

Configurez les paramètres de base de Pare-feu sur RV110W

Objectif

Un Pare-feu est un système de sécurité que les moniteurs et contrôle l'écoulement d'entrant et du trafic sortant au réseau utilisant des règles de sécurité configurées. Le Pare-feu sert de barrière entre un réseau interne de confiance et sécurisé et des réseaux non approuvés externes.

L'objectif de ce document est de t'afficher comment configurer des paramètres de base de Pare-feu sur le RV110W.

Remarque: Pour des configurations de configuration avancée (telles que des services spécifiques d'activation ou désactivation dans le Pare-feu), référez-vous à la [gestion des services de Pare-feu sur RV110W](#).

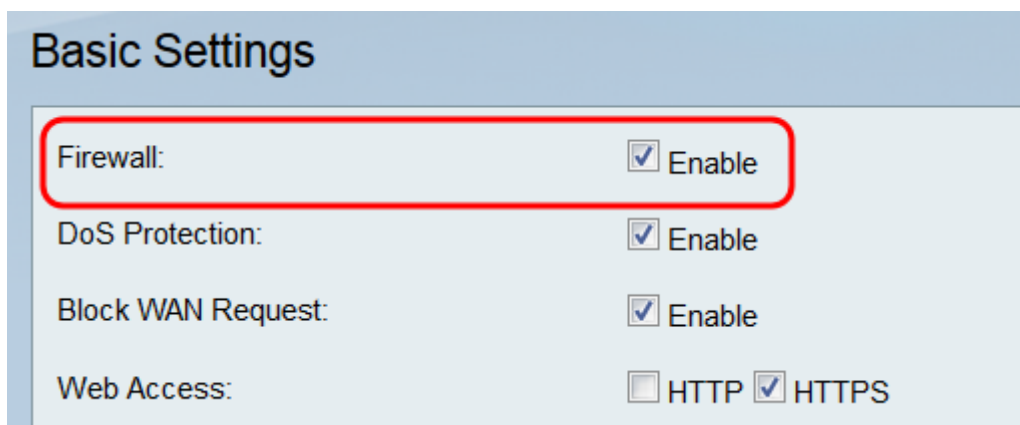
Périphériques applicables

- RV110W

Configuration de base de Pare-feu

Étape 1. Employez l'utilitaire de configuration Web pour choisir le **Pare-feu > les paramètres de base**. La page de *paramètres de base* paraît :

Étape 2. Dans le domaine de *Pare-feu*, cochez la case d'**enable** pour activer des paramètres du pare-feu.



The image shows a screenshot of a configuration interface titled "Basic Settings". It contains four rows of settings, each with a label on the left and a checkbox followed by the word "Enable" on the right. The "Firewall:" row is highlighted with a red rounded rectangle. The "DoS Protection:" row has a checked checkbox. The "Block WAN Request:" row has a checked checkbox. The "Web Access:" row has two checkboxes: "HTTP" (unchecked) and "HTTPS" (checked).

Setting	Enable
Firewall:	<input checked="" type="checkbox"/> Enable
DoS Protection:	<input checked="" type="checkbox"/> Enable
Block WAN Request:	<input checked="" type="checkbox"/> Enable
Web Access:	<input type="checkbox"/> HTTP <input checked="" type="checkbox"/> HTTPS

Étape 3. Dans le domaine de *protection DOS*, cochez la case d'**enable** pour protéger votre réseau contre des attaques du Déni de service (DOS).

Basic Settings

Firewall:	<input checked="" type="checkbox"/> Enable
DoS Protection:	<input checked="" type="checkbox"/> Enable
Block WAN Request:	<input checked="" type="checkbox"/> Enable
Web Access:	<input type="checkbox"/> HTTP <input checked="" type="checkbox"/> HTTPS

Étape 4. Dans le domaine *BLÈME de demande de bloc*, cochez la case d'**enable** pour refuser des requêtes pings au RV110W des réseaux externes.

Basic Settings

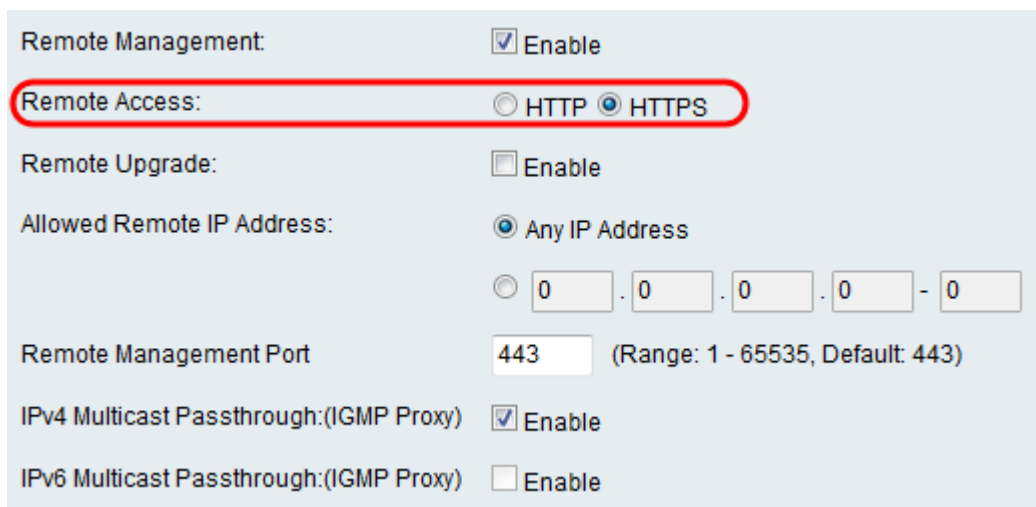
Firewall:	<input checked="" type="checkbox"/> Enable
DoS Protection:	<input checked="" type="checkbox"/> Enable
Block WAN Request:	<input checked="" type="checkbox"/> Enable
Web Access:	<input type="checkbox"/> HTTP <input checked="" type="checkbox"/> HTTPS

Étape 5. Dans le domaine d'*accès au Web*, cochez la case de **HTTP** et/ou la case **HTTPS** pour activer le trafic de ces protocoles. HTTPS est une version de HTTP qui chiffre des paquets pour la Sécurité accrue.

Étape 6. Dans le domaine de *gestion à distance*, cochez la case d'**enable** pour activer des configurations de gestion à distance.

Remarque: Si vous choisissez de ne pas activer la gestion à distance, ignorez à l'étape 11.

Étape 7. Dans le domaine d'*Accès à distance*, choisissez le type d'accès de Web utilisé pour se connecter au Pare-feu en cliquant sur la case d'option de **HTTP** ou la case d'option **HTTPS**. HTTPS chiffre des paquets pour la sécurité accrue.



Remote Management: Enable

Remote Access: HTTP HTTPS

Remote Upgrade: Enable

Allowed Remote IP Address: Any IP Address

0 . 0 . 0 . 0 - 0

Remote Management Port: 443 (Range: 1 - 65535, Default: 443)

IPv4 Multicast Passthrough:(IGMP Proxy) Enable

IPv6 Multicast Passthrough:(IGMP Proxy) Enable

Étape 8. Dans le domaine de *mise à niveau à distance*, cochez la case d'**enable** pour permettre le micrologiciel RV110W à mettre à jour à distance.

Remote Management:	<input checked="" type="checkbox"/> Enable
Remote Access:	<input type="radio"/> HTTP <input checked="" type="radio"/> HTTPS
Remote Upgrade:	<input checked="" type="checkbox"/> Enable
Allowed Remote IP Address:	<input checked="" type="radio"/> Any IP Address <input type="radio"/> 0 . 0 . 0 . 0 - 0
Remote Management Port	443 (Range: 1 - 65535, Default: 443)
IPv4 Multicast Passthrough:(IGMP Proxy)	<input checked="" type="checkbox"/> Enable
IPv6 Multicast Passthrough:(IGMP Proxy)	<input type="checkbox"/> Enable

Étape 9. Dans le *champ IP Address distant permis*, cliquez sur la **n'importe quelle** case d'option d'**adresse IP** pour permettre des mises à niveau à distance au routeur de n'importe quel IP, ou cliquez sur la case d'option dessous pour écrire une plage des adresses IP qui sont permises pour promouvoir à distance le routeur dans les domaines vers la droite.

Remote Management:	<input checked="" type="checkbox"/> Enable
Remote Access:	<input type="radio"/> HTTP <input checked="" type="radio"/> HTTPS
Remote Upgrade:	<input checked="" type="checkbox"/> Enable
Allowed Remote IP Address:	<input checked="" type="radio"/> Any IP Address <input type="radio"/> 0 . 0 . 0 . 0 - 0
Remote Management Port	443 (Range: 1 - 65535, Default: 443)
IPv4 Multicast Passthrough:(IGMP Proxy)	<input checked="" type="checkbox"/> Enable
IPv6 Multicast Passthrough:(IGMP Proxy)	<input type="checkbox"/> Enable

Étape 10. Dans le domaine de *port de gestion à distance*, écrivez le port ou la plage de port sur lesquels on permet la gestion à distance.

Remote Management:	<input checked="" type="checkbox"/> Enable
Remote Access:	<input type="radio"/> HTTP <input checked="" type="radio"/> HTTPS
Remote Upgrade:	<input checked="" type="checkbox"/> Enable
Allowed Remote IP Address:	<input checked="" type="radio"/> Any IP Address <input type="radio"/> 0 . 0 . 0 . 0 - 0
Remote Management Port	443 (Range: 1 - 65535, Default: 443)
IPv4 Multicast Passthrough:(IGMP Proxy)	<input checked="" type="checkbox"/> Enable
IPv6 Multicast Passthrough:(IGMP Proxy)	<input type="checkbox"/> Enable

Étape 11. Dans la *fonction émulation de Multidiffusion d'ipv4 : (Proxy IGMP)* mettez en place, cochez la case d'**enable** pour activer la fonction émulation de Multidiffusion pour l'ipv4.

IPv4 Multicast Passthrough:(IGMP Proxy)	<input checked="" type="checkbox"/> Enable
IPv6 Multicast Passthrough:(IGMP Proxy)	<input type="checkbox"/> Enable
<hr/>	
UPnP	<input checked="" type="checkbox"/> Enable
Allow Users to Configure	<input checked="" type="checkbox"/> Enable
Allow Users to Disable Internet Access	<input type="checkbox"/> Enable
<hr/>	
Block Java:	<input type="checkbox"/> <input checked="" type="radio"/> Auto <input type="radio"/> Manual Port: <input type="text"/>
Block Cookies:	<input type="checkbox"/> <input checked="" type="radio"/> Auto <input type="radio"/> Manual Port: <input type="text"/>
Block ActiveX:	<input type="checkbox"/> <input checked="" type="radio"/> Auto <input type="radio"/> Manual Port: <input type="text"/>
Block Proxy:	<input type="checkbox"/> <input checked="" type="radio"/> Auto <input type="radio"/> Manual Port: <input type="text"/>

Étape 12. Dans la *fonction émulation de Multidiffusion IPv6 : (Proxy IGMP)* mettez en place, cochez la case d'**enable** pour activer la fonction émulation de Multidiffusion pour l'IPv6.

IPv4 Multicast Passthrough:(IGMP Proxy)	<input checked="" type="checkbox"/> Enable
IPv6 Multicast Passthrough:(IGMP Proxy)	<input checked="" type="checkbox"/> Enable
<hr/>	
UPnP	<input checked="" type="checkbox"/> Enable
Allow Users to Configure	<input checked="" type="checkbox"/> Enable
Allow Users to Disable Internet Access	<input type="checkbox"/> Enable
<hr/>	
Block Java:	<input type="checkbox"/> <input checked="" type="radio"/> Auto <input type="radio"/> Manual Port: <input type="text"/>
Block Cookies:	<input type="checkbox"/> <input checked="" type="radio"/> Auto <input type="radio"/> Manual Port: <input type="text"/>
Block ActiveX:	<input type="checkbox"/> <input checked="" type="radio"/> Auto <input type="radio"/> Manual Port: <input type="text"/>
Block Proxy:	<input type="checkbox"/> <input checked="" type="radio"/> Auto <input type="radio"/> Manual Port: <input type="text"/>

Remarque: Vous pouvez seulement activer cette option si le périphérique est configuré pour fonctionner en mode d'IPv6 à la page de **réseau > de mode IP**.

Étape 13. Dans le domaine *UPnP*, cochez la case d'**enable** pour activer l'Universal Plug and Play (UPnP) qui permet la détection automatique des périphériques qui peuvent se connecter au routeur.

IPv4 Multicast Passthrough:(IGMP Proxy)	<input checked="" type="checkbox"/> Enable
IPv6 Multicast Passthrough:(IGMP Proxy)	<input checked="" type="checkbox"/> Enable
UPnP	<input checked="" type="checkbox"/> Enable
Allow Users to Configure	<input checked="" type="checkbox"/> Enable
Allow Users to Disable Internet Access	<input type="checkbox"/> Enable
Block Java:	<input type="checkbox"/> <input checked="" type="radio"/> Auto <input type="radio"/> Manual Port: <input type="text"/>
Block Cookies:	<input type="checkbox"/> <input checked="" type="radio"/> Auto <input type="radio"/> Manual Port: <input type="text"/>
Block ActiveX:	<input type="checkbox"/> <input checked="" type="radio"/> Auto <input type="radio"/> Manual Port: <input type="text"/>
Block Proxy:	<input type="checkbox"/> <input checked="" type="radio"/> Auto <input type="radio"/> Manual Port: <input type="text"/>

Remarque: Si vous choisissez de ne pas activer l'UPnP, ignorez à l'étape 16.

Étape 14. Dans l'utilisateur d'autoriser pour configurer le champ, cochez la case d'**enable** pour permettre à des utilisateurs pour placer les règles O. de mappage de ports.

UPnP	<input checked="" type="checkbox"/> Enable
Allow Users to Configure	<input type="checkbox"/> Enable
Allow Users to Disable Internet Access	<input type="checkbox"/> Enable
Block Java:	<input type="checkbox"/> <input checked="" type="radio"/> Auto <input type="radio"/> Manual Port: <input type="text"/>
Block Cookies:	<input type="checkbox"/> <input checked="" type="radio"/> Auto <input type="radio"/> Manual Port: <input type="text"/>
Block ActiveX:	<input type="checkbox"/> <input checked="" type="radio"/> Auto <input type="radio"/> Manual Port: <input type="text"/>
Block Proxy:	<input type="checkbox"/> <input checked="" type="radio"/> Auto <input type="radio"/> Manual Port: <input type="text"/>

Save Cancel

Étape 15. Dans les *utilisateurs d'autoriser pour désactiver le champ d'accès Internet*, cochez la case d'**enable** pour permettre à des utilisateurs pour désactiver l'accès Internet.

UPnP	<input checked="" type="checkbox"/> Enable
Allow Users to Configure	<input checked="" type="checkbox"/> Enable
Allow Users to Disable Internet Access	<input type="checkbox"/> Enable
<hr/>	
Block Java:	<input type="checkbox"/> <input checked="" type="radio"/> Auto <input type="radio"/> Manual Port: <input type="text"/>
Block Cookies:	<input type="checkbox"/> <input checked="" type="radio"/> Auto <input type="radio"/> Manual Port: <input type="text"/>
Block ActiveX:	<input type="checkbox"/> <input checked="" type="radio"/> Auto <input type="radio"/> Manual Port: <input type="text"/>
Block Proxy:	<input type="checkbox"/> <input checked="" type="radio"/> Auto <input type="radio"/> Manual Port: <input type="text"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

Étape 16. Dans le *bloc Javas* mettent en place, cochant la case d'**enable** si vous voudriez bloquer des applet Java. Prochain clic la case d'option **automatique** pour bloquer Javas sur tous les ports, ou pour cliquer sur la case d'option **manuelle** pour introduire le numéro de port dans le domaine de *port* sur lequel pour bloquer Javas.

UPnP	<input checked="" type="checkbox"/> Enable
Allow Users to Configure	<input checked="" type="checkbox"/> Enable
Allow Users to Disable Internet Access	<input type="checkbox"/> Enable
<hr/>	
Block Java:	<input type="checkbox"/> <input checked="" type="radio"/> Auto <input type="radio"/> Manual Port: <input type="text"/>
Block Cookies:	<input checked="" type="checkbox"/> <input checked="" type="radio"/> Auto <input type="radio"/> Manual Port: <input type="text"/>
Block ActiveX:	<input checked="" type="checkbox"/> <input type="radio"/> Auto <input checked="" type="radio"/> Manual Port: <input type="text" value="80"/>
Block Proxy:	<input type="checkbox"/> <input checked="" type="radio"/> Auto <input type="radio"/> Manual Port: <input type="text"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

Étape 17. Dans le *bloc les Témoins* mettent en place, cochant la case d'**enable** si vous voudriez bloquer des Témoins. Prochain clic la case d'option **automatique** pour bloquer des Témoins sur tous les ports, ou pour cliquer sur la case d'option **manuelle** pour introduire le numéro de port dans le domaine de *port* sur lequel pour bloquer des Témoins.

The screenshot shows the Windows Firewall settings for blocking ActiveX content. The 'Block ActiveX' section is highlighted with a red rectangle. The 'Enable' checkbox is checked, and the 'Manual' radio button is selected, with the port number '80' entered in the adjacent text box. Other settings include 'UPnP' (checked), 'Allow Users to Configure' (checked), and 'Allow Users to Disable Internet Access' (unchecked). The 'Block Java' and 'Block Proxy' sections are also visible, both with 'Auto' selected. The 'Block Cookies' section is also highlighted with a red rectangle, with 'Auto' selected.

UPnP	<input checked="" type="checkbox"/> Enable
Allow Users to Configure	<input checked="" type="checkbox"/> Enable
Allow Users to Disable Internet Access	<input type="checkbox"/> Enable
Block Java:	<input type="checkbox"/> <input checked="" type="radio"/> Auto <input type="radio"/> Manual Port: <input type="text"/>
Block Cookies:	<input checked="" type="checkbox"/> <input checked="" type="radio"/> Auto <input type="radio"/> Manual Port: <input type="text"/>
Block ActiveX:	<input checked="" type="checkbox"/> <input type="radio"/> Auto <input checked="" type="radio"/> Manual Port: 80
Block Proxy:	<input type="checkbox"/> <input checked="" type="radio"/> Auto <input type="radio"/> Manual Port: <input type="text"/>

Save Cancel

Étape 18. Dans le domaine d'*ActiveX de bloc*, cochez la case d'**enable** si vous voudriez bloquer le contenu d'ActiveX. Prochain clic la case d'option **automatique** pour bloquer le contenu d'ActiveX sur tous les ports, ou pour cliquer sur la case d'option **manuelle** pour introduire le numéro de port dans le domaine de *port* sur lequel pour bloquer ActiveX contentez.

The screenshot shows the Windows Firewall settings for blocking proxy servers. The 'Block Proxy' section is highlighted with a red rectangle. The 'Enable' checkbox is checked, and the 'Manual' radio button is selected, with the port number '80' entered in the adjacent text box. Other settings include 'UPnP' (checked), 'Allow Users to Configure' (checked), and 'Allow Users to Disable Internet Access' (unchecked). The 'Block Java' and 'Block Cookies' sections are also visible, both with 'Auto' selected.

UPnP	<input checked="" type="checkbox"/> Enable
Allow Users to Configure	<input checked="" type="checkbox"/> Enable
Allow Users to Disable Internet Access	<input type="checkbox"/> Enable
Block Java:	<input type="checkbox"/> <input checked="" type="radio"/> Auto <input type="radio"/> Manual Port: <input type="text"/>
Block Cookies:	<input checked="" type="checkbox"/> <input checked="" type="radio"/> Auto <input type="radio"/> Manual Port: <input type="text"/>
Block ActiveX:	<input checked="" type="checkbox"/> <input type="radio"/> Auto <input checked="" type="radio"/> Manual Port: 80
Block Proxy:	<input type="checkbox"/> <input checked="" type="radio"/> Auto <input type="radio"/> Manual Port: <input type="text"/>

Save Cancel

Étape 19. Dans le domaine de *proxy de bloc*, cochez la case d'**enable** pour bloquer des serveurs proxys. Prochain clic la case d'option automatique pour bloquer des serveurs proxys sur tous les ports, ou pour cliquer sur la case d'option manuelle pour introduire le numéro de port dans le domaine de port sur lequel pour bloquer des serveurs proxys.

UPnP	<input checked="" type="checkbox"/> Enable
Allow Users to Configure	<input checked="" type="checkbox"/> Enable
Allow Users to Disable Internet Access	<input type="checkbox"/> Enable
<hr/>	
Block Java:	<input type="checkbox"/> <input checked="" type="radio"/> Auto <input type="radio"/> Manual Port: <input type="text"/>
Block Cookies:	<input checked="" type="checkbox"/> <input checked="" type="radio"/> Auto <input type="radio"/> Manual Port: <input type="text"/>
Block ActiveX:	<input checked="" type="checkbox"/> <input type="radio"/> Auto <input checked="" type="radio"/> Manual Port: <input type="text" value="80"/>
Block Proxy:	<input type="checkbox"/> <input checked="" type="radio"/> Auto <input type="radio"/> Manual Port: <input type="text"/>
<hr/>	
<input type="button" value="Save"/>	<input type="button" value="Cancel"/>

Étape 20. **Sauvegarde de** clic pour sauvegarder des modifications ou **à annuler** pour les jeter.