Configuration du contrôle d'accès sur le routeur VPN RV315W

Objectif

La configuration du contrôle d'accès permet de restreindre l'accès à une adresse IP spécifique. Il existe diverses options pour personnaliser les restrictions. L'heure, les jours de la semaine, les adresses IP, le port physique et le type de protocole sont des exemples de certaines fonctions de personnalisation de la stratégie de contrôle d'accès.

Cet article explique comment utiliser et configurer les contrôles d'accès sur le routeur VPN RV315W.

Périphérique applicable

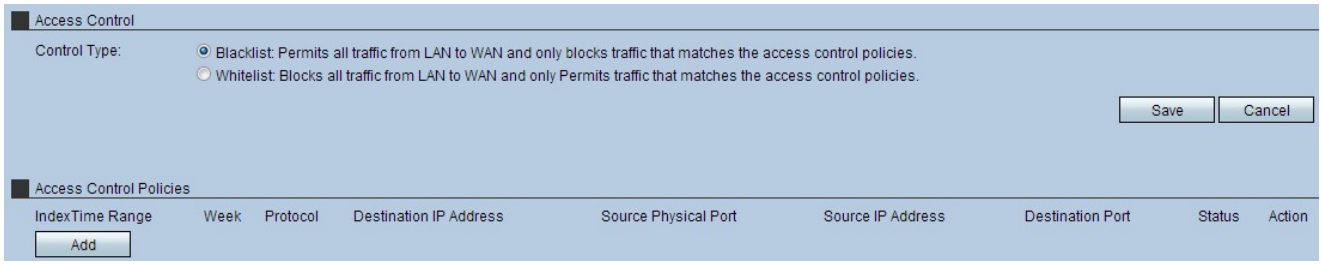
·RV315W

Version du logiciel

•1.01.03

Gestion de la configuration

Étape 1. Connectez-vous à l'utilitaire de configuration Web et choisissez **Security > Access Control**. La page *Contrôle d'accès* s'ouvre :



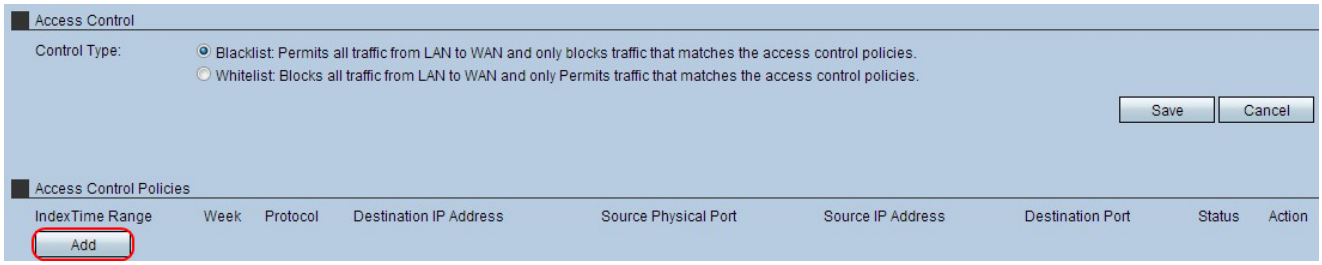
Étape 2. Cliquez sur la case d'option Bloquer ou Autoriser la liste dans le champ Type de contrôle.

·Block list : cette option autorise tout le trafic du LAN au WAN, à l'exception du trafic bloqué par les paramètres de contrôle d'accès.

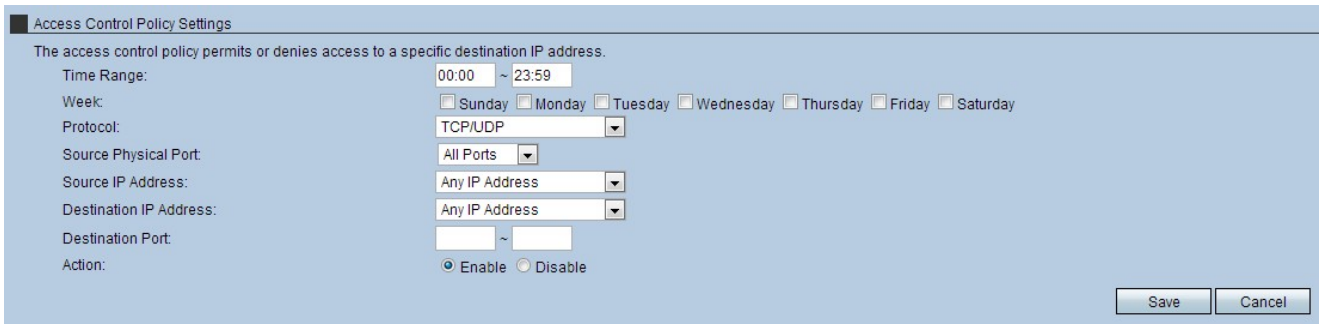
·Allow list : cette option bloque tout le trafic du LAN au WAN, à l'exception du trafic autorisé par les paramètres de contrôle d'accès.

Pour plus d'informations, reportez-vous au glossaire.

Étape 3. Cliquez sur **Enregistrer** pour appliquer les paramètres.



Étape 4. Cliquez sur **Ajouter** pour ajouter une nouvelle stratégie de contrôle d'accès. La page *Access Control Policy Settings* s'ouvre :



Étape 5. Saisissez une plage dans le champ Plage de temps. Cette option indique le moment où la stratégie de contrôle d'accès est efficace.

Étape 6. Sélectionnez les jours de la semaine pour autoriser ou restreindre l'accès. Cette option correspond aux jours de la semaine où la stratégie de contrôle d'accès est effective.

Étape 7. Dans la liste déroulante Protocole, sélectionnez le protocole auquel le contrôle d'accès s'applique.

·TCP : protocole utilisé pour transmettre des données d'une application au réseau. Le protocole TCP est généralement utilisé pour les applications où le transfert d'informations doit être terminé et les paquets ne doivent pas être abandonnés.

·UDP : ce protocole est destiné aux applications réseau client/serveur basées sur le protocole IP (Internet Protocol). L'objectif principal de ce protocole est d'utiliser des applications en direct. (VOIP, jeux, etc.)

·TCP/UDP : sélectionnez ce protocole pour utiliser TCP et UDP. Il s'agit du protocole par défaut.

·ICMP : ce protocole envoie des messages d'erreur et est responsable de la gestion des erreurs sur le réseau. Utilisez ce protocole pour obtenir une notification lorsque le réseau rencontre des problèmes de transmission de paquets.

·HTTP : ce protocole fournit une communication sécurisée entre un serveur Web et un navigateur. Utilisez ce protocole lorsqu'il est nécessaire de transférer des paquets en toute sécurité entre un serveur et un navigateur.

·FTP : ce protocole transmet les fichiers entre les ordinateurs. Sélectionnez ce protocole lorsque des fichiers sont échangés entre plusieurs périphériques.

·SMTP : ce protocole gère la transmission des e-mails. Sélectionnez ce protocole lors de l'échange de courriels.

·POP3 : ce protocole est associé au protocole SMTP en ce qui concerne les e-mails. POP3

télécharge les courriers électroniques d'un serveur de messagerie vers un ordinateur personnel. Sélectionnez ce protocole lors du téléchargement de courriels.

Étape 8. Dans la liste déroulante Port physique source, sélectionnez le port auquel le contrôle d'accès s'applique.

Étape 9. Dans la liste déroulante Adresse IP source, sélectionnez la ou les adresses IP auxquelles s'applique le contrôle d'accès.

·Any IP Address : sélectionnez cette option pour autoriser ou refuser toutes les adresses IP. Sélectionnez la case d'option activer ou désactiver pour cette option.

·Single IP Address : sélectionnez cette option pour autoriser ou refuser des adresses IP individuelles. Saisissez l'adresse IP applicable dans le champ Adresse IP source.

·IP Address Range : sélectionnez cette option pour autoriser ou refuser les adresses IP en fonction d'une plage sélectionnée. Saisissez la plage d'adresses IP applicable dans les champs First et Second Source IP Address.

Étape 10. Dans la liste déroulante Adresse IP de destination, sélectionnez la ou les adresses IP auxquelles le contrôle d'accès s'applique.

·Any IP Address : sélectionnez cette option pour autoriser ou refuser toutes les adresses IP. Activez la case d'option Activer ou Désactiver pour cette option.

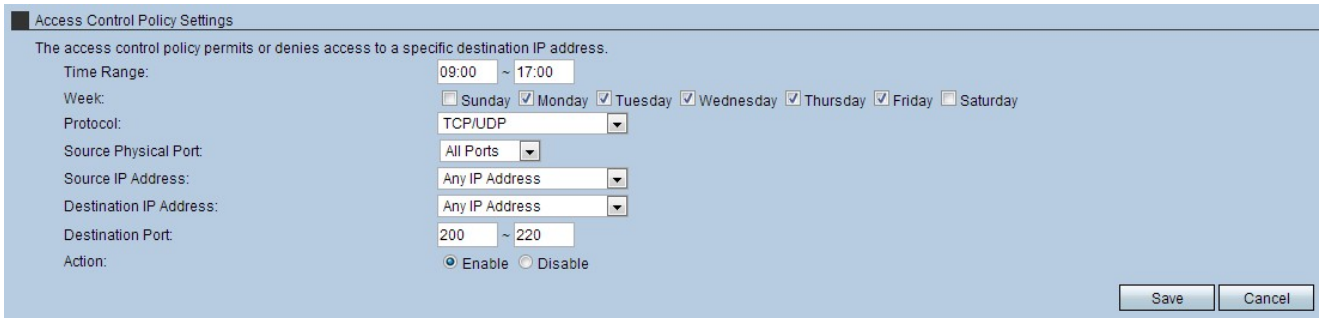
·Single IP Address : sélectionnez cette option pour autoriser ou refuser une adresse IP individuelle. Saisissez l'adresse IP applicable dans le champ Destination IP Address.

·IP Address Range : sélectionnez cette option pour autoriser ou refuser les adresses IP en fonction d'une plage sélectionnée. Saisissez la plage d'adresses IP applicable dans les champs First et Second Destination IP Address.

Étape 11. Dans les champs Port de destination, saisissez la plage de ports d'un protocole ou d'une application auquel le contrôle d'accès s'applique.

Étape 12. Cliquez sur la case d'option **Activer** pour activer la stratégie de contrôle d'accès.

Étape 13. Cliquez sur **Enregistrer** pour appliquer les paramètres.



Étape 14. (Facultatif) Afin de supprimer une stratégie de contrôle d'accès, cliquez sur l'icône de poubelle sous l'en-tête Action.

Étape 15. (Facultatif) Pour modifier une stratégie de contrôle d'accès, cliquez sur l'icône d'enveloppe sous l'en-tête Action.