GUIDE D'ADMINISTRATION

Cisco
Routeur VPN double WAN Gigabit RV320/RV325

Sommaire

Sommaire

Sommaire

1

Mise en route

Les paramètres par défaut sont suffisants pour la plupart des petites entreprises. Des requêtes réseau ou votre fournisseur d'accès à Internet (FAI) peuvent nécessiter de modifier les paramètres. Pour utiliser l'interface Web, vous devez disposer d'un ordinateur sur lequel est installé Internet Explorer (version 6 ou supérieure), Firefox ou Safari (pour Mac).

Pour lancer l'interface Web :

ÉTAPE 1 Connectez un ordinateur à un port LAN numéroté du périphérique. Si l'ordinateur est configuré pour devenir un 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'adresse, entrez l'adresse IP par défaut du périphérique, à savoir **192.168.1.1**. Il se peut que le navigateur émette un avertissement signalant que le site Web est non sécurisé. Accédez au site Web.

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

ÉTAPE 5 Cliquez sur **Connexion**. La page **Récapitulatif système** s'affiche. Cochez la case **Activité du port** pour voir si une connexion WAN est activée. Sinon, passez à l'étape suivante.

ÉTAPE 6 Pour configurer votre connexion Internet à l'aide de l'Assistant de configuration, cliquez sur **Assistant de configuration** sur la page Récapitulatif système. Ou cliquez sur **Assistant** dans l'arborescence de navigation, puis sur **Lancer maintenant** dans la section Paramètres de base. Suivez les instructions affichées à l'écran.

Si votre navigateur Web affiche un message d'alerte relatif à la fenêtre contextuelle, autorisez le contenu bloqué.

ÉTAPE 7 Pour configurer d'autres paramètres, cliquez sur les liens de l'arborescence.

Conseils de dépannage

Si vous ne parvenez pas à vous connecter à Internet ni à l'interface Web :

- Vérifiez que votre navigateur Web n'est pas configuré pour travailler hors connexion.
- Vérifiez les paramètres de la connexion au réseau local de votre adaptateur Ethernet. L'ordinateur doit obtenir une adresse IP via le protocole DHCP. Il peut également disposer d'une adresse IP statique comprise dans la plage 192.168.1.x, lorsque la passerelle par défaut est définie sur 192.168.1.1 (adresse IP par défaut du périphérique).
- Vérifiez que les paramètres que vous avez saisis dans l'Assistant pour configurer votre connexion Internet sont corrects.
- Réinitialisez le modem et le périphérique, en mettant ces deux appareils hors tension. Remettez ensuite le modem sous tension et patientez pendant 2 minutes environ. Remettez le périphérique sous tension. Vous devriez alors recevoir une adresse IP du réseau WAN.
- Si votre modem est de type DSL, demandez à votre fournisseur d'accès à Internet de le basculer en mode pont.

Fonctions de l'interface utilisateur

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

Navigation

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

Fenêtres contextuelles

Certains liens et boutons déclenchent l'apparition de fenêtres contextuelles contenant des informations supplémentaires ou les pages de configuration associées. Si votre navigateur Web affiche un message d'alerte relatif à la fenêtre contextuelle, autorisez le contenu bloqué.

Aide

Pour afficher des informations sur la page de configuration sélectionnée, cliquez sur le lien **Aide** situé en haut à droite de l'interface Web. Si votre navigateur Web affiche un message d'alerte relatif à la fenêtre contextuelle, autorisez le contenu bloqué.

Déconnexion

Pour quitter l'interface Web, cliquez sur le lien **Déconnexion** situé en haut à droite de l'interface Web. La page **Connexion** apparaît.

2

Récapitulatif système

Le récapitulatif système affiche des informations sur l'état actuel des connexions, de l'état, des paramètres et des journaux du périphérique.

Informations système

Description des informations système :

- **Numéro de série** : numéro de série du périphérique.
- **Version du microprogramme** : numéro de version du microprogramme installé.
- **PID VID** : numéro de version du matériel.
- **Somme de contrôle MD5** : valeur utilisée pour la validation de fichiers.
- **LAN IPv4/Masque de sous-réseau** : adresse IP et masque de sous-réseau de gestion IPv4 du périphérique.
- **LAN IPv6/Préfixe** : adresse IP et préfixe de gestion IPv6.
- **Mode de fonctionnement** : gère le comportement du périphérique par rapport à la connexion WAN. Le mode passerelle est sélectionné lorsque le périphérique héberge une connexion WAN. Le mode routeur est sélectionné lorsque le périphérique est sur un réseau sans connexion WAN ou un autre périphérique est utilisé pour établir la connexion WAN. Pour modifier ce paramètre, cliquez sur **Mode de fonctionnement** pour afficher la fenêtre Routage avancé.
- **LAN** : adresse IP de gestion IPv4. Si la double pile IP est activée dans la page **Configuration du réseau**, l'adresse IPv6 et la longueur du préfixe s'affichent également.
- **Disponibilité du système** : durée en jours, heures et minutes d'activité du périphérique.

Configuration (Assistant)

Pour accéder à l'Assistant de configuration de la connexion Internet et être guidé dans le processus, cliquez sur **Assistant de configuration** pour lancer l'**Assistant**.

Activité du port

L'activité du port identifie les interfaces de port et indique l'état de chaque port :

- **ID du port** : libellé du port.
- **Interface** : type d'interface : LAN, WAN ou DMZ. Les différentes interfaces WAN sont identifiées par un numéro, par exemple WAN1 et WAN2.
- **État** : état du port : Désactivé (rouge), Activé (noir) ou Connecté (vert). La valeur de l'état est un hyperlien. Cliquez dessus pour ouvrir la fenêtre **Informations sur le port**.

Pour afficher les informations détaillées sur l'activité du lien actuel, cliquez sur l'entrée **État** pour le port.

Informations sur le port (détails)

La fenêtre Informations sur le port contient des informations détaillées relatives à l'interface et à l'activité actuelle sur le port.

- **Type** : type de port : 10BASE-T ou 100BASE-TX ou 1000BASE-T.
- **Interface** : type d'interface : LAN, DMZ ou WAN.
- **État de la liaison** : état de la liaison : Actif ou Inactif.
- **Activité du port** : activité actuelle sur le port : Port activé, Port désactivé ou Port connecté.
- **Priorité** : niveau de priorité des données du port : Élevé ou Normal.
- **État du débit** : vitesse du port : 10 Mbit/s à 1000 Mbit/s.
- **État du duplex** : mode duplex : Semi-duplex ou Duplex intégral.
- **Négociation auto** : état du paramètre de la négociation automatique ; lorsqu'il est activé, il détecte le mode duplex et si la connexion nécessite une détection automatique, il choisit automatiquement la configuration MDI ou MDIX qui correspond à l'autre extrémité de la liaison.

- **VLAN** : ID du réseau VLAN de ce port. Il existe deux réseaux VLAN prédéfinis : 25 et 100. VLAN 25 peut être utilisé pour l'accès VLAN invité et VLAN 100 peut être utilisé pour le trafic vocal. Par défaut, VLAN 25 et VLAN 100 ne sont pas activés.
- **Nombre de paquets reçus** : nombre de paquets reçus sur ce port.
- **Nombre d'octets de paquets reçus** : nombre d'octets reçus sur ce port.
- **Nombre de paquets émis** : nombre de paquets émis par ce port.
- **Nombre d'octets de paquets émis** : nombre d'octets émis par ce port.
- **Nombre d'erreurs de paquets** : nombre total d'erreurs de paquets.

IPv4 et IPv6

La section IPv4 ou IPv6 identifie les statistiques de chaque port WAN. (L'onglet IPv6 n'est disponible que si vous avez activé la double pile IP dans la page **Configuration du réseau**.)

Informations sur le WAN

Informations sur le réseau WAN :

- **Adresse IP** : adresse IP publique de l'interface.
- **Passerelle par défaut** : passerelle par défaut de l'interface.
- **DNS** : adresse IP du serveur DNS de l'interface.
- **DNS dynamique** : réglages DDNS du port : Activé ou Désactivé.
- **Libérer** et **Renouveler** : ces boutons apparaissent si le port est défini de façon à obtenir une adresse IP depuis un serveur. Cliquez sur **Libérer** pour libérer l'adresse IP. Cliquez sur **Renouveler** pour actualiser la durée de bail ou obtenir une nouvelle adresse IP.
- **Connecter** et **Déconnecter** : ces boutons apparaissent si le port est défini sur PPPoE ou PPTP. Cliquez sur **Déconnecter** pour vous déconnecter du service Internet. Cliquez sur **Connecter** pour établir la connexion.

Informations sur la DMZ

Informations sur la DMZ :

- **Adresse IP** : adresse IP publique actuelle de l'interface.
- **Hôte DMZ** : adresse IP privée de l'hôte DMZ. La valeur par défaut est **Désactivé**.

État de la sécurité

Cette section affiche l'état des fonctions de sécurité :

- **SPI (Stateful Packet Inspection)** : état du pare-feu : Activé (vert) ou Désactivé (rouge). Surveille l'état des connexions réseau (flux TCP, communication UDP, etc.) qui passent par le pare-feu. Le pare-feu distingue les paquets légitimes pour différents types de connexion. Le pare-feu autorise uniquement les paquets correspondant à une connexion active connue ; les autres sont rejetés.
- **DoS (Denial of Service)** : état du filtre DoS. Activé (vert) ou Désactivé (rouge). Une attaque DoS vise à rendre un ordinateur ou un réseau indisponible.
- **Bloquer la requête WAN** : cette fonction permet de rendre plus difficile l'accès au réseau pour les utilisateurs extérieurs en *masquant* les ports réseau des périphériques Internet ; elle permet également de prémunir le réseau contre les opérations ping et les détections par d'autres utilisateurs Internet. L'état est Activé) (vert) ou Désactivé (rouge). Bloquer la requête WAN
- **Gestion à distance** : indique si une connexion à distance destinée à gérer le périphérique est autorisée ou refusée. Activé (vert) indique que la gestion à distance est autorisée. Désactivé (rouge) indique que la gestion à distance est refusée.
- **Règles d'accès** : nombre de règles d'accès définies.

Pour afficher des informations détaillées sur les fonctions de sécurité, cliquez sur le libellé de la fonction.

État des paramètres VPN

Cette section affiche l'état des tunnels VPN :

- **Tunnel(s) VPN utilisé(s)** : tunnels VPN utilisés.
- **Tunnel(s) VPN disponible(s)** : tunnels VPN disponibles.
- **Tunnel(s) Easy VPN utilisé(s)** : tunnels Easy VPN utilisés.
- **Tunnel(s) Easy VPN disponible(s)** : tunnels Easy VPN disponibles.

- **Tunnel(s) PPTP utilisé(s)** : tunnels PPTP (Point to Point Tunneling Protocol) utilisés. PPTP est une méthode de mise en place de réseaux privés virtuels. PPTP utilise un canal de contrôle sur TCP et un tunnel d'encapsulation d'acheminement générique (GRE) pour encapsuler les paquets PPP.
- **Tunnel(s) PPTP disponible(s)** : tunnels PPTP disponibles.

État VPN SSL

Un réseau VPN SSL permet d'établir une connexion depuis des sites où IPsec rencontre des problèmes avec la traduction des adresses réseau (NAT) et les règles de pare-feu :

- **Tunnel(s) VPN SSL utilisé(s)** : tunnels VPN SSL utilisés.
- **Tunnel(s) VPN SSL disponible(s)** : tunnels VPN SSL encore disponibles.

État des paramètres de journaux

Cette section affiche l'état des journaux :

- **Serveur Syslog** : état du SYSLOG : Activé (vert) ou Désactivé (rouge).
- **Journal de messagerie)** : état du journal de messagerie : Activé (vert) ou Désactivé (rouge).

3

Configuration

Utilisez la page Configuration > Réseau pour configurer vos réseaux LAN, WAN (Internet), DMZ, etc.

Configuration du réseau

Certains FAI requièrent que vous indiquiez un nom d'hôte et un nom de domaine pour identifier votre périphérique. Des valeurs par défaut sont fournies, mais vous pouvez les modifier si vous le souhaitez.

- **Nom d'hôte** : conservez le paramètre par défaut ou saisissez le nom d'hôte spécifié par votre FAI.
- **Nom de domaine** : conservez le paramètre par défaut ou saisissez le nom de domaine spécifié par votre FAI.

Mode IP

Choisissez le type d'adressage à utiliser sur les réseaux :

- **IPv4 uniquement** : utilisez uniquement l'adressage IPv4.
- **Double pile IP** : utilisez l'adressage IPv4 et IPv6. Une fois les paramètres enregistrés, vous pouvez configurer les adresses IPv4 et IPv6 des réseaux LAN, WAN et DMZ.

Ajout ou modification d'un réseau IPv4

Un sous-réseau LAN IPv4 est configuré par défaut (192.168.1.1). Un sous-réseau est généralement suffisant pour la plupart des petites entreprises. Le pare-feu refuse l'accès si l'adresse IP source du périphérique se trouve sur un sous-réseau qui n'est pas spécifiquement autorisé. Vous pouvez autoriser le trafic en provenance d'autres sous-réseaux et utiliser ce périphérique comme routeur de périphérie qui fournit une connectivité Internet à un réseau.

ÉTAPE 1 Cliquez sur l'onglet **IPv4** pour afficher la table de sous-réseaux multiples.

ÉTAPE 2 Pour ajouter un sous-réseau, cliquez sur **Ajouter**. Les champs Adresse IP et Masque de sous-réseau s'affichent dans les colonnes. Après avoir cliqué sur le bouton **Enregistrer**, vous pouvez modifier le sous-réseau afin qu'il fasse partie du réseau VLAN, gérer les adresses IP via le serveur DHCP ou définir les paramètres du serveur TFTP.

ÉTAPE 3 Saisissez l'**adresse IP** et le **masque de sous-réseau** du périphérique.

ÉTAPE 4 Cliquez sur **Enregistrer** pour enregistrer vos modifications ou sur **Annuler** pour les annuler.

Pour modifier un sous-réseau, sélectionnez le sous-réseau IPv4 à modifier et cliquez sur **Modifier**. La section **Configuration DHCP** décrit le processus de modification des paramètres de sous-réseau.

Modification du préfixe d'adresse IPv6

Si vous avez activé l'option Double pile IP pour le mode IP, vous pouvez configurer le préfixe IPv6.

Pour configurer le préfixe IPv6, cliquez sur l'onglet **IPv6**, sélectionnez le préfixe IPv6 et cliquez sur **Modifier**. L'adresse IP par défaut est fc00::1 tandis que la longueur du préfixe par défaut est 7. L'onglet IPv6 est seulement disponible si l'option **Double pile IP** est activée dans la table **Mode IP**. La fenêtre **Configuration DHCP** apparaît.

Paramètres des ports WAN1 et WAN2

La table Paramètre WAN affiche l'interface (USB1, WAN1 ou WAN2, par exemple) et le type de connexion. Vous pouvez modifier les paramètres des interfaces.

REMARQUE Si vous utilisez l'IPv6, sélectionnez l'onglet **IPv6** avant de sélectionner l'interface WAN à configurer. Sinon, les paramètres IPv6 ne s'affichent pas dans la fenêtre **Paramètres de la connexion WAN**.

Afin de configurer les **paramètres de la connexion WAN**, sélectionnez une interface WAN et cliquez sur **Modifier**. La fenêtre **Paramètres de la connexion WAN** apparaît.

Sélectionnez **Type de connexion WAN** dans le menu et modifiez les paramètres associés, comme décrit dans les sections suivantes :

Obtenir une adresse IP automatiquement

Sélectionnez cette option si votre FAI attribue une adresse IP de manière dynamique au périphérique. (La plupart des abonnés aux modems-câbles utilisent ce type de connexion). Le FAI affecte l'adresse IP du périphérique pour ce port, y compris les adresses IP du serveur DNS.

Pour spécifier un serveur DNS, cochez la case **Utiliser les adresses de serveur DNS suivantes** et saisissez l'adresse IP du **serveur DNS 1**. Vous pouvez éventuellement saisir un second serveur DNS. Le premier serveur DNS disponible est utilisé.

Afin de définir automatiquement la taille maximale des unités de transmission (**MTU**), sélectionnez **Automatique**. Sinon, afin de définir manuellement la taille des **MTU**, sélectionnez **Manuel** et saisissez la taille des MTU. (Taille en octets de l'unité de données du protocole la plus importante que la couche peut traiter).

Pour configurer les paramètres IPv6, cochez la case **Activer**. Le processus client DHCPv6 et les demandes de délégation de préfixe via l'interface sélectionnée sont activés. Utilisez cette option lorsque votre FAI est en mesure d'envoyer des préfixes LAN à l'aide du DHCPv6. Si votre FAI ne prend pas cette option en charge, configurez manuellement un préfixe LAN :

REMARQUE Si la fonctionnalité DHCP-PD est activée, l'adressage manuel LAN IPv6 est désactivé. Si la fonctionnalité DHCP-PD est désactivée, l'adressage manuel LAN IPv6 est activé.

- **Adresse LAN IPv6** : préfixe IPv6 global attribué par votre FAI à vos périphériques LAN, le cas échéant. (Pour en savoir plus à ce sujet, renseignez-vous auprès de votre FAI).
- **Longueur du préfixe** : longueur du préfixe IPv6. Le réseau (sous-réseau) IPv6 est identifié par les premiers bits de l'adresse, qui constituent le préfixe. Tous les hôtes du réseau comportent les mêmes bits initiaux dans leur adresse IPv6. Saisissez le nombre de bits initiaux communs des adresses du réseau. La longueur par défaut du préfixe est 64.
- **Affectation du préfixe du LAN** :
  - **Sans action** : ne fournit pas d'adresse IPv6 sans état ou avec état aux ordinateurs côté LAN.
  - **Configurer sur annonce du routeur automatiquement** : fournit une adresse IPv6 *sans état* aux ordinateurs côté LAN.
  - **Configurer sur DHCPv6 automatiquement** : fournit une adresse IPv6 *avec état* aux ordinateurs côté LAN.

- Configurer sur annonce du routeur et DHCPv6 automatiquement : fournit des adresses IPv6 sans état et avec état aux ordinateurs côté LAN.

IP statique

Sélectionnez cette option si votre FAI a attribué une adresse IP permanente à votre compte. Saisissez les paramètres qui vous ont été communiqués par votre FAI.

- **Spécifier l'adresse IP de réseau WAN** : adresse IP que votre FAI a attribué à votre compte.
- **Masque de sous-réseau (IPv4)** : masque du sous-réseau.
- **Adresse de la passerelle par défaut** : adresse IP de la passerelle par défaut.

Pour spécifier un serveur DNS, saisissez l'adresse IP du **serveur DNS 1**. Vous pouvez éventuellement saisir un second serveur DNS. Le premier serveur DNS disponible est utilisé.

Afin de définir automatiquement la taille maximale des unités de transmission (**MTU**), sélectionnez **Automatique**. Sinon, afin de définir manuellement la taille des **MTU**, sélectionnez **Manuel** et saisissez la taille des MTU. (Taille en octets de l'unité de données du protocole la plus importante que la couche peut traiter).

Pour configurer les paramètres IPv6 :

- **Adresse LAN IPv6** : préfixe IPv6 global attribué par votre FAI à vos périphériques LAN, le cas échéant. (Pour en savoir plus à ce sujet, renseignez-vous auprès de votre FAI).
- **Longueur du préfixe** : longueur du préfixe IPv6. Le réseau (sous-réseau) IPv6 est identifié par les premiers bits de l'adresse, qui constituent le préfixe. Tous les hôtes du réseau comportent les mêmes bits initiaux dans leur adresse IPv6. Saisissez le nombre de bits initiaux communs des adresses du réseau. La longueur par défaut du préfixe est 64.
- **Affectation du préfixe du LAN**
  - **Sans action** : ne fournit pas d'adresse IPv6 sans état ou avec état aux ordinateurs côté LAN.
  - **Configurer sur annonce du routeur automatiquement** : fournit une adresse IPv6 *sans état* aux ordinateurs côté LAN.
  - **Configurer sur DHCPv6 automatiquement** : fournit une adresse IPv6 *avec état* aux ordinateurs côté LAN.
  - **Configurer sur annonce du routeur et DHCPv6 automatiquement** : fournit des adresses IPv6 sans état et avec état aux ordinateurs côté LAN.

PPPoE

Sélectionnez cette option si votre FAI utilise le protocole PPPoE (Point-to-Point Protocol over Ethernet) pour établir des connexions à Internet (ce qui est généralement le cas des lignes ADSL). Saisissez ensuite les paramètres spécifiés par votre fournisseur d'accès à Internet :

- **Nom d'utilisateur** et **Mot de passe** : nom d'utilisateur et mot de passe de votre compte FAI. Le nombre maximal de caractères pour chaque entrée est de 255.
- **Nom du service** : un ensemble de services fourni par le FAI identifié par le nom du service.
- **Compteurs de connexion** : la connexion prend fin après une période d'inactivité.
  - **Connexion à la demande** : lorsque cette fonctionnalité est activée, le périphérique établit automatiquement la connexion. Si cette fonctionnalité est activée, saisissez le **délai d'inactivité maximale**, le nombre de minutes durant lesquelles la connexion peut rester inactive avant de prendre fin. Le délai d'inactivité maximal par défaut est de 5 minutes.
  - **Maintenir actif** : cette fonctionnalité permet de garantir que votre routeur est toujours connecté à Internet. Lorsque cette fonctionnalité est sélectionnée, le routeur garde cette connexion active en envoyant régulièrement quelques paquets de données. Cette option permet de maintenir votre connexion active indéfiniment, même si le lien reste inactif pendant une durée prolongée. Si vous activez cette fonctionnalité, définissez également la valeur **Intervalle de nouvelle numérotation** pour spécifier la fréquence à laquelle le routeur doit vérifier votre connexion Internet. La période par défaut est de 30 secondes.
- **Utiliser les adresses de serveur DNS suivantes** : active l'obtention des informations relatives à la connexion depuis les serveurs DNS.
- **Serveur DNS 1** et **Serveur DNS 2** : adresse IP des serveurs DNS. Vous pouvez éventuellement saisir un second serveur DNS. Le premier serveur DNS disponible est utilisé.
- **MTU** : taille maximale des unités de transmission (**MTU**). Sélectionnez **Automatique** pour définir automatiquement la taille. Sinon, afin de définir manuellement la taille des **MTU**, sélectionnez **Manuel** et saisissez la taille des MTU. (Taille en octets de l'unité de données du protocole la plus importante que la couche peut traiter).

Pour configurer les paramètres IPv6, cochez la case **Activer**. Le processus client DHCPv6 et les demandes de délégation de préfixe via l'interface sélectionnée sont activés. Utilisez cette option lorsque votre FAI est en mesure d'envoyer des préfixes LAN à l'aide du DHCPv6. Si votre FAI ne prend pas cette option en charge, configurez manuellement un préfixe LAN :

REMARQUE Si la fonctionnalité DHCP-PD est activée, l'adressage manuel LAN IPv6 est désactivé. Si la fonctionnalité DHCP-PD est désactivée, l'adressage manuel LAN IPv6 est activé.

- **Adresse LAN IPv6** : préfixe IPv6 global attribué par votre FAI à vos périphériques LAN, le cas échéant. (Pour en savoir plus à ce sujet, renseignez-vous auprès de votre FAI).
- **Longueur du préfixe** : longueur du préfixe IPv6. Le réseau (sous-réseau) IPv6 est identifié par les premiers bits de l'adresse, qui constituent le préfixe. Tous les hôtes du réseau comportent les mêmes bits initiaux dans leur adresse IPv6. Saisissez le nombre de bits initiaux communs des adresses du réseau. La longueur par défaut du préfixe est 64.
- **Affectation du préfixe du LAN** :
  - **Sans action** : ne fournit pas d'adresse IPv6 sans état ou avec état aux ordinateurs côté LAN.
  - **Configurer sur annonce du routeur automatiquement** : fournit une adresse IPv6 *sans état* aux ordinateurs côté LAN.
  - **Configurer sur DHCPv6 automatiquement** : fournit une adresse IPv6 *avec état* aux ordinateurs côté LAN.
  - **Configurer sur annonce du routeur et DHCPv6 automatiquement** : fournit des adresses IPv6 sans état et avec état aux ordinateurs côté LAN.

PPTP (IPv4)

Sélectionnez cette option si votre FAI l'exige. Le protocole PPTP (Point-to-Point Tunneling Protocol - protocole de tunnellisation point à point) est un service utilisé en Europe et en Israël uniquement.

- **Spécifier l'adresse IP de réseau WAN** : adresse IP que votre FAI a attribué à votre compte.
- **Masque de sous-réseau (IPv4)** : masque du sous-réseau affecté à votre compte.
- **Adresse de la passerelle par défaut** : adresse IP de la passerelle par défaut.
- **Nom d'utilisateur** et **Mot de passe** : nom d'utilisateur et mot de passe de votre compte FAI. Le nombre maximal de caractères est fixé à 60.

- **Compteurs de connexion** : la connexion prend fin après une période d'inactivité.
  - **Connexion à la demande** : lorsque cette fonctionnalité est activée, le périphérique établit automatiquement la connexion. Si cette fonctionnalité est activée, saisissez le **délai d'inactivité maximale**, le nombre de minutes durant lesquelles la connexion peut rester inactive avant de prendre fin. Le délai d'inactivité maximal par défaut est de 5 minutes.
  - **Maintenir actif** : cette fonctionnalité permet de garantir que votre routeur est toujours connecté à Internet. Lorsque cette fonctionnalité est sélectionnée, le routeur garde cette connexion active en envoyant régulièrement quelques paquets de données. Cette option permet de maintenir votre connexion active indéfiniment, même si le lien reste inactif pendant une durée prolongée. Si vous activez cette fonctionnalité, définissez également la valeur **Intervalle de nouvelle numérotation** pour spécifier la fréquence à laquelle le routeur doit vérifier votre connexion Internet. La période par défaut est de 30 secondes.
- **MTU** : taille maximale des unités de transmission (**MTU**). Sélectionnez **Automatique** pour définir automatiquement la taille. Sinon, afin de définir manuellement la taille des **MTU**, sélectionnez **Manuel** et saisissez la taille des MTU. (Taille en octets de l'unité de données du protocole la plus importante que la couche peut traiter).

Pont transparent (IPv4)

Sélectionnez cette option si vous utilisez ce routeur pour connecter deux segments de réseau. Une seule interface WAN peut être configurée comme pont transparent.

- **Spécifier l'adresse IP de réseau WAN** : adresse IP externe que votre FAI a attribué à votre compte.
- **Masque de sous-réseau** : masque de sous-réseau spécifié par votre FAI.
- **Adresse de la passerelle par défaut** : adresse IP de la passerelle par défaut.
- **Serveur DNS 1** et **Serveur DNS 2** : adresses IP des serveurs DNS. Vous pouvez éventuellement saisir un second serveur DNS. Le premier serveur DNS disponible est utilisé.
- **Plage d'adresses IP de réseau LAN interne** : plage d'adresses IP du réseau LAN interne raccordé. Les réseaux WAN et LAN du pont transparent doivent partager le même sous-réseau.
- **MTU** : taille maximale des unités de transmission (**MTU**). Sélectionnez **Automatique** pour définir automatiquement la taille. Sinon, afin de définir manuellement la taille des **MTU**, sélectionnez **Manuel** et saisissez la taille des MTU. (Taille en octets de l'unité de données du protocole la plus importante que la couche peut traiter).

Configuration automatique de l'adresse sans état (IPv6)

Sélectionnez cette option si votre FAI utilise des sollicitations et annonces de routeur IPv6. Les hôtes du réseau déterminent à quel réseau ils sont connectés et, une fois cela déterminé, ils sont en mesure de configurer automatiquement l'ID de l'hôte sur ce réseau.

Pour spécifier un serveur DNS, saisissez l'adresse IP du **serveur DNS 1**. Vous pouvez éventuellement saisir un second serveur DNS. Le premier serveur DNS disponible est utilisé.

Afin de définir automatiquement la taille maximale des unités de transmission (**MTU**), sélectionnez **Automatique**. Sinon, afin de définir manuellement la taille des **MTU**, sélectionnez **Manuel** et saisissez la taille des MTU. (Taille en octets de l'unité de données du protocole la plus importante que la couche peut traiter).

Pour configurer les paramètres IPv6 :

- **Adresse LAN IPv6** : préfixe IPv6 global attribué par votre FAI à vos périphériques LAN, le cas échéant. (Pour en savoir plus à ce sujet, renseignez-vous auprès de votre FAI).
- **Longueur du préfixe** : longueur du préfixe IPv6. Le réseau (sous-réseau) IPv6 est identifié par les premiers bits de l'adresse, qui constituent le préfixe. Tous les hôtes du réseau comportent les mêmes bits initiaux dans leur adresse IPv6. Saisissez le nombre de bits initiaux communs des adresses du réseau. La longueur par défaut du préfixe est 64.
- **Affectation du préfixe du LAN** :
  - **Sans action** : ne fournit pas d'adresse IPv6 sans état ou avec état aux ordinateurs côté LAN.
  - **Configurer sur annonce du routeur automatiquement** : fournit une adresse IPv6 *sans état* aux ordinateurs côté LAN.
  - **Configurer sur DHCPv6 automatiquement** : fournit une adresse IPv6 *avec état* aux ordinateurs côté LAN.
  - **Configurer sur annonce du routeur et DHCPv6 automatiquement** : fournit des adresses IPv6 sans état et avec état aux ordinateurs côté LAN.

Tunnel IPv6 dans IPv4 (IPv6)

Sélectionnez cette option si votre FAI utilise le tunnel IPv6 dans IPv4 pour établir la connexion Internet.

Vous devez saisir une adresse **IP statique** IPv4. Saisissez ensuite les paramètres spécifiés par votre fournisseur d'accès à Internet :

- **Adresse IPv6 locale** : adresse IPv6 locale de votre compte FAI.
- **Adresse IPv4 distante)** : adresse IPv4 distante de votre compte FAI.
- **Adresse IPv6 distante** : adresse IPv6 distante de votre compte FAI.
- **Serveur DNS 1** et **Serveur DNS 2** : adresses IP des serveurs DNS. Vous pouvez éventuellement saisir un second serveur DNS. Le premier serveur DNS disponible est utilisé.
- **Adresse LAN IPv6** : préfixe IPv6 global attribué par votre FAI à vos périphériques LAN, le cas échéant. (Pour en savoir plus à ce sujet, renseignez-vous auprès de votre FAI).
- **Longueur du préfixe** : longueur du préfixe IPv6. Le réseau (sous-réseau) IPv6 est identifié par les premiers bits de l'adresse, qui constituent le préfixe. Tous les hôtes du réseau comportent les mêmes bits initiaux dans leur adresse IPv6. Saisissez le nombre de bits initiaux communs des adresses du réseau. La longueur par défaut du préfixe est 64.
- **Affectation du préfixe du LAN**
  - **Sans action** : ne fournit pas d'adresse IPv6 sans état ou avec état aux ordinateurs côté LAN.
  - **Configurer sur annonce du routeur automatiquement** : fournit une adresse IPv6 *sans état* aux ordinateurs côté LAN.
  - **Configurer sur DHCPv6 automatiquement** : fournit une adresse IPv6 *avec état* aux ordinateurs côté LAN.
  - **Configurer sur annonce du routeur et DHCPv6 automatiquement** : fournit des adresses IPv6 sans état et avec état aux ordinateurs côté LAN.

Tunnel 6to4 (IPv6)

Sélectionnez cette option pour établir un tunnel automatique au niveau du réseau IPv4 (ou une connexion Internet IPv4 réelle) entre deux réseaux IPv6 indépendants. Saisissez les paramètres suivants :

Adresse IPv4 du relais : permet à l'hôte 6to4 de communiquer avec l'Internet IPv6 natif. Il doit contenir une passerelle IPv6 par défaut définie sur une adresse 6to4 contenant l'adresse IPv4 du routeur de relais 6to4. Afin que les utilisateurs n'aient pas à définir cette adresse manuellement, l'adresse de pluridiffusion `192.88.99.1` a été attribuée au routeur de relais 6to4 pour l'envoi des paquets.

- **Serveur DNS 1** et **Serveur DNS 2** : adresses IP des serveurs DNS. Vous pouvez éventuellement saisir un second serveur DNS. Le premier serveur DNS disponible est utilisé.
- **Adresse LAN IPv6** : préfixe IPv6 global attribué par votre FAI à vos périphériques LAN, le cas échéant. (Pour en savoir plus à ce sujet, renseignez-vous auprès de votre FAI).
- **Longueur du préfixe** : longueur du préfixe IPv6. Le réseau (sous-réseau) IPv6 est identifié par les premiers bits de l'adresse, qui constituent le préfixe. Tous les hôtes du réseau comportent les mêmes bits initiaux dans leur adresse IPv6. Saisissez le nombre de bits initiaux communs des adresses du réseau. La longueur par défaut du préfixe est 64.
- **Affectation du préfixe du LAN**
  - **Sans action** : ne fournit pas d'adresse IPv6 sans état ou avec état aux ordinateurs côté LAN.
  - **Configurer sur annonce du routeur automatiquement** : fournit une adresse IPv6 *sans état* aux ordinateurs côté LAN.
  - **Configurer sur DHCPv6 automatiquement** : fournit une adresse IPv6 *avec état* aux ordinateurs côté LAN.
  - **Configurer sur annonce du routeur et DHCPv6 automatiquement** : fournit des adresses IPv6 sans état et avec état aux ordinateurs côté LAN.

Tunnel 6rd (IPv6 Rapid Deployment)

Sélectionnez cette option si votre FAI utilise le tunnel 6rd (IPv6 Rapid Deployment) pour établir la connexion Internet. Saisissez les paramètres qui vous ont été communiqués par votre FAI.

- **Mode de configuration 6rd** :
  - **Manuel** : définissez manuellement le préfixe 6rd, l'adresse IPv4 du relais et la longueur du masque IPv4 fournis par votre FAI.
  - **Automatique (DHCP)** : utilisez le DHCP (option 212) pour obtenir le préfixe 6rd, l'adresse IPv4 du relais et la longueur du masque IPv4.
- **Préfixe 6rd** : préfixe 6rd de votre compte FAI.
- **Adresse IPv4 distante** : adresse IPv4 distante de votre compte FAI.
- **Longueur du masque IPv4** : longueur du masque de sous-réseau IPv4 6rd de votre compte FAI. (Cette valeur est généralement égale à 0).
- **Serveur DNS 1** et **Serveur DNS 2** : adresses IP des serveurs DNS. Vous pouvez éventuellement saisir un second serveur DNS. Le premier serveur DNS disponible est utilisé.
- **Adresse LAN IPv6** : préfixe IPv6 global attribué par votre FAI à vos périphériques LAN, le cas échéant. (Pour en savoir plus à ce sujet, renseignez-vous auprès de votre FAI).
- **Longueur du préfixe** : longueur du préfixe IPv6. Le réseau (sous-réseau) IPv6 est identifié par les premiers bits de l'adresse, qui constituent le préfixe. Tous les hôtes du réseau comportent les mêmes bits initiaux dans leur adresse IPv6. Saisissez le nombre de bits initiaux communs des adresses du réseau. La longueur par défaut du préfixe est 64.
- **Affectation du préfixe du LAN**
  - **Sans action** : ne fournit pas d'adresse IPv6 sans état ou avec état aux ordinateurs côté LAN.
  - **Configurer sur annonce du routeur automatiquement** : fournit une adresse IPv6 *sans état* aux ordinateurs côté LAN.
  - **Configurer sur DHCPv6 automatiquement** : fournit une adresse IPv6 *avec état* aux ordinateurs côté LAN.
  - **Configurer sur annonce du routeur et DHCPv6 automatiquement** : fournit des adresses IPv6 sans état et avec état aux ordinateurs côté LAN.

Paramètres du port USB1 ou USB2

La configuration du port USB permet de gérer la connexion entre ce périphérique et le dongle USB. Elle permet également de gérer le basculement du port WAN (redondance). Certains dongles USB configurent automatiquement leurs informations. D'autres, tels que le dongle Verizon UML290VW 4G, nécessitent une configuration manuelle. Reportez-vous à la documentation du fabricant du dongle pour obtenir plus d'informations.

Connexion 3G/4G

Pour établir une connexion 3G ou 4G, saisissez les éléments suivants :

- **Code PIN** et **Confirmer le code PIN** : code PIN associé à la carte SIM. Ce champ s'affiche uniquement pour les cartes SIM GSM.
- **Nom du point d'accès** : réseau Internet avec lequel l'appareil mobile a établi une connexion. Entrez le nom du point d'accès spécifié par votre prestataire de services de réseau mobile. Si vous ne connaissez pas le nom du point d'accès, contactez votre prestataire de services.
- **Composer un numéro** : numéro fourni par votre prestataire de services de réseau mobile pour accéder à Internet.
- **Nom d'utilisateur** et **Mot de passe** : nom d'utilisateur et mot de passe spécifiés par votre prestataire de services de réseau mobile.
- **Activer DNS** : cochez cette case pour activer le DNS.
- **Serveur DNS (obligatoire)** et **Serveur DNS (facultatif)** : adresses IP des serveurs DNS. Vous pouvez éventuellement saisir un second serveur DNS. Le premier serveur DNS disponible est utilisé.
- **MTU** : taille maximale des unités de transmission (**MTU**). Sélectionnez **Automatique** pour définir automatiquement la taille. Sinon, afin de définir manuellement la taille des **MTU**, sélectionnez **Manuel** et saisissez la taille des MTU. (Taille en octets de l'unité de données du protocole la plus importante que la couche peut traiter).

Configuration du basculement et de la récupération

Si une connexion Ethernet et une liaison du réseau mobile sont disponibles, une seule connexion peut être utilisée à la fois pour établir une liaison WAN. Chaque fois qu'une connexion WAN échoue, le périphérique essaie d'établir une autre connexion sur une autre interface. Cette fonctionnalité est connue sous le nom de *basculement.* Lorsque la connexion WAN principale est restaurée, ce chemin est rétabli et la connexion de secours est abandonnée. Cette fonctionnalité est connue sous le nom de *récupération.*

ÉTAPE 1 Pour afficher la fenêtre Basculement et récupération, cliquez sur **Configuration** > **Réseau**.

ÉTAPE 2 Sélectionnez un port USB et cliquez sur **Modifier**. La fenêtre Réseau apparaît.

ÉTAPE 3 Cliquez sur l'onglet **Paramètres de basculement USB** et saisissez les éléments suivants :

- **Mode de fonctionnement** : en cas de défaillance du lien WAN Ethernet, le périphérique tente d'afficher le liaison du réseau mobile sur l'interface USB. Configurez le comportement de basculement :
  - Réserve à chaud du basculement 3G/4G : une connexion de port WAN Ethernet perdue entraîne la redirection du trafic WAN vers le lien USB 3G/4G. Le dongle USB est mis sous tension alors qu'il se trouve en mode de réserve.
  - Reprise progressive du basculement 3G/4G : une connexion de port WAN Ethernet perdue entraîne la redirection du trafic WAN vers le lien USB 3G/4G. Le dongle USB est mis hors tension alors qu'il se trouve en mode de réserve.
  - Mode principal : le lien 3G/4G est utilisé comme connexion WAN principale.
- **Qualité du signal** : indique la puissance du signal entre le dongle USB 3G/4G et le point d'accès. Cliquez sur **Actualiser** pour mettre à jour l'affichage.

ÉTAPE 4 Pour éviter les excédents de données, sélectionnez un **compteur de facturation**. **Trafic (Ko)** permet de suivre le volume de données en kilo-octets reçues ou envoyées via le lien USB. **Heure (min)** permet de compter le nombre de minutes durant lesquelles la connexion 3G/4G est active.

- Si vous choisissez Trafic (Ko), saisissez les éléments suivants :
  - **Prime** : coût en dollars pour un volume spécifié de données.
  - **Frais supplémentaires** : coût en dollars par kilo-octet de données si un volume spécifié est dépassé.
  - **Arrêter la connexion...** : cochez cette case pour activer le rejet de la connexion lorsque le volume dépasse le volume donné.

- Si vous choisissez Heure (min), saisissez les éléments suivants :
  - **Prime** : coût en dollars pour une période donnée.
  - **Frais supplémentaires** : coût en dollars si une période donnée est dépassée.
  - **Arrêter la connexion...** : cochez cette case pour activer le rejet de la connexion lorsque la durée dépasse la durée donnée.

La fenêtre apparaît :

- **Temps cumulé précédent** : durée pendant laquelle la connexion 3G/4G est restée active jusqu'à sa réinitialisation.
- **Temps cumulé actuel** : durée écoulée depuis le moment où le périphérique a établi une connexion 3G/4G.
- **Coût** : coût estimé de la connexion depuis la réinitialisation des compteurs.

ÉTAPE 5 Définissez les comportements **Diagnostic** :

- **Redémarrer le compteur** : cochez cette case et saisissez le jour du mois auquel la réinitialisation des compteurs est activée. Si la valeur est supérieure au nombre de jours dans le mois (par exemple, une valeur de 31 dans un mois ne comptant que 30 jours), les compteurs sont redémarrés le dernier jour du mois.
- **Auto-test tous les jours à** : cochez cette case et saisissez l'heure (format 24 heures) à laquelle tester la connexion. Un auto-test est considéré comme réussi si le périphérique peut obtenir une adresse IP du fournisseur de service. Les échecs sont envoyés vers le fichier journal.
- **Consigner l'auto-test** : cochez cette case pour consigner toute l'activité d'auto-test. (Tous les résultats du test sont envoyés vers le fichier journal).

ÉTAPE 6 Cliquez sur **Enregistrer** pour enregistrer vos paramètres.

Activation de la DMZ

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

Pour configurer la DMZ :

ÉTAPE 1 Sélectionnez **Configuration** > **Réseau** et cochez la case **Activer la DMZ**. Un message apparaît.

ÉTAPE 2 Cliquez sur **Oui** pour accepter la modification.

ÉTAPE 3 Sélectionnez l'interface DMZ dans la table **Paramètres DMZ** et cliquez sur **Modifier**. La fenêtre **Modifier la connexion de DMZ** apparaît.

ÉTAPE 4 Sélectionnez **Subnet (Sous-réseau)** afin d'identifier un sous-réseau pour les services DMZ, puis saisissez l'**adresse IP de la DMZ** et le **masque de sous-réseau**. Ou sélectionnez **Plage** pour réserver un groupe d'adresses IP sur le même sous-réseau pour les services DMZ et saisissez la plage d'adresses IP.

ÉTAPE 5 Cliquez sur **Enregistrer**.

Mot de passe

Le nom d'utilisateur et le mot de passe permettent l'accès des administrateurs au périphérique. Le nom d'utilisateur par défaut est **cisco**. Le mot de passe par défaut est **cisco**. Le nom d'utilisateur et le mot de passe peuvent être modifiés. Nous vous conseillons vivement de remplacer le mot de passe par un mot de passe sécurisé.

Si la gestion à distance est activée sur la page **Général** (Pare-feu), le mot de passe *doit* être modifié.

AVERTISSEMENT Il n'est pas possible de récupérer ce mot de passe si vous l'oubliez ou le perdez. Si vous avez perdu ou oublié votre mot de passe, le périphérique doit être réinitialisé sur les paramètres d'origine, supprimant toutes les modifications apportées à la configuration. Si vous accédez au périphérique à distance et réinitialisez ses paramètres d'origine, vous ne pourrez pas vous connecter au périphérique jusqu'à ce que vous ayez établi une liaison locale câblée sur le même sous-réseau.

Lorsque vous modifiez le nom d'utilisateur ou le mot de passe, vous êtes déconnecté. Connectez-vous au périphérique en utilisant vos nouvelles informations d'identification.

Pour changer le nom d'utilisateur ou le mot de passe :

ÉTAPE 1 Choose **Configuration**>**Mot de passe**.

ÉTAPE 2 Dans le champ **Nom d'utilisateur** , saisissez le nouveau nom d'utilisateur. Pour conserver le nom d'utilisateur actuel, ne renseignez pas ce champ.

ÉTAPE 3 Dans le champ **Ancien mot de passe**, saisissez le mot de passe actuel. Cela est nécessaire si vous modifiez le nom d'utilisateur en conservant le mot de passe actuel.

REMARQUE Si vous modifiez le nom d'utilisateur en conservant le mot de passe actuel, laissez les champs **Nouveau mot de passe** et **Confirmer le nouveau mot de passe** vides.

ÉTAPE 4 Dans le champ **Nouveau mot de passe** , saisissez le nouveau mot de passe pour le périphérique. Utilisez une combinaison de symboles et de caractères alphanumériques. Le mot de passe ne doit contenir aucun espace. Saisissez le nouveau mot de passe à nouveau dans le champ **Confirmer le nouveau mot de passe**. Assurez-vous que les deux mots de passe sont identiques.

ÉTAPE 5 Dans le champ **Délai d'expiration de la session**, saisissez le nombre de minutes au bout duquel la session expire. Enregistrez vos modifications.

Pour configurer les paramètres de complexité du mot de passe :

ÉTAPE 1 Dans le champ **Paramètres de complexité du mot de passe**, cochez la case **Activer**.

ÉTAPE 2 Configurez les paramètres dans les champs suivants :

Longueur minimale du mot de passe	Saisissez la longueur minimale du mot de passe (entre 0 et 64 caractères). La longueur minimale par défaut est 8.

Nombre minimal de classes de caractères	Saisissez le nombre de classes que le mot de passe doit inclure. Par défaut, le mot de passe doit contenir des caractères d'au moins trois de ces classes : ▪ Lettres majuscules. ▪ Lettres minuscules. ▪ Chiffres. ▪ Caractères spéciaux disponibles sur un clavier standard.
Le nouveau mot de passe doit être différent de l'actuel	Cochez la case **Activer** si le nouveau mot de passe doit être différent du mot de passe actuel.
Expiration du mot de passe	Cochez la case **Activer** si le mot de passe doit expirer après un délai donné.
Délai d'expiration du mot de passe	Saisissez le nombre de jours au bout duquel le mot de passe expire (1–365). Le délai d'expiration par défaut est de 180 jours

Lorsque l'option **Complexité de mot de passe minimale** - **Activer** est cochée, la **Mesure de la fiabilité du mot de passe** indique le niveau de fiabilité du mot de passe, en fonction des règles de complexité définies. L'échelle va du rouge (inacceptable) au vert (élevé), en passant par le jaune (acceptable).

ÉTAPE 3 Cliquez sur **Enregistrer**.

Heure

L'heure est indispensable pour un périphérique réseau. Cela permet qu'il s'affiche correctement dans le journal système et les messages d'erreur, et qu'il synchronise le transfert des données avec les autres périphériques du réseau.

Vous pouvez configurer le fuseau horaire, indiquer s'il faut ou non prendre en compte l'heure d'été et définir le serveur NTP (Network Time Protocol) avec lequel synchroniser la date et l'heure. Le routeur obtient alors ses informations de date et d'heure du serveur NTP.

Pour configurer le serveur NTP et les paramètres de l'heure, sélectionnez **Configuration** > **Heure**.

- **Fuseau horaire** : fuseau horaire par rapport à l'heure de Greenwich (GMT).
- **Heure d'été** : activez ou désactivez ce réglage pour l'heure d'été. Saisissez l'heure de début dans le champ **De** et l'heure de fin dans le champ **À**.
- **Définir la date et l'heure** : **Automatique** permet d'activer le serveur NTP. Si vous choisissez Automatique, saisissez le nom complet du **serveur NTP** ou l'adresse IP. **Manuel** permet de régler la date et l'heure localement, et utilise l'horloge du périphérique pour conserver l'heure. Si vous choisissez **Manuel**, saisissez la **date et l'heure**.

Hôte DMZ

L'hôte DMZ permet à un hôte du réseau local d'être exposé sur Internet pour utiliser des services de vidéoconférence ou de jeu. L'accès à l'hôte DMZ depuis Internet peut être restreint davantage via l'utilisation de règles d'accès à travers un pare-feu.

Pour configurer un hôte DMZ, saisissez une **adresse IP privée de DMZ** et cliquez sur **Enregistrer**.

Redirection (port)

La redirection de port permet un accès public aux services des périphériques réseau du LAN en ouvrant un port spécifique ou une plage de ports, comme FTP. Le déclenchement de port ouvre une plage de ports pour des services, tels que les jeux sur Internet, qui utilisent d'autres ports pour communiquer entre le serveur et l'hôte LAN.

Configuration de la redirection de ports

Lorsque les utilisateurs demandent des services sur votre réseau, le périphérique redirige ces demandes vers votre serveur en fonction des paramètres de redirection de port. L'accès aux services non spécifiés est refusé. Par exemple, lorsque le port numéro 80 (HTTP) est redirigé vers l'adresse IP 192.168.1.2, toutes les demandes HTTP présentent sur l'interface sont redirigées vers 192.168.1.2. Le reste du trafic est refusé, sauf s'il est spécifiquement autorisé par une autre entrée.

Utilisez cette fonction pour établir un serveur Web ou un serveur FTP. Veillez à saisir une adresse IP valide. (Pour exécuter un serveur Internet, il peut s'avérer nécessaire d'utiliser une adresse IP statique). Pour plus de sécurité, les utilisateurs extérieurs peuvent communiquer avec le serveur mais ils ne sont autorisés à se connecter aux périphériques réseau.

Pour ajouter ou modifier un service de la table :

ÉTAPE 1 Pour ajouter un service, cliquez sur **Ajouter** dans la table de redirection de plages de ports.

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

Les champs sont ouverts pour la modification.

ÉTAPE 2 Configurez les options suivantes :

- Sélectionnez un **service** dans le menu déroulant. (Si le service n'y figure pas, vous pouvez modifier la liste en suivant les instructions de la section **Ajout ou modification d'un nom de service**).
- Saisissez l'**adresse IP** du serveur.
- Sélectionnez l'**interface** voulue.
- Sélectionnez **État**. Cochez la case pour activer le service. Décochez la case pour désactiver le service.

ÉTAPE 3 Cliquez sur **Enregistrer**.

Ajout ou modification d'un nom de service

Pour ajouter ou modifier une entrée de la liste Service :

ÉTAPE 1 Cliquez sur **Gestion des services**. Si le navigateur Web affiche une mise en garde relative à la fenêtre contextuelle, autorisez le contenu bloqué.

ÉTAPE 2 Pour ajouter un service, cliquez sur **Ajouter** dans la table Gestion des services.

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

Les champs sont ouverts pour la modification. Si le navigateur Web affiche une mise en garde relative à la fenêtre contextuelle, autorisez le contenu bloqué.

ÉTAPE 3 La liste peut comporter jusqu'à 30 services :

- **Nom de service** : courte description.
- **Protocole :** protocole requis. Reportez-vous à la documentation du service que vous hébergez.

- **Plage de ports** : plage des numéros de ports réservés à ce service.

ÉTAPE 4 Cliquez sur **Enregistrer**.

Configuration du déclenchement de ports

Le déclenchement de ports permet au périphérique de contrôler les données sortantes à la recherche des numéros de port spécifiés. L'adresse IP du client qui envoie les données correspondantes est enregistrée par le périphérique. Lorsque les données requises sont renvoyées par le périphérique, les données sont transmises au client adéquat à l'aide de l'adressage IP et des règles de mappage de ports.

Certains jeux ou applications Internet utilisent des ports atypiques pour communiquer entre le serveur et l'hôte LAN. Pour utiliser ces applications, saisissez le port de déclenchement (sortant) et l'autre port entrant dans la table de déclenchement de ports.

Pour ajouter ou modifier un nom d'application de la table :

ÉTAPE 1 Cliquez sur **Configuration** > **Redirection**.

ÉTAPE 2 Pour ajouter un nom d'application, cliquez sur **Ajouter** dans la table de redirection de plages de ports.

Pour modifier un nom d'application, sélectionnez la ligne et cliquez sur **Modifier**. Les champs sont ouverts pour la modification.

Si le navigateur Web affiche une mise en garde relative à la fenêtre contextuelle, autorisez le contenu bloqué.

ÉTAPE 3 Configurez les options suivantes :

- **Nom de l'application** : nom de l'application.
- **Plage de ports de déclenchement** : numéros de port de début et de fin de la plage de ports de déclenchement. Reportez-vous à la documentation de l'application pour obtenir des informations supplémentaires.
- **Plage de ports entrants** : numéros de port de début et de fin de la plage de ports entrants. Reportez-vous à la documentation de l'application pour obtenir des informations supplémentaires.

ÉTAPE 4 Cliquez sur **Enregistrer**.

Suppression d'une entrée de table

Pour supprimer une entrée de table, cliquez sur l'entrée que vous souhaitez supprimer, puis sur **Supprimer**.

Traduction d'adresses de ports

La technologie PAT (Port Address Translation) est une extension de la technologie NAT (Network Address Translation) qui autorise le mappage de plusieurs périphériques d'un réseau LAN sur une seule adresse IP publique pour conserver les adresses IP.

Le mécanisme PAT est identique à la redirection de port, sauf qu'un paquet entrant avec un port de destination (port externe) est traduit vers un port de destination de paquet différent (port interne). Le fournisseur d'accès à Internet attribue une adresse IP unique au périphérique de bordure de réseau. Lorsque l'ordinateur se connecte à Internet, ce périphérique attribue au client un numéro de port qui est ajouté à l'adresse IP interne, attribuant à l'ordinateur une adresse IP unique.

Si un autre ordinateur se connecte à Internet, ce périphérique lui attribue la même adresse IP publique mais un numéro de port différent. Bien que les deux ordinateurs partagent la même adresse IP publique, ce périphérique sait à quel ordinateur envoyer ses paquets car le périphérique utilise les numéros de port pour attribuer aux paquets l'adresse IP interne unique des ordinateurs.

Pour ajouter ou modifier un PAT :

ÉTAPE 1 Pour ajouter un service, cliquez sur **Ajouter** dans la table de traduction d'adresses de ports.

Pour modifier un service, sélectionnez la ligne et cliquez sur **Modifier**. Les champs sont ouverts pour la modification.

Si le navigateur Web affiche une mise en garde relative à la fenêtre contextuelle, autorisez le contenu bloqué.

ÉTAPE 2 Sélectionnez le **service** dans le menu déroulant. Vous pouvez avoir jusqu'à 30 services différents. (Si le service n'y figure pas, vous pouvez modifier la liste en suivant les instructions de la section **Ajout ou modification d'un nom de service**).

ÉTAPE 3 Saisissez l'adresse IP ou le nom du périphérique réseau sur lequel se trouve le service.

ÉTAPE 4 Cliquez sur **Enregistrer**.

Ajout ou modification d'un nom de service

Pour ajouter ou modifier une entrée de la liste Service :

ÉTAPE 1 Cliquez sur **Gestion des services**. Si le navigateur Web affiche une mise en garde relative à la fenêtre contextuelle, autorisez le contenu bloqué.

ÉTAPE 2 Pour ajouter un service, cliquez sur **Ajouter** dans la table Gestion des services.

Pour modifier un service, sélectionnez la ligne et cliquez sur **Modifier**. Les champs sont ouverts pour la modification.

Si le navigateur Web affiche une mise en garde relative à la fenêtre contextuelle, autorisez le contenu bloqué.

ÉTAPE 3 La liste peut comporter jusqu'à 30 services :

- **Nom de service** : courte description.
- **Protocole :** protocole requis. Reportez-vous à la documentation du service que vous hébergez.
- **Port externe** : numéro de port externe.
- **Port interne** : numéro de port interne.

ÉTAPE 4 Cliquez sur **Enregistrer**.

Configuration de la fonctionnalité NAT un à un

La fonctionnalité NAT un à un crée une relation qui permet de mettre en correspondance une adresse IP de réseau WAN valide avec des adresses IP LAN masquées sur le WAN (Internet) par le mécanisme NAT. Cela permet de protéger les périphériques LAN contre la détection et les attaques.

Pour obtenir des résultats optimaux, réservez les adresses IP des ressources internes auxquelles vous souhaitez accéder via la fonctionnalité NAT un à un.

Vous pouvez procéder à la mise en correspondance d'une seule adresse IP LAN ou d'une plage d'adresses IP avec une plage d'adresses IP de réseau WAN externes (trois adresses internes et trois adresses externes, par exemple). La première adresse interne est associée à la première adresse externe, la deuxième adresse IP interne à la seconde adresse externe et ainsi de suite.

Pour activer cette fonctionnalité, cochez la case **Activer**.

Pour ajouter une entrée à la liste, cliquez sur **Ajouter** et saisissez les informations suivantes :

- **Début de la plage privée** : adresse IP de départ de la plage d'adresses IP internes que vous souhaitez mettre en correspondance avec la plage publique. N'incluez pas l'adresse IP de gestion du routeur dans cette plage.
- **Début de la plage publique** : adresse IP de départ de la plage d'adresses IP publiques spécifiée par le fournisseur d'accès à Internet. N'incluez pas l'adresse IP du réseau WAN du routeur dans cette plage.
- **Longueur de la plage** : nombre d'adresses IP de la plage. La longueur de la plage ne doit pas dépasser le nombre d'adresses IP valides. Pour associer une seule adresse, saisissez 1.

Pour modifier une entrée, sélectionnez l'entrée que vous souhaitez modifier et cliquez sur **Modifier**. Les informations apparaissent dans les zones de texte. Apportez les modifications voulues, puis cliquez sur **Enregistrer**.

Clonage de l'adresse MAC

Certains FAI requièrent l'enregistrement d'une adresse MAC (code d'identification unique à 12 chiffres attribué à chaque périphérique réseau). Si vous avez déjà enregistré un adresse MAC pour le périphérique auprès de votre FAI, sélectionnez cette fonctionnalité pour cloner cette adresse sur votre périphérique. Sinon, contactez votre FAI pour modifier l'adresse MAC enregistrée.

REMARQUE Lorsque la fonctionnalité Clone d'adresse MAC est activée, la mise en miroir des ports ne fonctionne pas.

Pour cloner une adresse MAC, procédez comme suit :

ÉTAPE 1 Sélectionnez la case d'option **Interface**.

ÉTAPE 2 Cliquez sur **Modifier** pour afficher la page Modifier le clone d'adresse MAC.

- **Adresse MAC WAN définie par l'utilisateur** : sélectionnez cette case d'option et saisissez l'adresse MAC à 12 chiffres enregistrée auprès de votre FAI.
- **Adresse MAC de cet ordinateur** : cliquez pour utiliser l'adresse MAC de votre ordinateur comme adresse MAC clone pour le périphérique.

ÉTAPE 3 Cliquez sur **Enregistrer**.

Attribution d'un DNS dynamique à l'interface WAN

Le service DDNS (Dynamic Domain Name System) attribue un nom de domaine fixe à une adresse IP dynamique de réseau WAN. Vous pouvez ainsi héberger votre propre serveur Web, FTP ou tout autre type de serveur TCP/IP dans votre réseau local. Sélectionnez cette fonctionnalité pour configurer les interfaces WAN à l'aide de vos informations DDNS.

Avant de configurer le service DNS dynamique sur le routeur, visitez le site www.dyndns.org et enregistrez un nom de domaine. Ce service est fourni par DynDNS.org. Pour les utilisateurs résidant en Chine, visitez le site www.3322.org pour procéder à l'enregistrement.

La page Modifier la configuration du DNS dynamique apparaît après avoir sélectionné une interface et cliqué sur **Modifier**.

Pour modifier le service DDNS, procédez comme suit :

ÉTAPE 1 Dans la liste **Service DDNS**, sélectionnez un service.

ÉTAPE 2 Saisissez les informations de votre compte :

- **Nom d'utilisateur** : nom d'utilisateur du compte DDNS. Si vous n'avez pas encore enregistré de nom d'hôte, cliquez sur **S'inscrire** pour accéder au site Web DynDNS.com et vous inscrire gratuitement au service DNS dynamique.
- **Mot de passe** : mot de passe de votre compte DDNS.
- **Nom d'hôte** : nom d'hôte enregistré auprès de votre fournisseur DDNS. Par exemple, si votre nom d'hôte est *mamaison.dyndns.org*, saisissez *mamaison* dans le premier champ, *dyndns* dans le second et *org* dans le dernier.

Les informations en lecture seule suivantes s'affichent :

- **Adresse IP Internet** : adresse IP de réseau WAN de l'interface.
- **État** : état du service DDNS. Si les informations sur l'état indiquent une erreur, vérifiez que vous avez correctement saisi les informations relatives à votre compte, pendant la configuration du service DDNS.

ÉTAPE 3 Cliquez sur **Enregistrer**.

Routage avancé

Cette fonctionnalité permet d'effectuer un routage dynamique et d'ajouter des itinéraires statiques à la table de routage pour IPv4 et IPv6.

Pour consulter la table de routage, cliquez sur **Consulter la table de routage**. Cliquez sur **Actualiser** pour mettre à jour les données. Cliquez sur **Fermer** pour fermer la fenêtre contextuelle.

Configuration du routage dynamique

Le routage dynamique permet d'établir automatiquement les tables de routage, en fonction des informations supportées par les protocoles de routage, et d'autoriser le réseau à agir manière presque autonome en évitant les défaillances et blocages du réseau.

Pour configurer le routage dynamique IPv4 à l'aide du protocole RIP (Routing Information Protocol), cliquez sur l'onglet **IPv4**.

Pour configurer le routage dynamique IPv6 à l'aide du protocole RIPng (Routing Information Protocol) nouvelle génération, cliquez sur l'onglet **IPv6**.

Configuration du routage dynamique IPv4

ÉTAPE 1 Sélectionnez le Mode de fonctionnement :

- **Passerelle** : sélectionnez ce mode si le périphérique héberge la connexion réseau à Internet. Il s'agit du paramètre par défaut.
- **Routeur** : sélectionnez ce mode si le périphérique se trouve sur un réseau comportant d'autres routeurs et si un autre périphérique joue le rôle de la passerelle réseau à Internet ou si le réseau n'est pas connecté à Internet. En mode Routeur, la connectivité à Internet n'est disponible pour les périphériques réseau que si vous disposez d'un autre routeur jouant le rôle de passerelle. Étant donné que la protection par pare-feu est assurée par la passerelle, désactivez le pare-feu de ce périphérique.

ÉTAPE 2 Activez le protocole **RIP** pour permettre au périphérique d'échanger automatiquement ses informations de routage avec d'autres routeurs et d'adapter ses tables de routage de manière dynamique, en fonction des changements survenant sur le réseau. Le paramètre par défaut est Désactivé. Si vous activez cette fonctionnalité, configurez également les paramètres suivants :

- **Recevoir des version RIP** : sélectionnez le protocole RIP permettant de recevoir les données réseau : **None**, **RIPv1**, **RIPv2** ou **Both RIP v1 and v2**.

  RIPv1 est une version de routage à base de classes. Il n'inclut pas d'informations de sous-réseau et ne prend pas en charge, par conséquent, les masques de sous-réseau à longueur variable (VLSM). RIPv1 ne propose pas non plus de prise en charge pour l'authentification du routeur, ce qui le rend vulnérable aux attaques. **RIPv2** dispose d'un masque de sous-réseau et prend en charge la sécurité avec authentification par mot de passe.

- **Transmettre des versions RIP** : sélectionnez le protocole RIP permettant de transmettre les données réseau : **None**, **RIPv1**, **RIPv2 - Broadcast**, or **RIPv2 - Multicast**.

  RIPv2 - Broadcast (recommandé) diffuse les données dans l'ensemble du sous-réseau. **RIPv2 - Multicast** envoie les données vers des adresses de multidiffusion. RIPv2 - Multicast permet également d'éviter toute charge inutile en diffusant des tables de routage à des routeurs adjacents au lieu de les transmettre à l'ensemble du réseau.

ÉTAPE 3 Cliquez sur **Enregistrer**.

Configuration du routage dynamique IPv6

L'onglet IPv6 n'est disponible que si vous avez activé l'option Double pile IP dans la page Configuration > Réseau.

Pour activer le protocole RIPng, cochez la case **RIPng**.

Configuration du routage statique

Le routage statique peut être configuré pour IPv4 ou IPv6. Ces itinéraires n'ont pas une durée de vie limitée dans la table de routage. Vous pouvez spécifier jusqu'à 30 itinéraires.

Pour configurer un itinéraire statique, cliquez sur **Ajouter** ou sélectionnez une entrée, puis sur **Modifier** :

- **IP de destination** : adresse de sous-réseau du segment LAN distant. Pour un domaine IP de classe C, l'adresse de réseau correspond aux trois premiers champs de l'adresse IP du LAN de destination ; le dernier champ doit être un zéro.
- **Masque de sous-réseau (IPv4 uniquement)** : masque de sous-réseau utilisé dans le domaine IP LAN de destination. Pour les domaines IP de classe C, le masque de sous-réseau est généralement 255.255.255.0.
- **Longueur du préfixe (IPv6 uniquement)** : longueur du préfixe IPv6.
- **Passerelle par défaut** : adresse IP du routeur de dernier recours.
- **Nombre de sauts** : nombre maximal de nœuds ou de sauts (le maximum étant de 15 sauts) qu'un paquet traverse avant d'être rejeté. Un nœud désigne un périphérique du réseau tel qu'un commutateur ou un routeur.
- **Interface** : interface à utiliser pour cet itinéraire.

Pour supprimer une entrée de la liste, cliquez sur l'entrée que vous souhaitez supprimer, puis sur **Supprimer**.

Pour consulter les données actuelles, cliquez sur **Consulter la table de routage**. La liste d'entrées de la table de routage apparaît. Vous pouvez cliquer sur **Actualiser** pour mettre à jour les données ou sur **Fermer** pour fermer la fenêtre-contextuelle.

Équilibrage de la charge entrante

L'équilibrage de la charge entrante permet de distribuer le trafic entrant de manière égale sur chaque port WAN afin d'optimiser l'utilisation de la bande passante. Il permet également d'empêcher la distribution inégale et la surcharge.

Pour activer et configurer l'équilibrage de la charge entrante, procédez comme suit :

ÉTAPE 1 Cliquez sur **Activer l'équilibrage de la charge entrante**.

ÉTAPE 2 Saisissez les informations concernant le **nom de domaine** :

- **Nom de domaine** : nom de domaine attribué par le fournisseur de service DNS.
- **TTL** (Time-to-Live) : intervalle de temps pour les requêtes DNS (0 à 65 535 secondes). Un long intervalle affecte l'intervalle d'actualisation. Un intervalle plus court augmente la charge du système, mais améliore la précision de l'équilibrage de la charge entrante. Vous pouvez régler ce paramètre pour optimiser les performances de votre réseau.
- **Admin** : adresse e-mail de l'administrateur.

ÉTAPE 3 Saisissez les paramètres du **serveur DNS** :

- **Serveur de noms** : serveur DNS qui traduit le nom de domaine.
- **Interface** : interface WAN correspondant au serveur de noms. Le système afficher les adresses IP de réseau WAN acquises et activées.

ÉTAPE 4 Saisissez le nom d'hôte qui fournit des services, tel que le serveur Web ou FTP dans le champ **Nom** (enregistrement) **d'hôte** et sélectionnez l'interface **Adresse IP de réseau WAN** vers laquelle le trafic entrant est distribué.

ÉTAPE 5 Saisissez l'**alias** qui permet d'attribuer différents noms à un hôte d'ordinateur susceptible de fournir différents services et la **cible**, un nom de domaine Enregistrement A existant.

ÉTAPE 6 Cliquez sur **Paramètres SPF** pour ajouter du texte SPF. SPF (Sender Policy Framework) est un système de validation des e-mails qui bloque les spams grâce à la détection des tentatives d'usurpation (vulnérabilité fréquente) en vérifiant les adresses IP de l'expéditeur. (La configuration de ce champ n'est pas obligatoire. Plus d'informations disponibles à l'adresse http://www.openspf.org/Tools#wizard?mydomain=&x=35&y=6).

ÉTAPE 7 Saisissez les paramètres du **serveur de messagerie** :

- **Nom d'hôte** : nom (sans le nom de domaine) de l'hôte de messagerie.
- **Poids** : ordre des hôtes de messagerie. Plus le nombre est faible, plus la priorité est haute.
- **Serveur de messagerie** : nom du serveur enregistré dans Enregistrement A ou nom d'un serveur de messagerie externe.

ÉTAPE 8 Cliquez sur **Enregistrer**.

Mise à jour du périphérique USB

Le micrologiciel du périphérique USB peut être mis à jour à l'aide de ce périphérique réseau.

Pour mettre à niveau un périphérique USB connecté à un port USB, recherchez le fichier à télécharger depuis l'ordinateur sur le périphérique USB et cliquez sur **Mise à niveau**.

4

DHCP

Le protocole DHCP (Dynamic Host Configuration Protocol) est un protocole réseau permettant de configurer les périphériques réseau pour communiquer sur un réseau IP. Un client DHCP utilise le protocole DHCP pour obtenir des informations de configuration, comme une adresse IP, un acheminement par défaut ou une ou plusieurs adresses de serveur DNS depuis un serveur DHCP. Le client DHCP utilise ensuite ces informations pour configurer l'hôte. Une fois le processus de configuration terminé, l'hôte peut communiquer sur Internet.

Le serveur DHCP conserve une base de données des adresses IP disponibles ainsi que les informations de configuration. Lorsque vous recevez une requête d'un client, le serveur DHCP détermine le réseau auquel le client DHCP est connecté et attribue une adresse IP ou un préfixe approprié au client, puis envoie les informations de configuration nécessaires concernant ce dernier.

Le serveur DHCP et le client DHCP doivent être connectés à la même liaison de réseau. Dans les réseaux plus importants, chaque liaison contient un ou plusieurs agents de relais DHCP. Ces agents reçoivent des messages des clients DHCP et les transmettent aux serveurs DHCP. Les serveurs DHCP renvoient une réponse à l'agent de relais, qui à son tour les transfère au client DHCP sur la liaison de réseau local.

Généralement, les serveurs DHCP allouent des adresses IP aux clients pour une durée limitée appelé *bail*. Les clients DHCP sont responsables du renouvellement de leur adresse IP avant qu'elle n'expire et ne doivent plus l'utiliser s'ils n'ont pas pu la renouveler avant l'expiration du délai.

Le protocole DHCP est utilisé pour IPv4 et IPv6. Bien que les deux versions soient destinées au même usage, les détails du protocole pour IPv4 et IPv6 sont suffisamment différents pour qu'ils soient considérés comme deux protocoles distincts.

Configuration DHCP

La configuration DHCP définit le protocole DHCP pour IPv4 ou IPv6. Elle permet également à certains périphériques de télécharger leur configuration depuis un serveur TFTP. Lorsqu'un périphérique démarre, et si l'adresse IP et l'adresse IP du serveur TFTP n'ont pas été préconfigurées, il envoie une requête avec les options 66, 67 et 150 au serveur DHCP pour obtenir ces informations.

L'option 150 DHCP appartient à Cisco. La norme IEEE similaire à cette exigence est l'option 66. Comme l'option 150, l'option 66 est utilisée pour spécifier le nom du serveur TFTP. L'option 67 fournit le nom du fichier de démarrage.

L'option 82 (option des informations sur l'agent de relais DHCP) 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 DHCP IPv4, cliquez sur l'onglet **IPv4**. Pour configurer DHCP IPv6, cliquez sur l'onglet **IPv6**.

Configuration du protocole DHCP pour IPv4

Pour configurer le protocole DHCP pour IPv4 :

ÉTAPE 1 Choisissez **VLAN** ou **Option 82**.

ÉTAPE 2 Si vous choisissez **Option 82**, ajoutez des identifiants de circuit en passant par DHCP > **Option 82**. Ces identifiants sont ensuite répertoriés dans le menu déroulant **ID de circuit**.

Si vous choisissez **VLAN**, sélectionnez le réseau VLAN dans le menu **ID de réseau VLAN** et saisissez les informations suivantes :

- **Adresse IP du périphérique** : adresse IP de gestion.
- **Masque de sous-réseau** : masque de sous-réseau IP de gestion.

ÉTAPE 3 Sélectionnez le **Mode DHCP** :

- **Désactiver** : désactive le protocole DHCP sur le périphérique. Aucun autre paramètre ne doit être défini.
- **Serveur DHCP** : transmet les requêtes DHCP client au serveur DHCP du périphérique.

- **Relais DHCP** : transmet les requêtes DHCP et les réponses provenant d'un autre serveur DHCP via le périphérique. Si le relais DHCP a été choisi, saisissez l'adresse IP du **Serveur DHCP distant**.
- **Durée de bail du client** : durée en minutes pendant laquelle l'utilisateur d'un réseau est autorisé à se connecter au routeur à l'aide de l'adresse IP actuelle. Les valeurs acceptables sont comprises entre 5 et 43200 minutes. La valeur par défaut est 1440 minutes (soit 24 heures).
- **Début de la plage** et **Fin de la plage** : adresses IP de début et de fin qui créent une plage d'adresses IP pouvant être attribuées de manière dynamique. La plage peut aller jusqu'au nombre maximal d'adresses IP que le serveur peut attribuer sans chevauchement des fonctions, comme PPTP et VPN SSL. N'incluez pas l'adresse IP de réseau LAN du périphérique dans cette plage IP dynamique. 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 plus.
- **Serveur DNS** : type de service DNS ; emplacement où l'adresse IP du serveur DNS est obtenue.
- **DNS statique 1** et **DNS statique 2** : adresse IP statique d'un serveur DNS. (Facultatif) Si vous saisissez un deuxième serveur DNS, le périphérique utilise le premier serveur DNS pour répondre à une requête.
- **WINS** : adresse IP facultative d'un serveur WINS (Windows Internet Naming Service) qui résout les noms NetBIOS en adresses IP. Si vous ne connaissez pas l'adresse IP du serveur WINS, utilisez la valeur par défaut 0.0.0.0.

ÉTAPE 4 Saisissez les paramètres du serveur TFTP :

- **Nom d'hôte de serveur TFTP** : nom d'hôte du serveur TFTP.
- **IP du serveur TFTP** : adresse IP du serveur TFTP.
- **Nom du fichier de configuration** : nom de configuration du fichier utilisé pour actualiser un périphérique.

Configuration du protocole DHCP pour IPv6

Pour configurer le protocole DHCP pour IPv6 :

ÉTAPE 1 Saisissez l'**adresse IPv6**.

ÉTAPE 2 Saisissez la **longueur du préfixe**.

ÉTAPE 3 Sélectionnez le **Mode DHCP** :

- **Désactiver** : désactive le protocole DHCP sur le périphérique. Aucun autre paramètre ne doit être défini.
- **Serveur DHCP** : transmet les requêtes DHCP client au serveur DHCP du périphérique.

- **Relais DHCP** : transmet les requêtes DHCP et les réponses provenant d'un autre serveur DHCP via le périphérique.
- **Durée de bail du client** : durée pendant laquelle l'utilisateur d'un réseau est autorisé à se connecter au routeur à l'aide de l'adresse IP actuelle. Saisissez la durée, en minutes. Les valeurs acceptables sont comprises entre 5 et 43200 minutes. La valeur par défaut est 1440 minutes (soit 24 heures).
- **Serveur DNS 1** et **Serveur DNS 2** : (Facultatif) adresse IP d'un serveur DNS. Si vous saisissez un deuxième serveur DNS, le périphérique utilise le premier serveur DNS pour répondre. Saisir un serveur DNS peut offrir un accès plus rapide qu'utiliser un serveur DNS attribué de manière dynamique. Utilisez le paramètre par défaut (0.0.0.0) pour choisir un serveur DNS attribué de manière dynamique.

ÉTAPE 4 Saisissez le groupe d'adresses IPv6 :

- **Adresse de début** : adresse de début du groupe d'adresses IPv6.
- **Adresse de fin** : adresse de fin du groupe d'adresses IPv6.
- **Longueur du préfixe** : longueur du préfixe de l'adresse IP IPv6.

Affichage de l'état du serveur DHCP

L'état du DHCP affiche l'état du serveur DHCP et de ses clients.

L'onglet IPv6 n'est disponible que si vous avez activé la double pile IP sur la page **Configuration du réseau**.

Pour afficher l'état du serveur DHCP et de ses clients, cliquez sur l'onglet **IPv4** ou **IPv6**. Pour IPv4, sélectionnez **VLAN** ou **Option 82**. Pour IPv6, sélectionnez **Préfixe**.

Pour le serveur DHCP, les informations suivantes s'affichent :

- **Serveur DHCP** : adresse IP du serveur DHCP.
- **Adresse IP dynamique utilisée** : nombre d'adresses IP dynamiques utilisées.
- **Adresse IP statique utilisée (IPv4 uniquement)** : nombre d'adresses IP statiques utilisées.
- **DHCP disponible** : nombre d'adresses IP dynamiques disponibles.
- **Total** : nombre total d'adresses IP dynamiques gérées par le serveur DHCP.

La table des clients affiche les informations relatives au client DHCP :

- **Nom d'hôte client** : nom attribué à l'hôte client.
- **Adresse IP** : adresse IP dynamique attribuée au client.
- **Adresse MAC (IPv4 uniquement)** : adresse MAC d'un client.
- **Durée de bail du client** : durée pendant laquelle l'utilisateur d'un réseau peut rester connecté au routeur à l'aide d'une adresse IP dynamique.

Pour libérer une adresse IP du client IPv4, sélectionnez **Nom d'hôte client** et cliquez sur **Supprimer**.

Cliquez sur **Actualiser** pour renouveler les données.

Option 82

L'option 82 (option des informations sur l'agent de relais DHCP) 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.

L'identifiant de circuit configurable de l'option 82 du DHCP améliore la sécurité du processus de validation en vous permettant de déterminer les informations à fournir dans la description de l'identifiant de circuit de l'option 82.

Pour ajouter un **ID de circuit**, cliquez sur **Ajouter**. Une nouvelle ligne est ajoutée à la table et les identifiants de circuit sont répertoriés dans le menu déroulant ID de circuit de la fenêtre **Configuration DHCP**.

Pour modifier un **ID de circuit**, sélectionnez la ligne et cliquez sur **Modifier**. La ligne est ouverte pour modification.

Liaison IP et MAC

Lorsque le périphérique est configuré comme serveur DHCP ou pour un relais DHCP, vous pouvez lier les adresses IP statiques à 100 périphériques réseau, comme un serveur Web ou un serveur FTP. Une liaison n'attribue pas d'adresse IP à un périphérique. Vous devez vous assurer que chaque périphérique lié à une adresse IP statique dans la table de liaisons IP/MAC est configuré pour utiliser une adresse IP statique.

L'adresse MAC d'un périphérique figure généralement sur une étiquette située au-dessous ou à l'arrière du périphérique.

Liaison des adresses IP par découverte

Pour lier des adresses IP connues à des adresses MAC et nommer la liaison :

ÉTAPE 1 Cliquez sur **Afficher l'adresse MAC inconnue**. La table de liaisons IP/MAC s'affiche. Si le navigateur Web affiche un message relatif à la fenêtre contextuelle, autorisez l'affichage du contenu bloqué.

Les périphériques sont répertoriés en fonction de leurs adresses IP et MAC. Au besoin, cliquez sur **Actualiser** pour mettre à jour les données.

ÉTAPE 2 Saisissez un **nom** descriptif.

ÉTAPE 3 Cochez la case **Activer**. Vous pouvez également sélectionner tous les périphériques de la liste en cochant la case située en haut de la colonne Activer.

ÉTAPE 4 Cliquez sur **Enregistrer** pour ajouter les périphériques à la liste d'adresses IP statiques ou cliquez sur **Fermer** pour fermer la fenêtre contextuelle sans ajouter les périphériques sélectionnés.

Liaison manuelle des adresses IP

Pour ajouter une nouvelle liaison à la liste, cliquez sur **Ajouter** et saisissez les informations suivantes :

- **Adresse IP statique** : adresse IP statique. Saisissez 0.0.0.0 si vous voulez que le routeur attribue une adresse IP statique à ce périphérique.
- **Adresse MAC** : adresse MAC du périphérique. Saisissez l'adresse sans marque de ponctuation.
- **Nom** : nom descriptif du périphérique.
- **Activer** : cochez cette case pour lier une adresse IP statique à ce périphérique.

Modification ou suppression des entrées de liaison

Pour **modifier** les paramètres, sélectionnez une entrée dans la liste et cliquez sur **Modifier**. Les informations apparaissent dans les zones de texte. Apportez les modifications voulues, puis cliquez sur **Enregistrer**.

Pour **supprimer** une entrée de la liste, sélectionnez l'entrée à supprimer et cliquez sur **Supprimer**. Pour sélectionner un bloc d'entrées, cliquez sur la première entrée, maintenez la touche **Maj** enfoncée, puis cliquez sur la dernière entrée du bloc. Pour sélectionner des entrées individuellement, maintenez la touche **Ctrl** enfoncée, tout en cliquant sur chacune des entrées en question. Pour annuler la sélection d'une entrée, maintenez la touche **Ctrl** enfoncée tout en cliquant sur l'entrée.

Utilisation de la liste d'adresses IP statiques pour bloquer des périphériques

La liste d'adresses IP statiques peut être utilisée pour contrôler l'accès à votre réseau.

Pour interdire l'accès aux périphériques qui ne figurent pas sur la liste ou qui ne possèdent pas la bonne adresse IP :

- **Bloquer les adresses MAC de la liste correspondant à une adresse IP incorrecte** : cochez cette case pour empêcher un périphérique d'accéder à votre réseau si son adresse IP a été modifiée. Par exemple, si vous avez attribué l'adresse IP statique 192.168.1.100 et qu'une autre personne configure le périphérique pour utiliser l'adresse 192.168.149, le périphérique n'est pas autorisé à se connecter à votre réseau. Cette fonctionnalité permet de dissuader les utilisateurs de changer les adresses IP de leur périphérique sans votre autorisation. Décochez la case pour autoriser l'accès quelle que soit l'adresse IP actuellement attribuée.
- **Bloquer les adresses MAC ne figurant pas dans la liste** : cochez cette case pour interdire l'accès aux périphériques qui ne figurent pas dans la liste d'adresses IP statiques. Cette fonctionnalité permet d'empêcher que des périphériques inconnus accèdent à votre réseau. Décochez la case pour autoriser l'accès à n'importe quel périphérique configuré avec une adresse IP comprise dans la plage correcte.

Base de données DNS locale

Le service DNS (Domain Name Service) fait correspondre un nom de domaine à des adresses IP routables. Vous pouvez configurer une base de données DNS locale qui permet au périphérique d'agir en tant que serveur DNS local pour les noms de domaine couramment utilisés. L'utilisation d'une base de données locale peut s'avérer plus rapide que celle d'un serveur DNS externe. Si un nom de domaine demandé n'est pas trouvé dans la base de données locale, la demande est transmise au serveur DNS spécifié à la page **Configuration du réseau** > Paramètre WAN.

Si vous activez cette fonctionnalité, vous devez également configurer les périphériques clients pour utiliser le périphérique en tant que serveur DNS. Par défaut, les ordinateurs fonctionnant sous Windows sont configurés pour obtenir une adresse de serveur DNS automatiquement depuis la passerelle par défaut.

Pour modifier les paramètres de connexion TCP/IP, par exemple, sur un ordinateur équipé de l'environnement Windows, allez dans la fenêtre *Propriétés de la connexion au réseau local* > *Protocole Internet* > *Propriétés TCP/IP*. Choisissez **Utiliser l'adresse de serveur DNS suivante**, puis saisissez l'adresse IP LAN du routeur comme serveur DNS préféré. Pour obtenir plus d'informations, reportez-vous à la documentation du client que vous configurez.

Ajout, modification ou suppression des entrées DNS locales

Pour ajouter une nouvelle entrée, cliquez sur **Ajouter**, puis saisissez les informations suivantes :

- **Nom d'hôte** : saisissez le nom du domaine, comme *exemple.com* ou *exemple.org*. Si vous n'incluez pas la fin du nom de domaine, Microsoft Windows® termine automatiquement votre saisie par *.com*.
- **Adresse IP** : saisissez l'adresse IP de la ressource.

Pour **modifier** les paramètres, sélectionnez une entrée dans la liste. Les informations apparaissent dans les zones de texte. Apportez les modifications voulues, puis cliquez sur **Enregistrer**.

Pour **supprimer** une entrée de la liste, sélectionnez l'entrée à supprimer et cliquez sur **Supprimer**. Pour sélectionner un bloc d'entrées, cliquez sur la première entrée, maintenez la touche **Maj** enfoncée, puis cliquez sur la dernière entrée du bloc. Pour sélectionner des entrées individuellement, maintenez la touche **Ctrl** enfoncée, tout en cliquant sur chacune des entrées en question. Pour annuler la sélection d'une entrée, maintenez la touche **Ctrl** enfoncée tout en cliquant sur l'entrée.

Annonce de routeur (IPv6)

Le démon RADVD (Router Advertisement Daemon) est utilisé pour la configuration automatique et le routage des adresses IPv6. Lorsque cette option est activée, des messages sont envoyés régulièrement par le routeur et en réponse aux sollicitations. Un hôte utilise les informations pour connaître les préfixes et les paramètres du réseau local. Si vous désactivez cette option, la configuration automatique est alors désactivée et vous devrez configurer manuellement l'adresse IPv6, le préfixe de sous-réseau et la passerelle par défaut sur chaque périphérique.

Cette page est disponible si vous avez activé la double pile IP sur la page **Configuration du réseau**. Si tel n'est pas le cas, un message s'affiche lorsque vous tentez d'accéder à cette page.

Pour **activer l'annonce du routeur**, cochez cette case et remplissez les autres champs :

- **Mode d'annonce** : sélectionnez l'une des options suivantes :
  - **Multidiffusion non demandée** : envoyez les messages de notification du routeur à toutes les interfaces appartenant au groupe de multidiffusion. Il s'agit de l'option par défaut. Renseignez également le champ **Intervalle d'annonce**, qui indique à quelle fréquence les messages sont envoyés. Saisissez une valeur comprise entre 10 et 1800 millisecondes. La valeur par défaut est 30 secondes.
  - **Monodiffusion uniquement** : envoyez les messages de notification de routeur uniquement aux adresses IPv6 connues.

- **Indicateurs d'annonce** : définit si les hôtes peuvent utiliser DHCPv6 pour obtenir des adresses IP et d'autres informations. Les options sont les suivantes :
  - **Gérés** : les hôtes utilisent un protocole de configuration administré/dynamique (DHCPv6) pour obtenir les adresses dynamiques et d'autres informations via DHCPv6.
  - **Autre** : utilise un protocole de configuration administré/dynamique (DHCPv6) pour obtenir d'autres informations, telles que des adresses de serveur DNS.
- **Préférence de routeur** : la mesure de préférence **Élevé, Moyen** ou **Faible** est utilisée dans une topologie réseau dans laquelle des hôtes à plusieurs hébergements ont accès à plusieurs routeurs. Cette valeur permet aux hôtes de choisir un routeur approprié. Si deux routeurs sont accessibles, celui avec la valeur de préférence la plus élevée est choisi. Ces valeurs sont ignorées par les hôtes qui ne mettent pas en œuvre la préférence de routeur. La valeur par défaut est Élevé.
- **MTU** : taille du paquet le plus volumineux pouvant être transmis sur le réseau. L'unité maximale de transmission (MTU) est utilisée dans les messages de notification de routeur pour que tous les nœuds du réseau utilisent la même valeur de MTU lorsque la MTU du réseau LAN n'est pas connue. La valeur par défaut est 1500 octets, ce qui correspond à la valeur standard des réseaux Ethernet. Pour les connexions PPPoE, la valeur standard est de 1492 octets. Sauf si votre FAI exige une autre valeur, cette valeur ne doit pas être changée.
- **Durée de vie du routeur** : nombre de secondes pendant lesquelles les messages de notification de routeur figurent sur le routage. La valeur par défaut est 3600 secondes.

Pour ajouter un nouveau sous-réseau, cliquez sur **Ajouter** puis remplissez les champs **Adresse IPv6**, **Longueur du préfixe** et **Durée de vie**.

5

Gestion du système

Le module Gestion du système vous permet de configurer les paramètres avancés, comme les outils de diagnostic, et de réaliser des tâches, comme les mises à niveau de micrologiciels, les sauvegardes et les redémarrages du périphérique.

Connexions double WAN

Utilisez cette fonction pour configurer les paramètres de vos connexions Internet, si vous utilisez plusieurs interfaces WAN.

Pour configurer l'équilibrage de charge et gérer vos connexions WAN, vous pouvez choisir l'un des modes suivants :

- **Sauvegarde de liaisons intelligentes** : assure une connectivité en continu. Si la connexion WAN principale n'est pas disponible, la connexion WAN de secours est utilisée. Sélectionnez l'interface WAN principale dans le menu déroulant.
- **Équilibrage de charge** : utilisez les deux connexions WAN simultanément afin d'augmenter la bande passante disponible. Le routeur équilibre le trafic entre les deux interfaces, par permutation pondérée.

REMARQUE Les requêtes DNS ne sont pas soumises à l'équilibrage de charge.

Pour configurer les paramètres d'interface, sélectionnez **Interface WAN** et cliquez sur **Modifier**. La fenêtre de paramétrage de l'interface s'affiche. Saisissez les paramètres suivants :

Bande passante maximale fournie par le FAI

Saisissez les valeurs maximales de la bande passante, telles qu'elles vous ont été communiquées par votre FAI. Si la bande passante excède la valeur spécifiée, le routeur utilise une autre interface WAN pour la connexion suivante.

- **Amont :** bande passante maximale en amont spécifiée par votre FAI. La valeur par défaut est 10000 Kbit/s. La valeur maximale est 1000000 kbit/s.
- **Aval :** bande passante maximale en aval spécifiée par votre FAI. La valeur par défaut est 10000 Kbit/s.

Détection de services réseau

Vous pouvez cocher cette case pour permettre au périphérique de détecter la connectivité réseau en envoyant une commande Ping aux périphériques spécifiés. Saisissez ensuite les paramètres comme indiqué ci-après :

- **Nombre de nouvelles tentatives :** nombre d'envois d'une commande Ping à un périphérique. La plage est comprise entre 1 et 99999. La valeur par défaut est 3.
- **Délai d'expiration des nouvelles tentatives :** nombre de secondes devant s'écouler entre deux commandes Ping. La plage est comprise entre 1 et 9999999. La valeur par défaut est 10 secondes.
- **En cas d'échec :** action à effectuer en cas d'échec d'un test Ping.
  - **Générer la condition d'erreur dans le journal système :** enregistre l'échec dans le journal système. Aucun basculement n'a lieu vers l'autre interface.
  - **Conserver le journal système et supprimer la connexion** : un basculement se produit et l'interface de secours est utilisée. Lorsque la connectivité du port WAN est restaurée, le trafic reprend.
- **Passerelle par défaut, Hôte du FAI, Hôte distant** et **Hôte de recherche DNS :** sélectionnez le périphérique pour lequel vous souhaitez déterminer la connectivité réseau à l'aide d'une commande Ping. Dans le cas d'un hôte de fournisseur d'accès à Internet ou d'un hôte distant, saisissez l'adresse IP. Dans le cas d'un hôte DNS Lookup, saisissez un nom d'hôte ou un nom de domaine. Décochez la case appropriée si vous ne souhaitez pas envoyer de commande Ping à ce périphérique pour la détection d'un service réseau.

Liaison de protocoles

La fonction Liaison de protocoles exige que cette interface soit utilisée pour les protocoles spécifiés, ainsi que pour les adresses sources et de destination indiquées. Cette fonction permet à un administrateur de lier un trafic sortant spécifique à une interface WAN. Cette opération est souvent utilisée lorsque les deux interfaces WAN ont des caractéristiques différentes ou lorsque du trafic allant d'un réseau LAN vers un réseau WAN doit passer par la même interface WAN.

Pour ajouter ou modifier des entrées de table, cliquez sur **Ajouter** ou **Modifier**, puis entrez les informations suivantes :

- **Service :** service (ou Tout le trafic) à lier à cette interface WAN. Si un service particulier ne figure pas dans la liste, vous pouvez cliquer sur **Gestion des services** pour l'ajouter. Pour plus d'informations, reportez-vous à la section **Ajout ou modification d'un service**.
- **IP source** et **IP de destination :** source interne et destination externe du trafic transitant par ce port WAN. Dans le cas d'une plage d'adresses IP, saisissez la première adresse dans le premier champ et la dernière, dans le champ *À*. Dans le cas d'une adresse IP unique, saisissez la même adresse dans les deux champs.

En ce qui concerne la liaison de protocoles, cochez ou décochez la case pour activer ou désactiver la règle.

Pour **modifier** les paramètres, sélectionnez une entrée dans la liste. Les informations apparaissent dans les zones de texte. Apportez les modifications voulues, puis cliquez sur **Enregistrer**.

Pour **supprimer** une entrée de la liste, sélectionnez l'entrée à supprimer et cliquez sur **Supprimer**. Pour sélectionner un bloc d'entrées, cliquez sur la première entrée, maintenez la touche **Maj** enfoncée, puis cliquez sur la dernière entrée du bloc. Pour sélectionner des entrées individuellement, maintenez la touche **Ctrl** enfoncée, tout en cliquant sur chacune des entrées en question. Pour annuler la sélection d'une entrée, maintenez la touche **Ctrl** enfoncée tout en cliquant sur l'entrée.

Ajout ou modification d'un service

Pour ajouter une nouvelle entrée à la liste Service ou pour modifier une entrée, cliquez sur **Gestion des services**. La liste peut comporter jusqu'à 30 services. Si le navigateur Web affiche une mise en garde relative à la fenêtre contextuelle, autorisez le contenu bloqué.

Pour ajouter un service à la liste, cliquez sur **Ajouter** et entrez les informations suivantes :

- **Nom du service :** brève description du service en question.
- **Protocole :** protocole requis. Reportez-vous à la documentation du service que vous hébergez.
- **Plage de ports :** plage de ports requise.

Pour **modifier** les paramètres, sélectionnez une entrée dans la liste et cliquez sur **Modifier**. Les informations apparaissent dans les zones de texte. Apportez les modifications voulues, puis cliquez sur **Enregistrer**.

Pour **supprimer** une entrée de la liste, sélectionnez l'entrée à supprimer et cliquez sur **Supprimer**. Pour sélectionner un bloc d'entrées, cliquez sur la première entrée, maintenez la touche **Maj** enfoncée, puis cliquez sur la dernière entrée du bloc. Pour sélectionner des entrées individuellement, maintenez la touche **Ctrl** enfoncée, tout en cliquant sur chacune des entrées en question. Pour annuler la sélection d'une entrée, maintenez la touche **Ctrl** enfoncée tout en cliquant sur l'entrée.

Gestion de la bande passante

La fonction Gestion de la bande passante permet de configurer les paramètres de la bande passante du trafic en amont et en aval, ainsi que les paramètres de qualité de service (QoS) des différents types de trafic, comme les services vocaux.

Bande passante maximale fournie par le FAI

Saisissez les valeurs maximales de la bande passante, telles qu'elles vous ont été communiquées par votre FAI :

- **Amont :** bande passante maximale en amont spécifiée par votre FAI.
- **Aval :** bande passante maximale en aval spécifiée par votre FAI.

Type de gestion de la bande passante

Sélectionnez l'une des options de gestion suivantes :

- **Contrôle du débit :** valeurs de bande passante minimale (garantie) et maximale (limitée) de chaque service ou adresse IP. Vous pouvez ajouter jusqu'à 100 services.
- **Priorité :** gérer la bande passante en identifiant les services à haute priorité et à basse priorité.

Contrôle du débit

Pour ajouter une interface qui fait l'objet d'une gestion de la bande passante, cliquez sur **Ajouter**, puis entrez les paramètres :

- **Interface** : interface prenant en charge le service.
- **Service :** service à gérer. Si un service particulier ne figure pas dans la liste, vous pouvez cliquer sur **Gestion des services** pour l'ajouter.
- **IP :** adresse IP ou plage d'adresses IP à contrôler.
- **Direction :** sélectionnez **Amont** pour le trafic sortant. Sélectionnez **Aval** pour le trafic entrant.
- **Fréquence minimale** : débit minimal en Kbit/s de la bande passante garantie.
- **Fréquence maximale :** débit maximal en Kbit/s de la bande passante garantie.

Cochez la case pour activer le service.

Configuration de la priorité

Pour ajouter une interface qui fait l'objet d'une gestion de la bande passante, cliquez sur **Ajouter**, puis entrez les paramètres :

- **Interface : interface prenant en charge le service.**
- **Service :** service à gérer. Si un service particulier ne figure pas dans la liste, vous pouvez cliquer sur **Gestion des services** pour l'ajouter.
- **Direction :** sélectionnez **Amont** pour le trafic sortant. Sélectionnez **Aval** pour le trafic entrant.
- **Priorité :** sélectionnez le niveau de priorité pour ce service : **Élevé** ou **Faible**. Le niveau de priorité par défaut est Moyen ; il ne s'affiche donc pas dans l'interface Web.

Cochez la case pour activer le service.

Pour **modifier** les paramètres, sélectionnez une entrée dans la liste et cliquez sur **Modifier**. Les informations apparaissent dans les zones de texte. Apportez les modifications voulues, puis cliquez sur **Enregistrer**.

Pour **supprimer** une entrée de la liste, sélectionnez l'entrée à supprimer et cliquez sur **Supprimer**. Pour sélectionner un bloc d'entrées, cliquez sur la première entrée, maintenez la touche **Maj** enfoncée, puis cliquez sur la dernière entrée du bloc. Pour sélectionner des entrées individuellement, maintenez la touche **Ctrl** enfoncée, tout en cliquant sur chacune des entrées en question. Pour annuler la sélection d'une entrée, maintenez la touche **Ctrl** enfoncée tout en cliquant sur l'entrée.

SNMP

Le protocole réseau SNMP (Simple Network Management Protocol) permet aux administrateurs réseau de gérer, de surveiller et de recevoir des notifications d'événements critiques, à mesure qu'ils se produisent sur le réseau. Le périphérique prend en charge les protocoles SNMP v1/v2c et SNMP v3. Le périphérique accepte également les bases d'informations de gestion MIB (Management Information Bases) standard, telles que MIBII, ainsi que les bases MIB privées.

Le périphérique fait office d'agent SNMP dans la mesure où il répond aux commandes SNMP des systèmes de gestion de réseau SNMP. Il prend en charge les commandes SNMP standard, get/next/set. Il génère également des messages d'interception « trap » afin de prévenir le gestionnaire SNMP en cas d'alarme. C'est le cas notamment lors des réinitialisations, des cycles de mise hors tension et sous tension, ainsi que lors des autres événements de la liaison du réseau WAN.

Configuration du protocole SNMP

- **Nom du système :** nom d'hôte du périphérique.
- **Contact système :** nom de l'administrateur réseau à contacter si des mises à jour sont disponibles pour le périphérique.
- **Emplacement du système :** coordonnées de l'administrateur réseau **:** adresse e-mail, numéro de téléphone ou encore numéro de récepteur de radio-messagerie.
- **Nom de la communauté d'interruptions :**mot de passe envoyé avec chaque interruption au gestionnaire SNMP. La chaîne peut comporter au maximum 64 caractères alphanumériques. La valeur par défaut est **public**.

- **Activer SNMPv1/v2c :** active SNMP v1/v2c.
  - **Nom de communauté Get** : chaîne de communauté permettant d'authentifier les commandes SNMP GET. Le nom que vous saisissez ne doit pas comporter plus de 64 caractères alphanumériques. La valeur par défaut est *public*.
  - **Nom de communauté Set** : chaîne de communauté permettant d'authentifier les commandes SNMP SET. Le nom que vous saisissez ne doit pas comporter plus de 64 caractères alphanumériques. La valeur par défaut est *privé*.
  - **Adresse IP du récepteur d'interruptions SNMPv1/v2c** : adresse IP ou nom de domaine du serveur sur lequel vous exécutez le logiciel de gestion SNMP.
- **Activer SNMPv3 :** active SNMPv3. (Cochez la case et cliquez sur **Enregistrer** avant de créer des groupes et des utilisateurs SNMP.) Suivez les instructions figurant dans la section **Configuration de SNMPv3**.
  - **Adresse IP du récepteur d'interruptions SNMPv3** : adresse IP ou nom de domaine du serveur sur lequel vous exécutez le logiciel de gestion SNMP.
  - **Utilisateur récepteur d'interruptions SNMPv3** : nom d'utilisateur du serveur sur lequel vous exécutez le logiciel de gestion SNMP.

Configuration de SNMPv3

Vous pouvez créer des groupes SNMPv3 pour gérer l'accès aux objets MIB de SNMP et identifier les utilisateurs ayant accès aux différents groupes.

Pour ajouter ou modifier un groupe :

ÉTAPE 1 Cliquez sur **Ajouter** ou sélectionnez un groupe, puis cliquez sur **Modifier** dans la table des groupes.

ÉTAPE 2 Entrez le **nom du groupe**.

ÉTAPE 3 Sélectionnez le **niveau de sécurité** dans le menu déroulant. Les options **Authentification** ou **Confidentialité** oblige les utilisateurs à s'identifier par mot de passe. Lorsque l'option **Aucune authentification**, **Aucune confidentialité** est sélectionnée, aucun des utilisateurs du groupe n'est tenu de définir un mot de passe d'authentification ou un mot de passe de confidentialité. Le réglage par défaut est **Aucune authentification, Aucune confidentialité**. Les mots de passe d'authentification et de confidentialité doivent contenir au moins 8 caractères.

ÉTAPE 4 Sélectionnez les bases **MIB** accessibles aux membres du groupe.

ÉTAPE 5 Cliquez sur **Enregistrer**.

Pour ajouter ou modifier un utilisateur :

ÉTAPE 1 Cliquez sur **Ajouter** ou sélectionnez un utilisateur, puis cliquez sur **Modifier** dans la table des utilisateurs.

ÉTAPE 2 Entrez le **nom d'utilisateur**.

ÉTAPE 3 Sélectionnez le **groupe** dans le menu déroulant.

ÉTAPE 4 Sélectionnez la **méthode d'authentification** et saisissez le **mot de passe d'authentification**.

ÉTAPE 5 Sélectionnez la **méthode de protection de la confidentialité** et saisissez le **mot de passe de confidentialité**.

ÉTAPE 6 Cliquez sur **Enregistrer**.

Détection - Bonjour

Bonjour est un protocole de découverte de service qui localise les périphériques réseau, tels que les ordinateurs et les serveurs reliés à votre réseau LAN. Lorsque cette fonction est activée, le périphérique diffuse régulièrement des enregistrements du service Bonjour au réseau LAN pour faire connaître son existence.

REMARQUE Dans le cadre de la découverte des produits Cisco, Cisco fournit un utilitaire qui fonctionne via une simple barre d'outils, dans le navigateur Web FindIt. Cet utilitaire détecte les périphériques Cisco sur le réseau et affiche les informations de base les concernant, telles que leur numéro de série et leur adresse IP. Pour obtenir plus d'informations sur l'utilitaire et le télécharger, rendez-vous sur la page www.cisco.com/go/findit.

Pour activer Bonjour au niveau global, cochez la case **Activer la découverte**. Le protocole Bonjour est activé par défaut.

Si vous souhaitez Bonjour pour un réseau VLAN, cochez la case de la colonne **Activer Bonjour**. Le protocole Bonjour est activé par défaut.

Propriétés 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, qui consiste en grande partie d'un Ethernet câblé. Les informations LLDP sont envoyées par des périphériques depuis chacune des interfaces à intervalles fixes, sous 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 activer les propriétés LLDP, cochez la case **Activer**. (Les propriétés LLDP sont activées par défaut.)

Pour activer les propriétés LLDP sur une interface, cochez la case **Activer**, **WAN1** ou **WAN2**. (Les propriétés LLDP sont activées par défaut.)

La table des voisins LLDP affiche les informations suivantes :

- **Port local** : identifiant du port.
- **Sous-type d'ID de châssis** : type d'identifiant du 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 périphérique est affichée.
- **Sous-type d'ID de port** : type d'identifiant du port.
- **ID du port** : identifiant du port.
- **Nom du système** : nom du périphérique.
- **Durée de vie** : fréquence (en secondes) d'envoi des mises à jour des annonces LLDP.

Utilisation du diagnostic

La page Diagnostic permet d'accéder à deux outils intégrés, Recherche de nom DNS et Ping. Si vous suspectez un problème de connectivité, vous pouvez recourir à ces outils pour procéder à des investigations sur son origine.

Si vous souhaitez utiliser le serveur DNS pour acquérir une adresse IP, sélectionnez **Recherche DNS**, saisissez le**nom du domaine de recherche** (ex. : www.cisco.com), puis cliquez sur **OK**. L'adresse IP s'affiche.

Pour tester la connectivité à un hôte spécifié, sélectionnez **Ping**, entrez une adresse IP ou un nom d'hôte et cliquez sur **OK**. Si vous ne connaissez pas l'adresse IP, faites appel à l'outil de recherche DNS pour l'obtenir. Le test Ping indique si le périphérique peut envoyer un paquet à un hôte distant et recevoir une réponse de sa part.

Si le test réussit, les informations suivantes apparaissent :

- **État :** état du test : Test, Test réussi ou Échec du test
- **Paquets :**nombre de paquets émis, nombre de paquets reçus et pourcentage de paquets perdus lors du test Ping.
- **Durée de l'aller-retour :**durées minimale, maximale et moyenne- des boucles lors du test Ping.

Valeurs d'origine

Pour redémarrer le périphérique et restaurer les paramètres d'origine, cliquez sur **Valeurs d'origine**.

Pour restaurer les paramètres d'origine du périphérique, y compris les certificats par défaut, cliquez sur **Paramètres d'origine, y compris les certificats**.

Mise à niveau du micrologiciel

Cette fonction permet de télécharger le micrologiciel pour votre périphérique à partir d'un ordinateur ou d'une clé USB, et de l'installer. La fenêtre affiche la **version du micrologiciel** en cours d'utilisation sur le périphérique.

REMARQUE Si vous choisissez une version antérieure du micrologiciel, il se peut que le périphérique restaure les paramètres d'origine. Nous vous conseillons de faire une sauvegarde de votre configuration en suivant la procédure **Sauvegarde et restauration** avant de mette à jour le micrologiciel.

La mise à niveau du micrologiciel peut prendre quelques minutes.

Ne mettez pas le périphérique hors tension, n'appuyez pas sur le bouton de réinitialisation, ne fermez pas le navigateur et ne mettez pas fin à la liaison au cours de ce processus.

Pour télécharger le micrologiciel à partir d'un ordinateur, sélectionnez **Mise à niveau du micrologiciel depuis un ordinateur** et sélectionnez le fichier.

Pour télécharger le micrologiciel à partir d'une clé USB, sélectionnez **Mise à niveau du micrologiciel depuis un périphérique USB** et sélectionnez le fichier.

Sélection de la langue ou Configuration de la langue

Utilisez la page Sélection de la langue ou la page Configuration de la langue pour modifier la langue associée à l'interface utilisateur et à l'aide de votre périphérique.

Pour les versions de micrologiciels ultérieures à la version 1.0.2.03, utilisez la page Sélection de la langue pour sélectionner une langue.

ÉTAPE 1 Accédez à la page **Gestion du système** > **Sélection de la langue**.

ÉTAPE 2 Dans la liste déroulante **Sélectionner une langue**, sélectionnez une langue.

ÉTAPE 3 Cliquez sur **Enregistrer**.

Vous pouvez également sélectionner une langue comme suit :

- Dans la page Connexion, sélectionnez une langue dans la liste déroulante **Langue**.
- Dans toutes les pages de configuration, sélectionnez une langue dans la liste déroulante située en haut à droite.

Pour les versions de micrologiciels correspondant à la version 1.0.2.03 ou antérieures, utilisez la page Configuration de la langue pour sélectionner une nouvelle langue en téléchargeant un module linguistique sur votre périphérique.

Pour ajouter un module linguistique et sélectionner une langue :

ÉTAPE 1 Accédez à la page **Gestion du système** > **Configuration de la langue**.

ÉTAPE 2 Dans la liste déroulante **Mode**, sélectionnez **Ajouter**.

ÉTAPE 3 Saisissez le **nom de la nouvelle langue**.

ÉTAPE 4 Recherchez le **Nom du fichier de langue** pour télécharger le nouveau fichier de langue.

ÉTAPE 5 Cliquez sur **Enregistrer**.

ÉTAPE 6 Une fois le module linguistique téléchargé, sélectionnez une langue dans la liste déroulante située en haut à droite de la page Configuration de la langue ou sur les autres pages de configuration.

Redémarrage

Lorsque vous effectuez un redémarrage à partir de la page Redémarrer, le routeur vous fait parvenir un fichier journal (si la consignation est activée), avant la réinitialisation du périphérique. Les paramètres du périphérique sont conservés.

Pour redémarrer le périphérique, cliquez sur **Redémarrer le routeur**.

Sauvegarde et restauration

Les fichiers de configuration peuvent être importés, exportés et copiés. Le routeur propose deux fichiers de configuration gérés : le fichier de démarrage et le fichier miroir. Le périphérique charge le fichier de démarrage à partir de la mémoire lorsqu'il démarre dans la configuration d'exécution et copie le fichier de démarrage dans le fichier miroir. Le fichier miroir contient ainsi les dernières informations de configuration valides connues.

Si le fichier de configuration de démarrage est corrompu ou échoue pour une raison quelconque, le fichier de configuration miroir est utilisé. Le routeur copie automatiquement le fichier de configuration de démarrage dans le fichier de configuration miroir, après 24 heures d'exécution dans des conditions stables (aucun redémarrage et aucun changement de configuration au cours des 24 heures précédentes).

Restauration des paramètres à partir d'un fichier de configuration

Pour restaurer la configuration de démarrage à partir d'un fichier précédemment enregistré sur un ordinateur ou un périphérique USB :

ÉTAPE 1 Dans la section Restaurer le fichier de configuration de démarrage, sélectionnez **Restaurer le fichier de configuration de démarrage depuis un ordinateur** et cliquez sur **Parcourir**. Vous pouvez également sélectionner **Restaurer le fichier de configuration de démarrage depuis un périphérique USB** et cliquez sur **Actualiser**.

ÉTAPE 2 Sélectionnez un fichier de configuration (.config).

ÉTAPE 3 Cliquez sur **Restaurer**. Ce processus peut prendre jusqu'à une minute. Si le fichier de configuration contient un autre mot de passe que le mot de passe de gestion du périphérique actuel, vous êtes invité à saisir ce mot de passe avant la restauration du fichier de configuration.

ÉTAPE 4 Cliquez sur **Gestion système > Redémarrer** dans l'arborescence.

Les paramètres importés ne sont appliqués qu'après le redémarrage du périphérique en sélectionnant **Gestion système > Redémarrer**.

Vous pouvez également appuyer sur le bouton **Réinitialiser** du périphérique pendant une seconde pour redémarrer le routeur.

Sauvegarde des fichiers de configuration et des fichiers miroir

Pour enregistrer les fichiers de configuration de démarrage et miroir sur votre ordinateur ou votre clé USB :

ÉTAPE 1 Sélectionnez **Fichier de configuration de secours vers un ordinateur** ou **Fichier de configuration de secours vers un périphérique USB.**

ÉTAPE 2 Cliquez sur **Sauvegarder la configuration de démarrage** ou sur **Sauvegarder la configuration du miroir**. La fenêtre Téléchargement de fichiers s'affiche.

ÉTAPE 3 Cliquez sur **Enregistrer** et choisissez un emplacement. Vous pouvez également entrer un nom de fichier, puis cliquer sur **Enregistrer**.

CONSEIL Les noms de fichier par défaut sont respectivement *Startup.config* et *Mirror.config*. L'extension *.config* est obligatoire. Afin de faciliter l'identification, il peut être utile de saisir un nom de fichier incluant la date et l'heure actuelles.

Copie du fichier miroir dans le fichier de démarrage

Vous pouvez copier manuellement le fichier de configuration de démarrage du périphérique dans le fichier de configuration miroir.

Ce processus vous permet, par exemple, de sauvegarder une configuration connue correcte avant de modifier la configuration de démarrage :

- Le fichier de configuration de démarrage est automatiquement copié dans le fichier de configuration miroir toutes les 24 heures.
- Lorsque vous enregistrez les modifications apportées aux paramètres du périphérique, le compteur horaire est réinitialisé et la copie automatique suivante a lieu 24 heures plus tard, à moins que vous ne forciez l'enregistrement du fichier de démarrage en tant que fichier miroir.

Pour copier le fichier de démarrage dans le fichier miroir, cliquez sur **Copier le miroir vers le démarrage**. La copie est exécutée immédiatement et ne peut être annulée. À l'issue de l'opération, la page est actualisée.

Nettoyage de la configuration

Le nettoyage de la configuration entraîne la suppression du fichier miroir et du fichier de configuration de démarrage.

Pour supprimer le fichier miroir et le fichier de configuration de démarrage, cliquez sur **Expurger la configuration**.

AVERTISSEMENT La configuration miroir est supprimée immédiatement et l'opération ne peut pas être annulée. L'appareil est réinitialisé en utilisant les paramètres d'Valeurs d'origine et le redémarrage de l'appareil a lieu.

Sauvegarde du micrologiciel sur une clé USB

Pour sauvegarder le micrologiciel sur une clé USB connectée au port USB, sélectionnez la clé dans le menu déroulant et cliquez sur **Sauvegarder**. Le périphérique enregistre l'image du micrologiciel en tant qu'**`image.bin`**.

6

Gestion des ports

Utilisez la gestion des ports pour configurer les paramètres de port et afficher leur état.

Vous pouvez activer la mise en miroir des ports, désactiver un port ou encore définir les paramètres de priorité, de vitesse, de mode duplex et de négociation automatique. Vous pouvez également activer des réseaux locaux virtuels (VLAN) basés sur les ports pour contrôler le trafic entre les périphériques de votre réseau.

Configuration des ports

Vous pouvez définir la mise en miroir des ports et gérer les ports, comme les paramètres liés à la priorité et au mode. La mise en miroir des ports envoie une copie des paquets réseau détectés sur un port donné vers une connexion de surveillance réseau située sur un autre port. Cette opération est souvent utilisée sur les équipements réseau qui nécessitent une surveillance du trafic réseau, par exemple un système de détection des intrusions. La mise en miroir des ports sur un commutateur Cisco Systems est généralement appelée Analyseur de port commuté (SPAN).

Les ingénieurs et administrateurs réseau utilisent la mise en miroir des ports pour analyser et déboguer des données, ou détecter des erreurs dans le réseau. Cette fonction vous permet de surveiller la performance du réseau et vous avertit en cas de problème.

REMARQUE Lorsque le **Clonage de l'adresse MAC** est activé, la mise en miroir des ports ne fonctionne pas.

Pour activer la mise en miroir des ports du routeur RV320, cochez la case **Activer la mise en miroir des ports**. Les paquets entrants et sortants sur les ports WAN et LAN sont copiés vers LAN1.

Pour activer la mise en miroir des ports du routeur RV325, cochez la case **Activer la mise en miroir des ports**. Les paquets entrants et sortants sur les ports LAN sont copiés vers LAN1.

Les informations en lecture seule qui suivent sont affichées pour chaque port :

- **ID du port** : numéro ou nom du port indiqué sur le périphérique.
- **Interface** : type d'interface : LAN, WAN ou DMZ.

Saisissez les paramètres suivants :

- **Désactiver** : cochez cette case pour désactiver un port. Par défaut, tous les ports sont activés.

- **EEE** : cochez cette case pour activer le mode EEE (Energy-Efficient Ethernet) qui permet de réduire la consommation d'énergie durant les périodes de faible activité au niveau du transfert de données.
- **Priorité** : pour chaque port, sélectionnez le niveau de priorité approprié, **Élevé** ou **Normal**. Ceci garantit la qualité de service en donnant la priorité au trafic des périphériques branchés sur des ports spécifiques. Par exemple, vous pouvez attribuer une priorité élevée à un port utilisé pour les jeux ou la vidéoconférence. Le paramètre par défaut est Normal.
- **Mode** : vitesse du port et mode duplex. Lorsque l'option **Négociation automatique** est sélectionnée, le périphérique négocie automatiquement les vitesses de connexion et le mode duplex avec le périphérique connecté.

État des ports

Cette option affiche un récapitulatif de l'état des ports. Cliquez sur **Actualiser** pour mettre à jour les données.

La table Ethernet affiche les informations suivantes :

- **ID du port** : emplacement du port.
- **Type** : type de port.
- **État de la liaison** : état de la connexion.
- **Activité du port** : état du port.
- **Priorité** : priorité du port définie dans la fenêtre Configuration des ports.
- **État du débit** : vitesse du port, 10 Mbit/s ou 100 Mbit/s ou 1000 Mbit/s.
- **État du duplex** : mode Duplex, *Semi-duplex* ou *Duplex intégral*.
- **Négociation automatique** : état du mode Duplex.

Statistiques sur le trafic

Les informations suivantes concernant le port sélectionné s'affichent dans la table des statistiques :

- **ID du port** : emplacement du port.
- **État de la liaison** : état de la connexion.

- **Paquets reçus** : nombre de paquets reçus sur le port.
- **Paquets reçus** : nombre de paquets reçus, en octets.
- **Paquets émis** : nombre de paquets envoyés sur le port.
- **Paquets émis** : nombre de paquets envoyés, en octets.
- **Erreur de paquets** : nombre d'erreurs de paquets.

Membres du réseau VLAN

Par défaut, tous les ports LAN se trouvent sur le réseau VLAN 1.

Pour activer les réseaux VLAN, cochez la case **Activer le VLAN**.

Pour ajouter ou modifier un réseau VLAN :

- **ID de réseau VLAN** : identifiant du réseau VLAN.
- **Description** : description du réseau VLAN.
- **Routage inter-VLAN** : permet aux paquets de transiter entre les réseaux VLAN. Un réseau VLAN ayant le paramètre de routage inter VLAN désactivé est isolé des autres réseaux VLAN. Les règles d'accès du pare-feu peuvent être configurées pour mieux réguler (autoriser ou refuser) le trafic inter-VLAN.
- **Pour le RV320**, **LAN 1** à **LAN 4** : un port peut être balisé, non balisé ou exclu du réseau VLAN.
- **Pour le RV325**, **LAN 1** à **LAN 14** : un port peut être balisé, non balisé ou exclu du réseau VLAN.

QoS:CoS/Paramètre DSCP

Cette option regroupe le trafic par qualités de service (CoS) pour garantir une bande passante et un niveau de priorité plus élevé pour les services spécifiés. Tout le trafic qui n'est pas ajouté au groupe IP utilise le mode Intelligent Balancer.

Pour configurer les files d'attente de service, sélectionnez la priorité de la **file d'attente** (4 étant le niveau de priorité le plus élevé et 1 le plus faible) dans le menu déroulant.

Pour définir la valeur DSCP (Differential Services Code Point), sélectionnez **File d'attente** dans les menus déroulants.

Marquage DSCP

Le point de code de services différenciés, ou DiffServ, définit une méthode simple et évolutive permettant de classer et de gérer le trafic réseau, mais aussi de fournir des garanties de qualité de service (QoS). DiffServ peut être utilisé pour assurer une faible latence au trafic réseau critique, comme le contenu vocal ou multimédia en continu, tout en proposant un service au mieux et des services non critiques, comme le trafic Web ou le transfert de fichiers.

Pour configurer les files d'attente de service, cliquez sur **Modifier** et définissez la valeur Cos/802.1p, avant de saisir l'état et la priorité.

Configuration 802.1X

Le contrôle d'accès réseau par port 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. Il empêche également l'accès à ce port en cas d'échec de l'authentification et de l'autorisation. Dans ce contexte, un port est un point de liaison unique vers l'infrastructure LAN.

Pour configurer l'authentification basée sur les ports :

ÉTAPE 1 Cochez la case **Authentification basée sur les ports** pour activer cette fonction.

ÉTAPE 2 Saisissez l'adresse IP du serveur RADIUS.

ÉTAPE 3 Saisissez le numéro du **port UDP RADIUS**.

ÉTAPE 4 Saisissez la **clé secrète RADIUS**.

ÉTAPE 5 Sélectionnez l'**état de l'administration** dans la table des ports du menu déroulant :

- **Autorisation forcée** : aucune autorisation n'est requise. Lorsqu'un port LAN est en état d'autorisation forcée, les ordinateurs connectés à ce port doivent avoir une adresse IP statique. *Vous devez choisir au moins un port LAN pour l'autorisation forcée.*
- **Non-autorisation forcée** : l'état du port contrôlé est défini pour bloquer le trafic ; les paquets ne peuvent pas transiter.
- **Automatique** : active l'authentification basée sur les ports. L'interface est définie sur l'état autorisé ou l'état non autorisé en fonction de l'échange d'authentification entre le périphérique et le client.

ÉTAPE 6 Cliquez sur **Enregistrer**.

7

Pare-feu

L'objectif principal d'un pare-feu est de contrôler le trafic entrant et sortant d'un réseau en analysant les paquets de données et en déterminant si le trafic est autorisé à transiter, en fonction des règles prédéterminées. Un pare-feu réseau crée un pont entre un réseau interne considéré comme sécurisé et un autre réseau, généralement un (inter-) réseau externe, comme l'Internet, qui n'est pas considéré comme sécurisé.

Général

Les commandes générales de pare-feu gèrent les fonctions généralement utilisées par les navigateurs et les applications Internet.

Activation des fonctions de pare-feu

Pour activer le **pare-feu**, cochez la case **Activer**. Les fonctions de pare-feu suivantes peuvent être activées ou désactivées selon vos besoins :

- **SPI (Stateful Packet Inspection)** : surveille l'état des connexions réseau (flux TCP, communication UDP, etc.) qui passe par le pare-feu. Le pare-feu distingue les paquets légitimes pour différents types de connexion. Le pare-feu autorise uniquement les paquets correspondant à une connexion active connue ; les autres sont rejetés.
- **DoS (Denial-of-service)** : détecte les attaques visant à surcharger le serveur. D'une manière générale, les attaques DoS sont mises en place de la façon suivante : par une réinitialisation forcée du ou des ordinateurs cible, par l'utilisation de ses ressources de sorte qu'il soit dans l'incapacité d'assurer le service prévu ou par le blocage des moyens de communication entre les utilisateurs cible et la victime afin de rendre impossible toute communication.
- **Bloquer la requête WAN** : abandonne les requêtes TCP et les paquets ICMP.
- **Gestion à distance** : si cette option est activée, elle permet de gérer à distance le périphérique. Le port par défaut est 443. Il peut être remplacé par n'importe quel port défini par l'utilisateur. L'adresse est la suivante : https://<wan-ip>:<remote-management-port>

- **Intercommunication de multidiffusion** : permet aux messages de multidiffusion de transiter par le périphérique.
- **HTTPS** : le protocole S-HTTP (Secure HyperText Transfer Protocol) est un protocole de communication permettant d'assurer une communication sécurisée dans un réseau d'ordinateurs, avec un déploiement particulièrement étendu sur Internet.
- **VPN SSL** : autorise les connexions VPN SSL.
- **ALG SIP** : passerelle de la couche application qui augmente un pare-feu ou une traduction NAT. Elle permet de brancher des filtres de traversée NAT personnalisés dans la passerelle pour prendre en charge la traduction des adresses et des ports pour les protocoles de *contrôle/données* SIP.
- **UPnP** : le protocole Universal Plug and Play est un ensemble de protocoles réseau permettant aux périphériques réseau, comme les ordinateurs, les imprimantes, les passerelles Internet, les points d'accès Wi-Fi et les périphériques mobiles, de se détecter mutuellement sur le réseau et d'établir des services réseau opérationnels pour le partage des données et la communication.

Restriction de l'utilisation des fonctionnalités Web

Pour restreindre l'utilisation de fonctions Web, telles que **Java**, les **cookies**, **ActiveX** ou l'**accès aux serveurs proxy HTTP**, cochez cette case.

Pour autoriser *uniquement* les fonctions sélectionnées (Java, les cookies, ActiveX ou l'accès aux serveurs proxy HTTP) et restreindre l'utilisation de toutes les autres, cochez la case **Exception**.

Configuration des noms de domaines sécurisés

Pour ajouter des domaines sécurisés, cliquez sur **Ajouter**, puis saisissez le **nom de domaine**.

Pour modifier un domaine sécurisé, cliquez sur **Modifier**, puis changez le **nom de domaine**.

Règles d'accès

Les règles d'accès limitent l'accès au sous-réseau en autorisant ou en refusant l'accès au moyen de services ou de périphériques spécifiques identifiés par leur adresse IP.

Si vous devez ajouter ou modifier un service, cliquez sur **Gestion des services**. Cette fonction est décrite dans la section **Ajout ou modification d'un nom de service**.

Ajout d'une règle d'accès à la table des règles d'accès IPv4

Pour ajouter (ou modifier) une règle d'accès IPv4 :

ÉTAPE 1 Cliquez sur l'onglet **IPv4**.

ÉTAPE 2 Cliquez sur **Ajouter** (ou sélectionnez la ligne et cliquez sur **Modifier**).

ÉTAPE 3 Dans le menu déroulant, sélectionnez l'action puis **Autoriser** ou **Refuser** pour cette règle.

ÉTAPE 4 Sélectionnez un **service** dans le menu déroulant.

ÉTAPE 5 Sélectionnez **Consigner les paquets correspondant à cette règle** ou **Aucun journal**.

ÉTAPE 6 Sélectionnez l'**interface source** dans le menu déroulant.

ÉTAPE 7 Sélectionnez l'**adresse IP source** dans le menu déroulant. Si vous avez sélectionné **Individuelle**, saisissez l'adresse IP source. Si vous avez sélectionné **Plage**, saisissez la plage des adresses IP source.

ÉTAPE 8 Sélectionnez l'**adresse IP de destination** dans le menu déroulant. Si vous avez sélectionné **Individuelle**, saisissez l'adresse IP de destination. Si vous avez sélectionné **Plage**, saisissez la plage des adresses IP de destination.

ÉTAPE 9 Configurez **Planification** pour cette règle d'accès en sélectionnant la période. Sélectionnez **Toujours** pour que la règle d'accès soit appliquée 24 heures sur 24. Sélectionnez **Intervalle** pour définir une période, puis saisissez les heures et les minutes pendant lesquelles la règle d'accès sera appliquée dans les champs **De** et **À**. Par exemple, de *07:00* à *20:00*. La règle d'accès ne permet pas de définir deux intervalles de temps.

ÉTAPE 10 Sélectionnez les jours **Appliqué le** de la semaine.

ÉTAPE 11 Cliquez sur **Enregistrer**.

Ajout d'une règle d'accès à la table des règles d'accès IPv6

Pour ajouter (ou modifier) une règle d'accès IPv6 :

ÉTAPE 1 Cliquez sur l'onglet **IPv6**.

ÉTAPE 2 Cliquez sur **Ajouter** (ou sélectionnez la ligne et cliquez sur **Modifier**).

ÉTAPE 3 Dans le menu déroulant, sélectionnez l'action puis **Autoriser** ou **Refuser** pour cette règle.

ÉTAPE 4 Sélectionnez le **service** dans le menu déroulant.

ÉTAPE 5 Sélectionnez un **journal** dans le menu déroulant.

ÉTAPE 6 Sélectionnez l'**interface source** dans le menu déroulant.

ÉTAPE 7 Sélectionnez la **longueur du préfixe IP source** dans le menu déroulant. Si vous avez sélectionné **Individuel**, saisissez le préfixe IP source. Si vous avez sélectionné **Plage**, saisissez le préfixe IP de début et la longueur du préfixe.

ÉTAPE 8 Sélectionnez la **longueur du préfixe de destination** dans le menu déroulant. Si vous avez sélectionné **Individuel**, saisissez le préfixe IP de destination. Si vous avez sélectionné **Plage**, saisissez le préfixe IP de début et la longueur du préfixe.

ÉTAPE 9 Cliquez sur **Enregistrer**.

Filtre de contenu

Le filtre de contenu refuse les domaines spécifiés ainsi que des sites Web contenant des mots clés spécifiques. Le filtre de contenu autorise ou refuse les domaines spécifiés ainsi que des sites Web contenant des mots de passe spécifiques.

Bloquage des domaines interdits

Pour bloquer des domaines :

ÉTAPE 1 Sélectionnez **Bloquer les domaines interdits**.

ÉTAPE 2 Ajoutez (ou modifiez) le domaine dans la table **Domaines interdits**.

ÉTAPE 3 Définissez une période en saisissant les heures et les minutes pendant lesquelles la règle d'accès sera appliquée dans les champs **De** et **À**.

ÉTAPE 4 Sélectionnez les jours **Appliqué le** de la semaine.

ÉTAPE 5 Cliquez sur **Enregistrer**.

Blocage de sites Web par mots clés

Pour définir des mots clés bloquant des sites Web :

ÉTAPE 1 Sélectionnez **Bloquer les domaines interdits**.

ÉTAPE 2 Cliquez sur **Ajouter** (ou **Modifier**) dans la table **Blocage de sites Web par mots clés**.

ÉTAPE 3 Saisissez un mot clé dans la colonne **Mot clé**.

ÉTAPE 4 Cliquez sur **Enregistrer**.

Acceptation des domaines autorisés

Pour accepter un domaine :

ÉTAPE 1 Sélectionnez **Accepter les domaines autorisés**.

ÉTAPE 2 Cliquez sur **Ajouter** (ou **Modifier**) dans la table **Domaines autorisés**.

ÉTAPE 3 Saisissez un nom dans la colonne **Nom de domaine**.

ÉTAPE 4 Cliquez sur **Enregistrer**.

Planification

Les restrictions peuvent être planifiées pour une période précise, à des jours spécifiques.

Pour planifier l'heure et les jours :

ÉTAPE 1 Sélectionnez **Heure** dans le menu déroulant. Sélectionnez **Toujours** pour que la règle soit appliquée 24 heures sur 24. Sélectionnez **Intervalle** pour définir une période.

ÉTAPE 2 Si vous avez sélectionné Toujours à l'ÉTAPE 1, passez à l'ÉTAPE 4. Si vous avez sélectionné Intervalle, définissez une période en saisissant les heures et les minutes pendant lesquelles la règle d'accès sera appliquée dans les champs **De** et **À**. Par exemple, de *07:00* à *20:00*. Le filtre de contenu ne permet pas de définir deux intervalles de temps.

ÉTAPE 3 Cochez les jours **Appliqué le** de la semaine.

ÉTAPE 4 Cliquez sur **Enregistrer**.

8

VPN

Un réseau VPN (réseau privé virtuel) est une connexion entre deux points de terminaison situés dans différents réseaux, qui permet l'envoi sécurisé de données privées sur un réseau partagé ou public, comme Internet. Ce tunnel permet de créer un réseau privé capable d'envoyer des données de manière sécurisée, en faisant appel à des techniques d'authentification et de cryptage qui sont la norme dans l'industrie, afin de sécuriser les données envoyées.

Récapitulatif

Cette fonction affiche des informations générales relatives aux paramètres des tunnels VPN. Le périphérique prend en charge jusqu'à 100 tunnels. La plage d'adresses IP virtuelles est réservée aux utilisateurs EasyVPN ou aux clients VPN qui se connectent au périphérique lorsque l'option Configuration du mode (voir **Paramètres avancés des modes IKE avec clé prépartagée et IKE avec certificat**) est activée.

Pour définir une plage d'adresses IP à utiliser pour les tunnels VPN, cliquez sur **Modifier** et saisissez les paramètres suivants :

- **Début de la plage** et **Fin de la plage** : adresses IP de début et de fin utilisées pour les tunnels VPN.
- **Serveur DNS 1** et **Serveur DNS 2** : adresse IP facultative d'un serveur DNS. Si vous saisissez un deuxième serveur DNS, le périphérique utilise le premier serveur DNS pour répondre. Saisir un serveur DNS peut offrir un accès plus rapide qu'utiliser un serveur DNS attribué de manière dynamique. Utilisez le paramètre par défaut (0.0.0.0) pour choisir un serveur DNS attribué de manière dynamique.
- **Serveur WINS1** et **Serveur WINS2** : adresse IP facultative d'un serveur WINS. Le service WINS (Windows Internet Naming Service) résout les noms NetBIOS en adresses IP. Si vous ne connaissez pas l'adresse IP du serveur WINS, utilisez la valeur par défaut 0.0.0.0.

- **Nom de domaine 1** à **4** : si ce routeur dispose d'une adresse IP statique et d'un nom de domaine inscrit (ex. : *MyServer.MyDomain.com*), saisissez le **nom de domaine** à utiliser pour l'authentification. Un nom de domaine ne peut être utilisé que pour une seule connexion de tunnel.

L'option **État du tunnel VPN** affiche le nombre de **tunnels utilisés**, de **tunnels disponibles**, de **tunnels activés** et de **tunnels définis**.

Table des connexions d'états des tunnels

La table des connexions affiche les entrées créées dans **VPN** > **Passerelle à passerelle** et **VPN** > **Client-à-passerelle** :

- **N° du tunnel** : numéro d'identification de tunnel généré automatiquement.
- **Nom du tunnel :** nom de ce tunnel VPN : Bureau de Paris, Succursale de Lyon ou Service de Bordeaux, par exemple. Cette description sert uniquement de référence et ne doit pas obligatoirement correspondre au nom utilisé à l'autre extrémité du tunnel.
- **État** : état du tunnel VPN, *Connecté* ou *En attente de connexion.*
- **Phase2 Enc/Auth/Grp :** 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.
- **Groupe distant** : adresse IP et masque de sous-réseau du groupe distant.
- **Passerelle distante** : adresse IP de la passerelle distante.
- **Test du tunnel :** état du tunnel VPN.

Table des connexions d'états du VPN de groupe

La table des connexions affiche les entrées créées dans **VPN** > **Client-à-passerelle** :

- **Nom de groupe :** nom du tunnel VPN. Cette description sert uniquement de référence et ne doit pas obligatoirement correspondre au nom utilisé à l'autre extrémité du tunnel.
- **Tunnels** : nombre d'utilisateurs connectés au VPN de groupe.
- **Phase2 Enc/Auth/Grp :** 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.

- **Client distant** : adresse IP et masque de sous-réseau du client distant.
- **Détails** : adresse IP de la passerelle distante.
- **Test du tunnel :** état du tunnel VPN.

Passerelle à passerelle

Dans un VPN de site à site ou de passerelle à passerelle, un routeur local situé dans un bureau se connecte à un routeur distant via un tunnel VPN. Les périphériques client ont accès aux ressources réseau comme s'ils se trouvaient tous sur le même site. Ce modèle peut servir à plusieurs utilisateurs situés dans un bureau 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. Par ailleurs, si l'un des routeurs possède uniquement une adresse IP dynamique, vous pouvez effectuer l'authentification à l'aide d'une adresse e-mail afin d'établir la connexion.

Les deux extrémités du tunnel ne doivent pas se trouver sur le même sous-réseau. Si, par exemple, le site A LAN utilise le masque de sous-réseau 192.168.1.x/24, le site B peut utiliser le masque 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*. Lors de la configuration de 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*.

Ajouter un nouveau tunnel

Saisissez les paramètres pour un tunnel :

- **N° du tunnel :** numéro d'identification du tunnel.
- **Nom de tunnel :** nom de ce tunnel VPN : Bureau de Paris, Succursale de Lyon ou Service de Bordeaux, par exemple. La description vous sert de référence. Il n'est pas nécessaire qu'elle corresponde au nom utilisé à l'autre extrémité du tunnel.
- **Interface :** port WAN à utiliser pour ce tunnel.
- **Mode de génération de clés** : identifie la sécurité du tunnel : Manuel, IKE avec clé prépartagée, IKE avec certificat.

- **Activer :** cochez ou décochez cette case pour activer ou désactiver le tunnel VPN. Par défaut, le tunnel est activé.

Configuration du groupe local

Saisissez les paramètres de configuration du groupe local pour ce routeur. (Reproduisez ces paramètres lors de la configuration du tunnel VPN sur l'autre routeur.)

REMARQUE Toutes les options sont documentées, mais seules les options liées au paramètre sélectionné s'affichent.

Mode de génération de clés = Manuel ou IKE avec clé prépartagée

- **Type de passerelle de sécurité locale :** méthode à utiliser pour identifier le routeur et établir le tunnel VPN. Le paramètre Passerelle de sécurité locale est sur ce routeur, tandis que le paramètre Passerelle de sécurité distante est sur l'autre routeur. Au moins un des routeurs doit posséder une adresse IP statique ou un nom d'hôte DNS afin d'établir une connexion.
  - **IP uniquement :** ce routeur dispose d'une adresse IP statique du réseau WAN. L'adresse IP du réseau WAN s'affiche automatiquement.
  - **IP et certificat :** ce routeur dispose d'une adresse IP statique du réseau WAN qui s'affiche automatiquement. Cette option n'est disponible que lorsque l'option IKE avec certificat est sélectionnée.
  - **Authentification par IP et nom de domaine (FQDN) :** ce périphérique dispose d'une adresse IP statique et d'un nom de domaine inscrit comme *MyServer.MyDomain.com*. Saisissez également le **nom de domaine** à utiliser pour l'authentification. Le nom de domaine ne peut être utilisé que pour une seule connexion de tunnel.
  - **Authentification par IP et adresse e-mail (Utilisateur_FQDN) :** ce périphérique dispose d'une adresse IP statique et d'une adresse e-mail pour l'authentification. L'adresse IP du réseau WAN s'affiche automatiquement. Saisissez l'**adresse e-mail** à utiliser pour l'authentification.
  - **Authentification par IP dynamique et nom de domaine (FQDN) :** ce routeur dispose d'une adresse IP dynamique et d'un nom d'hôte DNS dynamique inscrit (disponible auprès de fournisseurs, comme DynDNS.com). Saisissez le **nom de domaine** à utiliser pour l'authentification. Le nom de domaine ne peut être utilisé que pour une seule connexion de tunnel.

- **Authentification par IP dynamique et adresse e-mail (Utilisateur_FQDN) :** ce routeur dispose d'une adresse IP dynamique, mais pas d'un nom d'hôte DNS dynamique. Saisissez une **adresse e-mail** à utiliser pour l'authentification.

  Si les routeurs disposent tous deux d'adresses IP dynamiques (par exemple, dans le cas de connexions PPPoE), ne choisissez pas l'option **IP dynamique et adresse e-mail** pour les deux passerelles. Pour la passerelle distante, choisissez **Adresse IP** et **Adresse IP par DNS résolu**.

Mode de génération de clés = IKE avec certificat

- **Type de passerelle de sécurité locale :** ressources LAN pouvant utiliser ce tunnel. La seule option possible est **IP et certificat**.
  - **Adresse IP :** affiche l'adresse IP du réseau WAN du périphérique.
- **Certificat local** : certificats disponibles dans la fenêtre Gestion des certificats > **Mon certificat**. Sélectionnez le certificat dans le menu déroulant.

  Générateur automatique affiche la fenêtre **Générateur de certificat**.

  Importer un certificat affiche la fenêtre **Mon certificat**.
- **Type de groupe de sécurité local** : permet la sélection d'une seule adresse **IP**, d'un **masque de sous-réseau** ou d'une **plage** (d'adresse) **IP** dans un sous-réseau.
  - **Adresse IP :** indiquez un périphérique pouvant utiliser ce tunnel. Saisissez l'**adresse IP** du périphérique.
  - **Masque de sous-réseau :** autorisez tous les périphériques d'un sous-réseau donné à utiliser le tunnel VPN. Saisissez l'**adresse IP** du sous-réseau et le **masque de sous-réseau**.
  - **IP de début** et **IP de fin** (Plage IP) : plage des périphériques que le tunnel VPN peut utiliser. Saisissez la première adresse IP dans **IP de début** et l'adresse IP de fin dans **IP de fin**.

Configuration du groupe distant

Saisissez les paramètres de configuration du groupe distant pour ce routeur :

- **Type de passerelle de sécurité distante :** méthode à utiliser pour identifier le routeur et établir le tunnel VPN. La passerelle de sécurité distante correspond à l'autre routeur. Au moins un des routeurs doit posséder une adresse IP statique ou un nom d'hôte DNS dynamique afin qu'une connexion puisse être établie.
  - **IP uniquement :** adresse IP statoque du réseau WAN. Si vous connaissez l'adresse IP du routeur VPN distant, choisissez **Adresse IP** puis saisissez l'adresse. Si vous ne connaissez pas l'adresse IP du routeur VPN distant, choisissez **Adresse IP par DNS résolu** puis saisissez le nom de domaine du routeur. Un routeur Cisco peut obtenir l'adresse IP d'un périphérique VPN distant grâce au paramètre Par DNS résolu.
  - **Authentification par IP et nom de domaine (FQDN) :** ce routeur dispose d'une adresse IP statique et d'un nom de domaine inscrit comme *MyServer.MyDomain.com*. Si vous connaissez l'adresse IP du routeur VPN distant, choisissez **Adresse IP** puis saisissez l'adresse. Si vous ne connaissez pas l'adresse IP du routeur VPN distant, choisissez **Adresse IP par DNS résolu** puis saisissez le nom de domaine du routeur. Un routeur Cisco peut obtenir l'adresse IP d'un périphérique VPN distant grâce au paramètre Par DNS résolu.
  - **Authentification par IP et adresse e-mail (Utilisateur_FQDN) :** ce routeur dispose d'une adresse IP statique et d'une adresse e-mail pour l'authentification. Si vous connaissez l'adresse IP du routeur VPN distant, choisissez **Adresse IP** puis saisissez l'adresse IP. Si vous ne connaissez pas l'adresse IP du routeur VPN distant, choisissez **Adresse IP par DNS résolu** puis saisissez le vrai nom de domaine du routeur. Un routeur Cisco peut obtenir l'adresse IP d'un périphérique VPN distant grâce au paramètre Par DNS résolu.
  - **Authentification par IP dynamique et nom de domaine (FQDN) :** ce routeur dispose d'une adresse IP dynamique et d'un nom d'hôte DNS dynamique inscrit (disponible auprès de fournisseurs, comme DynDNS.com). Saisissez le **nom de domaine** à utiliser pour l'authentification. Le nom de domaine ne peut être utilisé que pour une seule connexion de tunnel.
  - **Authentification par IP dynamique et adresse e-mail (Utilisateur_FQDN) :** ce routeur dispose d'une adresse IP dynamique, mais pas d'un nom d'hôte DNS dynamique. Saisissez une **adresse e-mail** à utiliser pour l'authentification.
    Si les routeurs disposent tous deux d'adresses IP dynamiques (par exemple, dans le cas de connexions PPPoE), *ne choisissez pas* l'option **IP dynamique et adresse e-mail** pour les deux passerelles. Pour la passerelle distante, choisissez **Adresse IP** ou **Adresse IP par DNS résolu**.

- **Type de groupe de sécurité local :** ressources LAN pouvant utiliser ce tunnel. Le paramètre Local Security Group correspond à celui des ressources LAN de ce routeur, tandis que le paramètre Remote Security Group correspond aux ressources LAN de l'autre routeur.
  - **Adresse IP :** indiquez un périphérique pouvant utiliser ce tunnel. Saisissez l'**adresse IP** du périphérique.
  - **Masque de sous-réseau :** autorisez tous les périphériques d'un sous-réseau donné à utiliser le tunnel VPN. Saisissez l'**adresse IP** du sous-réseau et le **masque de sous-réseau**.
  - **Plage IP :** plage de périphériques pouvant utiliser le tunnel VPN. Saisissez la première adresse IP dans **IP de début** et l'adresse IP de fin dans **IP de fin**.

Configuration IPSec

Afin que le cryptage réussisse, les deux extrémités du tunnel VPN doivent être configurées avec les mêmes méthodes de cryptage, de décryptage et d'authentification. Saisissez exactement les mêmes paramètres sur les deux routeurs.

Saisissez les paramètres des phases 1 et 2. La phase 1 consiste à établir les clés prépartagées afin de créer un canal de communication authentifié et sécurisé. Lors de la phase 2, les homologues IKE utilisent le canal sécurisé pour négocier les associations de sécurité pour le compte d'autres services, tels qu'IPsec. Veillez à saisir les mêmes paramètres lors de la configuration de l'autre routeur pour ce tunnel.

- **Phase 1 / Phase 2 - Groupe DH :** DH (Diffie-Hellman) est un protocole d'échange de clés. On distingue trois groupes de longueurs de clés principales : Groupe 1 - 768 bits, Groupe 2 - 1 024 bits et Groupe 5 - 1 536 bits. Si vous souhaitez un débit élevé, moyennant un niveau de sécurité inférieur, choisissez **Groupe 1**. Si vous souhaitez un niveau de sécurité supérieur, moyennant un débit inférieur, choisissez **Groupe 5**. Par défaut, l'option Groupe 1 est sélectionnée.
- **Phase 1/Phase 2 - Cryptage :** méthode de cryptage pour cette phase : DES, 3DES, AES-128, AES-192 ou AES-256. La méthode de cryptage détermine la longueur de clé utilisée pour crypter et décrypter les paquets ESP. Il est recommandé de choisir AES-256, car cette méthode est plus sûre.
- **Phase 1/Phase 2 - Authentification :** méthode d'authentification pour cette phase : MD5 ou SHA1. La méthode d'authentification détermine la manière dont les paquets d'en-tête ESP (Encapsulating Security Payload) sont validés. MD5 est un algorithme de hachage unidirectionnel qui produit une assimilation 128 bits. SHA1 est un algorithme de hachage unidirectionnel qui produit une assimilation 160 bits. SHA1 est recommandé, car il est plus sûr. Assurez-vous que les deux extrémités du tunnel VPN utilisent la même méthode d'authentification.
- **Phase 1 / Phase 2 Durée de vie de l'association de sécurité :** durée pendant laquelle le tunnel VPN est actif dans cette phase. La valeur par défaut de la phase 1 est de 28800 secondes. La valeur par défaut de la phase 2 est de 3600 secondes.

- **Confidentialité de transmission parfaite :** si la fonction Confidentialité de transmission parfaite est activée, la négociation IKE de phase 2 génère de nouvelles clés destinées au cryptage et à l'authentification du trafic IP. Les pirates informatiques lançant des attaques en force, dans le but d'obtenir les clés de cryptage, ne sont ainsi pas en mesure d'obtenir les futures clés IPSec. Cochez ou décochez cette case pour activer ou désactiver cette fonction. L'activation de cette fonction est recommandée.
- **Clé prépartagée :** clé prépartagée à utiliser pour l'authentification de l'homologue IKE distant. Vous pouvez saisir jusqu'à 30 valeurs hexadécimales et caractères (présents sur les claviers standard). Exemple : My_@123 ou 4d795f40313233 (' ' " \ ne sont pas pris en charge). Les deux extrémités du tunnel VPN doivent utiliser la même clé prépartagée. Nous vous recommandons vivement de modifier régulièrement la clé prépartagée afin d'optimiser la sécurité du VPN.
- **Complexité de clé prépartagée minimale :** cochez la case **Activer** pour activer l'option Mesure de la fiabilité de la clé prépartagée.
- **Mesure de la fiabilité de la clé prépartagée :** si vous activez l'option Complexité de clé prépartagée minimale, cet indicateur vous informe sur le niveau de sécurité de la clé prépartagée. Lorsque vous saisissez une clé prépartagée, des barres colorées apparaissent. La palette de couleurs s'étend du rouge (faible) au vert (élevé), en passant par le jaune (acceptable).

CONSEIL Saisissez une clé prépartagée complexe contenant plus de huit caractères et comprenant des minuscules, des majuscules, des chiffres et des symboles tels que -*^+=.

Paramètres avancés des modes IKE avec clé prépartagée et IKE avec certificat

Pour la plupart des utilisateurs, les paramètres de base suffisent. Les utilisateurs expérimentés peuvent afficher les paramètres avancés, en cliquant sur **Avancés**. Si vous modifiez les paramètres avancés sur un routeur, assurez-vous de faire de même sur l'autre routeur.

- **Mode agressif :** deux modes de négociation des associations de sécurité IKE sont possibles : Mode principal et Mode agressif. Si la sécurité du réseau est prioritaire, nous vous recommandons de choisir le mode principal. Si le débit du réseau est prioritaire, nous vous recommandons de choisir le mode agressif. Cochez cette case pour activer le mode agressif ou décochez-la pour utiliser le mode principal.

  Si le paramètre Type de passerelle de sécurité distante est réglé sur l'un des types *IP dynamique*, le mode agressif est obligatoire. La case est cochée automatiquement et il n'est pas possible de la décocher.

- **Compresser (prend en charge le protocole de compression de la charge utile IP (IP Comp)) :** protocole réduisant la taille des datagrammes IP. Cochez cette case pour permettre au routeur de proposer la compression lors de l'initiation de connexions. Si l'entité qui répond refuse cette proposition, le routeur ne procède pas à la compression. Lorsque le routeur est le répondeur, il accepte la compression, même si l'option n'est pas activée. Si vous activez cette option sur ce routeur, activez-la également sur le routeur situé à l'autre extrémité du tunnel.

- **Maintenir actif :** essaie de rétablir une connexion VPN si elle a été perdue.

- **Algorithme de hachage avec en-tête d'authentification :** le protocole d'en-tête d'authentification décrit le format des paquets et les normes par défaut de la structure des paquets. L'utilisation du protocole d'en-tête d'authentification en tant que protocole de sécurité assure une protection étendue jusqu'à l'en-tête IP afin de vérifier l'intégrité du paquet complet. Cochez la case pour utiliser cette fonction et sélectionnez une méthode d'authentification : MD5 ou SHA1. MD5 produit une assimilation de 128 bits pour authentifier les données de paquets. SHA1 produit une assimilation de 160 bits pour authentifier les données de paquets. Le même algorithme doit être utilisé aux deux extrémités du tunnel.

- **Diffusion NetBIOS :** messages de diffusion utilisés dans le cadre de la résolution de noms, sur le réseau Windows, pour identifier les ressources tels que les ordinateurs, les imprimantes et les serveurs de fichiers. Ces messages sont utilisés par certaines applications logicielles et par certaines fonctionnalités Windows, dont le voisinage réseau. Le trafic de diffusion LAN n'est généralement pas transféré via un tunnel VPN. Toutefois, vous pouvez cocher cette case pour permettre la rediffusion des NetBIOS d'une extrémité du tunnel à l'autre.

- **Traversée NAT :** grâce à la traduction d'adresses réseau (NAT), les utilisateurs possédant des adresses LAN privées peuvent accéder aux ressources Internet en utilisant une adresse IP acheminée publiquement en tant qu'adresse source. Toutefois, concernant le trafic interne, la passerelle NAT ne dispose d'aucune méthode automatique de traduction de l'adresse IP publique vers une destination spécifique du réseau LAN privé. Ce problème empêche le bon déroulement des échanges IPsec. Si votre routeur VPN se trouve derrière une passerelle NAT, cochez cette case pour activer la traversée NAT. Vous devez utiliser le même paramètre sur les deux extrémités du tunnel.
- **Détection d'homologue indisponible :** envoie régulièrement des messages HELLO/ACK (bonjour/accusé de réception) afin de vérifier l'état du tunnel VPN. Cette option doit être activée à chaque extrémité du tunnel VPN. Indiquez l'intervalle souhaité entre les messages HELLO/ACK (bonjour/accusé de réception) dans le champ **Intervalle**.
- **Authentification étendue** : utilise un nom d'utilisateur et un mot de passe d'un hôte IPsec pour authentifier les clients VPN ou utilise la base de données utilisateur trouvé dans la gestion des utilisateurs. L'hôte IPsec et l'appareil en périphérie de réseau doivent activer l'authentification étendue. Pour utiliser l'**hôte IPsec**, cliquez sur la case d'option puis saisissez le **nom d'utilisateur** et le **mot de passe**. Pour utiliser l'**appareil en périphérie de réseau**, cliquez sur la case d'option puis sélectionnez la base de données dans le menu déroulant. Pour ajouter ou modifier une base de données, cliquez sur **Ajouter/Modifier** pour afficher la fenêtre Gestion des utilisateurs.
- **Sauvegarde du tunnel :** lorsque la fonction DPD détecte que l'homologue distant est indisponible, cette fonction permet au routeur de rétablir le tunnel VPN à l'aide d'une autre adresse IP de l'homologue distant ou d'une autre interface du réseau WAN local. Cochez la case pour activer cette fonction et définissez les paramètres suivants. Cette fonction est disponible uniquement si la fonction Détection d'homologue indisponible est activée.
  - **Adresse IP de sauvegarde à distance :** autre adresse IP de l'homologue distant, ou saisissez à nouveau l'adresse IP du réseau WAN déjà indiquée pour la passerelle distante.
  - **Interface locale :** interface WAN à utiliser pour rétablir la connexion.
  - **Temps d'inactivité de sauvegarde du tunnel VPN :** au moment du démarrage du routeur, si le tunnel principal n'est pas connecté dans l'intervalle spécifié, le tunnel de sauvegarde est utilisé. L'intervalle d'inactivité par défaut est de 30 secondes.

- **DNS séparé :** envoie certaines des requêtes DNS à un serveur DNS donné et d'autres requêtes DNS à un autre serveur DNS, en fonction des noms de domaine spécifiés. Lorsque le routeur reçoit une requête de résolution d'adresse de la part du client, le routeur examine le nom de domaine. S'il correspond à l'un des noms de domaine des paramètres DNS séparé, il transmet la requête au serveur DNS spécifié. Dans le cas contraire, la requête est transmise au serveur DNS spécifié dans les paramètres d'interface WAN.

  Serveur DNS 1 et **Serveur DNS 2 :** adresse IP du serveur DNS à utiliser pour les domaines spécifiés. Vous pouvez également indiquer un serveur DNS secondaire dans le champ **Serveur DNS 2**.

  Nom de domaine 1 à **Nom de domaine 4 :** indiquez les noms de domaine de ces serveurs DNS. Les requêtes destinées à ces domaines sont transmises aux serveurs DNS spécifiés.

Client-à-passerelle

Cette fonction crée 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 tel que TheGreenBow.

Configurez un tunnel VPN pour un seul utilisateur distant, un VPN de groupe pour plusieurs utilisateurs distants, ou un Easy VPN :

- **Tunnel :** crée un tunnel pour un seul utilisateur distant. Le numéro du tunnel est généré automatiquement.
- **VPN de groupe :** crée un tunnel pour un groupe d'utilisateurs et élimine la nécessité de configurer un à un les utilisateurs. Tous les utilisateurs distants peuvent utiliser la même clé prépartagée pour se connecter au périphérique, dans la limite du nombre maximal de tunnels pouvant être pris en charge. Le routeur prend en charge jusqu'à deux VPN de groupe. Le numéro du groupe est généré automatiquement.
- **Easy VPN** : permet aux utilisateurs de connecter ce périphérique à l'aide de l'utilitaire Cisco VPN Client, également connu sous le nom de *Cisco Easy VPN Client* (disponible sur le CD-ROM du produit) :
  - La version 5.0.07 prend en charge Windows 7 (32 bits et 64 bits), Windows Vista (32 bits et 64 bits) et Windows XP (32 bits).
  - La version 4.9 prend en charge les systèmes d'exploitation Mac OS X 10.4 et 10.5.
  - La version 4.8 prend en charge le système d'exploitation Linux basé sur Intel.

Pour configurer Easy VPN, choisissez un mot de passe de groupe sur cette page et définissez un nom d'utilisateur et un mot de passe pour chaque utilisateur Cisco VPN Client dans la table de gestion des utilisateurs de la section **Gestion des utilisateurs**. Lors de l'ajout d'un utilisateur, le groupe Non attribué doit être sélectionné. Les autres groupes sont utilisés pour VPN SSL.

Configuration d'un tunnel ou d'un VPN de groupe

Saisissez les informations suivantes :

- **Nom du tunnel :** nom descriptif du tunnel. Si celui-ci est destiné à un seul utilisateur, vous pouvez saisir le nom d'utilisateur ou l'emplacement. Pour un VPN de groupe, vous pouvez identifier le rôle du groupe au sein de l'entreprise ou son emplacement. Cette description sert uniquement de référence et ne doit pas obligatoirement correspondre au nom utilisé à l'autre extrémité du tunnel.
- **Interface :** port WAN.
- **Mode de génération de clés :** choisissez une méthode de gestion des clés :
  - **Manuelle :** générez vous-même la clé, mais n'activez pas la négociation de clé. La gestion manuelle des clés est utilisée dans les petits environnements statiques ou à des fins de dépannage. Saisissez les paramètres souhaités.
  - **IKE** (Internet Key Exchange) **avec clé prépartagée :** utilisez le protocole IKE (Internet Key Exchange) pour configurer une association de sécurité destinée à votre tunnel. Ce paramètre est recommandé. Si vous avez sélectionné **VPN de groupe**, il s'agit de la seule option disponible.
  - **IKE avec certificat** : utilise une clé prépartagée pour authentifier un homologue IKE distant.
- **Activer :** cochez cette case pour activer ce réseau VPN.

Configuration d'Easy VPN

Saisissez les informations suivantes :

- **Nom :** nom descriptif du tunnel. Si celui-ci est destiné à un seul utilisateur, vous pouvez saisir le nom d'utilisateur ou l'emplacement. Cette description sert uniquement de référence et ne doit pas obligatoirement correspondre au nom utilisé à l'autre extrémité du tunnel.
- **Complexité de mot de passe minimale** : lorsque cette option est activée, les exigences minimales en termes de mot de passe sont les suivantes :
  - Longueur : huit caractères.
  - Doit être différent du nom d'utilisateur.
  - Doit être différent du mot de passe actuel.

  - Doit contenir des caractères provenant d'au moins 3 des catégories suivantes : lettres majuscules, lettres minuscules, chiffres et caractères spéciaux que l'on trouve sur un clavier standard (' ' " \ ne sont pas pris en charge).

- **Mot de passe** : mot de passe Easy VPN.
- **Mesure de la fiabilité du mot de passe :** si l'option Complexité de mot de passe minimale est activée, cette option indique le niveau de fiabilité du mot de passe, en fonction des règles de complexité définies. L'échelle va du rouge (inacceptable) au vert (élevé), en passant par le jaune (acceptable).
- **Interface :** port WAN à utiliser pour ce tunnel.
- **Activer :** cochez ou décochez cette case pour activer ou désactiver le tunnel VPN. Par défaut, le tunnel est activé.
- **Mode de tunnelisation** : le mode **Tunnel fractionné** permet l'envoi direct et sans cryptage du trafic destiné à Internet sur Internet. Le mode **Tunnel complet** envoie tout le trafic vers le périphérique d'extrémité, où il est ensuite acheminé vers les ressources de destination (en supprimant le réseau de l'entreprise du chemin d'accès Web).
- **Adresse IP** : adresse IP attribuée à l'interface VPN.
- **Masque de sous-réseau** : masque de sous-réseau.
- **Authentification étendue** : utilise un nom d'utilisateur et un mot de passe d'un hôte IPsec pour authentifier les clients VPN ou utilise la base de données utilisateur trouvé dans la gestion des utilisateurs. Pour utiliser l'**hôte IPsec**, cliquez sur la case d'option puis saisissez le **nom d'utilisateur** et le **mot de passe**. Pour utiliser l'**appareil en périphérie de réseau**, cliquez sur la case d'option puis sélectionnez la base de données dans le menu déroulant. Pour ajouter ou modifier une base de données, cliquez sur **Ajouter/Modifier** pour afficher la fenêtre Gestion des utilisateurs.

Configuration du groupe local

Saisissez les informations suivantes :

- **Type de passerelle de sécurité locale :** méthode à utiliser pour identifier le routeur et établir le tunnel VPN. La passerelle de sécurité distante correspond à l'autre routeur. Au moins un des routeurs doit posséder une adresse IP statique ou un nom d'hôte DNS dynamique afin qu'une connexion puisse être établie.
  - **IP uniquement :** adresse IP statique du réseau WAN. Si vous connaissez l'adresse IP du routeur VPN distant, choisissez **Adresse IP** puis saisissez l'adresse. Si vous ne connaissez pas l'adresse IP du routeur VPN distant, choisissez **Adresse IP par DNS résolu** puis saisissez le nom de domaine du routeur. Un routeur Cisco peut obtenir l'adresse IP d'un périphérique VPN distant grâce au paramètre Par DNS résolu.

- **Authentification par IP et nom de domaine (FQDN) :** ce périphérique dispose d'une adresse IP statique et d'un nom de domaine inscrit comme *MyServer.MyDomain.com*. Si vous connaissez l'adresse IP du routeur VPN distant, choisissez **Adresse IP** puis saisissez l'adresse. Si vous ne connaissez pas l'adresse IP du routeur VPN distant, choisissez **Adresse IP par DNS résolu** puis saisissez le nom de domaine du routeur. Un routeur Cisco peut obtenir l'adresse IP d'un périphérique VPN distant grâce au paramètre Par DNS résolu.
- **Authentification par IP et adresse e-mail (Utilisateur_FQDN) :** ce périphérique dispose d'une adresse IP statique et d'une adresse e-mail pour l'authentification. Si vous connaissez l'adresse IP du routeur VPN distant, choisissez **Adresse IP** puis saisissez l'adresse IP. Si vous ne connaissez pas l'adresse IP du routeur VPN distant, choisissez **Adresse IP par DNS résolu** puis saisissez le vrai nom de domaine du routeur. Un routeur Cisco peut obtenir l'adresse IP d'un périphérique VPN distant grâce au paramètre Par DNS résolu.
- **Authentification par IP dynamique et nom de domaine (FQDN) :** ce routeur dispose d'une adresse IP dynamique et d'un nom d'hôte DNS dynamique inscrit (disponible auprès de fournisseurs, comme DynDNS.com). Saisissez le **nom de domaine** à utiliser pour l'authentification. Le nom de domaine ne peut être utilisé que pour une seule connexion de tunnel.
- **Authentification par IP dynamique et adresse e-mail (Utilisateur_FQDN) :** ce routeur dispose d'une adresse IP dynamique, mais pas d'un nom d'hôte DNS dynamique. Saisissez une **adresse e-mail** à utiliser pour l'authentification.

  Si les routeurs disposent tous deux d'adresses IP dynamiques (par exemple, dans le cas de connexions PPPoE), ne choisissez pas l'option IP dynamique et adresse e-mail pour les deux passerelles. Pour la passerelle distante, choisissez **Adresse IP** et **Adresse IP par DNS résolu**.

- **Type de groupe de sécurité local :** ressources LAN pouvant utiliser ce tunnel.
  - **Adresse IP :** choisissez cette option pour permettre à un seul périphérique LAN d'accéder au tunnel VPN. Saisissez ensuite l'adresse IP de l'ordinateur. Seul ce périphérique peut utiliser ce tunnel VPN.
  - **Sous-réseau :** choisissez cette option (option par défaut) pour autoriser tous les périphériques d'un sous-réseau donné à accéder au tunnel VPN. Saisissez ensuite l'adresse IP de sous-réseau et le masque.
  - **Plage IP :** choisissez cette option pour qu'une plage donnée de périphériques puisse accéder au tunnel VPN. Définissez ensuite la plage d'adresses IP souhaitée. Pour ce faire, saisissez la première adresse de la plage dans le champ **IP de début** et la dernière adresse de la plage dans le champ **IP de fin**.

- **Nom de domaine :** si vous souhaitez utiliser l'authentification par nom de domaine, saisissez le nom de domaine.
- **E-mail :** si vous souhaitez utiliser l'authentification par e-mail, saisissez l'adresse e-mail.

Configuration du client distant pour un seul utilisateur

Spécifiez la méthode à utiliser pour identifier le client afin d'établir le tunnel VPN. Les options suivantes sont disponibles pour un VPN mono-utilisateur ou de type *Tunnel*.

- **IP uniquement :**le client VPN distant dispose d'une adresse IP statique du réseau WAN. Si vous connaissez l'adresse IP du client, choisissez l'option **Adresse IP** puis saisissez l'adresse. Si vous ne connaissez pas l'adresse IP du client, choisissez **Adresse IP par DNS résolu** puis saisissez le nom de domaine du client sur Internet. Le routeur obtient l'adresse IP du client VPN distant grâce au paramètre DNS résolu. L'adresse IP du client VPN distant s'affiche ensuite dans la section État du VPN de la page Récapitulatif.
- **Authentification par IP et nom de domaine (FQDN) :** le client dispose d'une adresse IP statique et d'un nom de domaine. Saisissez également un **nom de domaine** à utiliser pour l'authentification. Le nom de domaine ne peut être utilisé que pour une seule connexion de tunnel.

  Si vous connaissez l'adresse IP du client VPN distant, choisissez **Adresse IP**, puis saisissez l'adresse. Si vous ne connaissez pas l'adresse IP du client VPN distant, choisissez **Adresse IP par DNS résolu** puis saisissez le vrai nom de domaine du client sur Internet. Le routeur obtient l'adresse IP du client VPN distant grâce au paramètre DNS résolu. L'adresse IP du client VPN distant s'affiche ensuite dans la section État du VPN de la page Récapitulatif.
- **Authentification par IP et adresse e-mail (Utilisateur_FQDN) :** le client dispose d'une adresse IP statique et d'une adresse e-mail pour l'authentification. L'adresse IP actuelle du réseau WAN s'affiche automatiquement. Saisissez les **adresses e-mail** à utiliser pour l'authentification.

  Si vous connaissez l'adresse IP du client VPN distant, choisissez **Adresse IP**, puis saisissez l'adresse. Si vous ne connaissez pas l'adresse IP du client VPN distant, choisissez **Adresse IP par DNS résolu** puis saisissez le vrai nom de domaine du client sur Internet. Le périphérique obtient l'adresse IP du client VPN distant grâce au paramètre DNS résolu. L'adresse IP du périphérique VPN distant s'affiche ensuite dans la section État du VPN de la page Récapitulatif.
- **Authentification par IP dynamique et nom de domaine (FQDN) :** le client dispose d'une adresse IP dynamique et d'un nom d'hôte DNS dynamique inscrit (disponible auprès de fournisseurs, comme DynDNS.com). Saisissez le **nom de domaine** à utiliser pour l'authentification. Le nom de domaine ne peut être utilisé que pour une seule connexion de tunnel.

- **Authentification par IP dynamique et adresse e-mail (Utilisateur_FQDN) :** ce client dispose d'une adresse IP dynamique, mais pas d'un nom d'hôte DNS dynamique. Saisissez les **adresses e-mail** à utiliser pour l'authentification.

Configuration du client distant pour un groupe

Spécifiez la méthode à utiliser pour identifier les clients afin d'établir le tunnel VPN. Les options suivantes sont disponibles pour un VPN de groupe :

- **Authentification par nom de domaine (FQDN) :** identifie le client par son nom de domaine. Saisissez le **nom de domaine** à utiliser pour l'authentification. Le nom de domaine ne peut être utilisé que pour une seule connexion de tunnel.
- **Authentification par adresse e-mail (Utilisateur_FQDN) :** identifie le client par une adresse e-mail pour l'authentification. Saisissez l'adresse dans les champs appropriés.
- **Microsoft XP/2000 VPN Client :** le logiciel client est le client VPN Microsoft XP/2000 intégré.

Configuration IPSec

Afin que le cryptage réussisse, les deux extrémités du tunnel VPN doivent être configurées avec les mêmes méthodes de cryptage, de décryptage et d'authentification. Saisissez exactement les mêmes paramètres sur les deux routeurs.

Saisissez les paramètres des phases 1 et 2. La phase 1 consiste à établir les clés prépartagées afin de créer un canal de communication authentifié et sécurisé. Lors de la phase 2, les homologues IKE utilisent le canal sécurisé pour négocier les associations de sécurité pour le compte d'autres services, tels qu'IPsec. Veillez à saisir les mêmes paramètres lors de la configuration de l'autre routeur pour ce tunnel.

- **Phase 1 / Phase 2 - Groupe DH :** DH (Diffie-Hellman) est un protocole d'échange de clés. On distingue trois groupes de longueurs de clés principales : Groupe 1 - 768 bits, Groupe 2 - 1 024 bits et Groupe 5 - 1 536 bits. Si vous souhaitez un débit élevé, moyennant un niveau de sécurité inférieur, choisissez **Groupe 1**. Si vous souhaitez un niveau de sécurité supérieur, moyennant un débit inférieur, choisissez **Groupe 5**. Par défaut, l'option Groupe 1 est sélectionnée.
- **Phase 1/Phase 2 - Cryptage :** méthode de cryptage pour cette phase : DES, 3DES, AES-128, AES-192 ou AES-256. La méthode de cryptage détermine la longueur de clé utilisée pour crypter et décrypter les paquets ESP. Il est recommandé de choisir AES-256, car cette méthode est plus sûre.

- **Phase 1/Phase 2 - Authentification :** méthode d'authentification pour cette phase : MD5 ou SHA1. La méthode d'authentification détermine la manière dont les paquets d'en-tête ESP (Encapsulating Security Payload) sont validés. MD5 est un algorithme de hachage unidirectionnel qui produit une assimilation 128 bits. SHA1 est un algorithme de hachage unidirectionnel qui produit une assimilation 160 bits. SHA1 est recommandé, car il est plus sûr. Assurez-vous que les deux extrémités du tunnel VPN utilisent la même méthode d'authentification.
- **Phase 1 / Phase 2 Durée de vie de l'association de sécurité :** durée pendant laquelle le tunnel VPN est actif dans cette phase. La valeur par défaut de la phase 1 est de 28800 secondes. La valeur par défaut de la phase 2 est de 3600 secondes.
- **Confidentialité de transmission parfaite :** si la fonction Confidentialité de transmission parfaite est activée, la négociation IKE de phase 2 génère de nouvelles clés destinées au cryptage et à l'authentification du trafic IP. Les pirates informatiques lançant des attaques en force, dans le but d'obtenir les clés de cryptage, ne sont ainsi pas en mesure d'obtenir les futures clés IPSec. Cochez ou décochez cette case pour activer ou désactiver cette fonction. L'activation de cette fonction est recommandée.
- **Complexité de clé prépartagée minimale :** cochez la case **Activer** pour activer l'option Mesure de la fiabilité de la clé prépartagée.
- **Clé prépartagée :** clé prépartagée à utiliser pour l'authentification de l'homologue IKE distant. Vous pouvez saisir jusqu'à 30 valeurs hexadécimales et caractères (présents sur les claviers standard). Exemple : My_@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 d'optimiser la sécurité du VPN.
- **Mesure de la fiabilité de la clé prépartagée :** si vous activez l'option Complexité de clé prépartagée minimale, cet indicateur vous informe sur le niveau de sécurité de la clé prépartagée. Lorsque vous saisissez une clé prépartagée, des barres colorées apparaissent. La palette de couleurs s'étend du rouge (faible) au vert (élevé), en passant par le jaune (acceptable).

CONSEIL Saisissez une clé prépartagée complexe contenant plus de huit caractères et comprenant des minuscules, des majuscules, des chiffres et des symboles tels que -*^+= (Les signes ' ' " \ ne sont pas pris en charge).

Paramètres avancés des modes IKE avec clé prépartagée et IKE avec certificat

Pour la plupart des utilisateurs, les paramètres de base suffisent. Les utilisateurs expérimentés peuvent afficher les paramètres avancés, en cliquant sur **Avancés**. Si vous modifiez les paramètres avancés sur un routeur, assurez-vous de faire de même sur l'autre routeur.

- **Mode agressif :** deux modes de négociation des associations de sécurité IKE sont possibles : le mode principal et le mode agressif. Si la sécurité du réseau est prioritaire, nous vous recommandons de choisir le mode principal. Si le débit du réseau est prioritaire, nous vous recommandons de choisir le mode agressif. Cochez cette case pour activer le mode agressif ou décochez-la pour utiliser le mode principal.
  Si le paramètre **Type de passerelle de sécurité distante** est réglé sur l'un des types *IP dynamique*, le mode agressif est obligatoire. La case est cochée automatiquement et il n'est pas possible de la décocher.
- **Compresser (prend en charge le protocole de compression de la charge utile IP (IP Comp)) :** protocole réduisant la taille des datagrammes IP. Cochez cette case pour permettre au routeur de proposer la compression lors de l'initiation de connexions. Si l'entité qui répond refuse cette proposition, le routeur ne procède pas à la compression. Lorsque le routeur est le répondeur, il accepte la compression, même si l'option n'est pas activée. Si vous activez cette option sur ce routeur, activez-la également sur le routeur situé à l'autre extrémité du tunnel.
- **Maintenir actif :** essaie de rétablir une connexion VPN si elle a été perdue.
- **Algorithme de hachage avec en-tête d'authentification :** le protocole d'en-tête d'authentification décrit le format des paquets et les normes par défaut de la structure des paquets. L'utilisation du protocole d'en-tête d'authentification en tant que protocole de sécurité assure une protection étendue jusqu'à l'en-tête IP afin de vérifier l'intégrité du paquet complet. Cochez la case pour utiliser cette fonction et sélectionnez une méthode d'authentification : MD5 ou SHA1. MD5 produit une assimilation de 128 bits pour authentifier les données de paquets. SHA1 produit une assimilation de 160 bits pour authentifier les données de paquets. Le même algorithme doit être utilisé aux deux extrémités du tunnel.
- **Diffusion NetBIOS :** messages de diffusion utilisés dans le cadre de la résolution de noms, sur le réseau Windows, pour identifier les ressources tels que les ordinateurs, les imprimantes et les serveurs de fichiers. Ces messages sont utilisés par certaines applications logicielles et par certaines fonctionnalités Windows, dont le voisinage réseau. Le trafic de diffusion LAN n'est généralement pas transféré via un tunnel VPN. Toutefois, vous pouvez cocher cette case pour permettre la rediffusion des NetBIOS d'une extrémité du tunnel à l'autre.

- **Traversée NAT :** grâce à la traduction d'adresses réseau (NAT), les utilisateurs possédant des adresses LAN privées peuvent accéder aux ressources Internet en utilisant une adresse IP acheminée publiquement en tant qu'adresse source. Toutefois, concernant le trafic interne, la passerelle NAT ne dispose d'aucune méthode automatique de traduction de l'adresse IP publique vers une destination spécifique du réseau LAN privé. Ce problème empêche le bon déroulement des échanges IPsec. Si votre routeur VPN se trouve derrière une passerelle NAT, cochez cette case pour activer la traversée NAT. Vous devez utiliser le même paramètre sur les deux extrémités du tunnel.
- **Authentification étendue** : permet de spécifier un nom d'utilisateur et un mot de passe pour authentifier les requêtes du tunnel IPSec entrant, en plus d'une clé prépartagée ou d'un certificat.
  - **Hôte IPsec** : indique l'utilisation d'un **hôte IPsec** pour une authentification étendue.
    Nom d'utilisateur : nom d'utilisateur d'authentification.
    Mot de passe : mot de passe d'authentification.
  - **Appareil en périphérie de réseau** : offre une adresse IP à l'émetteur de la requête de tunnel entrant (après authentification) à partir de la plage d'adresses IP virtuelles configurée dans la fenêtre **Récapitulatif**. Sélectionnez le périphérique dans le menu déroulant. Pour ajouter ou modifier le domaine du périphérique, cliquez sur **Ajouter/Modifier** pour afficher la fenêtre **Gestion des utilisateurs**.
- **Configuration du mode** : offre une adresse IP à l'émetteur de la requête de tunnel entrant (après authentification) à partir de la plage d'adresses IP virtuelles configurée dans la fenêtre > **Récapitulatif** du VPN.

Intercommunication VPN

L'option Intercommunication VPN permet aux clients VPN de communiquer via ce routeur et de se connecter au point de terminaison VPN. Cette option est activée par défaut.

Pour activer l'option Intercommunication VPN, cochez la case **Activer** pour les protocoles autorisés.

- **Intercommunication IPSec :** IPsec (Internet Protocol Security) 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 de transmettre le protocole PPP (Point-to-Point Protocol, protocole point à point) via un réseau IP.
- **Intercommunication L2TP :** le protocole L2TP (Layer 2 Tunneling Protocol) est la méthode utilisée pour activer les sessions point-à-point au niveau de couche 2 via Internet.

Serveur PPTP

Jusqu'à 10 tunnels VPN PPTP destinés aux utilisateurs exécutant un logiciel client PPTP peuvent être activés. Par exemple, dans Windows XP ou 2000, un utilisateur ouvre la fenêtre Connexions réseau et crée une connexion. Dans l'Assistant, il choisit l'option qui lui permet d'établir une connexion avec son lieu de travail via un réseau privé virtuel. L'utilisateur doit connaître l'adresse IP du réseau WAN de ce périphérique. Pour en savoir plus, reportez-vous à la documentation ou aux fichiers d'aide de votre système d'exploitation.

Pour activer le serveur PPTP et autoriser des tunnels VPN PPTP, cochez la case **Activer** et définissez la plage :

Début de la plage et **Fin de la plage** : plage d'adresses LAN à attribuer aux clients VPN PPTP. La plage d'adresses IP LAN des clients VPN PPTP doit se situer en dehors de la plage DHCP normale du routeur.

La **table des connexions** affiche les tunnels utilisés. Des comptes utilisateur PPTP sont ajoutés dans la fenêtre **Gestion des utilisateurs** (Sélectionnez **Non attribué** dans la colonne Groupe).

9

Gestion des certificats

Un certificat numérique certifie la propriété d'une clé publique par l'objet nommé du certificat. Cela permet à des tiers (aux parties utilisatrices) d'utiliser les signatures ou les assertions faites par la clé privée correspondant à la clé publique certifiée. Dans ce modèle de relations de confiance, une autorité de certification (CA) est une partie tierce de confiance validée par l'objet (le propriétaire) du certificat et la partie utilisatrice du certificat. Les autorités de certification sont caractéristiques de nombreux systèmes d'infrastructure à clé publique (PKI).

Utilisez la gestion des certificats pour générer et installer des certificats SSL.

Mon certificat

Vous pouvez ajouter jusqu'à 50 certificats en les autosignant ou en obtenant l'autorisation d'un tiers. Vous pouvez également créer des certificats à l'aide du **Générateur de certificat** ou en importer depuis un ordinateur ou un périphérique USB.

Les certificats SSL autosignés ne sont pas en soi reconnus comme valides par les navigateurs et même s'ils peuvent être utilisés pour le cryptage, les navigateurs affichent des messages d'avertissement indiquant à l'utilisateur que le certificat n'a pas été émis par une entité qu'il considère comme étant de confiance.

Autre avantage : les utilisateurs peuvent se connecter sans avoir à installer de certificat sur leur ordinateur. L'utilisateur voit s'afficher un avertissement de sécurité lors de la connexion au tunnel VPN, mais peut néanmoins continuer sans disposer de ce dispositif de protection supplémentaire.

Pour définir un certificat comme certificat principal, activez la case d'option du certificat souhaité, puis cliquez sur **Sélectionner comme certificat principal**.

Pour afficher les informations sur le certificat, cliquez sur l'icône **Détails**.

Exportation ou affichage d'un certificat ou d'une clé privée

Le certificat client permet au client de se connecter au réseau VPN. Pour exporter ou afficher un certificat ou une clé privée :

ÉTAPE 1 Cliquez sur l'icône correspondante : **Exporter le certificat pour le client**, **Exporter le certificat pour l'administrateur** ou **Exporter la clé privée**. La fenêtre Téléchargement de fichiers s'affiche.

Exporter le certificat pour le client : certificat client permettant au client de se connecter au réseau VPN.

Exporter le certificat pour l'administrateur : contient la clé privée. Une copie de sauvegarde peut être exportée. Par exemple, si vous restaurez les paramètres d'origine du périphérique, vous pouvez exporter le certificat. Après avoir redémarré le périphérique, importez ce fichier pour restaurer le certificat.

Exporter la clé privée : certains logiciels client VPN nécessitent des informations de connexion distinctes consistant en une clé privée, un certificat CA et un certificat.

ÉTAPE 2 Cliquez sur **Ouvrir** pour afficher la clé. Cliquez sur **Enregistrer** pour enregistrer la clé.

Importation d'un certificat tiers ou autosigné

Une demande de signature de certificat (CSR) générée en externe ne peut pas faire l'objet d'une autorisation ou d'une signature ; une demande CSR externe doit être ajoutée à l'aide d'une **Autorisation de demande de signature de certificat**.

Pour importer un certificat :

ÉTAPE 1 Cliquez sur **Ajouter**.

ÉTAPE 2 Sélectionnez **Tiers autorisé** ou **Autosigné**.

ÉTAPE 3 Sélectionnez **Importer depuis un ordinateur** ou **Importer depuis un périphérique USB**.

ÉTAPE 4 Allez dans **Certificat CA**. (Tiers uniquement.)

ÉTAPE 5 Allez dans **Certificat et clé privée** (Tiers ou Autosigné).

ÉTAPE 6 Cliquez sur **Enregistrer**.

Certificat SSL approuvé

Le protocole de sécurisation SSL (Secure socket Layer) est une norme de sécurité permettant de créer une liaison cryptée entre un serveur Web et un navigateur. Cette liaison assure que toutes les données transmises entre le serveur Web et le navigateur restent privées et intactes. SSL est une norme industrielle utilisée par des millions de sites Web souhaitant protéger les transactions en ligne qu'ils effectuent avec leurs clients. Pour pouvoir créer une liaison SSL, un serveur Web a besoin d'un certificat SSL.

Les certificats SSL émis par des autorités de certification approuvées n'affichent pas d'avertissement et établissent une liaison sécurisée entre le site Web et le navigateur, de façon transparente. Le cadenas indique que l'utilisateur a établi une liaison cryptée avec une entreprise qui a émis un certificat SSL approuvé depuis une autorité de certification approuvée.

La table de certificats active les certificats et affiche les informations qui s'y rapportent.

Pour afficher d'autres informations sur les certificats, cliquez sur **Détails**.

Pour importer un certificat tiers, cliquez sur **Ajouter** et importez le certificat :

ÉTAPE 1 Sélectionnez **Importer depuis un ordinateur** ou **Importer depuis un périphérique USB**.

ÉTAPE 2 Allez dans **Certificat CA**.

ÉTAPE 3 Cliquez sur **Enregistrer**.

Certificat IPSec approuvé

Le certificat IPsec est utilisé dans l'échange de données de génération et d'authentification de clés et avec les protocoles d'établissement de clés, les algorithmes de cryptage ou encore les mécanismes d'authentification sécurisée et de validation des transactions en ligne rattachées à des certificats SSL.

Pour afficher les informations du certificat, cliquez sur l'icône **Détails**.

Pour exporter ou afficher un certificat, cliquez sur l'icône **Exporter le certificat**. Une fenêtre contextuelle s'affiche lorsque vous pouvez **ouvrir** le certificat pour l'inspecter et l'**enregistrer** sur un ordinateur.

Pour importer un certificat tiers, cliquez sur **Ajouter** et importez le certificat :

ÉTAPE 1 Sélectionnez **Certificat CA**.

ÉTAPE 2 Sélectionnez **Importer depuis un ordinateur** ou **Importer depuis un périphérique USB**.

ÉTAPE 3 Allez dans **Certificat**. (Tiers ou Autosigné.)

ÉTAPE 4 Cliquez sur **Enregistrer**.

Générateur de certificat

Le générateur de demande de certificat collecte des informations et génère un fichier de clé privée ainsi qu'une demande de certificat. Vous pouvez choisir de générer un certificat autosigné ou une demande de signature de certificat (CSR) pour une autorité de certification externe à signer. Lorsque la configuration a été enregistrée, la demande CSR générée ou le certificat autosigné s'affiche sous **Mon certificat**.

Pour générer un certificat :

ÉTAPE 1 Saisissez les paramètres suivants :

- **Type** : type de demande de certificat.
- **Nom du pays** : nom du pays d'origine.
- **Nom du département ou de la région** : nom du département ou de la région (facultatif).
- **Locality Name (Nom de la localité)** : municipalité (facultatif).
- **Nom de l'organisation** : organisation (facultatif).
- **Organizational Unit Name (Nom de l'unité de travail)** : sous-groupe de l'organisation.
- **Nom courant** : nom courant de organisation.
- **Adresse e-mail** : adresse e-mail du contact (facultatif).
- **Longueur de clé de cryptage** : longueur de la clé.
- **Valid Duration (Durée valide)** : nombre de jours de validité du certificat.

ÉTAPE 2 Cliquez sur **Enregistrer**. La fenêtre **Mon certificat** apparaît.

Autorisation de demande de signature de certificat

La demande de signature de certificat (CSR) est un certificat numérique généré par un générateur de certificat. Le certificat n'est complet qu'une fois signé par l'autorité de certification. Ce périphérique peut fonctionner en tant qu'autorité de certification et signer/autoriser une demande CSR générée en externe sous Gestion des certificats > Autorisation de demande de signature de certificat. Après qu'une demande CSR générée en externe a été signée par le périphérique, elle devient un certificat valide et s'affiche dans la fenêtre **Certificat IPSec approuvé** (Pour restaurer les paramètres d'origine de la configuration du périphérique, y compris les certificats par défaut, allez dans la fenêtre **Valeurs d'origine**.)

Pour signer un certificat :

ÉTAPE 1 Cliquez sur **Parcourir** pour identifier la demande de signature de certificat.

ÉTAPE 2 Pour sélectionner la clé privée correspondante permettant d'autoriser et de signer la demande CSR, sélectionnez le certificat à associer à la demande dans le menu déroulant **Mon certificat**.

ÉTAPE 3 Cliquez sur **Enregistrer**.

10

Journal

Les journaux affichent l'état du système, soit à l'aide des messages « trap » ou à intervalles périodiques.

Journal système

Configurez le service de messagerie SMS (Short Message Service) pour les journaux et les alertes.

Configuration du service de messagerie SMS pour les journaux système

Pour configurer la liaison du journal, suivez les étapes ci-dessous :

ÉTAPE 1 Cliquez sur **Activer**.

ÉTAPE 2 Sélectionnez **USB1** ou **USB2** pour envoyer le journal via les ports USB.

ÉTAPE 3 Cochez la case **Composer le numéro 1** et/ou **Composer le numéro 2**, puis saisissez le numéro de téléphone à composer.

ÉTAPE 4 Cliquez sur **Test** pour tester la liaison.

ÉTAPE 5 Sélectionnez quand envoyer le journal :

- Lorsqu'une liaison est établie.
- Lorsqu'une liaison prend fin.
- Lorsque l'authentification échoue.
- Lorsque le système démarre.

ÉTAPE 6 Cliquez sur **Enregistrer**.

Configuration des serveurs de journalisation système

Pour activer un serveur, cliquez sur **Activer**, puis saisissez le nom du **serveur Syslog**.

Configuration de la notification par e-mail

Pour configurer la notification par e-mail, cochez **Activer** et suivez les étapes ci-dessous :

- **Serveur de messagerie** : nom ou adresse IP du serveur de messagerie.
- **Authentification** : type d'authentification de la connexion du serveur de messagerie.
  - **Aucun** : aucune authentification.
  - **Connexion simple** : authentification sous forme de texte en clair.
  - **TLS** : protocole d'authentification de la connexion sécurisée (par exemple, Gmail utilise l'option d'authentification TLS sur le port 587).
  - **SSL** : protocole d'authentification de la connexion sécurisée (par exemple, Gmail utilise l'option d'authentification SSL sur le port 465).
- **Port SMTP** : numéro de port du protocole de transfert de courrier simple.
- **Nom d'utilisateur** : nom d'utilisateur de la messagerie. Par exemple :
  Serveur de messagerie : smtp.gmail.com
  Authentification : PORT SMTP
  SSL : 465
  Nom d'utilisateur : xxxxx@gmail.com
  Mot de passe : yyyyyy
- **Mot de passe** : mot de passe de la messagerie.
- **Envoyer un e-mail à 1** et (facultatif) à **2** : adresse e-mail. Par exemple, Envoyer un e-mail à : `zzz@company.com`.
- **Consigner la longueur des files d'attente** : nombre d'entrées au journal avant l'envoi de la notification. Par exemple, *10* entrées.
- **Consigner le seuil de temps** : intervalle entre deux notifications du journal. Par exemple, *10* minutes.
- **Alerte en temps réel** : événement qui déclenche une notification immédiate.
- **Envoyer une alerte par e-mail en cas d'accès au contenu bloqué/filtré** : e-mail d'alerte envoyé lorsqu'une tentative d'accès est effectuée par un périphérique bloqué ou filtré.
- **Envoyer une alerte par e-mail en cas d'attaque de pirate** : e-mail d'alerte envoyé lorsqu'une tentative d'accès est effectuée par un pirate via une attaque de refus de service (DoS).

Pour définir l'envoi immédiat par e-mail du journal, cliquez sur **Envoyer le journal par e-mail maintenant**.

Configuration des journaux

Pour déclencher des entrées au journal, sélectionnez les événements suivants :

- **Inondation SYN** : les requêtes de connexion TCP sont reçues plus rapidement que le périphérique ne peut les traiter.
- **Usurpation d'adresse IP** : paquets IP avec des adresses IP source visiblement falsifiées envoyées dans le but de masquer l'identité de l'expéditeur ou d'imiter un autre système informatique.
- **Tentative de connexion non autorisée** : tentative de connexion au réseau rejetée.
- **Ping fatal** : détection d'un ping malformé ou malveillant envoyé à un ordinateur. Normalement, la taille d'un ping est de 32 octets (ou de 84 octets avec l'en-tête Internet Protocol [IP]) ; dans le passé, beaucoup de systèmes informatiques ne pouvaient pas traiter les paquets de pings supérieurs à 65 535 octets (taille de paquet IPv4 maximale). L'envoi d'un ping trop volumineux peut bloquer l'ordinateur cible.
- **WinNuke** : attaque par refus de service (DoS) à distance affectant les systèmes d'exploitation Microsoft Windows 95, Microsoft Windows NT et Microsoft Windows 3.1x.
- **Stratégies de refus** : l'accès a été refusé sur la base des stratégies configurées.
- **Connexion autorisée** : un utilisateur autorisé s'est connecté au réseau.
- **Messages d'erreurs système** : des messages d'erreur système ont été consignés.
- **Stratégies d'autorisation** : un utilisateur autorisé s'est connecté au réseau via les stratégies configurées.
- **Noyau** : tous les messages de noyau système.
- **Modifications de la configuration** : cas où la configuration du périphérique a été modifiée.
- **VPN IPsec et PPTP** : état de négociation, de connexion et de déconnexion du tunnel VPN.
- **VPN SSL** : état de négociation, de connexion et de déconnexion du tunnel VPN SSL.
- **Réseau** : l'interface WAN/DMZ est connectée ou déconnectée.

Informations supplémentaires (boutons relatifs aux journaux)

Si le navigateur Web affiche une mise en garde relative à la fenêtre contextuelle, autorisez le contenu bloqué. Cliquez sur **Actualiser** pour actualiser les données.

Cliquez sur les boutons suivants pour afficher des informations supplémentaires :

- **Afficher le journal système** : affichez le **journal système**. Pour spécifier un journal, sélectionnez le filtre dans le menu déroulant.

  Les entrées du journal contiennent la date et l'heure de l'événement, le type d'événement et un message. Ce message indique le type de stratégie utilisé, par exemple Règle d'accès, l'adresse IP du réseau LAN de la source (SRC) et l'adresse MAC.

- **Table des journaux sortants** : informations relatives aux paquets sortants.
- **Table des journaux entrants** : informations relatives aux paquets entrants.
- **Effacer le journal maintenant** : cliquez sur ce bouton pour effacer le journal sans l'envoyer par e-mail uniquement si vous êtes sûr de ne plus avoir besoin de consulter ces informations.

Statistiques du système

Des informations détaillées sur les ports et les périphériques associés s'affichent.

Processus

Des informations détaillées sur les processus de fonctionnement s'affichent.

11

VPN SSL

Un VPN SSL (réseau privé virtuel Secure Sockets Layer) permet d'établir un tunnel VPN d'accès à distance sécurisé avec ce périphérique à l'aide d'un navigateur Web. Il n'est pas nécessaire qu'un client logiciel ou matériel soit préinstallé sur l'ordinateur. 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. Ceci inclut :

- Les sites Web internes
- Les applications Web
- Les partages de fichier NT/Active Directory (c.-à-d. Mon emplacement réseau)
- L'accès Web à MS Outlook
- L'accès à l'application (accès à la redirection de port vers d'autres applications TCP)

Le VPN SSL utilise le protocole Secure Sockets Layer et son successeur, le protocole Transport Layer Security, pour offrir une connexion sécurisée entre l'utilisateur distant et les ressources internes spécifiques prises en charge et configurées sur un site central. Ce périphérique reconnaît les connexions devant être mandatées et le portail Web VPN SSL interagit avec le sous-système d'authentification pour authentifier les utilisateurs.

L'accès aux ressources par les utilisateurs de sessions VPN SSL est attribué au groupe. Les utilisateurs, tels que les partenaires commerciaux, peuvent être affectés à un groupe disposant d'un accès direct aux ressources du réseau interne. Ou, pour les utilisateurs qui requièrent un accès à toutes les ressources du réseau interne, ce périphérique prend en charge le passage virtuel, qui permet aux utilisateurs d'obtenir une adresse IP depuis ce périphérique via un tunnel VPN SSL et de faire partie du réseau interne.

État

Fournit l'état des tunnels VPN SSL. L'utilisateur peut être déconnecté de cette fenêtre.

La table d'états SSL affiche les éléments suivants :

- **Utilisateur** : nom de l'utilisateur.
- **Groupe** : groupe associé.
- **IP** : adresse IP.
- **Heure de la connexion** : heure de connexion de l'utilisateur au tunnel.

Pour déconnecter un utilisateur, cliquez sur l'icône dans la colonne **Se déconnecter**.

Gestion des groupes

La gestion des groupes permet de contrôler les groupes d'utilisateurs, y compris l'accès aux ressources. Un administrateur peut créer plusieurs groupes d'utilisateurs, où chaque groupe a accès à différents ensembles de ressources sur le LAN. Un scénario typique comporte deux groupes d'utilisateurs, où un groupe contient les employés et l'autre groupe contient les partenaires commerciaux. Bien que le périphérique prenne en charge plusieurs domaines, il est courant qu'une petite entreprise avec un seul domaine soit liée à une base de données d'authentification particulière (une base de données locale RADIUS ou LDAP, par exemple).

La table d'états SSL contient les informations suivantes :

- **Groupe** : nom du groupe.
- **Domaine** : base de données pour laquelle l'utilisateur dispose d'un droit d'accès.
- **Utilisateur** : noms d'utilisateurs et types. Cliquez sur **Détails** pour les afficher.
- **Ressource** : ressources du système pour lesquelles le groupe dispose d'un droit d'accès. Cliquez sur **Détails** pour les afficher.
- **État** : état du groupe.

Suppression d'un groupe

Pour supprimer un groupe, cliquez sur le nom du groupe que vous souhaitez supprimer dans la table d'**états SSL** et cliquez sur **Supprimer**. Si les utilisateurs n'appartiennent qu'à un seul groupe, lorsque l'administrateur supprime le groupe, les utilisateurs correspondants sont supprimés automatiquement.

Pour supprimer un groupe qui constitue le groupe par défaut d'un domaine d'authentification, supprimez le domaine correspondant (vous ne pouvez pas supprimer le groupe dans la fenêtre Modifier les paramètres du groupe.

Si le groupe ne correspond pas au groupe par défaut du domaine d'authentification, supprimez tous les utilisateurs du groupe, puis supprimez le groupe.

Ajout ou modification d'un groupe

Pour ajouter (ou modifier) un groupe, cliquez sur **Ajouter** (ou sélectionnez une entrée et cliquez sur **Modifier**) et saisissez les paramètres suivants :

- **Nom du groupe** : nom du groupe. Si vous modifiez un groupe existant, ce paramètre n'est pas modifiable.
- **Domaine** : domaine du groupe. Cliquez sur **Ajouter** ou **Modifier** pour afficher la fenêtre **Gestion des groupes**.
- **Activé** : cochez cette case pour activer le groupe.
- **Durée d'inactivité du service** : durée d'inactivité de la connexion avant que la session ne soit interrompue.

Sélectionnez les ressources à activer pour ce groupe :

- **Service** : services disponibles pour ce groupe.
- **Favori de service personnalisé** : les services (Telnet, SSH, FTP) et les services de bureau distant (RDP5, VNC) peuvent utiliser les favoris établis par le-groupe. Ainsi, les utilisateurs ne sont pas obligés de se souvenir ou de définir un nom de serveur ou une adresse IP. Ils peuvent simplement cliquer pour utiliser les ressources préconfigurées par l'administrateur.

  Les administrateurs peuvent voir tous les favoris configurés qui s'affichent sur le portail Web de l'utilisateur.

- **Mon bureau** : permet d'activer le RDP5 et le VNC. Les favoris ActiveX **RDP5** (améliorations du client Remote Desktop Protocol) prennent à présent en charge les options Windows avancées pour le mappage des ressources, avec des options permettant de rediriger les lecteurs, les imprimantes, les ports et les smartCards. Le **VNC** (Virtual Network Computing) est un système de partage de bureau graphique qui utilise le protocole RFB (Remote Frame Buffer) pour contrôler à distance un autre ordinateur. Il transmet les événements du clavier et de la souris d'un ordinateur à l'autre, relayant les mises à jour de l'écran graphique dans l'autre direction, via un réseau.
- **Service Terminal Server** : autorise les applications telles que Word, Excel et PowerPoint.
- **Autres** : permet l'accès aux options Mon emplacement réseau et Passage virtuel. Le passage virtuel peut être un tunnel fractionné (où le trafic qui n'est pas spécialement balisé pour le tunnel est envoyé via une autre connexion virtuelle) ou un tunnel complet (où l'ensemble du trafic est envoyé via le tunnel).

Les ressources de chaque groupe d'utilisateur par défaut sont indiquées dans la table.

Nom de la ressource/Nom du groupe	Tous les utilisateurs	Superviseur	Utilisateur mobile	Personnel du site
Services Internet				
Telnet	v			
SSH	v			
FTP	v	v	v	v
Terminal Microsoft				
Services	v	v	v	
Word	v	v	v	
Excel	v	v	v	
PowerPoint	v	v	v	
Accès	v	v	v	
Outlook	v	v	v	
Internet Explorer	v			

Nom de la ressource/Nom du groupe	Tous les utilisateurs	Superviseur	Utilisateur mobile	Personnel du site
FrontPage	v			
ERP	v	v	v	v
Bureau à distance				
RDP5	v		v	
VNC	v			
Mon emplacement réseau	v	v		
Passage virtuel	v	v		

Gestion des ressources

Le VPN SSL prend en charge les services courants du terminal Microsoft (Word, Excel, PowerPoint, Access, Outlook, Internet Explorer, FrontPage et ERP). Pour que chaque service du terminal soit disponible pour les utilisateurs, configurez une ressource et spécifiez l'adresse IP du serveur d'application et le chemin d'accès de l'application.

Pour ajouter (ou modifier) un groupe, cliquez sur **Ajouter** (ou sélectionnez une entrée et cliquez sur **Modifier**) et saisissez les paramètres suivants :

- **Description de l'application** : description de l'application.
- **Application et chemin d'accès** : chemin d'accès et noms des fichiers exécutables.
- **Répertoire de fonctionnement** : répertoire de l'application.
- **Adresse de l'hôte)** : adresse IP de l'ordinateur hôte du service.
- **Icône de l'application** : icône à afficher.
- **Activer** : permet d'activer la ressource.

Paramètre avancé

Les paramètres VPN SSL avancés permettent de limiter la plage d'adresses IP pouvant accéder au service, de modifier le port de service ou de modifier les bannières.

Pour modifier les paramètres avancés, saisissez les paramètres suivants :

- **Début de la plage d'adresses client** : adresse IP de début de la plage autorisée.
- **Fin de la plage d'adresses client** : adresse IP de fin de la plage autorisée.
- **Port de service** : numéro de port du VPN SSL.
- **Nom de l'entreprise** : chaîne affichée sous forme de bannière pour le nom de l'entreprise.
- **Nom de la ressource** : chaîne affichée sous forme de bannière pour le nom de la ressource.

12

Assistant

Sur la page de l'Assistant, vous pouvez lancer l'Assistant de configuration de base qui vous guidera tout au long du processus de configuration initiale du périphérique. L'Assistant des règles d'accès vous guidera tout au long du processus de configuration des stratégies de sécurité sur le réseau.

Paramètres de base

Utilisez l'Assistant de configuration de base pour changer le nombre de ports WAN ou configurer la connexion Internet.

Cliquez sur **Lancer maintenant** pour exécuter l'Assistant de configuration de base. Suivez les instructions à l'écran pour continuer. Reportez-vous aux informations que vous a fournies votre FAI pour spécifier les paramètres requis par votre connexion.

Configuration des règles d'accès

Utilisez l'Assistant de configuration des règles d'accès pour créer les règles d'accès du pare-feu. Cliquez sur **Lancer maintenant** pour exécuter l'Assistant de configuration des règles d’accès. Cet Assistant fournit des informations sur les règles par défaut appliquées au périphérique. Suivez les instructions à l'écran pour continuer.

13

Gestion des utilisateurs

La gestion des utilisateurs commande les domaines et l'accès des utilisateurs ; elle est utilisée avant tout pour le protocole PPTP, Cisco VPN Client (également connu sous le nom d'EasyVPN) et VPN SSL.

Pour ajouter (ou modifier) un domaine :

ÉTAPE 1 Cliquez sur **Ajouter** (ou sélectionnez une entrée et cliquez sur **Modifier**).

ÉTAPE 2 Sélectionnez le **type d'authentification** et saisissez les informations requises :

- **Base de données locale** : authentification auprès d'une base de données locale.
  - **Domaine** : nom de domaine que les utilisateurs sélectionnent pour se connecter au portail VPN SSL.
- **Radius (PAP, CHAP, MSCHAP, MSCHAPv2)** : authentification auprès d'un serveur RADIUS à l'aide d'un protocole PAP (Password Authentication Protocol), d'un protocole CHAP (Challenge Handshake Authentication Protocol), d'un protocole MSCHAP (Microsoft Challenge Handshake Authentication Protocol) ou d'un protocole MSCHAPv2 (Microsoft Challenge Handshake Authentication Protocol Version 2).
  - **Domaine** : nom de domaine que les utilisateurs sélectionnent pour se connecter au portail VPN SSL.
  - **Serveur RADIUS** : adresse IP du serveur RADIUS.
  - **Mot de passe RADIUS** : *secret* d'authentification.
- Active Directory : authentification d'Active Directory de Windows. Notez que l'authentification Active Directory représente la plus grande source d'erreurs. Si vous ne pouvez pas effectuer une authentification à l'aide d'Active Directory, consultez les conseils de dépannage à la fin de cette section.
  - **Domaine** : nom de domaine que les utilisateurs sélectionnent pour se connecter au portail VPN SSL.
  - **Adresse du serveur Active Directory** : adresse IPv4 du serveur Active Directory.
  - **Nom du domaine Active Directory** : nom du domaine du serveur Active Directory.

- **LDAP** : protocole LDAP (Lightweight Directory Access Protocol).
  - **Domaine** : nom de domaine que les utilisateurs sélectionnent pour se connecter au portail VPN SSL.
  - **Adresse du serveur LDAP** : adresse IPv4 du serveur LDAP.
  - **Nom de domaine de base LDAP** : base de recherche pour des requêtes LDAP. Exemple d'une chaîne de base de recherche : `CN=Users,DC=yourdomain,DC=com`.

ÉTAPE 3 Cliquez sur **OK**.

Pour ajouter (ou modifier) un utilisateur, cliquez sur **Ajouter** (ou sélectionnez une entrée et cliquez sur **Modifier**), puis saisissez les informations suivantes :

- **Nom d'utilisateur** : nom que l'utilisateur saisi pour se connecter au portail VPN SSL.
- **Mot de passe** : mot de passe utilisé pour l'authentification.
- **Groupe** : groupes provenant de la table d'états SSL dans **Gestion des groupes**. Par défaut, le menu déroulant Groupe contient 5 options : 4 groupes VPN SSL par défaut et 1 groupe Non attribué. Le groupe Non attribué contient des utilisateurs VPN PPTP et des utilisateurs EasyVPN. Le groupe Administrateur n'a qu'un utilisateur. Le nom d'utilisateur par défaut de ce groupe est **cisco**.
- **Domaine** : nom du domaine répertorié dans la table de gestion des domaines.

14

Pour en savoir plus

Assistance	
Communauté d'assistance Cisco	www.cisco.com/go/smallbizsupport
Assistance et ressources Cisco	www.cisco.com/go/smallbizhelp
Coordonnées de l'assistance téléphonique	www.cisco.com/en/US/support/tsd_cisco_small_business_support_center_contacts.html
Téléchargements de microprogrammes Cisco	www.cisco.com/cisco/software/navigator.html?i=!ch Sélectionnez un lien pour télécharger le microprogramme d'un produit Cisco. Aucune connexion n'est requise.
Demande Open Source Cisco	www.cisco.com/go/smallbiz_opensource_request
Cisco Partner Central (connexion partenaire requise)	www.cisco.com/web/partners/sell/smb
Documentation sur les produits	
Routeurs et pare-feu Cisco	www.cisco.com/go/smallbizrouters

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

Version révisée du 18 avril 2014 78-21284-01B0

14

Pour en savoir plus