Configurez le réseau privé virtuel de Secure Sockets Layer (VPN SSL) sur le routeur RV340 ou RV345

Avis spécial : Structure d'autorisation - Versions 1.0.3.15 et ultérieures de micrologiciels. Avançant, AnyConnect occasionnera des frais pour des permis de client seulement.

Pour des informations supplémentaires sur AnyConnect autorisant sur les Routeurs de gamme RV340, vérifiez l'article AnyConnect autorisant pour les Routeurs de gamme RV340.

Objectif

La passerelle de réseau privé virtuel de Secure Sockets Layer (VPN SSL) permet à des utilisateurs distants pour établir un tunnel VPN sécurisé utilisant un navigateur Web. Cette caractéristique permet l'accès facile à un large éventail de ressources web et les applications Web-activées utilisant le Protocole HTTP (Hypertext Transfer Protocol) indigène au-dessus de l'hypertexte Transfer Protocol SSL sécurisent la prise en charge du navigateur (HTTPS).

Le VPN SSL permet à des utilisateurs pour accéder à distance les réseaux restreints, utilisant une voie sécurisée et authentifiée en chiffrant le trafic réseau.

Les Routeurs RV340 et RV345 prennent en charge le Cisco AnyConnect VPN Client, ou également connu en tant que client sécurisé de mobilité d'Anyconnect. Ces Routeurs prennent en charge deux tunnels de VPN SSL par défaut, et l'utilisateur peut enregistrer un permis de prendre en charge jusqu'à 50 tunnels. Une fois qu'installé et lancé, le VPN SSL établira un sécurisé, tunnel VPN de remote-access.

Ce buts de l'article de t'afficher comment configurer le VPN SSL sur le RV340 ou le routeur RV345.

Périphériques applicables

- RV340
- RV345
- Client Cisco Secure de mobilité

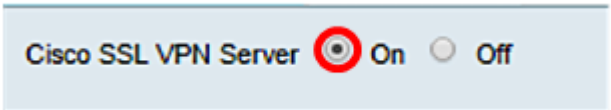
Version de logiciel

- 1.0.03.15 — RV340, RV345
- 4.4.01054 — Client sécurisé de mobilité d'AnyConnect

Configurez le VPN SSL

Étape 1. Accédez à l'utilitaire basé sur le WEB de routeur et choisissez **VPN > VPN SSL**.

Étape 2. Cliquez sur **en fonction la** case d'option pour activer le serveur de VPN SSL de Cisco.

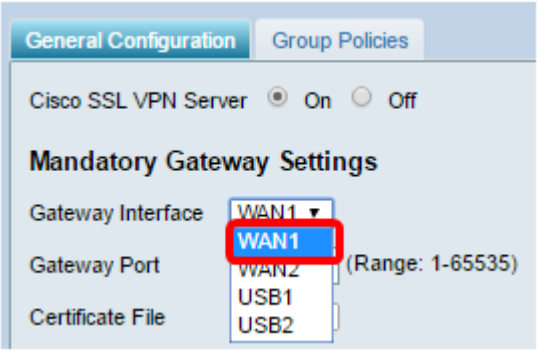


Paramètres de passerelle obligatoires

Les paramètres de configuration suivants sont obligatoires :

Étape 3. Choisissez l'interface de passerelle de la liste déroulante. Ce sera le port qui sera utilisé pour passer le trafic par les tunnels de VPN SSL. Les options sont :

- WAN1
- WAN2
- USB1
- USB2

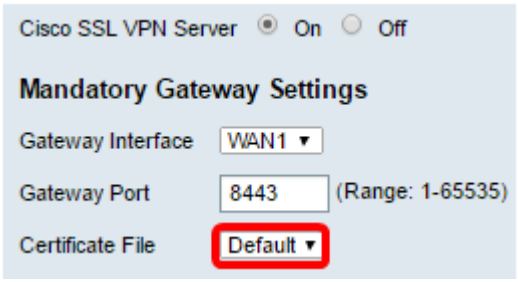


Remarque: Dans cet exemple, WAN1 est choisi.

Étape 4. Introduisez le numéro de port qui est utilisé pour la passerelle de VPN SSL dans le domaine de *port de passerelle* s'étendant de 1 à 65535.

Remarque: Dans cet exemple, 8443 est utilisés comme numéro de port.

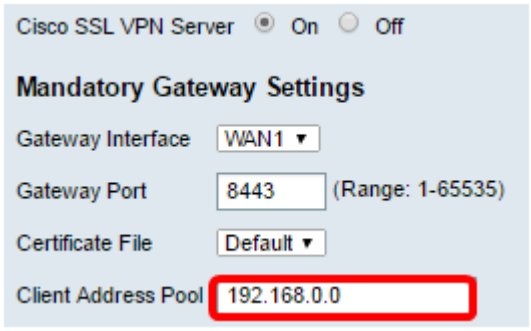
Étape 5. Choisissez le fichier du certificat de la liste déroulante. Ce certificat authentifie les utilisateurs qui tentent d'accéder à la ressource de réseau par les tunnels de VPN SSL. La liste déroulante contient un certificat par défaut et les Certificats qui sont importés.



Remarque: Dans cet exemple, le par défaut est choisi.

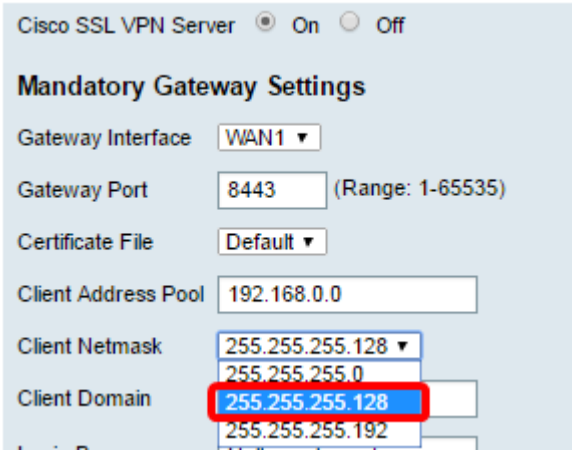
Étape 6. Écrivez l'adresse IP du groupe d'adresse du client dans le domaine de *groupe d'adresse du client*. Ce groupe sera la plage des adresses IP qui seront allouées aux clients vpn distants.

Remarque: Assurez-vous que la plage d'adresses IP ne superpose pas avec les adresses IP l'unes des sur le réseau local.



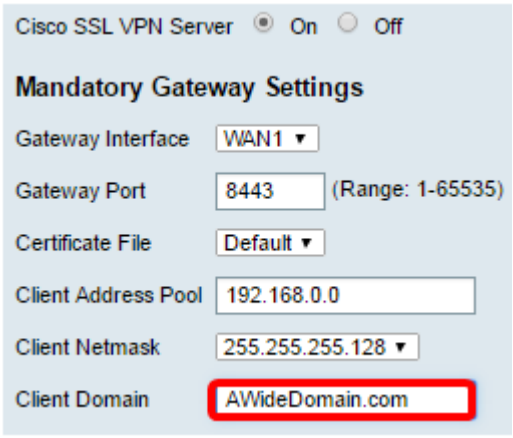
Remarque: Dans cet exemple, 192.168.0.0 est utilisé.

Étape 7. Choisissez le netmask de client de la liste déroulante.



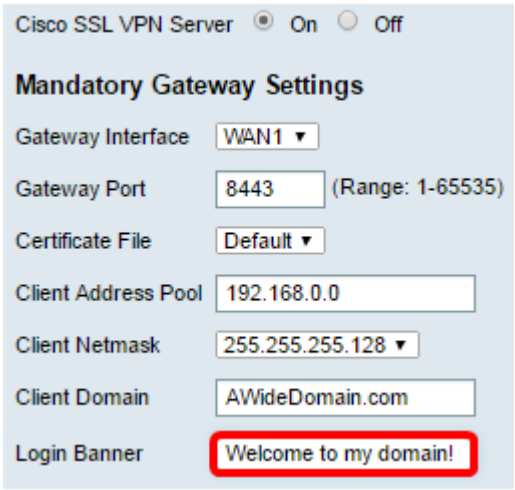
Remarque: Dans cet exemple, 255.255.255.128 est choisi.

Étape 8. Écrivez le nom de domaine de client dans le *champ Domain de client*. Ce sera le nom de domaine qui devrait être poussé aux clients de VPN SSL.



Remarque: Dans cet exemple, AWideDomain est utilisé comme nom de domaine de client.

Étape 9. Entrez dans le texte qui paraîtrait comme bannière de procédure de connexion dans le domaine de *bannière de procédure de connexion*. Ce sera la bannière qui sera chaque fois affichés les logins d'un client.



Remarque: Dans cet exemple, accueil à mon domaine ! est utilisé comme bannière de procédure de connexion.

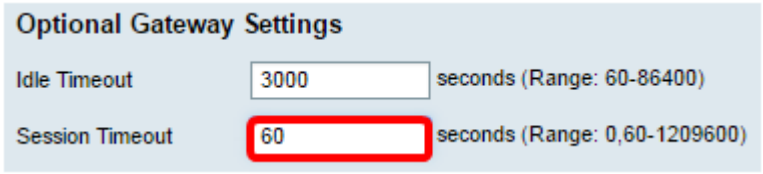
Paramètres de passerelle facultatifs

Les paramètres de configuration suivants sont facultatifs :

Étape 1. Écrivez une valeur en quelques secondes pour le délai d'attente de veille s'étendant de 60 à 86400. Ce sera la durée de temps que la session de VPN SSL peut demeurer de veille.

Remarque: Dans cet exemple, 3000 est utilisés.

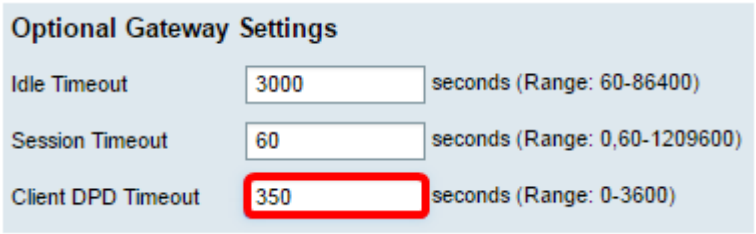
Étape 2. Écrivez une valeur en quelques secondes dans le domaine de *Session Timeout*. C'est le temps où il prend pour que la session de Protocole TCP (Transmission Control Protocol) ou de Protocole UDP (User Datagram Protocol) chronomètre après le temps d'inactivité spécifié. La plage est de 60 à 1209600.



Remarque: Dans cet exemple, 60 est utilisés.

Étape 3. Écrivez une valeur en quelques secondes dans le domaine de *délai d'attente de ClientDPD* s'étendant de 0 à 3600. Cette valeur spécifie l'envoi périodique des messages HELLO/ACK pour vérifier le statut du tunnel VPN.

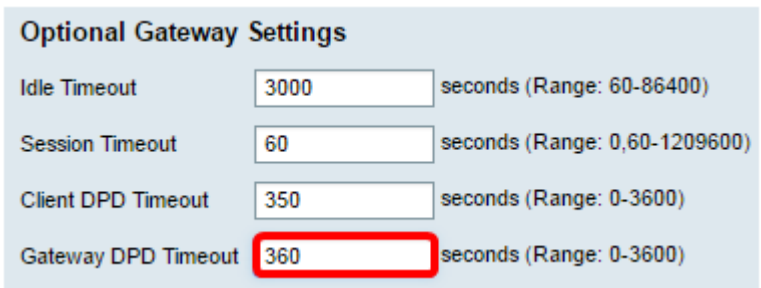
Remarque: Cette caractéristique doit être activée sur les deux extrémités du tunnel VPN.



Remarque: Dans cet exemple, 350 est utilisés.

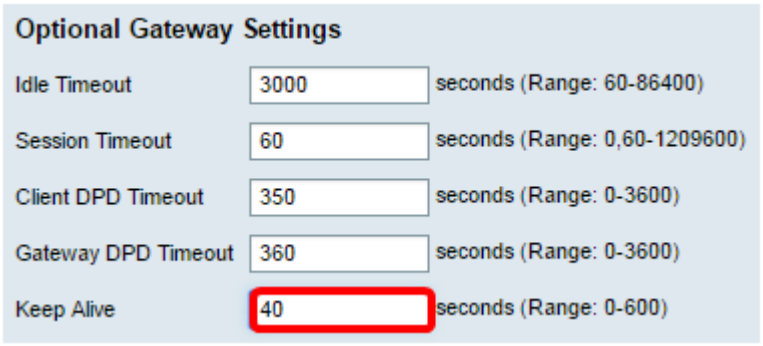
Étape 4. Écrivez une valeur en quelques secondes dans le domaine de *délai d'attente de GatewayDPD* s'étendant de 0 à 3600. Cette valeur spécifie l'envoi périodique des messages HELLO/ACK pour vérifier le statut du tunnel VPN.

Remarque: Cette caractéristique doit être activée sur les deux extrémités du tunnel VPN.



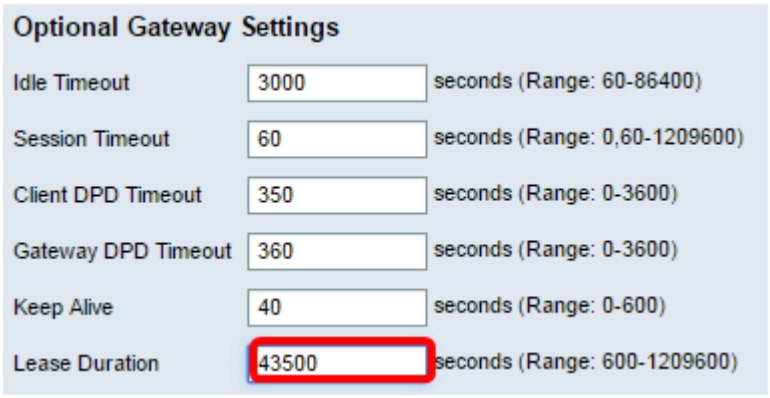
Remarque: Dans cet exemple, 360 est utilisés.

Étape 5. Écrivez une valeur en quelques secondes dans le domaine de *keepalive* s'étendant de 0 à 600. Cette caractéristique s'assure que votre routeur est toujours connecté à l'Internet. Il tentera de rétablir la connexion VPN s'il est relâché.



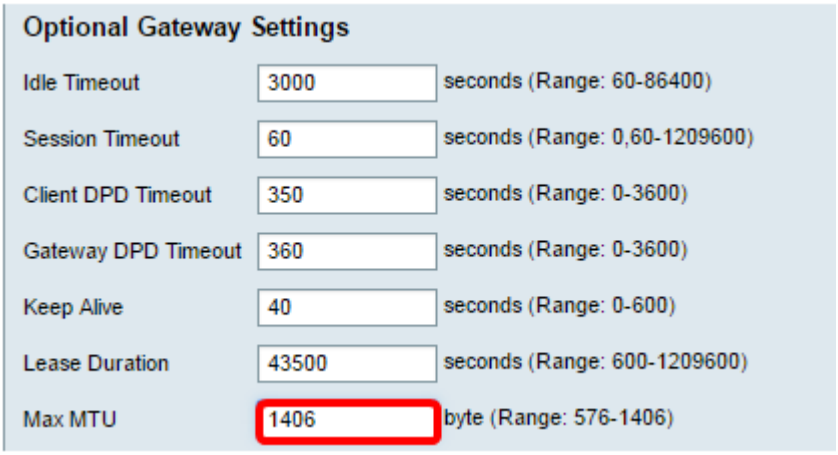
Remarque: Dans cet exemple, 40 est utilisés.

Étape 6. Écrivez une valeur en quelques secondes pour la durée du tunnel à connecter dans le domaine de *durée de bail*. La plage est de 600 à 1209600.



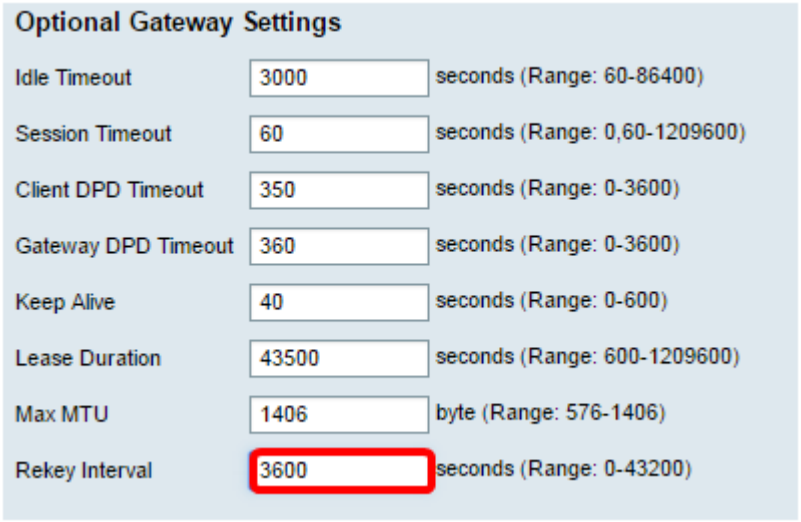
Remarque: Dans cet exemple, 43500 est utilisés.

Étape 7. Écrivez la longueur de paquet dans les octets qui peuvent être envoyés au-dessus du réseau. La plage est de est de 576 à 1406.



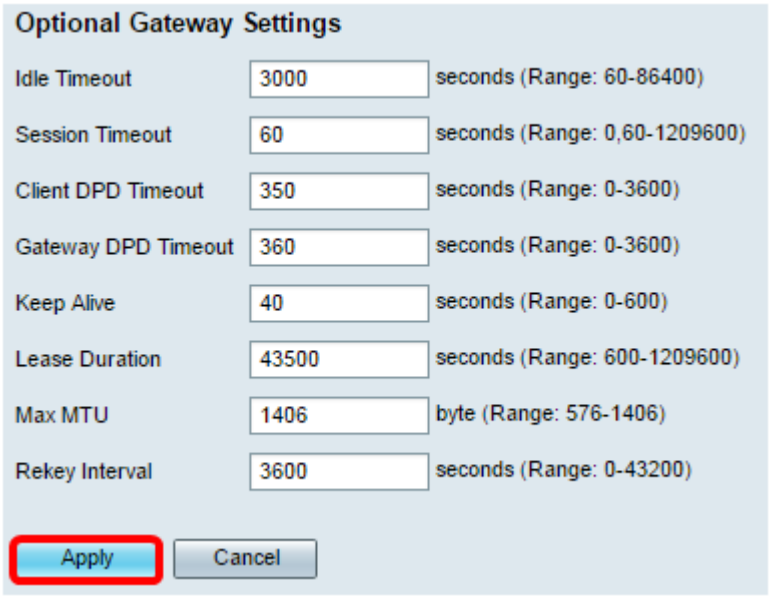
Remarque: Dans cet exemple, 1406 est utilisés.

Étape 8. Écrivez l'intervalle de relais dans le domaine d'*intervalle de rekey*. La caractéristique de rekey permet aux clés SSL pour renégocier après que la session ait été établie. La plage est de 0 à 43200.



Remarque: Dans cet exemple, 3600 est utilisés.

Étape 9. Cliquez sur Apply.



Étape 10. (facultative) pour sauvegarder de manière permanente la configuration, cliquent sur en fonction l'icône 

de clignotement.

Vous devriez avoir maintenant avec succès configuré le VPN SSL sur votre routeur RV34x.