Contenu

[Introduction](#)
[Conditions préalables](#)
[Conditions requises](#)
[Composants utilisés](#)
[Les informations d'autorisation pour différentes versions IOS](#)
[Améliorations logicielles significatives](#)
[Configurez](#)
[Étape 1. Confirmez le permis est activé](#)
[Étape 2. Téléchargez et installez le module sécurisé de client de mobilité d'AnyConnect sur le routeur](#)
[Étape 3. Activez le serveur de HTTP sur le routeur](#)
[Étape 4. Générez RSA Keypair et certificat Auto-signé](#)
[Étape 5. Configurez les comptes utilisateurs locaux VPN](#)
[Étape 6. Définissez la liste d'accès de pool d'adresses et de tunnel partagé à utiliser par des clients](#)
[Étape 7. Configurez l'interface de modèle virtuel (VTI)](#)
[Étape 8. Configurez le webvpn gateway](#)
[Étape 9. Configurez le contexte et la stratégie de groupe de webvpn](#)
[Étape 10 (facultative). Configurez un profil de client](#)
[Vérifiez](#)
[Dépannez](#)
[Informations connexes](#)

Introduction

Ce document décrit la configuration de base d'un routeur Cisco IOS comme Headend d'AnyConnect SSLVPN.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Internetwork Operating System (IOS)
- Client sécurisé de mobilité d'AnyConnect
- Exécution du Général Secure Sockets Layer (SSL)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de

logiciel suivantes :

- Routeur de Cisco 892W exécutant 15.3(3)M5
- Client sécurisé 3.1.08009 de mobilité d'AnyConnect

Les informations d'autorisation pour différentes versions IOS

- L'ensemble de caractéristiques securityk9 est exigé pour utiliser les caractéristiques SSLVPN, dont indépendamment la version IOS est utilisée.
- IOS 12.x - la caractéristique SSLVPN est intégrée dans toutes les images 12.x qui commencent par 12.4(6)T qui ont au moins un permis de Sécurité (IE. advsecurityk9, adventerprisek9, et ainsi de suite).
- IOS 15.0 - des versions antérieures exigent d'un fichier LIC d'être installé sur le routeur qui tiendra compte de 10, 25, ou 100 connexions utilisateur. Droit aux permis d'Use* ont été mis en application dans 15.0(1)M4
- IOS 15.1 - des versions antérieures exigent d'un fichier LIC d'être installé sur le routeur qui tiendra compte de 10, 25, ou 100 connexions utilisateur. Droit aux permis d'Use* ont été mis en application dans 15.1(1)T2, 15.1(2)T2, 15.1(3)T, et 15.1(4)M1
- IOS 15.2 - chacune des 15.2 versions offre juste aux permis d'Use* pour SSLVPN
- IOS 15.3 et au-delà - les versions antérieures offrent juste aux permis d'Use*. Commençant dans 15.3(3)M, la caractéristique SSLVPN est disponible après que vous démarriez dans un technologie-module securityk9

Pour le RTU autorisant, un permis d'évaluation sera activé quand la première caractéristique de webvpn est configuré (c'est-à-dire, webvpn gateway GATEWAY1) et le contrat de licence utilisateur final (CLUF) a été reçu. Après 60 jours, ce permis d'évaluation devient un permis permanent. Ces permis sont honneur basé et exigent un permis de papier d'être acheté afin d'utiliser la caractéristique. Supplémentaire, plutôt qu'étant limité à un certain nombre d'utilisations, le RTU tiennent compte du nombre maximal de connexions simultanées que la plate-forme de routeur peut prendre en charge simultanément.

Améliorations logicielles significatives

Ces id de bogues ont eu comme conséquence les caractéristiques ou les difficultés significatives pour AnyConnect :

- CSCti89976 : Soutien ajouté d'AnyConnect 3.x à l'IOS
- CSCtx38806 : Difficulté pour la vulnérabilité de BÊTE, Microsoft KB2585542

Configurez

Étape 1. Confirmez le permis est activé

La première étape quand AnyConnect est configuré sur un headend de routeur IOS est de confirmer que le permis a été correctement installé (si c'est approprié) et activé. Référez-vous aux informations d'autorisation dans la section précédente pour les particularités d'autorisation sur des différentes versions. Il dépend de la version du code et de la plate-forme si le show license répertorie un permis SSL_VPN ou securityk9. Indépendamment de la version et du permis, le CLUF devra être reçu et le permis affichera en tant qu'Active.

Étape 2. Téléchargez et installez le module sécurisé de client de mobilité d'AnyConnect sur le routeur

Pour télécharger une image d'AnyConnect aux services de headend VPN deux buts. Premièrement, on permettra seulement aux des systèmes d'exploitation qui ont des images d'AnyConnect actuelles sur le headend d'AnyConnect pour se connecter. Par exemple, des clients Windows exigent d'un module de Windows pour être installés sur le headend, Linux les clients que 64-bit ont besoin d'un module 64-bit de Linux, et ainsi de suite. Deuxièmement, l'image d'AnyConnect installée sur le headend automatiquement sera abaissée à la machine cliente sur la connexion. Les utilisateurs qui se connectent pour la première fois pourront télécharger le client du portail web et les utilisateurs que le retour pourra promouvoir, si le module d'AnyConnect sur le headend est plus nouveau que ce qui est installé sur leur machine cliente.

Des modules d'AnyConnect peuvent être obtenus par la section sécurisée de client de mobilité d'AnyConnect du site Web de téléchargements logiciels de Cisco. Tandis qu'il y a beaucoup d'options disponibles, les modules qui doivent être installés sur le headend seront étiquetés avec le système d'exploitation et le déploiement de tête de réseau (MODULE). Les modules d'AnyConnect sont actuellement disponibles pour ces Plateformes du système d'exploitation : Windows, Mac OS X, Linux (de 32 bits), et Linux 64-bit. Notez que pour le Linux, il y a les deux 32 et modules 64-bit. Chaque système d'exploitation exige du module approprié d'être installé sur le headend pour qu'on laisse des connexions.

Une fois que le module d'AnyConnect a été téléchargé, il peut être téléchargé à l'éclair du routeur avec la Commande **COPY** par l'intermédiaire du TFTP, du FTP, du SCP, ou de quelques autres options. Voici un exemple :

Après que vous copiiez l'image d'AnyConnect sur l'éclair du routeur, il doit être installé par l'intermédiaire de la ligne de commande. De plusieurs modules d'AnyConnect peuvent être installés quand vous spécifiez un numéro de séquence à la fin de la commande d'installation ; ceci tiendra compte pour que le routeur agisse en tant que headend pour de plusieurs systèmes d'exploitation de client. Quand vous installez le module d'AnyConnect, il le déplacera également à l'**éclair : répertoire /webvpn/** s'il n'était pas copié là au commencement.

Sur les versions du code qui ont été libérées avant 15.2(1)T, la commande d'installer le MODULE est légèrement différente.

Étape 3. Activez le serveur de HTTP sur le routeur

Étape 4. Générez RSA Keypair et certificat Auto-signé

Quand vous configurez le SSL ou n'importe quelle caractéristique qui implémente l'Infrastructure à clés publiques (PKI) et les Certificats numériques, un keypair de Rivest-Shamir-Adleman (RSA) est exigé pour la signature du certificat. La commande de suivre génèrera un keypair RSA qui sera alors utilisé quand le certificat auto-signé de PKI est généré. Quand vous vous servez d'un module de 2048 bits, ce n'est pas une condition requise, il est recommandé d'utiliser le plus grand module disponible pour la sécurité optimisée et la compatibilité avec les machines cliente d'AnyConnect. Pour utiliser une étiquette descriptive est également recommandé car elle tiendra compte de la facilité de la gestion des clés. La génération de clés peut être confirmée avec la

commande de **show crypto key mypubkey rsa**.

> Remarque: Car il y a beaucoup de risques de sécurité associés avec rendre des clés RSA exportables, la méthode recommandée est de s'assurer que des clés sont configurées pour être non exportables qui est le par défaut. Les risques qui sont impliqués quand vous rendez les clés RSA exportables sont discutés dans le ce document : Déployer des clés RSA dans un PKI.

Une fois que le keypair RSA a été avec succès généré, un point de confiance de PKI doit être configuré avec les informations de notre routeur et le keypair RSA. Le nom commun (NC) dans le subject-name devrait être configuré avec l'adresse IP ou le plein nom de domaine qualifié (FQDN) que les utilisateurs les utilisent pour connecter à la passerelle d'AnyConnect ; dans cet exemple, les clients utilisent le FQDN de fdenofa-SSLVPN.cisco.com quand ils tentent de se connecter. Tandis qu'il n'est pas obligatoire, quand vous entrez correctement dans la NC, elle aide à réduire le nombre d'erreurs de certificat qui sont incitées à la procédure de connexion.

> Remarque: Plutôt qu'utilisant un certificat auto-signé généré par le routeur, il est possible d'utiliser un certificat délivré par une tierce partie CA. Ceci peut être fait par l'intermédiaire de quelques différentes méthodes comme évoqué dans ce document : Configurer l'inscription de certificat pour un PKI.

Après que le point de confiance ait été correctement défini, le routeur doit générer le certificat à l'aide de la commande de **crypto pki enroll**. Avec ce processus, il est possible de spécifier quelques autres paramètres tels que le numéro de série et l'adresse IP. Cependant, ceci n'est pas exigé. La génération de certificat peut être confirmée avec la commande de **show crypto pki certificates**.

Étape 5. Configurez les comptes utilisateurs locaux VPN

Tandis qu'il est possible d'utiliser une authentification externe, serveur d'autorisation, et de comptabilité (AAA), parce que cette authentification locale d'exemple est utilisé. Ces commandes créeront un nom d'utilisateur VPNUSER et créeront également une authentification SSLVPN_AAA nommé par liste d'AAA.

Étape 6. Définissez la liste d'accès de pool d'adresses et de tunnel partagé à utiliser par des clients

Un groupe d'adresse IP locale doit être créé pour que des adaptateurs de client d'AnyConnect obtiennent une adresse IP. Assurez que vous configurez un assez grand groupe pour prendre en charge le nombre maximal de connexions client simultanées d'AnyConnect.

Par défaut, AnyConnect fonctionnera dans le plein tunnel mode qui signifie que n'importe quel trafic généré par la machine cliente sera envoyé à travers le tunnel. Car ce n'est typiquement pas desirable, il est possible de configurer une liste de contrôle d'accès (ACL) qui définit alors le trafic qui devrait ou ne devrait pas être envoyé à travers le tunnel. Comme avec d'autres réalisations d'ACL, les implicites refusent à l'extrémité éliminent le besoin d'explicite refusent ; donc, il est seulement nécessaire de configurer des déclarations d'autorisation pour le trafic qui devrait être percé un tunnel.

Étape 7. Configurez l'interface de modèle virtuel (VTI)

VTIs dynamique fournissez une interface d'accès virtuel distincte sur demande pour chaque session VPN qui permet la Connectivité fortement sécurisée et extensible pour la remote-access VPN. La technologie DVTI remplace les crypto-cartes dynamiques et la méthode dynamique d'en étoile que les aides établissent des tunnels. Puisque fonction de DVTIs comme toute autre vraie interface qu'ils permettent pour un déploiement distant plus complexe d'Accesss parce qu'ils prennent en charge QoS, Pare-feu, attribtues de par-utilisateur et d'autres Services de sécurité dès que le tunnel sera en activité.

```
interface Loopback0 ip address 172.16.1.1 255.255.255.255
!
interface Virtual-Template 1 ip unnumbered Loopback0
```

Étape 8. Configurez le webvpn gateway

Le webvpn gateway est ce qui définit l'adresse IP et les ports qui seront utilisés par le headend d'AnyConnect, aussi bien que l'algorithme de ssl encryption et le certificat de PKI qui sera présenté aux clients. Par défaut, la passerelle prendra en charge tous les algorithmes de chiffrement possibles, qui varient selon la version IOS sur le routeur.

```
interface Loopback0 ip address 172.16.1.1 255.255.255.255
!
interface Virtual-Template 1 ip unnumbered Loopback0
```

Étape 9. Configurez le contexte et la stratégie de groupe de webvpn

Le contexte et la stratégie de groupe de webvpn définissent quelques paramètres supplémentaires qui seront utilisés pour la connexion client d'AnyConnect. Pour une configuration de base d'AnyConnect, le contexte sert simplement de mécanisme utilisé pour appeler la stratégie de groupe par défaut qui sera utilisée pour AnyConnect. Cependant, le contexte peut être utilisé pour personnaliser plus loin la page de splash de webvpn et l'exécution de webvpn. Au policy group défini, la liste SSLVPN_AAA est configurée comme liste d'authentification d'AAA les utilisateurs sont dont un membre. La commande svc-**activée par fonctions** est la partie de la configuration qui permet à des utilisateurs pour se connecter au **client de VPN SSL d'**AnyConnect plutôt que juste le webvpn par un navigateur. Pour finir, les commandes supplémentaires de SVC définissent les paramètres qui sont appropriés seulement aux connexions de SVC : **le svc address-pool** indique la passerelle aux adresses de document dans l'ACPool aux clients, le **svc split incluent** définit la stratégie de tunnel partagé par ACL 1 défini ci-dessus, et le **svc dns-server** définit le serveur DNS ce qui sera utilisé pour la résolution de nom de domaine. Avec cette configuration, toutes les requêtes DNS seront envoyées au serveur DNS spécifié. L'adresse qui est reçue dans la réponse de requête dictera si le trafic est envoyé à travers le tunnel.

```
webvpn context SSL_Context gateway SSLVPN_Gateway inservice policy group SSL_Policy  aaa
authentication list SSLVPN_AAA  functions svc-enabled  svc address-pool "SSLVPN_POOL" netmask
255.255.255.0  svc split include acl 1  svc dns-server primary 8.8.8.8
virtual-template 1
default-group-policy SSL_Policy
```

Étape 10 (facultative). Configurez un profil de client

Àla différence de sur des ASA, le Cisco IOS n'a pas une interface gui intégrée qui peut aider des admins en créant le profil de client. Le profil de client d'AnyConnect doit être créé/édité séparément avec l'éditeur autonome de profil.

Conseil : Recherchez anyconnect-profileeditor-win-3.1.03103-k9.exe

Suivez ces étapes pour faire déployer au routeur le profil :

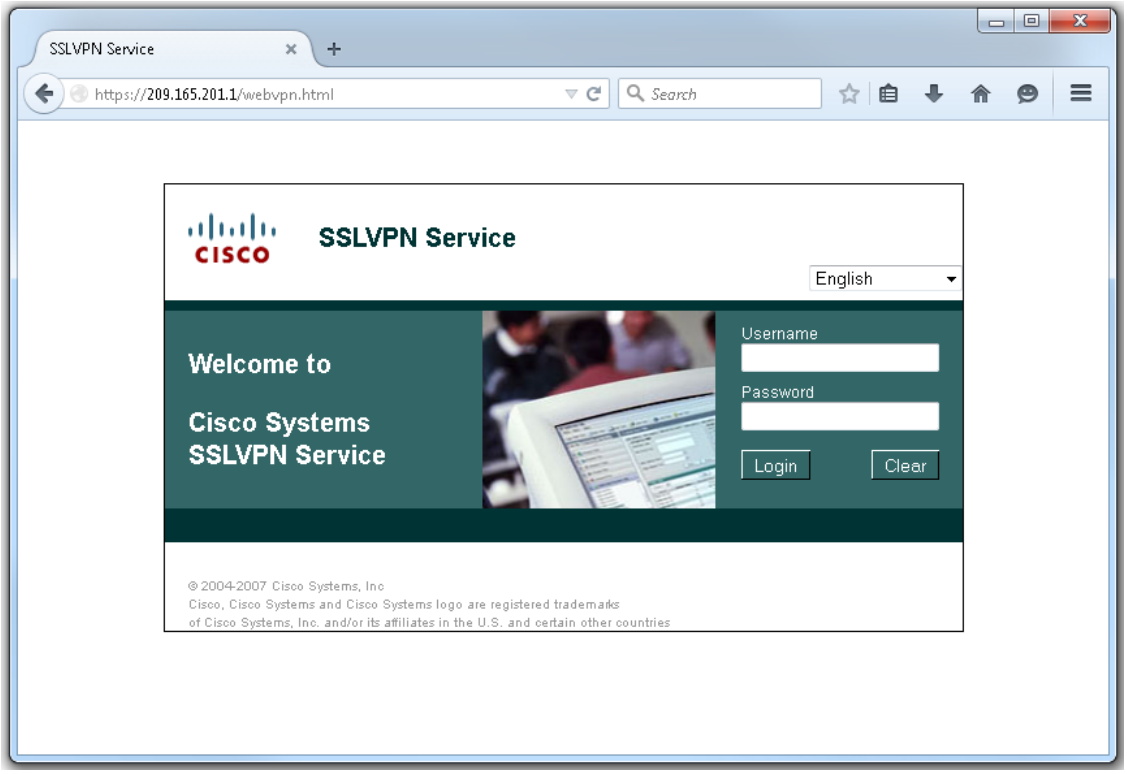
1. Téléchargez-le à l'éclair IOS utilisant le FTP/tftp
2. Utilisez cette commande d'identifier le profil qui a été juste téléchargé :

1. ```
   webvpn context SSL_Context gateway SSLVPN_Gateway inservice policy group SSL_Policy  aaa
   authentication list SSLVPN_AAA  functions svc-enabled  svc address-pool "SSLVPN_POOL"
   netmask 255.255.255.0  svc split include acl 1  svc dns-server primary 8.8.8.8
   virtual-template 1
   default-group-policy SSL_Policy
   ```
   Conseil : Sur des versions IOS plus anciennes que 15.2(1)T, cette commande doit être utilisée :
   éclair de <profile_name> de profil de svc d'importation de webvpn : <profile.xml>
3. Sous le contexte, utilisez cette commande de lier le profil à ce contexte :

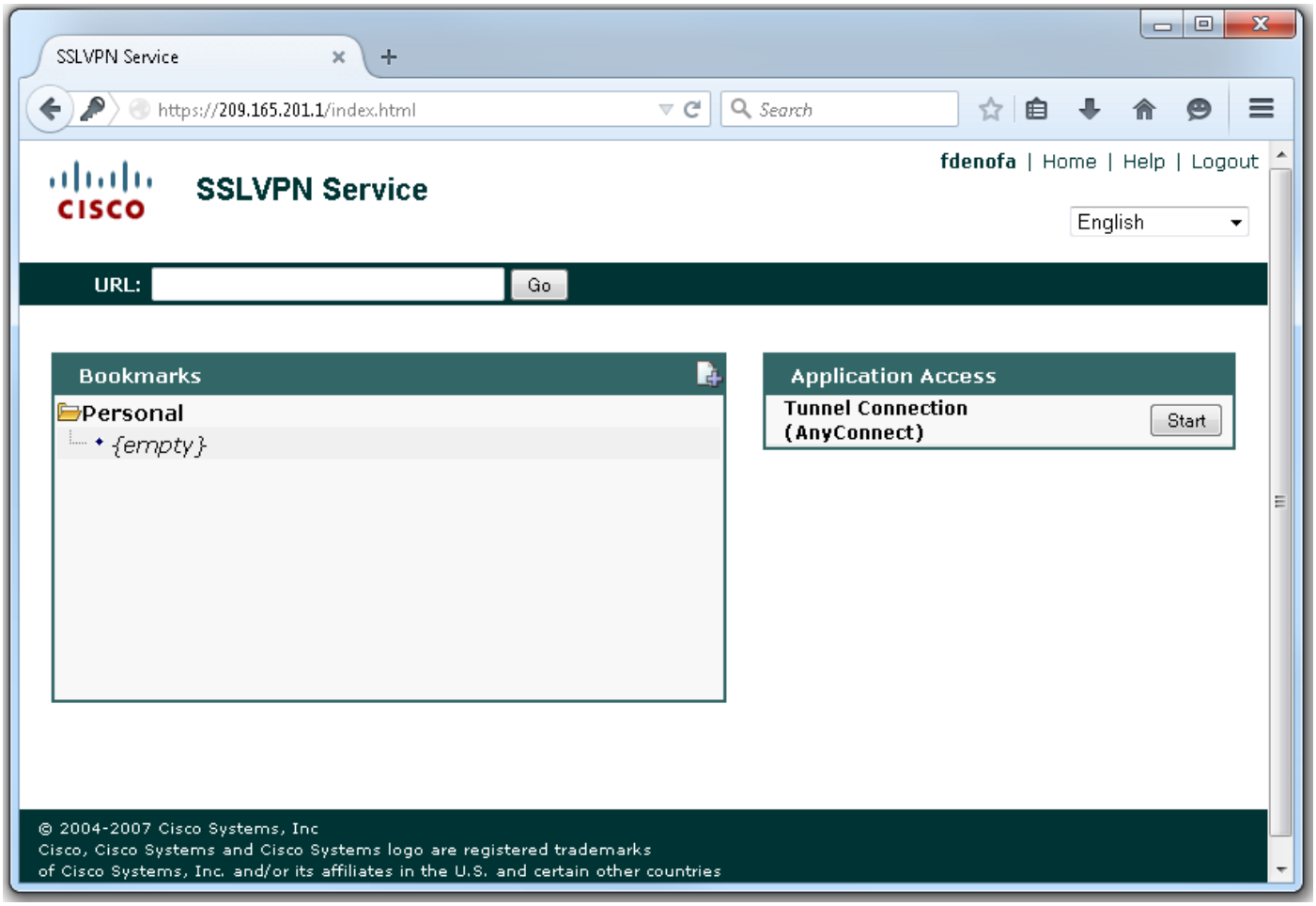
1. ```
   webvpn context SSL_Context gateway SSLVPN_Gateway inservice policy group SSL_Policy  aaa
   authentication list SSLVPN_AAA  functions svc-enabled  svc address-pool "SSLVPN_POOL"
   netmask 255.255.255.0  svc split include acl 1  svc dns-server primary 8.8.8.8
   virtual-template 1
   default-group-policy SSL_Policy
   ```
   Remarque: Utilisez l'Outil de recherche de commande (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

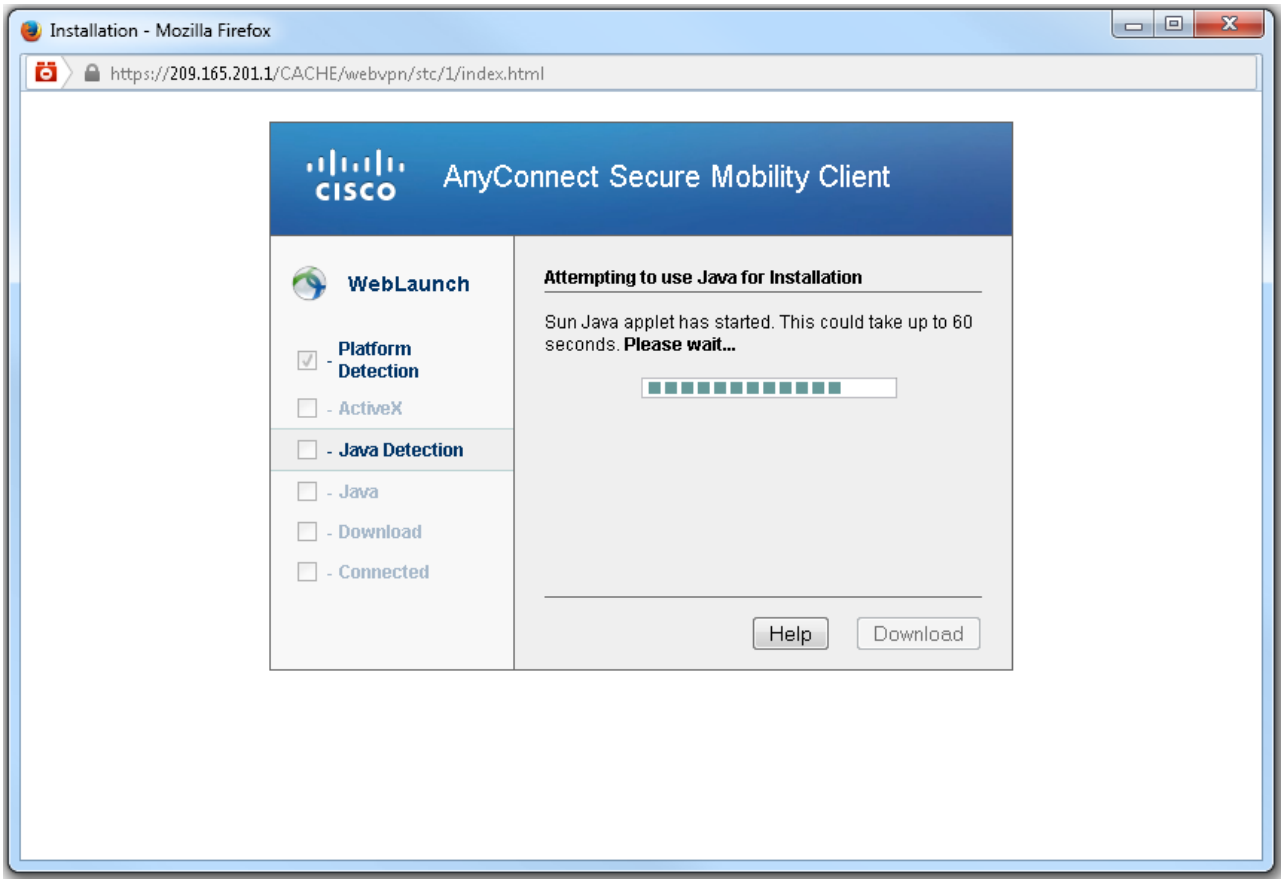
Vérifiez

Une fois que la configuration est complète, quand vous accédez à l'adresse de passerelle et mettez en communication par l'intermédiaire du navigateur, elle reviendra à la page de splash de webvpn.



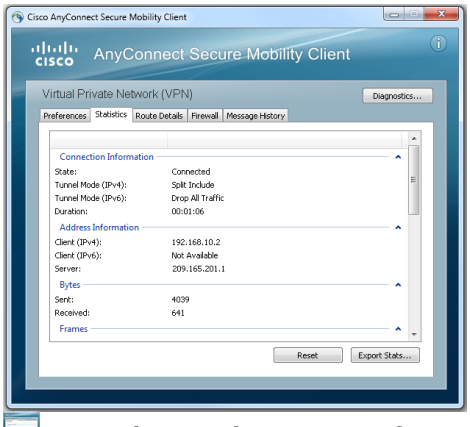
Après que vous ouvriez une session, la page d'accueil de webvpn est affichée. D'ici, **connexion en tunnel de** clic **(AnyConnect).** Quand l'Internet Explorer est utilisé, ActiveX est utilisé pour abaisser et installer le client d'AnyConnect. S'il n'est pas détecté, Javas seront utilisées à la place. Toutes autres Javas d'utilisation de navigateurs immédiatement.





Une fois que l'installation est terminée, AnyConnect tentera automatiquement de se connecter au webvpn gateway. Car un certificat auto-signé est utilisé pour que la passerelle s'identifie, les avertissements de plusieurs certificat apparaîtront pendant la tentative de connexion. Ceux-ci sont prévus et doivent être reçus pour que la connexion continue. Pour éviter ces avertissements de certificat, le certificat auto-signé étant présenté doit être installé dans le stock de certificat de confiance de la machine cliente, ou si un tiers certificat est utilisé alors le certificat d'autorité de certification doit être dans la mémoire de certificat de confiance.

Quand la connexion se termine la négociation, cliquez sur en fonction l'icône d'**équipement** dans en bas à gauche d'AnyConnect affichera quelques informations avancées sur la connexion. À cette page il est possible de visualiser quelques statistiques de connexion et de conduire des détails atteints de l'ACL de tunnel partagé dans la configuration de stratégie de groupe.



Voici le résultat final de configuration courante des étapes de configuration :

```
webvpn context SSLVPN_Gateway  ssl authenticate verify all  inservice  policy group SSL_Policy  aaa
authentication list SSLVPN_AAA  functions svc-enabled  svc address-pool "SSLVPN_POOL" netmask
```

```
255.255.255.0  svc split include acl 1  svc dns-server primary 8.8.8.8
virtual-template 1
default-group-policy SSL_Policy
```

Dépannez

Il y a quelques composants communs à vérifier quand vous dépannez des questions de connexion d'AnyConnect :

- Comme le client doit présenter un certificat, c'est une condition que le certificat a spécifié dans le webvpn gateway soit valide. Pour délivrer un **crypto certificat de PKI d'exposition** affichera les informations qui concernent tous les Certificats sur le routeur.
- Toutes les fois qu'on modifie la configuration de webvpn, il est dans une pratique recommandée de n'émettre un aucun inservice et l'inservice sur la passerelle et le contexte. Ceci s'assurera que les modifications les prennent effet correctement.
- Comme cité précédemment, c'est une condition requise d'avoir un MODULE d'AnyConnect pour chaque système d'exploitation de client qui se connectera à cette passerelle. Par exemple, les clients Windows ont besoin d'un MODULE de Windows, Linux les clients que de 32 bits ont besoin d'un MODULE de 32 bits de Linux, et ainsi de suite.
- Quand vous considérez le client d'AnyConnect et le webvpn basé sur navigateur utilisent le SSL, pouvoir accéder à la page de splash de webvpn indique généralement qu'AnyConnect pourra se connecter (supposez que la configuration pertinente d'AnyConnect est correcte).

Le Cisco IOS offre quelques diverses options de debug webvpn qui peuvent être utilisées pour dépanner les connexions manquantes. C'est le résultat généré de l'AAA de debug webvpn, met au point le tunnel de wevpn, et le show webvpn session sur une tentative réussie de connexion :

```
webvpn context SSL_Context gateway SSLVPN_Gateway inservice policy group SSL_Policy  aaa
authentication list SSLVPN_AAA  functions svc-enabled  svc address-pool "SSLVPN_POOL" netmask
255.255.255.0  svc split include acl 1  svc dns-server primary 8.8.8.8
virtual-template 1
default-group-policy SSL_Policy
```

Informations connexes

- Guide de configuration de VPN SSL, version de Cisco IOS 15M&T
- Exemple de configuration de client VPN AnyConnect (SSL) sur routeur IOS avec CCP