AnyConnect SSL VPN 연결 흐름 이해

목차

소개

이 문서에서는 SSLVPN 연결 중에 AnyConnect와 보안 게이트웨이 간에 발생하는 이벤트의 흐름에 초점을 맞춥니다.

배경 정보

AnyConnect

AnyConnect는 SSL 및 IKEv2 프로토콜을 위해 설계된 Cisco VPN 클라이언트입니다. 대부분의 데스크톱 및 모바일 플랫폼에서 사용할 수 있습니다. AnyConnect는 주로 Firepower FTD(Threat Defense), ASA(Adaptive Security Appliance) 또는 Cisco IOS®/Cisco IOS® XE 라우터를 통해 보안 게이트웨이(Secure Gateway)를 통해 보안 연결을 설정합니다.

보안 게이트웨이

Cisco 용어에서는 SSL VPN 서버를 Secure Gateway라고 하며 IPSec(IKEv2) 서버를 Remote Access VPN Gateway라고 합니다. Cisco는 다음 플랫폼에서 SSL VPN 터널 종료를 지원합니다.

- Cisco ASA 5500 및 5500-X 시리즈
- Cisco FTD(2100, 4100 및 9300 Series)
- Cisco ISR 4000 및 ISR G2 Series
- Cisco CSR 1000 시리즈
- Cisco Catalyst 8000 시리즈

AnyConnect SSL VPN 연결 흐름

이 문서에서는 SSL VPN 연결 설정 중에 AnyConnect와 Secure Gateway 간에 발생하는 이벤트를 다음 6단계로 분류합니다.

1. SSL 핸드셰이크

2. POST - 그룹 선택

3. POST - 사용자 이름/비밀번호를 사용한 사용자 인증(선택 사항)

4. VPN 다운로더(선택 사항)

5. CSTP 연결

6. DTLS 연결(선택 사항)

1. SSL 핸드셰이크

SSL 핸드셰이크는 'Client Hello' 메시지와 함께 TCP 3-way 핸드셰이크가 완료된 후 AnyConnect 클라이언트에 의해 시작됩니다. 이벤트의 흐름과 핵심 요점은 앞서 언급한 바와 같습니다.

클라이언트 Hello

SSL 세션은 클라이언트가 'Client Hello' 메시지를 보내는 것으로 시작합니다. 이 메시지에서 다음을 수행합니다.

a) SSL 세션 ID가 0으로 설정되어 새 세션의 시작을 나타냅니다.

b) 페이로드는 클라이언트가 지원하는 암호 그룹과 클라이언트가 생성한 랜덤 논스를 포함한다.

서버 Hello

서버는 다음을 포함하는 "Server Hello" 메시지로 응답합니다.

a) 클라이언트가 제공한 목록에서 선택한 암호 그룹.

b) 서버에서 SSL 세션 ID를 생성하고 서버에서 임의의 nonce를 생성했습니다.

서버 인증서

'Server Hello' 이후 서버는 ID 역할을 하는 SSL 인증서를 전송합니다. 주요 내용은 다음과 같습니다
.

a) 이 인증서의 엄격한 유효성 검사가 실패할 경우 AnyConnect는 기본적으로 서버를 차단합니다.

b) 사용자는 이 차단을 비활성화할 수 있는 옵션이 있지만, 보고된 오류가 해결될 때까지 후속 연결에 경고가 표시됩니다.

클라이언트 인증서 요청

서버는 또한 클라이언트 인증서를 요청하여 보안 게이트웨이에 로드된 모든 CA 인증서의 주체 이름 DN 목록을 전송할 수 있습니다. 이 요청은 두 가지 목적으로 사용됩니다.

a) 여러 ID 인증서를 사용할 수 있는 경우 클라이언트(사용자)가 올바른 ID 인증서를 선택할 수 있도록 지원합니다.

b) 추가 인증서 검증이 계속 수행되어야 하지만 반환된 인증서가 보안 게이트웨이에서 신뢰되는지 확인합니다.

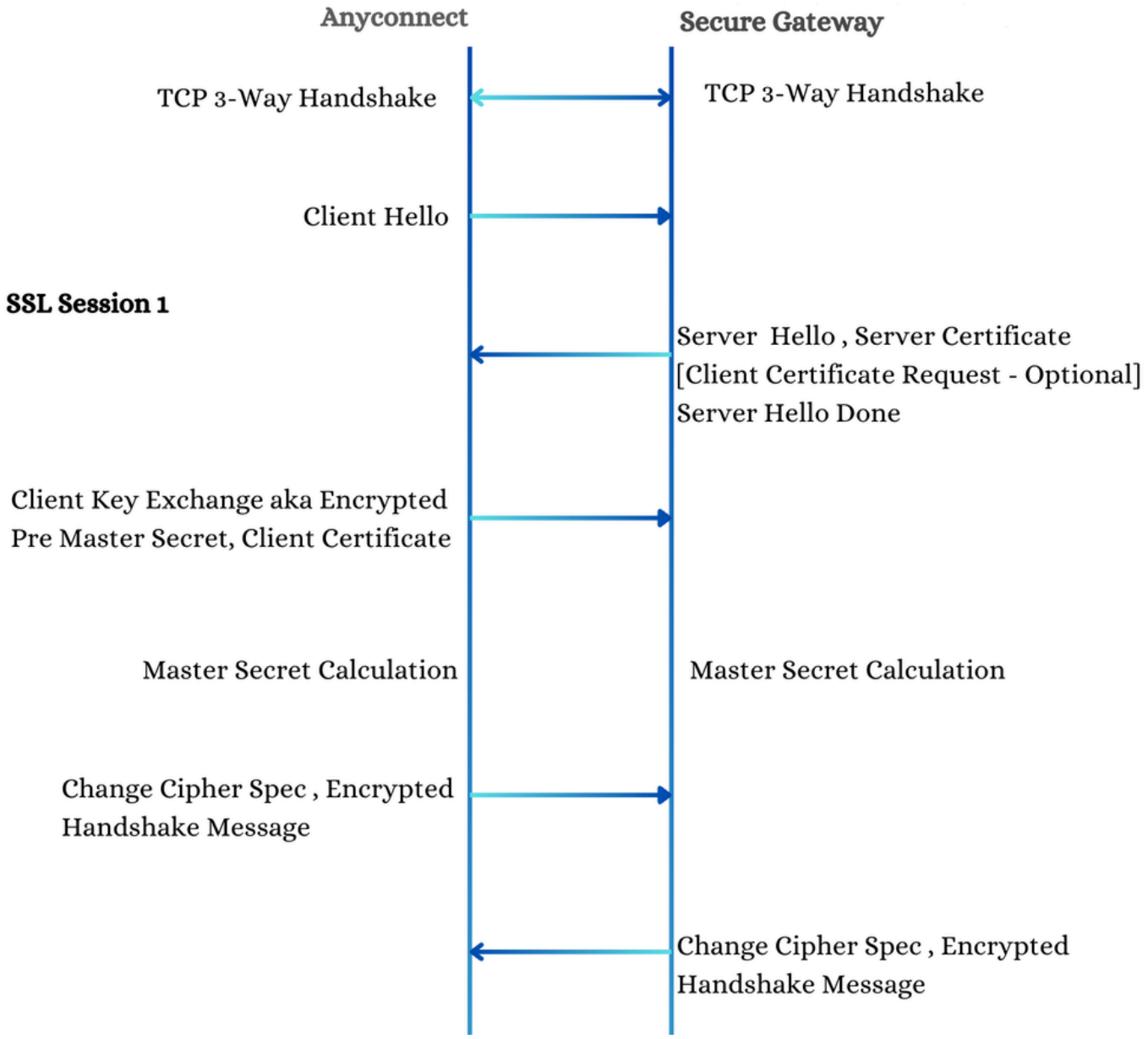
클라이언트 키 교환

그런 다음 클라이언트는 사전 마스터 비밀 키를 포함하는 '클라이언트 키 교환' 메시지를 보냅니다. 이 키는 다음을 사용하여 암호화됩니다.

a) 선택한 암호 그룹이 RSA 기반인 경우 서버 인증서의 서버 공개 키(예: TLS_RSA_WITH_AES_128_CBC_SHA).

b) 선택한 암호 그룹이 DHE 기반(예: TLS_DHE_DSS_WITH_AES_256_CBC_SHA)인 경우 Server Hello 메시지에 제공된 서버의 DH 공개 키.

사전 마스터 비밀, 클라이언트에서 생성한 랜덤 논스 및 서버에서 생성한 랜덤 논스를 기반으로 클라이언트와 보안 게이트웨이 모두 독립적으로 마스터 비밀을 생성합니다. 그런 다음 이 마스터 암호를 사용하여 세션 키를 파생시킴으로써 클라이언트와 서버 간의 안전한 통신을 보장합니다.



SSL 세션 1

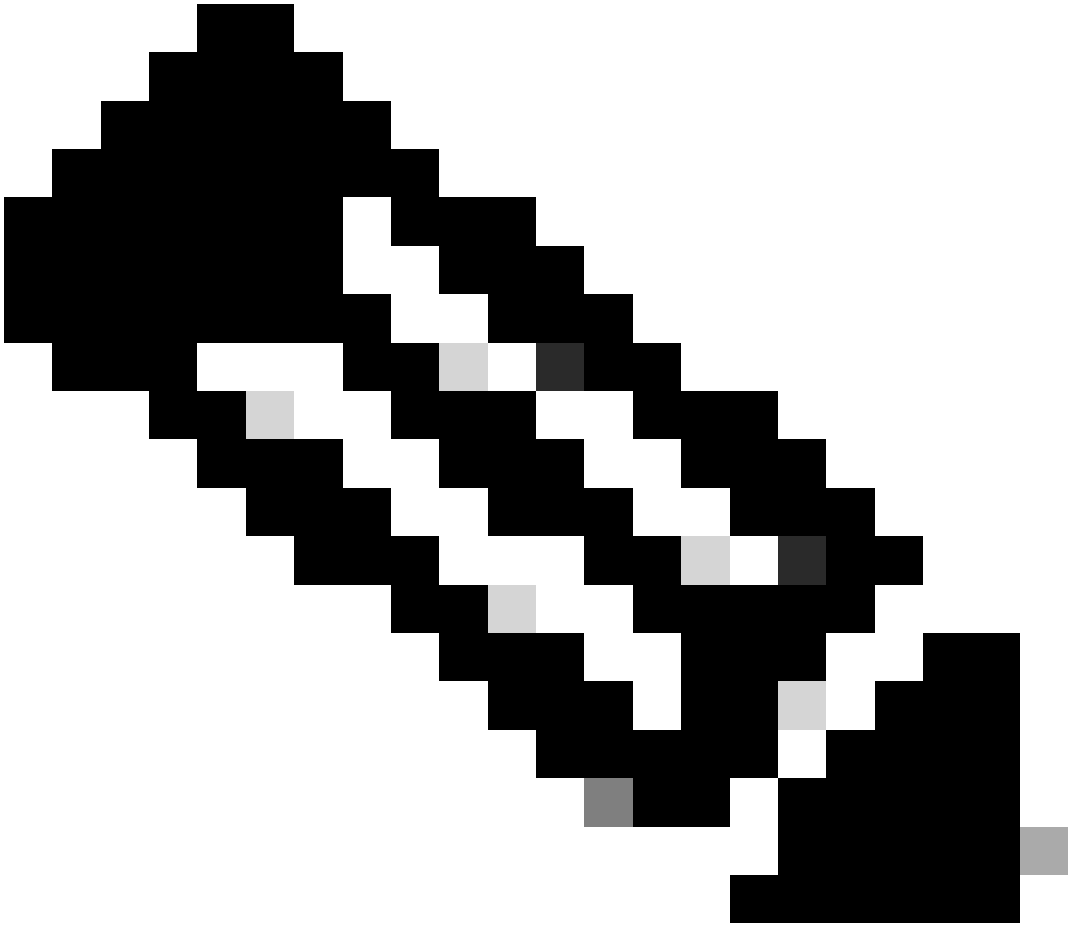
2. POST - 그룹 선택

이 작업 중에 클라이언트는 사용자가 명시적으로 지정하지 않는 한 연결 프로파일에 대한 정보를 보유하지 않습니다. 연결 시도는 요청의 'group-access' 요소에 표시된 대로 보안 게이트웨이 URL(asav.cisco.com)로 전달됩니다. 클라이언트는 'aggregate-authentication' 버전 2에 대한 지원을 나타냅니다. 이 버전은 특히 효율적인 XML 트랜잭션의 측면에서 이전 버전에 비해 크게 향상되었습니다. 보안 게이트웨이와 클라이언트 모두 사용할 버전에 동의해야 합니다. 보안 게이트웨이가 버전 2를 지원하지 않는 시나리오에서는 추가 POST 작업이 트리거되어 클라이언트가 해당 버전으로 되돌아갑니다.

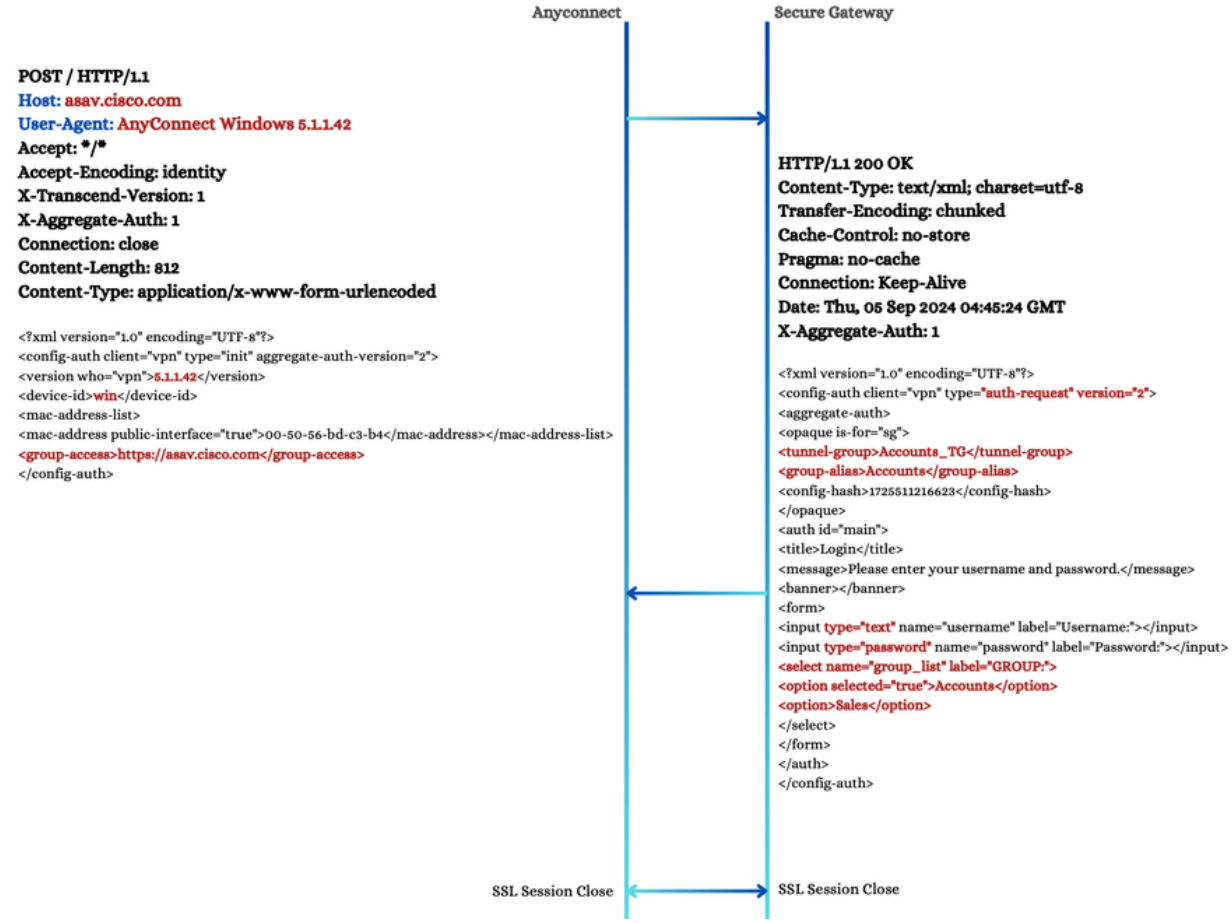
HTTP 응답에서 보안 게이트웨이는 다음을 나타냅니다.

1. 보안 게이트웨이가 지원하는 종합 인증의 버전.

2. 터널 그룹 목록 및 사용자 이름/비밀번호 양식

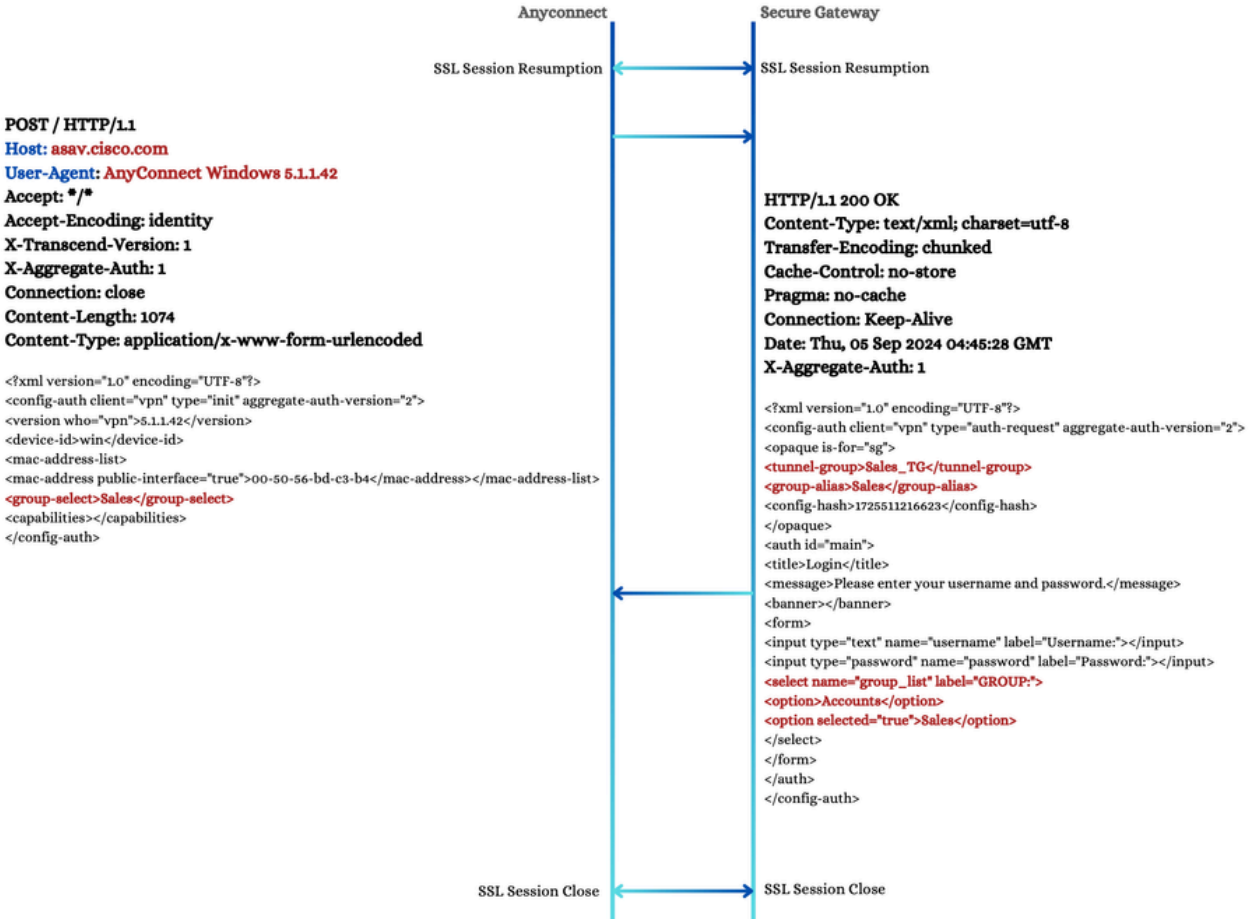


참고: 양식에는 보안 게이트웨이에 구성된 모든 연결 프로파일의 그룹 별칭을 나열하는 'select' 요소가 포함됩니다. 기본적으로 이러한 그룹 별칭 중 하나는 선택된 = "true" 부울 특성으로 강조 표시됩니다. tunnel-group 및 group-alias 요소는 선택한 이 연결 프로파일에 해당합니다.



POST - 그룹 선택 1

사용자가 이 목록에서 다른 연결 프로파일을 선택하면 다른 POST 작업이 수행됩니다. 이 경우 클라이언트는 여기에 표시된 것처럼 선택한 연결 프로파일을 반영하기 위해 업데이트된 'group-select' 요소와 함께 POST 요청을 보냅니다.



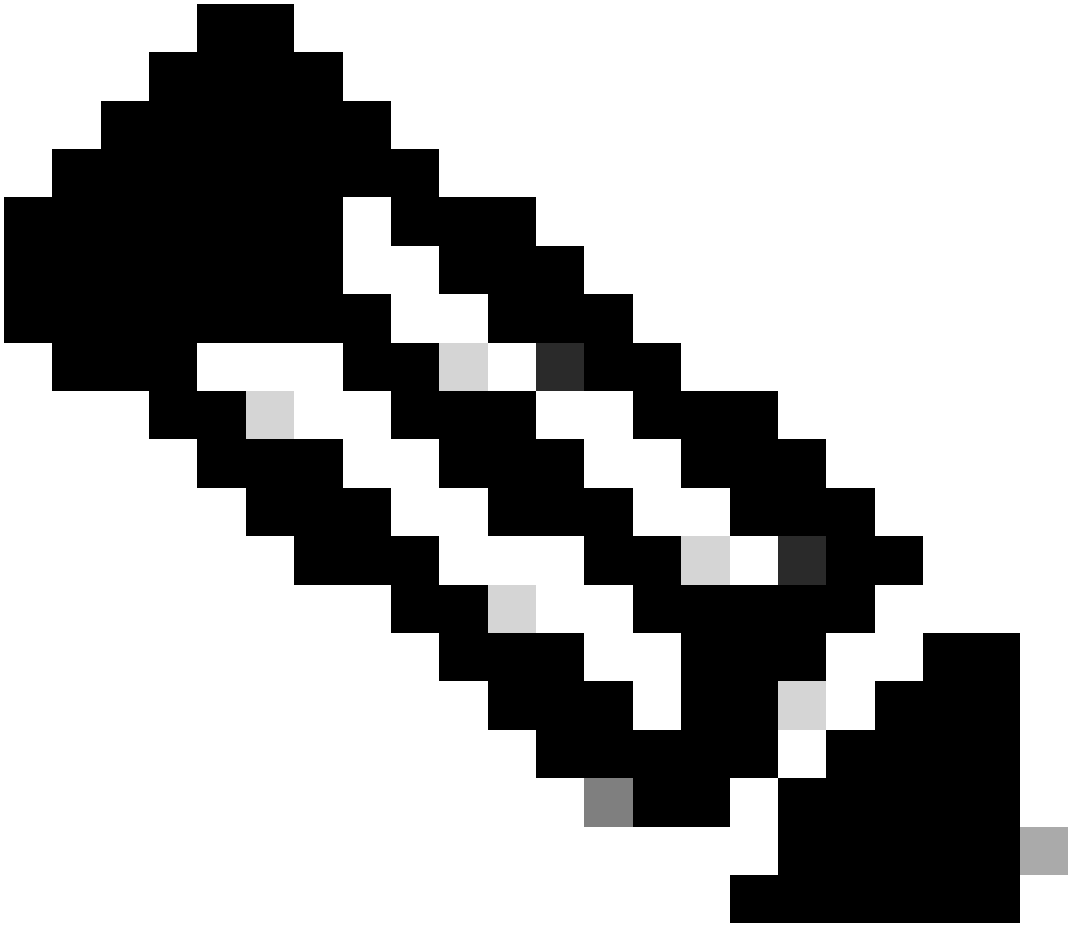
POST - 그룹 선택 2

3. POST - 사용자 인증

POST-Group Selection(POST 그룹 선택) 다음에 오는 이 작업에서 AnyConnect는 이 정보를 보안 게이트웨이로 전송합니다.

1. 선택된 연결 프로파일 정보: 이전 작업에서 보안 게이트웨이에 지정된 대로 터널 그룹 이름 및 그룹 별칭이 포함됩니다.

2. 사용자 이름 및 비밀번호: 사용자의 인증 자격 증명



참고: 이 흐름은 AAA 인증에만 적용되므로 다른 인증 방법과 다를 수 있습니다.

POST 작업에 대한 응답으로 보안 게이트웨이는 다음 정보가 포함된 XML 파일을 전송합니다.

1. 세션 ID: SSL 세션 ID와 다릅니다.

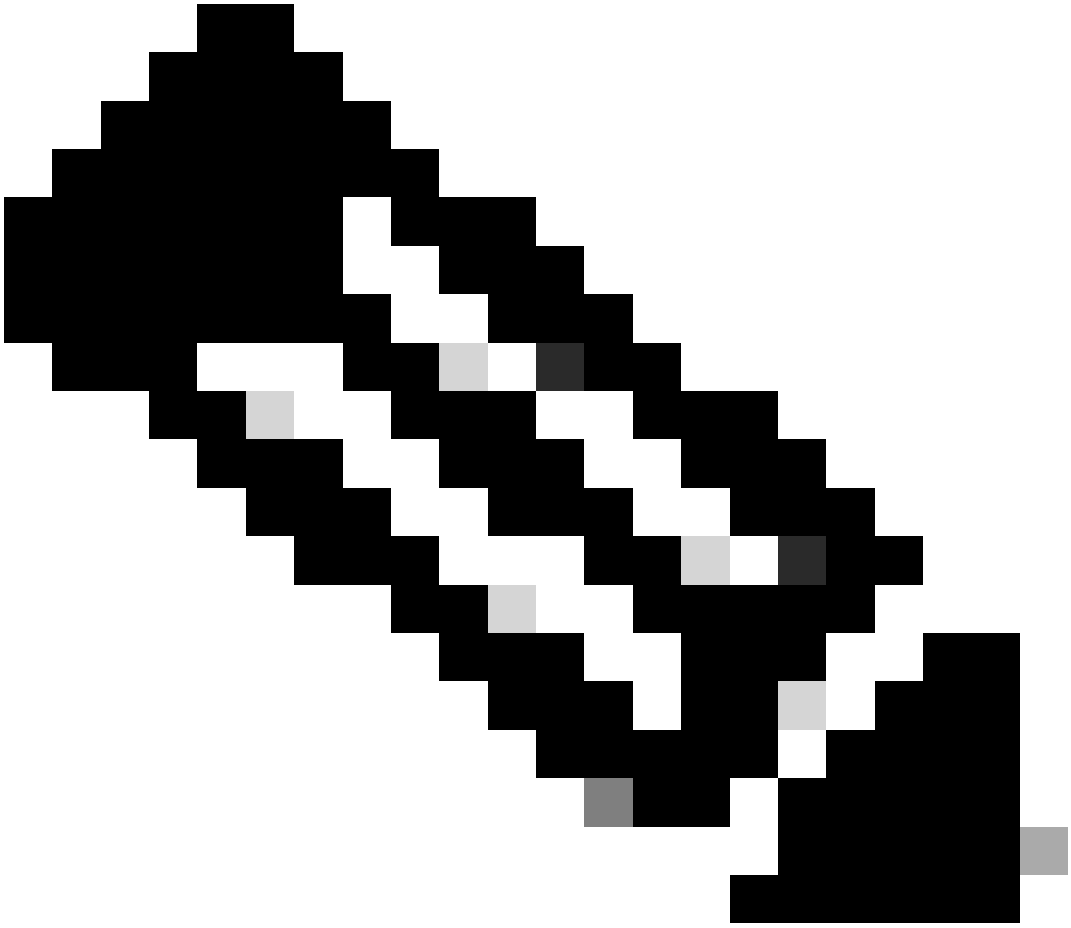
2. 세션 토큰: 이 토큰은 나중에 클라이언트에서 WebVPN 쿠키로 사용됩니다.

3. 인증 상태: id = '성공'인 auth 요소로 표시됩니다.

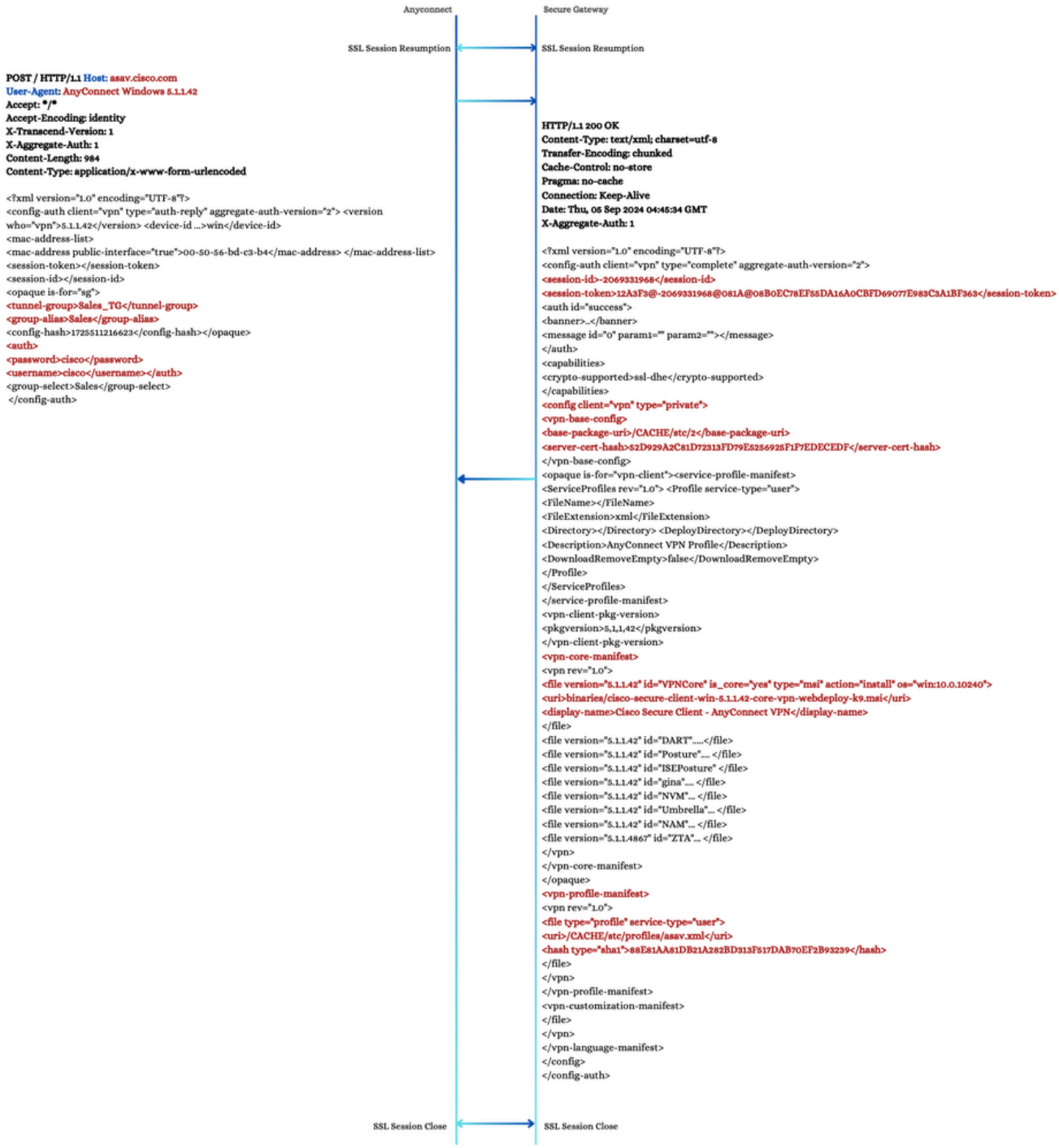
4. 서버 인증서 해시: 이 해시는 preferences.xml 파일에 캐시됩니다.

5. vpn-core-manifest 요소: 이 요소는 AnyConnect 코어 패키지의 경로 및 버전과 Dart, Posture, ISE Posture 등의 다른 구성 요소를 나타냅니다. 다음 섹션의 VPN 다운로더에서 사용됩니다.

6. vpn-profile-manifest 요소: 이 요소는 프로파일의 경로(프로파일 이름) 및 SHA-1 해시를 나타냅니다.



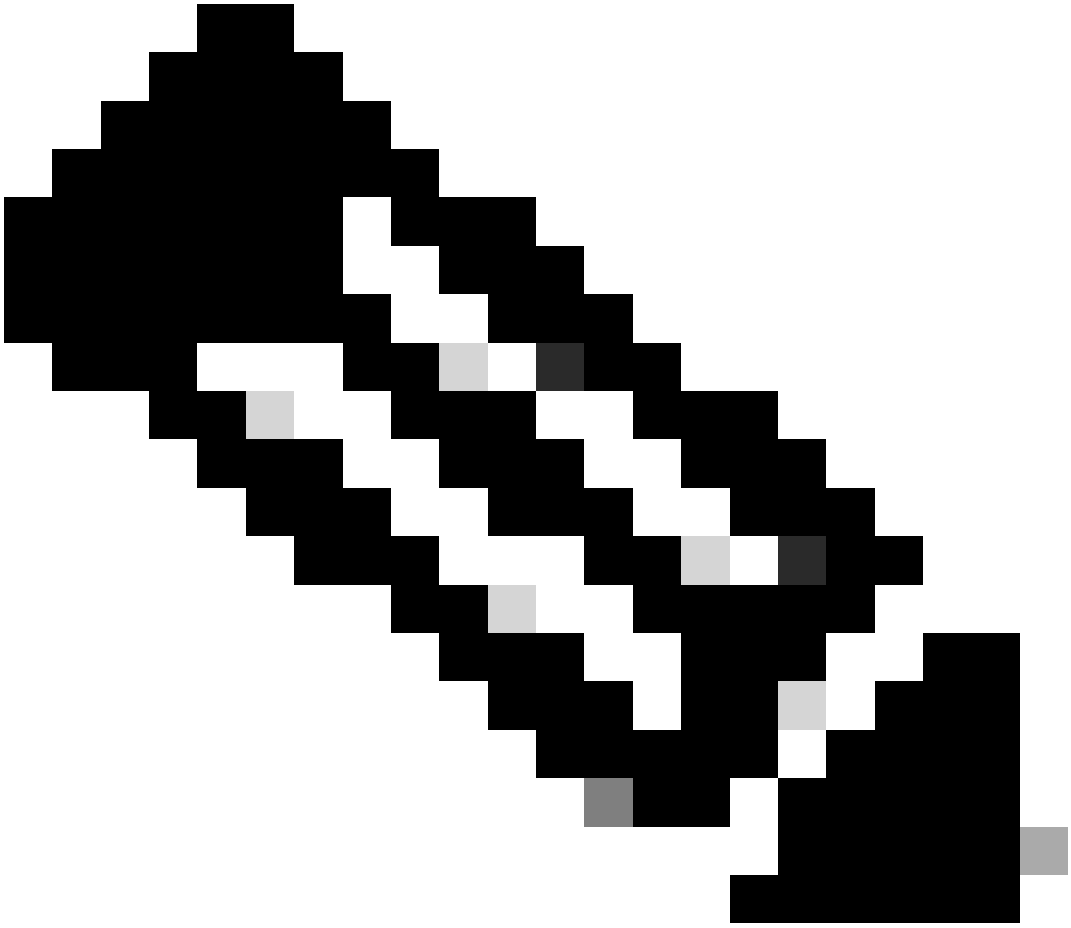
참고: 클라이언트에 프로필이 없는 경우 다음 섹션의 VPN 다운로더가 프로필을 다운로드합니다. 클라이언트가 이미 프로필을 가지고 있는 경우 클라이언트 프로필의 SHA-1 해시를 서버의 SHA-1 해시와 비교합니다. 불일치하는 경우 VPN 다운로더는 클라이언트 프로파일을 보안 게이트웨이의 프로파일로 덮어씁니다. 이렇게 하면 보안 게이트웨이의 프로파일이 클라이언트 사후 인증에 적용됩니다.



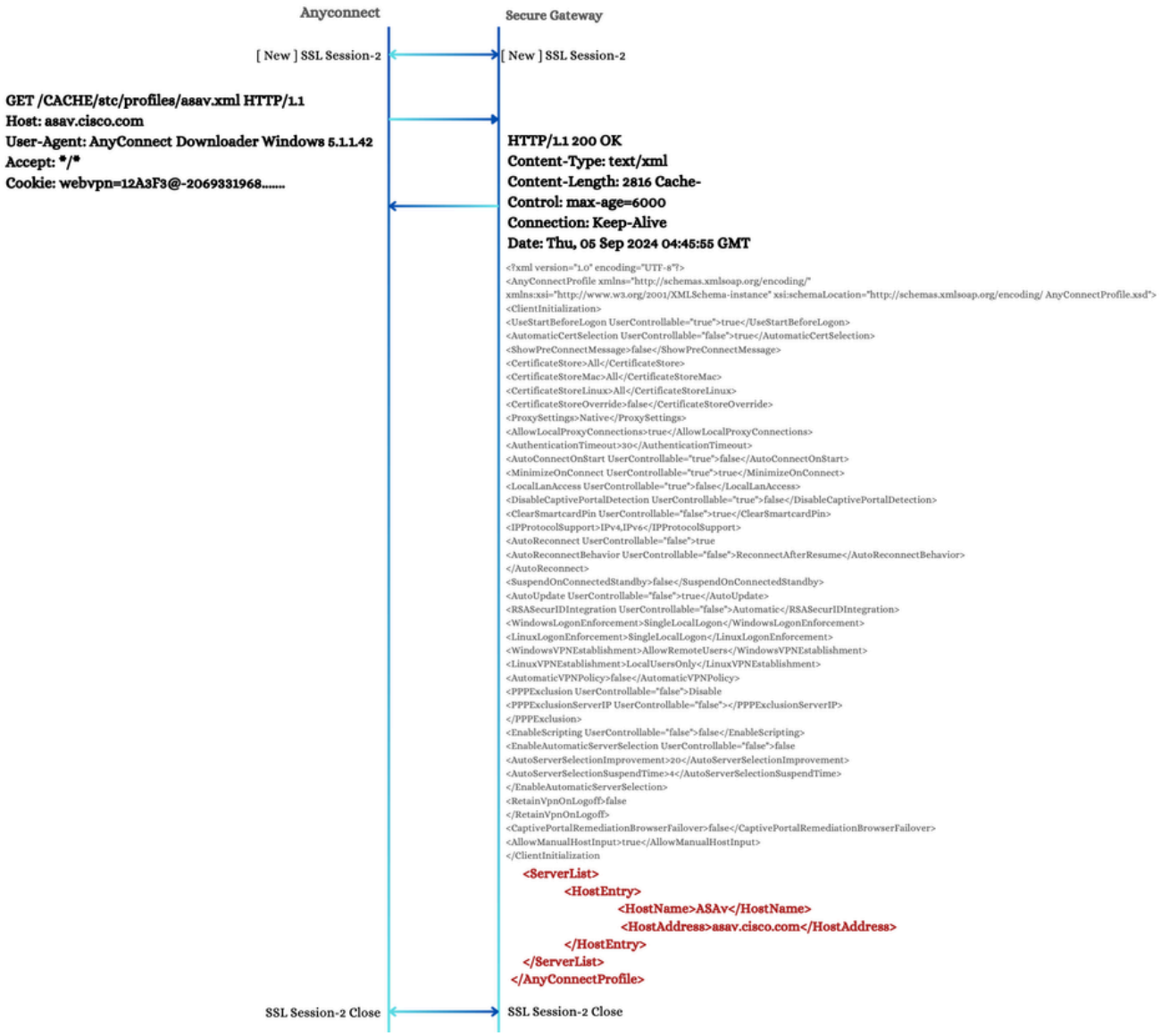
POST - 사용자 인증

4. AnyConnect 다운로더

AnyConnect 다운로더는 항상 새 SSL 세션을 시작하므로 사용자는 보안 게이트웨이의 인증서를 신뢰할 수 없는 경우 두 번째 인증서 경고를 경험할 수 있습니다. 이 단계에서는 다운로드해야 하는 각 항목에 대해 별도의 GET 작업을 수행합니다.



참고: 클라이언트 프로파일이 보안 게이트웨이에 업로드되면 반드시 다운로드해야 합니다. 그렇지 않으면 전체 연결 시도가 종료됩니다.

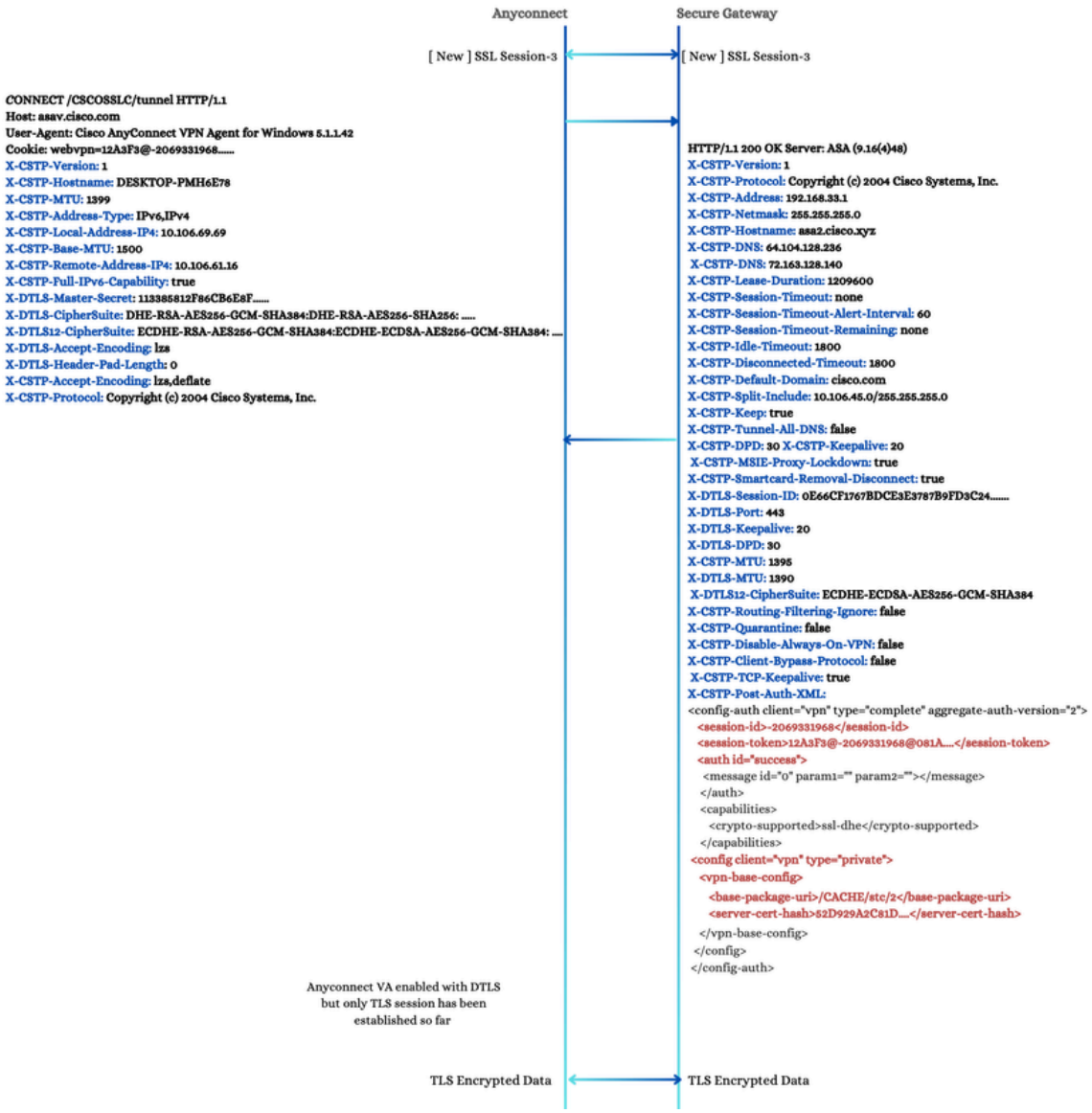


VPN 다운로더

5. CSTP 연결

AnyConnect는 보안 채널 설정의 최종 단계로 CONNECT 작업을 수행합니다. CONNECT 작업 중에 AnyConnect 클라이언트는 프로세스를 위해 보안 게이트웨이에 대한 다양한 X-CSTP 및 X-DTLS 특성을 전송합니다. 보안 게이트웨이는 클라이언트가 현재 연결 시도에 적용하는 추가 X-CSTP 및 X-DTLS 특성으로 응답합니다. 이 교환에는 X-CSTP-Post-Auth-XML과 XML 파일이 포함되며, 이는 POST - 사용자 인증 단계에서 표시되는 것과 대부분 유사합니다.

성공적인 응답을 받은 후 AnyConnect는 TLS 데이터 채널을 시작합니다. 동시에 AnyConnect 가상 어댑터 인터페이스는 X-DTLS-MTU와 동일한 MTU 값으로 활성화되며, 이는 후속 DTLS 핸드셰이크가 성공적임을 전제로 합니다.



CSTP 연결

6. DTLS 핸드셰이크

DTLS 핸드셰이크는 여기에 설명된 대로 진행됩니다. 이 설정은 CONNECT 이벤트 동안 클라이언트와 서버 간에 교환된 특성 때문에 비교적 빠릅니다.

클라이언트

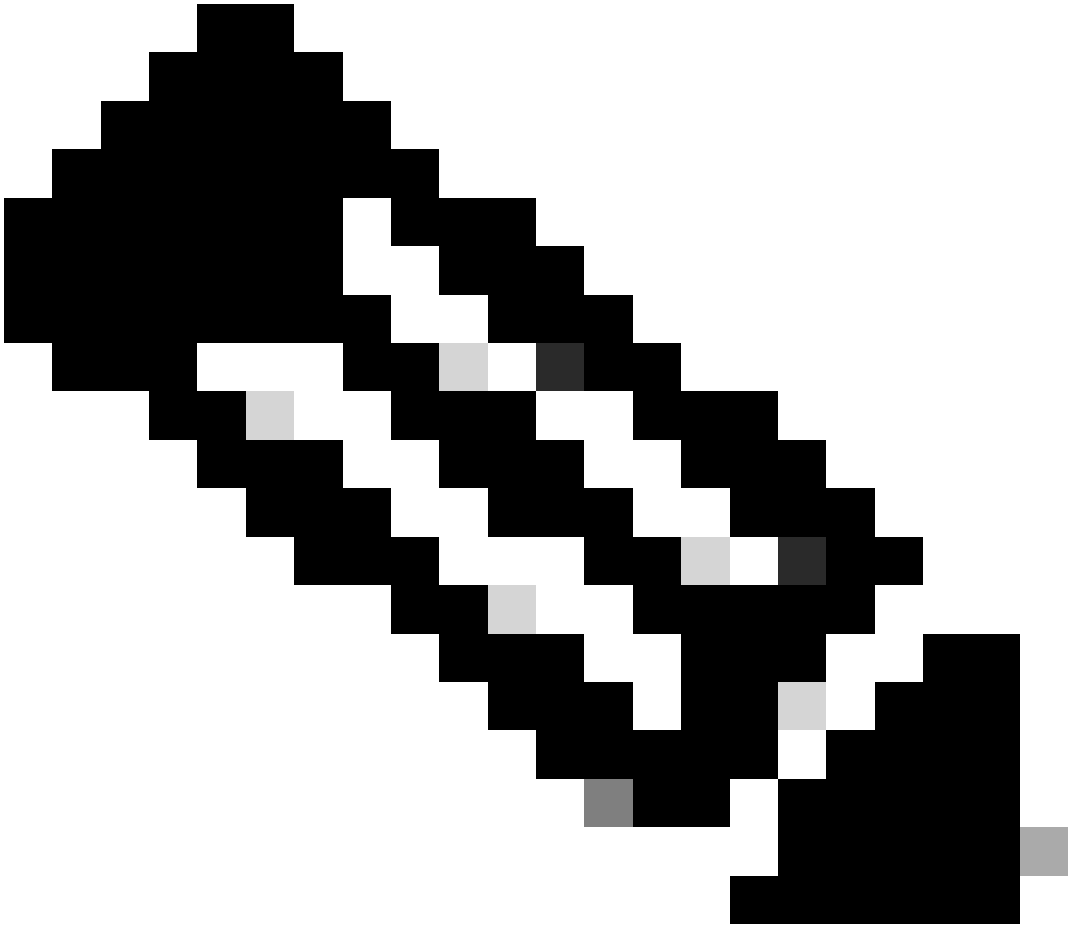
X-DTLS-Master-Secret: DTLS 마스터 암호는 클라이언트에 의해 생성되고 서버와 공유됩니다. 이 키는 안전한 DTLS 세션을 설정하는 데 중요합니다.

X-DTLS-CipherSuite: 클라이언트에서 지원하는 DTLS 암호 그룹 목록으로, 클라이언트의 암호화 기능을 나타냅니다.

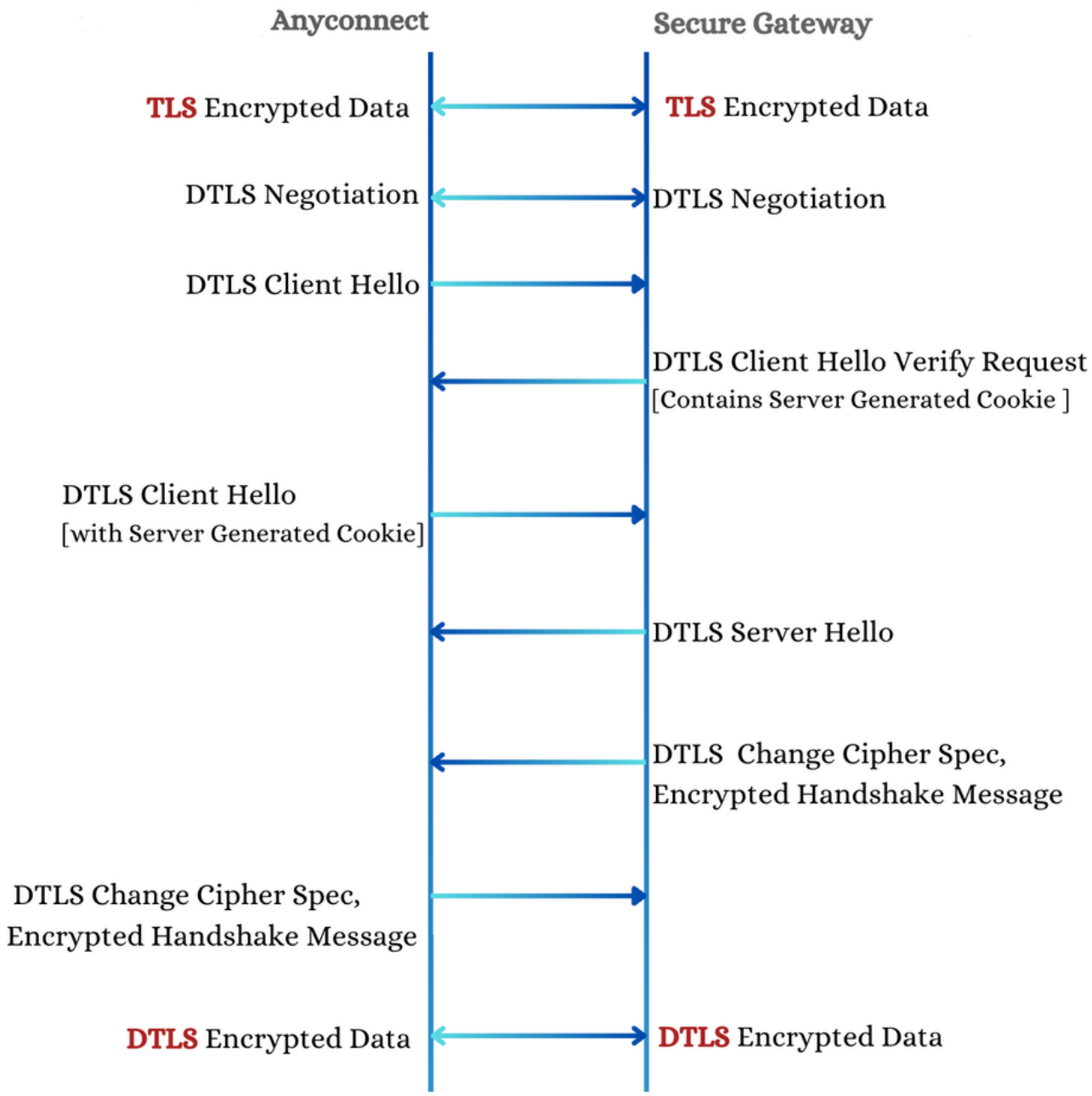
서버

X-DTLS-Session-ID: 클라이언트가 사용하도록 서버가 할당한 DTLS 세션 ID로, 세션 연속성을 보장합니다.

X-DTLS-CipherSuite: 클라이언트가 제공한 목록에서 서버가 선택한 암호 그룹으로, 양 당사자가 호환되는 암호화 방법을 사용하도록 보장합니다.



참고: DTLS 핸드셰이크가 진행 중인 동안에는 TLS 데이터 채널이 계속 작동합니다. 이는 핸드셰이크 프로세스 동안 데이터 전송이 일관되고 안전하게 유지되도록 보장합니다. DTLS 데이터 암호화 채널로의 원활한 전환은 DTLS 핸드셰이크가 완료된 후에만 발생합니다.

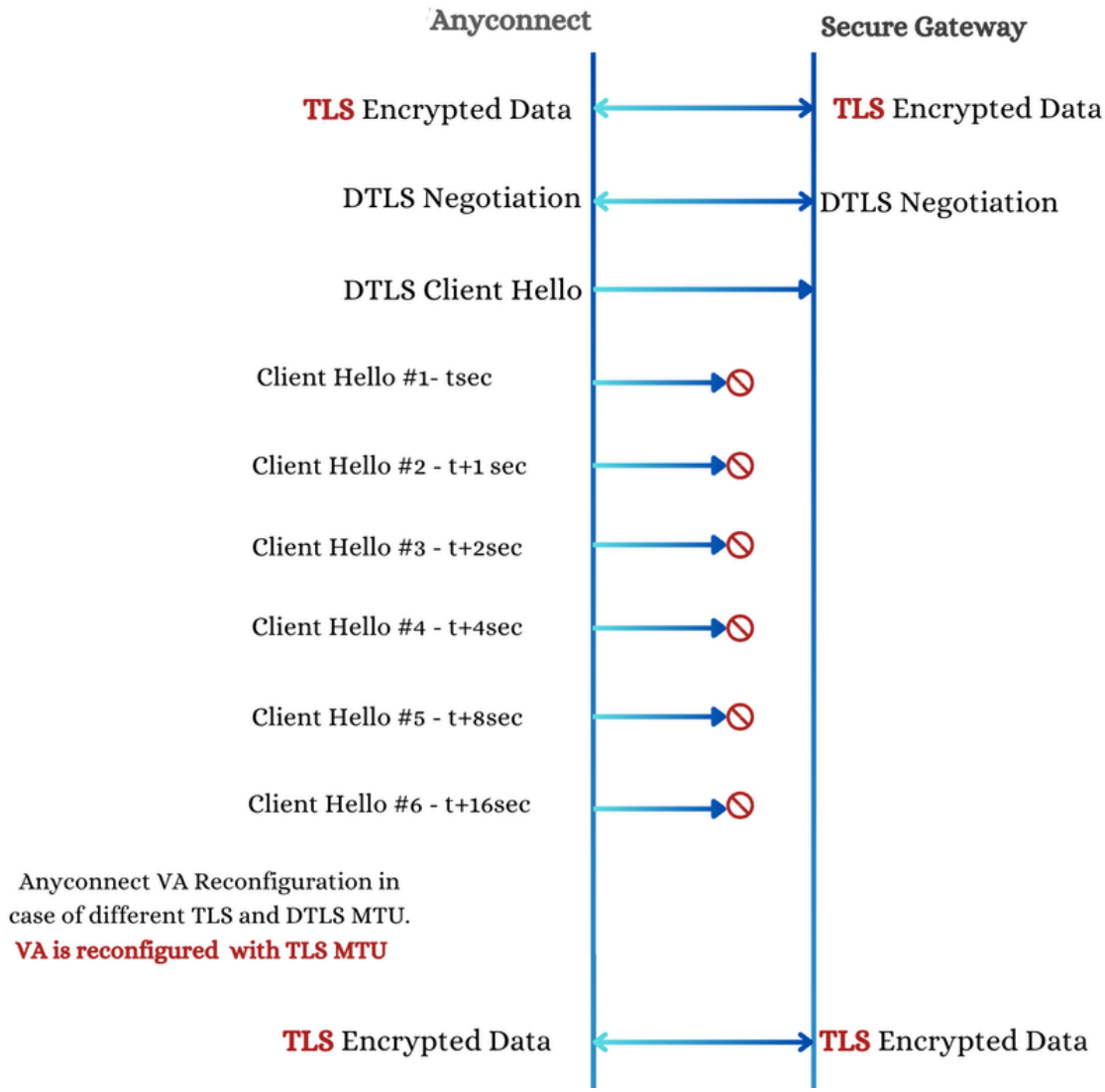


DTLS 핸드셰이크

6.1. DTLS 포트 차단됨

DTLS 포트가 차단되거나 보안 게이트웨이가 DTLS 클라이언트 Hello 패킷에 응답하지 못할 경우 AnyConnect는 최대 5번의 재시도를 통해 1초 지연부터 시작하여 최대 16초까지 증가하는 지수 백오프를 수행합니다.

이러한 시도가 실패하면 AnyConnect는 5단계에서 보안 게이트웨이에서 반환한 X-CSTP-MTU 값에 따라 지정된 실제 TLS MTU를 AnyConnect 가상 어댑터에 적용합니다. 이 MTU는 이전에 적용된 MTU(X-DTLS-MTU)와 다르므로 가상 어댑터를 재구성해야 합니다. 이러한 재구성은 최종 사용자에게 재연결 시도로 나타나지만, 이 프로세스 동안 새로운 협상이 발생하지 않습니다. 가상 어댑터가 다시 구성되면 TLS 데이터 채널이 계속 작동합니다.



DTLS 포트 블록

관련 정보

- Cisco VPN 기술 설명서 참조
- Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.