

Configuration des paramètres de base du pare-feu sur le routeur de la gamme RV34x

Objectif

L'objectif de cet article est d'expliquer comment configurer les paramètres de base du pare-feu sur le routeur de la gamme RV34x.

Introduction

L'objectif principal d'un pare-feu est de contrôler le trafic réseau entrant et sortant en analysant les paquets de données et en déterminant s'il doit être autorisé à traverser ou non, sur la base d'un ensemble de règles prédéfini. Un routeur est considéré comme un pare-feu matériel puissant en raison de fonctions permettant le filtrage des données entrantes. Un pare-feu de réseau crée un pont entre un réseau interne supposé être sécurisé et fiable et un autre réseau, généralement un interréseau externe tel qu'Internet, supposé ne pas être sécurisé et non fiable.

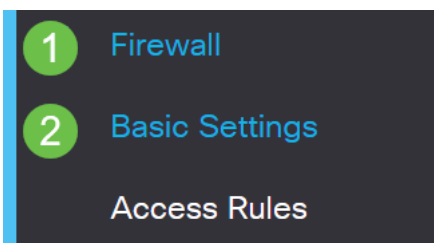
Périphériques pertinents | Version du micrologiciel

- Gamme RV34x | 1.0.03.21 ([Télécharger la dernière version](#))

Configuration des paramètres de base du pare-feu

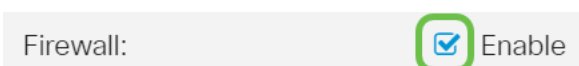
Étape 1

Connectez-vous à l'interface utilisateur Web et choisissez **Firewall > Basic Settings**.



Étape 2

Cochez la case **Activer** le pare-feu pour activer la fonction de pare-feu. Ceci est activé par défaut.



Étape 3

Cochez la case **Activer** Dos (Denial of Service) pour sécuriser votre réseau contre les attaques DoS. Ceci est activé par défaut.

Dos (Denial of Service): Enable

Étape 4

Cochez la case **Enable** Block WAN Request pour refuser les requêtes ping au routeur de la gamme RV34x. Ceci est activé par défaut.

Firewall: Enable

Dos (Denial of Service): Enable

Block WAN Request: Enable

Étape 5

Dans la zone LAN/VPN Web Management, cochez la case **HTTP** et/ou **HTTPS** pour activer le trafic de ces protocoles. Dans cet exemple, la case HTTPS est cochée.

- HTTP : le protocole Hyper Text Transfer Protocol est un protocole de transfert de données utilisé sur Internet.
- HTTPS — Hyper Text Transfer Protocol Secure est une version sécurisée de HTTP qui chiffre les paquets pour une sécurité accrue.

LAN/VPN Web Management: HTTP 80 (Default: 80, Range: 1025 - 65535)
 HTTPS 443 (Default: 443, Range: 1025 - 65535)

Étape 6 (facultative)

Cochez la case **Activer** la gestion Web à distance pour activer la gestion à distance. Sinon, passez à l'étape 8.

Sélectionnez le type de protocole utilisé pour se connecter au pare-feu en sélectionnant une case d'option. Les options sont **HTTP** et **HTTPS**.

Entrez un numéro de port compris entre 1025 et 65535, que la gestion à distance est autorisée. Il est défini par défaut à 443. Dans cet exemple, 1666 est utilisé.

Remote Web Management: Enable 1
 HTTP HTTPS 2
3 Port 1666 (Default: 443, Range: 1025 - 65535)

Étape 7

Dans la zone Allowed Remote IP Addresses (Adresses IP distantes autorisées), sélectionnez une case d'option pour autoriser toute adresse IP à accéder au réseau à

distance ou pour spécifier une plage d'adresses IPv4 ou IPv6. Dans cet exemple, une plage IP a été choisie. Dans cet exemple, l'adresse IP de début est 128.112.59.21 et l'adresse IP de fin est 128.112.59.34.

Allowed Remote IP Addresses: Any IP Address

to (IPv4 or IPv6 address range)

Étape 8 (facultative)

Cochez la case **Enable** SIP ALG pour activer la passerelle ALG (Application Layer Gateway) SIP (Session Initiation Protocol) à travers le pare-feu. Cette fonctionnalité peut être activée pour aider les paquets SIP à traverser le pare-feu. Un paquet SIP est utilisé pour initier les connexions du trafic vocal. Si votre fournisseur VoIP utilise un protocole de traversée NAT (Network Address Translation) différent, cette fonctionnalité peut être désactivée, qui est le paramètre par défaut.

Spécifiez le port FTP (File Transfer Protocol) de SIP ALG dans le champ *FTP ALG Port*. Il est défini par défaut à 21.

Cochez la case **Activer** UPnP pour activer Universal Plug and Play (UPnP). Cette fonction est désactivée par défaut.

Pour cet exemple, ces options sont désactivées.

SIP ALG: Enable

FTP ALG Port:

UPnP: Enable

Étape 9 (facultative)

Sous la zone Restrict Web Feature, cochez les cases correspondant aux types de fonctions Web à bloquer dans la zone Block. Ces cases à cocher sont désactivées par défaut. Les options sont les suivantes :

Java : tous les éléments Web contenant ce type d'élément Web seront bloqués. Ce paramètre peut aider à prévenir les attaques Web basées sur Java.

Cookies : les cookies sont des données stockées dans l'ordinateur pour aider les sites Web à comprendre qui y accède. Les bloquer peut empêcher les cookies malveillants d'accéder aux données.

ActiveX — Il s'agit d'un plugin développé par Microsoft pour améliorer une expérience de navigation. Le bloquer peut empêcher les plug-ins ActiveX malveillants de nuire aux périphériques réseau.

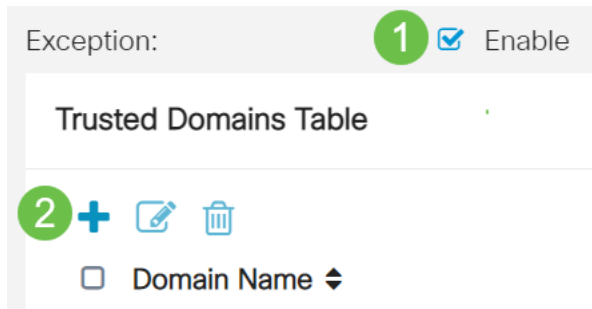
Access to Proxy HTTP Server — Les serveurs proxy HTTP masquent les détails des utilisateurs finaux aux pirates. Ils travaillent comme intermédiaires, de sorte qu'un client n'a pas accès directement à Internet. Cependant, si les utilisateurs locaux ont accès aux serveurs proxy WAN, ils peuvent trouver un moyen de contourner les filtres de contenu sur le routeur pour accéder aux sites Internet bloqués par le routeur.

Dans cet exemple, les cases à cocher sont désactivées.

Étape 11 (facultative)



Cochez la case **Activer** l'exception pour autoriser uniquement les fonctionnalités Web sélectionnées telles que Java, Cookies, ActiveX ou Access to HTTP Proxy Servers et pour restreindre toutes les autres fonctionnalités. Ceci est désactivé par défaut. Dans cet exemple, il est désactivé.

Dans le tableau Domaines approuvés, cliquez sur l'**icône Ajouter** pour ajouter des domaines auxquels vous êtes autorisé ou approuvé à accéder sur le réseau.



Exception: Enable 1

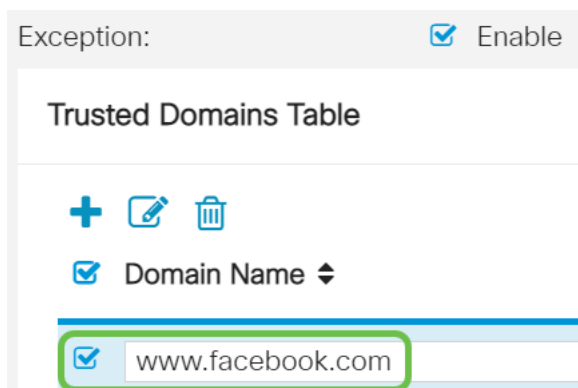
Trusted Domains Table

2 +  

Domain Name ▾



Étape 12

Dans le champ *Nom de domaine*, saisissez un nom de domaine auquel l'accès au réseau doit être accordé. Pour cet exemple, www.facebook.com est utilisé.



Exception: Enable

Trusted Domains Table

+  

Domain Name ▾

www.facebook.com

Étape 13

Cliquez sur Apply.



Apply Cancel

Étape 14 (facultative)

Pour enregistrer définitivement la configuration, accédez à la page Copier/Enregistrer la configuration ou cliquez sur l'**icône Enregistrer** dans la partie supérieure de la page.



Conclusion

Vous devez maintenant avoir correctement configuré les paramètres de pare-feu de base sur votre routeur de la gamme RV34x.