# ASA 8.x:자체 서명 인증서 컨피그레이션을 사용하여 AnyConnect VPN 클라이언트를 통한 VPN 액세스 예

## 목차



# 소개

이 문서에서는 자체 서명 인증서를 사용하여 Cisco AnyConnect 2.0 클라이언트에서 ASA에 대한 원격 액세스 SSL VPN 연결을 허용하는 방법에 대해 설명합니다.

# 사전 요구 사항

## 요구 사항

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- 소프트웨어 버전 8.0을 실행하는 기본 ASA 구성
- ASDM 6.0(2)

## 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ASA 8.0(2), ASDM 6.0(2)
- Cisco AnyConnect 2.0

## 표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

# 배경 정보

Cisco AnyConnect 2.0 클라이언트는 SSL 기반 VPN 클라이언트입니다.AnyConnect 클라이언트는 Windows 2000, XP, Vista, Linux(다중 총판사) 및 MAC OS X와 같은 다양한 운영 체제에 사용 및 설치할 수 있습니다. AnyConnect 클라이언트는 시스템 관리자가 원격 PC에 수동으로 설치할 수 있습니다.또한 보안 어플라이언스에 로드되어 원격 사용자에게 다운로드할 수 있도록 준비될 수 있습니다.애플리케이션이 다운로드되면 연결이 종료되면 자동으로 자동으로 제거되거나, 향후 SSL VPN 연결을 위해 원격 PC에 남아 있을 수 있습니다.이 예에서는 브라우저 기반 SSL 인증 성공 시 AnyConnect 클라이언트를 다운로드할 수 있도록 합니다.

AnyConnect 2.0 클라이언트에 대한 자세한 내용은 AnyConnect 2.0 릴리스 정보를 참조하십시오.

**참고:** MS 터미널 서비스는 AnyConnect 클라이언트와 함께 지원되지 않습니다.컴퓨터에 RDP를 연결한 다음 AnyConnect 세션을 시작할 수 없습니다.AnyConnect를 통해 연결된 클라이언트에는 RDP를 사용할 수 없습니다.

**참고:** AnyConnect를 처음 설치하려면 사용자에게 관리자 권한이 있어야 합니다(독립형 AnyConnect msi 패키지를 사용하든 ASA에서 pkg 파일을 푸시든). 사용자에게 관리자 권한이 없는 경우 이 요구 사항을 설명하는 대화 상자가 나타납니다.이후 업그레이드에서는 이전에 AnyConnect를 설치한 사용자에게 관리자 권한이 필요하지 않습니다.

# 구성

AnyConnect 클라이언트를 사용하여 VPN 액세스용 ASA를 구성하려면 다음 단계를 완료하십시오.

1. 자체 발급된 인증서를 구성합니다.
2. SSL VPN 클라이언트 이미지를 업로드하고 식별합니다.
3. AnyConnect 액세스를 활성화합니다.
4. 새 그룹 정책을 만듭니다.
5. VPN 연결에 대한 액세스 목록 우회를 구성합니다.
6. AnyConnect 클라이언트 연결을 위한 연결 프로파일 및 터널 그룹을 생성합니다.
7. AnyConnect 클라이언트에 대한 NAT 예외를 구성합니다.
8. 로컬 데이터베이스에 사용자를 추가합니다.

## 1단계. 자체 발급된 인증서 구성

기본적으로 보안 어플라이언스에는 디바이스를 재부팅할 때마다 재생성되는 자체 서명 인증서가

있습니다.Verisign 또는 EnTrust와 같은 벤더로부터 자체 인증서를 구매하거나 ID 인증서를 자체적으로 발급하도록 ASA를 구성할 수 있습니다.이 인증서는 디바이스를 재부팅해도 동일하게 유지됩니다.디바이스가 재부팅될 때 유지되는 자체 발급된 인증서를 생성하려면 이 단계를 완료합니다.

### ASDM 절차

1. Configuration(컨피그레이션)을 클릭한 다음 **Remote Access VPN(원격 액세스 VPN)을 클릭합니다**.
2. Certificate **Management(인증서 관리)**를 확장한 다음 Identity **Certificates(ID 인증서)를 선택합니다**.
3. Add(**추가**)를 클릭한 다음 **Add a new identity certificate(새 ID 인증서 추가)** 라디오 버튼을 클릭합니다.
4. New(**새로 만들기)를 클릭합니다**.
5. Add Key Pair(키 쌍 추가) 대화 상자에서 **Enter new key pair name(새 키 쌍 이름 입력)** 라디오 버튼을 클릭합니다.
6. 키 쌍을 식별할 이름을 입력합니다.이 예에서는 sslvpnkeypair를 *사용합니다*.
7. Generate Now(**지금 생성)를 클릭합니다**.
8. Add Identity Certificate(ID 인증서 추가) 대화 상자에서 새로 생성된 키 쌍이 선택되었는지 확인합니다.
9. Certificate Subject DN의 경우 VPN 종료 인터페이스에 연결하는 데 사용할 FQDN(정규화된 도메인 이름)을 입력합니다.**CN=sslvpn.cisco.com**
10. Advanced(**고급**)를 클릭하고 Certificate Subject DN(인증서 주체 DN) 필드에 사용되는 FQDN을 입력합니다.예: **FQDN**:sslvpn.cisco.com
11. **확인**을 **클릭합니다**.
12. Generate Self **Signed Certificate**(자체 서명 인증서 생성) 확인란을 선택하고 Add Certificate(인증서 **추가)를 클릭합니다**.
13. **확인**을 **클릭합니다**.
14. Configuration(컨피그레이션)을 클릭한 다음 **Remote Access VPN(원격 액세스 VPN)을 클릭합니다**.
15. Advanced(**고급**)를 확장하고 **SSL** Settings(**SSL 설정)를 선택합니다**.
16. Certificates(인증서) 영역에서 SSL VPN(외부)을 종료하는 데 사용할 인터페이스를 선택하고 Edit(**수정)를** 클릭합니다.
17. Certificate(인증서) 드롭다운 목록에서 이전에 생성한 자체 서명 인증서를 선택합니다.
18. OK(**확인**)를 클릭한 다음 Apply(적용)를 **클릭합니다**.

### 명령줄 예

**ciscoasa**

```
ciscoasa(config)#crypto key generate rsa label
sslvpnkeypair
INFO: The name for the keys will be: sslvpnkeypair
Keypair generation process begin. Please wait...
!--- Generate an RSA key for the certificate. (The name
should be unique. !--- For example, sslvpnkeypair.)
ciscoasa(config)#crypto ca trustpoint localtrust
!--- Create a trustpoint for the self-issued
certificate. ciscoasa(config-ca-trustpoint)#enrollment
self
ciscoasa(config-ca-trustpoint)#fqdn sslvpn.cisco.com
ciscoasa(config-ca-trustpoint)#subject-name
CN=sslvpn.cisco.com
!--- The fully qualified domain name is used for both
```

```
fqdn and CN. !--- The name should resolve to the ASA
outside interface IP address. ciscoasa(config-ca-
trustpoint)#keypair sslvpnkeypair
!--- The RSA key is assigned to the trustpoint for
certificate creation. ciscoasa(config-ca-
trustpoint)#crypto ca enroll localtrust noconfirm
% The fully-qualified domain name in the certificate
will be: sslvpn.cisco.com
ciscoasa(config)# ssl trust-point localtrust outside
!--- Assign the trustpoint to be used for SSL
connections on the outside interface.
```

## 2단계. SSL VPN 클라이언트 이미지 업로드 및 식별

이 문서에서는 AnyConnect SSL 2.0 클라이언트를 사용합니다.Cisco Software Download 웹 사이트에서 이 클라이언트를 가져올 수 있습니다.원격 사용자가 사용하려는 각 운영 체제마다 별도의 AnyConnect 이미지가 필요합니다.자세한 내용은 Cisco AnyConnect 2.0 릴리스 정보를 참조하십시오.

AnyConnect 클라이언트를 가져온 후 다음 단계를 완료합니다.

### ASDM 절차

1. Configuration(컨피그레이션)을 클릭한 다음 **Remote Access VPN(원격 액세스 VPN)을 클릭합니다**.
2. **네트워크(클라이언트) 액세스를** 확장한 다음 **고급을 확장합니다**.
3. SSL **VPN**을 확장하고 Client **Settings**(클라이언트 설정)를 **선택합니다**.
4. SSL VPN Client Images(SSL VPN 클라이언트 이미지) 영역에서 **Add(추가)**를 클릭한 다음 **Upload(업로드)**를 클릭합니다.
5. AnyConnect 클라이언트를 다운로드한 위치로 이동합니다.
6. 파일을 선택하고 Upload **File**(파일 업로드)**을** 클릭합니다.클라이언트가 업로드되면 파일이 플래시에 업로드되었다는 메시지가 표시됩니다.
7. **확인을 클릭합니다**.새로 업로드한 이미지를 현재 SSL VPN 클라이언트 이미지로 사용할 것임을 확인하는 대화 상자가 나타납니다.
8. **확인을 클릭합니다**.
9. OK(**확인**)를 클릭한 다음 Apply(적용)를 **클릭합니다**.
10. 사용할 각 운영 체제별 Anyconnect 패키지에 대해 이 섹션의 단계를 반복합니다.

### 명령줄 예

**ciscoasa**

```
ciscoasa(config)#copy tftp://192.168.50.5/anyconnect-
win-2.0.0343-k9.pkg flash

Address or name of remote host [192.168.50.5]?

Source filename [anyconnect-win-2.0.0343-k9.pkg]?

Destination filename [anyconnect-win-2.0.0343-k9.pkg]?

Accessing tftp://192.168.50.5/anyconnect-win-2.0.0343-
k9.pkg...!!!!!!!!!!!!!
Writing file disk0:/anyconnect-win-2.0.0343-k9.pkg...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
!!!!!!!!!!!!!!!!!!!!
2635734 bytes copied in 4.480 secs (658933 bytes/sec)
!--- AnyConnect image is downloaded to ASA via TFTP.
ciscoasa(config)#webvpn
ciscoasa(config-webvpn)#svc image disk0:/anyconnect-win-
2.0.0343-k9.pkg 1
!--- Specify the AnyConnect image to be downloaded by
users. The image that is !--- downloaded the most should
have the lowest number. This image uses 1 for the !---
AnyConnect Windows image.
```

## 3단계. AnyConnect 액세스 활성화

AnyConnect 클라이언트가 ASA에 연결할 수 있도록 하려면 SSL VPN 연결을 종료하는 인터페이스에서 액세스를 활성화해야 합니다.이 예에서는 Anyconnect 연결을 종료하기 위해 외부 인터페이스를 사용합니다.

**ASDM 절차**

1. Configuration(컨피그레이션)을 클릭한 다음 **Remote Access VPN(원격 액세스 VPN)을 클릭합니다**.
2. Network **(Client) Access(네트워크(클라이언트) 액세스)**를 확장한 다음 **SSL VPN Connection Profiles(SSL VPN 연결 프로파일)를 선택합니다**.
3. Enable **Cisco AnyConnect VPN Client(Cisco AnyConnect VPN 클라이언트 활성화)** 확인란을 선택합니다.
4. 외부 인터페이스의 **Allow Access**(액세스 허용) 확인란을 선택하고 Apply(적용)를 **클릭합니다**.

**명령줄 예**

**ciscoasa**

```
ciscoasa(config)#webvpn
ciscoasa(config-webvpn)#enable outside
ciscoasa(config-webvpn)#svc enable
!--- Enable AnyConnect to be downloaded to remote
computers.
```

## 4단계. 새 그룹 정책 생성

그룹 정책은 연결할 때 클라이언트에 적용해야 하는 컨피그레이션 매개변수를 지정합니다.이 예에서는 SSLClientPolicy라는 그룹 정책*을 생성합니다*.

**ASDM 절차**

1. Configuration(컨피그레이션)을 클릭한 다음 Remote Access VPN(**원격 액세스 VPN)을 클릭합니다**.
2. **Network (Client) Access(네트워크(클라이언트) 액세스)**를 확장하고 Group Policies(**그룹 정책**)**를** 선택합니다.
3. Add(**추가)를 클릭합니다**.
4. General(**일반**)을 선택하고 **Name(이름)** 필드에 SSLClientPolicy를 입력합니다.
5. Address Pools Inherit(주소 풀 **상속**) 확인란의 선택을 취소합니다.
6. 선택**을** 클릭한 다음 **추가**를 클릭합니다.Add IP Pool 대화 상자가 나타납니다.
7. 네트워크에서 현재 사용 중이 아닌 IP 범위에서 주소 풀을 구성합니다.이 예에서는 다음 값을

사용합니다.이름:SSLClient풀**시작 IP 주소**:192.168.25.1**종료 IP 주소**:192.168.25.50**서브넷 마스크**:255.255.255.0

8. **확인**을 **클릭합니다**.
9. 새로 생성된 풀을 선택하고 Assign(할당)을 **클릭합니다**.
10. **확인**을 클릭한 다음 **추가 옵션**을 클릭합니다.
11. Tunneling Protocols Inherit(터널링 프로토콜 **상속**) 확인란의 선택을 취소합니다.
12. **SSL VPN 클라이언트를 확인합니다**.
13. 왼쪽 창에서 Servers(**서버)를** 선택합니다.
14. DNS Servers Inherit(DNS 서버 **상속**) 확인란의 선택을 취소하고 AnyConnect 클라이언트에서 사용할 내부 DNS 서버의 IP 주소를 입력합니다.이 예에서는 *192.168.50.5를 사용합니다*.
15. More **Options를 클릭합니다**.
16. Default Domain Inherit(기본 도메인 **상속**) 확인란의 선택을 취소합니다.
17. 내부 네트워크에서 사용하는 도메인을 입력합니다.예: *tsweb.local*.
18. OK(**확인**)를 클릭한 다음 Apply(적용)를 **클릭합니다**.

**명령줄 예**

**ciscoasa**

```
ciscoasa(config)#ip local pool SSLClientPool
192.168.25.1-192.168.25.50 mask 255.255.255.0
!--- Define the IP pool. The IP pool should be a range
of IP addresses !--- not already in use on the internal
network. ciscoasa(config)#group-policy SSLCLientPolicy
internal
ciscoasa(config)#group-policy SSLCLientPolicy attributes
ciscoasa(config-group-policy)#dns-server value
192.168.50.5
!--- Specify the internal DNS server to be used.
ciscoasa(config-group-policy)#vpn-tunnel-protocol svc
!--- Specify VPN tunnel protocol to be used by the Group
Policy. ciscoasa(config-group-policy)#default-domain
value tsweb.local
!--- Define the default domain assigned to VPN users.
ciscoasa(config-group-policy)#address-pools value
SSLClientPool
!--- Assign the IP pool created to the SSLClientPolicy
group policy.
```

## VPN 연결을 위한 액세스 목록 우회 구성

이 옵션을 활성화하면 SSL/IPsec 클라이언트가 인터페이스 액세스 목록을 우회하도록 허용합니다.

**ASDM 절차**

1. Configuration(컨피그레이션)을 클릭한 다음 **Remote Access VPN(원격 액세스 VPN)을 클릭합니다**.
2. **네트워크(클라이언트) 액세스를** 확장한 다음 **고급을 확장합니다**.
3. SSL **VPN**을 확장하고 Bypass **Interface Access List를 선택합니다**.
4. Enable inbound **SSL VPN and IPSEC Sessions to bypass interface access lists(인바운드 SSL VPN 및 IPSEC 세션이 인터페이스 액세스 목록을 우회하도록 활성화**) 확인란을 선택하고 Apply(적용)를 **클릭합니다**.

**명령줄 예**

**ciscoasa**

```
ciscoasa(config)#sysopt connection permit-vpn
!--- Enable interface access-list bypass for VPN
connections. !--- This example uses the vpn-filter
command for access control.

ciscoasa(config-group-policy)#
```

## 6단계. AnyConnect 클라이언트 연결을 위한 연결 프로파일 및 터널 그룹 생성

VPN 클라이언트가 ASA에 연결되면 연결 프로파일 또는 터널 그룹에 연결됩니다.터널 그룹은 IPsec L2L, IPsec 원격 액세스, 클라이언트리스 SSL, 클라이언트 SSL 등 특정 유형의 VPN 연결에 대한 연결 매개변수를 정의하는 데 사용됩니다.

### ASDM 절차

1. Configuration(컨피그레이션)을 클릭한 다음 **Remote Access VPN(원격 액세스 VPN)을 클릭합니다**.
2. **Network (Client) Access(네트워크(클라이언트) 액세스)**를 확장한 다음 **SSL VPN을 확장합니다**.
3. Connection **Profiles(연결 프로파일)**를 선택하고 Add(**추가**)를 클릭합니다.
4. 기본**을** 선택하고 다음 값을 입력합니다.이름:SSLClient프로필**인증**:로컬**기본 그룹 정책**:SSLC클라이언트 정책
5. SSL **VPN Client Protocol(SSL VPN 클라이언트 프로토콜)** 확인란이 선택되었는지 확인합니다.
6. 왼쪽 창에서 **Advanced**(고급)를 확장하고 **SSL VPN을** 선택합니다.
7. Connection Aliases(연결 별칭)에서 **Add(추가)**를 클릭하고 사용자가 VPN 연결을 연결할 수 있는 이름을 입력합니다.예를 들어, SSLVPNClient*를 선택합니다*.
8. OK(**확인**)를 클릭한 다음 **OK(확인)를** 다시 클릭합니다.
9. ASDM 창 하단에서 **Allow user to select connection, identified by the table at login page** 확인란**을** 선택하고 **Apply**를 클릭합니다.

### 명령줄 예

**ciscoasa**

```
ciscoasa(config)#tunnel-group SSLClientProfile type
remote-access
!--- Define tunnel group to be used for VPN remote
access connections. ciscoasa(config)#tunnel-group
SSLClientProfile general-attributes
ciscoasa(config-tunnel-general)#default-group-policy
SSLCLientPolicy
ciscoasa(config-tunnel-general)#tunnel-group
SSLClientProfile webvpn-attributes
ciscoasa(config-tunnel-webvpn)#group-alias SSLVPNClient
enable
!--- Assign alias for tunnel group. ciscoasa(config-
tunnel-webvpn)#webvpn
ciscoasa(config-webvpn)#tunnel-group-list enable
!--- Enable alias/tunnel group selection for SSL VPN
connections.
```

## 7단계. AnyConnect 클라이언트에 대한 NAT 예외 구성

SSL VPN 클라이언트가 액세스하도록 허용하려는 IP 주소 또는 범위에 대해 NAT 제외를 구성해야 합니다.이 예에서 SSL VPN 클라이언트는 내부 IP 192.168.50.5에만 액세스해야 합니다.

**참고:** NAT-control이 활성화되지 않은 경우 이 단계는 필요하지 않습니다.확인하려면 **show run nat-control** 명령을 사용합니다.ASDM을 통해 확인하려면 Configuration(컨피그레이션)을 클릭하고 **Firewall(방화벽)**을 클릭한 다음 **Nat Rules(NAT 규칙)를 선택합니다.Enable traffic through the firewall without address translation(주소 변환 없이 방화벽 통과 트래픽 활성화)** 확인란을 선택한 경우 이 단계를 건너뛸 수 있습니다.

**ASDM 절차**

1. Configuration(컨피그레이션)을 클릭한 다음 **Firewall(방화벽)**을 클릭합니다.
2. Nat **Rules를** 선택하고 Add를 **클릭합니다**.
3. Add **NAT Exempt Rule(NAT 제외 규칙 추가)**을 선택하고 다음 값을 입력합니다.**작업**:제외**인터페이스**:내부**출처**:192.168.50.5**대상**:192.168.25.0/24**NAT 제외 방향**:NAT 아웃바운드 트래픽을 '내부' 인터페이스에서 낮은 보안 인터페이스로 제외(기본값)
4. OK(**확인**)를 클릭한 다음 Apply(적용)를 **클릭합니다**.

**명령줄 예**

**ciscoasa**

```
ciscoasa(config)#access-list no_nat extended permit
                  ip host 192.168.50.5 192.168.25.0
255.255.255.0
!--- Define access list to be used for NAT exemption.
ciscoasa(config)#nat (inside) 0 access-list no_nat
!--- Allow external connections to untranslated internal
!--- addresses defined by access lisy no_nat.
ciscoasa(config)#
```

## 8단계. 로컬 데이터베이스에 사용자 추가

로컬 인증(기본값)을 사용하는 경우 사용자 인증을 위해 로컬 데이터베이스에서 사용자 이름과 비밀번호를 정의해야 합니다.

**ASDM 절차**

1. Configuration(컨피그레이션)을 클릭한 다음 **Remote Access VPN(원격 액세스 VPN)을 클릭합니다**.
2. AAA **Setup(AAA 설정)**을 확장하고 Local Users(**로컬 사용자)를 선택합니다**.
3. Add(**추가**)를 클릭하고 다음 값을 입력합니다.**사용자 이름**:메튜프**암호**:p@ssw0rd**암호 확인**:p@ssw0rd
4. No ASDM, **SSH, Telnet 또는 Console Access** 라디오 버튼을 선택합니다.
5. OK(**확인**)를 클릭한 다음 Apply(적용)를 **클릭합니다**.
6. 추가 사용자에 대해 이 단계를 반복한 다음 **저장**을 클릭합니다.

**명령줄 예**

**ciscoasa**

```
ciscoasa(config)#username matthewp password p@ssw0rd
ciscoasa(config)#username matthewp attributes
ciscoasa(config-username)#service-type remote-access
!--- Assign user remote access only. No SSH, Telnet,
ASDM access allowed. ciscoasa(config-username)#write
memory
!--- Save the configuration.
```

# 다음을 확인합니다.

SSL VPN 컨피그레이션이 성공했는지 확인하려면 이 섹션을 사용합니다.

### AnyConnect 클라이언트를 사용하여 ASA에 연결

PC에 직접 클라이언트를 설치하고 ASA 외부 인터페이스에 연결하거나 웹 브라우저에 ASA의 https 및 FQDN/IP 주소를 입력합니다.웹 브라우저를 사용하는 경우 로그인 시 클라이언트가 자동으로 설치됩니다.

### SSL VPN 클라이언트 연결 확인

연결된 SSL VPN 클라이언트를 확인하려면 **show vpn-sessiondb svc** 명령을 사용합니다.

```
ciscoasa(config-group-policy)#show vpn-sessiondb svc

Session Type: SVC

Username     : matthewp               Index        : 6
Assigned IP  : 192.168.25.1           Public IP    : 172.18.12.111
Protocol     : Clientless SSL-Tunnel DTLS-Tunnel
Encryption   : RC4 AES128             Hashing      : SHA1
Bytes Tx     : 35466                  Bytes Rx     : 27543
Group Policy : SSLClientPolicy        Tunnel Group : SSLClientProfile
Login Time   : 20:06:59 UTC Tue Oct 16 2007
Duration     : 0h:00m:12s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none

ciscoasa(config-group-policy)#
```

**vpn-sessiondb logoff name username *username* 명령은** 사용자 이름별로 사용자를 로그오프합니다.연결이 *끊기면* 관리자 재설정 메시지가 사용자에게 전송됩니다.

```
ciscoasa(config)#vpn-sessiondb logoff name matthewp
Do you want to logoff the VPN session(s)? [confirm]
INFO: Number of sessions with name "matthewp" logged off : 1

ciscoasa(config)#
```

AnyConnect 2.0 클라이언트에 대한 자세한 내용은 Cisco AnyConnect VPN 관리자 설명서를 참조하십시오.

# 문제 해결

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

## 문제 해결 명령(선택 사항)

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다.OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

**참고:** debug **명령**을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

- **debug webvpn svc 255** - WebVPN을 통해 SSL VPN 클라이언트에 대한 연결에 대한 디버그 메시지를 표시합니다.**AnyConnect 로그인 성공**

```
ciscoasa(config)#debug webvpn svc 255
INFO: debug webvpn svc enabled at level 255.
ciscoasa(config)#ATTR_FILTER_ID: Name:
 SSLVPNClientAccess
, Id: 1, refcnt: 1
webvpn_rx_data_tunnel_connect
CSTP state = HEADER_PROCESSING
http_parse_cstp_method()
...input: 'CONNECT /CSCOSSLC/tunnel HTTP/1.1'
webvpn_cstp_parse_request_field()
...input: 'Host: 10.10.1.5' - !--- Outside IP of ASA Processing CSTP header line: 'Host:
10.10.1.5'
webvpn_cstp_parse_request_field()
...input: 'User-Agent: Cisco AnyConnect VPN Client 2, 0, 0343' - !--- AnyConnect Version
Processing CSTP header line: 'User-Agent: Cisco AnyConnect VPN Client 2, 0, 0343' Setting
user-agent to: 'Cisco AnyConnect VPN Client 2, 0, 0343' webvpn_cstp_parse_request_field()
...input: 'Cookie: webvpn=3338474156@28672@1192565782@EFB9042D72C
63CE02164F790435897AC72EE70AE' Processing CSTP header line: 'Cookie:
webvpn=3338474156@28672@119 2565782@EFB9042D72C63CE02164F790435897AC72EE70AE' Found WebVPN
cookie: 'webvpn=3338474156@28672@1192565782@EFB9042D72C 63CE02164F790435897AC72EE70AE'
WebVPN Cookie: 'webvpn=3338474156@28672@1192565782@EFB9042D72C63CE02
164F790435897AC72EE70AE' IPADDR: '3338474156', INDEX: '28672', LOGIN: '1192565782'
webvpn_cstp_parse_request_field() ...input: 'X-CSTP-Version: 1' Processing CSTP header line:
'X-CSTP-Version: 1' Setting version to '1' webvpn_cstp_parse_request_field() ...input: 'X-
CSTP-Hostname: wkstation1' - !--- Client desktop hostname Processing CSTP header line: 'X-
CSTP-Hostname: wkstation1'
Setting hostname to: 'wkstation1'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Accept-Encoding: deflate;q=1.0'
Processing CSTP header line: 'X-CSTP-Accept-Encoding: deflate;q=1.0'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-MTU: 1206'
Processing CSTP header line: 'X-CSTP-MTU: 1206'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Address-Type: IPv4'
Processing CSTP header line: 'X-CSTP-Address-Type: IPv4'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Master-Secret: 72B8AD72F327059AE22CBB451CB0948AFBE98296FD849
                          49EB6CAEDC203865C76BDBD634845FA89634C668A67152ABB51'
Processing CSTP header line: 'X-DTLS-Master-Secret: 72B8AD72F327059AE22CBB451C
       B0948AFBE98296FD84949EB6CAEDC203865C76BDBD634845FA89634C668A67152ABB51'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-CipherSuite: AES256-SHA:AES128-SHA:DES-CBC3-SHA:DES-CBC-SHA'
Processing CSTP header line: 'X-DTLS-CipherSuite: AES256-SHA:AES128-SHA:
                             DES-CBC3-SHA:DES-CBC-SHA'
Validating address: 0.0.0.0
CSTP state = WAIT_FOR_ADDRESS
webvpn_cstp_accept_address: 192.168.25.1/255.255.255.0 - !--- IP assigned from IP Pool CSTP
state = HAVE_ADDRESS SVC: NP setup np_svc_create_session(0x7000, 0xD41612C8, TRUE)
webvpn_svc_np_setup SVC ACL Name: NULL SVC ACL ID: -1 SVC ACL ID: -1 vpn_put_uauth success!
SVC IPv6 ACL Name: NULL SVC IPv6 ACL ID: -1 SVC: adding to sessmgmt SVC: Sending response
Unable to initiate NAC, NAC might not be enabled or invalid policy CSTP state = CONNECTED
```

```
webvpn_rx_data_cstp webvpn_rx_data_cstp: got internal message Unable to initiate NAC, NAC
might not be enabled or invalid policy
```

### AnyConnect 로그인 실패(잘못된 비밀번호)

```
webvpn_portal.c:ewaFormSubmit_webvpn_login[1808]
ewaFormSubmit_webvpn_login: tgCookie = 0
ewaFormSubmit_webvpn_login: cookie = d53d2990
ewaFormSubmit_webvpn_login: tgCookieSet = 0
ewaFormSubmit_webvpn_login: tgroup = NULL
webvpn_portal.c:http_webvpn_kill_cookie[627]
webvpn_auth.c:http_webvpn_pre_authentication[1905]
WebVPN: calling AAA with ewsContext (-717386088) and nh (-717388536)!
WebVPN: started user authentication...
webvpn_auth.c:webvpn_aaa_callback[4380]
WebVPN: AAA status = (REJECT)
webvpn_portal.c:ewaFormSubmit_webvpn_login[1808]
ewaFormSubmit_webvpn_login: tgCookie = 0
ewaFormSubmit_webvpn_login: cookie = d53d2990
ewaFormSubmit_webvpn_login: tgCookieSet = 0
ewaFormSubmit_webvpn_login: tgroup = NULL
webvpn_auth.c:http_webvpn_post_authentication[1180]
WebVPN: user: (matthewp) rejected.
http_remove_auth_handle(): handle 9 not found!
webvpn_portal.c:ewaFormServe_webvpn_login[1749]
webvpn_portal.c:http_webvpn_kill_cookie[627]
```

## 관련 정보

- Cisco AnyConnect VPN 클라이언트 관리자 가이드, 버전 2.0
- AnyConnect VPN 클라이언트 릴리스 정보, 릴리스 2.0
- 기술 지원 및 문서 – Cisco Systems