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

Avis spécial : Structure des licences - Microprogramme versions 1.0.3.15 et ultérieures. À l'avenir, AnyConnect ne facturera que les licences client.

Pour plus d'informations sur les licences AnyConnect sur les routeurs de la gamme RV340, consultez l'article Licences AnyConnect pour les routeurs de la gamme RV340.

Objectif

La passerelle VPN SSL (Secure Sockets Layer Virtual Private Network) permet aux utilisateurs distants d'établir un tunnel VPN sécurisé à l'aide d'un navigateur Web. Cette fonctionnalité permet d'accéder facilement à un large éventail de ressources Web et d'applications Web à l'aide du support de navigateur HTTP (Hypertext Transfer Protocol) natif sur SSL HTTPS (Hypertext Transfer Protocol Secure).

Le VPN SSL permet aux utilisateurs d'accéder à distance à des réseaux restreints, en utilisant un chemin sécurisé et authentifié en chiffrant le trafic réseau.

Les routeurs RV340 et RV345 prennent en charge le client VPN Cisco AnyConnect, également appelé client AnyConnect Secure Mobility. Ces routeurs prennent en charge deux tunnels VPN SSL par défaut, et l'utilisateur peut enregistrer une licence pour prendre en charge jusqu'à 50 tunnels. Une fois installé et activé, le VPN SSL établit un tunnel VPN d'accès à distance sécurisé.

Cet article vise à vous montrer comment configurer le VPN SSL sur le routeur RV340 ou RV345.

Périphériques pertinents

- RV340
- RV345
- Client Cisco Secure Mobility

Version du logiciel

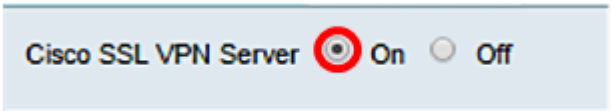
- 1.0.03.15 — RV340, RV345
- 4.4.01054 — Client AnyConnect Secure Mobility

Configurer le VPN SSL

Étape 1. Accédez à l'utilitaire Web du routeur et choisissez VPN > SSL VPN.



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



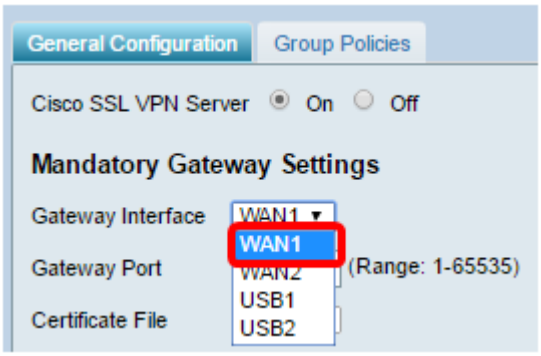
Paramètres de passerelle obligatoires

Les paramètres de configuration suivants sont obligatoires :

Étape 3. Sélectionnez l'interface de passerelle dans la liste déroulante. Il s'agit du port qui sera utilisé pour acheminer le trafic via les tunnels VPN SSL. Les options sont les suivantes :

- WAN1
- WAN2

- USB1
- USB2



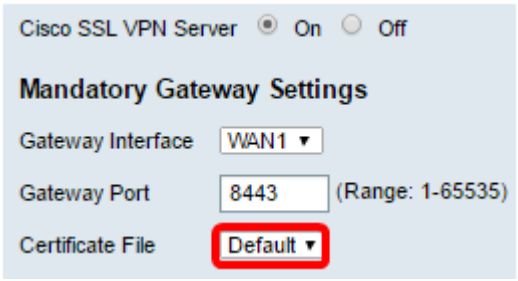
Remarque : Dans cet exemple, WAN1 est choisi.

Étape 4. Entrez le numéro de port utilisé pour la passerelle VPN SSL dans le champ Gateway Port compris entre 1 et 65535.



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

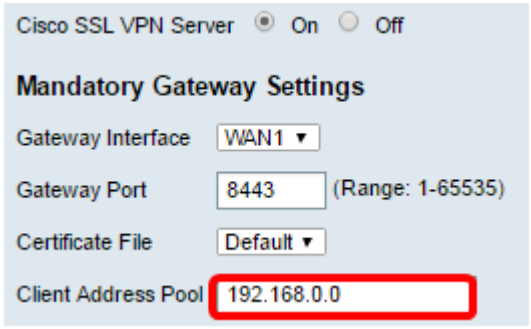
Étape 5. Sélectionnez le fichier de certificat dans la liste déroulante. Ce certificat authentifie les utilisateurs qui tentent d'accéder à la ressource réseau via les tunnels VPN SSL. La liste déroulante contient un certificat par défaut et les certificats importés.



Remarque : Dans cet exemple, Default est sélectionné.

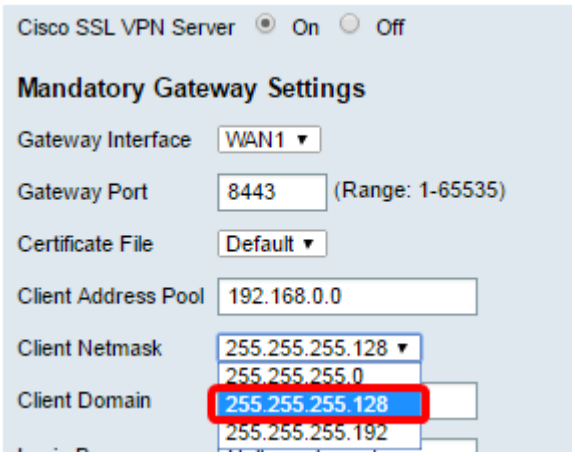
Étape 6. Entrez l’adresse IP du pool d’adresses client dans le champ Client Address Pool. Ce pool correspond à la plage d'adresses IP qui sera allouée aux clients VPN distants.

Remarque : Assurez-vous que la plage d'adresses IP ne chevauche aucune des adresses IP du réseau local.



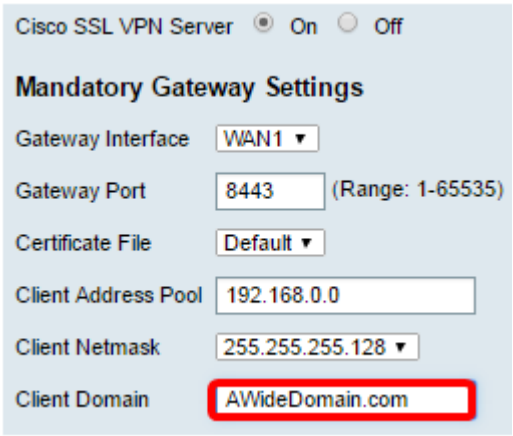
Remarque : Dans cet exemple, 192.168.0.0 est utilisé.

Étape 7. Choisissez le masque de réseau du client dans la liste déroulante.



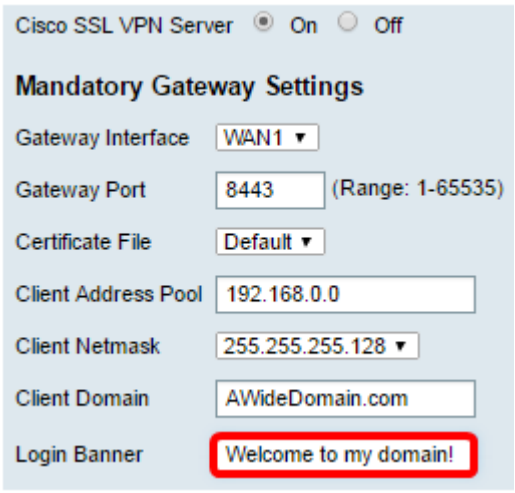
Remarque : Dans cet exemple, 255.255.255.128 est choisi.

Étape 8. Entrez le nom de domaine du client dans le champ Client Domain. Il s'agit du nom de domaine qui doit être envoyé aux clients VPN SSL.



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

Étape 9. Entrez le texte qui apparaîtra comme bannière de connexion dans le champ Bannière de connexion. Il s'agit de la bannière qui s'affiche chaque fois qu'un client se connecte.



Remarque : Dans cet exemple, Bienvenue dans mon domaine ! est utilisé comme bannière de connexion.

Paramètres de passerelle facultatifs

Les paramètres de configuration suivants sont facultatifs :

Étape 1. Entrez une valeur en secondes pour le délai d'inactivité compris entre 60 et 86400. Il s'agit de la durée pendant laquelle la session VPN SSL peut rester inactive.



Remarque : Dans cet exemple, l'adresse 3000 est utilisée.

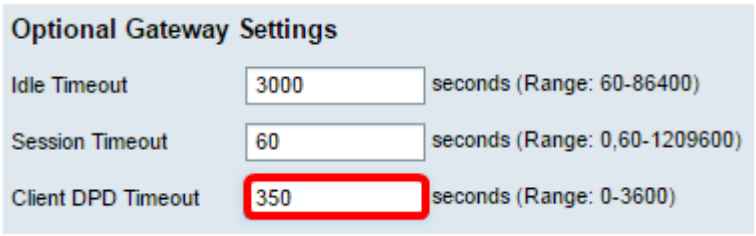
Étape 2. Entrez une valeur en secondes dans le champ Session Timeout. Il s'agit du temps nécessaire à la session TCP (Transmission Control Protocol) ou UDP (User Datagram Protocol) pour expirer après le temps d'inactivité spécifié. La plage est comprise entre 60 et 1209600.



Remarque : Dans cet exemple, l’adresse 60 est utilisée.

Étape 3. Entrez une valeur en secondes dans le champ ClientDPD Timeout comprise entre 0 et 3600. Cette valeur spécifie l'envoi périodique de messages HELLO/ACK pour vérifier l'état du tunnel VPN.

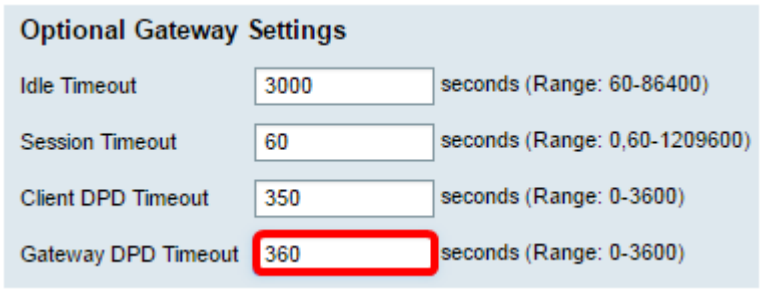
Remarque : Cette fonctionnalité doit être activée aux deux extrémités du tunnel VPN.



Remarque : Dans cet exemple, l’adresse 350 est utilisée.

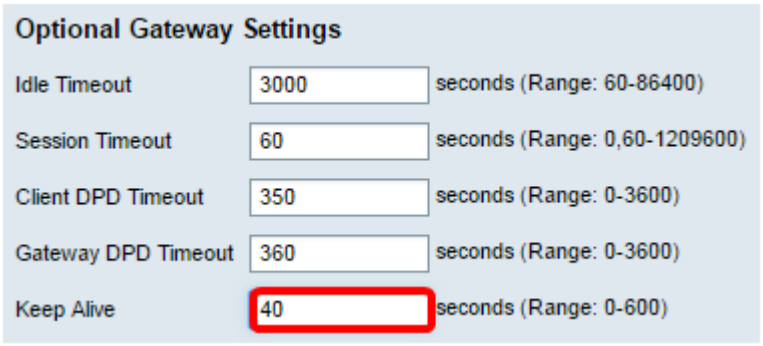
Étape 4. Entrez une valeur en secondes dans le champ GatewayDPD Timeout comprise entre 0 et 3600. Cette valeur spécifie l'envoi périodique de messages HELLO/ACK pour vérifier l'état du tunnel VPN.

Remarque : Cette fonctionnalité doit être activée aux deux extrémités du tunnel VPN.



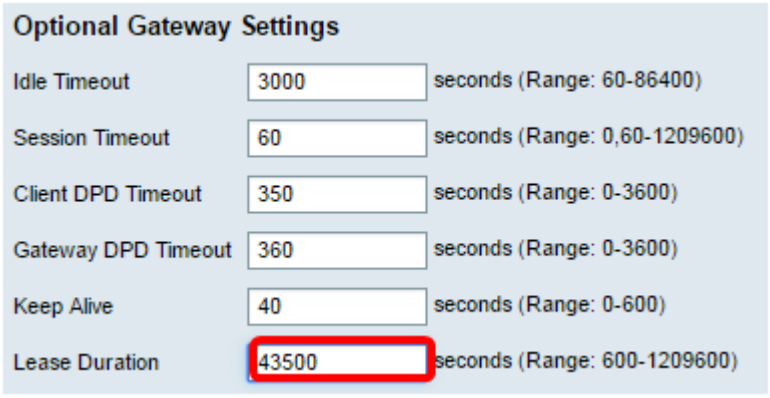
Remarque : Dans cet exemple, l’adresse 360 est utilisée.

Étape 5. Entrez une valeur en secondes dans le champ Keep Alive comprise entre 0 et 600. Cette fonctionnalité garantit que votre routeur est toujours connecté à Internet. Il tentera de rétablir la connexion VPN si elle est abandonnée.



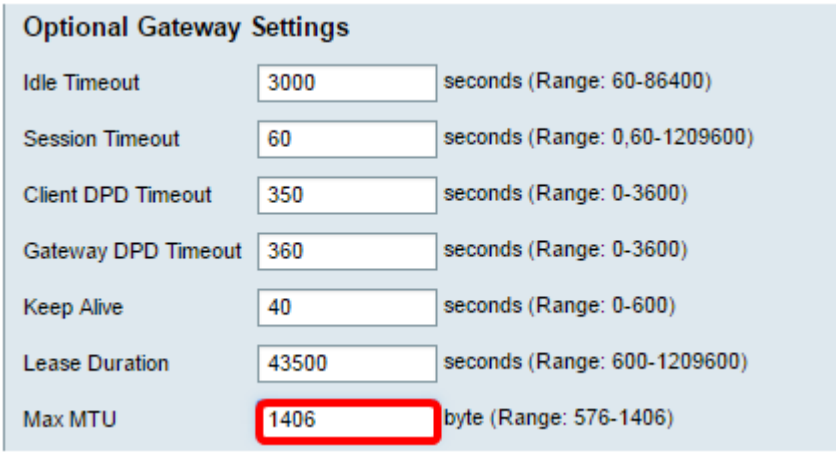
Remarque : Dans cet exemple, l'adresse 40 est utilisée.

Étape 6. Entrez une valeur en secondes pour la durée du tunnel à connecter dans le champ Lease Duration. La plage est comprise entre 600 et 1209600.



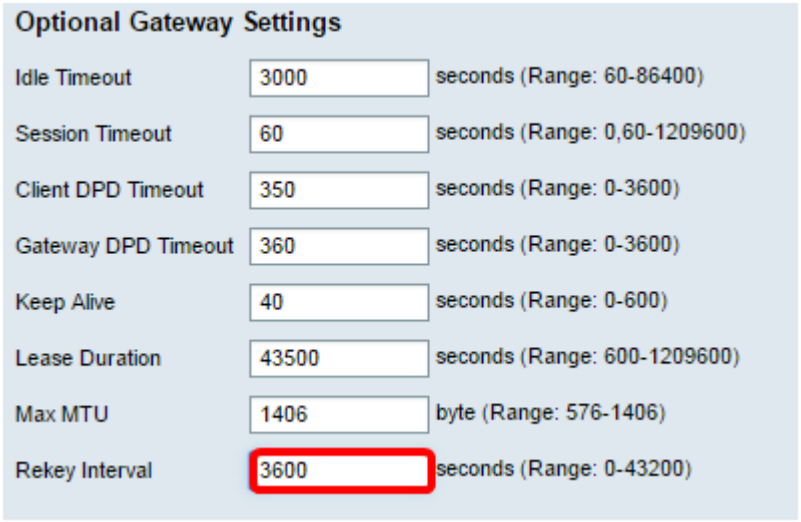
Remarque : Dans cet exemple, l'adresse 43500 est utilisée.

Étape 7. Entrez la taille du paquet en octets qui peut être envoyé sur le réseau. La plage est comprise entre 576 et 1406.



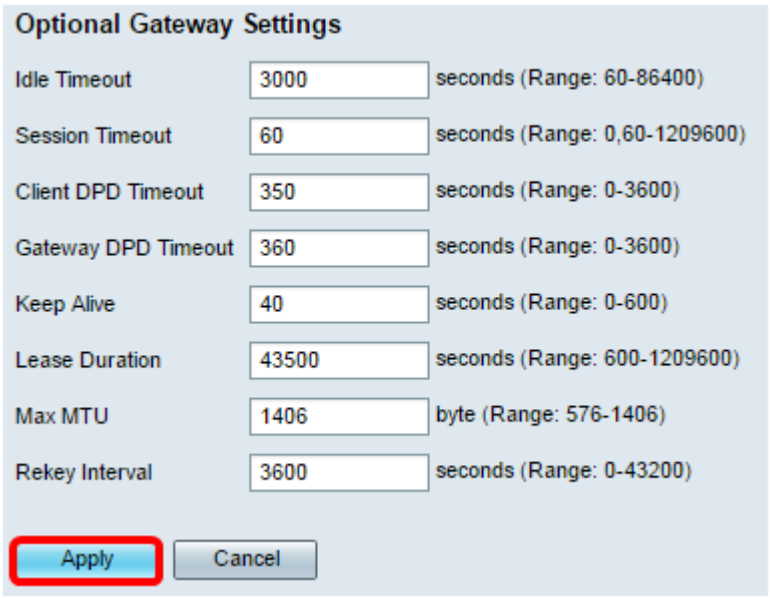
Remarque : Dans cet exemple, l'adresse 1406 est utilisée.

Étape 8. Entrez la durée de l'intervalle de relais dans le champ Rekey Interval. La fonction Rekey permet aux clés SSL de renégocier une fois la session établie. La plage est comprise entre 0 et 43200.



Remarque : Dans cet exemple, l'adresse 3600 est utilisée.

Étape 9. Cliquez sur Apply (appliquer).



Étape 10. (Facultatif) Pour enregistrer définitivement la configuration, cliquez sur l' 

icône clignotante.

Vous devez maintenant avoir correctement configuré le VPN SSL sur votre routeur RV34x.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.