



Guide d'administration du routeur RV340W

Première publication: 0

Dernière modification: 0

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 ASSUMENT LA PLEINE RESPONSABILITÉ DE L'UTILISATION QU'ILS FONT DE CES PRODUITS.

LA LICENCE LOGICIELLE ET LA LIMITATION DE GARANTIE APPLICABLES AU PRODUIT FAISANT L'OBJET DE CE MANUEL SONT EXPOSÉES DANS LA DOCUMENTATION LIVRÉE AVEC LE PRODUIT ET INTÉGRÉES À CE DOCUMENT SOUS CETTE RÉFÉRENCE. SI VOUS NE TROUVEZ PAS LA LICENCE LOGICIELLE OU LA LIMITATION DE GARANTIE, DEMANDEZ-EN UN EXEMPLAIRE À VOTRE REPRÉSENTANT CISCO.

Les informations suivantes sont relatives aux appareils de classe A et leur respect de la norme de la FCC : cet appareil a été testé et est conforme aux limites des appareils numériques de classe A, conformément à l'article 15 de la réglementation de la FCC. Ces limites ont pour but de fournir une protection raisonnable contre les interférences nuisibles susceptibles de se produire, lorsque l'équipement est utilisé dans un environnement commercial. Cet équipement génère, utilise et peut émettre de l'énergie radioélectrique. S'il n'est pas installé ni utilisé conformément au manuel d'instructions, il peut provoquer des interférences nuisibles aux communications radio. L'utilisation de cet équipement en zone résidentielle est susceptible de causer du brouillage nuisible, auquel cas les utilisateurs devront corriger le brouillage à leurs propres frais.

Les informations suivantes sont relatives aux appareils de classe B et leur respect de la norme de la FCC : cet appareil a été testé et est conforme aux limites des appareils numériques de classe B, conformément à l'article 15 de la réglementation de la 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 radioélectrique à haute fréquence et, s'il n'est pas installé et utilisé selon le manuel d'instructions, peut provoquer des interférences nuisibles pour les communications radio. Toutefois, rien ne garantit que son utilisation ne provoquera pas d'interférences dans une installation donnée. Si l'équipement provoque des interférences avec la réception radio ou télévisuelle, ce qui peut être déterminé en éteignant l'équipement et en le rallumant, nous encourageons les utilisateurs à tenter de corriger les interférences à l'aide de l'une ou de plusieurs des mesures suivantes :

- Réorientez ou déplacez l'antenne réceptrice.
- Augmentez la distance entre l'équipement et le récepteur.
- Branchez l'équipement sur une prise d'un circuit autre que celui auquel le récepteur est relié.
- Sollicitez l'aide du distributeur ou d'un technicien radio/télévision expérimenté.

Toute modification de ce produit effectuée sans l'autorisation de Cisco est susceptible d'entraîner l'annulation de l'autorisation accordée par la FCC et de rendre caduc votre droit d'utiliser ce produit.

La mise en œuvre Cisco de la compression d'en-tête TCP est l'adaptation d'un programme développé par l'Université de Californie, Berkeley (UCB), dans le cadre de la mise au point, par l'UCB, d'une version gratuite du système d'exploitation UNIX. Tous droits réservés. Droits d'auteur © 1981, Regents of the University of California.

NONOBTANT LES AUTRES GARANTIES MENTIONNÉES, TOUTS LES FICHIERS, DOCUMENTS ET LOGICIELS DE CES FOURNISSEURS SONT FOURNIS « TELS QUELS », AVEC TOUTS LEURS DÉFAUTS. 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.

CISCO OU SES FOURNISSEURS NE SERONT EN AUCUN CAS TENUS RESPONSABLES DES DOMMAGES INDIRECTS, PARTICULIERS, CONSÉCUTIFS OU ACCESSOIRES INCLUANT, SANS RESTRICTIONS, LES PERTES DE PROFITS, LA PERTE OU LA DÉTÉRIORATION DE DONNÉES RÉSULTANT DE L'UTILISATION OU DE L'IMPOSSIBILITÉ D'UTILISER CE MANUEL, MÊME SI CISCO OU SES FOURNISSEURS ONT ÉTÉ AVISÉS DE LA POSSIBILITÉ DE TELS DOMMAGES.

Les adresses IP (Internet Protocol) et les numéros de téléphone utilisés dans ce document sont fictifs. Tous les exemples, résultats d'affichage de commandes, schémas de topologie réseau et autres figures présentés dans ce document sont donnés à titre d'exemple uniquement. L'utilisation d'adresses IP ou de numéros de téléphone réels à titre d'exemple est non intentionnelle et fortuite.

Cisco et le logo Cisco sont des marques commerciales ou déposées de Cisco et/ou de ses filiales aux États-Unis et dans certains autres pays. Pour consulter la liste des marques de Cisco, rendez-vous à l'adresse : <http://www.cisco.com/go/trademarks> Les autres marques commerciales mentionnées dans le présent document sont la propriété de leurs détenteurs respectifs. L'utilisation du terme « partenaire » n'implique pas de relation de partenariat entre Cisco et toute autre entreprise. (1110R)



TABLE DES MATIÈRES

Introduction 1

- Mise en route 1
- Lancer l'Assistant de configuration 3
 - Conseils de dépannage 4
- Interface utilisateur 5

État et statistiques 7

- Récapitulatif du système 7
- Services TCP/IP 9
- Trafic sur les ports 9
- Statistiques de QoS WAN 10
- Statistiques de l'application 11
- Périphériques connectés 12
- État du routage 12
- Liaisons DHCP 12
- Réseau mobile 13
- État du VPN 13
- Afficher les journaux 15

Administration 17

- Redémarrage 17
- Gestion de fichiers 18
 - Mise à niveau manuelle 19
 - Mise à jour automatique 19
- Diagnostic 20
- Licence 21
 - Utilisation des licences intelligentes 21
- Certificat 22
 - Importer le certificat 22
 - Générer un CSR/un certificat 22
- Gestion de la configuration 23

Configuration du système	25
Assistant de configuration initiale	26
Système	27
Heure	27
Journal	28
Serveur de messagerie	29
Serveur Syslog distant	30
E-mail	30
Comptes d'utilisateur	31
Service d'authentification à distance	32
Groupes d'utilisateurs	33
Groupe d'adresses IP	35
SNMP	35
Détection Bonjour	36
LLDP	37
Mises à jour automatiques	37
Gestion des services	38
Horaire	39
Réseau WAN	41
Paramètres WAN	41
Multi-WAN	45
Réseau mobile	46
Configuration du réseau mobile	47
Paramètre de limite de bande passante	47
DNS dynamique	48
DMZ matérielle	48
Transition IPv6	49
Tunnel IPv6 en IPv4 (6in4)	49
Déploiement IPv6 rapide (6rd)	50
QoS	51
Classes de trafic	51
Mise en file d'attente WAN	52
Contrôle d'activité WAN	53
Gestion de la bande passante WAN	53
Classification des commutateurs	54

Mise en file d'attente des commutateurs	55
Réseau local	57
Paramètres des ports	57
Paramètres VLAN	58
Paramètres LAN/DHCP	59
DHCP statique	62
Configuration 802.1X	62
Base de données locale DNS	63
Annonce de routeur	63
Technologie sans fil	65
Paramètres de base	65
Configuration de la fréquence 2,4 GHz	69
Configuration de la fréquence 5 GHz	70
Paramètres avancés	70
Portail captif	72
WPS	74
Routage	75
Proxy IGMP	75
RIP	76
Routage statique	77
Pare-feu	79
Paramètres de base	79
Règles d'accès	81
Traduction des adresses réseau	82
NAT statique	83
Redirection de ports	83
Déclenchement de ports	84
Délai d'expiration de session	85
Hôte DMZ	86
VPN	87
Assistant de configuration VPN (site à site)	87
Profils IPsec	90
Site à site	92
Création d'une connexion VPN site à site	93
Création d'un tunnel GRE sécurisé	96

- Client à site 98
- Client VPN télétravailleur 102
- Serveur PPTP 104
- Serveur L2TP 104
- VPN SSL 105
- Intercommunication VPN 108
- Sécurité 109**
 - Assistant de contrôle d'application 109
 - Contrôle d'application 110
 - Filtrage Web 111
 - Filtrage de contenu 112
 - Protection de la source IP 113
- Pour en savoir plus 115**
 - Pour en savoir plus 115



CHAPITRE

1

Introduction

Merci d'avoir choisi le routeur Cisco RV340W. Ce manuel vous explique comment installer et gérer votre routeur. Ce chapitre contient des informations qui vous seront utiles pour commencer à utiliser votre périphérique. Le routeur Cisco RV340W a été configuré en usine. Votre fournisseur d'accès à Internet (FAI) peut néanmoins vous demander de modifier ces paramètres. Vous pouvez pour cela utiliser un navigateur Web tel qu'Internet Explorer (version 10 ou ultérieure), Firefox, ou Chrome (pour un PC) ou Safari (pour un Mac).

Cette section contient les rubriques suivantes :

- [Mise en route, page 1](#)
- [Lancer l'Assistant de configuration, page 3](#)
- [Interface utilisateur, page 5](#)

Mise en route

La section suivante décrit les tâches de configuration les plus courantes sur votre périphérique. Pour démarrer le routeur, 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.
- 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**.

- Remarque** Lors du démarrage du système, le voyant d'alimentation continue progressivement de clignoter jusqu'à la fin du démarrage.
- Au démarrage, les voyants PWR, LINK/ACT et GIGIBIT de LAN 1 clignotent. À 25 % du démarrage, les voyants PWR, LINK/ACT et GIGIBIT de LAN 1 et 2 clignotent. À 50 % du démarrage, les voyants PWR, LINK/ACT et GIGIBIT de LAN 1, 2 et 3 clignotent. À 75 % du démarrage, les voyants PWR, LINK/ACT et GIGIBIT de LAN 1, 2, 3 et 4 clignotent.
- La durée de démarrage du système est normalement inférieure à 3 minutes. Si le routeur est correctement configuré et que tous les paramètres de configuration sont définis sur les valeurs maximales, le démarrage complet du système peut prendre jusqu'à 7 minutes.

Tableau 1: Description des DEL du routeur

PWR	<p>Éteint lorsque l'appareil est hors tension.</p> <p>Vert continu lorsque l'unité est sous tension et a démarré.</p> <p>Clignote en vert lorsque l'appareil est en cours de démarrage.</p>
DIAG	<p>Éteint lorsque le système est sur le point de démarrer.</p> <p>Clignote lentement en rouge (1 Hz) lorsque la mise à niveau du microprogramme est en cours.</p> <p>Clignote rapidement en rouge (3 Hz) lorsque la mise à niveau du microprogramme a échoué.</p> <p>Rouge continu lorsque le système n'a pas pu démarrer avec à la fois une image active et inactive ou en mode sauvetage.</p>
LINK/ACT de WAN1, WAN2 et LAN1-4	<p>Éteint lorsqu'il n'y a pas de connexion Ethernet.</p> <p>Vert continu lorsque la liaison Ethernet GE est active.</p> <p>Vert clignotant lorsque la liaison Ethernet GE envoie ou reçoit des données.</p>
GIGABIT de WAN1, WAN2 et LAN1-4	<p>Vert continu pour un débit de 1 000 Mbit.</p> <p>Éteint pour les débits de moins de 1 000 Mbit.</p>
DMZ	<p>Vert continu lorsque le DMZ est activé.</p> <p>Éteint lorsque le DMZ est désactivé.</p>
VPN	<p>Éteint lorsqu'aucun tunnel VPN n'est défini ou lorsque tous les VPN définis ont été désactivés.</p> <p>Vert continu lorsqu'au moins un tunnel VPN est actif.</p> <p>Vert clignotant lors de l'envoi ou de la réception de données via le tunnel VPN.</p> <p>Orange continu lorsqu'aucun tunnel VPN n'est actif.</p>

USB1 et USB2	<p>Éteint lorsqu'aucun périphérique USB n'est connecté, ou qu'un périphérique USB est inséré sans être reconnu.</p> <p>Vert continu quand le dongle USB est connecté au FAI. La clé USB est reconnue.</p> <p>Vert clignotant lors de l'envoi ou de la réception de données.</p> <p>Orange continu quand le dongle USB est reconnu mais que la connexion au FAI a échoué (aucune adresse IP n'est affectée.) Ou en cas d'erreur d'accès de la clé USB.</p>
Réinitialiser	<p>Pour redémarrer le routeur, appuyez sur le bouton Reset pendant moins de dix secondes à l'aide d'un trombone ou de la pointe d'un stylo.</p> <p>Pour rétablir les paramètres par défaut définis en usine, appuyez sur le bouton Reset et maintenez-le enfoncé pendant 10 secondes.</p>
Technologie sans fil	<p>Le voyant est allumé quand le point d'accès interne est activé.</p> <p>Il est éteint quand le point d'accès interne est désactivé.</p>

Lancer l'Assistant de configuration

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

Pour ouvrir cette page, sélectionnez Lancer l'Assistant de configuration dans l'arborescence 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

Assistant de configuration initiale	Permet d'accéder à la page Assistant de configuration initiale .
Assistants de configuration du VPN	Permet d'accéder à la page Assistant d'état du VPN .
Assistant de contrôle d'application	Permet d'accéder à la page Assistant de contrôle d'application .

Configurations initiales

Modifier le mot de passe de l'administrateur	Permet d'accéder à 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	Permet d'accéder à la page Paramètres WAN , où vous pouvez modifier les paramètres WAN.
Configurer les paramètres USB	Permet d'accéder à la page Réseau mobile , où vous pouvez modifier les configurations USB.
Configurer les paramètres LAN	Permet d'accéder à la page Appartenance VLAN , où vous pouvez configurer le réseau VLAN.

Accès rapide

Mettre à niveau le microprogramme du routeur	Permet d'accéder à la page Gestion de fichiers , où vous pouvez mettre à jour le microprogramme du périphérique.
Configurer l'accès pour la gestion à distance	Permet d'accéder à la page Pare-feu > Paramètres de base , où vous pouvez activer les fonctions de base du périphérique.
Sauvegarder la configuration du périphérique	Permet d'accéder à la page Gestion de la configuration , où vous pouvez gérer la configuration du routeur.

État du périphérique

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

Conseils de dépannage

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 le périphérique. 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.

Interface utilisateur

L'interface utilisateur est conçue pour faciliter la configuration et la gestion de votre périphérique.

Navigation

Les principaux modules de l'interface Web sont représentés par des boutons à gauche du volet de navigation. Cliquez sur un bouton pour afficher d'autres options. Cliquez sur une option pour ouvrir une page.

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.

Aide

Pour afficher des informations sur la page de configuration sélectionnée, cliquez sur **Aide** dans l'angle supérieur droit de l'interface Web. Si un message d'avertissement concernant la fenêtre contextuelle s'affiche sur votre navigateur Web, autorisez le contenu bloqué.

Déconnexion

Pour quitter l'interface Web, cliquez sur **Déconnexion** dans l'angle supérieur droit de l'interface Web. La page de connexion s'affiche.



CHAPITRE 2

État et statistiques

Cette section décrit les divers paramètres de configuration de votre périphérique. Elle contient les rubriques suivantes :

- [Récapitulatif du système, page 7](#)
- [Services TCP/IP, page 9](#)
- [Trafic sur les ports, page 9](#)
- [Statistiques de QoS WAN, page 10](#)
- [Statistiques de l'application, page 11](#)
- [Périphériques connectés, page 12](#)
- [État du routage, page 12](#)
- [Liaisons DHCP, page 12](#)
- [Réseau mobile, page 13](#)
- [État du VPN, page 13](#)
- [Afficher les journaux, page 15](#)

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 réseaux mobiles et les paramètres du serveur VPN. Pour afficher la section Récapitulatif du système, cliquez sur **État et statistiques > Récapitulatif du système**.

Informations système

- **Nom d'hôte** : nom de l'hôte.
- **Numéro de série** : numéro de série du périphérique.
- **Temps de disponibilité du système** : durée (au format aa-mm-jj, heures et minutes) durant laquelle le périphérique est resté actif.

- **Heure actuelle** : heure et date actuelles.
- **PID VID** : numéro de version du matériel.

Informations sur le microprogramme

- **Version du microprogramme** : numéro de version du microprogramme installé.
- **Somme de contrôle MD5 du microprogramme** : valeur utilisée à des fins de validation des fichiers.

État des ports

- **ID du port** : nom défini et numéro de port.
- **Interface** : nom du port utilisé pour la connexion.
- **Activé** : état du port.
- **Vitesse** : vitesse (en Mbit/s) du périphérique après la négociation automatique.

IPv4 et IPv6

- **Interface** : nom de l'interface.
- **Adresse IP** : adresse IP attribuée à l'interface.
- **Passerelle par défaut** : passerelle par défaut de l'interface.
- **DNS** : adresse IP du serveur DNS.
- **DNS dynamique** : adresse IP du serveur DDNS de l'interface (paramètre désactivé ou activé).
- **Renouveler** : cliquez sur cette option pour renouveler l'adresse IP.
- **Libérer** : cliquez sur cette option pour libérer l'interface.

État du VPN

- **Type** : type de tunnel VPN.
- **Actif** : **Activé** ou **Désactivé**.
- **Configuré** : état du tunnel VPN, que ce dernier soit ou pas configuré.
- **Nombre maximal de sessions prises en charge** : nombre maximal de tunnels pris en charge sur le périphérique.
- **Session connectée** : état du tunnel.

État des paramètres du pare-feu

- **SPI (Inspection dynamique des paquets)** : également connue sous le nom de « filtrage dynamique des paquets », cette fonction contrôle l'état des connexions actives et utilise ces informations pour déterminer les paquets réseau autorisés par le pare-feu.
- **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 périphériques Internet ; elle permet également d'éviter que d'autres utilisateurs Internet puissent détecter le réseau.
- **Gestion à distance** : cette fonction indique si une connexion à distance pour gérer le périphérique est autorisée ou refusée.
- **Règle d'accès** : cette fonction indique le nombre de règles d'accès ayant été définies.

État des paramètres du journal

- **Serveur Syslog** : 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

- **Protocole** : type de protocole utilisé pour la communication.
- **Adresse IP d'écoute** : adresse IP d'écoute sur le périphérique.
- **Port d'écoute** : port d'écoute sur le périphérique.

État de la 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 du périphérique connecté.
- **Port externe** : port du périphérique 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** : nom défini et numéro de 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.
- **Actualiser** : actualisation des statistiques affichées.
- **Réinitialiser les compteurs** : remise à zéro de toutes les valeurs.

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) du périphérique 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**), il détecte le mode duplex et, si la connexion nécessite une détection automatique, choisit automatiquement la configuration MDI ou MDIX qui correspond à l'autre extrémité de la liaison.

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** : nom de l'interface.
- **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 envoyés** : nombre de paquets entrants de la classe de trafic envoyés.
- **Paquets rejetés** : nombre de paquets entrants rejetés.

Statistiques de l'application

La page Statistiques de l'application présente les données d'utilisation du routeur. Pour afficher la page Statistiques de l'application, cliquez sur **État et statistiques > Statistiques de l'application**.

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

Applications principales par catégorie

- **Catégorie** : liste des catégories d'applications auxquelles vous accédez.
- **Volume de trafic** : volume de trafic, en mégaoctets.

Applications principales par nom

- **Applications** : liste des applications auxquelles vous accédez.
- **Volume de trafic** : volume de trafic, en mégaoctets.

Locuteurs principaux

- **Locuteurs** : liste des adresses IP auxquelles vous accédez.
- **Volume de trafic** : volume de trafic, en mégaoctets.

Locuteurs principaux par type de périphérique

- **Périphérique** : liste des périphériques auxquels vous accédez.
- **Volume de trafic** : volume de trafic, en mégaoctets.

Locuteurs principaux par type de système d'exploitation

- **OS** : liste des systèmes d'exploitation utilisés.
- **Volume de trafic** : volume de trafic, en mégaoctets.



Remarque

Une fenêtre contextuelle indiquant que la solution AVC est désactivée ou que la licence a expiré peut s'afficher.

Périphériques connectés

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

IPv4

- **Nom d'hôte** : nom du périphérique connecté.
- **Adresse IPv4** : adresse IP du périphérique connecté.
- **Adresse MAC** : adresse MAC du périphérique connecté.
- **Type** : type d'adresse IP du périphérique.
- **Interface** : interface à laquelle le périphérique est connecté.

IPv6

- **Adresse IPv6** : adresse IPv6 du périphérique connecté.
- **Adresse MAC** : adresse MAC du périphérique connecté.

État du 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 du périphérique pour IPv4 et IPv6, cliquez sur **État et statistiques > État du routage**.

Routes IPv4 et IPv6

- **Destination** : adresse IP et masque de sous-réseau de la connexion.
- **Saut suivant** : adresse IP du saut suivant. Nombre maximal de sauts (15 sauts maximum) par lesquels transite un paquet.
- **Métrique** : nombre d'algorithmes de routage lors de la détermination de la route optimale pour l'envoi du trafic réseau.
- **Interface** : nom de l'interface à laquelle la route est liée.
- **Source** : source de la route.

Liaisons DHCP

La page Liaisons DHCP fournit des informations statistiques sur le client DHCP, telles que l'adresse IP, 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**.

La table de liaisons DHCP fournit les renseignements suivants :

- **Adresse IPv4** : adresse IP attribuée.
- **Adresse MAC** : adresse MAC de l'adresse IP attribuée au client.
- **Expiration du bail** : durée du bail du système du client.
- **Type** : état de la connexion (**Statique** ou **Dynamique**).

Réseau mobile

Les réseaux mobiles permettent à un routeur et à ses sous-réseaux de devenir mobiles tout en maintenant la connectivité IP aux hôtes IP qui se connectent au réseau via ce routeur mobile. Pour afficher le réseau mobile du routeur, cliquez sur **État et statistiques > Réseau mobile**. Sélectionnez ensuite les interfaces dans la liste déroulante (**USB1** ou **USB2**). Cliquez sur **Actualiser** pour actualiser l'état du réseau mobile.

Connexion

- **Adresse IP Internet** : adresse IP fournie par le fournisseur d'accès.
- **Masque de sous-réseau** : masque fourni par le fournisseur d'accès.
- **Passerelle par défaut** : passerelle par défaut fournie par le fournisseur d'accès.
- **Temps de disponibilité de la connexion** : durée d'utilisation du périphérique connecté.
- **Utilisation de la session d'accès à distance actuelle** : utilisation des données par session.
- **Utilisation mensuelle** : utilisation mensuelle des données.

État de la carte de données

- **Fabricant** : fabricant du périphérique.
- **Microprogramme de la carte** : version du microprogramme fourni par le fabricant.
- **État de la carte SIM** : état de la carte SIM.
- **IMSI** : numéro unique attribué au périphérique.
- **Porteuse** : nom ou type de porteuse de données.
- **Type de service** : type de service de données.
- **Force du signal** : intensité du signal de données.
- **État de la carte** : état de la carte (déconnectée ou connectée).

État du VPN

La page État du VPN indique l'état du tunnel des clients site à site, client à site, VPN SSL, PPTP, L2TP et VPN télétravailleur. Pour afficher la page État du VPN du périphérique, 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 (reportez-vous à la section [Site à site](#), à la page 92). 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 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 (reportez-vous à la section [Client à site](#), à la page 98).

La **Table des connexions** fournit les informations suivantes :

- **Nom du groupe ou du 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.

État du VPN SSL

Un réseau privé virtuel Secure Sockets Layer (VPN SSL) permet aux utilisateurs d'établir un tunnel VPN d'accès à distance sécurisé avec ce périphérique à l'aide d'un navigateur Web. Le VPN SSL offre un accès facile et sécurisé à un grand nombre de ressources et applications Web à partir de quasiment tous les ordinateurs connectés à Internet. Vous pouvez afficher l'état des tunnels VPN SSL.

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

La **Table des connexions** indique l'état des tunnels établis. Vous pouvez également ajouter, modifier ou supprimer les connexions.

- **Nom de la stratégie** : nom de la stratégie appliquée sur le tunnel.
- **Session** : nombre de sessions.

Vous pouvez également ajouter, modifier ou supprimer un VPN SSL (reportez-vous à la section [VPN SSL](#), à la page 105).

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 ces connexions.

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

État du tunnel 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. Vous pouvez afficher l'état du tunnel L2TP.

- **Tunnel(s) utilisé(s)** : tunnels L2TP utilisés pour la connexion VPN.
- **Tunnel(s) disponible(s)** : tunnels disponibles pour la connexion L2TP.

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

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

Afficher les 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	<p>Cliquez sur l'une des options d'affichage suivantes :</p> <ul style="list-style-type: none"> • 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 28.

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.



Administration

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

- [Redémarrage, page 17](#)
- [Gestion de fichiers, page 18](#)
- [Diagnostic, page 20](#)
- [Licence, page 21](#)
- [Certificat, page 22](#)
- [Gestion de la configuration, page 23](#)

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** ou **Image inactive x.x.xx.xx**) dans la liste déroulante.
- Étape 3** Sélectionnez l'option de redémarrage de votre choix.
- Redémarrez le périphérique.
 - 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.
-

Gestion de 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 de 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 mise à jour** : date de la dernière mise à jour du microprogramme.
- **Dernière version disponible sur Cisco.com** : dernière version du microprogramme.
- **Dernière vérification** : date de la dernière vérification.

Signature

- **Version actuelle de la signature** : version de la signature.
- **Dernière mise à jour** : date de la dernière mise à jour.
- **Dernière version disponible sur Cisco.com** : dernière version de la signature.
- **Dernière vérification** : date de la dernière vérification.

Pilote du dongle USB

- **Version actuelle du pilote du dongle** : version du pilote du dongle USB intégré.
- **Dernière mise à jour** : date de la dernière mise à jour.
- **Dernière version disponible sur Cisco.com** : dernière version du pilote du dongle.
- **Dernière vérification** : date de la dernière vérification.

Module linguistique

- **Version actuelle du module linguistique** : version du module linguistique.
- **Dernière mise à jour** : date de la dernière mise à jour.
- **Dernière version disponible sur Cisco.com** : dernière version du module linguistique.
- **Dernière vérification** : date de la dernière vérification.

Mise à niveau manuelle

La section Mise à niveau manuelle vous permet de charger et d'effectuer des mises à niveau vers une version plus récente du microprogramme, du fichier de signature, du pilote du dongle USB ou du fichier de langue.

Avertissement Lors d'une mise à niveau du microprogramme, n'essayez pas de naviguer en ligne, n'éteignez pas le périphérique, 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 appliquez 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 (**Image du microprogramme, Fichier de signature, Pilote du dongle USB ou Fichier de langue**).
- Étape 3** Dans la section Mise à niveau depuis, sélectionnez une option (**Cisco.com, PC ou USB**) et cliquez sur **Actualiser**.
- 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 repli automatique du microprogramme

Le routeur comprend deux images de microprogramme dans le flash pour fournir un mécanisme de repli automatique afin que le périphérique puisse passer automatiquement au microprogramme secondaire lorsque le microprogramme actif est corrompu ou ne peut pas démarrer correctement après cinq essais.

Le mécanisme de repli automatique fonctionne comme suit:

- 1 Le routeur démarre d'abord avec le microprogramme actif.
- 2 Si le microprogramme est corrompu, il passera automatiquement au microprogramme secondaire après que le microprogramme actif n'aura pas démarré après 5 fois. Si le routeur est coincé ne redémarre pas automatiquement, vous pouvez éteindre l'alimentation, réallumer, attendez 30 secondes, puis éteignez l'alimentation, pour 5 fois pour passer au microprogramme secondaire ou inactif.
- 3 Après le démarrage avec le microprogramme secondaire ou inactif, vérifiez s'il n'y a pas de problème avec le microprogramme actif.
- 4 Rechargez le nouveau microprogramme si nécessaire.

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.

Utilisation de l'utilitaire Ping ou Traceroute

Vous pouvez utiliser l'utilitaire Ping ou Traceroute pour tester la connectivité entre ce routeur et un autre périphérique sur le réseau. Pour utiliser l'utilitaire Ping ou Traceroute, procédez de la façon suivante :

-
- Étape 1** Sélectionnez **Administration > Diagnostic**.
 - Étape 2** Dans la section Exécuter un test Ping ou Traceroute sur une adresse IP, saisissez une adresse IP ou un nom de domaine dans le champ Adresse IP/Nom de domaine.
 - Étape 3** Cliquez sur **Ping**. Les résultats de la requête ping s'affichent. Ils vous indiquent si le périphérique est accessible. Vous pouvez également cliquer sur **Traceroute**. Les résultats du test Traceroute s'affichent.
 - Étape 4** Pour lancer une recherche DNS, saisissez l'adresse IP ou le nom de domaine dans le champ Effectuer une recherche DNS > Adresse IP/Nom de domaine, puis cliquez sur **Rechercher**.
-

Licence

La section Licence vous permet de configurer les licences ou d'enregistrer le routeur. Elle simplifie l'utilisation du logiciel Cisco et vous permet de mieux comprendre son mode de fonctionnement.

État des licences du logiciel intelligent

La section État des licences du logiciel intelligent fournit des informations sur les licences du périphérique.

État de l'enregistrement : Enregistré ou Non enregistré, et date de l'enregistrement.

État d'autorisation de la licence : Autorisée, Mode d'évaluation, Non conforme, Autorisation expirée ou Période d'évaluation expirée, et date d'autorisation de la licence.

Fonctionnalité d'exportation contrôlée : fonction désactivée par défaut.

Utilisation des licences intelligentes

Vous pouvez sélectionner la licence intelligente à utiliser pour le routeur. Assurez-vous de disposer de licences suffisantes pour le routeur dans le compte virtuel.

Pour configurer les licences intelligentes, procédez de la façon suivante :

-
- Étape 1** Sous Utilisation des licences intelligentes, cliquez sur **Sélectionner des licences**.
 - Étape 2** Sélectionnez les licences applicables et saisissez une valeur dans le champ **Nombre**.
 - Étape 3** Cliquez sur **Enregistrer**.
 - Étape 4** Lorsque la fenêtre contextuelle Renouvellement d'autorisation des licences s'affiche, cliquez sur **OK**.
-

Certificat

Les certificats sont essentiels dans le processus de communication. Un certificat signé par 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 auto-signé, local et CSR. Vous pouvez également importer un certificat CA, local ou PKCS#12. Vous pouvez par ailleurs importer un fichier de certificat (à partir d'un ordinateur ou d'une clé USB) dans un nouveau certificat.

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 local
 - Certificat CA
 - 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** Sélectionnez **Importer depuis un ordinateur**, puis cliquez sur **Choisir un fichier** 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** Cliquez sur **Charger**.
-

Générer un CSR/un certificat

-
- Étape 1** Cliquez sur **Générer un CSR/un certificat**.
- Étape 2** Sélectionnez le type de certificat à générer dans la liste déroulante :
- 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	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 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**.

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

La section Nom du fichier de configuration indique l'heure de dernière modification des paramètres suivants :

- Configuration de fonctionnement
- Configuration de démarrage
- Configuration miroir
- Configuration de sauvegarde

Copier/appliquer la configuration

La section Copier/appliquer la configuration fournit des renseignements sur la configuration par défaut du périphérique 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.

- **Nom du fichier source** : sélectionnez le nom du fichier source dans la liste déroulante.

- **Nom du fichier de destination** : sélectionnez le nom du fichier de destination dans la liste déroulante.
- **Clign. icône d'enregistrement** : indique si une icône clignote lorsque certaines données ne sont pas enregistrées. Pour activer/désactiver cette fonction, cliquez sur **Désactiver clignotement icône d'enr.**



Configuration du système

L'assistant de configuration système vous guide lors de l'installation et de la configuration du routeur. Cette section contient les rubriques suivantes :

- [Assistant de configuration initiale, page 26](#)
- [Système, page 27](#)
- [Heure, page 27](#)
- [Journal, page 28](#)
- [E-mail, page 30](#)
- [Comptes d'utilisateur, page 31](#)
- [Groupes d'utilisateurs, page 33](#)
- [Groupe d'adresses IP, page 35](#)
- [SNMP, page 35](#)
- [Détection Bonjour, page 36](#)
- [LLDP, page 37](#)
- [Mises à jour automatiques, page 37](#)
- [Gestion des services, page 38](#)
- [Horaire, page 39](#)

Assistant de configuration initiale

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 > Assistant de configuration initiale**.

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 Sélectionnez l'interface dans la liste déroulante.

Étape 4 Cliquez sur **Suivant**.

Étape 5 Sous **Configuration du routeur – Sélectionner le type de connexion**, sélectionnez votre type de connexion Internet.

Étape 6 Si vous sélectionnez **IP dynamique** ou **DHCP**, cliquez sur **Suivant**.

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

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 l'adresse IP du DNS.

Étape 8 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 9 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.
Serveur distant	Saisissez le serveur distant.
DNS	Saisissez l'adresse IP du DNS.

Étape 10 Sélectionnez le fuseau horaire du routeur dans le menu déroulant Fuseau horaire.

Étape 11 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. Saisissez la date et l'heure.

Étape 12 Cliquez sur **Suivant**.

Étape 13 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 14 Cliquez sur **Suivant**.

Étape 15 Dans la section Récapitulatif, vérifiez vos paramètres et cliquez sur **Soumettre**.

Systeme

Votre FAI peut attribuer un nom d'hôte et un nom de domaine pour identifier votre périphérique ou vous demander de les spécifier vous-même. Dans ce cas, vous pouvez modifier les valeurs par défaut en fonction de vos besoins. Procédez comme suit pour attribuer un nom d'hôte et un nom de domaine.

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

Étape 2 Dans le champ Nom d'hôte, saisissez un nom d'hôte.

Étape 3 Dans le champ Nom de domaine, saisissez un nom de domaine.

Étape 4 Cliquez sur **Appliquer**.

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 à l'heure de Greenwich (GMT).
- Étape 3** **Définir la date et l'heure** : sélectionnez **Auto** ou **Manuel**.
- a) **Auto** : cochez la case **Par défaut** ou **Défini par l'utilisateur** et saisissez un nom de serveur NTP qualifié.
- b) **Manuel** : saisissez la date et l'heure.
- Étape 4** **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 5** 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 serveur syslog 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.
Licence	Journaux impliquant des violations de licence.
Système	Journaux liés à des applications d'espace utilisateur (par exemple, NTP, Session et DHCP).
Filtre Web	Journaux liés à des événements ayant déclenché le filtrage Web.
Pare-feu	Journaux liés aux règles de pare-feu, attaques et filtrage de contenu.
Contrôle d'application	Journaux liés au contrôle d'application.
Réseau	Journaux liés au routage, à DHCP, au WAN, au LAN, et à la QoS.
Utilisateurs	Journaux liés aux activités des utilisateurs.
VPN	Journaux liés au VPN, y compris aux instances telles que l'échec de l'établissement du tunnel VPN, l'échec de la passerelle VPN, etc.
3G/4G	Journaux des dongles 3G/4G raccordés au routeur.
SSLVPN	Journaux liés au VPN SSL.

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 **Serveur de messagerie**, cochez la case **Envoyer les Syslogs par e-mail** de façon à ce que le routeur puisse envoyer des alertes par e-mail lors de la journalisation d'événements.
- 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.
-

Serveur Syslog distant

Un serveur Syslog distant permet de séparer le logiciel qui génère les messages et les événements du système qui les stocke et les analyse. Lorsque vous activez ce serveur, le pilote réseau envoie des messages à un serveur Syslog sur l'Intranet local ou sur Internet via un tunnel VPN. Il est possible de configurer le serveur Syslog en spécifiant le nom ou l'adresse IP.

-
- Étape 1** Dans la section **Serveur Syslog**, cochez la case **Activer** pour activer l'envoi de journaux système à un serveur distant.
- Étape 2** Dans le champ **Serveur Syslog 1**, saisissez l'adresse IP d'un serveur Syslog auquel envoyer les messages de journaux.
- Étape 3** Dans le champ **Serveur Syslog 2**, saisissez l'adresse IP d'un serveur Syslog 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 e-mail	Sélectionnez Aucun ou TLS/SSL comme méthode de cryptage.
Authentification	Sélectionnez le type d'authentification dans la liste déroulante : Aucun, Connexion, Texte en clair ou MD5 .
Envoyer un e-mail à 1	Saisissez l'adresse e-mail du destinataire.
Envoyer un 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 **Tester la connectivité au serveur de messagerie** pour tester la connectivité.

Étape 4 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, la connexion à l'interface Web graphique (GUI) et le VPN SSL. Les administrateurs sont ainsi en mesure de contrôler et d'autoriser uniquement les utilisateurs locaux à accéder au réseau.

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 Sous **Complexité des mots de passe des utilisateurs locaux**, cochez la case **Activer** pour activer la complexité des mots de passe.

Étape 3 Configurez les paramètres de complexité des mots de passe.

Longueur minimale du mot de passe	Saisissez la longueur minimale du mot de passe pour créer un nouveau mot de passe (plage comprise entre 0 et 64, valeur par défaut 8).
Nombre minimum de classes de caractères	Saisissez le nombre minimum de classes de caractères devant être utilisées pour le nouveau mot de passe (plage comprise entre 0 et 4, valeur par défaut 3). Composez un mot de passe à l'aide de trois des quatre classes suivantes : lettres majuscules, lettres minuscules, chiffres et caractères spéciaux.
Le nouveau mot de passe doit être différent de l'actuel	Activez cette option pour demander à l'utilisateur de saisir un mot de passe différent lors de l'expiration du mot de passe actuel.

Étape 4 Dans la table **Liste d'appartenance des utilisateurs locaux**, cliquez sur **Ajouter** pour ajouter un utilisateur sur le routeur.

Étape 5 Dans la page **Ajouter un compte d'utilisateur**, saisissez les informations suivantes :

Nom d'utilisateur	Saisissez un nom d'utilisateur.
Nouveau mot de passe	Saisissez un mot de passe.
Confirmer le nouveau mot de passe	Confirmez le mot de passe.
Mesure de la fiabilité du mot de passe	Indique la fiabilité du mot de passe.
Groupe	Sélectionnez un groupe (admin ou invité) dans la liste déroulante.

Étape 6 Cliquez sur **Appliquer**.

Étape 7 Cliquez sur **Modifier** ou sur **Supprimer** pour modifier ou supprimer un utilisateur existant.

Étape 8 Sur la page **Modifier le compte d'utilisateur**, saisissez les informations suivantes :

Ancien mot de passe	Saisissez l'ancien mot de passe.
Nouveau mot de passe	Saisissez le nouveau mot de passe.
Confirmer le nouveau mot de passe	Confirmez le mot de passe.
Groupe	Sélectionnez un groupe (admin ou invité) dans la liste déroulante.

Étape 9 Cliquez sur **Appliquer**.

Étape 10 Cliquez sur **Importer**, puis sur **Choisir un fichier** pour importer un fichier CSV de noms d'utilisateur et de mots de passe.

Étape 11 Cliquez sur **Télécharger la grille utilisateur** pour télécharger la grille utilisateur.

Service d'authentification à distance

Pour permettre l'authentification de l'utilisateur externe à l'aide de RADIUS et de LDAP, utilisez le service d'authentification à distance.

Étape 1 Sous la table **Service d'authentification à distance**, cliquez sur **Ajouter** et configurez les paramètres suivants :

Nom	Donnez un nom au domaine.
------------	---------------------------

Type d'authentification	<p>Sélectionnez un type d'authentification dans la liste déroulante.</p> <ul style="list-style-type: none"> • 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. • LDAP : protocole LDAP (Lightweight Directory Access Protocol).
Serveur principal	<p>Saisissez l'adresse IP du serveur principal. Port : saisissez le port principal du serveur.</p>
Serveur de secours	<p>Saisissez l'adresse IP du serveur de secours. Port : saisissez le port de secours du serveur.</p>
Clé prépartagée	<p>Si vous avez sélectionné RADIUS comme type d'authentification, saisissez la clé prépartagée du serveur RADIUS.</p>
Confirmer la clé prépartagée	<p>Saisissez de nouveau la clé prépartagée du serveur RADIUS pour la confirmer.</p>

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 EzVPN/tiers, le VPN SSL, le VPN PPTP/L2TP 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 la connexion Web, PPTP, L2TP et EzVPN.

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

- Étape 1** Cliquez sur **Configuration système > Groupes d'utilisateurs**.
- Étape 2** Sous la table 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 des utilisateurs locaux, cochez les cases souhaitées dans la colonne Joindre pour joindre la liste d'utilisateurs au groupe.
- Étape 5** Sous Services, sélectionnez les services auxquels doivent avoir accès les groupes d'utilisateurs et saisissez les informations suivantes.

Connexion Web	<p>Spécifiez les autorisations de connexion Web accordées aux utilisateurs rattachés au groupe :</p> <ul style="list-style-type: none"> • Désactivé : 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 modifier aucun paramètre. • Administrateur : tous les membres du groupe d'utilisateurs disposent de privilèges complets pour configurer et lire l'état système.
VPN site à site	<p>Cochez la case Autoriser dans ce groupe pour autoriser l'accès à une stratégie VPN site à site.</p> <ul style="list-style-type: none"> • Cliquez sur Ajouter pour ouvrir la fenêtre Ajouter une liste de fonctions. • Sélectionnez un profil dans la liste déroulante et cliquez sur Ajouter.
EzVPN/Tiers	<p>Cochez la case Autoriser dans ce groupe pour autoriser l'accès à une stratégie VPN site à site.</p> <ul style="list-style-type: none"> • Cliquez sur Ajouter pour ouvrir la fenêtre Ajouter une liste de fonctions. • Sélectionnez un profil dans la liste déroulante et cliquez sur Ajouter.
VPN SSL	Sélectionnez un profil dans la liste déroulante.
VPN PPTP	Cochez la case Autoriser pour autoriser l'authentification PPTP.
L2TP	Cochez la case Autoriser pour autoriser l'authentification L2TP.
802.1x	Cochez la case Autoriser pour autoriser l'authentification 802.1x.

- 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.

Groupe 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 > Groupe d'adresses IP**.

Étape 2 Dans la **Table des 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.

Protocole	Sélectionnez IPv4 ou IPv6 dans la liste déroulante.
Type et détails de l'adresse	<p>Sélectionnez le type de groupe dans la liste déroulante et saisissez les détails de l'adresse :</p> <ul style="list-style-type: none"> • Adresse IP : saisissez une adresse IP. • Sous-réseau de l'adresse IP : saisissez une adresse IP dans le champ correspondant et son masque de sous-réseau dans le champ Masque. • Plage d'adresses IP : saisissez l'adresse IP de début et l'adresse IP de fin.

Étape 4 Cliquez sur **Appliquer**.

SNMP

Le protocole SNMP (Simple Network Management Protocol) est un protocole Internet standard permettant de collecter et d'organiser les informations sur les périphériques gérés sur des réseaux IP, mais aussi de modifier ces informations en vue de changer le comportement des périphériques.

Étape 1 Pour configurer SNMP, 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.

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. Cet utilitaire détecte les périphériques 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 cet utilitaire, 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 dans Internet Protocol Suite, qui est utilisé par des périphériques 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 de paramètres 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** Pour afficher les détails concernant un port LLDP, sélectionnez le port local et cliquez sur **Détails**.
- Étape 7** Pour actualiser la Table de paramètres des voisins LLDP, cliquez sur **Actualiser**.
-

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 donc 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 (à savoir **Jamais, Semaine** ou **Mois**). Cliquez sur **Rechercher maintenant** pour lancer une recherche.
- Étape 3** Dans le champ **Notifier par**, sélectionnez E-mail 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**, sélectionnez **Notifier** pour recevoir des notifications de mise à jour.
- Étape 5** Dans la liste déroulante, sélectionnez l'heure de mise à jour automatique du microprogramme. Vous pouvez choisir de recevoir des notifications et de configurer les mises à jour pour les programmes suivants :
- Microprogramme du système
 - Microprogramme du modem USB
 - Signature de sécurité
- 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 de l'application**, saisissez le nom du service à des fins d'identification et de gestion.
- Étape 4** Dans le champ Protocole, sélectionnez le protocole de couche 4 utilisé par le service dans la liste déroulante : (**TCP et UDP, TCP, UDP, IP, ICMP**).
- 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**, saisissez le numéro de port.
- Étape 7** Cliquez sur **Appliquer**.
- Étape 8** Pour modifier une entrée, sélectionnez-la et cliquez sur **Modifier**. Apportez les modifications souhaitées, puis cliquez sur **Appliquer**.
-

Horaire

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 > Horaire**.
 - Étape 2** Dans la **Table des horaires**, cliquez sur **Ajouter** pour créer un nouvel horaire. Vous pouvez modifier un horaire existant en le sélectionnant et en cliquant sur **Modifier**.
 - 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** 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**.
-



CHAPITRE 5

Réseau WAN

Cette section fournit des renseignements sur le réseau étendu (WAN). Elle contient les rubriques suivantes :

- [Paramètres WAN, page 41](#)
- [Multi-WAN, page 45](#)
- [Réseau mobile, page 46](#)
- [DNS dynamique, page 48](#)
- [DMZ matérielle, page 48](#)
- [Transition IPv6, page 49](#)

Paramètres WAN

Deux interfaces WAN et VLAN physiques peuvent être configurées sur le routeur. Pour configurer les paramètres WAN, procédez de la façon suivante :

-
- Étape 1** Sélectionnez **WAN > Paramètres WAN**.
- Étape 2** Dans la **Table WAN**, cliquez sur **Ajouter**.
- Étape 3** Sélectionnez l'interface (**WAN1 ou WAN 2**). Selon l'interface sélectionnée, un nom de sous-interface s'affiche juste en dessous. Ajoutez cette sous-interface à la table Multi-WAN pour rediriger le trafic de la route par défaut ; dans le cas contraire, seul le trafic de la route connectée sera redirigé en fonction de la table de routage.
- Étape 4** Saisissez l'**ID du VLAN**.
- Étape 5** Configurez les paramètres des sections IPv4, IPv6 ou Avancés.
- Étape 6** Cliquez sur **Appliquer**.
- Connexions IPv4 et IPv6**
- Étape 7** Pour une connexion IPv4, cliquez sur l'onglet **IPv4**.
- Étape 8** Sélectionnez le type de connexion dans la liste :
- Lorsque la connexion IPv4 ou IPv6 utilise DHCP**
- Dans la section Paramètres DHCP, saisissez les informations suivantes :

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.

Lorsque la connexion IPv4 ou IPv6 utilise l'adresse IP statique

Dans la section **Paramètres IP statiques**, saisissez les informations suivantes :

Adresse IP WAN	Saisissez l'adresse IP.
Masque de réseau	Saisissez le 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.
DHCP-PD (IPv6 uniquement)	Sélectionnez cette option pour l'activer et saisissez un nom de préfixe.

Lorsque la connexion IPv4 ou IPv6 utilise PPPoE

Dans la section Paramètres PPPoE, saisissez les informations suivantes :

Nom d'utilisateur	Nom d'utilisateur que votre FAI vous a attribué.
Mot de passe	Mot de passe que votre FAI vous a attribué.
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.
Mode de connexion	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. 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 (Auto, PAP, CHAP, MS-CHAP, MS-CHAPv2).
Nom du service	Saisissez le nom du service.
DHCP-PD (IPv6 uniquement)	Sélectionnez cette option pour l'activer et saisissez un nom de préfixe.

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.

Lorsque la connexion IPv4 est établie via PPTP

Dans la section PPTP, saisissez les informations suivantes :

Affectation des adresses IP	Pour DHCP, 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.
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.
Mode de connexion	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. 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 (Auto, PAP, CHAP, MS-CHAP, MS-CHAPv2).
Cryptage MPPE	Cochez cette case pour activer le cryptage MPPE.

Lorsque la connexion IPv4 utilise L2TP

Dans la section Paramètres L2TP, saisissez les informations suivantes :

Affectation des adresses IP	Pour DHCP, 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.
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.

Mode de connexion	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. 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 (Auto, PAP, CHAP, MS-CHAP, MS-CHAPv2).

Lorsque la connexion IPv6 utilise le pont

Paramètres de pont

Pont vers	VLAN1 est la valeur par défaut.
Adresse IP	Saisissez l'adresse IP.
Masque de réseau	Saisissez le masque de réseau.
Passerelle par défaut	Saisissez la passerelle par défaut.
DNS statique 1 et 2	Saisissez l'adresse IP du serveur DNS statique principal et du serveur DNS statique secondaire dans les champs correspondants.

Lorsque la connexion IPv6 utilise SLAAC

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 dans les champs correspondants.
DHCP-PD (IPv6 uniquement)	Sélectionnez cette option pour l'activer et saisissez un nom de préfixe.

Étape 9 Cliquez sur **Appliquer**.

Pour Avancé

Étape 10 Cliquez sur l'onglet Avancé et configurez les paramètres suivants :

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 d'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 11 Cliquez sur **Appliquer**.

Remarque Ajoutez l'une de ces sous-interfaces à la table Multi-WAN pour rediriger le trafic de la route par défaut. Dans le cas contraire, seul le trafic de la route connectée sera redirigé en fonction de la table de routage.

Multi-WAN

Les fonctions Basculement WAN et Équilibrage de charge permettent d'optimiser l'utilisation des diverses interfaces WAN. Selon la configuration, cette fonction peut être utilisée pour distribuer le trafic parmi les interfaces. La fonction Multi-WAN fournit le trafic WAN sortant et l'équilibrage de charge sur plusieurs interfaces WAN (WAN et USB) en fonction d'une affectation des tailles numérique. Elle permet en outre de surveiller chaque connexion WAN à l'aide de tests Ping répétés et d'acheminer automatiquement le trafic sortant vers une autre interface WAN en cas de perte de connectivité. Il est par ailleurs possible de définir des règles de trafic sortant spécifiques grâce à une connexion à 5 tuples. L'équilibrage de charge du réseau sortant s'effectue sur des connexions IP spécifiques ; il n'existe aucune liaison de canaux, où une seule connexion utilise plusieurs connexions WAN simultanément. Les interfaces VLAN du réseau WAN peuvent également être configurées pour l'équilibrage de charge ou le basculement.

Pour configurer les paramètres Multi-WAN, procédez de la façon suivante :

Étape 1 Sélectionnez **WAN > Multi-WAN**.

Étape 2 Dans la Table des paramètres d'interface, configurez les paramètres suivants :

- **Interface** : nom de l'interface WAN à laquelle appliquer la configuration d'équilibrage de charge et de basculement. Sélectionnez l'interface souhaitée (**WAN1**, **WAN2**, **USB1** ou **USB2**).
- **Priorité (pour le basculement)** : saisissez la valeur de priorité pour que l'interface active une autre connexion sur une autre interface.
- **Pourcentage de pondération ou Bande passante de pondération (pour l'équilibrage de charge)** : saisissez le pourcentage ou la valeur de pondération pour chaque connexion. L'interface achemine le trafic vers la connexion secondaire en cas de surcharge sur la connexion principale suite à l'équilibrage de la charge de bande passante. Pour garantir une utilisation optimale des deux connexions, le pourcentage entre les pondérations d'équilibrage de charge des connexions doit correspondre au pourcentage entre les bandes passantes des connexions.

Étape 3 Cliquez sur **Configuration avancée** et configurez les paramètres suivants :

- a) **Activer la détection de services réseau** : cochez cette case pour autoriser le périphérique à détecter la connectivité réseau en envoyant une requête Ping aux périphériques spécifiés, puis définissez les paramètres ci-dessous.
- **Nombre de nouvelles tentatives** : nombre d'envois de requêtes Ping à un périphérique. La plage est comprise entre 1 et 10. La valeur par défaut est 3.
 - **Délai d'expiration des nouvelles tentatives** : nombre de secondes à attendre entre les requêtes Ping. La plage est comprise entre 1 et 300. La valeur par défaut est 5.
 - **Destination de détection** : sélectionnez **Passerelle par défaut** ou **Hôte distant**. Si vous sélectionnez l'hôte distant, saisissez l'hôte.

Étape 4 Cliquez sur **Appliquer**.

Étape 5 **Activer le routage basé sur des politiques** : sélectionnez cette option pour l'activer.

Étape 6 Cliquez ensuite sur **Ajouter** ou sur **Modifier**, puis configurez les paramètres suivants :

Priorité	Saisissez une valeur de priorité.
IP source	Saisissez l'adresse IP source.
IP de destination	Saisissez l'adresse IP de destination.
Services	Sélectionnez un service dans la liste déroulante. Si un service ne figure pas dans la liste, vous pouvez cliquer sur Gestion des services pour l'ajouter.
Interface sortante	Sélectionnez l'interface sortante (WAN1 , WAN2 , USB1 ou USB2) dans la liste déroulante.
Basculement vers le WAN de secours	Sélectionnez Activé ou Désactivé dans la liste déroulante Basculement vers le WAN de secours. Remarque Si vous sélectionnez Désactivé , le trafic est abandonné lorsque l'interface de liaison n'est plus en ligne ou est indisponible.
État	Sélectionnez Activer ou Désactiver pour activer ou désactiver l'état de la stratégie.

Étape 7 Vous pouvez également modifier ou supprimer une configuration en cliquant sur **Modifier** ou sur **Supprimer**.

Étape 8 Cliquez sur **Appliquer**.

Remarque Certains fournisseurs d'accès n'autorisent pas l'envoi de requêtes Ping sur la passerelle par défaut. Sélectionnez un hôte distant valide pour détecter la connectivité réseau ou désactivez simplement la détection. Dans le cas contraire, le trafic ne sera pas redirigé par le périphérique.

Réseau mobile

Un modem haut débit mobile est un type de modem permettant à un ordinateur portable, un ordinateur personnel ou un routeur de recevoir un accès Internet via une connexion haut débit mobile et non à l'aide d'une ligne téléphonique ou d'un câble.

Pour configurer le réseau mobile, procédez de la façon suivante :

Étape 1 Sélectionnez **WAN > Réseau mobile**.

Étape 2 Dans la section Paramètres généraux, sélectionnez l'interface (USB1 ou USB2) à laquelle appliquer les paramètres.

Étape 3 Dans la section État de la carte, cliquez sur **Connecter** pour établir la connexion.

Étape 4 Dans la section Type de service, sélectionnez le type de service dans la liste déroulante.

Configuration du réseau mobile

Pour configurer le réseau mobile, procédez de la façon suivante :

-
- Étape 1** En mode de configuration, sélectionnez **Auto** pour connecter le réseau automatiquement.
- Étape 2** Saisissez le code PIN associé à la carte SIM dans le champ **PIN SIM**.
- Étape 3** Vous pouvez également sélectionner **Manuel** et vous connecter au réseau manuellement en configurant les paramètres suivants :
- **Nom du point d'accès** : saisissez le nom du point d'accès fourni par votre fournisseur de services réseau mobiles.
 - **Composer le numéro** : saisissez le numéro fourni par votre fournisseur de services réseau mobiles pour la connexion Internet.
 - **Nom d'utilisateur et mot de passe** : saisissez le nom d'utilisateur et le mot de passe fournis par votre fournisseur de services réseau mobiles.
 - **PIN SIM** : saisissez le code PIN associé à la carte SIM.
 - **Nom du serveur** : saisissez le nom du serveur.
 - **Authentifier** : sélectionnez l'option d'authentification.
- Étape 4** Sélectionnez l'une des options suivantes pour le mode de connexion.
- **Connexion à la demande** : cette option spécifie le délai de connexion au terme duquel la connexion prend fin en cas d'inactivité. Saisissez la Durée d'inactivité max, en secondes, avant la fin de la connexion suite à une période d'inactivité. La valeur par défaut est de 5 minutes.
 - **Maintenir actif** : cette option vérifie régulièrement la connexion avec le routeur pour la rétablir en cas de déconnexion. Dans le champ Intervalle de nouvelle numérotation, saisissez le délai, en secondes, à l'issue duquel le routeur vérifie automatiquement la connexion. Le délai par défaut est de 30 secondes.
-

Paramètre de limite de bande passante

Le suivi de la limite de bande passante permet de limiter le transfert d'un nombre de données spécifique au cours d'une période donnée. Cette fonction est également appelée « limite de bande » ou « limite de données ». Pour configurer le paramètre de limite de bande passante, procédez de la façon suivante.

-
- Étape 1** Activez l'option **Suivi de la limite de bande passante** et définissez les paramètres suivants :
- **Date de renouvellement mensuel** : sélectionnez la durée d'application (en jours) des paramètres de limite de bande passante.
 - **Limite mensuelle de bande passante** : indiquez la taille des données.

- **Envoyer un e-mail à l'administrateur si l'utilisation de 3G/4G atteint x % de la limite mensuelle de bande passante** : sélectionnez le pourcentage de données pour la limite mensuelle de bande passante. Lorsque cette limite est atteinte, une alerte est envoyée par e-mail à l'administrateur.

Étape 2 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. DDNS 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. Vous avez donc la possibilité d'héberger votre propre serveur FTP Web ou tout autre type de serveur TCP/IP sur votre réseau LAN. Vous avez le choix entre plusieurs services DDNS, dont la plupart sont gratuits ou disponibles à un coût minime. Le service le plus utilisé est DynDNS.

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 (**WAN1**, **WAN2**, **USB1** ou **USB2**) 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.
- 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**.
- Étape 10** Cliquez sur **Actualiser** pour actualiser la Table de DNS dynamique.
-

DMZ matérielle

Une DMZ (zone démilitarisée) autorise l'ensemble du trafic entrant et du trafic sortant. Une DMZ est un sous-réseau ouvert au public, bien que derrière le pare-feu. Une DMZ permet de rediriger des paquets qui arrivent sur votre port WAN vers une adresse IP particulière. Vous pouvez configurer des règles de pare-feu pour autoriser l'accès à des services et ports particuliers sur la DMZ, depuis le LAN et depuis le WAN. En cas d'attaque d'un nœud de la DMZ, le réseau LAN n'est pas forcément vulnérable. Nous vous recommandons de placer les hôtes devant être exposés au WAN (comme les serveurs Web ou de messagerie) sur le réseau DMZ.

Pour configurer la DMZ matérielle, procédez de la façon suivante :

-
- Étape 1** Sélectionnez **WAN > DMZ matérielle**.
 - Étape 2** Cliquez sur **Activer** pour définir le réseau LAN4 sur le port DMZ.
 - Étape 3** Sélectionnez **Sous-réseau** pour identifier un sous-réseau pour les services DMZ, puis saisissez l'**Adresse IP de la DMZ** et le **Masque de sous-réseau**.
 - Étape 4** Sélectionnez **Plage** (DMZ et WAN au sein du même sous-réseau) et saisissez la plage d'adresses IP.
 - Étape 5** 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** Dans la table des tunnels, sélectionnez l'interface à configurer et cliquez sur **Modifier**.
 - Étape 3** Cochez la case **Activer**.
 - Étape 4** Saisissez une description.
 - Étape 5** Sélectionnez l'interface locale dans la liste déroulante (**WAN1** ou **WAN2**).
 - Étape 6** L'adresse IPv4 locale indique l'adresse de l'interface sélectionnée.
-

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**.
 - Étape 4** Saisissez l'**Adresse IPv6 distante**.
 - 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.

Pour ajouter le déploiement IPv6 rapide (6rd), saisissez les informations suivantes :

-
- Étape 1** Cliquez sur l'onglet Déploiement IPv6 rapide (6rd).
- Étape 2** 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.
- Saisissez l'**Adresse IPv4 du relais**.
 - Saisissez la **Longueur du préfixe commun IPv4**.
 - 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

QoS

Cette section fournit des informations sur la qualité de service (QoS), qui permet d'optimiser le trafic réseau en vue d'améliorer votre expérience. La QoS contrôle et gère les ressources du réseau en définissant des priorités pour des types de données spécifiques (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 contient les rubriques suivantes :

- [Classes de trafic, page 51](#)
- [Mise en file d'attente WAN, page 52](#)
- [Contrôle d'activité WAN, page 53](#)
- [Gestion de la bande passante WAN, page 53](#)
- [Classification des commutateurs, page 54](#)
- [Mise en file d'attente des commutateurs, page 55](#)

Classes de trafic

Les classes de trafic dirigent le trafic Internet 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.

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	Saisissez le nom du service.
Interface de réception	Sélectionnez une interface (WAN1, WAN2, USB1, USB2, LAN1, LAN2, LAN3, LAN4 ou VLAN1) dans la liste déroulante.
Version IP	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/Application	<ul style="list-style-type: none"> • Service : sélectionnez le nom du service à appliquer sur l'enregistrement de trafic. Indiquez le port source et le port de destination. • Application : sélectionnez l'application à appliquer sur l'enregistrement de trafic. Sélectionnez le comportement et la catégorie d'application. <p>Remarque Les règles d'application ne peuvent pas être configurées tant que l'utilisateur n'active pas le contrôle d'application dans la section Sécurité/Application.</p>
Type de périphérique	Dans la liste déroulante, sélectionnez le type de périphérique d'où provient le trafic.
Type d'OS	Dans la liste déroulante, sélectionnez le système d'exploitation d'où provient le trafic.
Mettre en correspondance DSCP	Le DSCP associe la valeur de classe du trafic dans l'en-tête IPv6 pour le trafic IPv6. La valeur de classe du trafic est 4 fois supérieure à la valeur configurée. Par exemple, si l'utilisateur configure la valeur DSCP mise en correspondance sur 10, réécrivez le DSCP sur 18. La règle met en correspondance les flux IPv6 avec la valeur de classe du trafic 40 et remplace la valeur DSCP par 72. Dans la liste déroulante, sélectionnez la valeur DSCP à mettre en correspondance avec la valeur DSCP dans les paquets entrants.
Réécrire DSCP	Dans la liste déroulante, sélectionnez la valeur DSCP à remplacer dans les paquets entrants.

Étape 4 Cliquez sur **Appliquer**.

Mise en file d'attente WAN

Il est possible de gérer le trafic réseau de LAN à WAN 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** Au-dessus de la table Mise en file d'attente WAN, sélectionnez le moteur de mise en file d'attente de votre choix (**Priorité, Contrôle du débit ou Latence faible**).
 - Étape 3** Dans la table Mise en file d'attente WAN, cliquez sur **Ajouter**, puis donnez un nom à la stratégie et décrivez-la.
 - Étape 4** Si vous avez sélectionné la mise en file d'attente Priorité, dans la table correspondante, sélectionnez la classe de trafic pour chaque file d'attente dans la liste déroulante.
 - Étape 5** Si vous avez sélectionné la mise en file d'attente Contrôle du débit, dans la table correspondante, sélectionnez la classe de trafic et saisissez le débit minimal et le débit maximal pour chaque file d'attente.
 - Étape 6** Si vous avez sélectionné la mise en file d'attente Faible latence, dans la table correspondante, sélectionnez la classe de trafic et configurez la valeur de partage de bande passante pour chaque file d'attente.
 - Étape 7** 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 Classe de stratégie, configurez les paramètres suivants pour chaque file d'attente :

Classe de trafic	Sélectionnez Non spécifiée ou Par défaut .
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 4** 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.

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 du commutateur QoS (**Basé sur les ports**, **Basé sur DSCP** ou **Basé sur CoS**).

Basé sur les ports	<p>Paquets entrants sur chaque port LAN mappés sur des files d'attente spécifiques en fonction des mappages.</p> <ul style="list-style-type: none"> • File d'attente du port LAN : sélectionnez la file d'attente du port LAN pour mapper le trafic entrant sur les ports LAN individuels. • File d'attente du port LAG : lorsque l'interface LAG est activée, l'ensemble du trafic entrant dans cette interface LAG est mappé à l'aide de la file d'attente configurée.
Basé sur DSCP	<p>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.</p> <ul style="list-style-type: none"> • Mappez le trafic sur différentes files d'attente en fonction de la valeur DSCP du paquet entrant.

Basé sur CoS	<p>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.</p> <ul style="list-style-type: none">• Mappez le trafic sur les différentes files d'attente en fonction de la valeur CoS du paquet entrant en sélectionnant les files d'attente dans la liste déroulante.
---------------------	--

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. Lorsque l'interface LAG est activée, l'utilisateur peut définir les tailles de file d'attente des quatre files.



Remarque

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

Pour configurer la taille des files d'attente du port LAN, cliquez sur QoS > Mise en file d'attente des commutateurs et procédez comme suit :

-
- Étape 1** Dans la zone Taille des files d'attente du port LAN, 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.
- Étape 4** Dans la table Taille des files d'attente du port LAN, les ports LAG et leur taille de file d'attente s'affichent.
-



Réseau local

Cette section fournit des informations sur le réseau local (LAN), qui est un réseau informatique couvrant une zone relativement restreinte, telle qu'un immeuble de bureaux, une école ou un logement. Cette section contient les rubriques suivantes :

- [Paramètres des ports, page 57](#)
- [Paramètres VLAN, page 58](#)
- [Paramètres LAN/DHCP, page 59](#)
- [DHCP statique, page 62](#)
- [Configuration 802.1X, page 62](#)
- [Base de données locale DNS, page 63](#)
- [Annonce de routeur, page 63](#)

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 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.
Activé	Cochez cette case pour activer le port et les paramètres correspondants. Si cette option est désactivée, tous les paramètres définis sur le port sont perdus.
EEE (Energy Efficient 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.

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	Sélectionnez l'un des réseaux LAN (LAN1 à LAN4) dans la liste déroulante.
Port contrôlé	Ce port permet de contrôler l'envoi de trafic à des fins de mise en miroir. Sélectionnez l'un des réseaux LAN (LAN1 à LAN4) dans la liste déroulante.

Étape 4

Dans la Table de configuration de l'agrégation de liaisons, saisissez les informations suivantes :

Nom du groupe	Indiquez le nom du groupe de liaisons.
Non attribué	Sélectionnez cette option pour supprimer le port du groupe LAG. Sélectionnez l'un des réseaux LAN (LAN1 à LAN4) dans la liste déroulante.
LAG1	Sélectionnez cette option pour appliquer l'agrégation de liaisons sur le port approprié pour le trafic. Sélectionnez l'un des réseaux LAN (LAN1 à LAN4) dans la liste déroulante.

Attention Toutes les configurations existantes sur les ports (qui vont faire partie du LAG) sont perdues.

Étape 5

Cliquez sur **Appliquer**.

Paramètres VLAN

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 32 VLAN dans le système. Certains VLAN sont utilisés par le réseau WAN, le reste est utilisé par le réseau LAN.

Pour configurer une paramètres VLAN, saisissez les informations suivantes.

-
- Étape 1** Sélectionnez **LAN > Paramètres VLAN**.
- Étape 2** Dans la table VLAN, cliquez sur **Ajouter**.
- Étape 3** Saisissez l'ID du VLAN (plage comprise entre 1 et 4 093).
- Étape 4** Cochez l'option permettant d'activer le routage inter-VLAN.
- Étape 5** Saisissez l'adresse IPv4.
- Étape 6** Saisissez le préfixe, la longueur du préfixe et l'identifiant d'interface.
- Étape 7** Cliquez sur **Modifier** ou sur **Supprimer** pour modifier ou supprimer les configurations de la table VLAN.
- Étape 8** Dans la table VLAN au port, cliquez sur **Modifier** pour attribuer un VLAN à un port LAN. Spécifiez les informations suivantes pour chacun des VLAN répertoriés dans la table.
- **Non balisé** : sélectionnez cette option dans la liste déroulante pour ne pas baliser le port.
 - **Balisé** : sélectionnez cette option 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. Lorsque les VLAN non balisés sont exclus d'un port, le port se connecte automatiquement au réseau VLAN par défaut.
- Étape 9** Cliquez sur **Appliquer**.
-

Paramètres LAN/DHCP

La configuration DHCP permet de configurer le serveur DHCP pour le relais ou l'option 82 (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.

L'option 82 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 les paramètres LAN/DHCP, procédez de la façon suivante :

-
- Étape 1** Sélectionnez **LAN > Paramètres LAN/DHCP**.
- Étape 2** Dans la Table des paramètres LAN/DHCP, cliquez sur **Ajouter**.
- Étape 3** Si vous choisissez **Interface**, sélectionnez un VLAN dans la liste déroulante et cliquez sur **Suivant**.
- Étape 4** Pour configurer le serveur DHCP pour IPv4, sélectionnez le type DHCP pour IPv4.

Désactivé	Le serveur DHCP est désactivé pour IPv4 sur ce périphérique. Aucun autre paramètre supplémentaire ne doit être défini.
------------------	--

Serveur	Le serveur DHCP attribue des adresses aux clients à partir de leurs pools respectifs.
Relais	Les requêtes et les réponses DHCP sont envoyées à partir d'un autre serveur DHCP au périphérique. Saisissez l'adresse IPv4 du serveur DHCP pour configurer l'agent de relais DHCP.

Configuration du serveur DHCP pour IPv4

Étape 5

Cliquez sur **Suivant** et configurez les paramètres suivants :

Durée de bail du client	Durée (en minutes) pendant laquelle un utilisateur du réseau est autorisé à se connecter au routeur avec l'adresse IP actuelle. 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.
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.
Serveur WINS	Adresse IP facultative d'un serveur WINS (Windows Internet Naming Service) qui résout les noms NetBIOS sur les adresses IP. L'adresse IP par défaut est 0.0.0.0.
Options DHCP	<ul style="list-style-type: none"> • 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.

Configuration du type DHCP pour IPv6

Étape 6

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

Désactiver	Le serveur DHCP est désactivé sur ce périphérique. Aucun autre paramètre supplémentaire ne doit être défini.
Serveur	Le serveur DHCP attribue des adresses aux clients à partir de leurs pools respectifs.

Étape 7

Cliquez sur **Suivant** et configurez les paramètres suivants :

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 1 460 minutes (24 heures). 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.
Début de plage	Adresse de début du pool d'adresses IPv6.

Fin de plage	Adresse de fin du pool d'adresses IPv6.
Serveur DNS	Type de DNS (serveur statique), proxy ou serveur DNS fourni par le FAI.
DNS statique 1 et DNS statique 2	(Facultatif) Adresse IP d'un serveur DNS. Si vous saisissez un deuxième serveur DNS, le routeur utilise le premier serveur DNS pour répondre. La spécification d'un serveur DNS peut fournir un accès plus rapide que l'utilisation d'un serveur DNS attribué de façon dynamique. L'adresse IP par défaut est 0.0.0.0.

Configuration du circuit de l'option 82

Étape 8

Pour configurer le circuit de l'option 82, saisissez les informations suivantes.

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.

Étape 9

Cliquez sur **Suivant** et définissez les paramètres suivants :

Adresse IP et masque de sous-réseau	Saisissez l'adresse IP et le masque de sous-réseau du périphérique.
--	---

Étape 10

Cliquez sur **Suivant**.

Étape 11

Pour ajouter une nouvelle configuration DHCP, définissez les paramètres suivants :

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 3200 minutes. La valeur par défaut est de 1 460 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.
Serveur WINS	Adresse IP facultative d'un serveur WINS (Windows Internet Naming Service) qui résout les noms NetBIOS sur les adresses IP. L'adresse IP par défaut est 0.0.0.0.
Options DHCP	<ul style="list-style-type: none"> • 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 12 Cliquez sur **OK**, puis sur **Appliquer**.

DHCP statique

La fonctionnalité DHCP statique permet d'attribuer une adresse IPv4 à une adresse MAC définie.

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 Dans la table DHCP statique, saisissez un nom dans le champ Nom.

Étape 4 Saisissez l'adresse IPv4 et l'adresse MAC dans les champs respectifs.

Étape 5 Cochez la case **Activer**.

Étape 6 Cliquez sur **Appliquer**.

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 périphériques connectés à un port LAN présentant des caractéristiques de connexion point à point. Dans ce contexte, un port est un point de liaison unique vers l'infrastructure LAN.

Le périphérique prend en charge le mode Hôtes multiples. Dans ce mode, seul l'un des hôtes rattachés doit être autorisé pour permettre l'accès au réseau à tous les hôtes. Si ce port n'est plus autorisé (notamment en cas d'échec de la nouvelle autorisation ou de la réception d'un message EAPOL-logoff), tous les clients rattachés se voient refuser l'accès au réseau.

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.

Remarque 802.1X requiert l'utilisation du serveur RADIUS pour l'authentification. Vérifiez que le serveur RADIUS est configuré à la section [Comptes d'utilisateur](#), à la page 31.

Étape 3 Dans la liste déroulante, sélectionnez l'état d'administration dans la table de configuration 802.1X.

- **Autorisation forcée** : aucune autorisation n'est requise. Au moins un port LAN doit être en mode d'autorisation forcée.
- **Auto** : 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.

Étape 4 Cliquez sur **Appliquer**.

Remarque Vérifiez que la configuration respective est active et correcte avant d'activer une authentification basée sur les ports.

Base de données locale DNS

Un serveur DNS (Domain Name Service) local est utilisé pour accélérer les réponses du service DNS. Le serveur DNS associe un nom de domaine à son adresse IP routable. Pour les noms de domaine couramment utilisés, une base de données locale DNS qui agit en tant que serveur DNS local peut donner de meilleurs résultats qu'un serveur DNS externe. Si un nom de domaine demandé est introuvable dans la base de données locale, la requête est transférée au serveur DNS spécifié sur la page de configuration.

Pour configurer la base de données DNS locale, procédez comme suit :

Étape 1 Sélectionnez **LAN > Base de données DNS locale**.

Étape 2 Cliquez sur **Ajouter** et saisissez le nom d'hôte et l'adresse IPv4 ou IPv6. Vous pouvez également modifier ou supprimer la base de données DNS.

Étape 3 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 sur leurs réseaux locaux 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 Sélectionnez l'ID du VLAN dans la liste déroulante.

Étape 3 Cochez la case **Activer** pour activer l'annonce de routeur, puis configurez les paramètres suivants :

Mode d'annonce	Sélectionnez le mode d'annonce dans la liste déroulante (Monodiffusion ou Multidiffusion non demandée).
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	<p>Ce paramètre détermine si les hôtes peuvent utiliser DHCPv6 pour obtenir les adresses IP et les informations connexes. Sélectionnez et activez l'une des options suivantes :</p> <ul style="list-style-type: none"> • 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	<p>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.</p>
Unité maximale de transmission (MTU)	<p>La MTU correspond au paquet le plus volumineux pouvant être transmis sur le réseau. La MTU est utilisée 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.</p>
Durée de vie du routeur	<p>Saisissez la durée d'existence des messages d'annonce de routeur sur la route, en secondes. La valeur par défaut est de 3 600 secondes.</p>

Étape 4 Dans la Table des préfixes, cliquez sur **AJOUTER** et donnez un nom au préfixe.

Étape 5 Saisissez la longueur et la durée de vie du préfixe dans les champs correspondants.

Étape 6 Cliquez sur **Appliquer**.



Technologie 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 fils pour communiquer d'un nœud à l'autre. Elle contient les rubriques suivantes :

- [Paramètres de base, page 65](#)
- [Paramètres avancés, page 70](#)
- [Portail captif, page 72](#)
- [WPS, page 74](#)

Paramètres de base

Le RV340W 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 b bande simultanée, 2,4 GHz 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.

Dans 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 Dans le tableau Sans fil, cliquez sur **Ajouter** ou **Modifier**.


Étape 3 Ensuite, sur la page Ajouter/Modifier les paramètres SSID sans fil, configurez les paramètres suivants :







SSID Name	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 sera 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.
SSID Broadcast	Cochez cette case 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, les clients sans fil peuvent se connecter à votre réseau sans fil uniquement s'ils fournissent le SSID et les informations de sécurité requises.

Security Mode	<p>Sélectionnez un mode de sécurité pour le réseau parmi les options suivantes :</p> <ul style="list-style-type: none"> • 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 doit être une chaîne comportant 10 caractères hexadécimaux. • WEP-128 : Sélectionnez le mode de sécurité WEP 128 bits et entrez une clé WEP si vous utilisez un équipement ancien qui ne prend pas en charge la sécurité WPA ou WPA2. La clé WEP doit être 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, entrez une phrase de sécurité alphanumérique. • WPA-WPA2-Personnel : 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, entrez 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 : <ul style="list-style-type: none"> ◦ 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). • WPA-WPA2-Entreprise : 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.
PMF	<ol style="list-style-type: none"> 1 Si aucun mode de sécurité n'est spécifié, PMF est défini sur Non requis et reste grisé (non modifiable). 2 Si le mode de sécurité est WPA2-XXX, PMF est défini sur Compatible par défaut. <ul style="list-style-type: none"> • Ce paramètre peut être modifié par l'utilisateur et réglé sur Non requis ou Requis. • Lorsque vous enregistrez après avoir sélectionné WPA-XXX, et que PMF est défini sur Compatible, un avertissement de type « PMF est activé » devrait s'afficher. Cependant, certains clients sans fil peuvent ne pas être complètement compatibles avec PMF et peuvent rencontrer des problèmes d'instabilité. <p>Remarque Pour définir les options de configuration de PMF, consultez le Tableau PMF ci-dessous.</p>

Wireless Isolation with 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 74.
VLAN	Spécifiez l'ID du VLAN auquel le SSID doit être 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.
Nombre max. de clients associés	Spécifiez le nombre maximal de clients à associer simultanément (50 pour 2,4 G et 124 for 5 G, par SSID, par défaut). Remarque Le nombre total de clients pouvant être associés pour tous les SSID activés ne doit pas dépasser 50 clients pour 2,4 G et 124 pour 5 G (128 lorsque MU-MIMO est activé).
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 spécifiant 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 cette case pour activer la vérification du portail captif pour le SSID et sélectionnez le profil du 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 72 pour plus d'informations sur l'ajout d'un profil de portail captif.

Tableau 2: Tableau PMF

Paramètre de point d'accès	Paramètre client	Résultat	Sécurité ?
Facultatif	Facultatif	Connexion sans PMF	

Facultatif	Compatible	Connexion sans PMF	
Facultatif	Obligatoire	Aucune connexion	
Compatible	Facultatif	Connexion sans PMF	
Compatible	Compatible	Connexion avec PMF	
Compatible	Obligatoire	Connexion avec PMF	
Obligatoire	Facultatif	Aucune connexion	
Obligatoire	Compatible	Connexion avec PMF	
Obligatoire	Obligatoire	Connexion avec PMF	

Configuration de la fréquence 2,4 GHz

Vous pouvez activer ou désactiver les fréquences bibandes, 2,4 GHz et 5 GHz, qui sont prises en charge par le routeur. Vous pouvez aussi spécifier le numéro de canal de chaque bande ou sélectionner **Sélection automatique du canal**. Ces paramètres seront appliqués 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 WLAN.

Pour configurer les paramètres de sélection de canaux simultanés, procédez comme suit :

Configuration de la fréquence 2,4 GHz

- Étape 1** Cliquez sur **Wireless > Basic Settings > 2.4G**.
- Étape 2** Cochez la case **Radio** pour activer la bande 2,4 GHz.
- Étape 3** Sélectionnez le mode de bande réseau (**B uniquement**, **G uniquement**, **N uniquement**, **B/G**, **G/N** ou **B/G/N**) dans la liste déroulante Mode de réseau sans fil.
- Étape 4** Cliquez sur **20 MHz** ou **20/40 MHz** pour sélectionner la bande passante du canal.
- Étape 5** Sélectionnez le canal primaire en cliquant sur la case d'option Inférieur ou Supérieur.

- Remarque** Vous ne pouvez pas sélectionner de canal primaire si vous avez sélectionné **Bande 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 primaire, 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** 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** Cochez la case **Radio** pour activer la bande 5 GHz.
- Étape 3** Sélectionnez le mode de bande réseau (**A uniquement, N/AC ou A/N/AC**) dans la liste déroulante Mode de réseau sans fil.
- Étape 4** Cliquez sur la case d'option **20 MHz, 40 MHz ou 80 MHz** pour sélectionner la bande passante du canal.
- Étape 5** Sélectionnez le canal primaire en cliquant sur **Inférieur** ou **Supérieur**.
Remarque Vous pouvez sélectionner un canal primaire, 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** Cochez la case **MIMO utilisateurs multiples** pour activer cette option. La méthode MIMO permet de servir jusqu'à 4 groupes parallèles simultanément sur la bande 5 G.
- 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 l'onglet **Sans fil** > **Paramètres avancés** > **2,4 G** ou **5 G**.

Étape 2

Configurez les paramètres suivants :

Frame Burst	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 sélectionner les valeurs par défaut des débits de base et de transmission.
Basic Rate	Sélectionnez les paramètres de débit de base, c'est-à-dire les vitesses auxquelles la plate-forme prête pour les services peut transmettre les données. L'appareil annonce son débit de base aux autres appareils sur le réseau, afin qu'ils connaissent les débits qui seront utilisés. La plate-forme prête pour les services annonce également qu'elle sélectionnera automatiquement la meilleure vitesse de transmission.
Transmission Rate	Sélectionnez les paramètres de débit de transmission, c'est-à-dire la vitesse de transmission des données en fonction de la vitesse de votre réseau sans fil.
CTS Protection Mode	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 l'intervalle de balise (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.
DTIM Interval	Spécifiez l'intervalle de carte DTIM (Delivery Traffic Indication Map). Cette carte informe les clients de la présence de données de multidiffusion/diffusion dans la mémoire tampon du point d'accès. Elle est générée 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 2 347. La valeur par défaut est 2 347.
Tx Power	Sélectionnez le volume de données à transmettre dans la liste déroulante Tx Power.

Étape 3 Cliquez sur **Appliquer**.

Portail captif

La fonctionnalité Portail captif 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 65 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 Choisir un fichier 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 Choisir un fichier et sélectionnez l'image du logo de société 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 Afficher le contrat d'utilisation 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 **Appliquer**.

Pour afficher un aperçu de ce profil, cliquez sur **Aperçu**. Pour activer le portail captif pour des comptes utilisateur spécifiques, voir **Configuration système > Comptes d'utilisateur** et **Configuration système > Groupes d'utilisateurs**.

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 (**2,4 G, 5 G ou Les deux**) dans la liste déroulante des 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.



Routage

Cette section décrit le processus de routage, qui consiste à sélectionner les chemins d'accès appropriés au sein d'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 du routeur est chargé de la création, de la maintenance et de la mise à jour de la table de routage dynamique dans le routage dynamique. Cette section contient les rubriques suivantes :

- [Proxy IGMP, page 75](#)
- [RIP, page 76](#)
- [Routage statique, page 77](#)

Proxy IGMP

Le protocole IGMP (Internet Group Management Protocol) permet aux hôtes et routeurs sur un réseau IP de créer des appartenances à des groupes de multidestination. 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 configurer 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 déroulante.
- **WAN-Auto** : le routeur peut prendre en charge le mode multi-WAN. Si vous sélectionnez le mode WAN auto, le routeur sélectionne le WAN actif comme port en amont. Si plusieurs WAN sont actifs et fonctionnent en mode d'équilibrage de charge, le port WAN portant le numéro de port le plus bas agit en tant que port en amont. Par exemple, si WAN1 et WAN2 sont en mode d'équilibrage de charge, WAN1 est le port en amont. Si WAN1 est indisponible, WAN2 devient le port en amont.
 - **Interface fixe** : l'interface fixe utilise systématiquement le port sélectionné comme port en amont, même si celui-ci est indisponible. Par exemple, si WAN1 et WAN2 sont en mode d'équilibrage de charge et que vous sélectionnez

WAN2 comme port en amont, WAN1 ne reçoit pas le trafic multidestination, que WAN2 soit actif ou pas. Si vous sélectionnez l'**Interface fixe**, veuillez également à sélectionner **WAN 1**, **WAN 2** ou **VLAN1**.

Étape 4 Sélectionnez l'interface en aval, à savoir **WAN** ou **VLAN1**.

Étape 5 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 **IPv4** ou **IPv6**, ou les deux, et configurez les paramètres suivants :

Interface	<p>Cochez la case Activer dans l'interface correspondante pour recevoir les routes en amont.</p> <p>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.</p>
RIP version 1	<p>Ce protocole utilise le routage par classe et n'inclut pas les informations ou l'authentification du sous-réseau.</p> <ul style="list-style-type: none"> • 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. <p>Remarque La configuration passive est activée uniquement lorsque vous cochez la case Activer.</p>
RIP version 2	<p>Ce protocole sans classe utilise la multidiffusion et l'authentification par mot de passe.</p> <ul style="list-style-type: none"> • 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. <p>Remarque La configuration passive est activée uniquement lorsque vous cochez la case Activer.</p>

RIPng (IPv6)	<p>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.</p> <ul style="list-style-type: none"> • Cochez la case Activer pour activer le routage RIP IPv6. • Cochez la case Passif pour désactiver l'envoi de la version RIPng. <p>Remarque La configuration passive est activée uniquement lorsque vous cochez la case Activer.</p>
Authentification	<p>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.</p> <ul style="list-style-type: none"> • 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**.

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 de routage, cliquez sur **Ajouter** ou sur **Modifier** et configurez les paramètres suivants :

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.
Métrieque	La valeur du champ Métrieque représente le nombre de routeurs entre votre réseau et la destination. Étant donné qu'il s'agit d'une connexion directe, ce paramètre peut être défini sur la valeur minimale (1).

Interface	Sélectionnez l'interface à utiliser pour cette route statique dans le menu déroulant.
------------------	---

Étape 3 Cliquez sur **Appliquer**.

Étape 4 Pour les routes IPv6, dans la Table de routage, cliquez sur **Ajouter** ou sur **Modifier** et configurez les paramètres suivants :

Préfixe	Saisissez le préfixe IPv6.
Longueur	Saisissez le nombre de bits de préfixe de l'adresse IP.
Saut suivant	Saisissez l'adresse IP du routeur utilisé en dernier recours.
Métrique	La valeur du champ Métrique représente le nombre de routeurs entre votre réseau et la destination. Étant donné qu'il s'agit d'une connexion directe, ce paramètre peut être défini sur la valeur minimale (1).
Interface	Sélectionnez l'interface à utiliser pour cette route statique dans le menu déroulant.

Étape 5 Cliquez sur **Appliquer**.



CHAPITRE 10

Pare-feu

Cette section fournit des informations sur le pare-feu, qui permet de protéger le réseau contre les intrus. Le pare-feu examine le trafic et filtre les transmissions qui ne répondent pas aux critères de sécurité établis. Le pare-feu sélectionne les paquets autorisés ou non à entrer dans un réseau ou à en sortir. Cette section contient les rubriques suivantes :

- [Paramètres de base, page 79](#)
- [Règles d'accès, page 81](#)
- [Traduction des adresses réseau, page 82](#)
- [NAT statique, page 83](#)
- [Redirection de ports, page 83](#)
- [Déclenchement de ports, page 84](#)
- [Délai d'expiration de session, page 85](#)
- [Hôte DMZ, page 86](#)

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], Usurpation d'adresse IP, Echo Storm, Saturation ICMP, Saturation UDP et Saturation TCP.

Bloquer la requête WAN	Cochez la case Activer pour bloquer les demandes d'écho ICMP à destination du réseau WAN.
Gestion Web LAN/VPN	Sélectionnez HTTP ou HTTPS .
Gestion Web à distance	Cochez la case Activer pour activer la gestion Web à distance et saisissez le port (443 par défaut, plage 1025-65535). • Sélectionnez HTTP ou HTTPS .
Adresse IP distante autorisée	Cochez la case Toutes les adresses IP ou saisissez la plage d'adresses IP 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). Cette passerelle de la couche application (ALG) est utilisée avec NAT pour traduire les messages SIP ou les messages SDP.
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 Universal Plug and Play.
Restreindre les fonctionnalités Web	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 2 Dans la **Table des domaines approuvés**, activez l'option **Nom du domaine** pour modifier les paramètres du domaine existant.

Étape 3 Cliquez sur **Ajouter**, **Modifier** ou **Supprimer** pour ajouter, modifier ou supprimer un domaine.

Étape 4 Cliquez sur **Appliquer**.

Règles d'accès

Pour configurer les règles d'accès, procédez de la façon suivante.

Étape 1

Sélectionnez **Pare-feu > Règles d'accès**. Dans la **Table des règles d'accès**, saisissez les informations suivantes :

Étape 2

Cliquez sur **Ajouter** ou sélectionnez la ligne, cliquez sur **Modifier** et saisissez les informations suivantes :

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	<ul style="list-style-type: none"> • 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	<p>Sélectionnez Vrai ou Jamais dans la liste déroulante.</p> <ul style="list-style-type: none"> • Vrai : le journal respecte les règles d'accès. • Jamais : aucun journal requis.
Interface source	Sélectionnez l'interface source (WAN1, WAN2, USB1, USB2, VLAN1 ou Toutes) dans la liste déroulante.
Adresse source	<p>Sélectionnez l'adresse IP source à laquelle la règle est appliquée, puis saisissez les informations suivantes :</p> <ul style="list-style-type: none"> • Toutes • IP unique : saisissez une adresse IP. • Plage IP : saisissez la plage d'adresses IP. • Sous-réseau : indiquez le sous-réseau d'un réseau.
Interface de destination	Sélectionnez l'interface de destination (WAN1, WAN2, USB1, USB2, VLAN1 ou Toutes) dans la liste déroulante.
Adresse de destination	<p>Sélectionnez l'adresse IP de destination à laquelle la règle est appliquée, puis saisissez les informations suivantes :</p> <ul style="list-style-type: none"> • Toutes • IP unique : saisissez une adresse IP. • Plage IP : saisissez la plage d'adresses IP. • Sous-réseau : indiquez le sous-réseau d'un réseau.

Nom de l'horaire	Sélectionnez Bureau, Soirée, Marketing ou Travail dans la liste déroulante pour appliquer la règle de pare-feu. Cliquez ensuite sur le lien pour configurer les horaires.
-------------------------	---

Étape 3 Cliquez sur **Appliquer**.

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

Étape 5 Cliquez sur **Gestion des services** pour configurer les services.

Étape 6 Pour ajouter un service, cliquez sur **Ajouter**. Pour modifier ou supprimer un service, sélectionnez la ligne et cliquez sur **Modifier** ou sur **Supprimer**.

Étape 7 Configurez les options suivantes :

- **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 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** en regard de chaque interface à activer 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 Cliquez sur **Ajouter** (ou sélectionnez la ligne et cliquez sur **Modifier**), puis saisissez les informations suivantes :

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.
Active	Sélectionnez l'option Active pour l'activer.

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 de l'application** : 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** : 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 périphériques réseau sur le LAN en ouvrant un port spécifique ou une plage de ports pour un service.

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 de redirection de ports**, cliquez sur **Ajouter** (ou sélectionnez la ligne et cliquez sur **Modifier**), puis configurez les paramètres suivants :

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.
État	Activez ou désactivez la règle de redirection de ports.

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**.

Remarque Les règles de redirection de ports pour UPnP sont ajoutées de façon dynamique à l'application UPnP.

Étape 6 Dans la **Table de redirection de ports UPnP**, cliquez sur **Actualiser** pour actualiser la liste 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 :

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.
État	Activez ou désactivez la règle de déclenchement de ports.

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** : dernier numéro de port réservé à ce service.

Étape 4

Cliquez sur **Appliquer**.

Délai d'expiration de session

La fonction Délai d'expiration de session permet de 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.
--	--

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.
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.
Nombre maximal de connexions simultanées	Saisissez le nombre maximal de connexions simultanées autorisées.
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. Nous vous conseillons de placer les hôtes devant être exposés aux services WAN sur le réseau DMZ.

Pour configurer la DMZ, procédez de la façon suivante :

-
- Étape 1** Sélectionnez **Pare-feu > DMZ**.
 - Étape 2** Dans **Hôte DMZ**, sélectionnez **Activer**.
 - Étape 3** Saisissez l'**Adresse IP de l'hôte DMZ**.
 - Étape 4** Cliquez sur **Appliquer**.
-



CHAPITRE 11

VPN

Cette section fournit des renseignements sur le réseau privé virtuel (VPN), qui permet d'établir une connexion cryptée sur un réseau moins sécurisé. Les réseaux privés virtuels assurent des connexions sécurisées à une infrastructure de réseau sous-jacente. Un tunnel établit un réseau privé capable d'envoyer des données de façon sécurisée via des techniques de cryptage et d'authentification. Cette section contient les rubriques suivantes :

- [Assistant de configuration VPN \(site à site\), page 87](#)
- [Profils IPsec, page 90](#)
- [Site à site, page 92](#)
- [Client à site, page 98](#)
- [Client VPN télétravailleur, page 102](#)
- [Serveur PPTP, page 104](#)
- [Serveur L2TP, page 104](#)
- [VPN SSL, page 105](#)
- [Intercommunication VPN, page 108](#)

Assistant de configuration VPN (site à site)

Le VPN permet à un hôte distant d'agir comme s'il se trouvait sur le même réseau local. Le routeur prend en charge 50 tunnels. L'Assistant de configuration VPN vous guide lors de la configuration d'une connexion sécurisée pour établir un tunnel IPSec site à site. Il permet de simplifier la configuration en évitant les paramètres complexes et facultatifs de façon à ce que tous les utilisateurs puissent configurer rapidement et efficacement un tunnel IPSec.

Pour démarrer l'Assistant de configuration VPN, cliquez sur **VPN > Assistant de configuration VPN**.
Procédez comme suit pour configurer l'Assistant.

- Étape 1** Dans la section Mise en route, saisissez un nom de connexion dans la zone **Donner un nom à cette connexion**.
- Étape 2** Sélectionnez une interface (**WAN1, WAN2, USB1 ou USB2**) dans la liste déroulante.
- Étape 3** Cliquez sur **Suivant**.
- Étape 4** Dans la section Paramètres du routeur distant, sélectionnez le **Type de connexion distante** dans la liste déroulante. Si vous sélectionnez **Adresse IP**, saisissez l'adresse IP ; si vous sélectionnez un nom de domaine complet (**Nom de domaine complet**), saisissez le nom du domaine.
- Étape 5** Cliquez sur **Suivant** pour passer à l'écran suivant.
- Étape 6** Dans la section Réseaux local et distant, sous Sélection de trafic en local, sélectionnez l'adresse IP locale (**Adresse IP ou Sous-réseau**) dans la liste déroulante. Si vous sélectionnez **Adresse IP**, saisissez l'adresse IP ; si vous sélectionnez **Sous-réseau**, saisissez l'adresse IP et le masque de sous-réseau.
- Étape 7** Sous Sélection de trafic distant, sélectionnez l'adresse IP distante (**Adresse IP ou Sous-réseau**) dans la liste déroulante. Si vous sélectionnez **Adresse IP**, saisissez l'adresse IP ; si vous sélectionnez **Sous-réseau**, saisissez l'adresse IP et le masque de sous-réseau.
- Étape 8** Cliquez sur **Suivant**.
- Étape 9** Dans la section Profil IPsec, sélectionnez le profil IPsec dans la liste déroulante.
- Étape 10** Si vous sélectionnez **Par défaut**, cliquez sur **Suivant**.
- Étape 11** Si vous sélectionnez **Nouveau profil**, configurez les paramètres suivants :

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. La valeur par défaut pour la phase 1 est de 28 800 secondes.

PFS (Perfect Forward Secrecy)	Cochez la case Activer pour activer PFS, puis saisissez la durée de vie en secondes ou décochez l'option Activer pour la désactiver. Si l'option PFS est activée, la phase 2 de la négociation IKE génère une nouvelle clé pour le cryptage et l'authentification du trafic IPSec. Il est recommandé d'activer cette fonction.
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

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. Remarque Ce paramètre est disponible uniquement lors de l'activation de la fonction Confidentialité de transmission parfaite sous les options de phase I.
Sélection du protocole	Sélectionnez un protocole dans la liste déroulante. <ul style="list-style-type: none"> • 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.

Étape 12 Cliquez sur **Suivant** pour afficher un récapitulatif de toutes les configurations.

Étape 13 Cliquez sur **Soumettre**.

Profils IPsec

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. Dans les enregistrements VPN IPsec, les profils IPsec sont appelés clients site à site, clients client à site ou clients VPN télétravailleur.

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

- Étape 1** Sélectionnez **VPN > Profils IPsec**.
- Étape 2** Dans la Table des profils IPsec, cliquez sur **Ajouter**.
- Étape 3** Sous Ajouter un nouveau profil IPsec, saisissez un nom dans la section Nom du profil.
- Étape 4** Sélectionnez le mode de génération de clés.
- Étape 5** Pour le **Mode de génération de clés automatique**, configurez 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. La valeur par défaut pour la phase 1 est de 28 800 secondes.
PFS (Perfect Forward Secrecy)	Cochez la case Activer pour activer PFS, puis saisissez la durée de vie en secondes ou décochez l'option Activer pour la désactiver. Si l'option PFS est activée, la phase 2 de la négociation IKE génère une nouvelle clé pour le cryptage et l'authentification du trafic IPsec. Il est recommandé d'activer cette fonction.

Options Phase 2

Sélection du protocole	Sélectionnez un protocole dans la liste déroulante. <ul style="list-style-type: none"> • 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.
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.

Étape 6 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 est 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).
Durée de vie SA (secondes)	Durée d'activité d'une association de sécurité (SA) IKE dans cette phase. La valeur par défaut pour la phase 1 est de 28 800 secondes.
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 7 Sélectionnez un profil IPsec et cliquez sur **Modifier** ou sur **Supprimer**.

Étape 8 Pour cloner un profil existant, sélectionnez un profil, puis cliquez sur **Cloner**.

Étape 9 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 > 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.
Point d'extrémité 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	<ul style="list-style-type: none"> • 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 désactiver la connexion.
Créer un VPN site à site	Cliquez sur ce bouton pour créer un nouveau tunnel site à site.
Créer un tunnel GRE sécurisé	Cliquez sur ce bouton pour créer un nouveau tunnel GRE.

Création d'une connexion VPN site à site

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.
Point d'extrémité 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.
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 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.

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

Mode agressif	Il existe deux modes de négociation SA IKE : le Mode principal et le Mode agressif . Le mode principal est recommandé lorsque la sécurité du réseau est primordiale. En revanche, si vous souhaitez donner la priorité au débit, nous vous recommandons d'utiliser le mode agressif. Cochez la case Activer pour activer le mode agressif ou décochez-la pour utiliser le mode principal. Si la passerelle de sécurité distante est définie sur l'un des types d'IP dynamiques, le mode agressif doit être configuré. Cette option est automatiquement sélectionnée et ne peut pas être modifiée.
Compresser	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.
Activer DPD (détection d'homologue indisponible)	Cliquez sur DPD pour activer la fonction 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 : <ul style="list-style-type: none"> • 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 de retard : 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	<p>Cochez l'option DNS fractionné pour l'activer.</p> <p>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.</p> <p>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.</p> <p>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.</p>
-----------------------	--

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.

Remarque Pour activer le basculement site à site, vous devez activer la fonction Maintenir actif sous l'onglet Paramètres avancés.

Étape 4 Cliquez sur **Appliquer**.

Création d'un tunnel GRE sécurisé

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.

Étape 1 Cliquez sur **Créer un tunnel GRE sécurisé**.

Étape 2 Cliquez sur **Activer** pour activer la configuration, puis renseignez les champs suivants :
Pour les informations sur le tunnel GRE

Nom de l'interface	Saisissez le nom de l'interface à connecter au tunnel.
---------------------------	--

Source du tunnel	Sélectionnez la source du tunnel (WAN1, WAN2, USB1 ou USB2) dans la liste déroulante.
Destination du tunnel	Sélectionnez la destination du tunnel (IP statique ou Nom de domaine complet dans la liste déroulante.
Adresse IP du tunnel GRE	Saisissez l'adresse IP du tunnel qui achemine le protocole de transport.
Masque de sous-réseau	Saisissez le masque de sous-réseau du tunnel GRE.

Pour le tunnel IPSec

Nom de la connexion	Nom de la connexion.
Profil IPSec	Sélectionnez le profil IPSec (Par défaut, Profil IPSec auto, Profil IPSec manuel, Manuel 1 ou Auto) dans la liste déroulante.
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'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.

Pour la 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.
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 le protocole de routage

Routage statique	<p>Cochez cette case pour activer le routage statique, puis sélectionnez les options suivantes dans la liste déroulante.</p> <ul style="list-style-type: none"> • Tunneling fractionné : cette option permet à un utilisateur mobile d'accéder à des domaines de sécurité distincts, notamment à un réseau public et à un réseau LAN ou WAN local de façon simultanée, à l'aide de la même connexion réseau ou de connexions différentes. • Tout le trafic sur le tunnel : cette option permet d'autoriser l'ensemble du trafic sur le tunnel.
Adresse IP	<p>Cliquez sur Ajouter, puis saisissez l'adresse IP. Vous pouvez également modifier ou supprimer la valeur existante en cliquant sur Modifier ou sur Supprimer.</p>
Masque de réseau	<p>Saisissez le masque de réseau.</p>
Réacheminement multidestination	<p>Sélectionnez Réacheminement multidestination pour permettre au routeur de réacheminer le trafic multidestination vers les réseaux auxquels d'autres périphériques multidestination sont connectés. Le réacheminement multidestination empêche le réacheminement du trafic multidestination vers les réseaux auxquels aucun nœud n'est connecté. Cliquez sur le lien pour configurer l'interface proxy IGMP.</p>
Mode agressif	<p>Cliquez sur cette option pour activer le mode agressif.</p>

Étape 3 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 configurer le tunnel client à site, procédez de la façon suivante :

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

Étape 2 Cliquez sur **Ajouter** pour afficher la table des groupes client à site IPsec.

Étape 3 Pour ajouter une connexion client à site, cliquez sur **Ajouter**.

Étape 4 Dans la section **Ajouter un nouveau groupe**, sélectionnez une option (**Client VPN Cisco** ou **Client tiers**).

Étape 5 Pour l'option Client VPN Cisco, configurez les paramètres suivants :

Activer	<p>Cliquez sur Activer pour activer la configuration.</p>
Nom du groupe	<p>Saisissez le nom du groupe. Ce nom sert d'identifiant à tous les membres de ce groupe lors des négociations IKE.</p>

Interface	Sélectionnez l'interface (WAN1, WAN2, USB1 ou USB2) dans la liste déroulante.
Méthode d'authentification IKE	<p>Méthode d'authentification à utiliser lors des négociations IKE dans les tunnels IKE.</p> <ul style="list-style-type: none"> • 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. • 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.
Groupe d'utilisateurs	Cliquez sur Nom du groupe et sélectionnez le groupe d'utilisateurs (admin ou invité). Cliquez sur Ajouter ou Supprimer pour modifier le groupe d'utilisateurs.
Mode	<p>Sélectionnez le mode parmi les options proposées.</p> <ul style="list-style-type: none"> • Client : la demande d'adresses IP et de serveur de la part du client fournit les adresses IP dans la plage d'adresses configurée. Sélectionnez Client, puis saisissez les adresses IP de début et de fin du réseau LAN du client. • NEM (Mode d'extension du réseau) : les clients proposent leur sous-réseau, et les services VPN doivent être appliqués sur le trafic entre le réseau LAN derrière le serveur et le sous-réseau proposé par le client.
Plage de pools pour le réseau LAN du client	IP de début : saisissez l'adresse IP de début pour la plage de pools. IP de fin : saisissez l'adresse IP de fin pour la plage de pools.

Pour la configuration du mode

DNS principal	Saisissez l'adresse IP du serveur DNS principal.
DNS secondaire	Saisissez l'adresse IP du serveur DNS secondaire.
Serveur WINS (Windows Internet Name Service) principal	Saisissez l'adresse IP du serveur WINS principal.
Serveur WINS secondaire	Saisissez l'adresse IP du serveur WINS secondaire.
Domaine par défaut	Saisissez le nom du domaine par défaut à utiliser dans le réseau distant.

Serveurs de secours 1, 2 et 3	Saisissez l'adresse IP ou le nom de domaine des serveurs de secours 1, 2 et 3. Lorsque la connexion au serveur VPN IPSec principal échoue, le dispositif de sécurité peut démarrer la connexion VPN sur les serveurs de secours. Le serveur de secours 1 a la priorité la plus haute et le serveur de secours 3 a la priorité la plus basse.
Tunnel 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.
DNS fractionné	Cochez cette case pour activer le DNS fractionné. Cliquez ensuite sur Ajouter pour saisir un nom de domaine pour le DNS fractionné. Vous pouvez également ajouter, modifier ou supprimer un tunnel fractionné.

Pour un client tiers

Étape 6

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

Activer	Cliquez sur Activer pour activer la configuration.
Nom du tunnel	Nom du tunnel VPN. Cette description est donnée à titre de référence. Il n'est pas nécessaire que ce nom corresponde au nom utilisé à l'autre extrémité du tunnel.
Interface	Sélectionnez l'interface (WAN1, WAN2, USB1 ou USB2) dans la liste déroulante.
Méthode d'authentification IKE	<p>Méthode d'authentification à utiliser lors des négociations IKE dans les tunnels IKE.</p> <ul style="list-style-type: none"> • 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. • 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 le type d'identifiant local (Adresse IP, Nom de domaine complet ou Nom de domaine complet de l'utilisateur) dans la liste déroulante, puis saisissez l'identifiant.
Identifiant distant	Sélectionnez l'identifiant distant (Adresse IP distante, Nom de domaine complet ou Nom de domaine complet de l'utilisateur) dans la liste déroulante, puis saisissez l'identifiant.
Authentification étendue	Sélectionnez l'option Authentification étendue pour l'activer. Cliquez sur Ajouter pour ajouter une authentification étendue, puis sélectionnez admin ou invité .

Plage de pools pour le réseau LAN du client	IP de début : saisissez l'adresse IP de début pour la plage de pools. IP de fin : saisissez l'adresse IP de fin pour la plage de pools.
--	---

Étape 7

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

Profil IPSec	Définissez ce paramètre sur la valeur par défaut.
Point d'extrémité distant	Sélectionnez le point d'extrémité distant (IP statique, Nom de domaine complet ou IP dynamique) dans la liste déroulante.

Pour la configuration du groupe local

Type d'IP locale	Sélectionnez le type d'IP locale (Adresse IP ou Sous-réseau) dans la liste déroulante.
Adresse IP	Saisissez l'adresse IP du périphérique.
Masque de sous-réseau	Saisissez le masque de sous-réseau.

Pour la configuration du mode

DNS principal	Saisissez l'adresse IP du serveur DNS principal.
DNS secondaire	Saisissez l'adresse IP du serveur DNS secondaire.
Serveur WINS (Windows Internet Name Service) principal	Saisissez l'adresse IP du serveur WINS principal.
Serveur WINS secondaire	Saisissez l'adresse IP du serveur WINS secondaire.
Domaine par défaut	Saisissez le nom du domaine par défaut à utiliser dans le réseau distant.
Serveurs de secours 1, 2 et 3	Saisissez l'adresse IP ou le nom de domaine des serveurs de secours 1, 2 et 3. Lorsque la connexion au serveur VPN IPSec principal échoue, le dispositif de sécurité peut démarrer la connexion VPN sur les serveurs de secours. Le serveur de secours 1 a la priorité la plus haute et le serveur de secours 3 a la priorité la plus basse.
Tunnel 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.
DNS fractionné	Cochez cette case pour activer le DNS fractionné. Cliquez ensuite sur Ajouter pour saisir un nom de domaine pour le DNS fractionné. Vous pouvez également ajouter, modifier ou supprimer un tunnel fractionné.

Paramètres supplémentaires

Mode agressif	Sélectionnez l'option Mode agressif pour l'activer. La fonction Mode agressif vous 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 les attributs du tunnel.
Compresser (prend en charge le protocole de compression de la charge utile IP [IP Comp])	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.

Étape 8 Cliquez sur **Appliquer**.

Client VPN télétravailleur

La fonctionnalité Client VPN télétravailleur minimise la configuration requise sur les sites distants en autorisant le périphérique à fonctionner en tant que client matériel VPN Cisco. Lorsque le client VPN télétravailleur démarre la connexion VPN, le serveur VPN IPSec transmet les stratégies IPSec au client VPN télétravailleur et crée le tunnel correspondant.

Pour configurer le client VPN télétravailleur, procédez de la façon suivante :

Étape 1 Cliquez sur **VPN > Client VPN télétravailleur** et configurez les paramètres suivants :

Client VPN télétravailleur	Cochez la case Activé ou Désactivé . Seul un client VPN télétravailleur peut être actif au démarrage. Si vous activez un client VPN télétravailleur au démarrage, cette option est désactivée sur d'autres règles du client.
Nouvelle tentative d'initiation automatique	Cochez la case Activé ou Désactivé .
Intervalle entre les tentatives	Saisissez la durée, en secondes (plage comprise entre 120 et 1 800 secondes).
Limite de tentatives	Saisissez le nombre maximal de nouvelles tentatives (plage comprise entre 0 et 16).

Étape 2 Cliquez sur **Appliquer**.

Étape 3 Dans la table Client VPN télétravailleur, cliquez sur **Ajouter**.

Étape 4 Fournissez les informations suivantes dans la section Paramètres de base :

Nom	Donnez un nom au profil.
Serveur (adresse distante)	Saisissez l'adresse IP du serveur distant.

Connexion active au démarrage	Ce paramètre permet d'activer la connexion au démarrage. Il est à tout moment possible de définir le profil sur l'état Activé pour activer les négociations au démarrage
Méthode d'authentification IKE	<p>Méthode d'authentification à utiliser lors des négociations IKE dans les tunnels IKE.</p> <ul style="list-style-type: none"> • 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. Cochez la case Clé prépartagée, puis saisissez le nom du groupe et le mot de passe dans les champs correspondants. • 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. Cochez la case Certificat et sélectionnez Par défaut.
Mode	<ul style="list-style-type: none"> • Client : la demande d'adresses IP et de serveur de la part du client fournit les adresses IP dans la plage d'adresses configurée. Sélectionnez Client et saisissez le nom d'utilisateur et le mot de passe. • NEM (Mode d'extension du réseau) : les clients proposent leur sous-réseau, et les services VPN doivent être appliqués sur le trafic entre le réseau LAN derrière le serveur et le sous-réseau proposé par le client. Le mode NEM du client ezvpn prend uniquement en charge l'adresse IP LAN 10.0.0/8, 172.16.0/12 ou 192.168.0/16. Par ailleurs, le réseau LAN derrière le serveur et le client doit se trouver dans un sous-réseau différent en mode NEM. Sélectionnez NEM, puis sélectionnez les réseaux VLAN dans les menus déroulants et saisissez le nom d'utilisateur et le mot de passe.
VLAN	Sélectionnez un réseau VLAN.
Nom d'utilisateur	Saisissez un nom d'utilisateur.
Mot de passe utilisateur	Saisissez un mot de passe.
Confirmer le mot de passe utilisateur	Confirmez le mot de passe.

Pour les paramètres avancés

Serveurs de secours 1, 2 et 3	Saisissez l'adresse IP ou le nom de domaine des serveurs de secours 1, 2 et 3. Lorsque la connexion au serveur VPN IPsec principal échoue, le dispositif de sécurité peut démarrer la connexion VPN sur les serveurs de secours. Le serveur de secours 1 a la priorité la plus haute et le serveur de secours 3 a la priorité la plus basse.
--------------------------------------	--

Délai d'expiration de l'homologue	Saisissez la durée, en secondes (plage comprise entre 30 et 480 secondes).
--	--

Étape 5 Cliquez sur **Appliquer**.

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 25 tunnels VPN PPTP pour les utilisateurs qui exécutent un logiciel client PPTP. Dans l'Assistant, l'utilisateur choisit l'option qui lui permet d'établir une connexion avec son lieu de travail via une connexion VPN.

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	Si vous avez activé PPTP, saisissez les adresses IP de début et de fin.
Adresses IP DNS1 et 2	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 Par défaut).
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**.

Serveur L2TP

Le protocole L2TP (Layer Two Tunneling Protocol) est une extension du protocole PPTP utilisée par un fournisseur d'accès à Internet (FAI) pour activer le VPN sur Internet. Le protocole L2TP ne crypte pas les données qu'il tunnelise. Le cryptage de ces données se fait via d'autres protocoles de sécurité tels qu'IPsec.

Le tunnel L2TP est établi entre le concentrateur d'accès L2TP (LAC) et le serveur réseau L2TP (LNS). Un tunnel IPsec est également établi entre ces périphériques, et l'ensemble du trafic du tunnel L2TP est chiffré à l'aide du protocole IPsec.

Pour configurer le serveur L2TP, procédez de la façon suivante :

Étape 1 Cliquez sur **VPN > Serveur L2TP**.

Étape 2 Saisissez les informations suivantes :

Serveur L2TP	Sélectionnez Activé ou Désactivé pour activer ou désactiver le serveur L2TP.
Unité maximale de transmission (MTU)	La MTU correspond au paquet le plus volumineux pouvant être transmis sur le tunnel L2TP. Si vous avez activé L2TP, saisissez la taille d'un paquet (plage 128-1 400, valeur par défaut 1 400).
Authentification de l'utilisateur	Sélectionnez l'authentification de l'utilisateur (Nom du groupe ou admin).
Pool d'adresses	<ul style="list-style-type: none"> • Adresse IP de début : saisissez l'adresse IP de début. • Adresse IP de fin : saisissez l'adresse IP de fin.
Adresses IP DNS1 et 2	Saisissez les adresses IP principale et secondaire des serveurs DNS1 et 2.
IPSec	Sélectionnez Activé pour activer la sécurité IPSec pour le tunnel L2TP.
Profil IPSec	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.
Confirmer la clé prépartagée	Saisissez de nouveau la clé prépartagée afin de la confirmer.

Étape 3 Cliquez sur **Appliquer**.

VPN SSL

Le VPN SSL (réseau privé virtuel Secure Sockets Layer) permet d'accéder à distance à des réseaux restreints via un chemin d'accès sécurisé et authentifié en cryptant le trafic réseau. Le routeur prend en charge le client VPN Cisco AnyConnect qui peut être téléchargé depuis [<http://www.cisco.com/go/anyconnect/>]. Le routeur prend en charge 2 tunnels VPN SSL par défaut et l'utilisateur peut demander une licence pour prendre en charge jusqu'à 50 tunnels. Une fois installé et activé, le VPN SSL établit un tunnel VPN sécurisé à accès distant.

**Remarque**

En outre, une licence Client pour la mobilité sécurisée Cisco AnyConnect est requise pour installer et utiliser le client pour la mobilité sécurisée Cisco AnyConnect sur votre appareil. Vous trouverez des informations sur la commande de licences utilisateur pour la mobilité sécurisée Cisco AnyConnect sur <http://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdf>. Nous recommandons une licence AnyConnect Plus pour 25 à 99 utilisateurs.

Pour configurer le VPN SSL, procédez de la façon suivante :

Étape 1

Cliquez sur **VPN > VPN SSL**.

Étape 2

Sous l'onglet Configuration générale du serveur, configurez les paramètres suivants :

Serveur VPN SSL Cisco	Sélectionnez Activé ou Désactivé pour activer ou désactiver le serveur.
------------------------------	---

Paramètres de passerelle obligatoires

Interface de passerelle	Sélectionnez l'interface de passerelle (WAN1, WAN2, USB1 ou USB2) dans la liste déroulante.
Port de passerelle	Saisissez le numéro de port de la passerelle (plage comprise entre 1 et 65 535).
Fichier de certificat	Valeur par défaut.
Pool d'adresses du client	Saisissez l'adresse IP du pool d'adresses du client.
Masque de réseau du client	Saisissez le masque de réseau du client.
Domaine du client	Saisissez le nom de domaine du client.
Bannière de connexion	Saisissez le texte devant s'afficher comme bannière de connexion.

Paramètres de passerelle facultatifs

Délai d'expiration de session inactive	Saisissez le délai d'expiration de session inactive, en secondes (plage comprise entre 60 et 86 400).
Délai d'expiration de session	Délai d'expiration d'une session TCP ou UDP après une période d'inactivité. Saisissez le délai d'expiration de session, en secondes (plage comprise entre 60 et 1 209 600).
Délai d'expiration DPD du client	Cette fonction permet d'envoyer des messages HELLO/ACK (bonjour/accusé de réception) régulièrement pour vérifier l'état du tunnel VPN. Cette fonction doit être activée sur les deux extrémités du tunnel VPN. Spécifiez l'intervalle entre les messages HELLO/ACK dans le champ Intervalle. Saisissez le délai d'expiration DPD du client, en secondes (plage comprise entre 0 et 3 600).
Délai d'expiration DPD de la passerelle	Cette fonction permet d'envoyer des messages HELLO/ACK (bonjour/accusé de réception) régulièrement pour vérifier l'état du tunnel VPN. Cette fonction doit être activée sur les deux extrémités du tunnel VPN. Spécifiez l'intervalle entre les messages HELLO/ACK dans le champ Intervalle. Saisissez le délai d'expiration DPD de la passerelle, en secondes (plage comprise entre 0 et 3 600).

Maintenir actif	Veillez à ce que votre routeur soit toujours connecté à Internet. Cette fonction tente de rétablir la connexion VPN si elle a été perdue. Saisissez le délai de maintien d'activité, en secondes (plage comprise entre 0 et 600).
Durée de la location	Saisissez la durée de connexion du tunnel, en secondes (plage comprise entre 600 et 1 209 600).
MTU max.	Saisissez la taille de paquet pouvant être envoyée sur le réseau, en octets (plage comprise entre 576 et 1 406).
Intervalle de relais	Saisissez l'intervalle de relais, en secondes (plage comprise entre 0 et 43 200).

Étape 3 Cliquez sur **Appliquer**.

Étape 4 Sous l'onglet Serveur de stratégies de groupe, cliquez sur **Ajouter** et saisissez les informations suivantes.

Paramètres de base

Nom de la stratégie	Saisissez le nom de la stratégie. Les stratégies de groupe permettent d'appliquer des ensembles d'attributs complets à un groupe d'utilisateurs plutôt que de spécifier chaque attribut individuellement pour chaque utilisateur.
DNS principal	Saisissez l'adresse IP du serveur DNS principal.
DNS secondaire	Saisissez l'adresse IP du serveur DNS secondaire.
WINS principal	Saisissez l'adresse IP du serveur WINS principal.
WINS secondaire	Saisissez l'adresse IP du serveur WINS secondaire.
Description	Saisissez une description.

Paramètres proxy IE

Stratégie de proxy IE	<p>Paramètres proxy d'Internet Explorer permettant d'établir le tunnel VPN. Sélectionnez la stratégie de proxy IE (Aucune, Auto, Ignorer-Local ou Désactivée) dans la liste déroulante.</p> <p>Si vous sélectionnez Auto ou Ignorer-Local, configurez les paramètres suivants :</p> <ul style="list-style-type: none"> • Adresse : adresse IP ou nom de domaine. • Port : saisissez un numéro de port (plage comprise entre 1 et 65 535).
------------------------------	---

Étape 5 Dans la table Proxy d'exceptions IE, cliquez sur **Ajouter, Modifier** ou **Supprimer** pour ajouter, modifier ou supprimer les exceptions IE.

Paramètres du tunneling fractionné

Activer le tunneling fractionné	Cochez la case Activer le tunneling fractionné pour autoriser l'envoi non crypté du trafic Internet directement sur Internet. Le tunneling intégral envoie l'ensemble du trafic au terminal, où il est ensuite acheminé vers les ressources de destination (éliminant ainsi le réseau d'entreprise du chemin pour l'accès Web).
--	--

Sélection du fractionnement	Sélectionnez Inclure le trafic pour inclure le trafic ou Exclure le trafic lors de l'application du tunneling fractionné.
------------------------------------	---

- Étape 6** Dans la table Fractionner le réseau, cliquez sur **Ajouter**, **Modifier** ou **Supprimer** pour ajouter, modifier ou supprimer les exceptions DNS de fractionnement.
- Étape 7** Configurez l'adresse IP et le masque de réseau.
- Étape 8** 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 l'intercommunication VPN, 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**.
-



Sécurité

Cette section fournit des renseignements sur la sécurité du réseau, à savoir les stratégies adoptées pour prévenir et gérer l'accès non autorisé, l'utilisation abusive, la modification ou le déni d'un réseau informatique. Elle contient les rubriques suivantes :

- [Assistant de contrôle d'application, page 109](#)
- [Contrôle d'application, page 110](#)
- [Filtrage Web, page 111](#)
- [Filtrage de contenu, page 112](#)
- [Protection de la source IP, page 113](#)

Assistant de contrôle d'application

Pour ajouter, configurer ou modifier les stratégies de contrôle d'application, procédez de la façon suivante :

-
- Étape 1** Cliquez sur **Sécurité > Assistant de contrôle d'application**.
 - Étape 2** Sur la page Contrôle d'application, sélectionnez **Activé** et saisissez le nom de la stratégie.
 - Étape 3** Cliquez sur **Suivant** puis, au-dessus de la table de la liste des applications, cliquez sur **Modifier** pour configurer les noms d'applications à filtrer (verrouiller ou consigner, etc.). Cliquez sur **Appliquer** après avoir sélectionné le contenu à filtrer.
 - Étape 4** Cliquez sur **Suivant**, puis sélectionnez l'horaire de verrouillage de l'application dans la liste déroulante.
 - Étape 5** Cliquez sur **Soumettre**.
-

Contrôle d'application

Pour ajouter, configurer ou modifier les stratégies de contrôle d'application, procédez de la façon suivante :

Étape 1 Cliquez sur **Sécurité > Contrôle d'application**.

Étape 2 Sur la page Contrôle d'application, sélectionnez **Activé**, puis cliquez sur **Appliquer**.

Étape 3 Pour créer une nouvelle stratégie de contrôle d'application, cliquez sur **Ajouter** sous la table des stratégies de contrôle d'application.

Étape 4 Dans la section Profil de stratégie - Ajouter/Modifier, spécifiez les informations suivantes :

Nom de la stratégie	Saisissez un nom.
Description	Saisissez une description.
Activer	Cochez cette option pour appliquer la stratégie de contrôle d'application.
Application	Cliquez sur Modifier , puis sélectionnez le contenu à filtrer (verrouiller ou consigner) dans la liste et cliquez sur Appliquer .
Table de la liste des applications	Cette table indique la catégorie, l'application et le comportement des filtres configurés.
Type de périphérique	Sélectionnez le type de périphérique dans la liste déroulante.
Type d'OS	Sélectionnez le système d'exploitation dans la liste déroulante.
Groupes IP	Sélectionnez un groupe IP dans la liste déroulante pour appliquer la stratégie.
Table de la liste d'exclusion	<p>Sous la table de la liste d'exclusion, cliquez sur Ajouter et configurez les paramètres suivants :</p> <ul style="list-style-type: none"> • Type : sélectionnez Mac ou Groupe IP • IP/ MAC : saisissez l'adresse MAC • Type de périphérique : sélectionnez le type de périphérique • Type d'OS : sélectionnez le type de système d'exploitation
Horaire	Pour spécifier l'horaire d'activation de la stratégie Contrôle d'application, sélectionnez l'horaire dans la liste déroulante ou cliquez sur Toujours activé pour appliquer le filtrage Web.

Étape 5 Cliquez sur **Appliquer**.

Filtrage Web

Le filtrage Web est une fonction qui vous protège contre l'accès à des sites Web inappropriés. Cette fonction peut filtrer les demandes d'accès Web du client afin d'autoriser ou non l'accès à la page sollicitée. Pour activer et configurer le filtrage Web, procédez de la façon suivante.

Étape 1 Cliquez sur **Sécurité > Filtrage Web**.

Étape 2 Dans la section Filtrage Web, sélectionnez **Activé ou Désactivé**, puis cliquez sur **Appliquer**.

Étape 3 Dans la table des stratégies de filtrage Web, cliquez sur **Ajouter**. Pour modifier une stratégie existante, cliquez sur **Modifier**.

Étape 4 Sur la page Filtrage Web — Ajouter/Modifier une stratégie, saisissez les informations suivantes :

Nom de la stratégie	Spécifiez un nom pour la stratégie de filtrage Web que vous créez.
Description	Décrivez brièvement la stratégie.
Activer	Cochez la case Activer pour activer la stratégie.
Catégorie	<ul style="list-style-type: none"> • Cliquez sur Modifier et sélectionnez le niveau de filtrage souhaité (sélectionnez les catégories Web appropriées à filtrer). Choisissez Élevé, Moyen, Bas ou Personnalisé pour définir le type de filtrage. Vous pouvez également choisir parmi les catégories Contenu pour adultes, Économie/Investissement, Divertissement, Contenu illicite/contestable, Ressources IT, Art de vivre/Culture, Autre et Sécurité. L'URL entrante appartenant aux catégories sélectionnées est bloquée. • Cliquez sur Appliquer pour revenir à la page Filtrage Web - Ajouter/Modifier la stratégie. Le contenu Web sélectionné s'affiche dans la table Liste des applications sous Catégorie. • Cliquez sur Restaurer les catégories par défaut pour restaurer les paramètres par défaut.
Type de périphérique	Dans la liste déroulante, sélectionnez le type de périphérique auquel appliquer la stratégie.
Type d'OS	Dans la liste déroulante, sélectionnez le système d'exploitation auquel appliquer la stratégie.
Réputation Web	Cochez cette case pour activer l'analyse de réputation Web.
Appliquée sur le groupe IP	Dans la liste déroulante, sélectionnez un groupe IP auquel appliquer la stratégie.

Liste d'exceptions	<p> Cliquez sur Modifier, puis sur Ajouter et définissez les paramètres suivants :</p> <ul style="list-style-type: none"> • Liste blanche : cliquez sur Ajouter pour définir le nom de domaine ou le mot-clé pour ignorer cette stratégie. • Liste noire : cliquez sur Ajouter pour définir le nom de domaine ou le mot-clé devant être bloqué. • Liste d'exclusion : cliquez sur Ajouter pour spécifier l'adresse IP exclue de cette stratégie. <p> Cliquez sur Appliquer.</p>
Horaire	<p>Sélectionnez l'horaire souhaité dans la liste déroulante. Cliquez sur Toujours activé pour appliquer le filtrage Web.</p>

Étape 5 Cliquez sur **OK** pour enregistrer la configuration.

Filtrage de contenu

Le filtrage de contenu permet de limiter l'accès aux clients à partir de 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 l'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 la case d'option souhaitée.

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 un domaine à filtrer/autoriser dans la colonne Nom de 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/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**.
-

Protection de la source IP

La protection de la source IP est une fonction de sécurité qui limite le trafic IP sur les adresses IP et MAC non approuvées en filtrant le trafic selon les liaisons IP/MAC configurées. Il s'agit d'un filtre qui autorise le trafic sur les ports LAN uniquement lorsque l'adresse IP et l'adresse MAC de chaque paquet correspondent aux entrées de la Table de liaisons IP/MAC. Cette fonction permet d'éviter les attaques d'usurpation d'adresse IP lorsqu'un hôte tente d'usurper et d'utiliser l'adresse IP d'un autre hôte.

Pour configurer la protection de la source IP, procédez de la façon suivante :

-
- Étape 1** Cliquez sur **Sécurité > Protection de la source IP**.
- Étape 2** Sélectionnez l'option **Activer la protection de la source IP** sur la liaison IP/MAC est requise.
- Étape 3** Sélectionnez l'option **Bloquer l'adresse MAC inconnue** uniquement si l'adresse MAC nécessite un filtrage, quelle que soit l'adresse IP.
- Étape 4** Dans la Table de liaisons IP/MAC, cliquez sur **Ajouter**, puis saisissez l'adresse IPv4 statique et l'adresse MAC pour la liaison.
- Étape 5** Cliquez sur **Appliquer**.
- Étape 6** Cliquez sur **Modifier** ou sur **Supprimer** pour modifier ou supprimer une adresse existante.
- Remarque** La Table des baux DHCP répertorie tous les baux DHCP statiques et dynamiques disponibles depuis le serveur/relais DHCP. Cliquez sur **Ajouter à la Table de liaisons IP/MAC** pour ajouter les baux disponibles à la table de liaisons.
- Vous devez ajouter manuellement les baux DHCP à la table de liaisons IP/MAC. Seules les baux de la table de liaisons IP/MAC fonctionnent.
- Remarque** L'IP Source Guard fonctionne uniquement sur l'hôte câblé du RV340W et non sur le réseau sans fil.
-



CHAPITRE 13

Pour en savoir plus

Cette section contient les rubriques suivantes :

- [Pour en savoir plus, page 115](#)

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	http://www.cisco.com/c/en/us/support/web/tsd-cisco-small-business-support-center-contacts.html
Téléchargement des microprogrammes Cisco	http://www.cisco.com/go/smallbizfirmware Sélectionnez un lien pour télécharger le microprogramme correspondant à votre produit Cisco. Aucune connexion n'est requise.
Demandes concernant les solutions 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/amointrie GNU), envoyez votre demande à l'adresse : external-opensource-requests@cisco.com . Dans votre demande, indiquez le nom et la version du produit Cisco, ainsi que le numéro de référence à 18 chiffres (par exemple : 7XEEX17D99-3X49X08 1) qui figure dans la documentation Open Source du produit.
Site Cisco Partner Central (connexion partenaire requise)	http://www.cisco.com/c/en/us/partners.html
Routeur Cisco RV340W	http://www.cisco.com/en/US/products/ps9923/tsd_products_support_series_home.html

