

Use AnyConnect to Configure Basic SSL VPN for Router Headend with CLI

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[License Information for Different IOS Versions](#)

[Significant Software Enhancements](#)

[Configure](#)

[Step 1. Confirm License is Enabled](#)

[Step 2. Upload and Install AnyConnect Secure Mobility Client Packageon Router](#)

[Step 3. GenerateRSA Keypair and Self-Signed Certificate](#)

[Step 4. Configure Local VPN User Accounts](#)

[Step 5. Define Address Pool and Split Tunnel Access List to be Used by Clients](#)

[Step 6. Configure the Virtual-Template Interface \(VTI\)](#)

[Step 7. Configure WebVPN Gateway](#)

[Step 8. Configure WebVPN Context and Group Policy](#)

[Step 9. Configure a Client Profile\(Optional\)](#)

[Verify](#)

[Troubleshoot](#)

[Related Information](#)

Introduction

This document describes the basic configuration of a Cisco IOS® Router as an AnyConnect Secure Sockets Layer VPN (SSL VPN) Headend.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco IOS
- AnyConnect Secure Mobility Client
- General SSL Operation

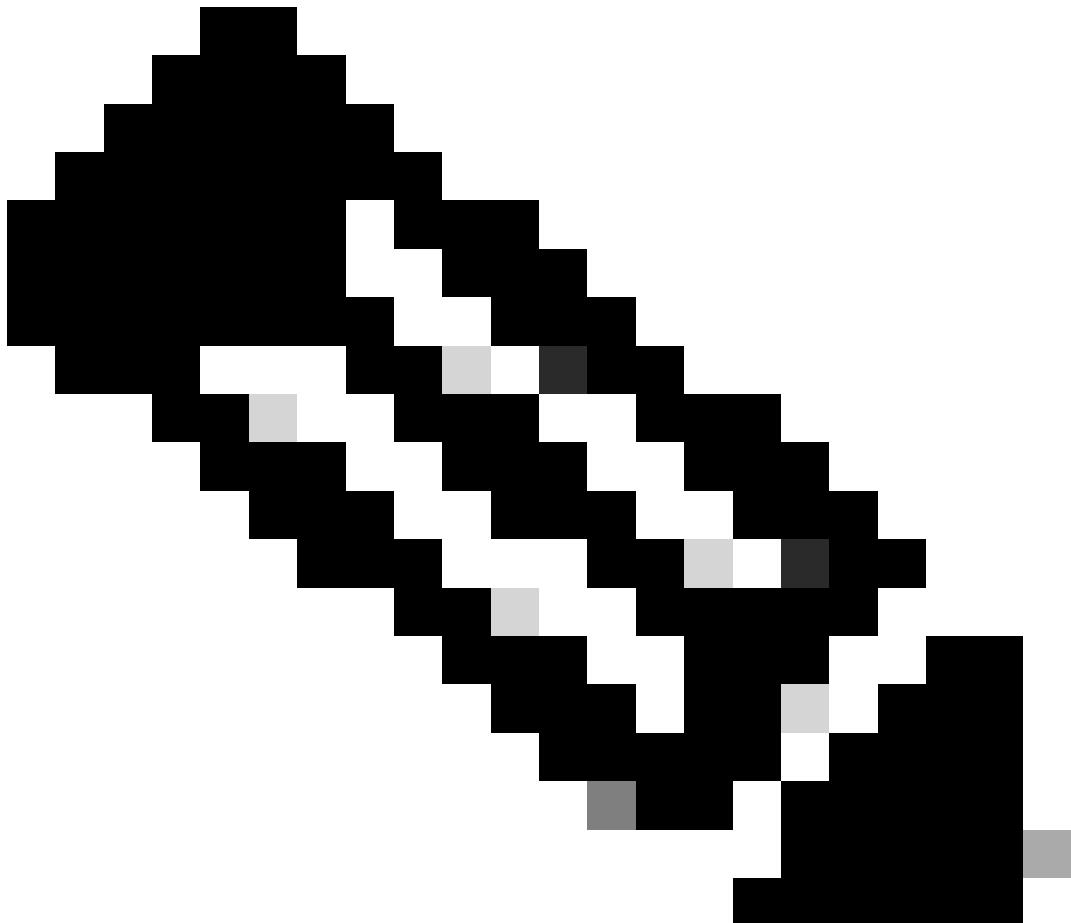
Components Used

The information in this document is based on these software and hardware versions:

- Cisco 892W Router with version 15.3(3)M5
- AnyConnect Secure Mobility Client 3.1.08009

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information



Note: AnyConnect has been rebranded to Cisco Secure Client. Nothing else changed, just the name, and the installation process is the same.

License Information for Different IOS Versions

- The securityk9 feature set is required to use the SSL VPN features, regardless of the Cisco IOS version is used.
- Cisco IOS 12.x - the SSL VPN feature is integrated into all 12.x images that start with 12.4(6)T which

- have at least a security license (that is, advsecurityk9, adenterprisek9, and so on).
- Cisco IOS 15.0 - earlier versions require a LIC file to be installed on the router, which allows for 10, 25, or 100 user connections. Right to Use* licenses were implemented in 15.0(1)M4.
 - Cisco IOS 15.1 - earlier versions require a LIC file to be installed on the router, which allows for 10, 25, or 100 user connections. Right to Use* licenses were implemented in 15.1(1)T2, 15.1(2)T2, 15.1(3)T, and 15.1(4)M1.
 - Cisco IOS 15.2 - all 15.2 versions offer Right to Use* licenses for SSL VPN.
 - Cisco IOS 15.3 and beyond - earlier versions offer the Right to Use* licenses. As of 15.3(3)M, the SSL VPN feature is available after you boot into a securityk9 technology-package.

For RTU licensing, an evaluation license is enabled when the first webvpn feature is configured (that is, webvpn gateway GATEWAY1) and the End User License Agreement (EULA) has been accepted. After 60 days, this evaluation license becomes a permanent license. These licenses are honor-based and require a paper license to be purchased in order to use the feature. Additionally, rather than the limitation of a certain number of uses, the RTU allows for the maximum number of simultaneous connections that the router platform can support concurrently.

Significant Software Enhancements

These bug IDs resulted in significant features or fixes for AnyConnect:

- Cisco bug ID [CSCti89976](#) Added support for AnyConnect 3.x to IOS.
- Cisco bug ID [CSCtx38806](#) Fix for BEAST Vulnerability, Microsoft KB2585542.

Configure

Step 1. Confirm License is Enabled

The first step when AnyConnect is configured on an IOS Router headend is to confirm that the license has been correctly installed (if applicable) and enabled. Refer to the licensing information in the previous section for the license specifics on different versions. It depends on the version of code and platform whether the show license lists an SSL_VPN or securityk9 license. Regardless of the version and license, the EULA needs to be accepted and the license then shows as Active.

Step 2. Upload and Install AnyConnect Secure Mobility Client Package on Router

In order to upload an AnyConnect image to the VPN, the headend serves two purposes. First, only operating systems that have AnyConnect images present on the AnyConnect headend are permitted to connect. For example, Windows clients require a Windows package to be installed on the headend, Linux 64-bit clients require a Linux 64-bit package to be installed, and so on. Second, the AnyConnect image installed on the headend is automatically pushed down to the client machine upon connection. Users who connect for the first time are able to download the client from the web portal and users who return are able to upgrade, provided the AnyConnect package on the headend is newer than what is installed on their client machine.

AnyConnect packages can be obtained through the AnyConnect Secure Mobility Client section of the [Cisco Software Downloads website](#). While there are many options available, the packages to be installed on the headend are labeled with the operating system and Head-end deployment (PKG). AnyConnect packages are currently available for these operating system platforms: Windows, Mac OS X, Linux (32-bit), and Linux 64-bit. For Linux, there are both 32- and 64-bit packages. Each operating system requires the proper

package to be installed on the headend in order for connections to be permitted.

Once the AnyConnect package has been downloaded, it can be uploaded to the router flash with the `copy` command by TFTP, FTP, SCP, or a few other options. Here is an example:

```
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)
```

After you copy the AnyConnect image to the flash of the router, it must be installed by the command line. Multiple AnyConnect packages can be installed when you specify a sequence number at the end of the installation command. This allows for the router to act as headend for multiple client operating systems. When you install the AnyConnect package, it also moves it to the `flash:/webvpn/` directory if it was not copied there initially.

```
crypto vpn anyconnect flash:/webvpn/anyconnect-win-3.1.08009-k9.pkg sequence 1  
SSLVPN Package SSL-VPN-Client (seq:1): installed successfully
```

On versions of code that were released before 15.2(1)T, the command to install the PKG is slightly different.

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

Step 3. Generate RSA Keypair and Self-Signed Certificate

When you configure SSL or any feature that implements Public Key Infrastructure (PKI) and digital certificates, a Rivest-Shamir-Adleman (RSA) keypair is required for the signing of the certificate. This command generates an RSA keypair, which then is used when the self-signed PKI certificate is generated. Make use of a modulus of 2048 bits, it is not a requirement but it is recommended to use the largest modulus available for enhanced security and compatibility with the AnyConnect client machines. It is also recommended to use a descriptive key label that assigns with key management. The key generation can be confirmed with the `show crypto key mypubkey rsa` command.

 **Note:** As there are many security risks when RSA keys are made exportable, the recommended

 practice is to ensure keys are configured to not be exportable, which is the default. The risks that are involved when you make the RSA keys exportable are discussed in this document: [Deploying RSA Keys Within a 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
```

Once the RSA keypair has successfully been generated, a PKI trustpoint must be configured with this router information and RSA keypair. The Common Name (CN) in the Subject-Name can be configured with the IP address or Fully Qualified Domain Name (FQDN) that users use to connect to the AnyConnect gateway. In this example, the clients use the FQDN of fdenofa-SSLVPN.cisco.com when they attempt to connect. While it is not mandatory, when you correctly enter in the CN, it helps reduce the number of certificate errors that are prompted at log in.

 **Note:** Rather than the use of a self-signed certificate generated by the router, it is possible to use a certificate issued by a third-party CA. This can be done by a few different methods, as discussed in this document: [Configuring Certificate Enrollment for a PKI](#).

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

After the trustpoint has been correctly defined, the router must generate the certificate by the use of the `crypto pki enroll` command. With this process, it is possible to specify a few other parameters, such as the serial

number and IP address; however, this is not required. The certificate generation can be confirmed with the `show crypto pki certificates` command.

```
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
```

Step 4. Configure Local VPN User Accounts

While it is possible to use an external Authentication, Authorization, and Accounting (AAA) server; for this example, local authentication is used. These commands create a user name `VPNUSER` and also create an AAA authentication list named `SSLVPN_AAA`.

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

Step 5. Define Address Pool and Split Tunnel Access List to be Used by Clients

A local IP address pool must be created in order for AnyConnect client adapters to obtain an IP address. Ensure you configure a large enough pool to support the maximum number of simultaneous AnyConnect client connections.

By default, AnyConnect operates in full tunnel mode, which means any traffic generated by the client machine is sent across the tunnel. As this is typically not desirable, it is possible to configure an Access Control List (ACL) that defines traffic, which can or cannot be sent across the tunnel. As with other ACL implementations, the implicit deny at the end eliminates the need for an explicit deny; therefore, it is only necessary to configure permit statements for the traffic that can be tunneled.

```
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
```

Step 6. Configure the Virtual-Template Interface (VTI)

[Dynamic VTIs](#) provide an on-demand separate Virtual-Access interface for each VPN session that allows highly secure and scalable connectivity for remote-access VPNs. The DVTI technology replaces dynamic crypto maps and the dynamic hub-and-spoke method that helps establish tunnels. Because DVTIs function like any other real interface they allow for more complex Remote Access deployment because they support QoS, firewall, per-user attributes and other security services as soon as the tunnel is active.

```
<#root>

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

Step 7. Configure WebVPN Gateway

The WebVPN Gateway is what defines the IP address and port(s) used by the AnyConnect headend, as well as the SSL encryption algorithm and PKI certificate presented to the clients. By default, the gateway supports all possible encryption algorithms, which vary, dependent on the Cisco IOS version on the router.

```
webvpn gateway SSLVPN_GATEWAY
 ip address 10.165.201.1 port 443
 http-redirect port 80
 ssl trustpoint SSLVPN_CERT
 inservice
```

Step 8. Configure WebVPN Context and Group Policy

The WebVPN Context and Group Policy define some additional parameters used for the AnyConnect client connection. For a basic AnyConnect configuration, the Context simply serves as a mechanism used to call the default Group Policy that is used for AnyConnect. However, the Context can be used to further customize the WebVPN splash page and WebVPN operation. In the defined Policy Group, the SSLVPN_AAA list is configured as the AAA authentication list that the users are a member of. The functions svc-enabled command is the piece of configuration that allows users to connect with the AnyConnect SSL VPN Client rather than just WebVPN through a browser. Last, the additional SVC commands define parameters that are relevant only to SVC connections: `svc address-pool` tells the gateway to handout addresses in the SSLVPN_POOL to the clients, `svc split include` defines the split tunnel policy per ACL 1 defined above, and `svc dns-server` defines the DNS server that is used for domain name resolution. With this configuration, all DNS queries are sent to the specified DNS server. The address received in the query response dictates whether or not the traffic is sent across the tunnel.

```
<#root>
```

```
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
```

Step 9. Configure a Client Profile (Optional)

Unlike on ASAs, Cisco IOS does not have a built-in GUI interface that can assist admins in the creation of the client profile. The AnyConnect client profile needs to be created/edited separately with the [Stand-Alone Profile Editor](#).

 **Tip:** Look for anyconnect-profileeditor-win-3.1.03103-k9.exe.

Perform these steps in order to have the router deploy the profile:

- Upload it to IOS Flash with the use of ftp/tftp.
- Use this command to identify the profile that was just uploaded:

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

 **Tip:** On Cisco IOS versions older than 15.2(1)T, this command needs to be used: webvpn import svc profile <profile_name> flash:<profile.xml>.

Under the context, use this command to link the profile to that context:

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

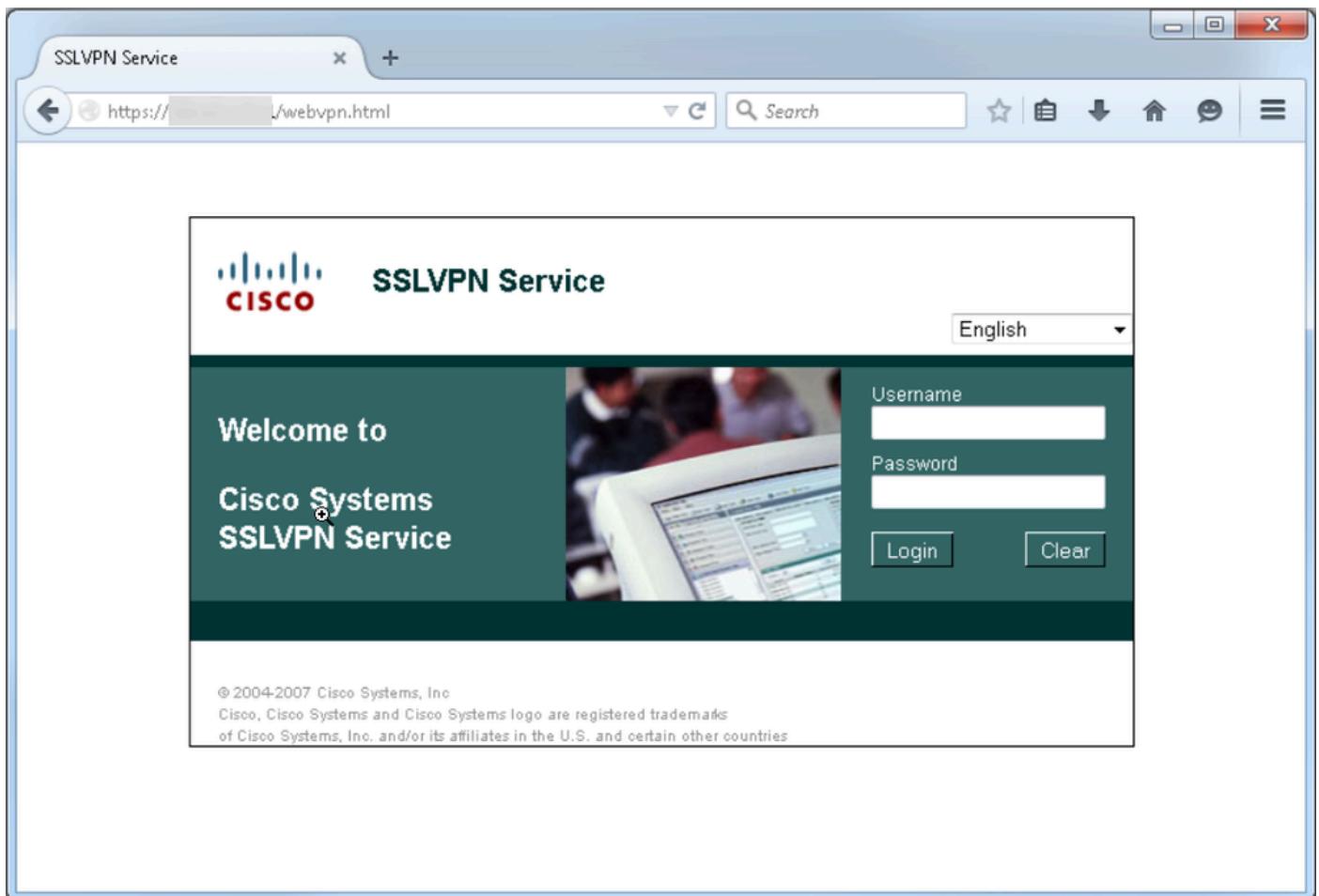
 **Note:** Use the [Command Lookup Tool](#) in order to obtain more information on the commands used in this section.

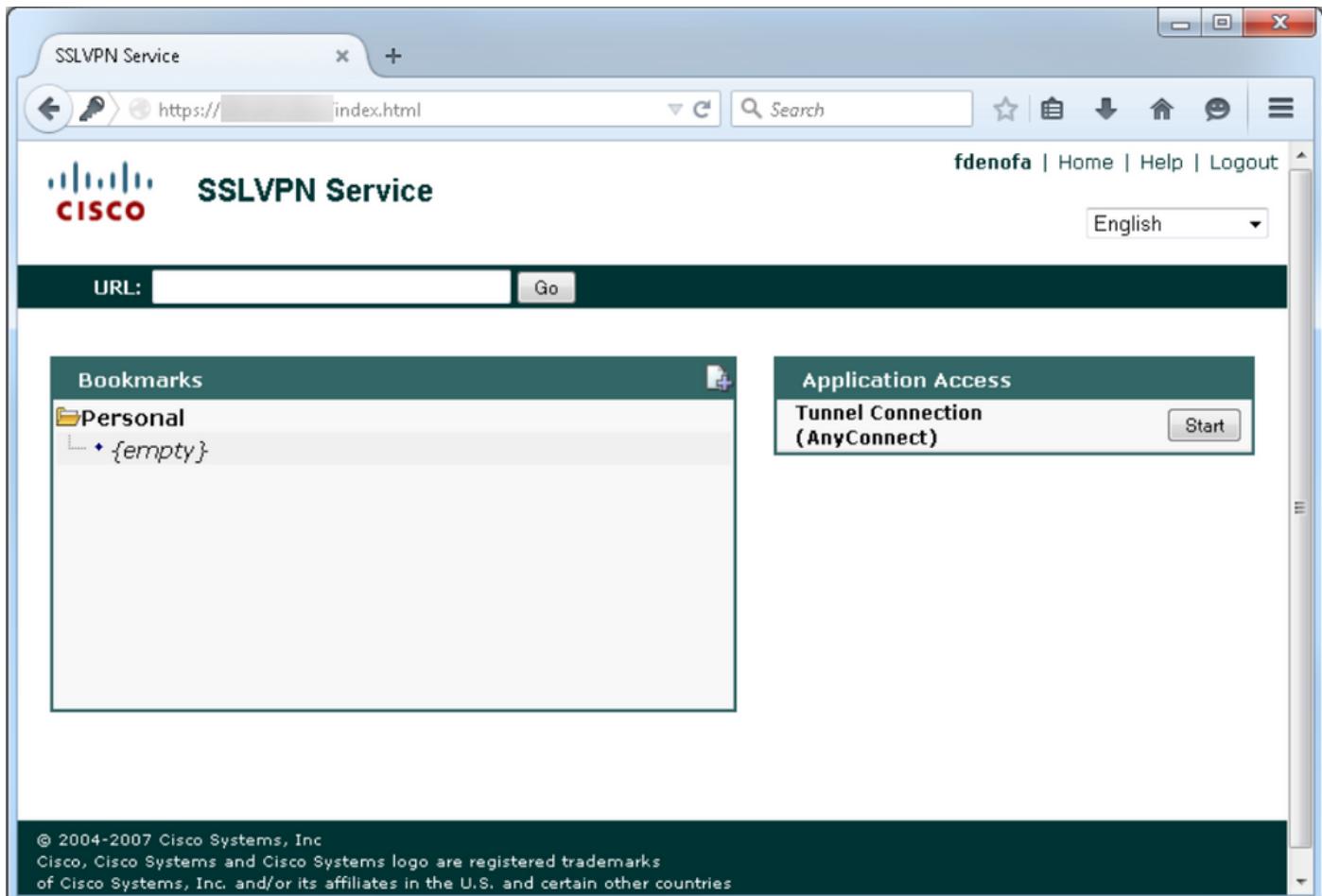
Verify

Use this section in order to confirm that your configuration works properly.

Once the configuration is complete, when you access the gateway address and port by the browser, it returns to the WebVPN splash page:

After you log in, the WebVPN home page displays. From there, click Tunnel Connection (AnyConnect). When Internet Explorer is used, ActiveX is used to push down and install the AnyConnect client. If it is not detected, Java is used instead. All other browsers use Java immediately.

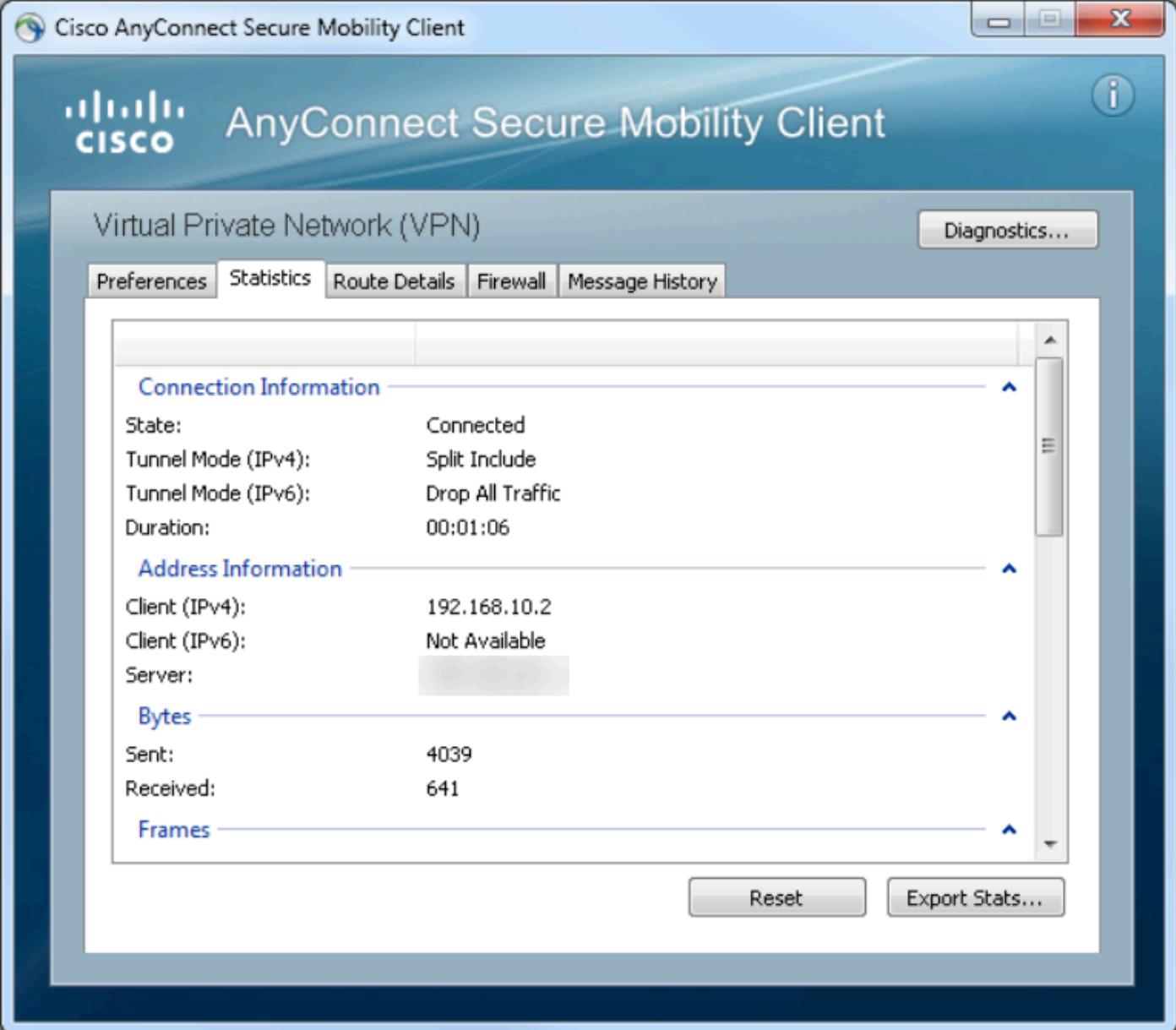


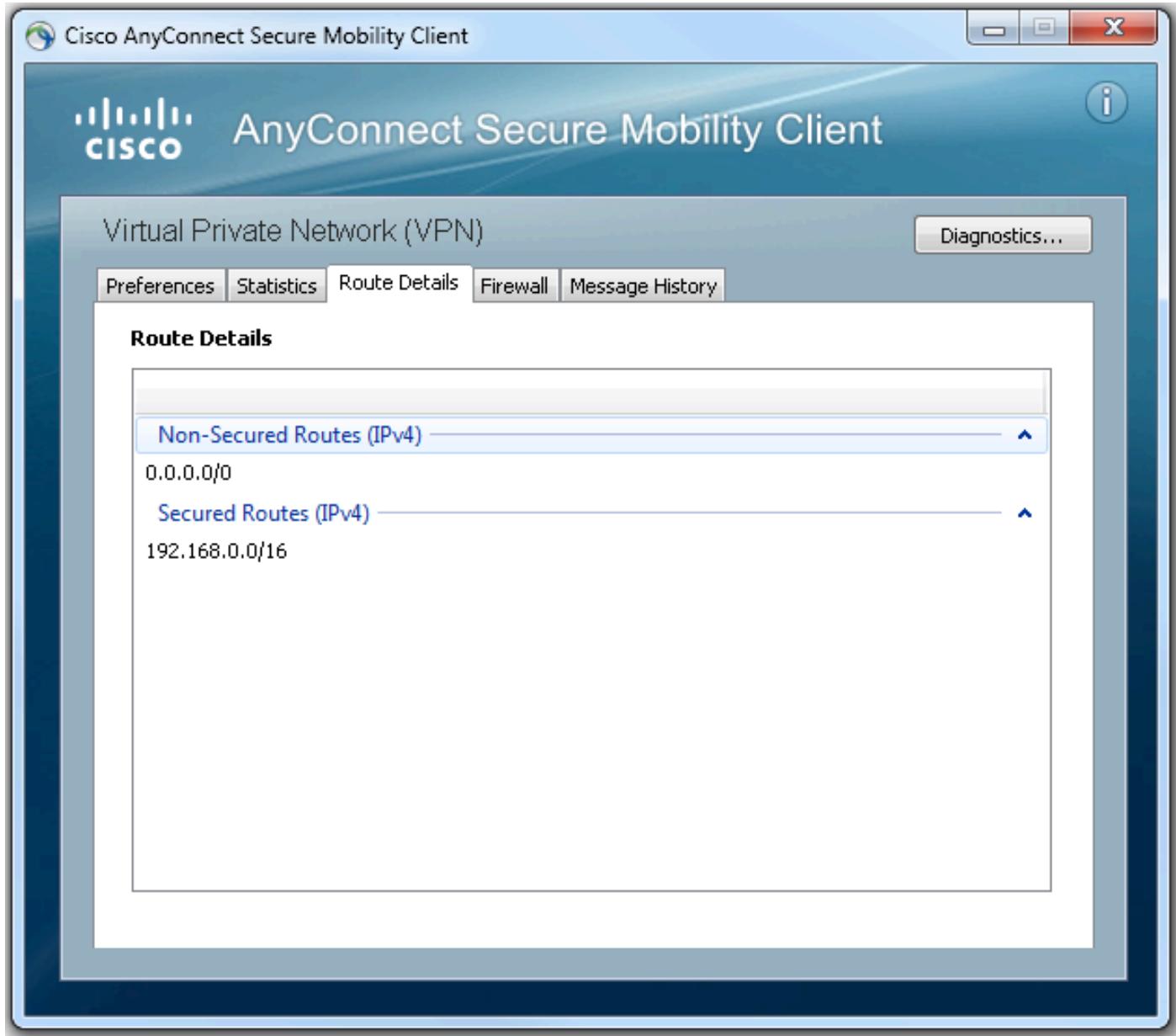


Once the installation is complete, AnyConnect automatically attempts to connect to the WebVPN gateway. As a self-signed certificate is used for the gateway to identify itself, multiple certificate warnings appear during the connection attempt. These are expected and must be accepted for the connection to continue. In order to avoid these certificate warnings, the self-signed certificate presented must be installed in the trusted certificate store of the client machine, or if a third-party certificate is used, then the Certificate Authority certificate must be in the trusted certificate store.



When the connection completes negotiation, click on the gear icon in the lower-left of AnyConnect, it displays some advanced information about the connection. On this page, it is possible to view some connection statistics and route details attained from the split tunnel ACL in the Group Policy configuration.





Here is the final run-configuration result from the configuration steps:

```
crypto pki trustpoint SSLVPN_TP_SELFSGNED
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 10.165.201.1 port 443
ssl trustpoint SSLVPN_TP_SELFSGNED
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

```

Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

There are a few common components to check for when you troubleshoot AnyConnect connection issues:

- As the client must present a certificate, it is a requirement that the certificate specified in the WebVPN gateway be valid. To issue a `show crypto pki certificate` shows information that pertains to all certificates on the router.
- Whenever a change is made to the WebVPN configuration, it is a best practice to issue a `no inservice` and `inservice` on both the gateway and Context. This ensures that the changes take effect properly.
- As mentioned earlier, it is a requirement to have an AnyConnect PKG for each client operating system that connects to this gateway. For example, Windows clients require a Windows PKG, Linux 32-bit clients require a Linux 32-bit PKG, and so on.
- When you consider both the AnyConnect client and browser-based WebVPN to use SSL, to be able to access the WebVPN splash page generally indicates that AnyConnect is able to connect (assume that the pertinent AnyConnect configuration is correct).

Cisco IOS offers various debug WebVPN options that can be used to troubleshoot failed connections. This is the output generated from `debug WebVPN aaa`, `debug WeVPN tunnel`, and `show WebVPN session` upon a successful connection attempt:

```
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 192.168.157.2.
*May 26 20:11:06.381: WV-AAA: AAA authentication request sent for user: "VPNUSER"AAA returned status: 2
*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 "192.168.157.2" 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
*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: 85939A3FE33ABAE5F02F8594D56DEDE389F6FB3C9EEC4D211EB71C0820DF8D
*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: [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 1
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
*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
*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: 22E54D9F1F6344BCB5BB30BC8BB3737907795E6F3C3665CDD294CBBA1DA4D0
*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         : 192.168.157.2       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
```

Related Information

- [SSL VPN Configuration Guide, Cisco IOS Release 15M&T](#)
- [AnyConnect VPN \(SSL\) Client on IOS Router with CCP Configuration Example](#)
- [Technical Support & Documentation - Cisco Systems](#)