IKEv2およびAnyConnect再接続機能について

内容

はじめに

このドキュメントでは、AnyConnectのCisco IOS®ルータおよびCisco IOS® XEルータでIKEv2自動再接続機能がどのように動作するかについて説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- インターネット キー交換バージョン 2（IKEv2）
- Cisco Secure Client(CSC)

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- バージョン17.16.01aを実行するCisco Catalyst 8000V(C8000V)
- Cisco Secure Clientバージョン5.1.8.105
- Cisco Secure Clientがインストールされたクライアント PC

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

IKEv2およびCisco Secure Clientの再接続機能

Cisco Secure Clientの自動再接続機能を使用すると、セッションを一定時間記憶しておき、セキュアチャネルを確立した後に接続を再開できます。Cisco Secure ClientはInternet Key Exchange Version 2(IKEv2)で広く使用されているため、IKEv2はCisco IOSソフトウェアでの自動再接続機能のサポートを、Cisco IOS IKEv2のセキュアクライアント機能の自動再接続機能のサポートを通じて拡張します。

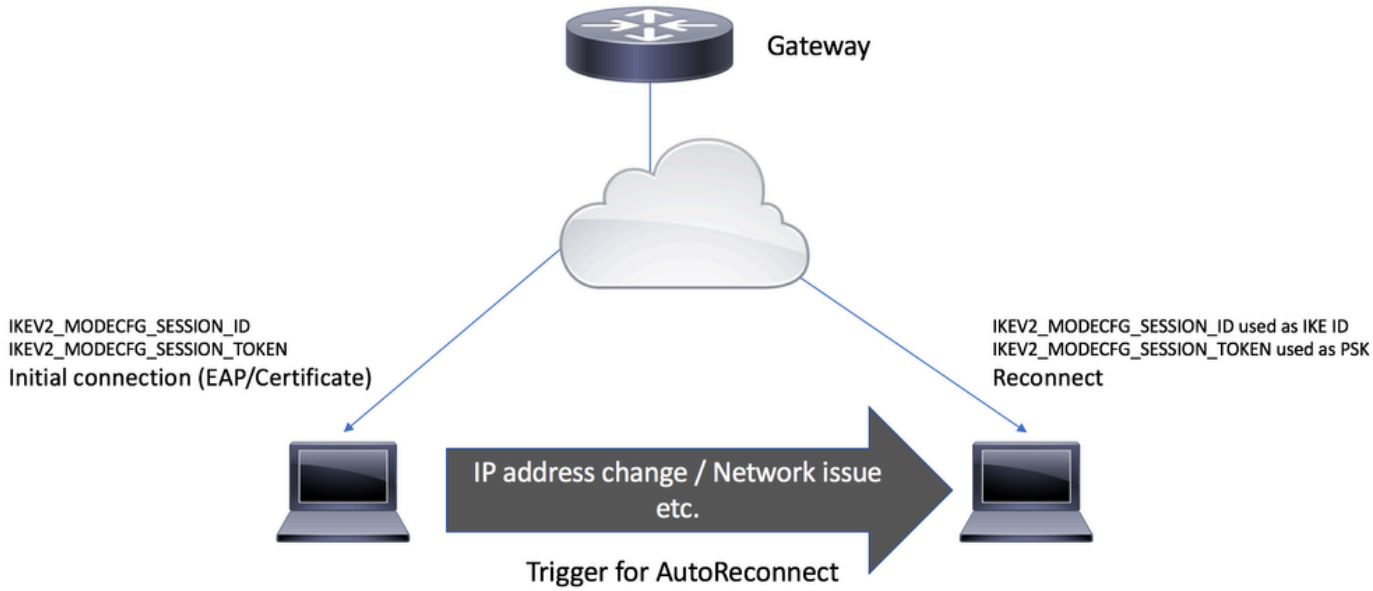
Cisco Secure Clientでの自動再接続は、次のシナリオで実行されます。

1. 中間ネットワークがダウンしています。Cisco Secure Clientは、アップ状態のときにセッションの再開を試みます。
2. Cisco Secure Clientデバイスは、ネットワーク間を切り替えます。この結果、送信元ポートが変更され、既存のセキュリティアソシエーション(SA)がダウンします。そのため、Cisco Secure Clientは自動再接続機能を使用してSAを再開しようとします。
3. Cisco Secure Clientデバイスは、スリープモードまたは休止モードから復帰した後、SAの再開を試みます。

自動再接続機能の利点

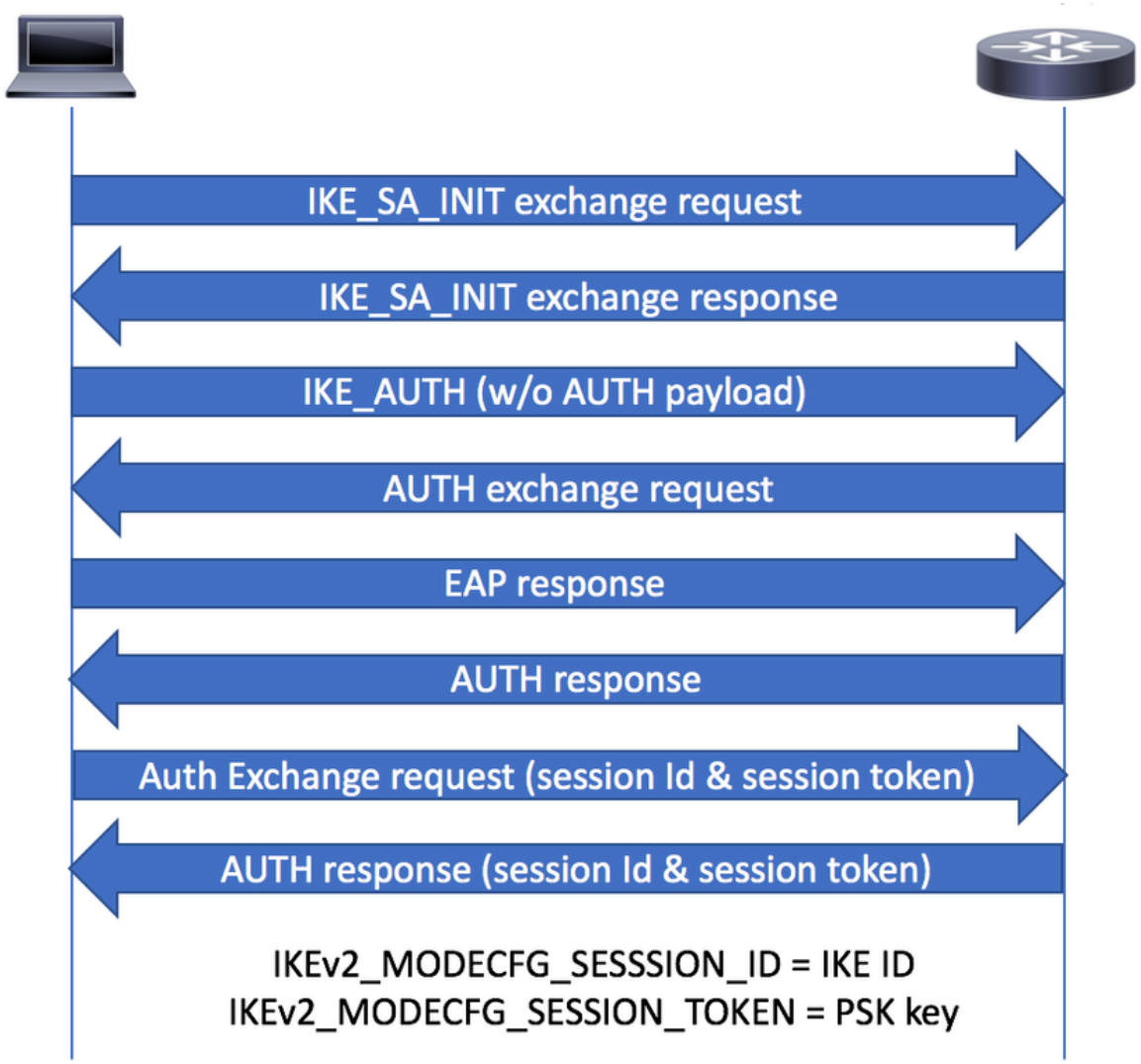
- 元のセッションで使用されていた設定属性は、認証、認可、アカウンティング(AAA)サーバに問い合わせることなく再利用されます。
- IKEv2ゲートウェイは、クライアントに再接続するためにRADIUSサーバに接続する必要はありません。
- セッションの再開時には、認証または許可のためのユーザ操作は必要ありません。
- 認証方式は、セッション再接続時の事前共有キーです。この認証方式は、他の認証方式に比べて高速です。
- 事前共有キー認証方式は、最小限のリソースでCisco IOSソフトウェアのセッションを再開するのに役立ちます。
- 未使用のセキュリティアソシエーション(SA)が削除され、暗号化リソースが解放されます。

自動再接続の接続フロー

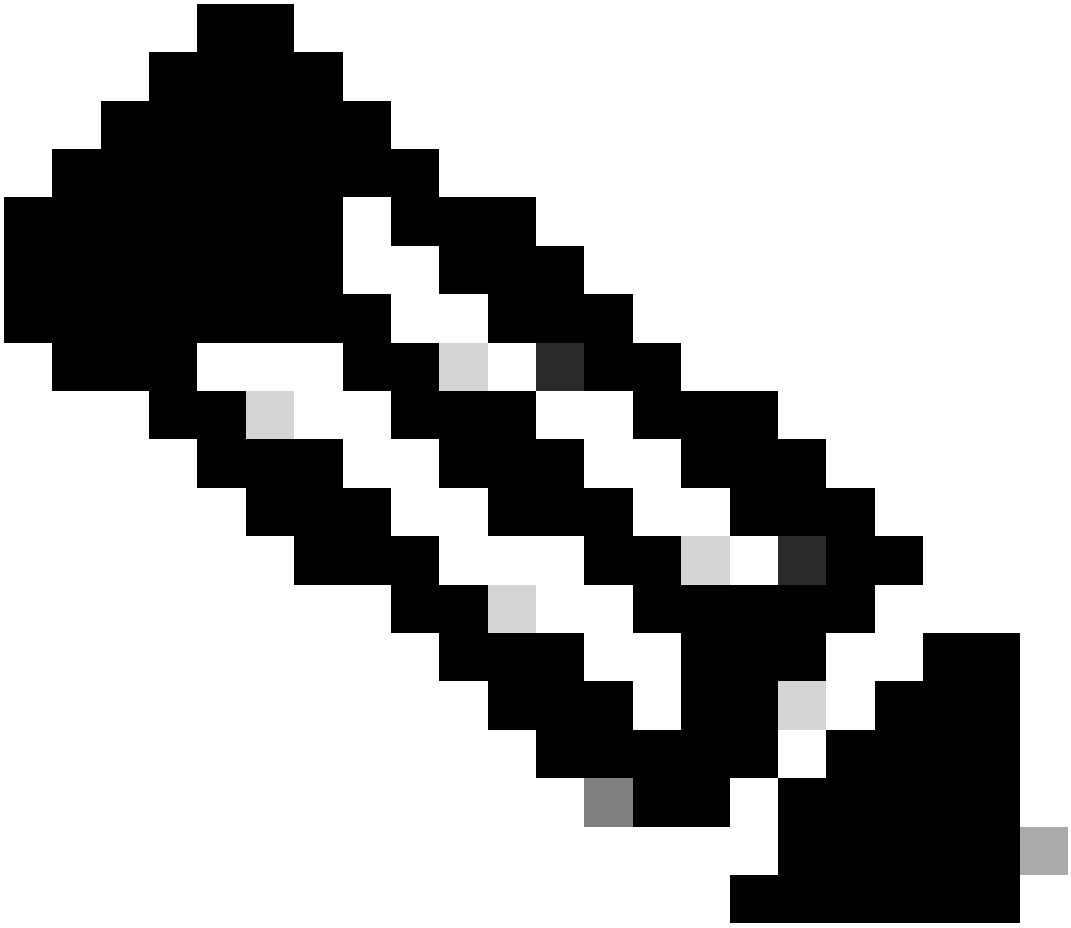


自動再接続のトリガー

1. AUTH交換中、Cisco Secure ClientはIKE_AUTH要求のMODECFG_REQペイロードに含まれるIKEv2ゲートウェイからのSession-token属性とSession-id属性を要求します。
2. IKEv2ゲートウェイは、Cisco IOS IKEv2でreconnectコマンドを使用してセキュアクライアントの自動再接続機能のサポートがIKEv2プロファイルで有効になっているかどうかを確認し、選択されたIKEv2プロファイルのIKEv2ポリシーを選択し、セッションIDおよびセッショントークン属性をIKE_AUTH応答のCFGMODE_REPLYペイロードでセキュアクライアントに送信します。

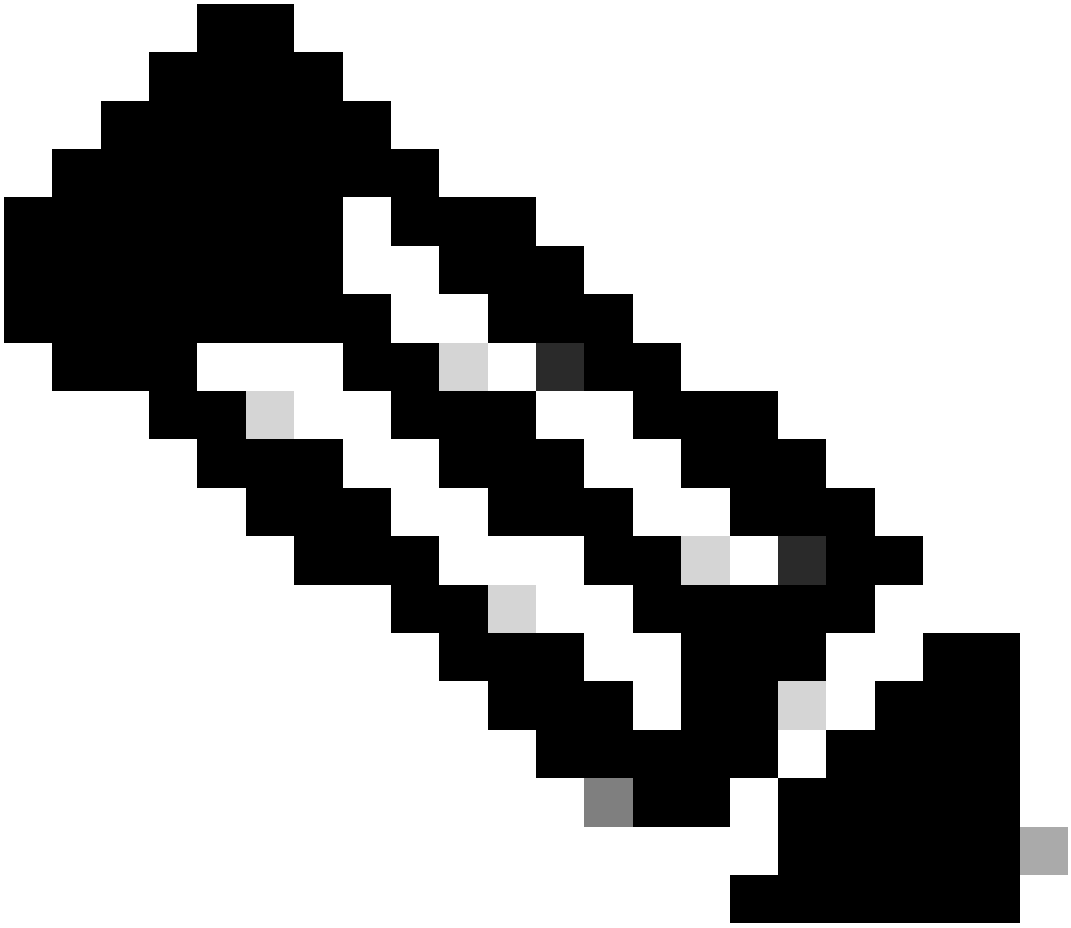

IKE_SA_INIT exchange request
IKE_SA_INIT exchange response
IKE_AUTH (w/o AUTH payload)
AUTH exchange request
EAP response
AUTH response
Auth Exchange request (session Id & session token)
AUTH response (session Id & session token)
IKEv2_MODECFG_SESSSION_ID = IKE ID
IKEv2_MODECFG_SESSION_TOKEN = PSK key

CFGMODE交换

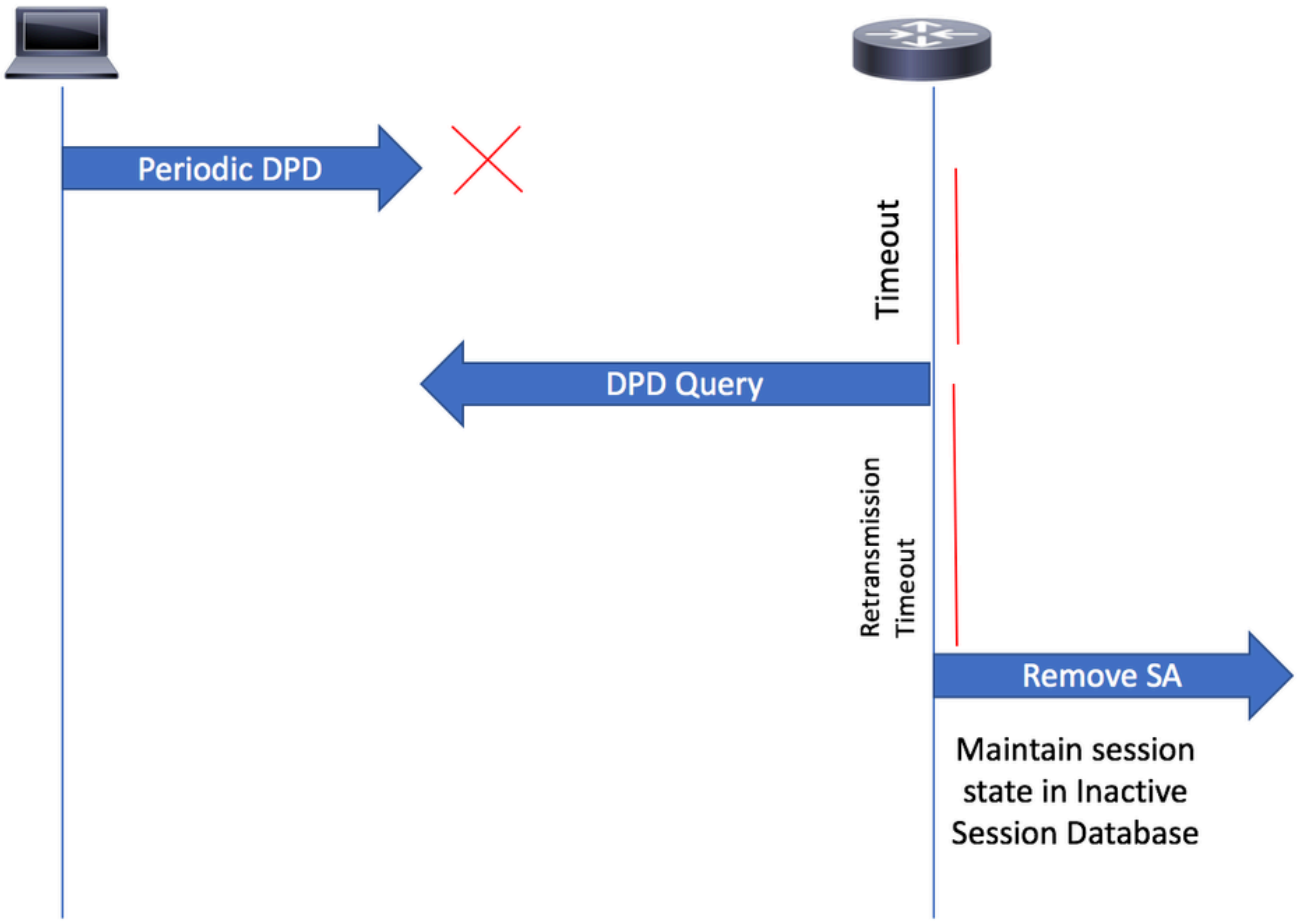


注：応答しないクライアントを特定するプロセスは、Dead Peer Detection(DPD)に基づいています。 IKEv2プロファイルで再接続機能が有効になっている場合は、DPDはオンデマンドでIKEv2にキューイングされるため、DPDを設定する必要はありません

3. Cisco Secure Clientは定期的にDPDメッセージをゲートウェイに送信します。DPDがオンデマンドでキューに入れられる場合、ゲートウェイはクライアントからDPDを受信するまで、DPDメッセージをクライアントに送信しません。（設定されたDPD間隔に従って）指定された期間内にセキュアクライアントからDPDが受信されない場合、ゲートウェイはDPDメッセージを送信します。セキュアクライアントから応答を受信しない場合、SAはアクティブセッションデータベースから削除されます。



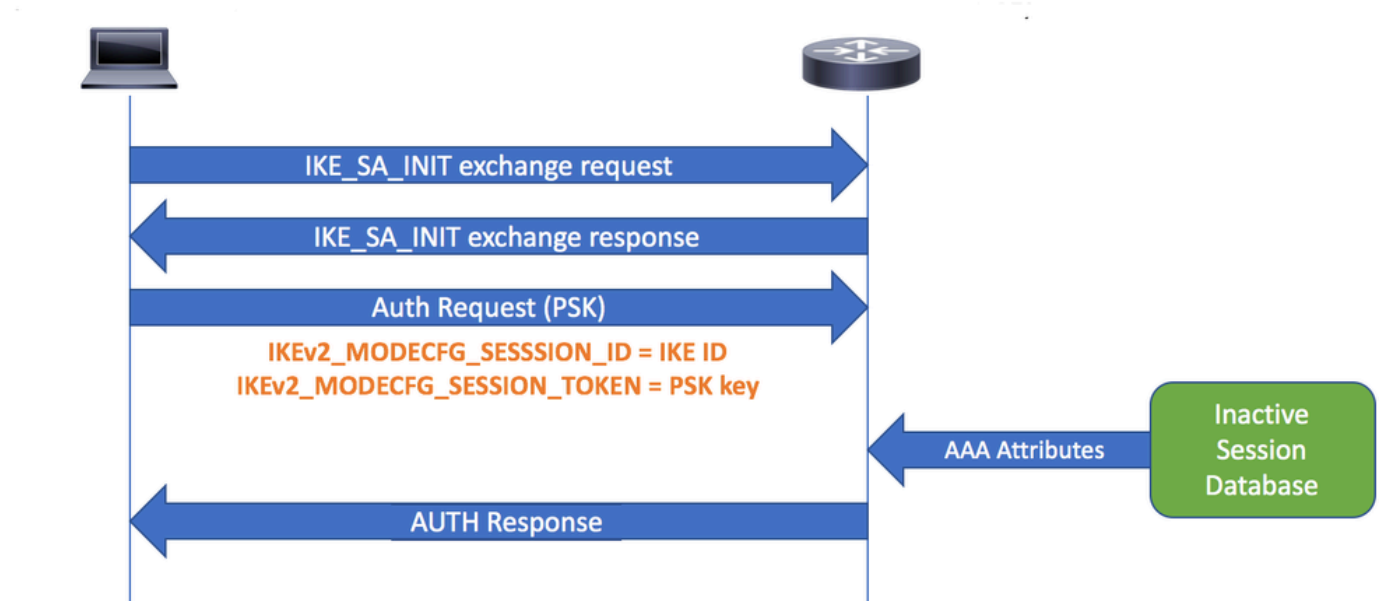
注：ゲートウェイは、設定済みの再接続タイムアウト期間に従って再接続できるように、引き続きセッション状態（AAA属性など）を個別の非アクティブセッションデータベースで維持します。



DPDクエリ

4. クライアントは再接続を試行すると、新しいIKE SAを作成し、MODECFG_REPLYペイロードから受信したIKE ID(ID)をセッションIDとして使用します。この時点で、Cisco Secure Clientは再接続にIKE PSK認証を使用します。事前共有キー(PSK)は、以前に受信したセッショントークンです。

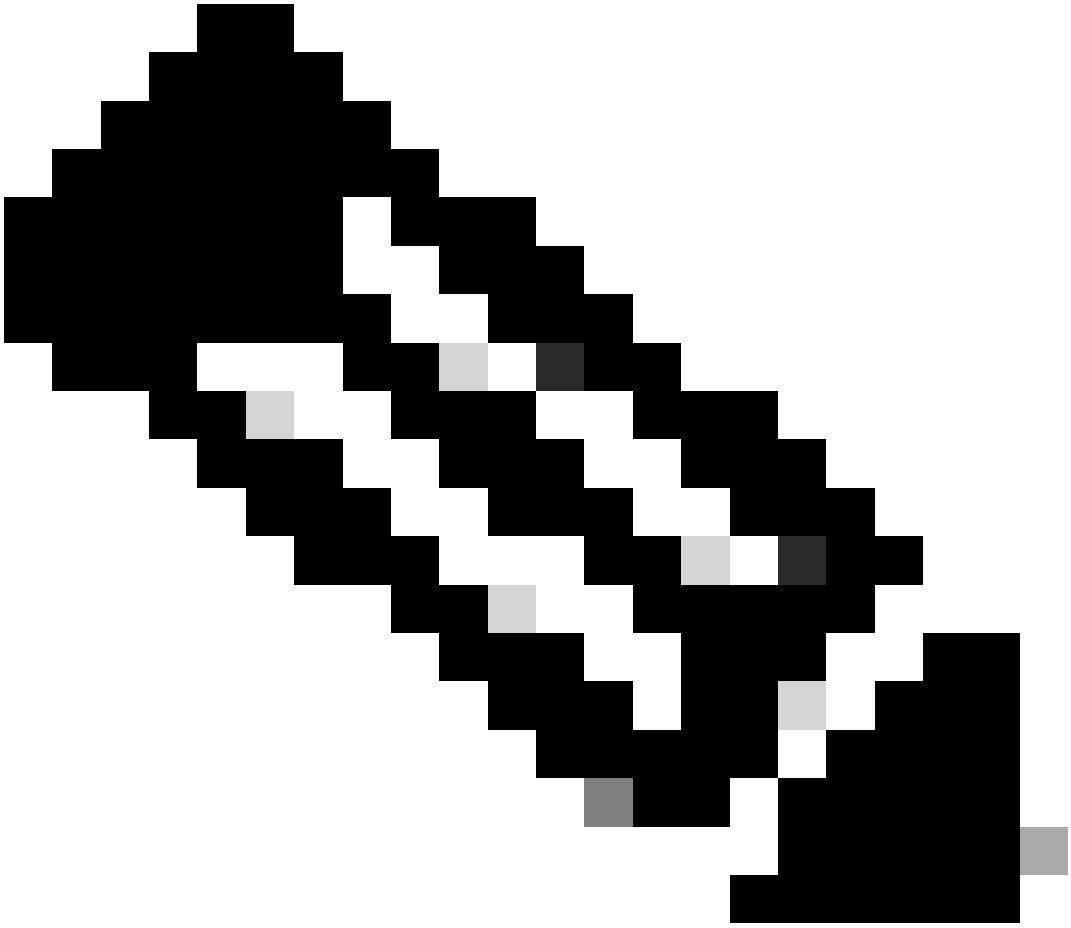
5. ゲートウェイは、再接続要求を受信すると、非アクティブセッションデータベースでピアのIKE ID（セッションIDとして機能）を検索します。 再接続中に、非アクティブデータベースから保存されたカスタム属性が取得され、新しいSAに適用されます。



再接続

設定

ルータの設定



注：ルータの設定については、ドキュメント『ローカルユーザデータベースを使用したセキュアクライアント(AnyConnect)IKEv2リモートアクセスのためのFlexVPNヘッドエンドの設定』も参照してください。

次の設定スニペットは、Cisco Secure Client IKEv2 Remote Access設定の例と、IKEv2プロファイルでreconnectを設定することによってAutoReconnectを有効にする方法を示しています。

<#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 Secure Clientプロファイル

<#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再接続の設定に関する制限事項

1. 事前共有キーの許可方法は、インターネットキーエクスチェンジバージョン2 (IKEv2)プロファイルでは構成できません。これは、Cisco Secure Client機能の自動再接続機能に対するCisco IOS IKEv2のサポートでは事前共有キー認証方式が使用されており、同じIKEv2プロファイルに事前共有キーを設定すると混乱が生じる可能性があるためです。
2. 次のコマンドは、IKEv2プロファイルでは設定できません。

- 認証ローカル事前共有
- 認証リモート事前共有
- キーリング、aaa authorization group psk
- aaa許可ユーザpsk

確認

<#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
```

次の出力は、現在、自動再接続が可能なアクティブなセッションが1つあることを示しています。

```
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
```

再接続後

Cisco Secure Clientが再接続すると、IKE IDとしてIKEV2_MODECFG_SESSION_IDが使用されます。したがって、再接続後、Phase1_idは$AnyConnectClient$ではなくなり、代わりに次に示すようにセッションIDになります。また、これらの機能にRが設定されていることに注意してください。ここで、Rは、これが再接続セッションであることを示します。

<#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
```

再接続後、認証方式は次のようにAnyConnect-EAPではなくPSK（事前共有キー）になります。

<#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ログ

<#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

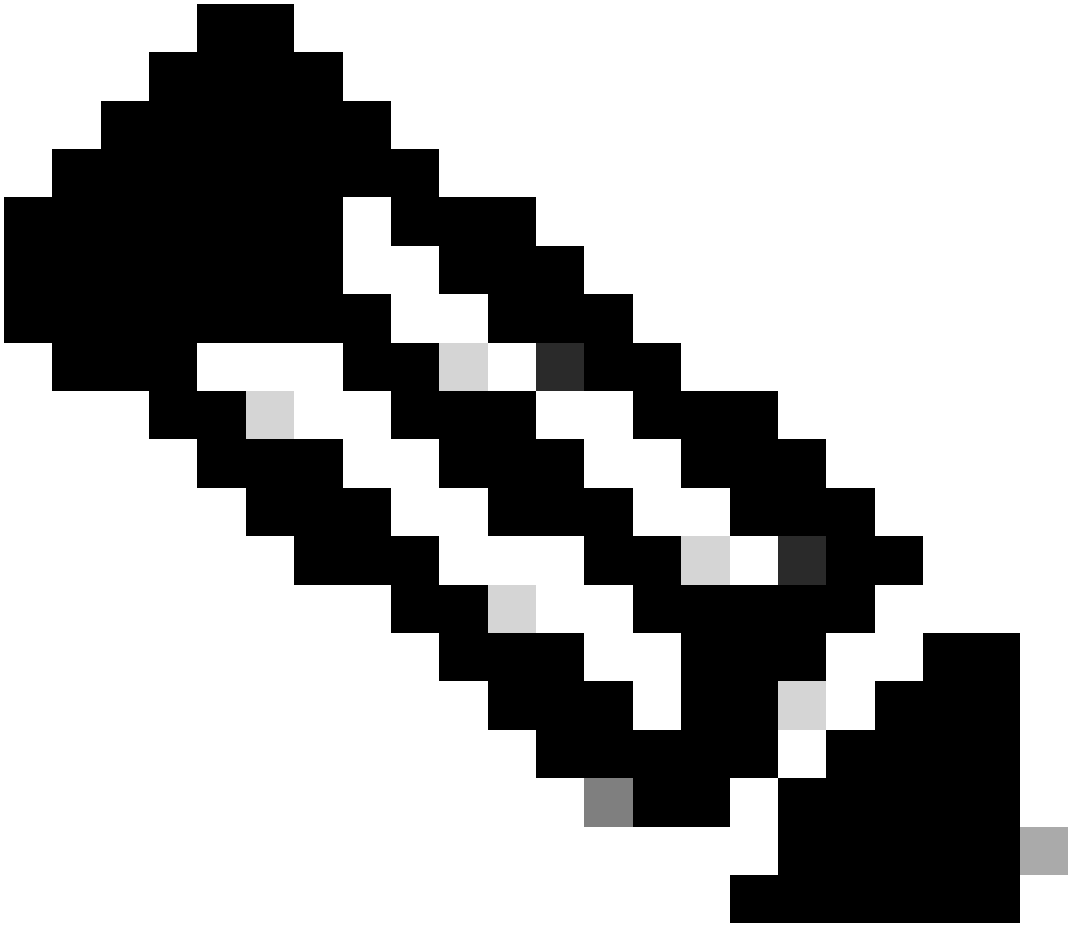
Description : Function: CIPsecProtocol::initiateTunnel
File: IPsecProtocol.cpp
Line: 613

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.



注:DARTログでは、IKE IDは「rIUHKccDRiUtFTATwq」として表示されます。これは、「724955484B6363445269557446544154771」のASCII表現であり、「show crypto session detail」の出力でリモートIDとして表示されます。

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

ゲートウェイとクライアント間のネゴシエーションを確認するためのIKEv2デバッグ。

```
Debug crypto condition peer ipv4


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

```
Debug crypto ikev2 error
```

関連情報

- セキュリティおよびVPNコンフィギュレーションガイド、Cisco IOS XE 17.x
- テクニカル サポートとドキュメント - Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。