ローカル認証を使用したC8000vでのAnyConnect SSL VPNの設定

内容

はじめに

このドキュメントでは、ローカルユーザデータベースを使用してAnyConnect SSL VPN向けにCisco IOS XEヘッドエンドC8000vを設定する方法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推奨されます。

- Cisco IOS XE
- Cisco Secure Client(CSC)
- 一般的なSSLの動作
- 公開キー インフラストラクチャ（PKI）

使用するコンポーネント

番目e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。

背景説明

Cisco IOS XE Secure Socket Layer(SSL)VPNは、ルータベースのソリューションであり、データ、音声、およびワイヤレスプラットフォームを統合し、業界をリードするセキュリティおよびルーティング機能と統合されたSSL VPNリモートアクセス接続を提供します。Cisco IOS XE SSL VPNを使用すると、エンドユーザは、自宅や、ワイヤレスホットスポットなどのインターネット対応の場所から安全にアクセスできます。 また、Cisco IOS XE SSL VPNを使用することで、企業はオフショアのパートナーやコンサルタントに企業ネットワークアクセスを拡張し、企業データを常に保護することができます。

この機能は、次のプラットフォームでサポートされています。

Platform	サポートされるCisco IOS XEリリース
シスコ クラウド サービス ルータ 1000V シリーズ	Cisco IOS XE Release 16.9
Cisco Catalyst 8000V	Cisco IOS XEバンガロール17.4.1
Cisco 4461 サービス統合型ルータ Cisco 4451 サービス統合型ルータ Cisco 4431 サービス統合型ルータ	Cisco IOS XEカッパーチーノ17.7.1a

設定

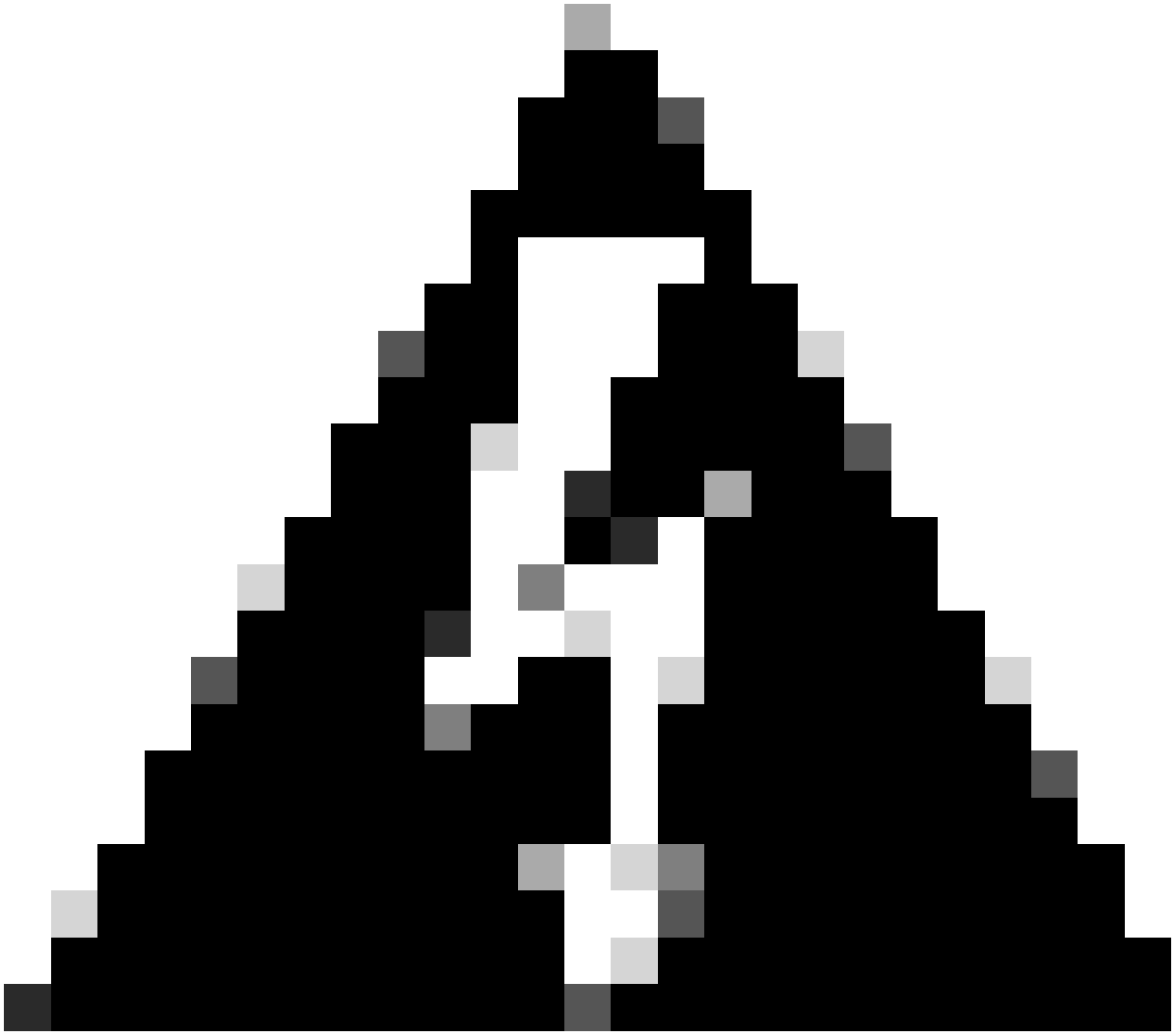
ネットワーク図

基本的なネットワーク図

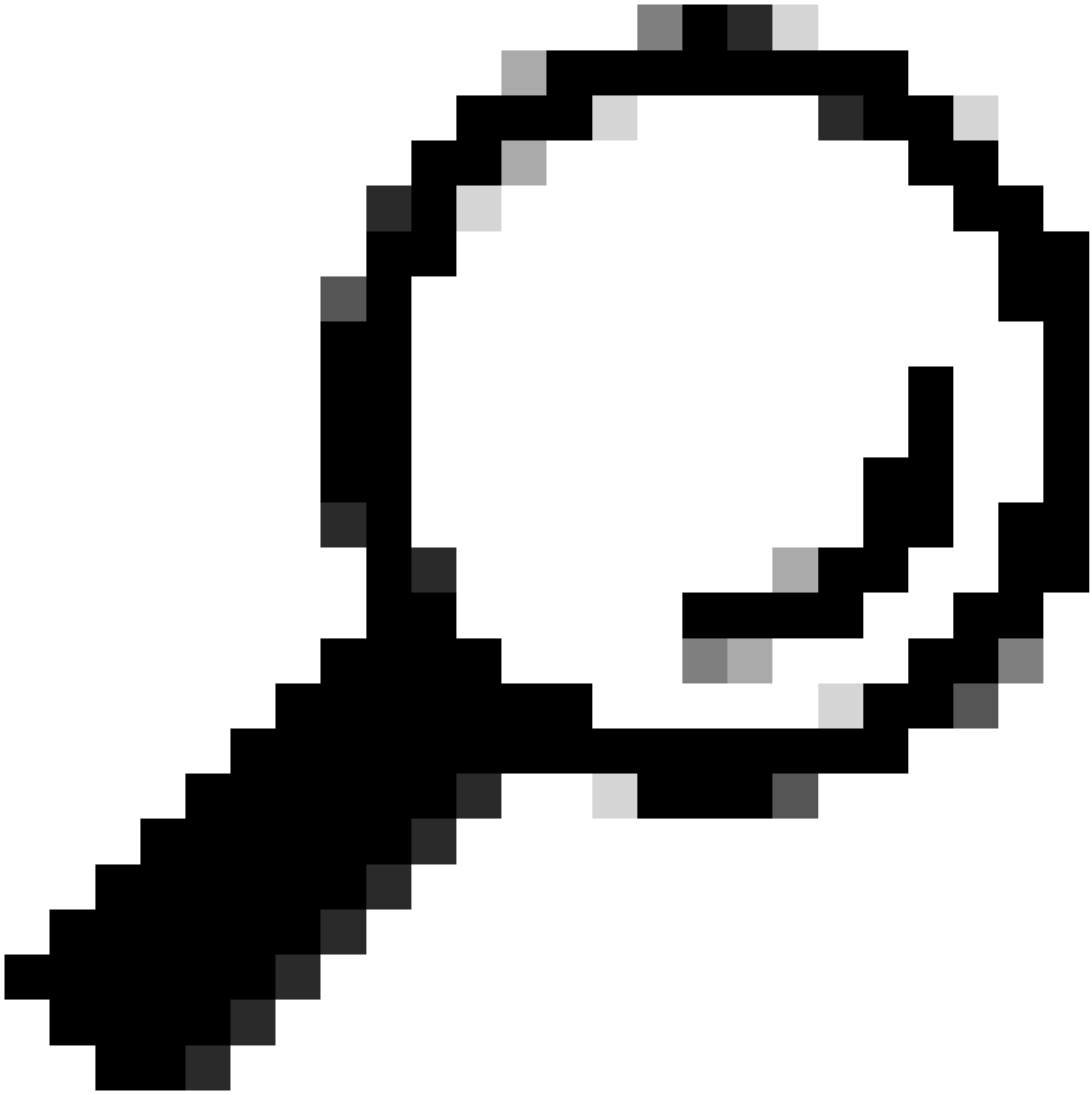
コンフィギュレーション

1. AAAを有効にし、認証リストと許可リストを設定し、ローカルデータベースにユーザ名を追加します。

```
aaa new-model
!
aaa authentication login SSLVPN_AUTHEN local
aaa authorization network SSLVPN_AUTHOR local
!
username test password cisco123
```



警告：aaa new-model コマンドにより、ローカル認証がすべての回線およびインターフェイス (コンソール回線 line con 0 を除く) にただちに適用されます。 このコマンドが有効になった後にルータへの Telnet セッションを開く場合 (または接続がタイムアウトになって再接続する必要がある場合)、ユーザーは、ルータのローカルデータベースで認証される必要があります。AAA設定を開始する前にルータにユーザ名とパスワードを定義しておくことを推奨します。これにより、ルータからロックアウトされることはありません。



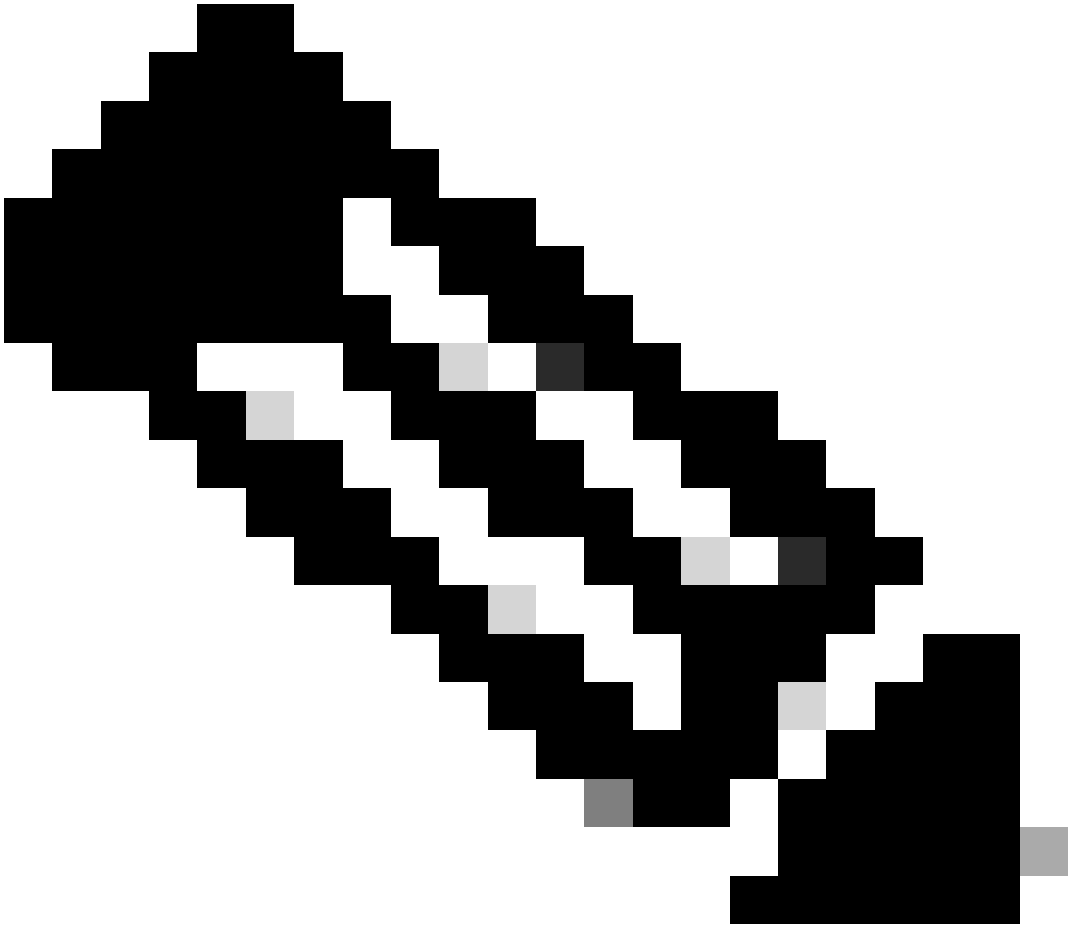
ヒント: AAAコマンドを設定する前に、設定を保存してください。AAAの設定が完了して（正しく動作することを確認した後）、設定を再度保存できます。 これにより、ルータのリロードによって変更をロールバックすることが可能になり、予期しないロックアウトから回復できます。

2.Rivest-Shamir-Adleman(RSA)キーペアを生成します。

```
crypto key generate rsa label AnyConnect modulus 2048 exportable
```

3. トラストポイントを作成して、ルータのID証明書をインストールします。証明書の作成の詳細については、『PKIの証明書登録を設定する方法』を参照してください。

```
crypto pki trustpoint TP_AnyConnect
enrollment terminal
fqdn sslvpn-c8kv.example.com
subject-name cn=sslvpn-c8kv.example.com
subject-alt-name sslvpn-c8kv.example.com
revocation-check none
rsakeypair AnyConnect
```



注：サブジェクト名の共通名(CN)は、ユーザがセキュアゲートウェイ(C8000V)に接続するために使用するIPアドレスまたは完全修飾ドメイン名(FQDN)で設定する必要があります。 必須ではありませんが、CNを正しく入力すると、ログイン時にユーザが遭遇する証明書エラーの数を減らすことができます。

---

4. Cisco Secure Clientにアドレスを割り当てるIPローカルプールを定義します。

```
ip local pool SSLVPN_POOL 192.168.13.1 192.168.13.10
```

5.（オプション）スプリットトンネルに使用する標準アクセスリストを設定します。このアクセスリストは、VPNトンネルを介してアクセス可能な宛先ネットワークで構成されます。デフォルトでは、スプリットトンネルが設定されていない場合、すべてのトラフィックはVPNトンネル（フルトンネル）を通過します。

```
ip access-list standard split-tunnel-acl
10 permit 192.168.11.0 0.0.0.255
20 permit 192.168.12.0 0.0.0.255
```

6.HTTPセキュアサーバを無効にします。

```
no ip http secure-server
```

7. SSLプロポーザルを設定します。

```
crypto ssl proposal ssl_proposal
protection rsa-aes128-sha1 rsa-aes256-sha1
```

8. SSLポリシーを設定し、SSLプロポーザルとPKIトラストポイントを呼び出します。

```
crypto ssl policy ssl_policy
ssl proposal ssl_proposal
pki trustpoint TP_AnyConnect sign
ip interface GigabitEthernet1 port 443
```

SSLポリシーは、SSLネゴシエーション中に使用されるプロポーザルとトラストポイントを定義

します。これは、SSLネゴシエーションに関係するすべてのパラメータのコンテナとして機能します。ポリシーの選択は、ポリシーの下で設定されたパラメータとセッションパラメータを照合することによって行われます。

9.（オプション）Cisco Secure Client Profile Editor Cisco Secure Client Profile Editorを使用して、AnyConnectプロファイルを作成します。プロファイルに相当するXMLのスニペットが参照用に提供されます。

<#root>

true

true

false

All

All

All

false

Native

```
true
```

```
30
```

```
false
```

```
true
```

```
false
```

false

true

IPv4,IPv6

true

ReconnectAfterResume

false

true

Automatic

SingleLocalLogon

SingleLocalLogon

AllowRemoteUsers

LocalUsersOnly

false

Disable

```
false
```

```
false
```

```
 20
```

```
 4
```

```
false
```

```
false
```

```
true
```

SSL_C8KV

sslvpn-c8kv.example.com

10. 作成したXMLプロファイルをルータのフラッシュメモリにアップロードし、プロファイルを定義します。

```
crypto vpn anyconnect profile acvpn bootflash:/acvpn.xml
```

11.HTTPセキュアサーバを無効にします。

```
no ip http secure-server
```

12. SSL認可ポリシーを設定します。

```
crypto ssl authorization policy ssl_author_policy
client profile acvpn
pool SSLVPN_POOL
dns 192.168.11.100
banner Welcome to C8kv SSLVPN
def-domain example.com
route set access-list split-tunnel-acl
```

SSL認可ポリシーは、リモートクライアントにプッシュされる認可パラメータのコンテナです。認可ポリシーはSSLプロファイルから参照されます。

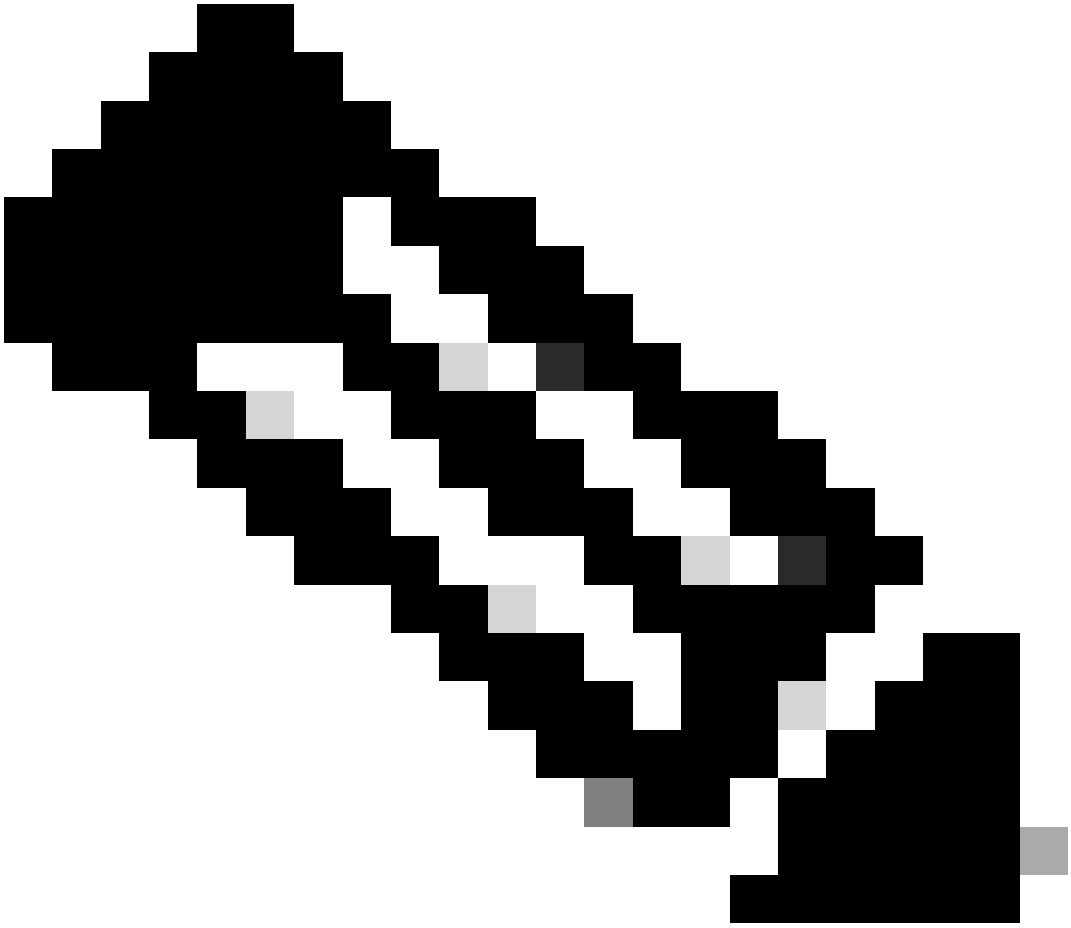
13. 仮想アクセスインターフェイスのクローニング元の仮想テンプレートを設定します。

```
interface Virtual-Template2 type vpn
ip unnumbered GigabitEthernet1
ip mtu 1400
ip tcp adjust-mss 1300
```

14. SSLプロファイルを設定し、 認証、アカウンティングリスト、および仮想テンプレートを定義します。

```
crypto ssl profile ssl_prof
match policy ssl_policy
match url https://sslvpn-c8kv.example.com
aaa authentication user-pass list SSLVPN_AUTHEN
aaa authorization group user-pass list SSLVPN_AUTHOR ssl_author_policy
authentication remote user-pass
virtual-template 2
```

プロファイルの選択は、ポリシーとURLの値によって異なります。



注：ポリシーとURLはSSL VPNプロファイルで一意である必要があり、セッションを開始するには少なくとも1つの認可方式を指定する必要があります。

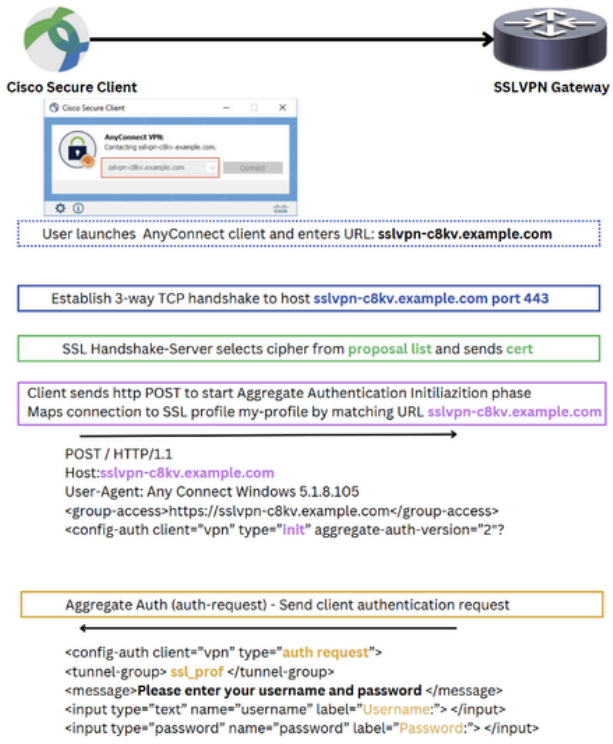
SSLプロファイルでは次のものが使用されます。

- match policy:matchステートメントで、SSLポリシー名ssl_policyでクライアントのSSLプロファイルssl_profを選択します。
- match url：ステートメントを照合して、URL sslvpn-c8kv.example.com上のクライアントのSSLプロファイルssl_profを選択します。
- aaa authentication user-pass list：認証時にSSLVPN_AUTHENリストが使用されます。
- aaa authorization group user-pass list：認可中、ネットワークリストSSLVPN_AUTHORが認可ポリシーssl_author_policyとともに使用されます。
- authentication remote user-pass：リモートクライアントの認証モードをユーザ名/パスワードベースとして定義します。
- virtual-template 2：クローニングするバーチャルテンプレートを定義します。

接続フロー

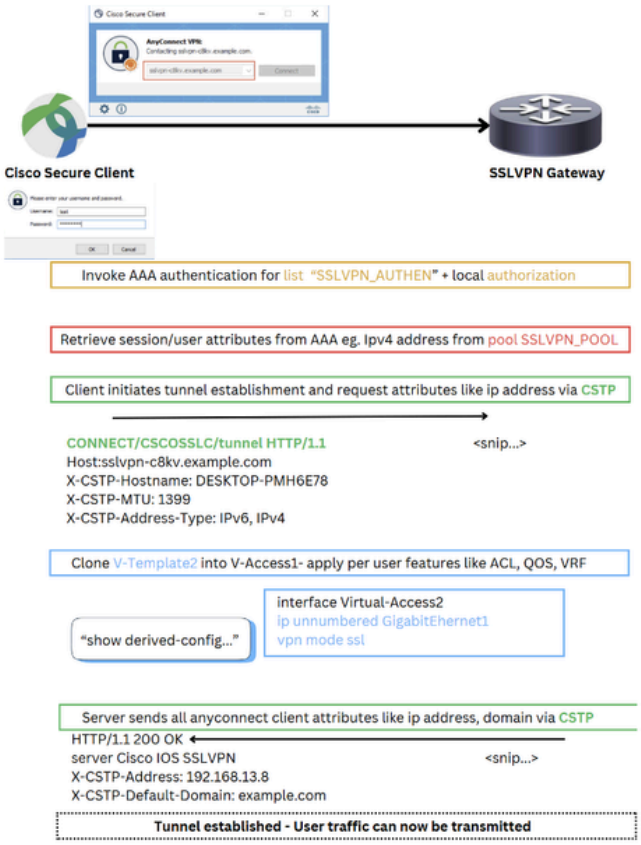
SSL VPN接続の確立中にCisco Secure ClientとSecure Gatewayの間で発生するイベントを理解するには、ドキュメント『AnyConnect SSL VPN接続フローについて』を参照してください。

Cisco Secure Client(AnyConnect)からC8000vへの高レベル接続フロー




```
aaa authentication login SSLVPN_AUTHEN local
aaa authorization network SSLVPN_AUTHOR local
crypto ssl proposal ssl_proposal
protection rsa-aes256-sha1 rsa-aes128-sha1
!
crypto ssl policy ssl_policy
ssl proposal ssl_proposal
pki trustpoint TP_AnyConnect sign
ip interface GigabitEthernet1 port 443
!
crypto ssl profile my-profile
match policy ssl_policy
match url https://sslvpn-c8kv.example.com
aaa authentication user-pass list SSLVPN_AUTHEN
aaa authorization group user-pass list SSLVPN_AUTHOR ssl_author_policy
authentication remote user-pass
virtual-template 2
!
crypto ssl authorization policy ssl_author_policy
pool SSLVPN_POOL
def domain example.com
!
ip local pool SSLVPN_POOL 192.168.13.1 192.168.13.10
interface Virtual-Template2 type vpn
  ip unnumbered GigabitEthernet1
  ip mtu 1400
  vpn mode ssl
```

ハイレベル接続フロー1

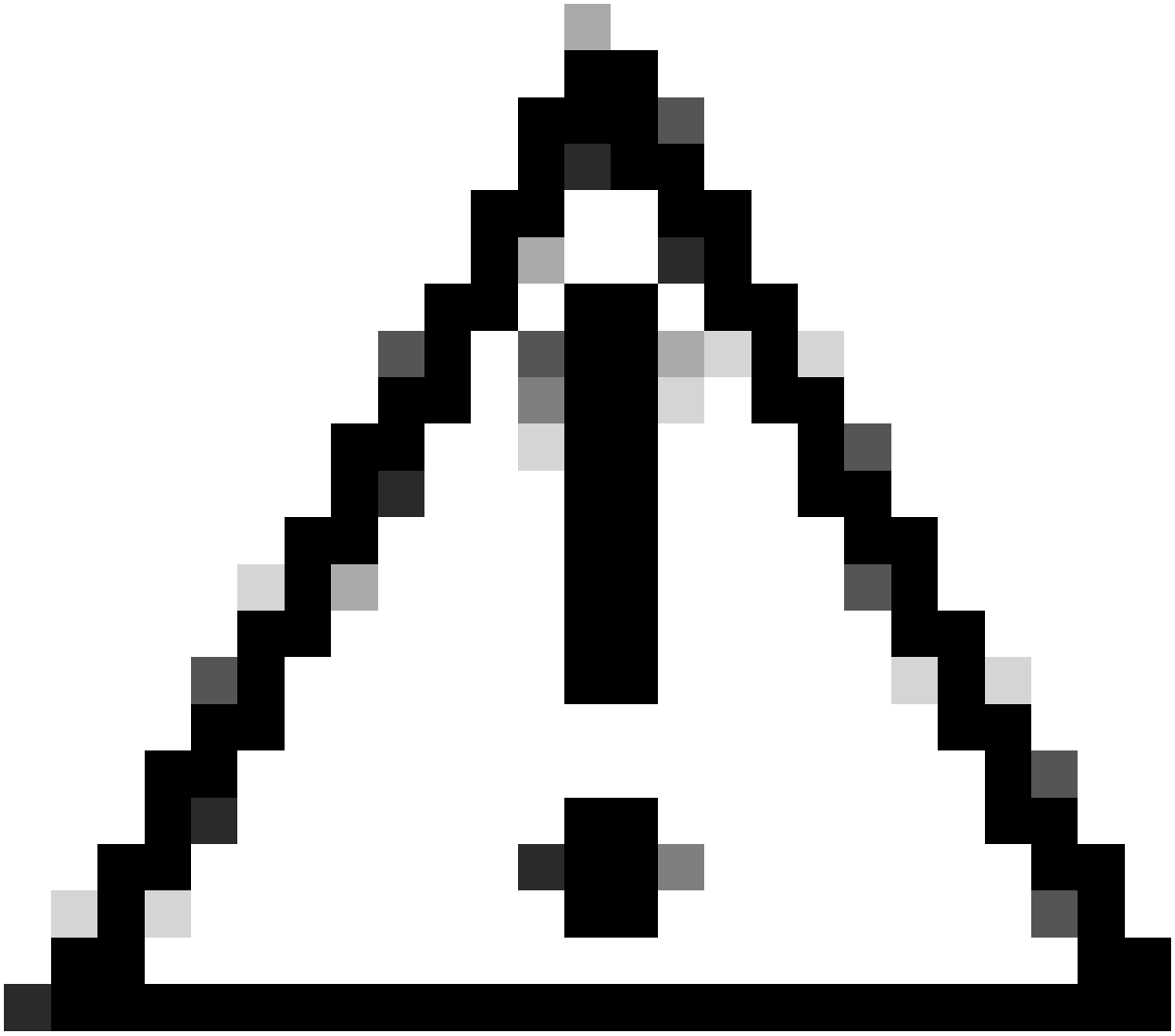



```
aaa authentication login SSLVPN_AUTHEN local
aaa authorization network SSLVPN_AUTHOR local
crypto ssl proposal ssl_proposal
protection rsa-aes256-sha1 rsa-aes128-sha1
!
crypto ssl policy ssl_policy
ssl proposal ssl_proposal
pki trustpoint TP_AnyConnect sign
ip interface GigabitEthernet1 port 443
!
crypto ssl profile my-profile
match policy ssl_policy
match url https://sslvpn-c8kv.example.com
aaa authentication user-pass list SSLVPN_AUTHEN
aaa authorization group user-pass list SSLVPN_AUTHOR ssl_author_policy
authentication remote user-pass
virtual-template 2
!
crypto ssl authorization policy ssl_author_policy
pool SSLVPN_POOL
def domain example.com
!
ip local pool SSLVPN_POOL 192.168.13.1 192.168.13.10
interface Virtual-Template2 type vpn
  ip unnumbered GigabitEthernet1
  ip mtu 1400
  vpn mode ssl
```

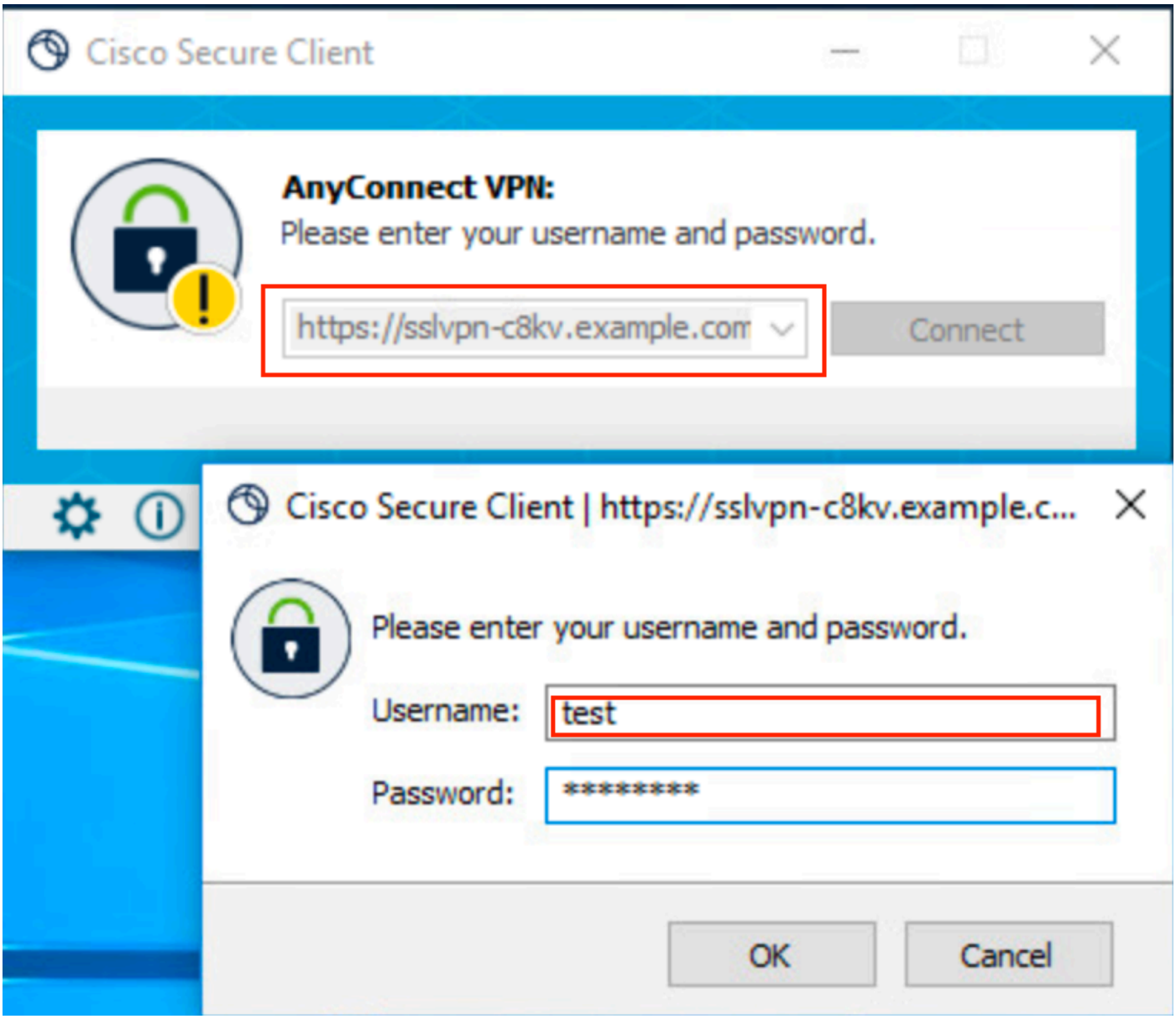
ハイレベル接続フロー2

確認

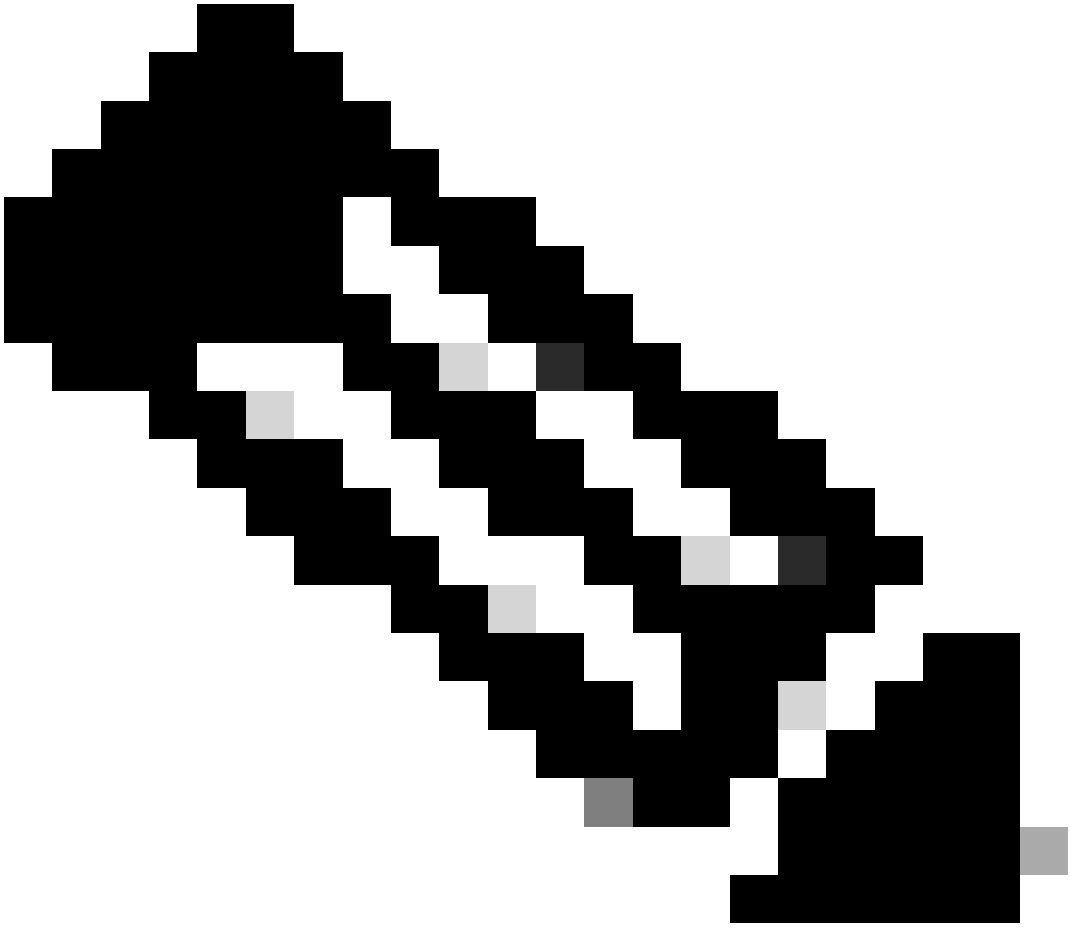
1. 認証をテストするには、Cisco Secure Clientから完全修飾ドメイン名(FQDN)またはC8000vのIPアドレスで接続し、クレデンシャルを入力します。



注意: C8000vでは、ヘッドエンドからのクライアントソフトウェアのダウンロードはサポートされていません。Cisco Secure ClientがPCにプリインストールされている必要があります。



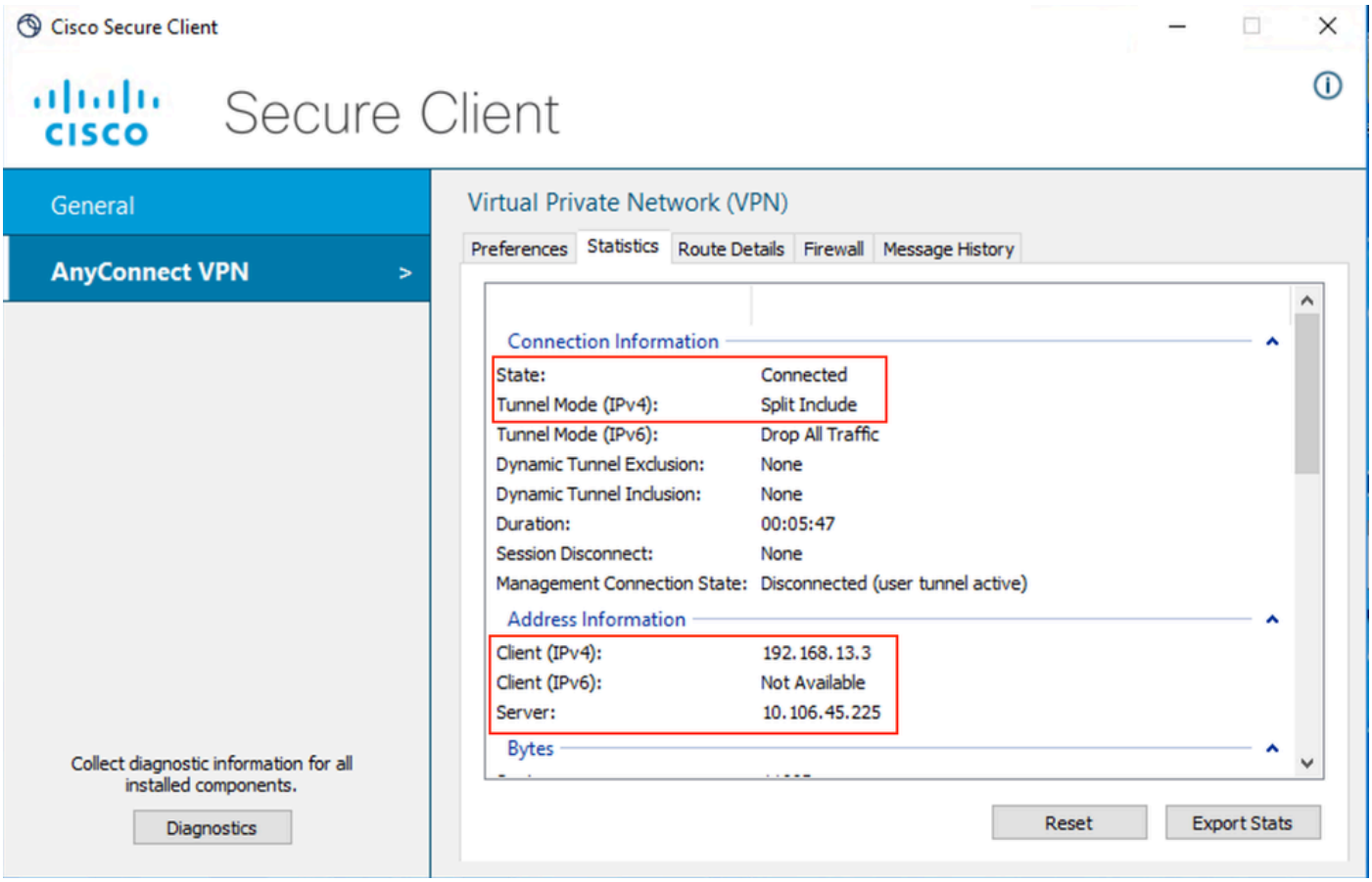
Cisco Secure Client接続の試行



注:Cisco Secure Clientを新規インストールする（XMLプロファイルを追加しない）と、ユーザはCisco Secure ClientのアドレスバーにVPNゲートウェイのFQDNを手動で入力できます。ログインに成功すると、Cisco Secure ClientはデフォルトでXMLプロファイルのダウンロードを試行します。ただし、プロファイルをGUIに表示するには、Cisco Secure Clientを再起動する必要があります。Cisco Secure Clientウィンドウを単に閉じるだけでは不十分です。プロセスを再起動するには、WindowsトレイのCisco Secure Clientアイコンを右クリックし、Quitオプションを選択します。

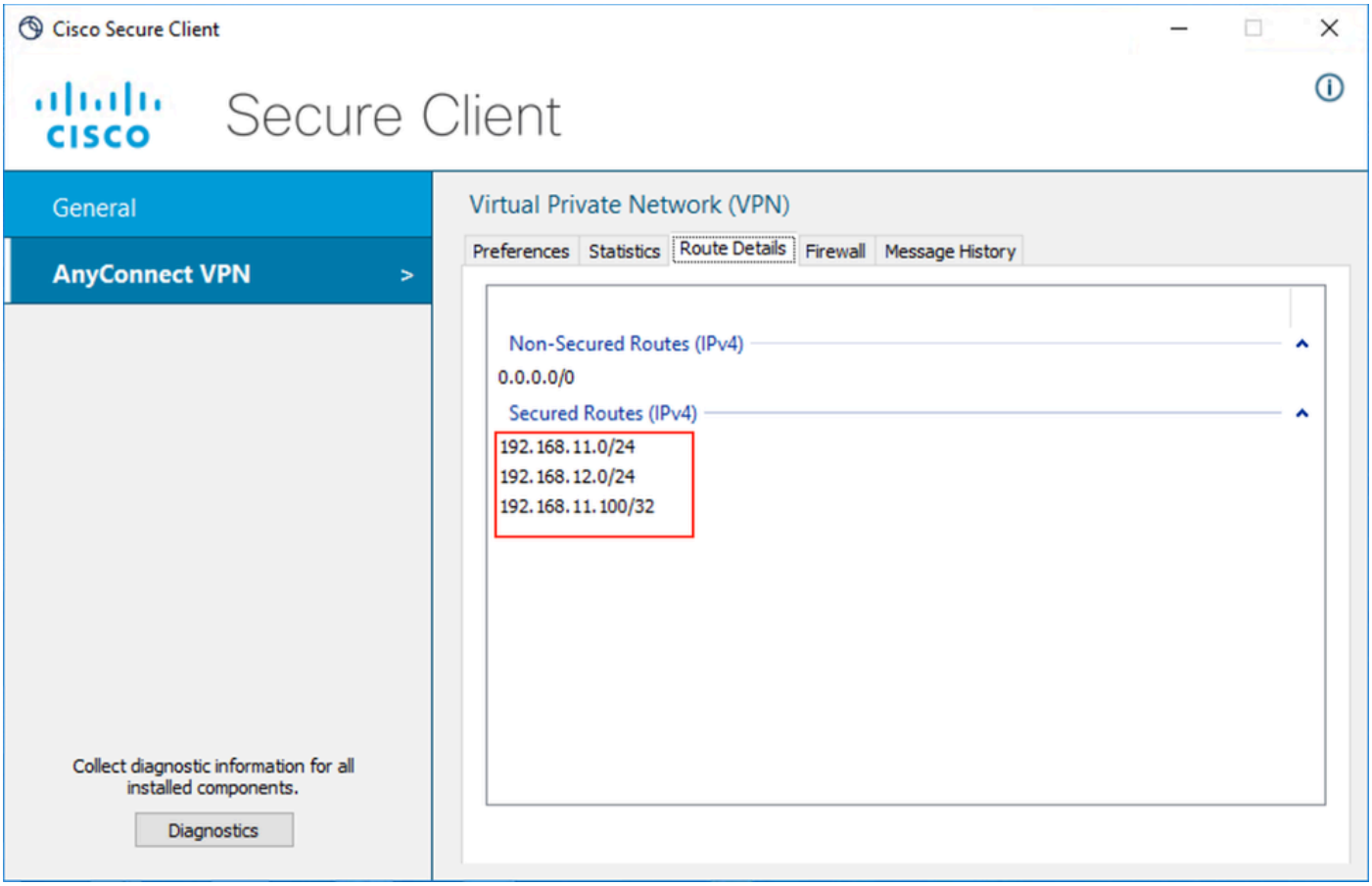
---

2. 接続が確立されたら、左下隅にあるgearアイコンをクリックして、AnyConnect VPN > Statisticsに移動します。 表示される情報が接続およびアドレス情報に対応していることを確認します。



Cisco Secure Client(AnyConnect)の統計情報

3. 次に移動します AnyConnectVPN >ルートの詳細 表示された情報が、セキュリティで保護されたルートと保護されていないルートに対応していることを確認します。



Cisco Secure Client(AnyConnect)ルートの詳細

ここでは、C8000vで設定が正しく動作していることを確認します。

1. SSLセッション情報を表示するには、show crypto ssl session{user user-name |profile profile-name}

<#root>

sal_c8kv#show crypto ssl session user test

Interface :

Virtual-Access1

Session Type : Full Tunnel
Client User-Agent : AnyConnect Windows 5.1.8.105

Username : test Num Connection : 1
Public IP : 10.106.69.69
Profile :

ssl_prof

Policy :

ssl_policy

```
Last-Used : 00:41:40                    Created : *15:25:47.618 UTC Mon Mar 3 2025
Tunnel IP : 192.168.13.3                Netmask : 0.0.0.0
Rx IP Packets : 542                     Tx IP Packets : 410
```

```
sal_c8kv#show crypto ssl session profile ssl_prof
```

```
SSL profile name: ssl_prof
Client_Login_Name  Client_IP_Address No_of_Connections Created   Last_Used
cisco                10.106.69.69             1        00:49:41  00:49:41
```

2. ssl vpn統計情報を表示するには、show crypto ssl stats [profile profile-name] [tunnel] [detail]

<#root>

```
sal_c8kv#show crypto ssl stats tunnel profile ssl_prof
```

```
SSLVPN Profile name : ssl_prof

Tunnel Statistics:

    Active connections       : 1
    Peak connections         : 1          Peak time               : 1d23h
    Connect succeed          : 13         Connect failed          : 0
    Reconnect succeed        : 0          Reconnect failed        : 0
    IP Addr Alloc Failed     : 0          VA creation failed      : 0
    DPD timeout              : 0

  Client

    in  CSTP frames          : 23         in  CSTP control        : 23
    in  CSTP data            : 0          in  CSTP bytes          : 872
    out CSTP frames          : 11         out CSTP control        : 11
    out CSTP data            : 0          out CSTP bytes          : 88
    cef in  CSTP data frames : 0          cef in  CSTP data bytes : 0
    cef out CSTP data frames : 0          cef out CSTP data bytes : 0

  Server

    In  IP pkts              : 0          In  IP bytes            : 0
    In  IP6 pkts             : 0          In  IP6 bytes           : 0
    Out IP pkts              : 0          Out IP bytes            : 0
    Out IP6 pkts             : 0          Out IP6 bytes           : 0
```

3. クライアントに関連付けられたバーチャルアクセスインターフェイスに適用される実際の設定を確認する。

<#root>

sal_c8kv#show derived-config interface Virtual-Access1

```
Building configuration...

Derived configuration : 143 bytes
!
interface Virtual-Access1
description ***Internally created by SSLVPN context ssl_prof***
ip unnumbered GigabitEthernet1
ip mtu 1400
end
```

トラブルシュート

このセクションでは、設定のトラブルシューティングに役立つ情報を紹介します。

1. ヘッドエンド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SSLデバッグ。

<#root>

debug crypto ssl condition client username

```
debug crypto ssl aaa
debug crypto ssl aggr-auth message
debug crypto ssl aggr-auth packets
debug crypto ssl tunnel errors
debug crypto ssl tunnel events
debug crypto ssl tunnel packets
debug crypto ssl package
```

2. SSL設定を確認するためのいくつかの追加コマンド。

```
# show crypto ssl authorization policy
# show crypto ssl diagnose error
# show crypto ssl policy
# show crypto ssl profile
# show crypto ssl proposal
# show crypto ssl session profile <profile_name>
# show crypto ssl session user <username> detail
# show crypto ssl session user <username> platform detail
```

3. Cisco Secure Client用の診断およびレポートツール(DART)。
DARTバンドルを収集するには、「トラブルシューティング用データを収集するためのDARTの実行」で説明されている手順を実行します。

接続が成功した場合のデバッグ例：

```
debug crypto ssl
debug crypto ssl tunnel events
debug crypto ssl tunnel errors
```

<#root>

```
*Mar 3 16:47:11.141: CRYPTO-SSL: sslvpn process rcvd context queue event
*Mar 3 16:47:14.149: CRYPTO-SSL: Chunk data written..
buffer=0x726BCA8891B8 total_len=621 bytes=621 tcb=0x0
*Mar 3 16:47:15.948: %SSLVPN-5-LOGIN_AUTH_PASSED: vw_ctx: ssl_prof vw_gw: ssl_policy remote_ip: 10.106.
*Mar 3 16:47:15.948: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: cisco] [Source: LOCAL] [localport
*Mar 3 16:47:15.949: CRYPTO-SSL: Chunk data written..
buffer=0x726BCA8891E0 total_len=912 bytes=912 tcb=0x0
*Mar 3 16:47:17.698: CRYPTO-SSL: sslvpn process rcvd context queue event
*Mar 3 16:47:20.755: [CRYPTO-SSL-TUNL-EVT]:[726BCA848AB0] CSTP Version recd , using 1
*Mar 3 16:47:20.755: [CRYPTO-SSL-TUNL-ERR]: IPv6 local addr pool not found
*Mar 3 16:47:20.755: [CRYPTO-SSL-TUNL-EVT]:[726BCA848AB0] No free IPv6 available, disabling IPv6
*Mar 3 16:47:20.755: [CRYPTO-SSL-TUNL-EVT]:[726BCA848AB0]
SSLVPN reuqesting a VA creation
*Mar 3 16:47:20.755: [CRYPTO-SSL-TUNL-EVT]:[726BCA848AB0] Per Tunnel Vaccess cloning 2 request sent
*Mar 3 16:47:20.760: %SYS-5-CONFIG_P: Configured programmatically by process VTEMPLATE Background Mgr f
*Mar 3 16:47:20.760: [CRYPTO-SSL-TUNL-EVT]:[0] VACCESS: Received VACCESS PER TUNL EVENT response.
*Mar 3 16:47:20.760: [CRYPTO-SSL-TUNL-EVT]:[726BCA848AB0] VACCESS: Received vaccess Virtual-Access1 fro
*Mar 3 16:47:20.760: [CRYPTO-SSL-TUNL-EVT]:[726BCA848AB0] VACCESS: Cloning Per Tunnel Vaccess
*Mar 3 16:47:20.760: [CRYPTO-SSL-TUNL-EVT]:[726BCA848AB0] VACCESS: Interface Vi1 assigned to Session Us
*Mar 3 16:47:20.761: [CRYPTO-SSL-TUNL-EVT]:[726BCA848AB0] Allocating IP 192.168.13.4 from address-pool
*Mar 3 16:47:20.761: [CRYPTO-SSL-TUNL-EVT]:[726BCA848AB0] Using new allocated IP 192.168.13.4 0.0.0.0
*Mar 3 16:47:20.761: %LINK-3-UPDOWN: Interface Virtual-Access1, changed state to up
*Mar 3 16:47:20.763: [CRYPTO-SSL-TUNL-EVT]:[726BCA848AB0] Full Tunnel CONNECT request processed, HTTP r
*Mar 3 16:47:20.763: HTTP/1.1 200 OK
*Mar 3 16:47:20.763: Server: Cisco IOS SSLVPN
*Mar 3 16:47:20.763: X-CSTP-Version: 1
*Mar 3 16:47:20.763: X-CSTP-Address: 192.168.13.4
*Mar 3 16:47:20.763: X-CSTP-Netmask: 0.0.0.0
*Mar 3 16:47:20.763: X-CSTP-DNS: 192.168.11.100
*Mar 3 16:47:20.764: X-CSTP-Lease-Duration: 43200
*Mar 3 16:47:20.764: X-CSTP-MTU: 1406
*Mar 3 16:47:20.764: X-CSTP-Default-Domain: example.com
*Mar 3 16:47:20.764: X-CSTP-Split-Include: 192.168.11.0/255.255.255.0
*Mar 3 16:47:20.764: X-CSTP-Split-Include: 192.168.12.0/255.255.255.0
*Mar 3 16:47:20.764: X-CSTP-Split-Include: 192.168.11.0/255.255.255.0
*Mar 3 16:47:20.764: X-CSTP-Split-Include: 192.168.12.0/255.255.255.0
*Mar 3 16:47:20.765: X-CSTP-Rekey-Time: 3600
*Mar 3 16:47:20.765: X-CSTP-Rekey-Method: new-tunnel
*Mar 3 16:47:20.765: X-CSTP-DPD: 300
*Mar 3 16:47:20.765: X-CSTP-Disconnected-Timeout: 0
*Mar 3 16:47:20.765: X-CSTP-Idle-Timeout: 1800
```

```
*Mar 3 16:47:20.765: X-CSTP-Session-Timeout: 43200
*Mar 3 16:47:20.765: X-CSTP-Keepalive: 30
*Mar 3 16:47:20.765: X-CSTP-Smartcard-Removal-Disconnect: false
*Mar 3 16:47:20.766: X-CSTP-Include-Local_LAN: false
*Mar 3 16:47:20.766: [CRYPTO-SSL-TUNL-EVT]:[726BCA848AB0] For User cisco, DPD timer started for 300 sec
*Mar 3 16:47:20.766: CRYPTO-SSL: Chunk data written..
buffer=0x726BCA8891E0 total_len=693 bytes=693 tcb=0x0
*Mar 3 16:47:21.762:
```

%LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed state to up

関連情報

- シスコのテクニカルサポートとダウンロード

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。