

Configuration des stratégies de groupe sur le routeur de la gamme RV34x

Objectif

Une stratégie de groupe est un ensemble de paires d'attributs ou de valeurs orientées utilisateur pour les connexions IPSec (Internet Protocol Security) stockées en interne (localement) sur le périphérique ou en externe sur un serveur RADIUS (Remote Authentication Dial-In User Service) ou LDAP (Lightweight Directory Access Protocol). Un groupe de tunnels utilise une stratégie de groupe qui définit les termes des connexions utilisateur VPN après l'établissement du tunnel.

Les stratégies de groupe vous permettent d'appliquer des ensembles entiers d'attributs à un utilisateur ou à un groupe d'utilisateurs, plutôt que de devoir spécifier chaque attribut individuellement pour chaque utilisateur. Vous pouvez également modifier les attributs de stratégie de groupe pour un utilisateur spécifique.

L'objectif de ce document est de vous montrer comment configurer les stratégies de groupe sur la gamme de routeurs VPN RV34x.

Périphériques pertinents

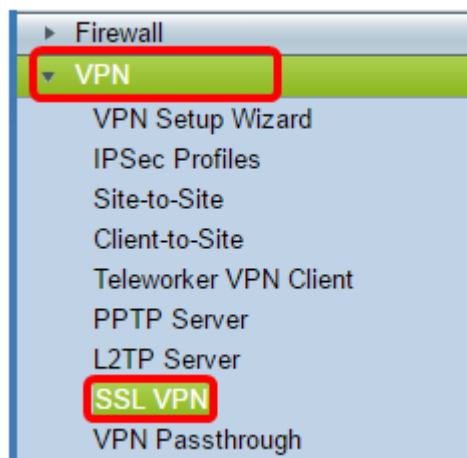
- Gamme RV34x

Version du logiciel

- 1.0.01.16

Configurer les stratégies de groupe

Étape 1. Connectez-vous à l'utilitaire Web du routeur et choisissez **VPN > SSL VPN**.



Étape 2. Sous la zone VPN SSL, cliquez sur l'onglet **Stratégies de groupe**.

SSL VPN

General Configuration

Group Policies

Étape 3. Cliquez sur le bouton **Add** sous la table de groupe VPN SSL pour ajouter une stratégie de groupe.

SSL VPN Group Table	
<input type="checkbox"/>	Policy Name
<input type="checkbox"/>	SSLVPNDefaultPolicy
<input type="button" value="Add"/>	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Note: Le tableau Groupe VPN SSL affiche la liste des stratégies de groupe sur le périphérique. Vous pouvez également modifier la première stratégie de groupe de la liste, nommée SSLVPNDefaultPolicy. Il s'agit de la stratégie par défaut fournie par le périphérique.

Étape 4. Entrez le nom de stratégie préféré dans le champ *Nom de la stratégie*.

SSL VPN	
General Configuration	Group Policies
SSLVPN Group Policy - Add/Edit	
Basic Settings	
Policy Name:	<input type="text" value="Group 1 Policy"/>
Primary DNS:	<input type="text" value="192.168.1.1"/>
Secondary DNS:	<input type="text"/>
Primary WINS:	<input type="text"/>
Secondary WINS:	<input type="text"/>

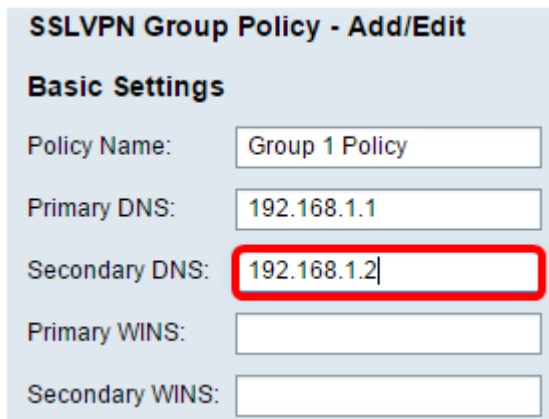
Note: Dans cet exemple, la stratégie de groupe 1 est utilisée.

Étape 5. Saisissez l'adresse IP du DNS principal dans le champ fourni. Par défaut, cette adresse IP est déjà fournie.

SSLVPN Group Policy - Add/Edit	
Basic Settings	
Policy Name:	<input type="text" value="Group 1 Policy"/>
Primary DNS:	<input type="text" value="192.168.1.1"/>
Secondary DNS:	<input type="text"/>
Primary WINS:	<input type="text"/>
Secondary WINS:	<input type="text"/>

Note: Dans cet exemple, 192.168.1.1 est utilisé.

Étape 6. (Facultatif) Saisissez l'adresse IP du DNS secondaire dans le champ fourni. Cela servira de sauvegarde en cas d'échec du DNS principal.



SSLVPN Group Policy - Add/Edit

Basic Settings

Policy Name:

Primary DNS:

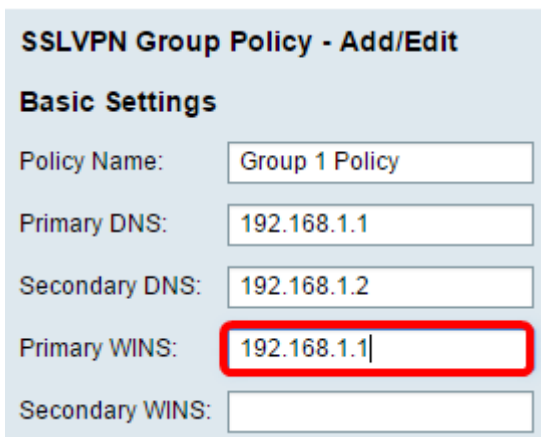
Secondary DNS:

Primary WINS:

Secondary WINS:

Note: Dans cet exemple, 192.168.1.2 est utilisé.

Étape 7. (Facultatif) Saisissez l'adresse IP du WINS principal dans le champ fourni.



SSLVPN Group Policy - Add/Edit

Basic Settings

Policy Name:

Primary DNS:

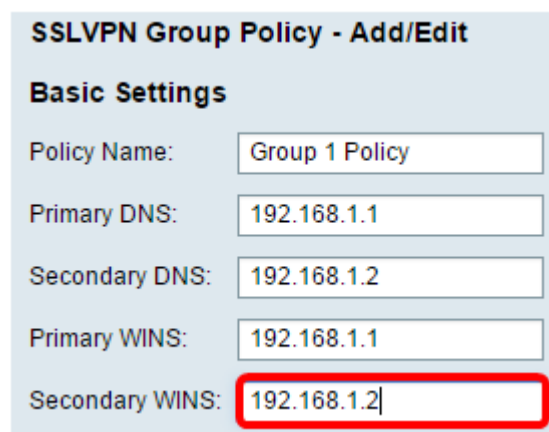
Secondary DNS:

Primary WINS:

Secondary WINS:

Note: Dans cet exemple, 192.168.1.1 est utilisé.

Étape 8. (Facultatif) Saisissez l'adresse IP du WINS secondaire dans le champ fourni.



SSLVPN Group Policy - Add/Edit

Basic Settings

Policy Name:

Primary DNS:

Secondary DNS:

Primary WINS:

Secondary WINS:

Note: Dans cet exemple, 192.168.1.2 est utilisé.

Étape 9. (Facultatif) Entrez une description de la stratégie dans le champ *Description*.

SSLVPN Group Policy - Add/Edit

Basic Settings

Policy Name:

Primary DNS:

Secondary DNS:

Primary WINS:

Secondary WINS:

Description:

Note: Dans cet exemple, la stratégie de groupe avec tunnel partagé est utilisée.

Étape 10. (Facultatif) Cliquez sur une case d'option pour sélectionner la stratégie de proxy IE pour activer les paramètres de proxy Microsoft Internet Explorer (MSIE) pour établir un tunnel VPN. Les options sont les suivantes :

- None : permet au navigateur d'utiliser aucun paramètre de proxy.
- Auto : permet au navigateur de détecter automatiquement les paramètres du proxy.
- Bypass-local : permet au navigateur de contourner les paramètres de proxy configurés sur l'utilisateur distant.
- Disabled : désactive les paramètres du proxy MSIE.

IE Proxy Settings

IE Proxy Policy None Auto Bypass-local Disabled

Note: Dans cet exemple, Désactivé est sélectionné. Voici la configuration par défaut .

Étape 11. (Facultatif) Dans la zone Split Tunneling Settings, cochez la case **Enable Split Tunneling** pour permettre au trafic destiné à Internet d'être envoyé sans cryptage directement à Internet. La transmission tunnel complète envoie tout le trafic vers le périphérique final où il est ensuite acheminé vers les ressources de destination, éliminant ainsi le réseau d'entreprise du chemin d'accès Web.

IE Proxy Settings

IE Proxy Policy None Auto Bypass-local Disabled

Split Tunneling Settings

Enable Split Tunneling

Étape 12. (Facultatif) Cliquez sur une case d'option pour choisir d'inclure ou d'exclure le trafic lors de l'application de la tunnellation fractionnée.

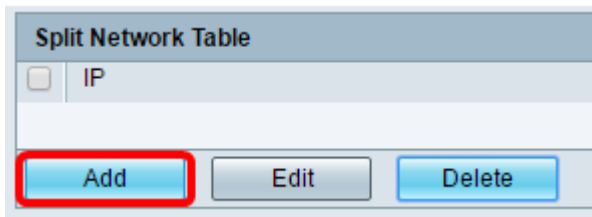
Split Tunneling Settings

Enable Split Tunneling

Split Selection Include Traffic Exclude Traffic

Note: Dans cet exemple, Inclure le trafic est sélectionné.

Étape 13. Dans la table Réseau divisé, cliquez sur le bouton **Ajouter** pour ajouter une exception Réseau fractionné.

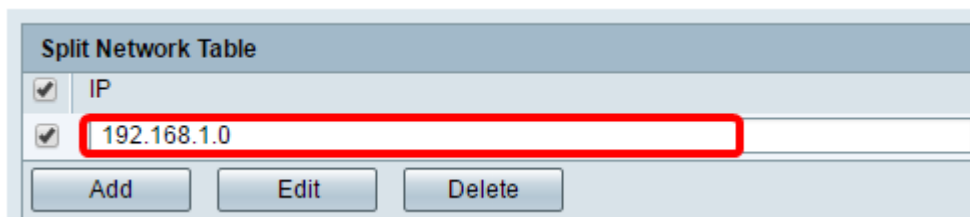


Split Network Table

<input type="checkbox"/>	IP
<input type="checkbox"/>	

Add Edit Delete

Étape 14. Saisissez l'adresse IP du réseau dans le champ prévu à cet effet.



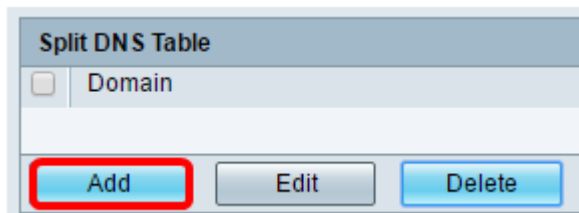
Split Network Table

<input checked="" type="checkbox"/>	IP
<input checked="" type="checkbox"/>	192.168.1.0

Add Edit Delete

Note: Dans cet exemple, 192.168.1.0 est utilisé.

Étape 15. Dans la table DNS fractionnée, cliquez sur le bouton **Add** pour ajouter une exception DNS fractionnée.

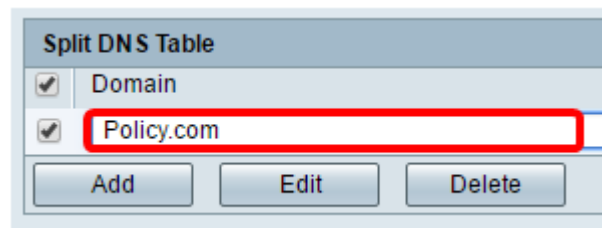


Split DNS Table

<input type="checkbox"/>	Domain
<input type="checkbox"/>	

Add Edit Delete

Étape 16. Saisissez le nom de domaine dans le champ fourni.



Split DNS Table

<input checked="" type="checkbox"/>	Domain
<input checked="" type="checkbox"/>	Policy.com

Add Edit Delete

Note: Dans cet exemple, Policy.com est utilisé.

Étape 17. Cliquez sur Apply.

Split DNS Table	
<input checked="" type="checkbox"/>	Domain
<input checked="" type="checkbox"/>	Policy.com

Add Edit Delete

Apply Cancel

Une fois les paramètres enregistrés, vous serez redirigé vers la table de groupe VPN SSL affichant la stratégie de groupe récemment ajoutée.

General Configuration Group Policies

SSL VPN Group Table	
Policy Name	Description
<input type="checkbox"/> Group 1 Policy	Group Policy with Split Tunneling
<input type="checkbox"/> SSLVPNDefaultPolicy	

Add Edit Delete

Apply Cancel

Vous devez maintenant avoir correctement configuré les stratégies de groupe sur le routeur de la gamme RV34x.

Si vous souhaitez consulter le Guide d'installation rapide du routeur RV340. cliquez [ici](#).

Si vous souhaitez consulter le Guide d'administration du routeur RV340. cliquez [ici](#). Les informations sur les stratégies de groupe se trouvent à la page 93.