PPTP, procédez de la façon suivante :

Étape 1 Cliquez sur **VPN > Serveur PPTP** et configurez les paramètres suivants :

Serveur PPTP	Sélectionnez **Activé** ou **Désactivé** pour activer ou désactiver le serveur PPTP.
Adresse IP de début et de fin	Plage d'adresses LAN à affecter aux clients VPN PPTP. La plage d'adresses IP LAN pour les clients VPN PPTP doit être en dehors de la plage DHCP normale du routeur. Saisissez les adresses IP de début et de fin si vous avez activé PPTP.
Adresses IP DNS1 et DNS2	Saisissez l'adresse IP du serveur DNS principal et du serveur DNS secondaire.
Authentification de l'utilisateur	Sélectionnez l'authentification de l'utilisateur (**Admin**) ou cliquez sur **Ajouter** pour ajouter un nouvel utilisateur.
Cryptage MPPE (Microsoft Point-to-Point Encryption)	Le cryptage MPPE crypte les données dans les connexions d'accès à distance PPP (Point-to-Point Protocol) ou les connexions via un réseau privé virtuel (VPN) PPTP. Les schémas de cryptage MPPE des clés 128 bits sont pris en charge. Sélectionnez le cryptage MPPE (**Aucun ou 128 bits**) dans la liste déroulante.

Étape 2 Cliquez sur **Appliquer**.

Tunnel GRE

L'encapsulation d'acheminement générique (GRE) est l'une des techniques de tunneling disponibles qui utilise une adresse IP comme protocole de transport et achemine de nombreux protocoles passagers différents. Les tunnels servent de liaisons point à point disposant de deux terminaux identifiés par les adresses sources et les adresses de destination du tunnel sur chaque terminal.

Pour créer et configurer un tunnel GRE sécurisé, procédez de la façon suivante :

Étape 1 Cliquez sur **VPN > Tunnel GRE**.

Étape 2 Cliquez sur **Ajouter** pour ajouter une nouvelle configuration, ou sur **Modifier** ou **Supprimer** pour modifier ou supprimer une configuration existante.

Étape 3 Dans la section Ajouter/modifier un tunnel GRE, configurez les paramètres suivants :

Nom de l'interface	Saisissez le nom de l'interface à connecter au tunnel.
Activer	Cochez cette case pour activer l'interface.
Source du tunnel	Sélectionnez la source du tunnel dans la liste déroulante.
Destination du tunnel	Indiquez la destination du tunnel (**IP statique ou Nom de domaine complet**).
Adresse IP du tunnel GRE	Saisissez l'adresse IP du tunnel GRE qui achemine le protocole de transport.
Masque de sous-réseau	Saisissez le masque de sous-réseau du tunnel GRE.
MTU	Saisissez l'unité de transmission maximale (MTU).

Étape 4 Cliquez sur **Appliquer**.

Intercommunication VPN

L'option Intercommunication VPN permet aux clients VPN de communiquer via ce routeur et de se connecter à un point d'extrémité VPN. Cette option est activée par défaut.

Pour configurer l'intercommunication VPN, procédez de la façon suivante :

Étape 1 Sélectionnez **VPN > Intercommunication VPN**.

Étape 2 Pour activer les intercommunications, cochez la case **Activer** en regard de chaque protocole approuvé :

- **Intercommunication IPSec** : IPSec est un ensemble de protocoles utilisé pour la mise en œuvre d'échanges sécurisés de paquets au niveau de la couche IP.
- **Intercommunication PPTP** : le protocole PPTP (Point-to-Point Tunneling Protocol) permet au protocole PPP (Point-to-Point Protocol) de traverser un réseau IP.
- **Intercommunication L2TP** : le protocole L2TP (Layer 2 Tunneling Protocol) constitue la méthode utilisée pour activer les sessions point à point via Internet sur la couche 2.

Étape 3 Cliquez sur **Appliquer**.

Allocation des ressources

L'allocation des ressources VPN permet d'allouer des ressources au réseau VPN. Pour configurer l'allocation des ressources VPN, procédez de la façon suivante :

Étape 1 Sélectionnez **VPN > Allocation des ressources**.

Étape 2 Dans la table des types VPN, configurez le nombre maximal de connexions pour chaque VPN.

- **VPN IPSec** : saisissez le nombre de connexions. Le nombre maximal de connexions est de 20.
- **VPN PPTP** : saisissez le nombre de connexions. Le nombre maximal de connexions est de 20.
- **OpenVPN** : saisissez le nombre de connexions. Le nombre maximal de connexions est de 20.

Étape 3 Cliquez sur **Appliquer**.

CHAPITRE 11

Sécurité

Cette section décrit les fonctions de sécurité de l'appareil. Elle comprend les rubriques suivantes :

Filtrage de contenu

Le filtrage de contenu permet de limiter l'accès à certains sites Web indésirables. Cette fonction peut bloquer l'accès aux sites Web en fonction des noms de domaines et des mots-clés. Il est également possible de programmer les périodes d'activation du filtrage de contenu.

Pour configurer et activer le filtrage de contenu, procédez de la façon suivante.

Étape 1 Cliquez sur **Sécurité > Filtrage de contenu**.

Étape 2 Sélectionnez l'option **Activer le filtrage de contenu**.

Étape 3 Sélectionnez l'une des options suivantes :

Bloquer les URL correspondantes	Cochez la case **Bloquer les URL correspondantes** pour bloquer des domaines et des mots-clés spécifiques.
Autoriser uniquement les URL correspondantes	Cochez la case **Autoriser uniquement les URL correspondantes** pour autoriser uniquement les domaines et mots-clés spécifiés.

Étape 4 Sous Filtrer par domaine, cliquez sur **Ajouter**.

Étape 5 Saisissez le domaine à filtrer ou autorisez-le dans la colonne Nom du domaine.

Étape 6 Pour spécifier l'horaire d'activation des règles de filtrage de contenu, sélectionnez-le dans la liste déroulante **Horaire**.

Étape 7 Sous Filtrer par mot-clé, cliquez sur **Ajouter**.

Étape 8 Saisissez les mots-clés à bloquer ou à autoriser dans la colonne Nom du mot-clé.

Étape 9 Pour spécifier l'horaire d'activation des règles de filtrage de contenu, sélectionnez-le dans la liste déroulante Horaire. Vous pouvez modifier un nom de domaine ou un mot-clé existant en le sélectionnant et en cliquant sur **Modifier**.

Étape 10 Cliquez sur **Appliquer**.

CHAPITRE 12

QoS

La qualité de service (QoS) permet d'optimiser la gestion du trafic réseau en vue d'améliorer l'expérience des utilisateurs. La QoS est une mesure de performance définie dans un réseau de communication. Elle donne la priorité à un type de transmission par rapport à un autre. La QoS augmente la capacité du réseau à maintenir la bande passante et à gérer d'autres éléments de performances tels que la latence, le taux d'erreurs et le temps de disponibilité.

La QoS permet en outre de contrôler et de gérer les ressources du réseau en définissant des priorités pour un type de données spécifique (vidéo, audio, fichiers) sur le réseau. Elle s'applique uniquement au trafic réseau généré pour la vidéo à la demande, la télévision IP, la VoIP, la lecture multimédia en continu, la visioconférence et les jeux en ligne.

Cette section décrit les fonctions de QoS de l'appareil. Elle comprend les rubriques suivantes :

Classes de trafic

Les classes de trafic permettent de diriger le trafic vers la file d'attente souhaitée en fonction du service. Le service peut être une application de port TCP ou UDP de couche 4, une adresse IP source ou de destination, une interface DSCP, une interface de réception, un système d'exploitation ou un périphérique. Vous pouvez aussi réécrire la valeur DSCP des paquets entrants. Par défaut, l'ensemble du trafic réseau correspond à la classe de trafic par défaut.

Pour configurer les classes de trafic, procédez de la façon suivante :

Étape 1 Cliquez sur **QoS > Classes de trafic**.

Étape 2 Dans la Table de trafic, cliquez sur **Ajouter** (ou sélectionnez la ligne et cliquez sur **Modifier**) et configurez les paramètres suivants :

- **Nom de la classe** : saisissez le nom de la classe définie.
- **Description** : saisissez la description de la classe.

- **En cours d'utilis.** : enregistrement de classe de trafic en cours d'utilisation par une stratégie de mise en file d'attente.

Étape 3 Dans la Table des services, cliquez sur **Ajouter** (ou sélectionnez la ligne et cliquez sur **Modifier**) et configurez les paramètres suivants :

Nom du service	Nom du service pour appliquer la classification du trafic. Saisissez le nom du service.
Interface de réception	Interface qui reçoit le trafic pour appliquer les enregistrements de classification. Sélectionnez l'une des interfaces dans la liste déroulante. • **Tous les réseaux VLAN** ou **Réseau VLAN spécifique** : trafic sortant (egress). • **WAN** : trafic entrant (ingress).
Version IP	Version IP du trafic. Sélectionnez **IPv4, IPv6 ou Les deux** (si vous ne connaissez pas la version du trafic).
IP source	Saisissez l'adresse IP source du trafic.
IP de destination	Saisissez l'adresse IP de destination du trafic.
Service	sélectionnez le nom du service à appliquer sur l'enregistrement de trafic. Indiquez le port source et le port de destination.
Mettre en correspondance DSCP	Valeur à mettre en correspondance avec la valeur DSCP des paquets entrants.
Réécrire DSCP	Valeur DSCP à remplacer dans les paquets entrants.

Étape 4 Cliquez sur **Appliquer**.

Mise en file d'attente WAN

La gestion de la congestion est la technique QoS qui offre le meilleur service lors d'un trafic intense. La gestion de la congestion utilise la mise en file d'attente sur l'interface des appareils réseau pour prendre en charge la congestion temporaire qui stocke en mémoire tampon les paquets en excès jusqu'à ce que la bande passante soit de nouveau suffisante. La configuration des files d'attente assure la fluidité du trafic prioritaire en cas de congestion. Il est donc possible de gérer le trafic Internet de LAN à WAN sur l'appareil selon trois modes différents (Contrôle du débit, Priorité et Latence faible), qui s'excluent mutuellement.

Pour configurer la mise en file d'attente WAN, procédez de la façon suivante :

Étape 1 Cliquez sur **QoS > Mise en file d'attente WAN**.

Étape 2 Sélectionnez le moteur de mise en file d'attente de votre choix et définissez les paramètres suivants.

Priorité	Utilisez ce paramètre lorsque toutes les files d'attente nécessitent une bande passante minimale. Dans ce mode, la bande passante des files d'attente est attribuée selon un rapport 4:3:2:1 (du plus élevé au plus faible) de la bande passante configurée sur l'interface. • Cochez la case **Priorité**. • Cliquez sur **Ajouter**, puis attribuez un nom à la stratégie et décrivez-la. • Dans la table Priorité de mise en file d'attente, sélectionnez ensuite la classe de trafic à associer à chaque file d'attente.
Contrôle du débit	Les paquets provenant de chaque file d'attente sont envoyés avec la bande passante maximale autorisée. Néanmoins, en cas de congestion, le débit minimal de chaque file d'attente configurée est appliqué sur le trafic réseau. La somme des débits minimum de toutes les files d'attente, ainsi que le débit maximal pour chaque file, ne doivent pas dépasser 100 %. • Cochez la case **Contrôle du débit**. • Cliquez sur **Ajouter**, puis attribuez un nom à la stratégie et décrivez-la. • Dans la table Priorité de mise en file d'attente, sélectionnez ensuite la classe de trafic à associer à chaque file d'attente. Configurez le débit minimal et maximal (en pourcentage) pour chaque file d'attente. **Remarque** Le trafic auquel n'est rattaché aucun enregistrement de classification est considéré comme file d'attente par défaut.
Latence faible	Ce paramètre permet d'appliquer une latence faible au trafic réseau critique (priorité élevée), par exemple les données vocales ou les données de diffusion. Les paquets dans une file de priorité élevée sont toujours programmés en premier, et les files d'attente de priorité inférieure sont transmises (selon le rapport configuré) une fois le trafic prioritaire envoyé. • Cochez la case **Faible latence**. • Cliquez sur **Ajouter**, puis attribuez un nom à la stratégie et décrivez-la. • Dans la table Priorité de mise en file d'attente, sélectionnez ensuite la classe de trafic à associer à chaque file d'attente. Configurez la valeur de partage de la bande passante pour chaque file d'attente. **Remarque** Le trafic auquel n'est rattaché aucun enregistrement de classification est considéré comme file d'attente par défaut.

Étape 3 Cliquez sur **Appliquer**.

Contrôle d'activité WAN

Dans le contrôle d'activité WAN, le mode de contrôle de débit prend en charge huit files d'attente. Chaque file d'attente peut être configurée avec un débit maximal.

Pour configurer le contrôle d'activité WAN, procédez de la façon suivante :

Étape 1 Cliquez sur **QoS > Contrôle d'activité WAN**.

Étape 2 Sélectionnez l'option **Activer le contrôle d'activité du trafic sur les interfaces WAN**.

Étape 3 Dans la table Contrôle d'activité WAN, cliquez sur **Ajouter** pour créer un nouveau contrôle d'activité.

Étape 4 Saisissez ensuite le nom et la description dans les champs prévus à cet effet.

Étape 5 Dans la table, sélectionnez une classe de trafic (**Non spécifiée** ou **Par défaut**) à appliquer à la file d'attente. Les classes de trafic permettent de diriger le trafic vers la file d'attente souhaitée en fonction du service. Par défaut, l'ensemble du trafic correspond à la classe de trafic par défaut.

Étape 6 Dans le champ Débit maximal, saisissez le débit de bande passante maximal de la file d'attente, en pourcentage, pour limiter le trafic entrant du réseau WAN vers le réseau LAN.

Étape 7 Cliquez sur **Appliquer**.

Gestion de la bande passante WAN

Les interfaces WAN peuvent être configurées avec la bande passante maximale fournie par le FAI. Lorsque la valeur (débit de transfert en kbit/s) est configurée, le trafic entrant dans l'interface est mis en forme au débit défini.

Pour configurer la gestion de la bande passante WAN, procédez de la façon suivante :

Étape 1 Cliquez sur **QoS > Gestion de la bande passante WAN**.

Étape 2 Dans la table Gestion de la bande passante WAN, sélectionnez l'interface et configurez les paramètres suivants :

Montant (Kbit/s)	Saisissez le débit de trafic montant, en Kbit/s.
Descendant (Kbit/s)	Saisissez le débit de trafic descendant, en Kbit/s. *Vous devez activer le contrôle d'activité WAN pour la bande passante descendante ; dans le cas contraire, celle-ci ne sera pas prise en compte.
Stratégie de mise en file d'attente sortante	Sélectionnez la stratégie de mise en file d'attente sortante à appliquer à l'interface WAN.
Contrôle d'activités entrantes	Sélectionnez le contrôle d'activités entrantes dans la liste déroulante.

Étape 3 Cliquez sur **Appliquer**.

Classification des commutateurs

Avec les modes QoS tels que Basé sur les ports, Basé sur DSCP et Basé sur CoS, les paquets sont envoyés.

Pour configurer la classification des commutateurs, cliquez sur **QoS > Classification des commutateurs** et procédez comme suit :

Étape 1 Sélectionnez le mode de QoS de commutation (**Basé sur les ports, Basé sur DSCP** ou **Basé sur CoS**).

Basé sur les ports	Paquets entrants sur chaque port LAN mappés sur des files d'attente spécifiques en fonction des mappages. • **File d'attente** : sélectionnez la file d'attente pour mapper le trafic entrant sur les ports LAN individuels.
Basé sur DSCP	Pour le trafic IPv6, DSCP mappe la valeur de classe du trafic dans l'en-tête IPv6 et la place dans des files d'attente différentes. La valeur de classe du trafic est 4 fois supérieure à la valeur DSCP. Par exemple, si un utilisateur configure le paramètre DSCP sur la valeur 10 et la mappe sur la File d'attente 1, les flux IPv6 avec la valeur de classe de trafic 40 sont placés dans la File d'attente 1. Le commutateur doit utiliser le champ DSCP des paquets entrants et planifier la hiérarchisation des paquets dans une file d'attente particulière à l'aide de la table de mappage. • En fonction de la valeur DSCP du paquet entrant, sélectionnez une file d'attente dans la liste déroulante pour mapper le trafic.
Basé sur CoS	Le commutateur utilise les bits du niveau de priorité CoS (classe de service) du paquet entrant et classe le paquet dans la file d'attente configurée par l'utilisateur. • En fonction de la valeur CoS du paquet entrant, sélectionnez une file d'attente dans la liste déroulante pour mapper le trafic.

Étape 2 Cliquez sur **Appliquer**.

Mise en file d'attente des commutateurs

La mise en file d'attente des commutateurs permet de configurer la taille des quatre files d'attente par port en attribuant des tailles à chaque file. La plage de tailles disponibles est comprise entre 1 et 100.

Remarque Si la taille est de 0, la file d'attente possède le niveau de priorité le plus élevé.

Pour configurer la mise en file d'attente des commutateurs, cliquez sur **QoS > Mise en file d'attente des commutateurs** et procédez comme suit :

Étape 1 Dans la zone Mise en file d'attente des commutateurs, sélectionnez la taille appropriée de chacune des files d'attente.

Étape 2 Cliquez sur **Appliquer**.

Étape 3 Cliquez sur **Restaurer les valeurs par défaut** pour restaurer les valeurs par défaut.

CHAPITRE 13

Documentation connexe

Cette section explique où trouver des informations complémentaires sur les produits Cisco.

• Pour en savoir plus, à la page 111

Pour en savoir plus

Assistance

Communauté d'assistance Cisco	http://www.cisco.com/go/smallbizsupport
Assistance et ressources Cisco	http://www.cisco.com/go/smallbizhelp
Coordonnées de l'assistance téléphonique	https://www.cisco.com/c/en/us/support/index.html
Téléchargements de microprogrammes Cisco	https://www.cisco.com/c/en/us/support/index.html Sélectionnez un lien pour télécharger le microprogramme correspondant à votre produit Cisco. Aucune connexion n'est requise.
Demandes Open Source Cisco	Si vous souhaitez recevoir une copie du code source auquel vous avez droit dans le cadre de la ou des licences gratuites ou Open Source (telles que la Licence publique générale/amoindrie GNU), envoyez votre demande à l'adresse : external-opensource-requests@cisco.com. N'oubliez pas de préciser le nom de votre produit Cisco, sa version, ainsi que son numéro de référence à 18 chiffres (par exemple : 7XEEX17D99-3X49X08 1) qui figure dans la documentation Open Source du produit.
Cisco Partner Central (connexion partenaire requise)	http://www.cisco.com/c/en/us/partners.html
Routeur Cisco RV160 Routeur Cisco RV160W	http://www.cisco.com/en/US/products/ps9923/tsd_products_support_series_home.html