AnyConnect:CLI를 사용하여 Cisco IOS Router 헤드엔드에 대한 기본 SSL VPN 구성

소개

목차

이 문서에서는 Cisco IOS® 라우터를 AnyConnect SSL VPN(Secure Sockets Layer VPN) 헤드엔드로 구성하는 기본 컨피그레이션에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco IOS
- AnyConnect Secure Mobility Client
- 일반 SSL 작업

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 15.3(3)M5를 실행하는 Cisco 892W 라우터
- AnyConnect Secure Mobility Client 3.1.08009

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

배경 정보

다양한 IOS 버전에 대한 라이센스 정보

- 어떤 Cisco IOS 버전이 사용되었는지에 관계없이 SSL VPN 기능을 사용하려면 securityk9 기능 집합이 필요합니다.
- Cisco IOS 12.x - SSL VPN 기능은 보안 라이센스(예:advsecurityk9, adventerprisek9 등)를 참조하십시오.
- Cisco IOS 15.0 - 이전 버전에서는 10, 25 또는 100명의 사용자 연결을 허용하는 라우터에 LIC 파일을 설치해야 합니다.Right to Use* 라이센스는 15.0(1)M4에서 구현됨
- Cisco IOS 15.1 이전 버전에서는 10, 25 또는 100명의 사용자 연결을 허용하는 라우터에 LIC 파일을 설치해야 합니다.사용권* 라이센스는 15.1(1)T2, 15.1(2)T2, 15.1(3)T 및 15.1(4)M1에서 구현되었습니다.
- Cisco IOS 15.2 - 모든 15.2 버전은 SSLVPN에 대한 사용권* 라이센스를 제공합니다.
- Cisco IOS 15.3 이상 - 이전 버전에서는 사용 권한* 라이센스를 제공합니다.15.3(3)M부터 securityk9 기술 패키지로 부팅한 후 SSLVPN 기능을 사용할 수 있습니다

RTU 라이센싱의 경우 첫 번째 webvpn 기능(즉, webvpn gateway GATEWAY1)이 구성되고 EULA(End User License Agreement)가 수락되면 평가판 라이센스가 활성화됩니다.60일이 지나면 이 평가판 라이센스는 영구 라이센스가 됩니다.이러한 라이센스는 명예에 기반하며 이 기능을 사용하려면 종이 라이센스를 구입해야 합니다.또한 RTU는 특정 수의 사용으로 제한되지 않고 라우터 플랫폼에서 동시에 지원할 수 있는 최대 동시 연결 수를 허용합니다.

소프트웨어 대폭 향상

이러한 버그 ID로 인해 AnyConnect에 중요한 기능 또는 수정 사항이 발생했습니다.

- CSCti89976: IOS에 AnyConnect 3.x 지원 추가
- CSCtx38806: BEAST 취약성 수정, Microsoft KB2585542

구성

1단계. 라이센스가 활성화되었는지 확인

IOS 라우터 헤드엔드에서 AnyConnect가 구성된 첫 번째 단계는 라이센스가 올바르게 설치되었고(해당되는 경우) 활성화되었는지 확인하는 것입니다.다른 버전에 대한 라이센스 세부 사항은 이전 섹션의 라이센스 정보를 참조하십시오.이는 코드 및 플랫폼 버전에 따라 다릅니다. show license에 SSL_VPN 또는 securityk9 라이센스가 나열되는지 여부.버전 및 라이센스와 상관없이 EULA에 동

의해야 하며 라이센스가 Active(활성)로 표시됩니다.

2단계. 라우터에 AnyConnect Secure Mobility Client 패키지 업로드 및 설치

AnyConnect 이미지를 VPN에 업로드하기 위해 헤드엔드는 두 가지 목적으로 사용됩니다.첫째, AnyConnect 헤드엔드에 AnyConnect 이미지가 있는 운영 체제만 연결할 수 있습니다.예를 들어, Windows 클라이언트는 헤드엔드에 Windows 패키지를 설치해야 하고 Linux 64비트 클라이언트에는 Linux 64비트 패키지가 필요한 등.둘째, 헤드엔드에 설치된 AnyConnect 이미지는 연결 시 자동으로 클라이언트 시스템으로 푸시됩니다.처음 연결하는 사용자는 웹 포털에서 클라이언트를 다운로드할 수 있으며 헤드엔드의 AnyConnect 패키지가 클라이언트 시스템에 설치된 것보다 최신 버전인 경우 해당 클라이언트를 업그레이드할 수 있습니다.

AnyConnect 패키지는 Cisco Software Downloads 웹 사이트의 AnyConnect Secure Mobility Client 섹션을 통해 얻을 수 있습니다.사용 가능한 옵션이 많이 있지만 헤드엔드에 설치할 패키지에는 운영 체제 및 헤드엔드 구축(PKG)이라는 레이블이 지정됩니다. 현재 AnyConnect 패키지는 다음 운영 체제 플랫폼에 사용할 수 있습니다.Windows, Mac OS X, Linux(32비트) 및 Linux 64비트.Linux에는 32비트 및 64비트 패키지가 모두 있습니다.각 운영 체제에서는 연결을 허용하려면 헤드엔드에 적절한 패키지를 설치해야 합니다.

AnyConnect 패키지가 다운로드되면 TFTP, FTP, SCP 또는 기타 몇 가지 옵션을 통해 **copy** 명령을 사용하여 라우터의 플래시에 업로드할 수 있습니다.예를 들면 다음과 같습니다.

```
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 이미지를 라우터의 플래시에 복사한 후 명령줄을 통해 설치해야 합니다.설치 명령 끝에 시퀀스 번호를 지정하면 여러 AnyConnect 패키지를 설치할 수 있습니다.이렇게 하면 라우터가 여러 클라이언트 운영 체제의 헤드엔드 역할을 할 수 있습니다.AnyConnect 패키지를 설치하면 **flash:/webvpn/ 디렉토리**로 이동하며 처음에**에** 복사되지 않은 경우에도 마찬가지입니다.

```
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 이전에 릴리스된 코드 버전에서는 PKG을 설치하는 명령이 약간 다릅니다.

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

3단계. RSA 키 쌍 및 자체 서명 인증서 생성

SSL 또는 PKI(Public Key Infrastructure) 및 디지털 인증서를 구현하는 기능을 구성할 때 인증서 서명에 Rivest-Shamir-Adleman(RSA) 키 쌍이 필요합니다.이 명령은 자체 서명된 PKI 인증서가 생성될 때 사용할 RSA 키 쌍을 생성합니다.2048비트의 모듈러스를 사용해야 하는 것은 아니지만, AnyConnect 클라이언트 시스템과의 보안 및 호환성 향상을 위해 사용 가능한 최대 모듈러스를 사용하는 것이 좋습니다.키 관리와 함께 할당할 설명 키 레이블을 사용하는 것도 좋습니다.키 생성은 show crypto **key mypubkey rsa** 명령으로 확인할 수 있습니다.

> **참고:**RSA 키를 내보낼 수 있도록 하는 데 많은 보안 위험이 수반되므로, 기본적으로 키를 내보낼 수 없도록 키를 구성하는 것이 좋습니다.RSA 키를 내보낼 때 발생할 수 있는 위험 요소는 이 문서에서 설명합니다.PKI 내에서 RSA 키를 배포하는 중입니다.

```
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 키 쌍이 성공적으로 생성되면 라우터의 정보 및 RSA 키 쌍을 사용하여 PKI 신뢰 지점을 구성해야 합니다.주체 이름의 CN(Common Name)은 사용자가 AnyConnect 게이트웨이에 연결하는 데 사용하는 IP 주소 또는 FQDN(Fully Qualified Domain Name)으로 구성해야 합니다.이 예에서 클라이언트는 연결을 시도할 때 fdenofa-SSLVPN.cisco.com의 FQDN을 사용합니다.필수 사항은 아니지만 CN에 올바르게 입력할 때 로그인 시 표시되는 인증서 오류 수를 줄이는 데 도움이 됩니다.

> **참고:**라우터에서 생성한 자체 서명 인증서를 사용하지 않고 서드파티 CA에서 발급한 인증서를 사용할 수 있습니다.이 방법은 이 문서에서 설명한 것처럼 PKI에 대한 인증서 등록 구성의 몇 가지 방법을 통해 수행할 수 있습니다.

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

신뢰 지점이 올바르게 정의되면 라우터는 crypto pki enroll 명령을 사용하여 인증서를 생성해야 **합니다**.이 프로세스에서는 일련 번호 및 IP 주소와 같은 몇 가지 다른 매개변수를 지정할 수 있습니다.그러나 이는 필요하지 않습니다.인증서 생성은 show crypto pki certificates 명령을 사용하여 확인할 수 있습니다.

```
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
```

4단계. 로컬 VPN 사용자 계정 구성

외부 AAA(Authentication, Authorization, and Accounting) 서버를 사용할 수 있지만 이 예에서는 로컬 인증이 사용됩니다.이러한 명령은 사용자 이름 VPNUSER를 생성하고 SSLVPN_AAA라는 AAA 인증 목록을 생성합니다.

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

5단계. 클라이언트에서 사용할 주소 풀 및 스플릿 터널 액세스 목록 정의

AnyConnect 클라이언트 어댑터가 IP 주소를 얻으려면 로컬 IP 주소 풀을 생성해야 합니다.최대 동시 AnyConnect 클라이언트 연결 수를 지원할 수 있도록 충분한 크기의 풀을 구성해야 합니다.

기본적으로 AnyConnect는 전체 터널 모드에서 작동하므로 클라이언트 시스템에서 생성된 모든 트래픽이 터널을 통해 전송됩니다.일반적으로 권장되지 않으므로 터널을 통해 전송해야 하거나 전송해서는 안 되는 트래픽을 정의하는 ACL(Access Control List)을 구성할 수 있습니다.다른 ACL 구현과 마찬가지로, 엔드 포인트에서 암시적 거부는 명시적 거부가 필요하지 않습니다.따라서 터널링해야 하는 트래픽에 대한 permit 문을 구성해야 합니다.

```
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
```

6단계. VTI(Virtual-Template Interface) 구성

동적 VTI 각 VPN 세션에 대해 온디맨드 개별 Virtual-Access 인터페이스를 제공하여 원격 액세스 VPN에 대해 매우 안전하고 확장 가능한 연결을 허용합니다.DVTI 기술은 동적 암호화 맵과 터널을 설정하는 데 도움이 되는 동적 허브 앤 스포크 방법을 대체합니다. DVTI는 다른 실제 인터페이스와 마찬가지로 작동하므로 터널이 활성화되는 즉시 QoS, 방화벽, 사용자별 특성 및 기타 보안 서비스를 지원하므로 더욱 복잡한 원격 액세스 구축을 허용합니다.

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

7단계. WebVPN 게이트웨이 구성

WebVPN Gateway는 AnyConnect 헤드엔드에서 사용할 IP 주소 및 포트, 클라이언트에 제공될 SSL 암호화 알고리즘 및 PKI 인증서를 정의합니다.기본적으로 게이트웨이는 라우터의 Cisco IOS 버전에 따라 달라지는 가능한 모든 암호화 알고리즘을 지원합니다.

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

8단계. WebVPN 컨텍스트 및 그룹 정책 구성

WebVPN 컨텍스트 및 그룹 정책은 AnyConnect 클라이언트 연결에 사용할 몇 가지 추가 매개변수를 정의합니다.기본 AnyConnect 컨피그레이션의 경우 Context는 AnyConnect에 사용할 기본 그룹 정책을 호출하는 데 사용되는 메커니즘으로 사용됩니다.그러나 컨텍스트를 사용하여 WebVPN 시작 페이지 및 WebVPN 작업을 추가로 사용자 지정할 수 있습니다.정의된 정책 그룹에서 SSLVPN_AAA 목록은 사용자가 속한 AAA 인증 목록으로 구성됩니다.**functions svc-enabled** 명령은 사용자가 브라우저를 통해 WebVPN이 아닌 AnyConnect SSL VPN 클라이언트에 연결할 수 있도록 하는 컨피그레이션의 일부입니다.마지막으로, 추가 SVC 명령은 SVC 연결과 관련된 매개 변수를 정의합니다.**svc address-pool**은 게이트웨이에게 SSLVPN_POOL의 주소를 클라이언트로 처리하도록 지시하고, **svc split include는** 위에서 정의한 ACL 1별로 스플릿 터널 정책을 정의하며, svc dns-server는 도메인 이름 확인에 사용할 DNS 서버를 정의합니다.이 컨피그레이션을 사용하면 모든 DNS 쿼리가 지정된 DNS 서버로 전송됩니다.쿼리 응답에서 수신된 주소는 트래픽을 터널을 통해 전송할지 여부를 결정합니다.

```
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
```

9단계(선택 사항) 클라이언트 프로파일 구성

ASA와 달리 Cisco IOS에는 관리자가 클라이언트 프로파일을 생성하는 데 도움이 되는 내장 GUI 인터페이스가 없습니다.AnyConnect 클라이언트 프로파일은 독립 실행형 프로파일 편집기를 사용

하여 별도로 작성/편집해야 합니다.

팁:anyconnect-profileeditor-win-3.1.03103-k9.exe를 찾습니다.

라우터가 프로파일을 배포하도록 하려면 다음 단계를 수행합니다.

- ftp/tftp를 사용하여 IOS 플래시에 업로드합니다.
- 이 명령을 사용하여 방금 업로드한 프로파일을 식별합니다.

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

팁:15.2(1)T 이전 Cisco IOS 버전에서는 이 명령을 사용해야 합니다. webvpn **import svc profile <profile_name> flash:<profile.xml>**

3. 컨텍스트 아래에서 이 명령을 사용하여 프로파일을 해당 컨텍스트에 연결합니다.

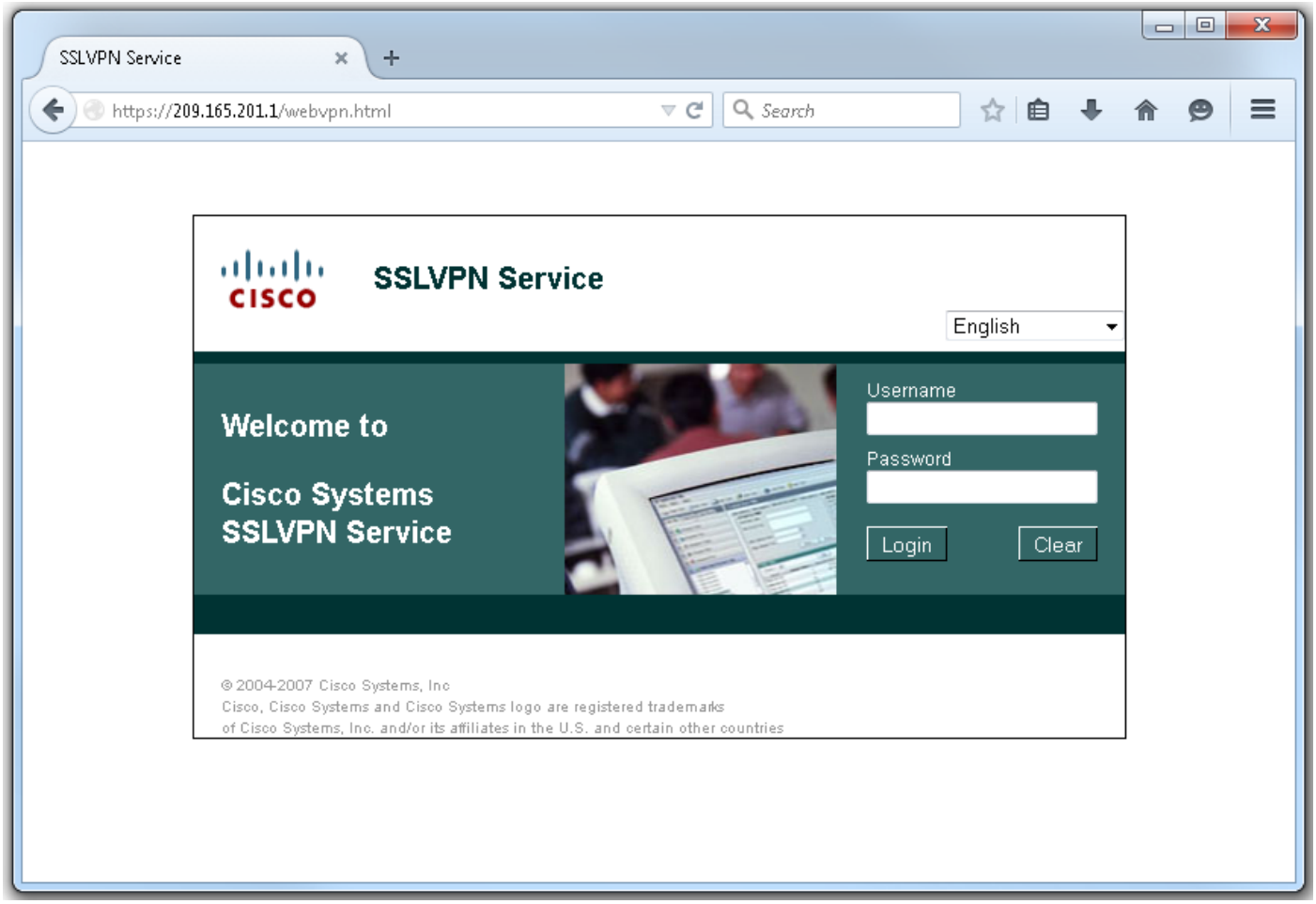
```
webvpn context SSLVPN_CONTEXT
 policy group SSLVPN_POLICY
 svc profile SSLVPN_PROFILE
```

참고:이 섹션에 사용된 명령에 대한 자세한 내용을 보려면 Command Lookup Tool(등록된 고객만 해당)을 사용합니다.

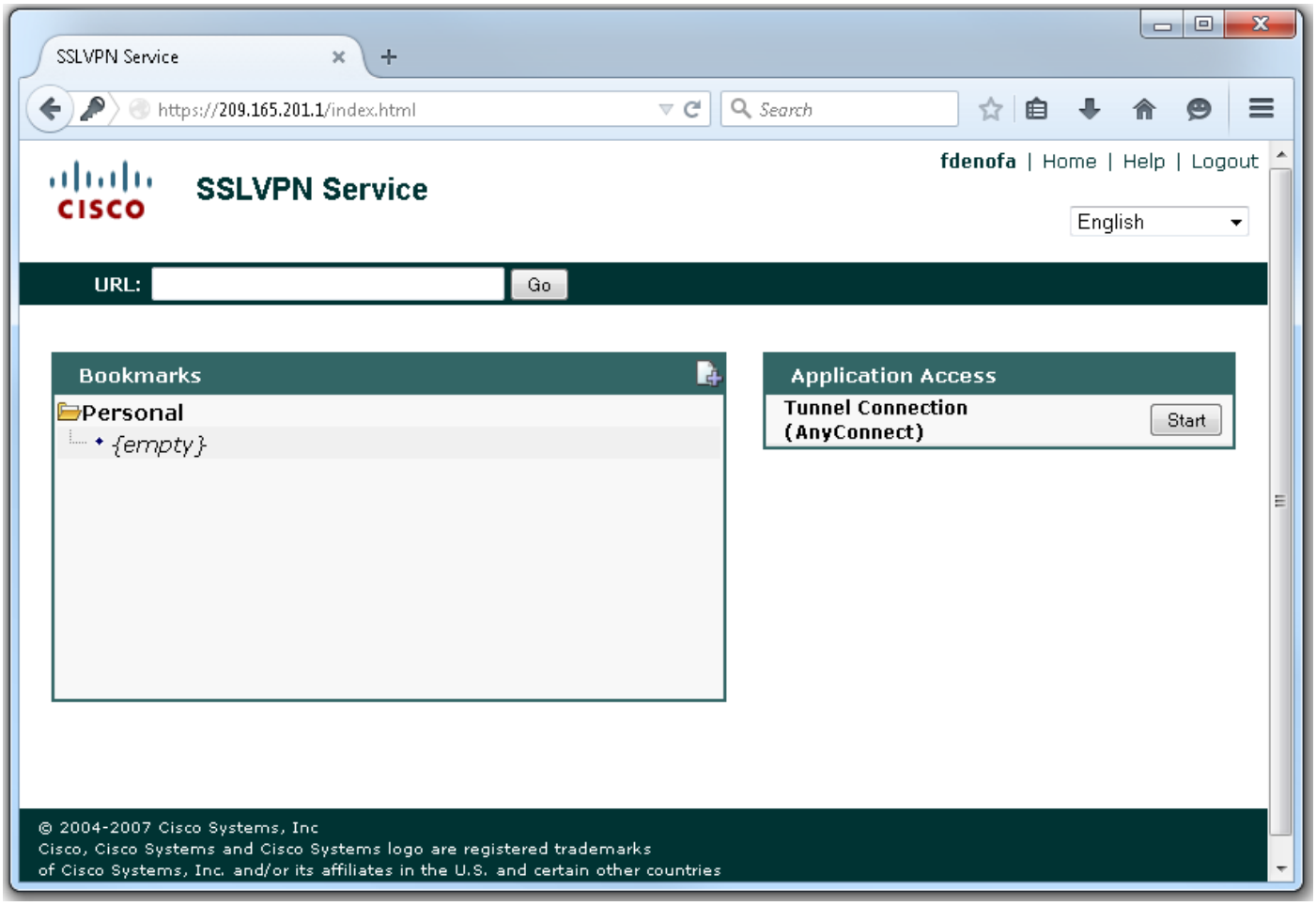
다음을 확인합니다.

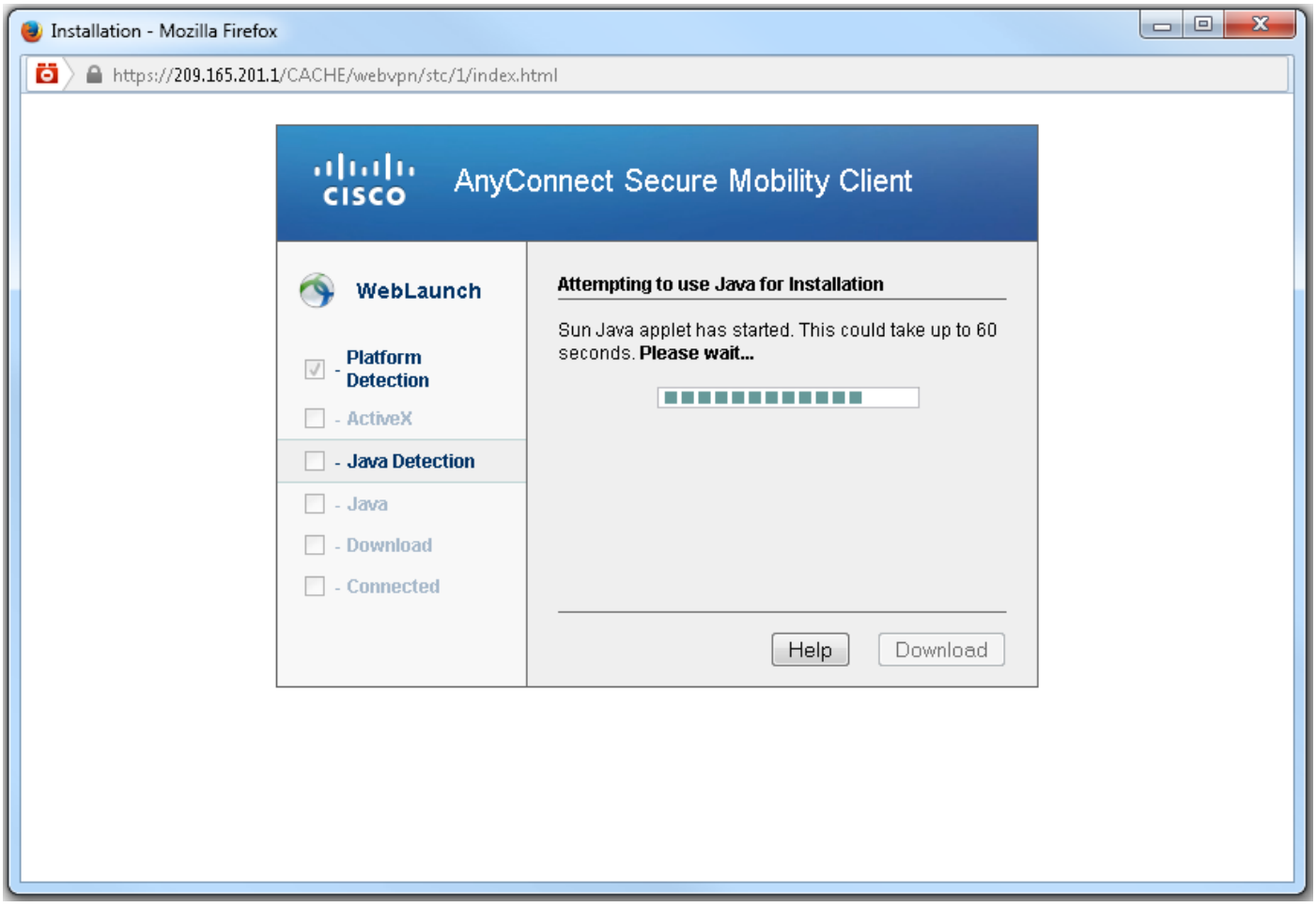
이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

컨피그레이션이 완료되면 브라우저를 통해 게이트웨이 주소 및 포트에 액세스하면 WebVPN 시작 페이지로 돌아갑니다.



로그인하면 WebVPN 홈 페이지가 표시됩니다.여기에서 **Tunnel Connection(AnyConnect)(터널 연결(AnyConnect)을** 클릭합니다. Internet Explorer를 사용할 경우 ActiveX를 사용하여 AnyConnect 클라이언트를 푸시하고 설치합니다.탐지되지 않으면 Java가 대신 사용됩니다.다른 모든 브라우저는 즉시 Java를 사용합니다.

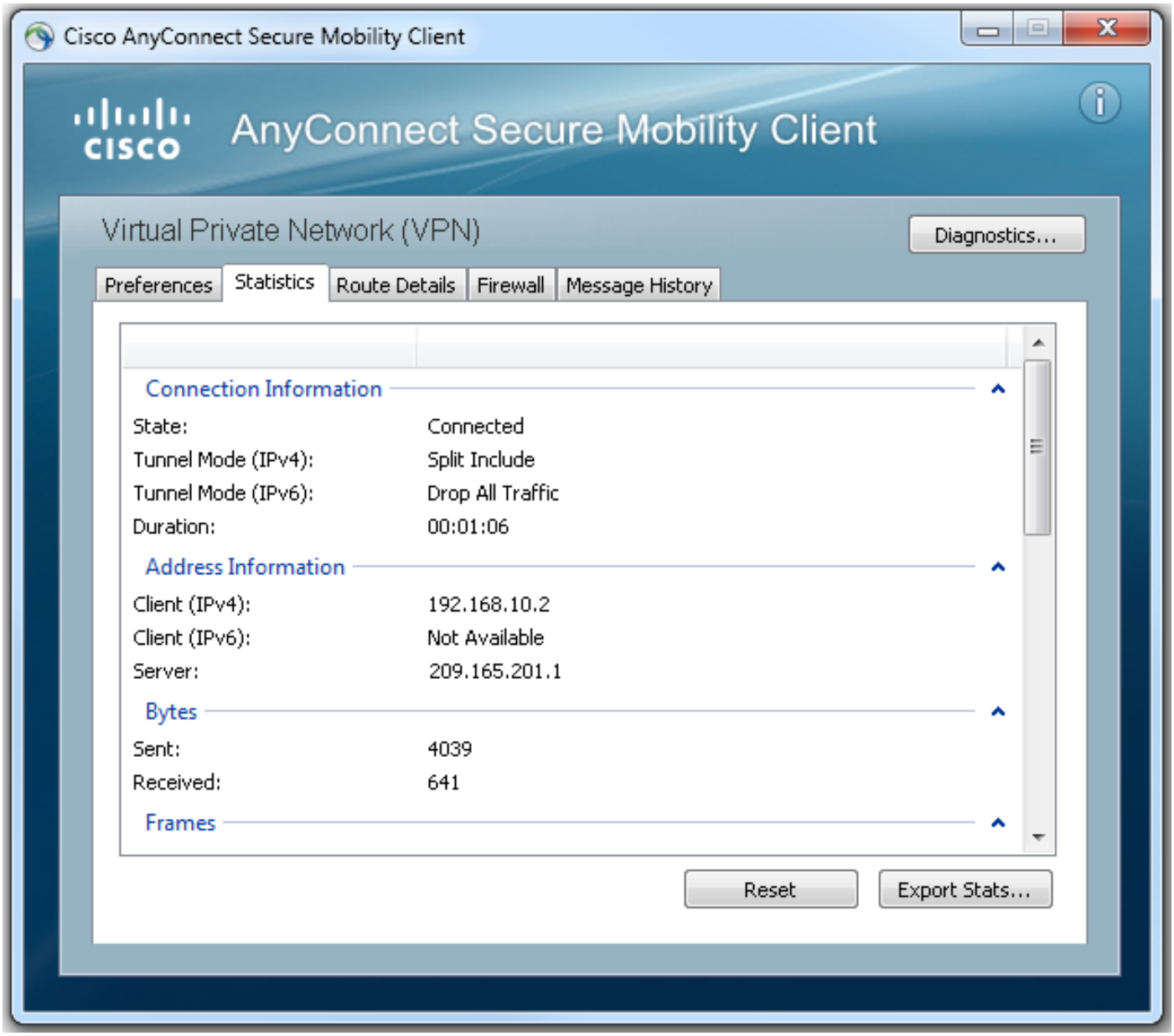


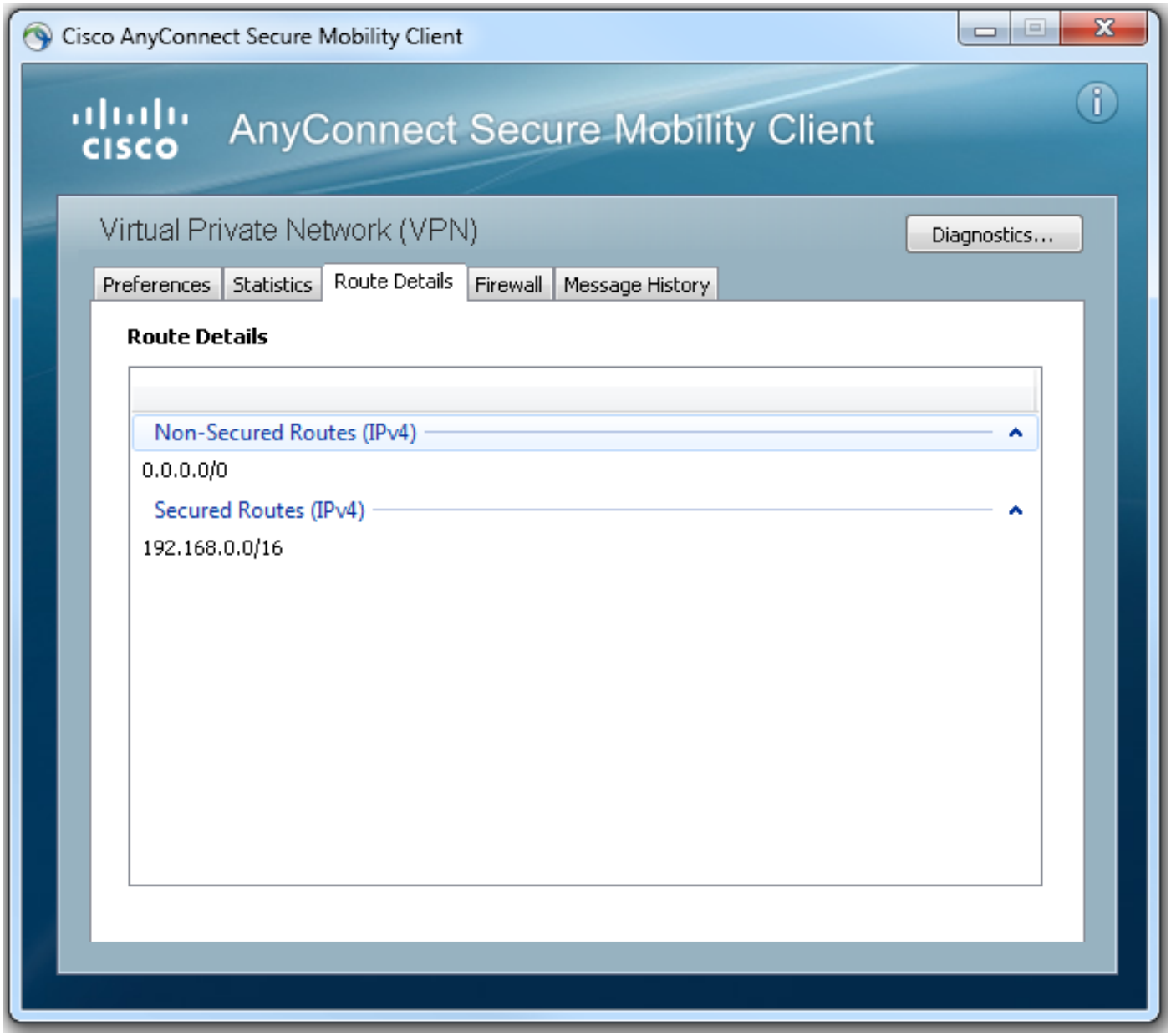


설치가 완료되면 AnyConnect는 자동으로 WebVPN 게이트웨이에 연결을 시도합니다.게이트웨이에서 자신을 식별하는 데 자체 서명 인증서가 사용되고 있으므로 연결 시도 중에 여러 인증서 경고

가 나타납니다.이러한 연결은 필수입니다.이러한 인증서 경고를 피하려면 표시되는 자체 서명 인증서가 클라이언트 컴퓨터의 신뢰할 수 있는 인증서 저장소에 설치되거나 서드파티 인증서가 사용 중인 경우 인증 기관 인증서가 신뢰할 수 있는 인증서 저장소에 있어야 합니다.

연결이 협상을 완료하면 AnyConnect의 왼쪽 아래에 있는 **기어** 아이콘을 클릭하면 연결에 대한 일부 고급 정보가 표시됩니다.이 페이지에서 그룹 정책 컨피그레이션의 스플릿 터널 ACL에서 가져온 일부 연결 통계 및 경로 세부 정보를 볼 수 있습니다.


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...



컨피그레이션 단계의 최종 실행 컨피그레이션 결과는 다음과 같습니다.

```
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
```

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

AnyConnect 연결 문제를 해결할 때 몇 가지 일반적인 구성 요소를 확인할 수 있습니다.

- 클라이언트는 인증서를 제공해야 하므로 WebVPN 게이트웨이에 지정된 인증서가 유효해야 합니다.show crypto pki **인증서**를 **발급하려면** 라우터의 모든 인증서와 관련된 정보가 표시됩니다.
- WebVPN 컨피그레이션이 변경될 때마다 게이트웨이와 컨텍스트 모두에서 서비스 없음 및 서비스를 사용하지 않는 것이 가장 좋습니다.이렇게 하면 변경 사항이 올바르게 적용됩니다.
- 앞에서 언급한 것처럼, 이 게이트웨이에 연결할 각 클라이언트 운영 체제에 대해 AnyConnect PKG을 보유해야 합니다.예를 들어 Windows 클라이언트에는 Windows PKG이 필요하고 Linux 32비트 클라이언트에는 Linux 32비트 PKG 등이 필요합니다.
- AnyConnect 클라이언트 및 브라우저 기반 WebVPN을 모두 사용하여 SSL을 사용하는 것을 고려할 때 WebVPN 시작 페이지에 액세스할 수 있는 것은 일반적으로 AnyConnect가 연결할 수 있음을 나타냅니다(관련 AnyConnect 구성이 올바르다고 가정).

Cisco IOS는 연결 실패 문제를 해결하는 데 사용할 수 있는 몇 가지 다양한 디버그 webvpn 옵션을 제공합니다.다음은 성공적인 연결 시도 시 debug webvpn aaa, debug webvpn tunnel 및 show webvpn 세션에서 생성된 출력입니다.

```
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
```

관련 정보

- SSL VPN 컨피그레이션 가이드, Cisco IOS 릴리스 15M&T
- CCP 컨피그레이션을 사용하는 IOS 라우터의 AnyConnect VPN(SSL) 클라이언트 예
- 기술 지원 및 문서 – Cisco Systems