AnyConnect : Configuration du VPN SSL de base pour la tête de réseau du routeur Cisco IOS avec CLI

Introduction

Contenu

Ce document décrit la configuration de base d'un routeur Cisco IOS® en tant que tête de réseau VPN SSL (Secure Sockets Layer VPN) AnyConnect.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco IOS
- Client de mobilité sécurisée AnyConnect
- Fonctionnement général de SSL

Components Used

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

- Routeur Cisco 892W exécutant 15.3(3)M5
- AnyConnect Secure Mobility Client 3.1.08009

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Informations de licence pour différentes versions IOS

- Le jeu de fonctions securityk9 est requis pour utiliser les fonctions VPN SSL, quelle que soit la version de Cisco IOS utilisée.
- Cisco IOS 12.x - la fonctionnalité VPN SSL est intégrée dans toutes les images 12.x qui commencent par 12.4(6)T et qui ont au moins une licence de sécurité (c.-à-d. advsecurityk9, adventerprisek9, etc.).
- Cisco IOS 15.0 - Les versions antérieures nécessitent l'installation d'un fichier LIC sur le routeur, qui autorise des connexions de 10, 25 ou 100 utilisateurs. Des licences de droit d'utilisation* ont été mises en oeuvre dans 15.0(1)M4
- Cisco IOS 15.1 - Les versions antérieures nécessitent l'installation d'un fichier LIC sur le routeur, qui autorise des connexions de 10, 25 ou 100 utilisateurs. Les licences de droit d'utilisation* ont été mises en oeuvre dans les versions 15.1(1)T2, 15.1(2)T2, 15.1(3)T et 15.1(4)M1
- Cisco IOS 15.2 - toutes les versions 15.2 offrent des licences de droit d'utilisation* pour SSLVPN
- Cisco IOS 15.3 et versions ultérieures - les versions antérieures offrent les licences de droit d'utilisation*. À partir de la version 15.3(3)M, la fonctionnalité SSLVPN est disponible après le démarrage dans un package technologique security9

Pour les licences RTU, une licence d'évaluation sera activée lorsque la première fonctionnalité webvpn est configurée (c'est-à-dire, webvpn gateway GATEWAY1) et que le contrat de licence utilisateur final (CLUF) a été accepté. Après 60 jours, cette licence d'évaluation devient une licence permanente. Ces licences sont basées sur l'honneur et nécessitent l'achat d'une licence papier pour pouvoir utiliser la fonctionnalité. En outre, plutôt que de se limiter à un certain nombre d'utilisations, le RTU permet le nombre maximal de connexions simultanées que la plate-forme du routeur peut prendre en charge simultanément.

Améliorations logicielles importantes

Ces ID de bogue ont généré des fonctionnalités ou des correctifs significatifs pour AnyConnect :

- CSCti89976 : Ajout de la prise en charge d'AnyConnect 3.x à IOS
- CSCtx38806 : correction pour la vulnérabilité BEAST, Microsoft KB2585542

Configuration

Étape 1. Confirmer l'activation de la licence

La première étape lorsque AnyConnect est configuré sur une tête de réseau de routeur IOS consiste à confirmer que la licence a été correctement installée (le cas échéant) et activée. Reportez-vous aux informations de licence de la section précédente pour connaître les détails de licence sur différentes versions. Cela dépend de la version du code et de la plate-forme, que la licence show répertorie une licence SSL_VPN ou securityk9. Quelle que soit la version et la licence, le CLUF devra être accepté et la licence apparaîtra comme Actif.

Étape 2. Télécharger et installer le package client AnyConnect Secure Mobility sur le routeur

Afin de télécharger une image AnyConnect sur le VPN, la tête de réseau a deux objectifs. Tout d’abord, seuls les systèmes d’exploitation qui ont des images AnyConnect présentes sur la tête de réseau AnyConnect seront autorisés à se connecter. Par exemple, les clients Windows ont besoin d'un package Windows pour être installés sur la tête de réseau, les clients Linux 64 bits nécessitent un package Linux 64 bits, etc. Deuxièmement, l’image AnyConnect installée sur la tête de réseau sera automatiquement repoussée vers la machine cliente dès la connexion. Les utilisateurs qui se connectent pour la première fois pourront télécharger le client à partir du portail Web et les utilisateurs qui retournent pourront effectuer une mise à niveau, à condition que le package AnyConnect de la tête de réseau soit plus récent que celui installé sur leur ordinateur client.

Les packages AnyConnect peuvent être obtenus via la section AnyConnect Secure Mobility Client du site Web de téléchargement de logiciels Cisco. Bien qu'il existe de nombreuses options disponibles, les paquets qui doivent être installés sur la tête de réseau seront étiquetés avec le système d'exploitation et le déploiement de tête de réseau (PKG). Les packages AnyConnect sont actuellement disponibles pour ces plates-formes de système d'exploitation : Windows, Mac OS X, Linux (32 bits) et Linux 64 bits. Notez que pour Linux, il existe des paquets 32 et 64 bits. Chaque système d'exploitation nécessite l'installation du package approprié sur la tête de réseau afin d'autoriser les connexions.

Une fois le package AnyConnect téléchargé, il peut être téléchargé dans la mémoire Flash du routeur avec la commande **copy** via TFTP, FTP, SCP ou quelques autres options. Voici un exemple :

```
copy tftp: flash:/webvpn/

Address or name of remote host []? 192.168.100.100
Source filename []? anyconnect-win-3.1.08009-k9.pkg
Destination filename [/webvpn/anyconnect-win-3.1.08009-k9.pkg]?
Accessing tftp://192.168.100.100/anyconnect-win-3.1.08009-k9.pkg...
Loading anyconnect-win-3.1.08009-k9.pkg from 192.168.100.100 (via GigabitEthernet0):
!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 37997096 bytes]
```

```
37997096 bytes copied in 117.644 secs (322984 bytes/sec)
```

Après avoir copié l'image AnyConnect dans la mémoire Flash du routeur, elle doit être installée via la ligne de commande. Plusieurs packages AnyConnect peuvent être installés lorsque vous spécifiez un numéro de séquence à la fin de la commande d'installation ; cela permettra au routeur d'agir comme tête de réseau pour plusieurs systèmes d'exploitation clients. Lorsque vous installez le package AnyConnect, il le déplace également vers le **répertoire flash:/webvpn/** s'il n'y a pas été copié initialement.

```
crypto vpn anyconnect flash:/webvpn/anyconnect-win-3.1.08009-k9.pkg sequence 1

SSLVPN Package SSL-VPN-Client (seq:1): installed successfully
```

Sur les versions de code publiées avant 15.2(1)T, la commande d'installation du PKG est légèrement différente.

```
webvpn install svc flash:/webvpn/anyconnect-win-3.1.08009-k9.pkg sequence 1
```

Étape 3. Générer un Keypair RSA et un certificat auto-signé

Lorsque vous configurez SSL ou toute fonctionnalité qui implémente l'infrastructure à clé publique (PKI) et les certificats numériques, une paire de clés Rivest-Shamir-Adleman (RSA) est requise pour la signature du certificat. Cette commande génère une paire de clés RSA qui sera ensuite utilisée lors de la génération du certificat PKI auto-signé. Utilisez un module de 2048 bits, il n'est pas obligatoire, mais il est recommandé d'utiliser le plus grand module disponible pour améliorer la sécurité et la compatibilité avec les machines clientes AnyConnect. Il est également recommandé d'utiliser une étiquette de clé descriptive qui sera attribuée avec la gestion des clés. La génération de clé peut être confirmée avec la commande **show crypto key mypubkey rsa**.

> **Remarque:** Comme il existe de nombreux risques de sécurité associés à l'exportation des clés RSA, la pratique recommandée consiste à s'assurer que les clés sont configurées pour ne pas être exportables, ce qui est le cas par défaut. Les risques associés à l'exportation des clés RSA sont abordés dans ce document : Déploiement des clés RSA dans une PKI.

```
crypto key generate rsa label SSLVPN_KEYPAIR modulus 2048

The name for the keys will be: SSLVPN_KEYPAIR

% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 3 seconds)

show crypto key mypubkey rsa SSLVPN_KEYPAIR

% Key pair was generated at: 14:01:34 EDT May 21 2015
Key name: SSLVPN_KEYPAIR
Key type: RSA KEYS
Storage Device: not specified
Usage: General Purpose Key
Key is not exportable.
```

```
Key Data:
30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
00C4C7D6 F9533CD3 A5489D5A 4DC3BAE7 6831E832 7326E322 CBECC41C 8395A5F7
4613AF70 827F581E 57F72074 FD803EEA 693EBACC 0EE5CA65 5D1875C2 2F19A432
84188F61 4E282EC3 D30AE4C9 1F2766EF 48269FE2 0C1AECAA 81511386 1BA6709C
7C5A2A40 2FBB3035 04E3770B 01155368 C4A5B488 D38F425C 23E430ED 80A8E2BD
E713860E F654695B C1780ED6 398096BC 55D410DB ECC0E2D9 2621E1AB A418986D
39F241FE 798EF862 9D5EAEEB 5B06D73B E769F613 0FCE2585 E5E6DFF3 2E48D007
3443AD87 0E66C2B1 4E0CB6E9 81569DF2 DB0FE9F1 1A9E737F 617DC68B 42B78A8B
952CD997 78B96CE6 CB623328 C2C5FFD6 18C5DA2C 2EAFA936 5C866DE8 5184D2D3
6D020301 0001
```

Une fois la paire de clés RSA générée, un point de confiance PKI doit être configuré avec les informations de notre routeur et la paire de clés RSA. Le nom commun (CN) du nom de sujet doit être configuré avec l'adresse IP ou le nom de domaine complet (FQDN) que les utilisateurs utilisent pour se connecter à la passerelle AnyConnect ; dans cet exemple, les clients utilisent le nom de domaine complet de fdenofa-SSLVPN.cisco.com lorsqu'ils tentent de se connecter. Bien qu'il ne soit pas obligatoire, lorsque vous entrez correctement dans le CN, il contribue à réduire le nombre d'erreurs de certificat qui sont demandées lors de la connexion.

> **Remarque:** Plutôt que d'utiliser un certificat auto-signé généré par le routeur, il est possible d'utiliser un certificat émis par une autorité de certification tierce. Ceci peut être fait via quelques méthodes différentes comme discuté dans ce document : Configuration de l'inscription de certificat pour une PKI.

```
crypto pki trustpoint SSLVPN_CERT
 enrollment selfsigned
 subject-name CN=fdenofa-SSLVPN.cisco.com
 rsakeypair SSLVPN_KEYPAIR
```

Une fois le point de confiance correctement défini, le routeur doit générer le certificat à l'aide de la commande **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, cela n'est pas nécessaire. La génération de certificats peut être confirmée à l'aide de la commande **show crypto pki certificate**.

```
crypto pki enroll SSLVPN_CERT

% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Generate Self Signed Router Certificate? [yes/no]: yes

Router Self Signed Certificate successfully created

show crypto pki certificates SSLVPN_CERT

Router Self-Signed Certificate
  Status: Available
  Certificate Serial Number (hex): 01
  Certificate Usage: General Purpose
  Issuer:
    hostname=fdenofa-892.fdenofa.lab
    cn=fdenofa-SSLVPN.cisco.com
  Subject:
    Name: fdenofa-892.fdenofa.lab
    hostname=fdenofa-892.fdenofa.lab
    cn=fdenofa-SSLVPN.cisco.com
  Validity Date:
    start date: 18:54:04 EDT Mar 30 2015
```

```
    end   date: 20:00:00 EDT Dec 31 2019
  Associated Trustpoints: SSLVPN_CERT
```

Étape 4. Configurer des comptes d'utilisateurs VPN locaux

Bien qu'il soit possible d'utiliser un serveur AAA (Authentication, Authorization, and Accounting) externe, pour cet exemple, l'authentification locale est utilisée. Ces commandes créeront un nom d'utilisateur VPNUSER et créeront également une liste d'authentification AAA nommée SSLVPN_AAA.

```
aaa new-model
aaa authentication login SSLVPN_AAA local
username VPNUSER password TACO
```

Étape 5. Définir le pool d'adresses et la liste d'accès du tunnel partagé à utiliser par les clients

Un pool d’adresses IP locales doit être créé pour que les adaptateurs client AnyConnect puissent obtenir une adresse IP. Assurez-vous de configurer un pool suffisamment grand pour prendre en charge le nombre maximal de connexions client AnyConnect simultanées.

Par défaut, AnyConnect fonctionnera en mode de tunnel complet, ce qui signifie que tout trafic généré par l’ordinateur client sera envoyé à travers le tunnel. Comme cela n'est généralement pas souhaitable, il est possible de configurer une liste de contrôle d'accès (ACL) qui définit ensuite le trafic qui doit ou ne doit pas être envoyé à travers le tunnel. Comme pour les autres mises en oeuvre de listes de contrôle d’accès, le refus implicite à la fin élimine la nécessité d’un refus explicite ; par conséquent, il est seulement nécessaire de configurer les instructions permit pour le trafic qui doit être tunnelisé.

```
ip local pool SSLVPN_POOL 192.168.10.1 192.168.10.10
access-list 1 permit 192.168.0.0 0.0.255.255
```

Étape 6. Configurer l'interface de modèle virtuel (VTI)

VTI dynamiques fournir une interface d'accès virtuel séparée à la demande pour chaque session VPN qui permet une connectivité hautement sécurisée et évolutive pour les VPN d'accès à distance. La technologie DVTI remplace les cartes de cryptage dynamiques et la méthode Hub and Spoke dynamique qui permet d'établir des tunnels. Comme les DVTI fonctionnent comme toute autre interface réelle, ils permettent un déploiement d'accès à distance plus complexe car ils prennent en charge la QoS, le pare-feu, les attributs par utilisateur et d'autres services de sécurité dès que le tunnel est actif.

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

Étape 7. Configurer la passerelle WebVPN

La passerelle WebVPN est ce qui définit l'adresse IP et les ports qui seront utilisés par la tête de réseau AnyConnect, ainsi que l'algorithme de chiffrement SSL et le certificat PKI qui seront

présentés aux clients. Par défaut, le modem routeur prend en charge tous les algorithmes de chiffrement possibles, qui varient en fonction de la version de Cisco IOS sur le routeur.

```
webvpn gateway SSLVPN_GATEWAY
 ip address 209.165.201.1 port 443
 http-redirect port 80
 ssl trustpoint SSLVPN_CERT
 inservice
```

Étape 8. Configurer le contexte WebVPN et la stratégie de groupe

Le contexte WebVPN et la stratégie de groupe définissent des paramètres supplémentaires qui seront utilisés pour la connexion client AnyConnect. Pour une configuration AnyConnect de base, 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 davantage la page de démarrage WebVPN et le fonctionnement de WebVPN. Dans le groupe de stratégies défini, la liste SSLVPN_AAA est configurée en tant que liste d'authentification AAA dont les utilisateurs sont membres. La commande **fonctions activées par svc** est la partie de configuration qui permet aux utilisateurs de se connecter au client VPN SSL AnyConnect plutôt que de se connecter à WebVPN via un navigateur. Enfin, les commandes SVC supplémentaires définissent des paramètres qui ne concernent que les connexions SVC : **svc address-pool** indique au modem routeur de distribuer des adresses dans SSLVPN_POOL aux clients, **svc split include** définit la stratégie de tunnel partagé par ACL 1 définie ci-dessus et **svc dns-server** définit le serveur DNS qui sera utilisé pour la résolution de noms 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 détermine si le trafic est envoyé ou non dans le tunnel.

```
webvpn context SSLVPN_CONTEXT
virtual-template 1
 aaa authentication list SSLVPN_AAA
gateway SSLVPN_GATEWAY inservice
policy group SSLVPN_POLICY 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
default-group-policy SSLVPN_POLICY
```

Étape 9 (Facultatif) - Configurez un profil de client

Contrairement aux ASA, Cisco IOS n'a pas d'interface GUI intégrée qui puisse aider les administrateurs à créer le profil client. Le profil client AnyConnect doit être créé/modifié séparément avec l'éditeur de profil autonome.

> **Astuce** : Recherchez anyconnect-profileeditor-win-3.1.03103-k9.exe.

Procédez comme suit pour que le routeur déploie le profil :

- Téléchargez-le dans la mémoire Flash IOS à l'aide de ftp/tftp.
- Utilisez cette commande pour identifier le profil qui vient d'être téléchargé :

```
crypto vpn annyconnect profile SSLVPN_PROFILE flash:test-profile.xml
```

> **Astuce** : Sur les versions de Cisco IOS antérieures à 15.2(1)T, cette commande doit être

utilisée : **webvpn import svc profile <profile_name> flash:<profile.xml>**

3. Dans le contexte, utilisez cette commande pour lier le profil à ce contexte :

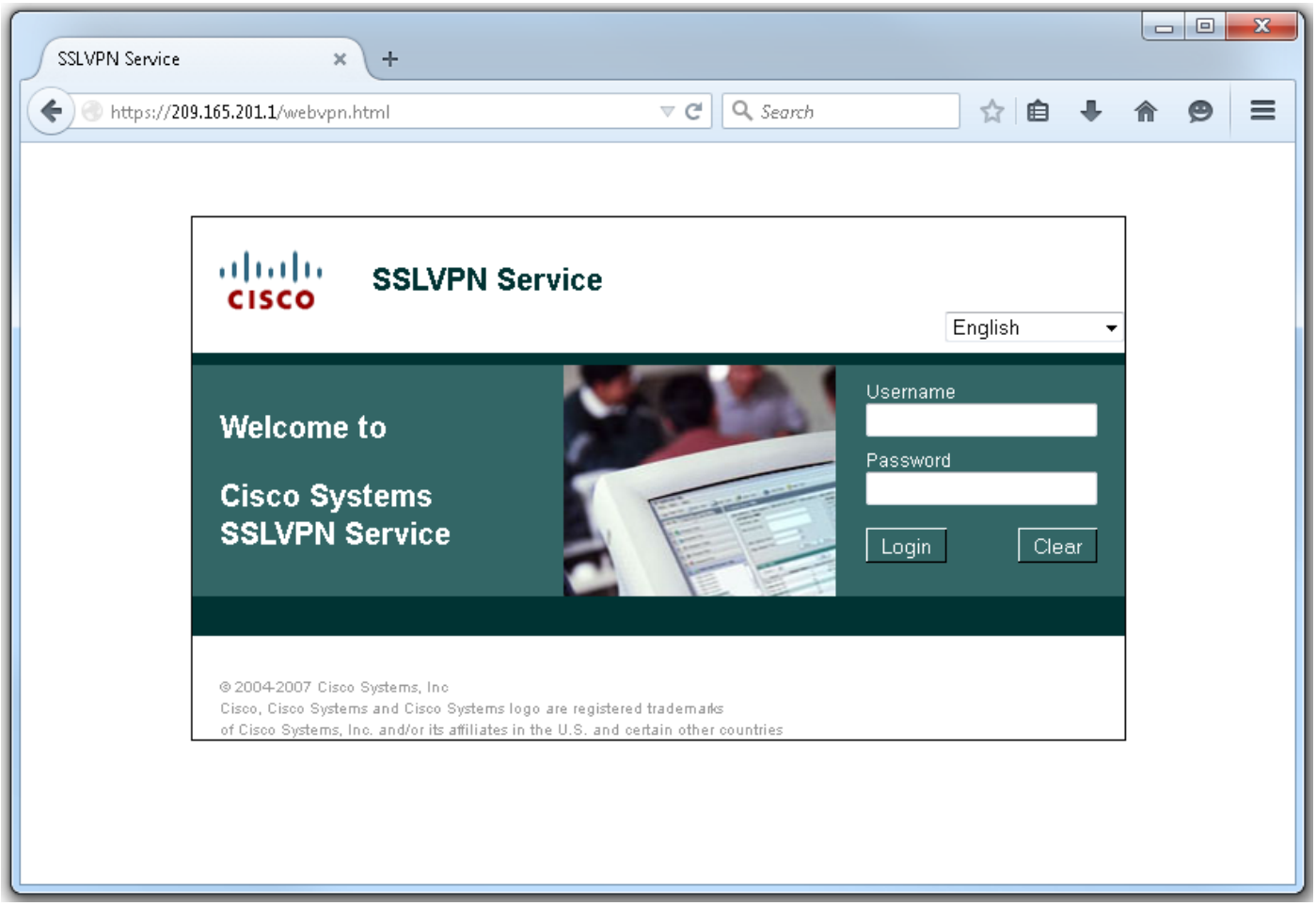
```
webvpn context SSLVPN_CONTEXT
 policy group SSLVPN_POLICY
 svc profile SSLVPN_PROFILE
```

Remarque: Utilisez l'Outil de recherche de commande (clients inscrits seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

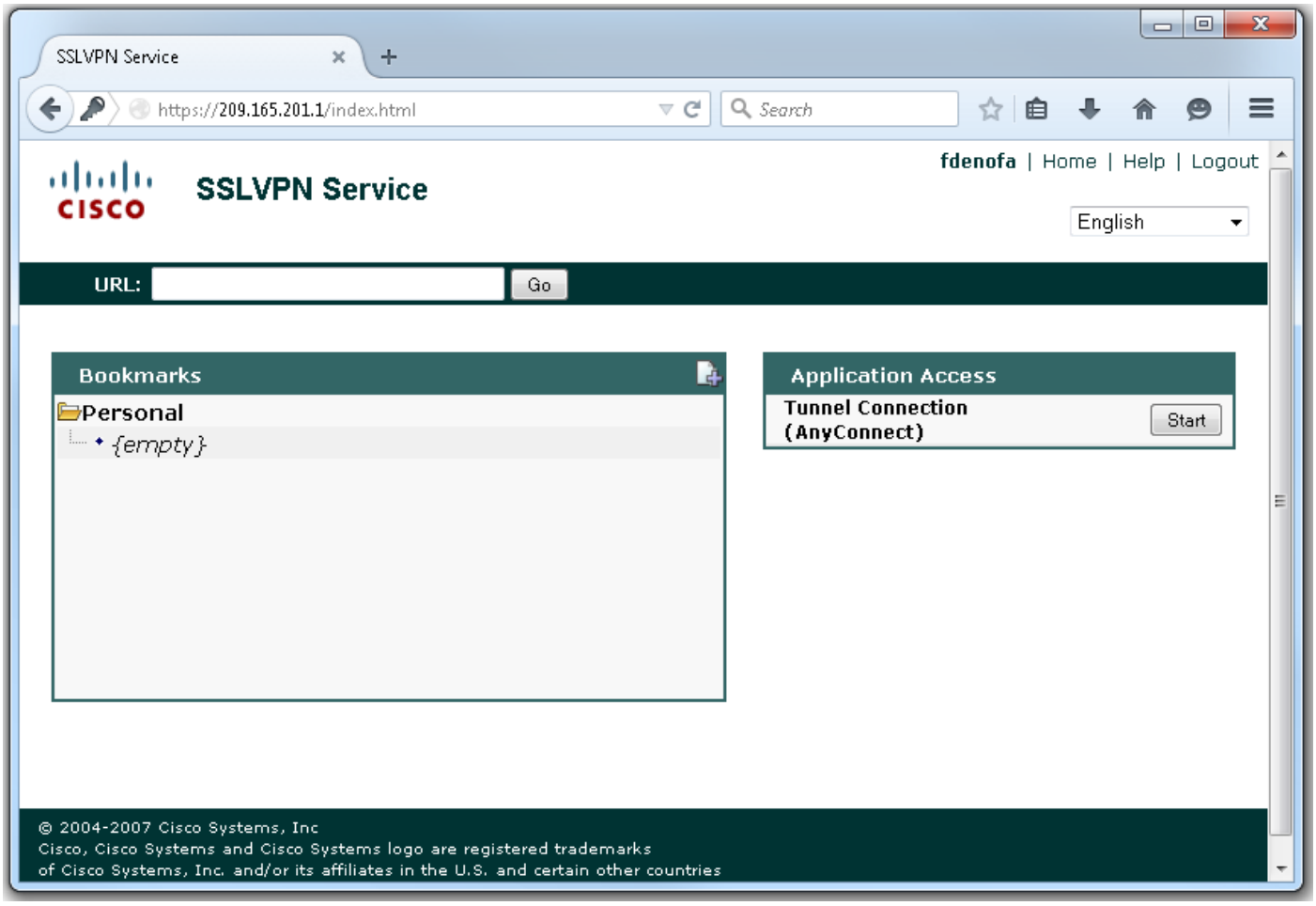
Vérification

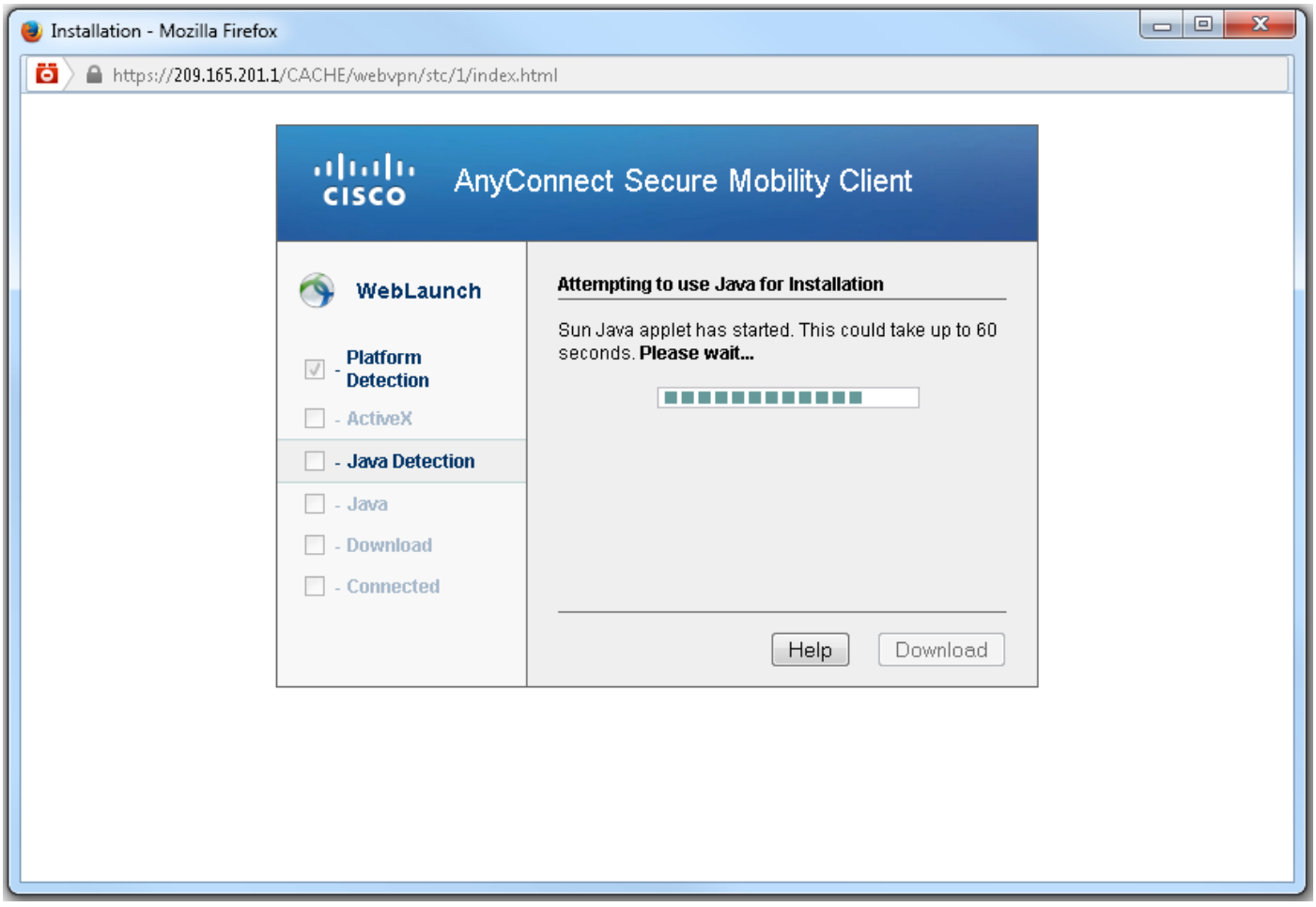
Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Une fois la configuration terminée, lorsque vous accédez à l'adresse et au port du modem routeur via le navigateur, il revient à la page d'accueil WebVPN.



Après vous être connecté, la page d'accueil WebVPN s'affiche. À partir de là, cliquez sur **Tunnel Connection (AnyConnect).** Lorsqu'Internet Explorer est utilisé, ActiveX est utilisé pour pousser vers le bas et installer le client AnyConnect. Si elle n'est pas détectée, Java sera utilisé à la place. Tous les autres navigateurs utilisent Java immédiatement.

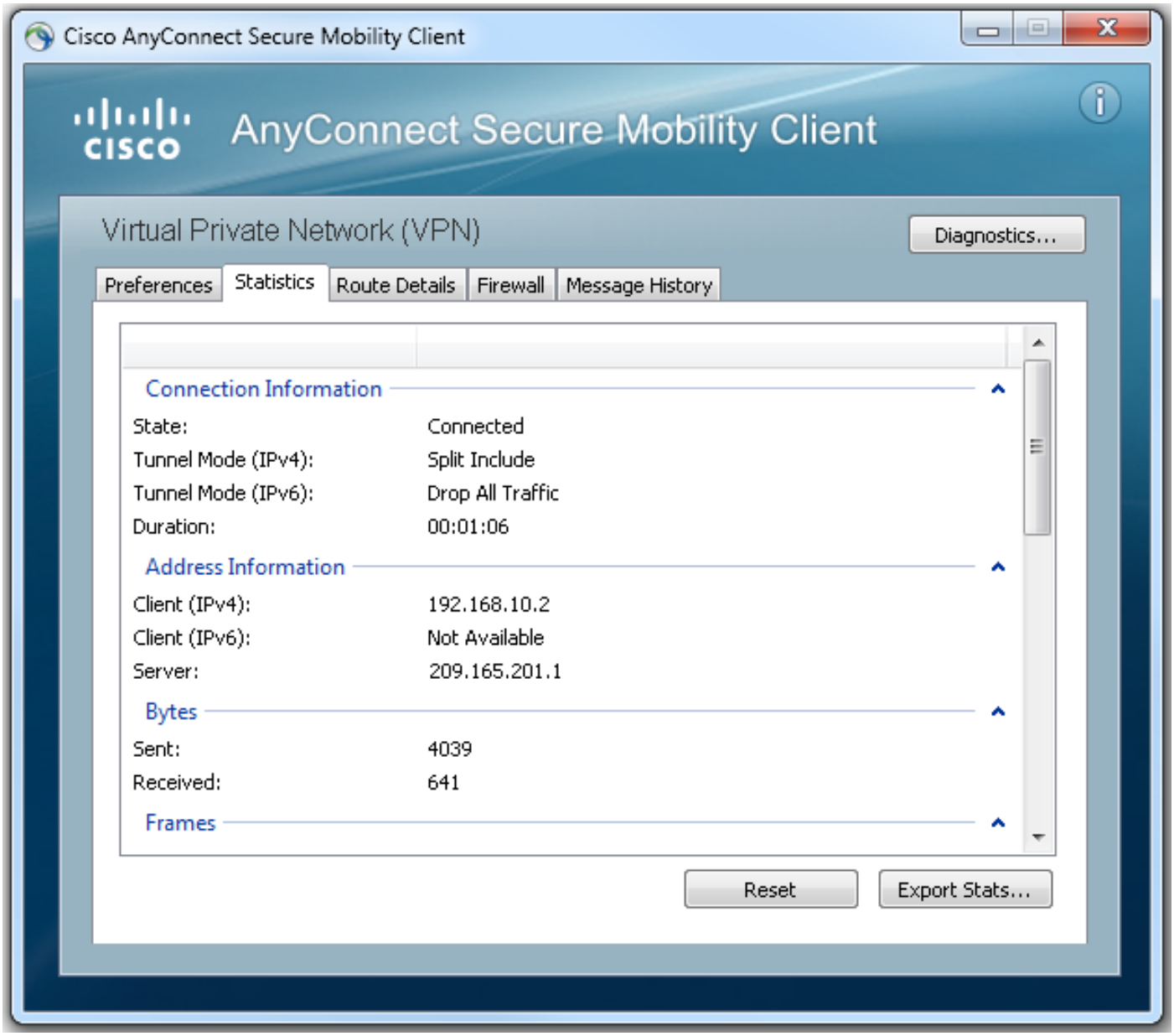


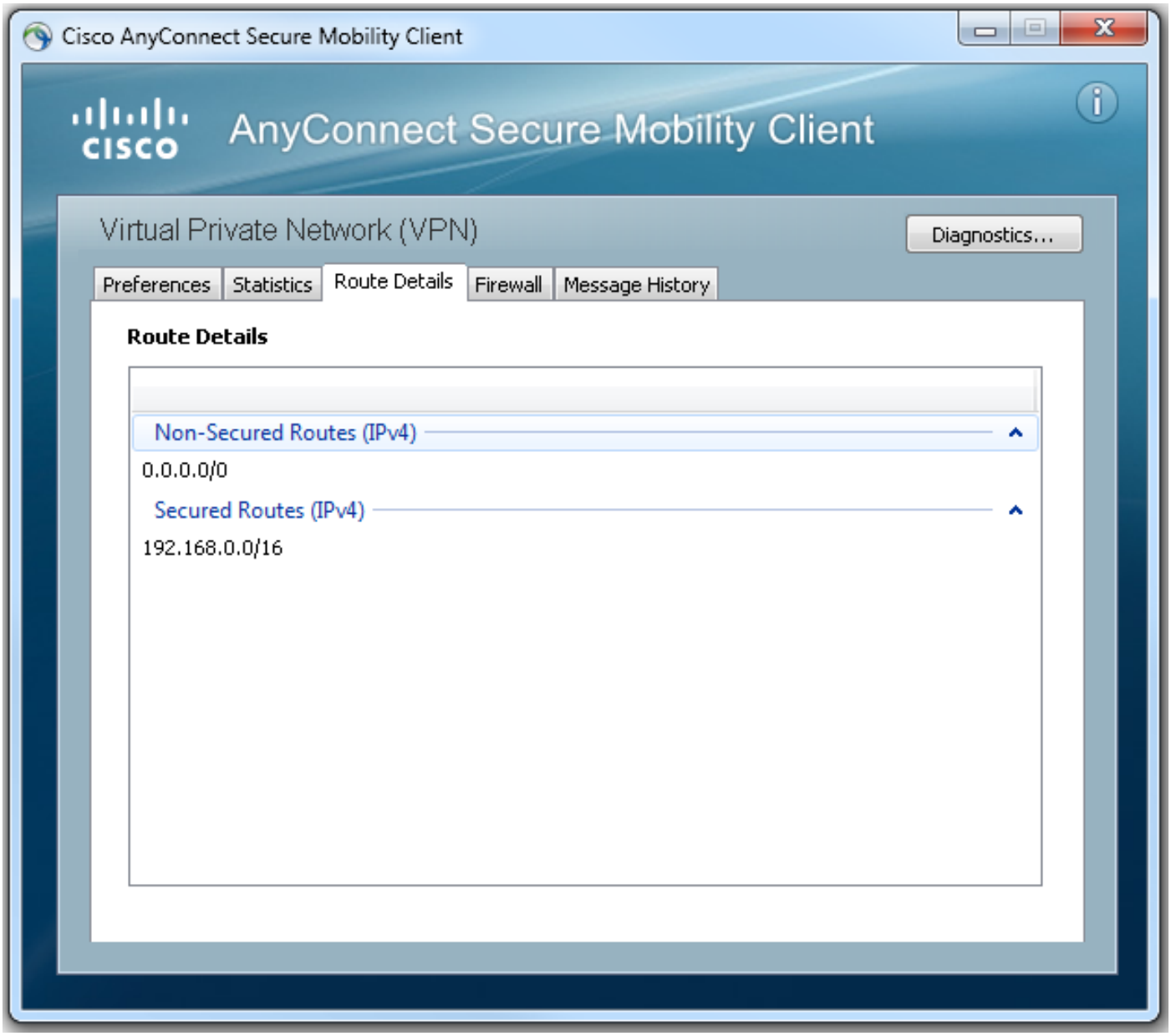


Une fois l'installation terminée, AnyConnect tente automatiquement de se connecter à la passerelle WebVPN. Lorsqu'un certificat auto-signé est utilisé pour que le modem routeur

s'identifie, plusieurs avertissements de certificat s'affichent lors de la tentative de connexion. Celles-ci sont attendues et doivent être acceptées pour que la connexion continue. Afin d'éviter ces avertissements de certificat, le certificat auto-signé présenté doit être installé dans le magasin de certificats de confiance de l'ordinateur client, ou si un certificat tiers est utilisé, le certificat d'autorité de certification doit être dans le magasin de certificats de confiance.

Une fois la négociation de la connexion terminée, cliquez sur l'icône **engrenage** dans la partie inférieure gauche d'AnyConnect. Elle affiche des informations avancées sur la connexion. Sur cette page, il est possible d'afficher certaines statistiques de connexion et les détails de route obtenus à partir de la liste de contrôle d'accès du tunnel partagé dans la configuration de la stratégie de groupe.


Cisco AnyConnect Secure Mobility Client
AnyConnect Secure Mobility Client
Virtual Private Network (VPN)
Diagnostics...
Preferences
Statistics
Route Details
Firewall
Message History
Connection Information
State: Connected
Tunnel Mode (IPv4): Split Include
Tunnel Mode (IPv6): Drop All Traffic
Duration: 00:01:06
Address Information
Client (IPv4): 192.168.10.2
Client (IPv6): Not Available
Server: 209.165.201.1
Bytes
Sent: 4039
Received: 641
Frames
Reset
Export Stats...



Voici le résultat final de la configuration en cours des étapes de configuration :

```
crypto pki trustpoint SSLVPN_TP_SELFSIGNED
 enrollment selfsigned
 serial-number
 subject-name cn=892_SELF_SIGNED_CERT
 revocation-check none
 rsakeypair SELF_SIGNED_RSA
!
crypto vpn anyconnect flash:/webvpn/anyconnect-win-3.1.08009-k9.pkg sequence 1
crypto vpn anyconnect profile SSLVPN_PROFILE flash:test-profile.xml ! access-list 1 permit
192.168.0.0 0.0.255.255 ! ip local pool SSLVPN_POOL 192.168.10.1 192.168.10.10 ! webvpn gateway
SSLVPN_GATEWAY ip address 209.165.201.1 port 443 ssl trustpoint SSLVPN_TP_SELFSIGNED inservice !
webvpn context SSLVPN_CONTEXT virtual-template 1
aaa authentication list SSLVPN_AAA
gateway SSLVPN_GATEWAY
! ssl authenticate verify all inservice ! policy group SSLVPN_POLICY 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
svc profile SSLVPN_PROFILE default-group-policy SSLVPN_POLICY
```

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Il existe quelques composants courants à vérifier lorsque vous dépannez des problèmes de connexion AnyConnect :

- Comme le client doit présenter un certificat, le certificat spécifié dans la passerelle WebVPN doit être valide. Pour émettre un **certificat show crypto pki**, les informations relatives à tous les certificats du routeur seront affichées.
- Àchaque fois qu'une modification est apportée à la configuration WebVPN, il est recommandé d'émettre un no inservice et inservice sur le modem routeur et le contexte. Cela permet de s'assurer que les modifications prennent effet correctement.
- Comme mentionné précédemment, il est nécessaire d'avoir un PKG AnyConnect pour chaque système d'exploitation client qui se connectera à ce modem routeur. Par exemple, les clients Windows ont besoin d'un PKG Windows, les clients Linux 32 bits ont besoin d'un PKG Linux 32 bits, etc.
- Lorsque vous considérez que le client AnyConnect et le WebVPN basé sur navigateur utilisent SSL, être en mesure d'accéder à la page d'accueil WebVPN indique généralement qu'AnyConnect sera en mesure de se connecter (supposez que la configuration AnyConnect appropriée est correcte).

Cisco IOS propose diverses options de débogage de webvpn qui peuvent être utilisées pour dépanner les connexions défaillantes. Voici la sortie générée par debug webvpn aaa, debug wevpn tunnel et show webvpn session lors d'une tentative de connexion réussie :

```
fdenofa-892#show debugging


WebVPN Subsystem:
  WebVPN AAA debugging is on
  WebVPN tunnel debugging is on
  WebVPN Tunnel Events debugging is on
  WebVPN Tunnel Errors debugging is on


*May 26 20:11:06.381: WV-AAA: Nas Port ID set to 64.102.157.2.
*May 26 20:11:06.381: WV-AAA: AAA authentication request sent for user: "VPNUSER"AAA returned
status: 2 for session 37
*May 26 20:11:06.381: WV-AAA: AAA Authentication Passed!
*May 26 20:11:06.381: WV-AAA: User "VPNUSER" has logged in from "64.102.157.2" to gateway
"SSLVPN_GATEWAY"
             context "SSLVPN_CONTEXT"
*May 26 20:11:12.265:
*May 26 20:11:12.265:
*May 26 20:11:12.265: [WV-TUNL-EVT]:[8A3AE410] CSTP Version recd , using 1
*May 26 20:11:12.265: [WV-TUNL-EVT]:[8A3AE410] Allocating IP 192.168.10.9 from address-pool
SSLVPN_POOL
*May 26 20:11:12.265: [WV-TUNL-EVT]:[8A3AE410] Using new allocated IP 192.168.10.9 255.255.255.0
*May 26 20:11:12.265:  Inserting static route: 192.168.10.9 255.255.255.255 Virtual-Access2 to
routing table
*May 26 20:11:12.265: [WV-TUNL-EVT]:[8A3AE410] Full Tunnel CONNECT request processed, HTTP reply
created
*May 26 20:11:12.265: HTTP/1.1 200 OK
*May 26 20:11:12.265: Server: Cisco IOS SSLVPN
```

```
*May 26 20:11:12.265: X-CSTP-Version: 1
*May 26 20:11:12.265: X-CSTP-Address: 192.168.10.9
*May 26 20:11:12.269: X-CSTP-Netmask: 255.255.255.0
*May 26 20:11:12.269: X-CSTP-Keep: false
*May 26 20:11:12.269: X-CSTP-DNS: 8.8.8.8
*May 26 20:11:12.269: X-CSTP-Lease-Duration: 43200
*May 26 20:11:12.269: X-CSTP-MTU: 1280
*May 26 20:11:12.269: X-CSTP-Split-Include: 192.168.0.0/255.255.0.0
*May 26 20:11:12.269: X-CSTP-DPD: 300
*May 26 20:11:12.269: X-CSTP-Disconnected-Timeout: 2100
*May 26 20:11:12.269: X-CSTP-Idle-Timeout: 2100
*May 26 20:11:12.269: X-CSTP-Session-Timeout: 0
*May 26 20:11:12.269: X-CSTP-Keepalive: 30
*May 26 20:11:12.269: X-DTLS-Session-ID:
85939A3FE33ABAE5F02F8594D56DEDE389F6FB3C9EEC4D211EB71C0820DF8DC8
*May 26 20:11:12.269: X-DTLS-Port: 443
*May 26 20:11:12.269: X-DTLS-Header-Pad-Length: 3
*May 26 20:11:12.269: X-DTLS-CipherSuite: AES256-SHA
*May 26 20:11:12.269: X-DTLS-DPD: 300
*May 26 20:11:12.269: X-DTLS-KeepAlive: 30
*May 26 20:11:12.269:
*May 26 20:11:12.269:
*May 26 20:11:12.269:
*May 26 20:11:12.269: [WV-TUNL-EVT]:[8A3AE410] For User VPNUSER, DPD timer started for 300
seconds
*May 26 20:11:12.273: [WV-TUNL-EVT]:[8A3AE410] CSTP Control, Recvd a Req Cntl Frame (User
VPNUSER, IP 192.168.10.9)
Severity ERROR, Type CLOSE_ERROR
Text: reinitiate tunnel to negotiate a different MTU
*May 26 20:11:12.273: [WV-TUNL-EVT]:[8A3AE410] CSTP Control, Recvd Close Error Frame
*May 26 20:11:14.105:
*May 26 20:11:14.105:
*May 26 20:11:14.105: [WV-TUNL-EVT]:[8A3AE690] CSTP Version recd , using 1
*May 26 20:11:14.109: [WV-TUNL-EVT]:[8A3AE690] Tunnel Client reconnecting removing existing tunl
ctx
*May 26 20:11:14.109: [WV-TUNL-EVT]:[8A3AE410] Closing Tunnel Context 0x8A3AE410 for Session
0x8A3C2EF8 and User VPNUSER
*May 26 20:11:14.109: [WV-TUNL-EVT]:[8A3AE690] Reusing IP 192.168.10.9 255.255.255.0
*May 26 20:11:14.109:  Inserting static route: 192.168.10.9 255.255.255.255 Virtual-Access2 to
routing table
*May 26 20:11:14.109: [WV-TUNL-EVT]:[8A3AE690] Full Tunnel CONNECT request processed, HTTP reply
created
*May 26 20:11:14.109: HTTP/1.1 200 OK
*May 26 20:11:14.109: Server: Cisco IOS SSLVPN
*May 26 20:11:14.109: X-CSTP-Version: 1
*May 26 20:11:14.109: X-CSTP-Address: 192.168.10.9
*May 26 20:11:14.109: X-CSTP-Netmask: 255.255.255.0
*May 26 20:11:14.109: X-CSTP-Keep: false
*May 26 20:11:14.109: X-CSTP-DNS: 8.8.8.8
*May 26 20:11:14.113: X-CSTP-Lease-Duration: 43200
*May 26 20:11:14.113: X-CSTP-MTU: 1199
*May 26 20:11:14.113: X-CSTP-Split-Include: 192.168.0.0/255.255.0.0
*May 26 20:11:14.113: X-CSTP-DPD: 300
*May 26 20:11:14.113: X-CSTP-Disconnected-Timeout: 2100
*May 26 20:11:14.113: X-CSTP-Idle-Timeout: 2100
*May 26 20:11:14.113: X-CSTP-Session-Timeout: 0
*May 26 20:11:14.113: X-CSTP-Keepalive: 30
*May 26 20:11:14.113: X-DTLS-Session-ID:
22E54D9F1F6344BCB5BB30BC8BB3737907795E6F3C3665CDD294CBBA1DA4D0CF
*May 26 20:11:14.113: X-DTLS-Port: 443
*May 26 20:11:14.113: X-DTLS-Header-Pad-Length: 3
*May 26 20:11:14.113: X-DTLS-CipherSuite: AES256-SHA
*May 26 20:11:14.113: X-DTLS-DPD: 300
*May 26 20:11:14.113: X-DTLS-KeepAlive: 30
```

```
*May 26 20:11:14.113:
*May 26 20:11:14.113:
*May 26 20:11:14.113:
*May 26 20:11:14.113: [WV-TUNL-EVT]:[8A3AE690] For User VPNUSER, DPD timer started for 300
seconds
```

```
fdenofa-892#show webvpn session user VPNUSER context SSLVPN_CONTEXT

Session Type      : Full Tunnel
Client User-Agent : AnyConnect Windows 3.1.08009

Username          : VPNUSER              Num Connection : 5
Public IP         : 64.102.157.2         VRF Name       : None
Context           : SSLVPN_CONTEXT       Policy Group   : SSLVPN_POLICY
Last-Used         : 00:00:00             Created        : *16:11:06.381 EDT Tue May 26 2015
Session Timeout   : Disabled             Idle Timeout   : 2100
DNS primary serve : 8.8.8.8
DPD GW Timeout    : 300                  DPD CL Timeout : 300
Address Pool      : SSLVPN_POOL          MTU Size       : 1199
Rekey Time        : 3600                 Rekey Method   :
Lease Duration    : 43200
Tunnel IP         : 192.168.10.9         Netmask        : 255.255.255.0
Rx IP Packets     : 0                    Tx IP Packets  : 42
CSTP Started      : 00:00:13             Last-Received  : 00:00:00
CSTP DPD-Req sent : 0                    Virtual Access : 2
Msie-ProxyServer  : None                 Msie-PxyPolicy : Disabled
Msie-Exception    :
Split Include     : ACL 1
Client Ports      : 17462 17463 17464 17465 17471
```

Informations connexes

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