IKEv2 및 AnyConnect 재연결 기능 이해

목차

소개

이 문서에서는 AnyConnect용 Cisco IOS® 및 Cisco IOS® XE 라우터에서 IKEv2 자동 재연결 기능이 작동하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- IKEv2(Internet Key Exchange 버전 2)
- CSC(Cisco Secure Client)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 버전 17.16.01a를 실행하는 Cisco Catalyst 8000V(C8000V)
- Cisco Secure Client 버전 5.1.8.105
- Cisco Secure Client가 설치된 클라이언트 PC

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

IKEv2 및 Cisco Secure Client Reconnect 기능

Cisco Secure Client의 자동 재연결 기능을 사용하면 일정 기간 세션을 기억하고 보안 채널을 설정한 후 연결을 다시 시작할 수 있습니다. Cisco Secure Client가 IKEv2(Internet Key Exchange Version 2)와 함께 널리 사용됨에 따라 IKEv2는 Secure Client 기능의 Auto Reconnect 기능에 대한 Cisco IKEv2 지원을 통해 Cisco IOS Software에서 Auto Reconnect 기능 지원을 확장합니다.

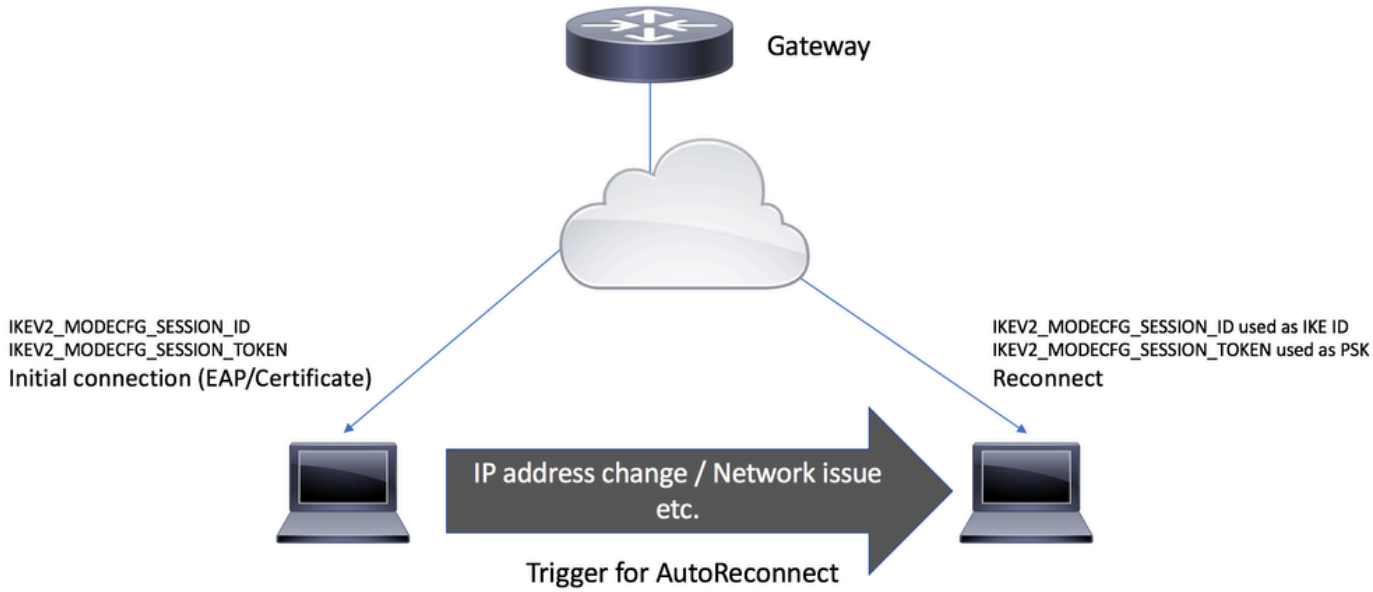
Cisco Secure Client에서 자동 재연결은 다음 시나리오에서 수행됩니다.

1. 중간 네트워크가 다운되었습니다. Cisco Secure Client는 세션이 가동 중일 때 재시작을 시도합니다.
2. Cisco Secure Client 디바이스는 네트워크 간에 전환됩니다. 그러면 소스 포트가 변경되어 기존 SA(Security Association)가 중단되므로 Cisco Secure Client는 자동 재연결 기능을 사용하여 SA를 다시 시작합니다.
3. Cisco Secure Client 디바이스는 절전 모드 또는 최대 절전 모드에서 돌아온 후 SA를 다시 시작하려고 시도합니다.

자동 재연결 기능의 장점

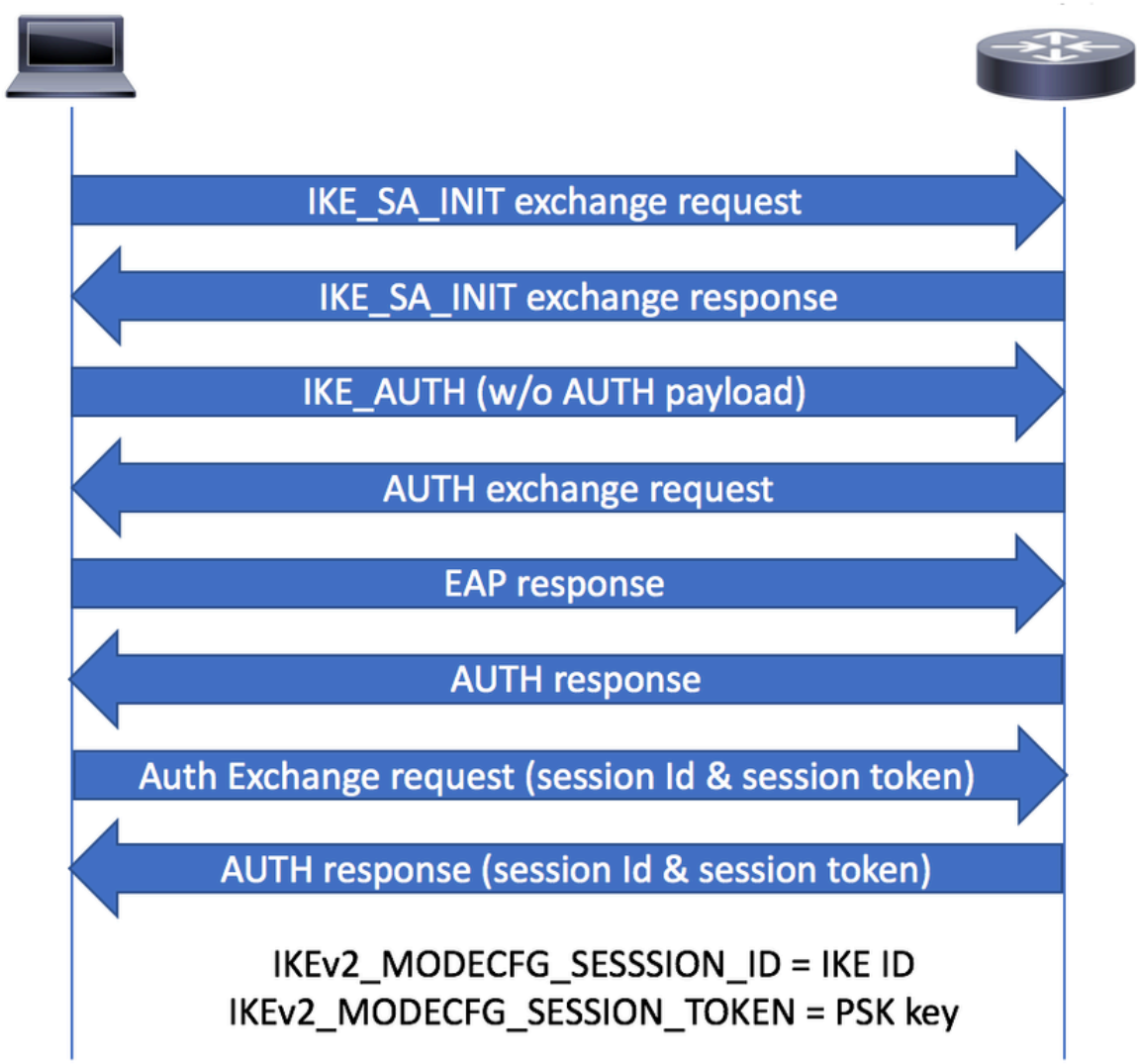
- 원래 세션에서 사용된 컨피그레이션 특성은 AAA(authentication, authorization, and accounting) 서버를 쿼리하지 않고 재사용됩니다.
- IKEv2 게이트웨이는 클라이언트에 다시 연결하기 위해 RADIUS 서버에 연결할 필요가 없습니다.
- 세션을 재개하는 동안 인증 또는 권한 부여에 대한 사용자 상호 작용이 필요하지 않습니다.
- 인증 방법은 세션을 다시 연결할 때 사전 공유 키입니다. 이 인증 방법은 다른 인증 방법에 비해 빠르다.
- 사전 공유 키 인증 방법은 최소한의 리소스로 Cisco IOS 소프트웨어에서 세션을 재개하는 데 도움이 됩니다.
- 사용되지 않은 SA(Security Association)가 제거되어 암호화 리소스가 해제됩니다.

자동 재연결 연결 흐름

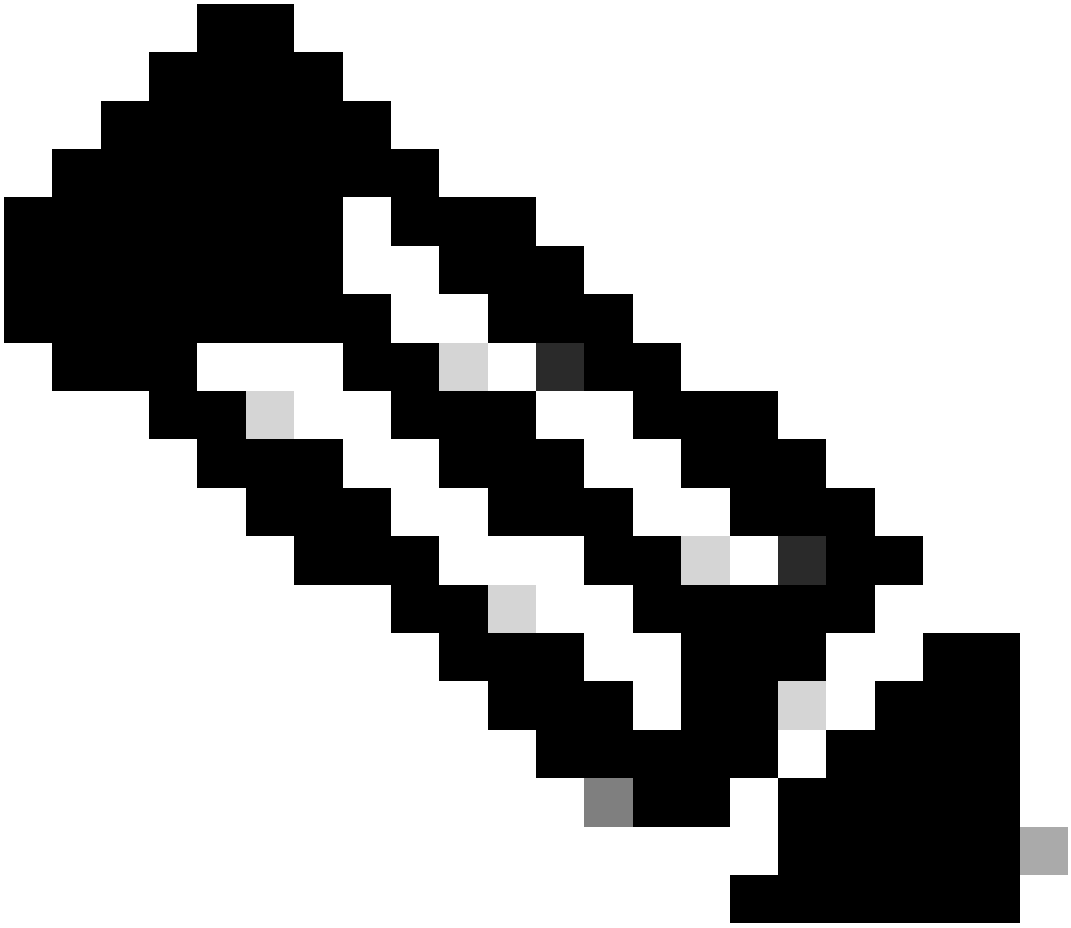


자동 재연결 트리거

1. AUTH 교환 중에 Cisco Secure Client는 IKE_AUTH 요청의 MODECFG_REQ 페이로드에서 IKEv2 게이트웨이의 Session-token 및 Session-id 특성에 대해 요청합니다.
2. IKEv2 게이트웨이는 Secure Client 기능의 자동 재연결 기능에 대한 Cisco IOS IKEv2 지원이 reconnect 명령을 사용하여 IKEv2 프로파일에서 활성화되었는지 확인하고, 선택한 IKEv2 프로파일의 IKEv2 정책을 선택하고, IKE_AUTH 응답의 CFGMODE_REPLY 페이로드에서 세션 ID 및 세션 토큰 특성을 보안 클라이언트로 전송합니다.



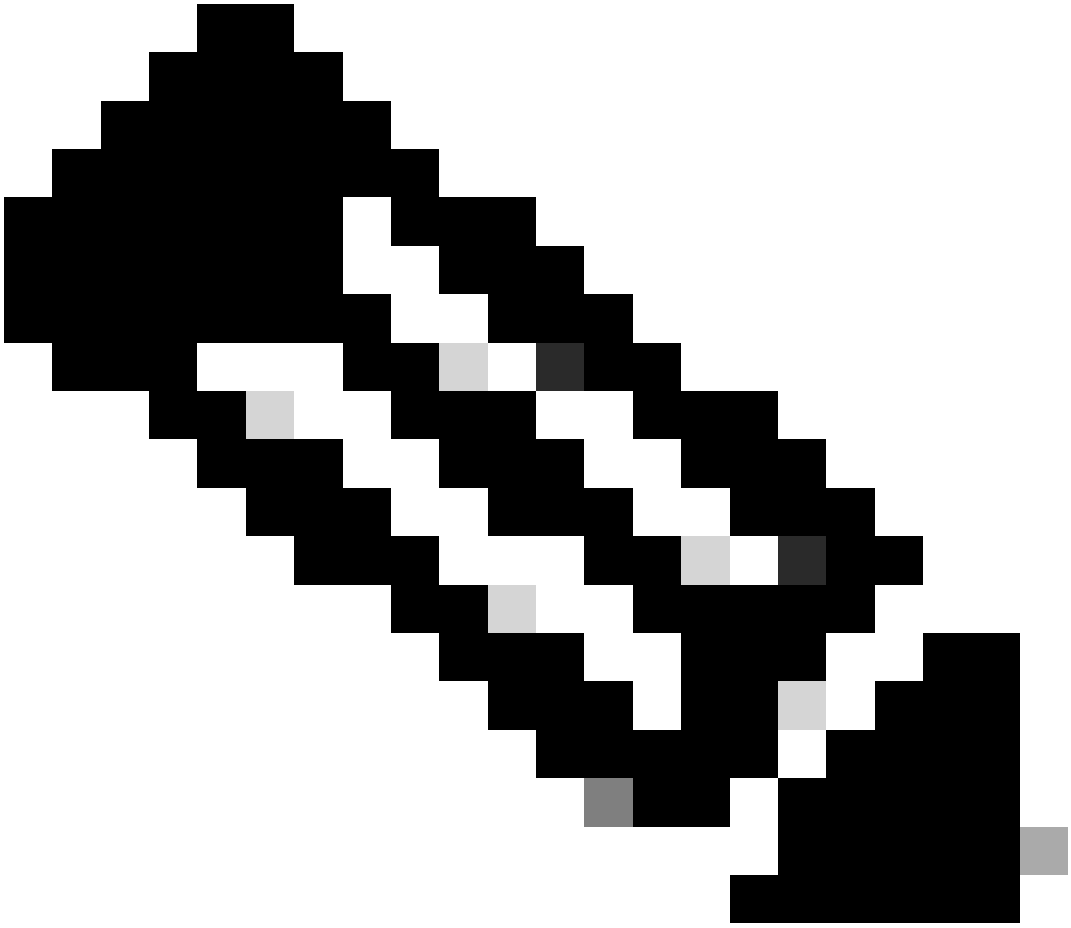
CFGMODE Exchange



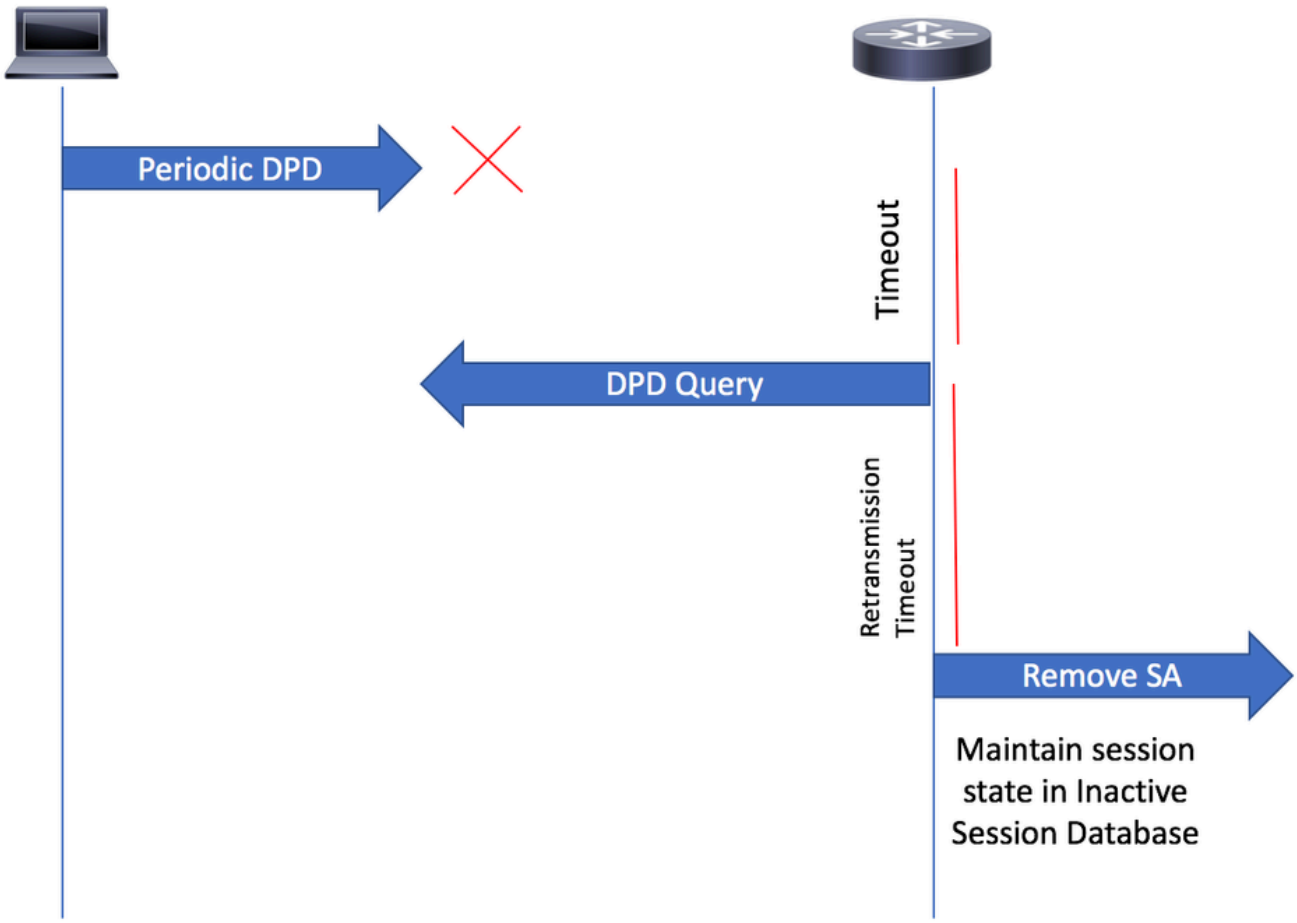
참고: 응답하지 않는 클라이언트를 식별하는 프로세스는 DPD(Dead Peer Detection)를 기반으로 합니다. IKEv2 프로파일에서 재연결 기능이 활성화된 경우 DPD가 IKEv2에서 온디맨드로 대기하므로 DPD를 구성할 필요가 없습니다

---

3. Cisco Secure Client가 게이트웨이로 DPD 메시지를 주기적으로 전송합니다. DPD가 온디맨드로 대기될 경우 게이트웨이는 클라이언트로부터 DPD를 수신할 때까지 클라이언트에 DPD 메시지를 보내지 않습니다. 보안 클라이언트에서 DPD가 지정된 기간 내에 수신되지 않으면(구성된 DPD 간격에 따라) 게이트웨이에서 DPD 메시지를 전송합니다. 보안 클라이언트에서 응답을 받지 못하면 SA가 활성 세션 데이터베이스에서 삭제됩니다.



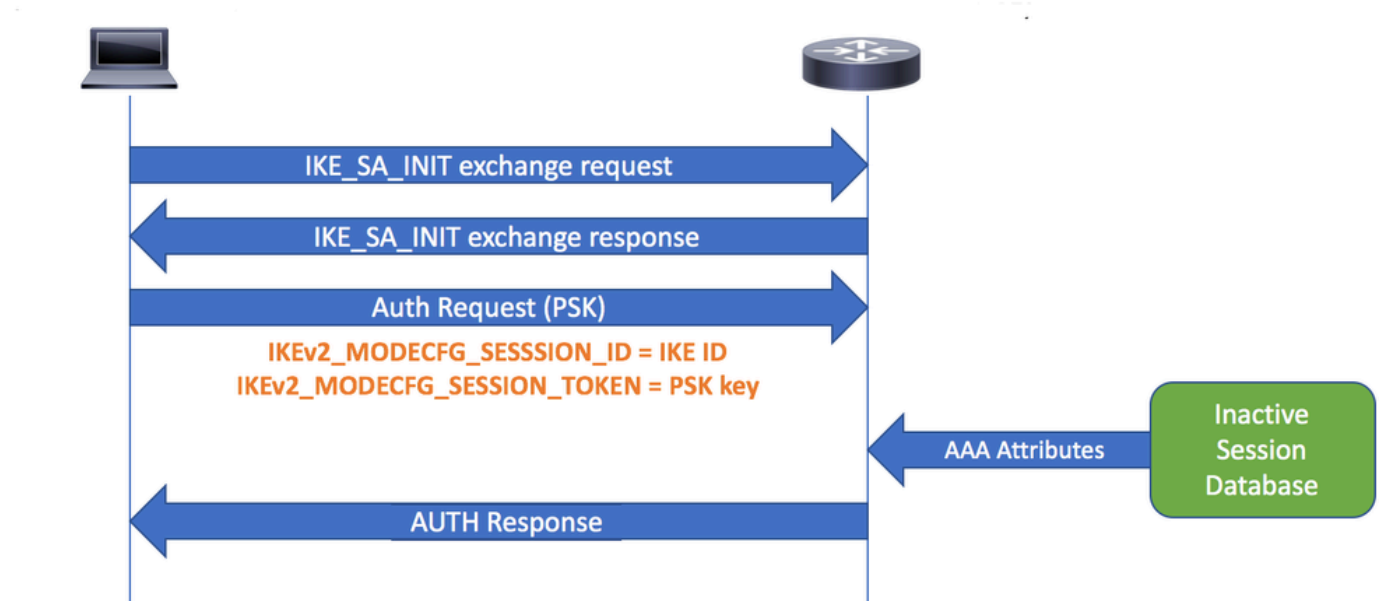
참고: 게이트웨이는 구성된 재연결 시간 초과 기간에 따라 재연결을 허용하기 위해 별도의 비활성 세션 데이터베이스에서 세션 상태(예: AAA 특성)를 계속 유지 관리합니다.



DPD 쿼리

4. 클라이언트가 다시 연결을 시도할 때 새 IKE SA를 생성하고 IKE ID(ID)를 세션 ID로 사용합니다. 이 세션 ID는 MODECFG_REPLY 페이로드에서 수신됩니다. 이때 Cisco Secure Client는 재연결을 위해 IKE PSK 인증을 사용하며, 사전 공유 키는 이전에 수신한 세션 토큰입니다.

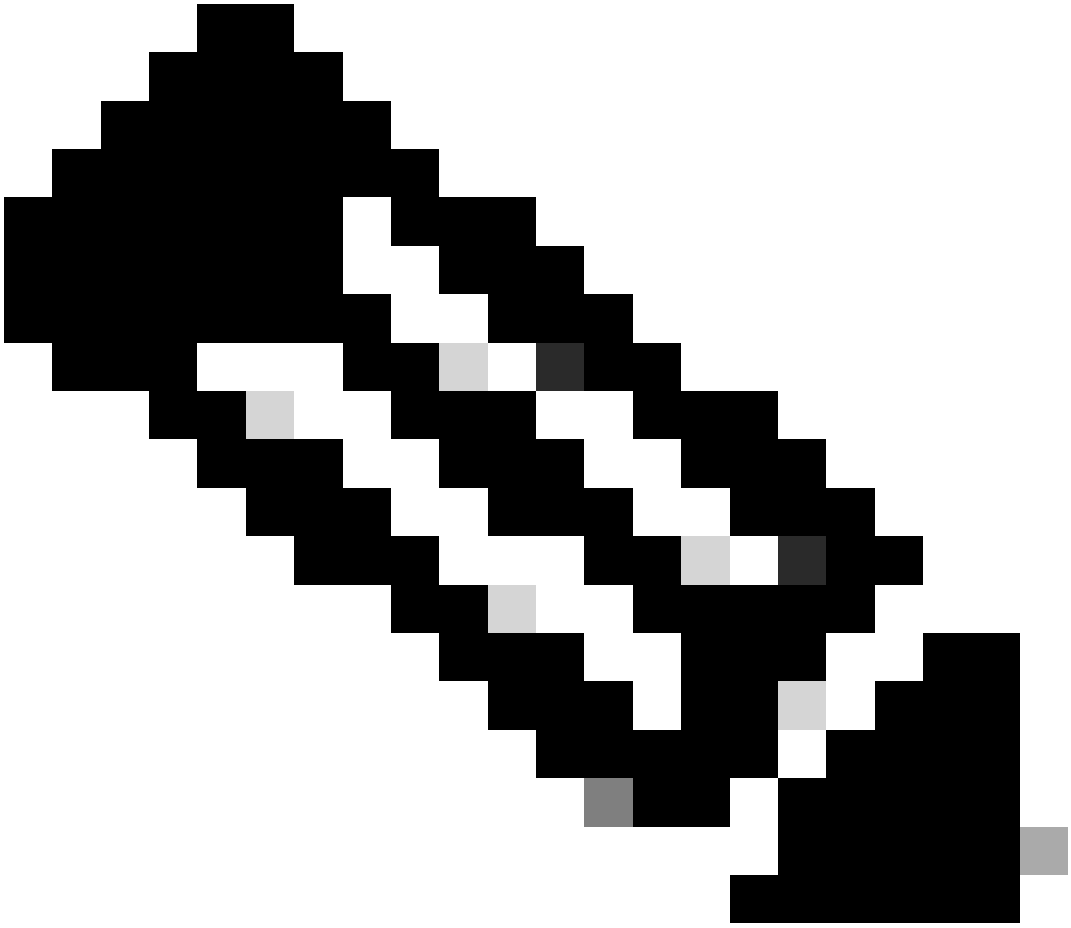
5. 게이트웨이가 재연결 요청을 받으면 비활성 세션 데이터베이스에서 피어 IKE ID(세션 ID 역할을 함)를 검색합니다. 다시 연결하는 동안 비활성 데이터베이스의 저장된 사용자 지정 특성이 검색되어 새 SA에 적용됩니다.



다시 연결

구성

라우터 컨피그레이션



참고: 라우터 컨피그레이션의 경우 Configure FlexVPN Headend for Secure Client (AnyConnect) IKEv2 Remote Access Using Local User Database(로컬 사용자 데이터베이스를 사용하여 보안 클라이언트(AnyConnect) IKEv2 원격 액세스 구성) 문서를 참조할 수도 있습니다

이 컨피그레이션 코드 조각은 Cisco Secure Client IKEv2 Remote Access 컨피그레이션의 예 및 IKEv2 프로필에서 재연결을 구성하여 자동 재연결을 활성화하는 방법을 보여줍니다.

<#root>

```
aaa new-model
!
!
aaa authentication login a-eap-authen-local local
aaa authorization network a-eap-author-grp local
!
username test password 0 cisco
!
ip local pool ACPOOL 192.168.20.5 192.168.20.10
```

```
!
ip access-list standard split_tunnel
10 permit 192.168.10.0 0.0.0.255
!
crypto ikev2 authorization policy ikev2-auth-policy
 pool ACPOOL
 def-domain example.com
 route set access-list split_tunnel
!
crypto ikev2 proposal default
encryption aes-cbc-256
integrity sha512 sha384
group 19 14 21
!
crypto ikev2 policy default
match fvrf any
proposal default
!
!
crypto ikev2 profile AnyConnect-EAP


match identity remote key-id *$AnyConnectClient$*


authentication local rsa-sig
authentication remote anyconnect-eap aggregate
pki trustpoint IKEv2-TP
aaa authentication anyconnect-eap a-eap-authen-local
aaa authorization group anyconnect-eap list a-eap-author-grp ikev2-auth-policy
aaa authorization user anyconnect-eap cached
virtual-template 10
anyconnect profile acvpn
reconnect timeout 900


!
no crypto ikev2 http-url cert
no ip http server
no ip http secure-server
!
crypto vpn anyconnect bootflash:cisco-secure-client-win-5.1.8.105-webdeploy-k9.pkg sequence
crypto vpn anyconnect profile acvpn bootflash:acvpn.xml
!
crypto ipsec transform-set TSET esp-aes 256 esp-sha384-hmac
mode tunnel
!
!
crypto ipsec profile AnyConnect-EAP
set transform-set TSET
set ikev2-profile AnyConnect-EAP
!
interface Virtual-Template10 type tunnel
 ip unnumbered GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile AnyConnect-EAP
```

Cisco 보안 클라이언트 프로파일

<#root>

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSc
    <ClientInitialization>
        <UseStartBeforeLogon UserControllable="true">false</UseStartBeforeLogon>
        <AutomaticCertSelection UserControllable="true">false</AutomaticCertSelection>
        <ShowPreConnectMessage>false</ShowPreConnectMessage>
        <CertificateStore>All</CertificateStore>
        <CertificateStoreOverride>false</CertificateStoreOverride>
        <ProxySettings>Native</ProxySettings>
        <AllowLocalProxyConnections>true</AllowLocalProxyConnections>
        <AuthenticationTimeout>12</AuthenticationTimeout>
        <AutoConnectOnStart UserControllable="true">false</AutoConnectOnStart>
        <MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
        <LocalLanAccess UserControllable="true">false</LocalLanAccess>
        <ClearSmartcardPin UserControllable="true">true</ClearSmartcardPin>
        <IPProtocolSupport>IPv4,IPv6</IPProtocolSupport>




      true




      ReconnectAfterResume




        <AutoUpdate UserControllable="false">true</AutoUpdate>
        <RSASecurIDIntegration UserControllable="false">Automatic</RSASecurIDIntegration>
        <WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
        <WindowsVPNEstablishment>AllowRemoteUsers</WindowsVPNEstablishment>
        <AutomaticVPNPolicy>false</AutomaticVPNPolicy>
        <PPPExclusion UserControllable="false">Disable
            <PPPExclusionServerIP UserControllable="false"></PPPExclusionServerIP>
        </PPPExclusion>
        <EnableScripting UserControllable="false">false</EnableScripting>
        <EnableAutomaticServerSelection UserControllable="false">false
            <AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
```

```
            <AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
        </EnableAutomaticServerSelection>
        <RetainVpnOnLogoff>false
        </RetainVpnOnLogoff>
        <AllowManualHostInput>true</AllowManualHostInput>
    </ClientInitialization>
    <ServerList>
        <HostEntry>
            <HostName>IKEv2_Gateway</HostName>
            <HostAddress>flexvpn-c8kv.example.com</HostAddress>
            <PrimaryProtocol>
```

IPsec

```
                <StandardAuthenticationOnly>true
                    <AuthMethodDuringIKENegotiation>
```

EAP-AnyConnect

```
</AuthMethodDuringIKENegotiation>
                <StandardAuthenticationOnly>
            </PrimaryProtocol>
        </HostEntry>
    </ServerList>
</AnyConnectProfile>
```

IKEv2 재연결 구성에 대한 제한 사항

1. IKEv2(Internet Key Exchange Version 2) 프로필에서 사전 공유 키 권한 부여 방법을 구성할 수 없습니다. Cisco Secure Client 기능의 AutoReconnect 기능에 대한 Cisco IOS IKEv2 지원에서는 사전 공유 키 인증 방법을 사용하며 동일한 IKEv2 프로필에서 사전 공유 키를 구성하면 혼란이 발생할 수 있습니다.
2. 다음 명령은 IKEv2 프로파일에서 구성할 수 없습니다.

- 인증 로컬 사전 공유
- 인증 원격 사전 공유
- keyring, aaa 권한 부여 그룹 psk
- aaa 권한 부여 사용자 psk

다음을 확인합니다.

<#root>

```
sal_c8kv#show crypto session detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation
R - IKE Auto Reconnect

Interface: Virtual-Access1
Profile: AnyConnect-EAP
```

```
Uptime: 00:00:15
Session status: UP-ACTIVE
Peer: 10.106.69.69 port 63516 fvrf: (none) ivrf: (none)
```

Phase1_id: *$AnyConnectClient$*

```
      Desc: (none)
  Session ID: 16
  IKEv2 SA: local 10.106.45.225/4500 remote 10.106.69.69/63516 Active
```

Capabilities:DN

```
 connid:1 lifetime:23:59:45
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 host 192.168.20.5
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 15 drop 0 life (KB/Sec) 4607998/3585
        Outbound: #pkts enc'ed 15 drop 0 life (KB/Sec) 4608000/3585
```

<#root>

```
sal_c8kv#show crypto ikev2 session detailed
 IPv4 Crypto IKEv2 Session

Session-id:16, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         10.106.45.225/4500    10.106.69.69/63516    none/none            READY
      Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:19, Auth sign: RSA, Auth verify:
```

AnyConnect-EAP

```
      Life/Active Time: 86400/620 sec
      CE id: 1016, Session-id: 16
      Status Description: Negotiation done
      Local spi: 67C3394ED1EAADE7        Remote spi: EBFE2587F20EA7C2
      Local id: 10.106.45.225
```

Remote id: *$AnyConnectClient$*

```
      Remote EAP id: user1
      Local req msg id:  0              Remote req msg id:  26
      Local next msg id: 0              Remote next msg id: 26
      Local req queued:  0              Remote req queued:  26
      Local window:      5              Remote window:      1
      DPD configured for 45 seconds, retry 2
      Fragmentation not  configured.
      Extended Authentication not configured.
      NAT-T is detected  outside
      Cisco Trust Security SGT is disabled
      Assigned host addr: 192.168.20.5
      Initiator of SA : No
      PEER TYPE: AnyConnect
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 192.168.20.5/0 - 192.168.20.5/65535
          ESP spi in/out: 0x2E14CBAF/0xD5590D3
          AH spi in/out: 0x0/0x0
```

```
          CPI in/out: 0x0/0x0
          Encr: AES-CBC, keysize: 256, esp_hmac: SHA384
          ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
```

이 출력은 현재 자동 재연결이 가능한 활성 세션이 1개 있음을 보여줍니다.

```
sal_c8kv#show crypto ikev2 stats reconnect
Total incoming reconnect connection: 0
Success reconnect connection: 0
Failed reconnect connection: 0
Reconnect capable active session count: 1
Reconnect capable inactive session count: 0
```

재연결 후

Cisco Secure Client가 다시 연결될 때 IKEV2_MODECFG_SESSION_ID를 IKE ID로 사용합니다. 따라서 다시 연결한 후에는 Phase1_id가 더 이상 $AnyConnectClient$;가 아닙니다. 대신 표시된 대로 세션 ID입니다. 또한 이제 기능이 R로 설정되었습니다. 여기서 R은 재접속 세션임을 나타낸다.

<#root>

```
sal_c8kv#show crypto session detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation
R - IKE Auto Reconnect

Interface: Virtual-Access2
Profile: AnyConnect-EAP
Uptime: 00:00:03
Session status: UP-ACTIVE
Peer: 10.106.69.69 port 54626 fvrf: (none) ivrf: (none)


Phase1_id: 724955484B6363445269557446544154771


      Desc: (none)
  Session ID: 17
  IKEv2 SA: local 10.106.45.225/4500 remote 10.106.69.69/54626 Active


Capabilities:DNR

 connid:1 lifetime:23:59:57
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 host 10.10.10.1
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 22 drop 0 life (KB/Sec) 4608000/3596
        Outbound: #pkts enc'ed 22 drop 0 life (KB/Sec) 4608000/3596
```

다시 연결하면 다음과 같이 인증 방법이 AnyConnect-EAP 대신 PSK(pre-shared key)가 됩니다.

<#root>

```
sal_c8kv#show crypto ikev2 session detail
 IPv4 Crypto IKEv2 Session

Session-id:39, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         10.106.45.225/4500    10.106.69.69/54626    none/none            READY
      Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:19, Auth sign: RSA,
Auth verify: PSK


      Life/Active Time: 86400/202 sec
      CE id: 1017, Session-id: 17
      Status Description: Negotiation done
      Local spi: 33F57D418CFAFEBD Remote spi: F2586DF08F2A8308
      Local id: 10.106.45.225


Remote id: 724955484B6363445269557446544154771


      Local req msg id:  0              Remote req msg id:  8
      Local next msg id: 0              Remote next msg id: 8
      Local req queued:  0              Remote req queued:  8
      Local window:      5              Remote window:      1
      DPD configured for 45 seconds, retry 2
      Fragmentation not  configured.
      Extended Authentication not configured.
      NAT-T is detected  outside
      Cisco Trust Security SGT is disabled
      Assigned host addr: 192.168.20.5
      Initiator of SA : No
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 192.168.20.5/0 - 192.168.20.5/65535
          ESP spi in/out: 0x38ADBE12/0xE3E00C0E
          AH spi in/out: 0x0/0x0
          CPI in/out: 0x0/0x0
          Encr: AES-CBC, keysize: 256, esp_hmac: SHA384
          ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
```

<#root>

```
sal_c8kv#show crypto ikev2 stats reconnect

Total incoming reconnect connection:        1


Success reconnect connection:               1


Failed reconnect connection:                0
Reconnect capable active session count:     1
Reconnect capable inactive session count:   0
IKEv2_Gateway#
```

Cisco Secure Client DART 로그

<#root>

```
Date         : 03/13/2025
Time         : 01:27:35
Type         : Information
Source       : acvpnagent

Description :
```

The IPsec connection to the secure gateway has been established.

```
.
.
Date         : 03/13/2025
Time         : 01:29:05
Type         : Information
Source       : acvpnagent

Description : Current Preference Settings:
ServiceDisable: false
CertificateStoreOverride: false
CertificateStore: All
ShowPreConnectMessage: false
AutoConnectOnStart: false
MinimizeOnConnect: false
LocalLanAccess: false
DisableCaptivePortalDetection: false
```

AutoReconnect: true

AutoReconnectBehavior: ReconnectAfterResume

```
UseStartBeforeLogon: true
AutoUpdate: true
<snip>
IPProtocolSupport: IPv4,IPv6
AllowManualHostInput: true
BlockUntrustedServers: false
PublicProxyServerAddress:
.
.
Date         : 03/13/2025
Time         : 01:29:21
Type         : Information
Source       : acvpnui

Description : Message type information sent to the user:
Connected to IKEv2_Gateway.
.
.
```

!! Now system is put to sleep and resumes back.

Date : 03/13/2025
Time : 03:08:44
Type : Information
Source : acvpnagent

Description : ..

Client Agent continuing from system suspend.

Date : 03/13/2025
Time : 03:08:44
Type : Warning
Source : acvpnagent

Description : Session level reconnect reason code 9:

System resume from suspend mode (Sleep, Stand-by, Hibernate, etc).

Originates from session level

Date : 03/13/2025
Time : 03:08:44
Type : Information
Source : acvpnui

Description : Message type information sent to the user:
Reconnecting to IKEv2_Gateway...
.
.
Date : 03/13/2025
Time : 03:10:34
Type : Information
Source : acvpnagent

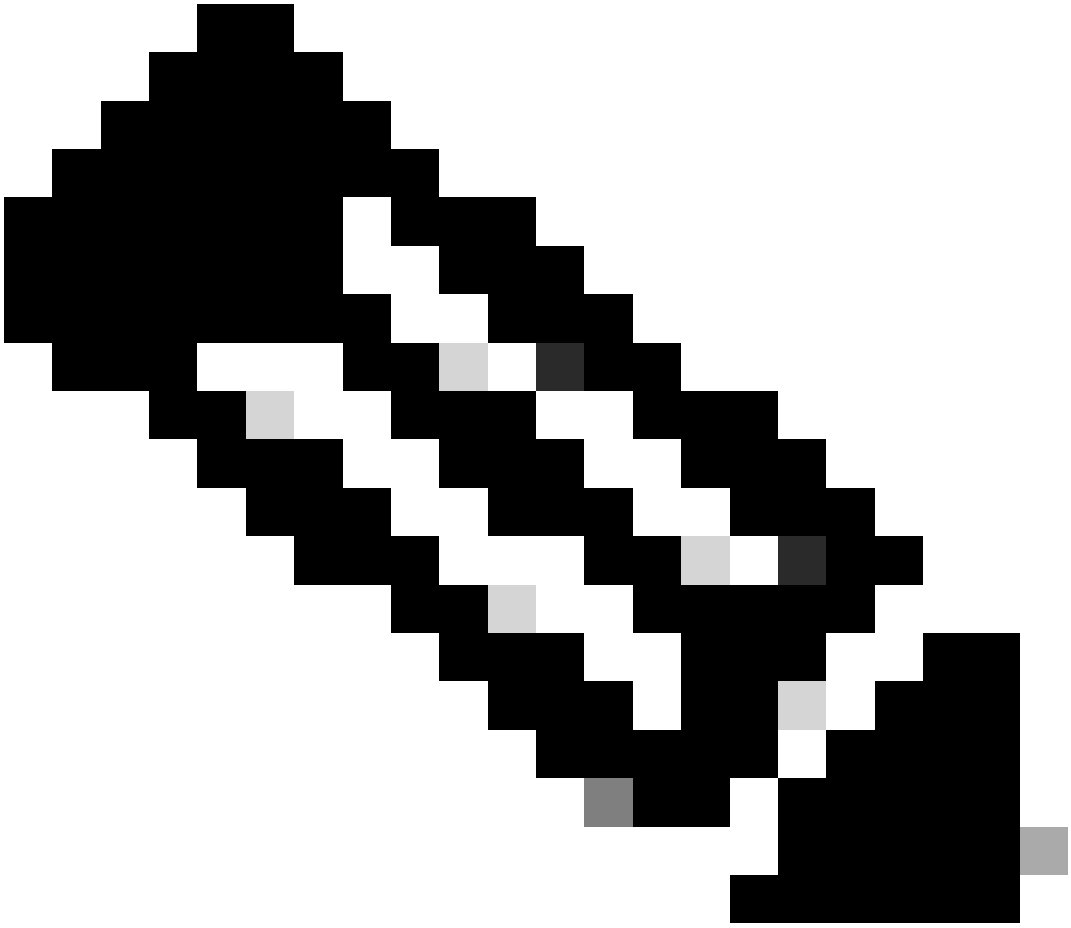
Description : Function: CIPsecProtocol::initiateTunnel
File: IPsecProtocol.cpp
Line: 613

Using IKE ID 'rIUHKccDRiUtFTATwq' for reconnect

.
.
Date : 03/13/2025
Time : 03:11:44
Type : Information
Source : acvpnui

Description : Message type information sent to the user:

Connected to IKEv2_Gateway.



참고: DART 로그에서 IKE ID는 '724955484B6363445269557446544154771'의 ASCII 표현인 'rIUHKccDRiUtFTATwq'로 표시되며, "show crypto session detail" 출력에 Remote ID로 표시됩니다.

문제 해결

이 섹션에서는 설정 문제 해결을 위해 사용할 수 있는 정보를 제공합니다.

IKEv2는 게이트웨이와 클라이언트 간의 협상을 확인하기 위해 디버깅합니다.

```
Debug crypto condition peer ipv4
```

```
Debug crypto ikev2
Debug crypto ikev2 packet
Debug crypto ikev2 internal
```

```
Debug crypto ikev2 error
```

관련 정보

- 보안 및 VPN 컨피그레이션 가이드, Cisco IOS XE 17.x
- 기술 지원 및 문서 – Cisco Systems

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.