AnyConnect により、CLIを使用したCisco IOSルータヘッドエンドの基本的なSSL VPNの設定

概要

内容

このドキュメントでは、AnyConnectセキュアソケットレイヤ(SSL VPN)ヘッドエンドとしてのCisco IOS®ルータの基本設定について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco IOS
- AnyConnect セキュア モビリティ クライアント
- 一般的なSSL操作

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- 15.3(3)M5が稼働するCisco 892Wルータ
- AnyConnectセキュアモビリティクライアント3.1.08009

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

さまざまなIOSバージョンのライセンス情報

- securityk9フィーチャセットは、使用されているCisco IOSバージョンに関係なく、SSL VPN機能を使用するために必要です。
- Cisco IOS 12.x:SSL VPN機能は、12.xのすべてのイメージに統合されています。このイメージは、12.4(6)Tで始まり、少なくとも1つのセキュリティライセンス(SSL VPN)を持ちます。advsecurityk9、adventerprisek9など)。
- Cisco IOS 15.0：以前のバージョンでは、10、25、または100ユーザ接続を可能にするルータにLICファイルをインストールする必要があります。Right to Use*ライセンスは15.0(1)M4で実装されました
- Cisco IOS 15.1：以前のバージョンでは、10、25、または100ユーザ接続を許可するルータにLICファイルをインストールする必要があります。Right to Use*ライセンスは、15.1(1)T2、15.1(2)T2、15.1(3)T、および15.1(4)M1で実装されました
- Cisco IOS 15.2：すべての15.2バージョンでSSLVPNのRight to Use*ライセンスが提供されます
- Cisco IOS 15.3以降 – 以前のバージョンではRight to Use*ライセンスが提供されています。15.3(3)M以降では、securityk9テクノロジーパッケージにブートした後にSSLVPN機能を使用できます

RTUライセンスでは、最初のwebvpn機能(webvpn gateway GATEWAY1)が設定され、エンドユーザライセンス契約(EULA)が承認されると、評価ライセンスが有効になります。60日後、この評価ライセンスは無期限ライセンスになります。これらのライセンスは名誉に基づいており、機能を使用するためにペーパーライセンスを購入する必要があります。また、RTUでは、特定の使用回数に制限するのではなく、ルータプラットフォームが同時にサポートできる最大同時接続数を許可します。

ソフトウェアの大幅な機能拡張

これらのバグIDにより、AnyConnectの重要な機能または修正が行われました。

- CSCti89976:AnyConnect 3.xからIOSへのサポートを追加
- CSCtx38806:Fix for BEAST Vulnerability, Microsoft KB2585542

設定

ステップ1：ライセンスが有効であることを確認する

IOSルータヘッドエンドでAnyConnectを設定する最初のステップは、ライセンスが正しくインストールされ（該当する場合）、有効になっていることを確認することです。各バージョンのライセンスの詳細については、前のセクションのライセンス情報を参照してください。show licenseでSSL_VPNライセンスとsecurityk9ライセンスのどちらをリストするかは、コードとプラットフォームのバージョンによって異なります。バージョンとライセンスに関係なく、EULAに同意する必要があり、ライセンスが[Active]と表示されます。

ステップ2：ルータへのAnyConnectセキュアモビリティクライアントパッケージのアップロードとインストール

AnyConnectイメージをVPNにアップロードするには、ヘッドエンドに2つの目的があります。まず、AnyConnectヘッドエンドにAnyConnectイメージが存在するオペレーティングシステムだけが接続を許可されます。たとえば、Windowsクライアントではヘッドエンドにwindowsパッケージをインストールする必要があり、Linux 64ビットクライアントではLinux 64ビットパッケージをインストールする必要があります。次に、ヘッドエンドにインストールされたAnyConnectイメージは、接続時に自動的にクライアントマシンにプッシュされます。初めて接続するユーザは、Webポータルからクライアントをダウンロードでき、ヘッドエンドのAnyConnectパッケージがクライアントマシンにインストールされているよりも新しい場合は、戻るユーザもアップグレードできます。

AnyConnectパッケージは、シスコソフトウェアダウンロードのWebサイトのAnyConnectセキュアモビリティクライアントセクションから入手できます。使用可能なオプションは多数ありますが、ヘッドエンドにインストールするパッケージには、オペレーティングシステムとヘッドエンドの導入(PKG)のラベルが付けられます。 AnyConnectパッケージは現在、次のオペレーティングシステムプラットフォームで使用できます。Windows、Mac OS X、Linux（32ビット）、およびLinux 64ビット。Linuxの場合、32ビットと64ビットの両方のパッケージがあることに注意してください。各オペレーティングシステムでは、接続を許可するために、ヘッドエンドに適切なパッケージをインストールする必要があります。

AnyConnectパッケージをダウンロードしたら、TFTP、FTP、SCPまたはその他のオプションを使用して**copyコマンドを使用**して、ルータのフラッシュにアップロードできます。以下が一例です。

```
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)
```

AnyConnectイメージをルータのフラッシュにコピーした後、コマンドラインからインストールする必要があります。インストールコマンドの最後にシーケンス番号を指定すると、複数の

AnyConnectパッケージをインストールできます。これにより、ルータが複数のクライアントオペレーティングシステムのヘッドエンドとして機能できるようになります。AnyConnectパッケージをインストールすると、最初にAnyConnectパッケージがコピーされなかった場合、**AnyConnectパッケージもflash:/webvpn/ディレクトリ**に移動します。

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

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

15.2(1)Tより前にリリースされたコードのバージョンでは、PKGをインストールするコマンドは若干異なります。

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

ステップ3:RSAキーペアと自己署名証明書の生成

SSLまたは公開キーインフラストラクチャ(PKI)とデジタル証明書を実装する機能を設定する場合、証明書の署名にはRivest-Shamir-Adleman(RSA)キーペアが必要です。このコマンドはRSAキーペアを生成し、自己署名PKI証明書の生成時に使用されます。2048ビットのモジュラスを使用してください。これは必須ではありませんが、セキュリティを強化し、AnyConnectクライアントマシンとの互換性を高めるために使用可能な最大モジュラスを使用することをお勧めします。また、キー管理とともに割り当てられる記述的キーラベルを使用することをお勧めします。キーの生成は、**show crypto key mypubkey rsaコマンドで確認で**きます。

> **注**：RSAキーをエクスポート可能にすることに関連するセキュリティ上のリスクが多いため、デフォルトのエクスポート不可にキーを設定することを推奨します。このドキュメントでは、RSAキーをエクスポート可能にするときに関連するリスクについて説明します。PKI内でのRSAキーの展開」を参照してください。

```
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
```

RSAキーペアが正常に生成されたら、ルータの情報とRSAキーペアを使用してPKIトラストポイントを設定する必要があります。サブジェクト名の共通名(CN)は、ユーザがAnyConnectゲートウェイへの接続に使用するIPアドレスまたは完全修飾ドメイン名(FQDN)で設定する必要があります。この例では、クライアントが接続を試みるときに、fdenofa-SSLVPN.cisco.comのFQDNを使用します。必須ではありませんが、CNに正しく入力すると、ログイン時にプロンプトが表示される証明書エラーの数を減らすことができます。

> **注**：ルータによって生成された自己署名証明書を使用するのではなく、サードパーティCAによって発行された証明書を使用できます。これは、このドキュメントで説明する複数の異なる方法(PKIの証明書登録の構成)で行えます。

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

トラストポイントが正しく定義された後、ルータはcrypto pki enrollコマンドを使用して証明書を生成する必要**があります**。このプロセスでは、シリアル番号やIPアドレスなどの他のパラメータをいくつか指定できます。ただし、これは必須ではありません。証明書の生成は、**show crypto pki certificatesコマンドで確認で**きます。

```
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
```

ステップ4：ローカルVPNユーザアカウントの設定

外部の認証、許可、アカウンティング(AAA)サーバを使用できますが、この例ではローカル認証が使用されます。これらのコマンドは、ユーザ名VPNUSERを作成し、SSLVPN_AAAという名前のAAA認証リストも作成します。

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

ステップ5：クライアントが使用するアドレスプールとスプリットトンネルアクセスリストの定義

AnyConnectクライアントアダプタがIPアドレスを取得するには、ローカルIPアドレスプールを作成する必要があります。同時AnyConnectクライアント接続の最大数をサポートするのに十分な大きさのプールを設定してください。

デフォルトでは、AnyConnectはフルトンネルモードで動作します。つまり、クライアントマシンによって生成されたトラフィックはトンネル経由で送信されます。これは通常は望ましくないため、アクセスコントロールリスト(ACL)を設定して、トンネル経由で送信する必要があるトラフィックを定義できます。他のACL実装と同様に、最後の暗黙的なdenyによって明示的なdenyが不要になります。したがって、必要なのは、トンネル化する必要があるトラフィックに対してpermit文を設定することだけです。

```
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
```

手順6：仮想テンプレートインターフェイス(VTI)を設定する

ダイナミックVTI リモートアクセスVPNの安全性と拡張性の高い接続を可能にする、オンデマンドの個別の仮想アクセスインターフェイスをVPNセッションごとに提供します。DVTIテクノロジーは、ダイナミック暗号マップと、トンネルの確立に役立つダイナミックハブアンドスポーク方式を置き換えます。 DVTIは他の実インターフェイスと同様に機能するため、トンネルがアクティブになるとすぐにQoS、ファイアウォール、ユーザごとの属性、およびその他のセキュリティサービスをサポートするため、リモートアクセスの複雑な展開が可能です。

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

ステップ 7： WebVPN ゲートウェイの設定

WebVPNゲートウェイは、AnyConnectヘッドエンドで使用されるIPアドレスとポート、およびクライアントに提示されるSSL暗号化アルゴリズムとPKI証明書を定義するものです。デフォルトでは、ゲートウェイは可能なすべての暗号化アルゴリズムをサポートします。これは、ルータのCisco IOSバージョンによって異なります。

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

ステップ8:WebVPNコンテキストとグループポリシーの設定

WebVPNコンテキストとグループポリシーは、AnyConnectクライアント接続に使用される追加のパラメータをいくつか定義します。基本的なAnyConnect設定の場合、コンテキストは単に、AnyConnectに使用されるデフォルトのグループポリシーを呼び出すために使用されるメカニズムとして機能します。ただし、コンテキストを使用して、WebVPNスプラッシュページとWebVPN操作をさらにカスタマイズできます。定義されたポリシーグループでは、SSLVPN_AAAリストが、ユーザが属するAAA認証リストとして設定されます。**functions svc-enabledコマンド**は、ユーザがブラウザ経由でWebVPNだけでなくAnyConnect SSL VPN Clientに接続できるようにする設定です。最後に、追加のSVCコマンドは、SVC接続だけに関連するパラメータを定義します。**svc address-pool**は、SSLVPN_POOL内のアドレスをクライアントに配布するようにゲートウェイに指示します。**svc split include**は、上記で定義したACL 1ごとにスプリットトンネルポリシーを定義し、**svc dns-serverはドメイン名解決に使用されるDNSサーバをします。**この設定では、すべてのDNSクエリが指定されたDNSサーバに送信されます。クエリー応答で受信されたアドレスは、トラフィックがトンネルを介して送信されるかどうかを指定します。

```
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
```

ステップ9（オプション）クライアントプロファイルの設定

ASAとは異なり、Cisco IOSには、管理者がクライアントプロファイルを作成するのを支援できるGUIインターフェイスが組み込まれていません。AnyConnectクライアントプロファイルは、スタンドアロンプロファイルエディタを使用して別々に作成/編集する必要があります。

> **ヒント**：anyconnect-profileeditor-win-3.1.03103-k9.exeを探します。

ルータにプロファイルを展開させるには、次の手順を実行します。

- ftp/tftpを使用してIOSフラッシュにアップロードします。
- アップロードしたプロファイルを特定するには、次のコマンドを使用します。

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

> **ヒント**：15.2(1)Tより前のCisco IOSバージョンでは、**webvpn import svc profile <profile_name> flash:<profile.xml>**

3.コンテキストの下で、プロファイルをそのコンテキストにリンクするには、次のコマンドを使用します。

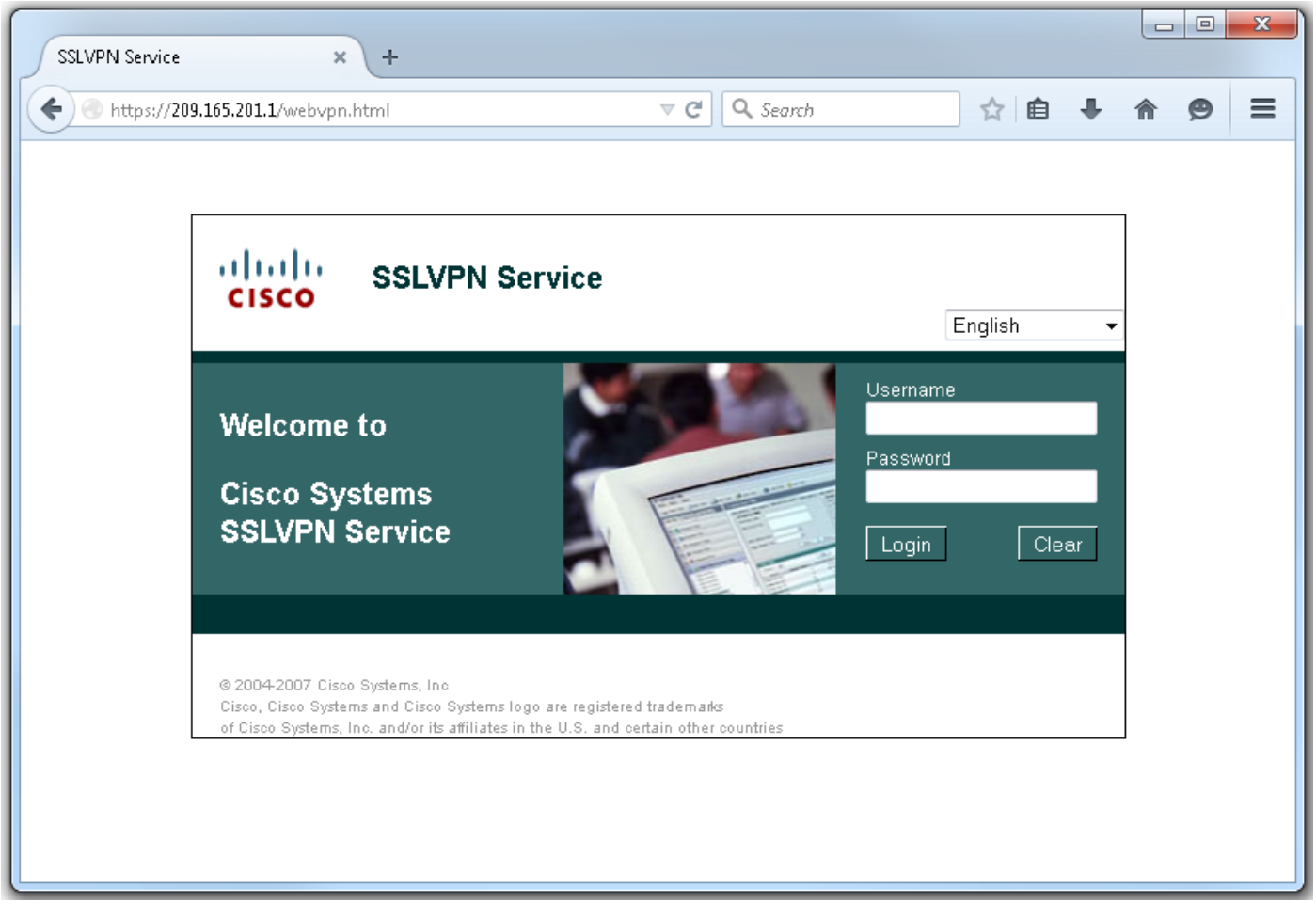
```
webvpn context SSLVPN_CONTEXT
 policy group SSLVPN_POLICY
 svc profile SSLVPN_PROFILE
```

> **注**：このセクションで使用されるコマンドの詳細については、Command Lookup Tool（登録ユーザ専用）を使用してください。

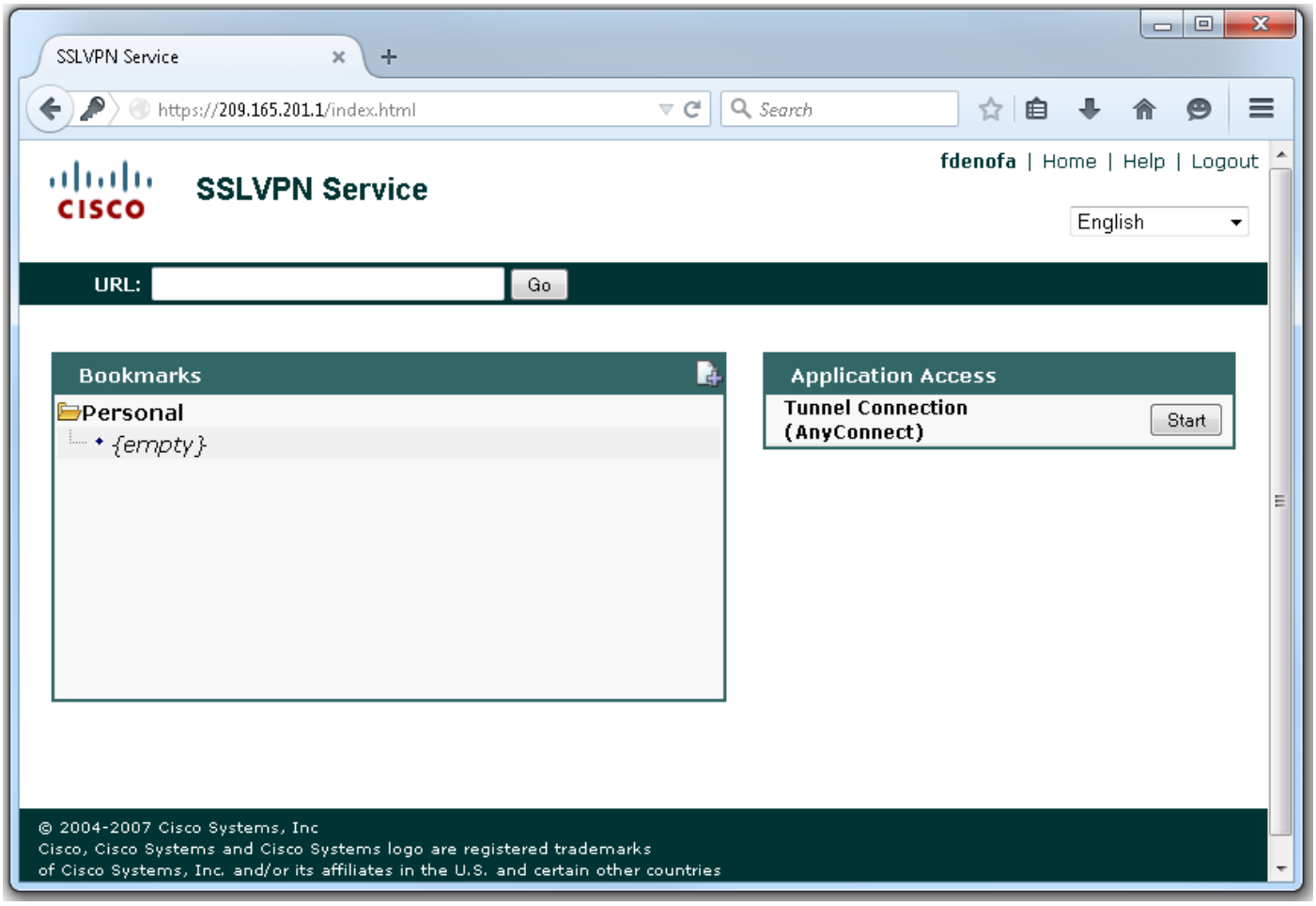
確認

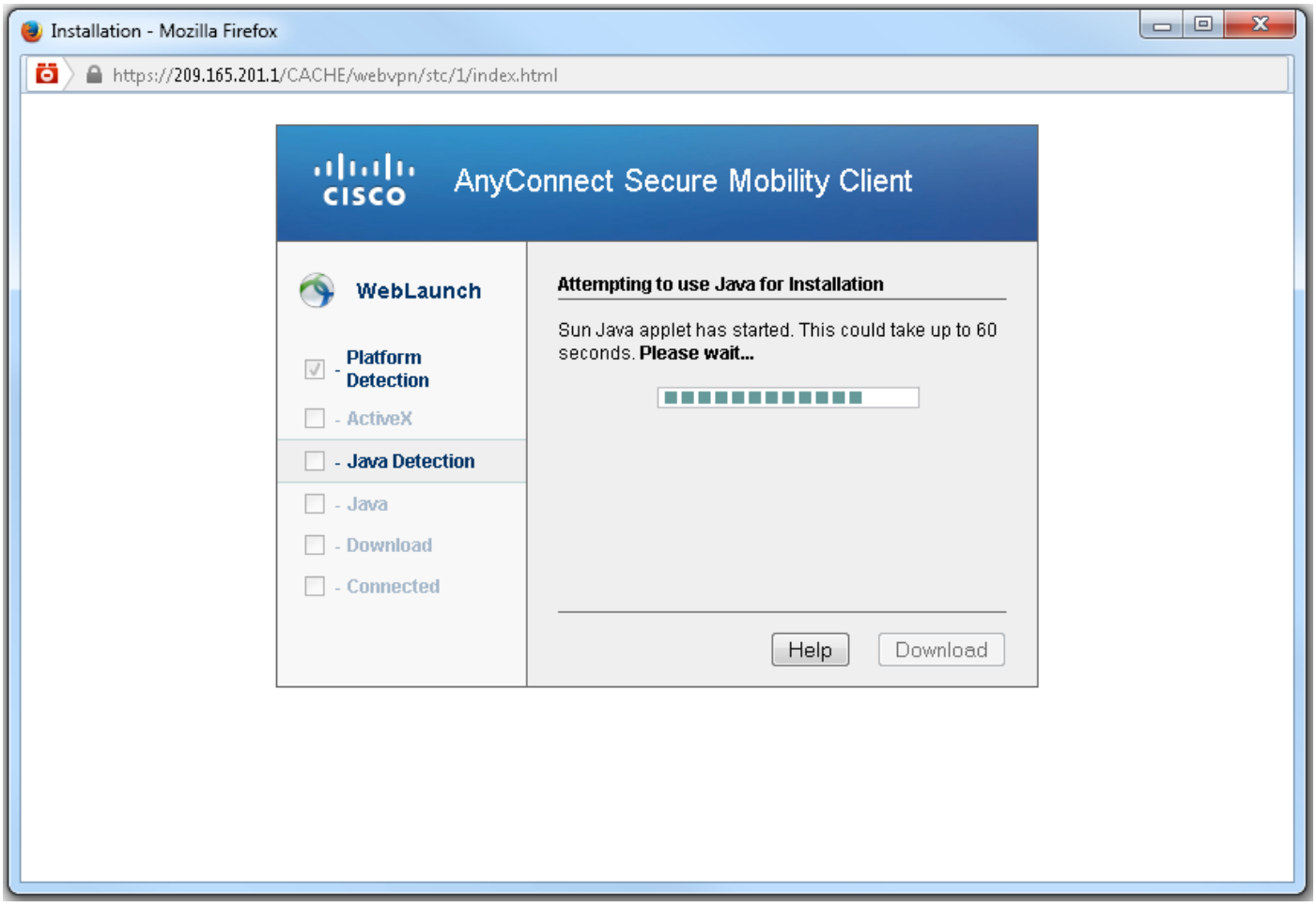
ここでは、設定が正常に機能しているかどうかを確認します。

設定が完了すると、ブラウザからゲートウェイアドレスとポートにアクセスすると、WebVPNスプラッシュページに戻ります。



ログインすると、WebVPNホームページが表示されます。ここから**[Tunnel Connection (AnyConnect)]をクリックします**。Internet Explorerを使用すると、ActiveXを使用してAnyConnectクライアントをプッシュダウンし、インストールします。検出されない場合は、代わりにJavaが使用されます。他のすべてのブラウザは、すぐにJavaを使用します。

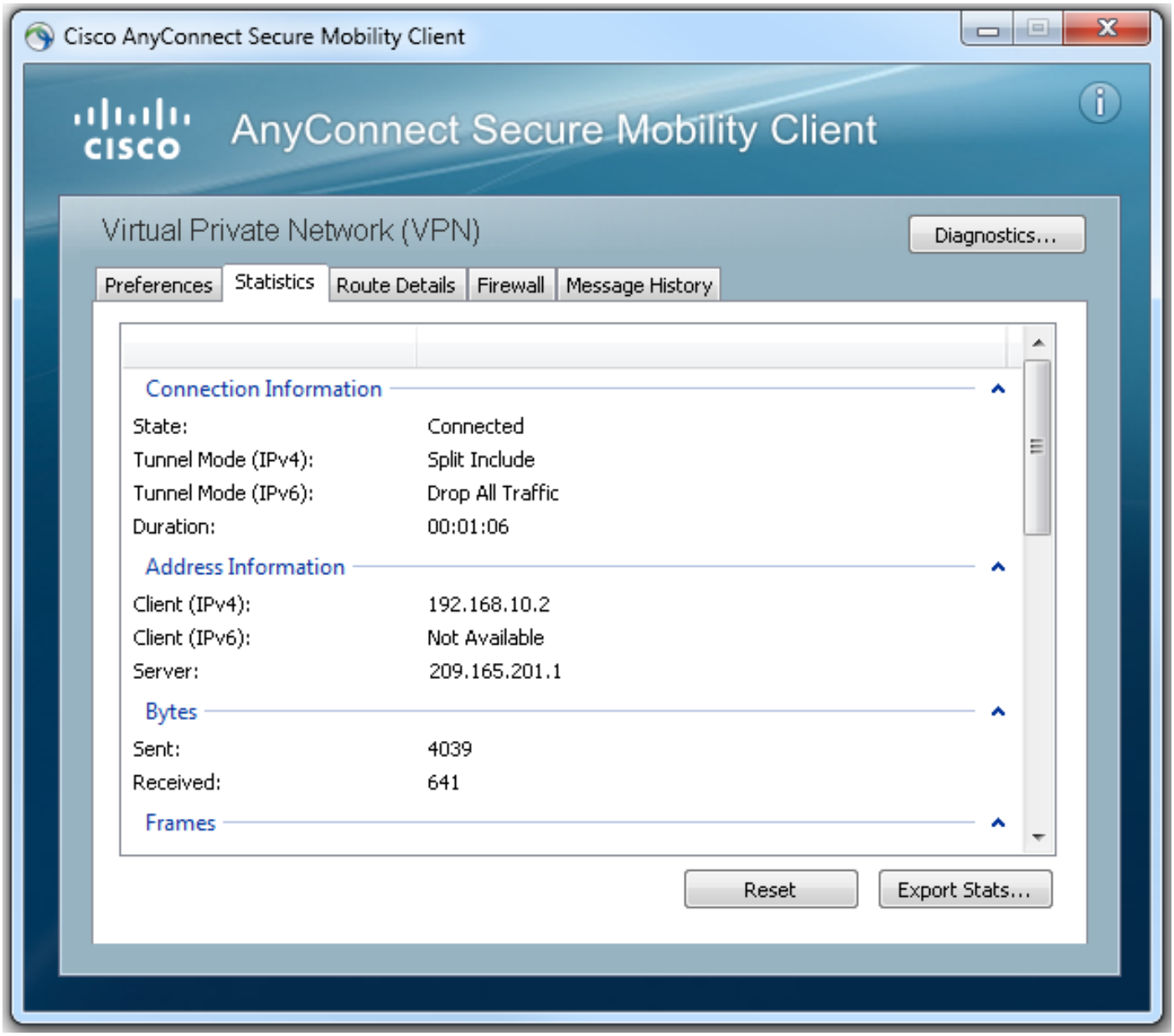


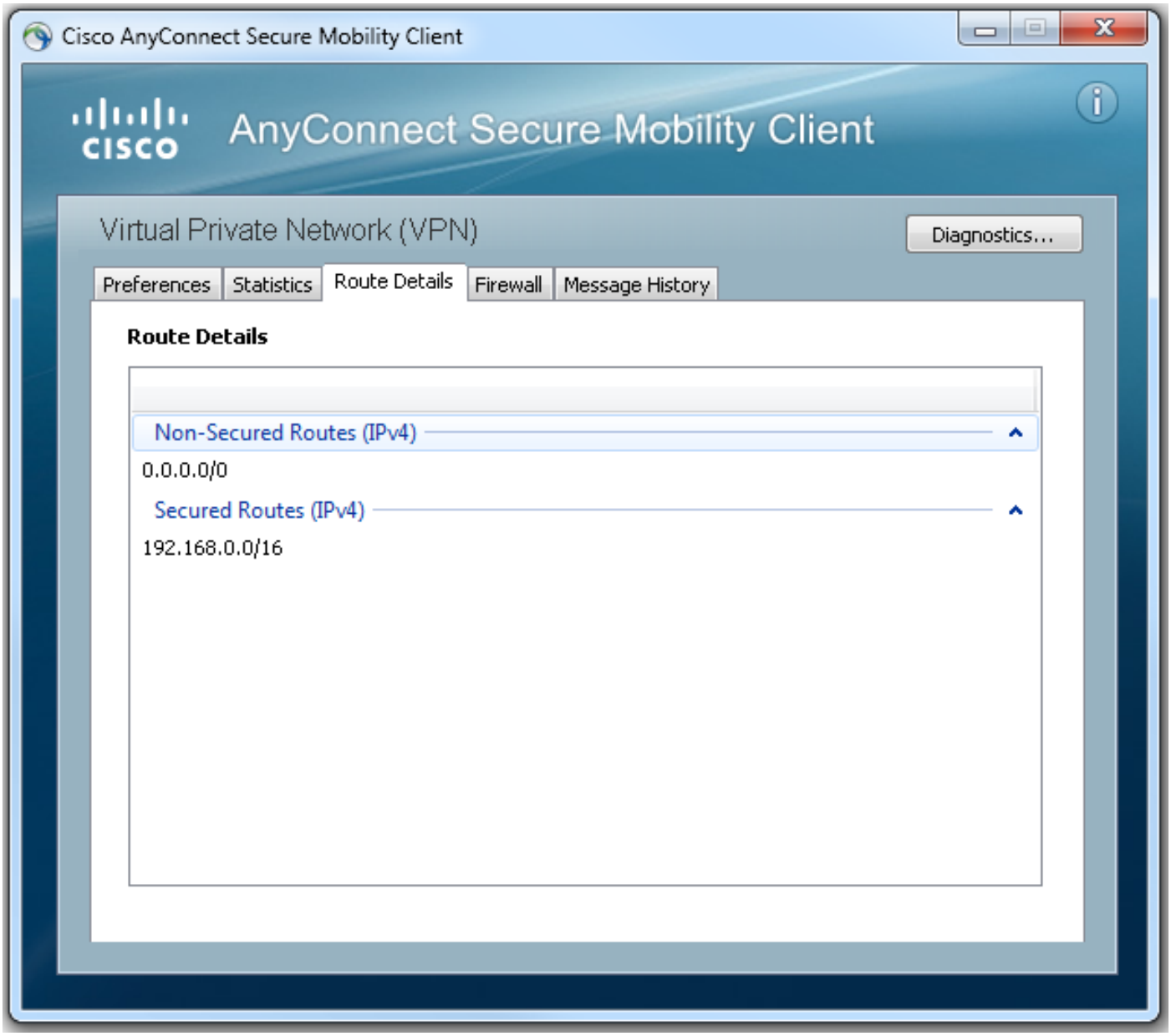


インストールが完了すると、AnyConnectは自動的にWebVPNゲートウェイへの接続を試行します。ゲートウェイが自身を識別するために自己署名証明書を使用しているため、接続の試行中に複

数の証明書警告が表示されます。接続を続行するには、これらが必要であり、承認される必要があります。これらの証明書の警告を回避するには、提示される自己署名証明書がクライアントマシンの信頼できる証明書ストアにインストールされているか、サードパーティ証明書が使用されている場合は、認証局(CA)証明書が信頼できる証明書ストアに保存されている必要があります。

接続がネゴシエーションを完了したら、AnyConnectの左下にある歯車アイコンをクリックします。接続に関する詳細情報が表示されます。このページでは、グループポリシー設定のスプリットトンネルACLから取得した接続統計情報とルートの詳細を表示できます。


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...



次に、設定手順による最終的な実行コンフィギュレーションの結果を示します。

```
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
```

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

AnyConnect接続の問題をトラブルシューティングする際にチェックする一般的なコンポーネントがいくつかあります。

- クライアントは証明書を提示する必要があるため、WebVPNゲートウェイで指定された証明書が有効であることが必要です。**show crypto pki certificate**を発行すると、ルータ上のすべての証明書に関連する情報が表示されます。
- WebVPN設定を変更する場合は常に、ゲートウェイとコンテキストの両方でサービスが無効でサービスが無効であることを確認することがベストプラクティスです。これにより、変更が正しく有効になります。
- 前述したように、このゲートウェイに接続する各クライアントオペレーティングシステムに対してAnyConnect PKGを用意することが要件です。たとえば、Windowsクライアントには Windows PKGが必要で、Linux 32ビットクライアントにはLinux 32ビットPKGが必要です。
- AnyConnectクライアントとブラウザベースのWebVPNの両方でSSLを使用することを検討すると、WebVPNスプラッシュページにアクセスできることは、一般にAnyConnectが接続できることを示します（関連するAnyConnect設定が正しいと仮定）。

Cisco IOSには、接続の失敗のトラブルシューティングに使用できるさまざまなdebug webvpnオプションがあります。次に、正常な接続試行時にdebug webvpn aaa、debug wevpn tunnel、およびshow webvpn sessionから生成された出力を示します。

```
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
```

関連情報

- SSL VPNコンフィギュレーションガイド、Cisco IOSリリース15M&T
- CCP による IOS ルータ上の AnyConnect VPN (SSL) クライアントの設定例
- テクニカル サポートとドキュメント – Cisco Systems