FlexVPN サーバーの設定

このモジュールでは、FlexVPN サーバーの機能、FlexVPN サーバーの設定に必要な IKEv2 コマンド、リモート アクセス クライアント、およびサポートされる RADIUS 属性について説明します。

（注） セキュリティに対する脅威は、そのような脅威からの保護に役立つ暗号化技術と同様に、絶え間なく変化しています。シスコの暗号化に関する最新の推奨事項の詳細は、『Next Generation Encryption』（NGE）ホワイトペーパーを参照してください。

FlexVPN サーバーの制限事項

デュアルスタック トンネル インターフェイスおよび VRF 認識 IPsec

VPN ルーティングおよび転送（VRF）認識 IPsec シナリオでデュアルスタック トンネル インターフェイスを設定する場合、**ip vrf forwarding** コマンドを使用して内部 VPN ルーティングおよび転送（IVRF）インスタンスを設定することはできません。これは有効な設定ではないためです。トンネル インターフェイスの IVRF を定義するには **vrf forwarding** *vrf-name* コマンドを使用します。ここで、*vrf-name* 引数は、定義内に IPv4 および IPv6 アドレス ファミリを指定した **vrf definition** コマンドを使用して定義されます。

SSO の制約事項

- ESP をリロードした場合（スタンバイ ESP なし）、SA シーケンス番号は 0 から再開されます。ピア ルータは、予期されたシーケンス番号を持たないパケットをドロップします。

単一の ESP を使用するシステムで ESP のリロード後にこの問題を回避するには、IPSec セッションを明示的に再確立することが必要になる場合があります。このような場合、リロード中に IPSec セッションでトラフィックの中断が発生することがあります。

FlexVPN サーバーに関する情報

EAP を使用するピア認証

FlexVPN サーバーは、Extensible Authentication Protocol（EAP：拡張可能認証プロトコル）を使用するピア認証をサポートし、クライアントとバックエンド EAP サーバー間で EAP メッセージを中継するパススルー オーセンティケータとして動作します。EAP バックエンド サーバーは、通常、EAP 認証をサポートする RADIUS サーバーです。

（注） FlexVPN クライアントは EAP を使用する FlexVPN クライアントを認証しますが、FlexVPN サーバーは証明書を使用して認証を受ける必要があります。

FlexVPN サーバーは、IKEv2 プロファイル設定モードの **authentication remote eap** コマンドによって、EAP を使用する FlexVPN クライアントを認証するよう設定されています。FlexVPN クライアントは、IKE_AUTH 要求内の AUTH ペイロードをスキップすることで、EAP を使用して認証します。

query-identity キーワードが設定されている場合、FlexVPN サーバーはクライアントからの EAP ID をクエリします。それ以外は、FlexVPN クライアントの IKEv2 ID が EAP ID として使用されます。ただし、**query-identity** キーワードが設定されておらず、FlexVPN クライアントの IKEv2 ID が IPv4 または IPv6 アドレスの場合、IP アドレスを EAP ID として使用できないため、セッションは終了します。

FlexVPN サーバーは、FlexVPN クライアントの EAP ID を EAP サーバーに渡すことで、EAP 認証を開始します。その後、FlexVPN サーバーは、認証が完了するまで、リモート アクセス（RA）クライアントと EAP サーバー間の EAP メッセージを中継します。認証が成功すると、EAP サーバーでは、EAP 成功メッセージ内で認証された EAP の ID が FlexVPN サーバーに返されることが予想されます。

EAP 認証の後、IKEv2 設定に使用された EAP ID は、次の送信元から任意の順で取得されます。

- EAP 成功メッセージで EAP サーバーから提供される EAP ID。
- **query-identity** キーワードの設定時にクライアントからクエリされる EAP ID。
- EAP ID として使用される FlexVPN クライアントの IKEv2 ID。

次の図は、**query-identity** キーワードなしの EAP 認証に対する IKEv2 交換を示します。

図 *1 : query-identity* キーワードなしの *IKEv2* 交換

IKEv2 RA client	IKEv2 RA server	RADIUS-EAP server
HDR, SAi1, KEi, Ni →		
	← HDR, SAr1, KEr, Nr, [CERTREQ]	
HDR, SK {IDi, [CERTREQ,] [IDr,] SAi2, TSi, TSr} →		
	RADIUS Access-Request/ EAP-Message/EAP-Response/(EAP-ID(IKEv2-ID)) →	
		← RADIUS Access-Challenge/EAP-Message/ EAP-Request/(EAP-method)
	← HDR, SK {IDr, [CERT,] AUTH, EAP(EAP-Request(EAP-method))}	
HDR, SK {EAP(EAP-Response(EAP-method)} →		
	RADIUS Access-Request/EAP-Message/EAP-Response/EAP-method) →	
		← RADIUS Access-Accept/EAP-Message/EAP-Success (other attributes))
	← HDR, SK {EAP (success)}	
HDR, SK {AUTH} →		
	← HDR, SK {AUTH, SAr2, TSi, TSr }	

209140

次の図は、**query-identity** キーワードありの EAP 認証に対する IKEv2 交換を示します。

図 *2 : query-identity* キーワードありの *IKEv2* 交換

IKEv2 RA client	IKEv2 RA server	RADIUS-EAP server
HDR, SAi1, KEi, Ni →		
	← HDR, SAr1, KEr, Nr, [CERTREQ]	
HDR, SK {IDi, [CERTREQ,] [IDr,] SAi2, TSi, TSr} →		
	← HDR, SK {IDr, [CERT,] AUTH, EAP (EAP-request (Identity)) }	
HDR, SK {EAP(EAP-Response(Identity)} →		
	RADIUS Access-Request/ EAP-Message/EAP-Response/(EAP-ID) →	
		← RADIUS Access-Challenge/EAP-Message/ EAP-Request/(EAP-method)
	← HDR, SK {IDr, [CERT,] AUTH, EAP(EAP-Request(EAP-method))}	
HDR, SK {EAP(EAP-Response(EAP-method)} →		
	RADIUS Access-Request/EAP-Message/EAP-Response/EAP-method) →	
		← RADIUS Access-Accept/EAP-Message/EAP-Success (EAP-identity) (other attributes))
	← HDR, SK {EAP (success)}	
HDR, SK {AUTH} →		
	← HDR, SK {AUTH, SAr2, TSi, TSr }	

209141

IKEv2 コンフィギュレーション モード

IKEv2 コンフィギュレーション モードで、IKE ピアは IP アドレスやルートなどの設定情報を交換できます。設定情報は、IKEv2 認証から取得されます。プル モデルとプッシュ モデルの両方がサポートされます。プル モデルには、設定要求と応答の交換が含まれます。プッシュ モデルには、設定セットと確認応答の交換が含まれます。

次の表に、発信側と応答側が異なる設定ペイロードタイプを送信するときの状況を示します。

表 *1*：設定ペイロード タイプ

設定ペイロード タイプ	送信元...	属性...
CFG_REQUEST	発信側	発信側が FlexVPN クライアントの場合。または、**config-exchange request** コマンドが IKEv2 プロファイルで有効になっている場合。
CFG_REPLY	応答側	応答側が CFG_REQUEST を受信する場合。
CFG_SET	発信側と応答側	発信側：**config-exchange set send** コマンドが IKEv2 プロファイルで有効になっている場合。 応答側：CFG_REQUEST が受信されておらず、設定データを使用可能で、**config-exchange set send** コマンドが IKEv2 プロファイルで有効になっている場合。
CFG_ACK	発信側と応答側	発信側：**config-exchange set accept** コマンドが IKEv2 プロファイルで有効になっている場合。 応答側：**config-exchange set accept** コマンドが IKEv2 プロファイルで有効になっている場合。

（注） 設定要求と設定セット ペイロードを送信するためのコマンドは、デフォルトで有効になっています。

ご使用のリリースに応じて、発信側が FlexVPN クライアントの場合に IKEv2 発信側がコンフィギュレーション モードをトリガーしたり、IKEv2 プロファイルで **config-mode** コマンドを有効にすることによって IKEv2 を発信するスタティック トンネル インターフェイスがコンフィギュレーション モードをトリガーすることができます。

IKEv2 FlexVPN サーバーは、次の標準 IPv4 設定属性をサポートします。

- INTERNAL_IP4_ADDRESS
- INTERNAL_IP4_NETMASK
- INTERNAL_IP4_DNS
- INTERNAL_IP4_NBNS
- INTERNAL_IP4_SUBNET

IKEv2 FlexVPN サーバーは、次の標準 IPv6 設定属性をサポートします。

- INTERNAL_IP6_ADDRESS
- INTERNAL_IP6_DNS
- INTERNAL_IP6_SUBNET

（注） IPv6 設定属性は、Microsoft Windows IKEv2 クライアントによってのみサポートされます。

IKEv2 認証ポリシーで **route set** コマンドと **aaa attribute list** コマンドによって制御されている INTERNAL_IP4_SUBNET および INTERNAL_IP6_SUBNET 設定属性は、SVTI（スタティック仮想トンネルインターフェイス）-to-SVTI トンネルを設定する場合はサポートされません。このような場合、IKEv2 ベースのルート交換の代わりにスタティック ルーティングまたはダイナミック ルーティングを使用する必要があります。

IKEv2 FlexVPN サーバーは、次の標準共通設定属性をサポートします。

- APPLICATION_VERSION

（注） この属性は、Cisco AnyConnect および FlexVPN クライアントにのみ送信されます。

IKEv2 FlexVPN サーバーは、次の Cisco Unity 設定属性をサポートします。

- MODECFG_BANNER
- MODECFG_DEFDOMAIN
- MODECFG_SPLITDNS_NAME
- MODECFG_BACKUPSERVERS
- MODECFG_PFS
- MODECFG_SMARTCARD_REMOVAL_DISCONNECT

（注） Cisco Unity 属性は、Cisco AnyConnect および FlexVPN クライアントにのみ送信されます。

IKEv2 FlexVPN サーバーは、次の Cisco FlexVPN 設定属性をサポートします。

- MODECFG_CONFIG_URL
- MODECFG_CONFIG_VERSION

（注） Cisco FlexVPN 属性は、Cisco FlexVPN クライアントにのみ送信されます。

INTERNAL_IP4_ADDRESS 属性値は、指定された順序で次の送信元から取得されます。

- AAA ユーザー認証で受信した Framed-IP-Address 属性。
- ローカル IP アドレス プール。
- DHCP サーバー。

DHCP サーバー（設定されている場合）は、ローカル IP アドレス プールが設定されていない場合にのみアドレスを割り当てます。ただし、ローカル プールから IP アドレスを割り当てるとエラーが発生する場合、その次のアドレス送信元の DHCP サーバーはアドレスの割り当てに使用されません。

INTERNAL_IP4_NETMASK 属性の値は、次から取得されます。

- IP アドレスが DHCP サーバーから取得される場合、ネットマスクも DHCP サーバーから取得されます。
- IP アドレスが AAA ユーザー認証の Framed-IP-Address 属性またはローカル IP アドレス プールのいずれかから取得される場合、ネットマスクはユーザー認証またはグループ認証で受信した IPv4 ネットマスク属性から取得されます。ネットマスクが使用できない場合、INTERNAL_IP4_NETMASK 属性は設定応答に含まれません。ネットマスクが使用可能な場合、INTERNAL_IP4_ADDRESS 属性が設定応答に含まれるときにのみ、INTERNAL_IP4_NETMASK 属性は含まれます。

IPv4 アドレスは、クライアントがアドレスを要求する場合にのみ割り当てられ、応答に含まれます。クライアントが複数の IPv4 アドレスを要求した場合、応答で送信される IPv4 アドレスは 1 つのみです。可能な場合は、クライアントが要求しなくても残りの属性が応答に含まれます。クライアントが IPv4 アドレスを要求して、FlexVPN サーバーがアドレスを割り当てることができない場合、INTERNAL_ADDRESS_FAILURE メッセージがクライアントに返されます。

ipv6 local pool 設定では常に、プレフィックス長に 128 を使用することをお勧めします。

たとえば、クライアント数が 4 の場合は、プレフィックス長として **ipv6 local pool pool1 afe0::/126 128** を設定する必要があります。クライアント数が 16 の場合は、プレフィックス長として **ipv6 local pool pool1 afe0::/124 128** を設定する必要があります。

IKEv2 認証

IKEv2 認証は、AAA を使用して認証されるセッションに対するポリシーを提供します。このポリシーは、ローカルに定義するか RADIUS サーバーで定義できます。また、このポリシーにはローカルおよび/またはリモート属性が含まれています。認証用のユーザー名は、**name-mangler** キーワードを使用してピア ID から取得するか、コマンドで直接指定することができます。

IKEv2 認証は、ピアがコンフィギュレーション モードを介して IP アドレスを要求する場合にのみ必要です。

IKEv2 認証タイプは、次のとおりです。

- ユーザー認証：ユーザー認証を有効にするには、IKEv2 プロファイルで **aaa authorization user** コマンドを使用します。ユーザー認証は、fqdn-hostname などのピア IKE ID のユーザー固有の部分に基づいています。ユーザー認証の属性は、ユーザー属性と呼ばれます。
- グループ認証：グループ認証を有効にするには、IKEv2 プロファイルで **aaa authorization group** コマンドを使用します。グループ認証は、fqdn-domain などのピア IKE ID の汎用部分に基づいています。グループ認証の属性は、グループ属性と呼ばれます。
- 暗黙的ユーザー認証：暗黙的ユーザー認証を有効にするには、IKEv2 プロファイルで **aaa authorization user cached** コマンドを使用します。暗黙的認証は、EAP 認証の一部として実行されるか、AAA 事前共有キーの取得時に実行されます。暗黙的ユーザー認証の属性は、キャッシュ属性と呼ばれます。

（注） ご使用のリリースに応じて、**aaa authorization user cached** コマンドが使用可能または使用不可能な場合があります。明示的ユーザー認証は、暗黙的ユーザー認証が属性を返さない場合または Framed-IP-Address 属性を持たない場合にのみ実行されます。

属性のマージおよびオーバーライド

異なる送信元からの属性は、使用前にマージされます。マージ属性の優先順位は、次のとおりです。

- 重複する属性をマージする場合、属性の送信元の優先順位が高くなります。
- ユーザー属性およびキャッシュ属性をマージする場合、ユーザー属性の優先順位が高くなります。
- マージ済みのユーザー属性およびグループ属性をマージする場合、デフォルトではマージ済みのユーザー属性の優先順位が高くなります。ただし、この優先順位は **aaa author group override** コマンドを使用して逆にすることができます。

IKEv2 認証ポリシー

IKEv2認証ポリシーでは、ローカル認証ポリシーが定義され、ローカルおよび/またはリモート属性が含まれています。VPN ルーティングおよび転送（VRF）や QOS ポリシーなどのローカル属性は、ローカルに適用されます。ルートなどのリモート属性は、コンフィギュレーションモードでピアにプッシュされます。ローカル ポリシーを定義するには、**crypto ikev2 authorization policy** コマンドを使用します。IKEv2 認証ポリシーは、**aaa authorization** コマンドによって IKEv2 プロファイルから示されます。

IKEv2 名前分割

IKEv2 名前分割は、IKEv2 認証用のユーザー名の取得およびピア IKE ID からの AAA 事前共有キーの取得に使用されます。

IKEv2 マルチ SA

IKEv2 マルチ SA 機能によって、IKEv2 応答側の IKEv2 ダイナミック仮想トンネル インターフェイス（DVTI）セッションは複数の IPsec セキュリティ アソシエーション（SA）をサポートできます。DVTI セッションあたりの IPSec SA の最大数は、AAA 認証から取得されるか IPsec プロファイルで設定されます。AAA からの値が優先されます。IPsec プロファイルでの *max-flow-limit* 引数への変更は現在のセッションには適用されませんが、後続のセッションに適用されます。IKEv2 マルチ SA 機能では、IPsec プロファイルでの IKEv2 プロファイルの設定は任意です。この任意設定によって、同じ仮想テンプレートを使用する IPsec DVTI セッションで異なる IKEv2 プロファイルを使用できるようになり、仮想テンプレート設定の数が削減されます。

（注） IKEv2 マルチ SA 機能では、非 any-any プロキシを持つ複数の IPsec SA が許可されます。ただし、IPSec SA プロキシが any-any の場合は 1 つの IPsec SA が許可されます。

詳細については、『*Security for VPNs with IPsec Configuration Guide*』の『Multi-SA Support for Dynamic Virtual Tunnel Interfaces for IKEv2』モジュールを参照してください。

AnyConnect プロファイルのダウンロード

FlexVPN AnyConnect プロファイルのダウンロード機能を使用すると、Cisco IOS XE ソフトウェアを実行しているデバイスが、Cisco AnyConnect セキュア モビリティ クライアントに IKEv2 プロトコルで接続してプロファイル情報をプッシュできます。

Cisco AnyConnect セキュア モビリティ クライアントには、VPN の設定に使用されるプロファイルが含まれています。このプロファイルは、手動で設定することも、ヘッドエンドからダウンロードすることもできます。ヘッドエンドは、Cisco AnyConnect セキュア モビリティ クライアントのすべてのユーザーにプロファイルをグローバルに展開するように設定できます。

VPN プロファイルを IKEv2 プロファイルと照合するには、**anyconnect profile** コマンドを使用します。

（注） AnyConnect プロファイルのダウンロード機能を設定する際、crypto ssl profile は必須ではありません。

サポートされる RADIUS 属性

次のテーブルに、IKEv2 FlexVPN サーバーがサポートする RADIUS 属性を示します。

- [Scope] フィールドは、属性の方向と、FlexVPN サーバーまたはクライアントでの使用方法を定義します。
  - [Inbound]：FlexVPN サーバーから RADIUS
  - [Outbound]：RADIUS から FlexVPN サーバー
  - [Local]：FlexVPN サーバーによってローカルで使用される
  - [Remote]：FlexVPN サーバーによってクライアントにプッシュされる
- [Local configuration] フィールドは、FlexVPN サーバーでローカルに属性を設定するために使用される、IKEv2 認証ポリシー コマンドを指定します。
- Cisco AV ペアは、vendor-id が 9、vendor-type が 1 の Cisco ベンダー固有属性（VSA）です。VSA は、RADIUS IETF 属性 26 のベンダー固有でカプセル化されます。Cisco AV ペアは、文字列形式「protocol:attribute=value」で指定されます。

例：

```
cisco-avpair = "ipsec:ipv6-addr-pool=v6-pool"
```

次に、標準アクセス リストの Cisco AV ペアの例を示します。

```
cisco-avpair = "ipsec:route-set=access-list 99"
```

表 *2*：着信および双方向の *IETF RADIUS* 属性

属性	スコープ
User-Name	着信と発信（双方向）
User-Password	着信
Calling-Station-Id	着信
Service-Type	着信
EAP-Message	双方向
Message-Authenticator	双方向

表 *3*：発信 *IETF* および *Cisco AV* ペアの *RADIUS* 属性

属性	タイプ	スコープ	ローカル設定
Tunnel-Type	IETF	Local	該当なし
Tunnel-Medium-Type	IETF	Local	該当なし

属性	タイプ	スコープ	ローカル設定
Tunnel-Password	IETF	Local	該当なし
ipsec:ikev2-password-local	Cisco AV ペア	Local	該当なし
ipsec:ikev2-password-remote	Cisco AV ペア	Local	該当なし
ipsec:addr-pool	Cisco AV ペア	Local	pool
ipsec:group-dhcp-server	Cisco AV ペア	Local	dhcp server
ipsec:dhcp-giaddr	Cisco AV ペア	Local	dhcp giaddr
ipsec:dhcp-timeout	Cisco AV ペア	Local	dhcp timeout
ipsec:ipv6-addr-pool	Cisco AV ペア	Local	ipv6 pool
ipsec:route-set=interface	Cisco AV ペア	Local	route set interface
ipsec:route-set=prefix	Cisco AV ペア	Local	該当なし
ipsec:route-accept	Cisco AV ペア	Local	route accept any
ip:interface-config	Cisco AV ペア	Local	aaa attribute list
ipsec:ipsec-flow-limit	Cisco AV ペア	Local	ipsec flow-limit
Framed-IP-Address	IETF	Remote	該当なし
Framed-IP-Netmask	IETF	Remote	netmask
ipsec:dns-servers	Cisco AV ペア	Remote	DNS
ipsec:wins-servers	Cisco AV ペア	Remote	wins
ipsec:route-set=access-list （注 1 を参照）	Cisco AV ペア	Remote	route set access-list （注 1 を参照）
ipsec:addrv6	Cisco AV ペア	Remote	n/a
ipsec:prefix-len	Cisco AV ペア	Remote	n/a
ipsec:ipv6-dns-servers-addr	Cisco AV ペア	Remote	ipv6 dns
ipsec:route-set=access-list ipv6	Cisco AV ペア	Remote	route set access-list ipv6
ipsec:banner	Cisco AV ペア	Remote	banner
ipsec:default-domain	Cisco AV ペア	Remote	def-domain
ipsec:split-dns	Cisco AV ペア	Remote	split-dns

属性	タイプ	スコープ	ローカル設定
ipsec:ipsec-backup-gateway	Cisco AV ペア	Remote	backup-gateway
ipsec:pfs	Cisco AV ペア	Remote	pfs
ipsec:include-local-lan	Cisco AV ペア	Remote	include-local-lan
ipsec:smartcard-removal-disconnect	Cisco AV ペア	Remote	smartcard-removal- disconnect
ipsec:configuration-url	Cisco AV ペア	Remote	configuration url
ipsec:configuration-version	Cisco AV ペア	Remote	configuration version

（注）
- 1. IKEv2 FlexVPN サーバーでアクセス リストを設定するための RADIUS 属性は、標準アクセス リストのみをサポートします。拡張アクセス リストはサポートされていません。

サポートされるリモート アクセス クライアント

FlexVPN サーバーは、Microsoft 7 IKEv2 クライアント、Cisco IKEv2 AnyConnect クライアント、および Cisco FlexVPN クライアントと相互運用されます。

Microsoft Windows 7 IKEv2 クライアント

Microsoft Windows 7 IKEv2 クライアントは、インターネット キー エクスチェンジ（IKE）ID として IP アドレスを送信します。この ID は、Cisco IKEv2 FlexVPN サーバーが IKE ID に基づいてリモート ユーザーを分類するのを防ぎます。Windows 7 IKEv2 クライアントが電子メール アドレス（user@domain）を IKE ID として送信できるようにするには、KB975488（http://support.microsoft.com/kb/975488）に記載されたホットフィックスを Windows 7 に適用し、電子メールアドレスの文字列を、プロンプトが表示された場合は [Username] フィールドまたは証明書の [CommonName] フィールドに、認証方式に応じて指定します。

証明書ベースの認証の場合は、次のように、FlexVPN サーバーと Microsoft Windows 7 クライアントの証明書に拡張キー使用法（EKU）フィールドが含まれている必要があります。

- クライアント証明書では、EKU フィールド = クライアント認証証明書です。
- サーバー証明書では、EKU フィールド = サーバー認証証明書です。
- 証明書は、Microsoft の証明書サーバーまたは IOS CA サーバーから取得できます。

EAP 認証の場合は、Microsoft Windows 7 IKEv2 クライアントが他の EAP 要求の前に EAP ID 要求を待ちます。クライアントに EAP ID 要求を送信するには、IKEv2 FlexVPN サーバー上の IKEv2 プロファイル内で **query-identity** キーワードが設定されていることを確認してください。

Cisco IKEv2 AnyConnect クライアント

証明書ベースの認証では、次のように FlexVPN サーバーと AnyConnect クライアントの証明書に拡張キー使用法（EKU）フィールドが含まれている必要があります。

- クライアント証明書では、EKU フィールド = クライアント認証証明書です。
- サーバー証明書では、EKU フィールド = サーバー認証証明書です。

FlexVPN サーバーが証明書を使用して AnyConnect クライアントを認証する場合、サーバーの IP アドレスまたは完全修飾ドメイン名（FQDN）を含む FlexVPN サーバーの証明書に SubjectAltName の拡張子が必要です。また、**no crypto ikev2 http-url cert** コマンドを使用して、HTTP 認証 URL を FlexVPN サーバーで無効にしておく必要があります。

次の例では、AnyConnect クライアント プロファイルの IKEv2 セッションの EAP-MD5 認証に固有の XML タグを示します。

```
<PrimaryProtocol>IPsec
       <StandardAuthenticationOnly>true
           <AuthMethodDuringIKENegotiation>
               EAP-MD5
           </AuthMethodDuringIKENegotiation>
           <IKEIdentity>DEPT24</IKEIdentity>
       </StandardAuthenticationOnly>
</PrimaryProtocol>
```

（注） 有効になっているすべてのフラップまたは FlexVPN トンネルについて、次のメッセージが表示されます。

```
*Jan 22 22:52:09.833: %SYS-5-CONFIG_P: Configured programmatically by process Crypto INT
 from console as console
*Jan 22 22:52:09.840: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access2,
changed state to up
```

詳細については、次のリンクで AnyConnect クライアント 3.0 のドキュメントを参照してください。
http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect30/release/notes/anyconnect30rn.html#wp1268255

FlexVPN サーバーの設定方法

FlexVPN サーバーの IKEv2 プロファイルの設定

このタスクでは、基本的な IKEv2 プロファイル コマンドに加えて、FlexVPN サーバーの設定に必要な IKEv2 プロファイル コマンドについて説明します。基本的な IKEv2 プロファイルの設定方法については、『*Configuring Internet Key Exchange Version 2 (IKEv2)*』機能モジュールの「Configuring IKEv2 Profile (Basic)」タスクを参照してください。

このタスクは、FlexVPN サーバーの IKEv2 プロファイルを設定するために実行します。

ステップ 1 **enable**

例：

特権 EXEC モードを有効にします。

```
Device> enable
```

プロンプトが表示されたらパスワードを入力します。

ステップ 2 **configure terminal**

例：

グローバル コンフィギュレーション モードを開始します。

```
Device# configure terminal
```

ステップ 3 **crypto ikev2 profile** *profile-name*

IKEv2 プロファイル名を定義し、IKEv2 プロファイル コンフィギュレーション モードを開始します。

例：

```
Device(config)# crypto ikev2 profile profile1
```

ステップ 4 **aaa authentication eap** *list-name*

例：

```
Device(config-ikev2-profile)# aaa authentication eap list1
```

（任意）IKEv2 リモートアクセスサーバーの実装中に EAP 認証用の AAA 認証リストを指定します。

- **eap**：外部 EAP サーバーを指定します。
- *list-name*：AAA 認証リスト名。

ステップ 5 **authentication** {**local** {**rsa-sig** | **pre-share** [**key** {**0** | **6**} *password*}] | **ecdsa-sig** | **eap** [**gtc** | **md5** | **ms-chapv2**] [**username** *username*] [**password** {**0** | **6**} *password*}]} | **remote** {**eap** [**query-identity** | **timeout** *seconds*] | **rsa-sig** | **pre-share** [**key** {**0** | **6**} *password*}] | **ecdsa-sig**}}

例：

```
Device(config-ikev2-profile)# authentication local ecdsa-sig
```

ローカルまたはリモートの認証方式を指定します。

- **rsa-sig**：認証方式として RSA-sig を指定します。
- **pre-share**：認証方式として事前共有キーを指定します。
- **ecdsa-sig**：認証方式として ECDSA-sig を指定します。
- **eap**：リモート認証方式として EAP を指定します。
- **query-identity**：ピアに EAP ID を問い合わせます。
- **timeout** *seconds*：最初の IKE_AUTH 応答を返してから次の IKE_AUTH 要求を受け取るまでの期間を秒単位で指定します。

（注）　ローカル認証方式は 1 つしか指定できませんが、リモート認証方式は複数指定できます。

ステップ 6 次のいずれかまたは両方を実行します。

- **aaa authorization user** {**eap** | **psk**} {**cached** | **list** *aaa-listname* [*aaa-username* | **name-mangler** *mangler-name*]}
- **aaa authorization user cert list** *aaa-listname* {*aaa-username* | **name-mangler** *mangler-name*}

例：

```
Device(config-ikev2-profile)# aaa authorization user eap cached
```

例：

```
Device(config-ikev2-profile)# aaa authorization user cert list list1 name-mangler mangler1
```

ユーザー認可用の AAA 方式リストとユーザー名を指定します。

- **user**：ユーザー認可を指定します。
- **cert**：ピアは証明書を使用して認証を受ける必要があることを指定します。
- **eap**：ピアは EAP を使用して認証を受ける必要があることを指定します。
- **psk**：ピアは事前共有キーを使用して認証を受ける必要があることを指定します。
- **cached**：EAP 認証中に受信した属性または AAA 事前共有キーから取得した属性をキャッシュする必要があることを指定します。
- *aaa-listname*：AAA 方式リスト名。
- *aaa-username*：AAA 認可要求で使用する必要があるユーザー名を指定します。
- **name-mangler**：ピア ID から AAA 認可ユーザー名を抽出する name mangler を指定します。
- *mangler-name*：使用する name mangler。

（注）
- **psk** 認証方式と **eap** 認証方式では、*aaa-username* 引数または **name-mangler** キーワードの指定は任意で、指定しなかった場合は、ピア ID がユーザー名として使用されます。
- **psk** 認証方式と **eap** 認証方式では、それぞれ、**cached** キーワードと **list** キーワードを使用して 2 つのユーザー認可用のバリアントを同時に設定できます。
- **cert** 認証ではタイプが識別名（DN）のピア ID を使用できないため、*aaa-username* 引数または **name-mangler** キーワードの指定が必須です。

ステップ 7 次のいずれかまたは両方を実行します。

- **aaa authorization group** [**override**] {**eap** | **psk**} **list** *aaa-listname* [*aaa-username* | **name-mangler** *mangler-name*]
- **aaa authorization group** [**override**] **cert list** *aaa-listname* {*aaa-username* | **name-mangler** *mangler-name*}

例：

```
Device(config-ikev2-profile)# aaa authorization group override psk list list1
```

例：

```
Device(config-ikev2-profile)# aaa authorization group cert list list1 name-mangler mangler1
```

グループ認可用の AAA 方式リストとユーザー名を指定します。

- **group**：グループ認可を指定します。
- **override**：（任意）属性のマージ中はグループ認可からの属性を優先する必要があることを指定します。デフォルトでは、ユーザー属性が優先されます。
- **cert**：ピアは証明書を使用して認証を受ける必要があることを指定します。
- **eap**：ピアは EAP を使用して認証を受ける必要があることを指定します。
- **psk**：ピアは事前共有キーを使用して認証を受ける必要があることを指定します。
- *aaa-listname*：AAA 方式リスト名。
- *aaa-username*：AAA 認可要求で使用する必要があるユーザー名。
- **name-mangler**：ピア ID から AAA 認可ユーザー名を抽出する name mangler を指定します。
- *mangler-name*：使用する name mangler。

（注）
- **psk** 認証方式と **eap** 認証方式では、*aaa-username* 引数または **name-mangler** キーワードの指定は任意で、指定しなかった場合は、ピア ID がユーザー名として使用されます。
- **psk** 認証方式と **eap** 認証方式では、それぞれ、**cached** キーワードと **list** キーワードを使用して 2 つのユーザー認可用のバリアントを同時に設定できます。
- **cert** 認証ではタイプが識別名（DN）のピア ID を使用できないため、*aaa-username* 引数または **name-mangler** キーワードの指定が必須です。

ステップ 8 **config-exchange** {**request** | **set** {**accept** | **send**}}

例：

```
Device(config-ikev2-profile)# config-exchange set accept
```

（任意）設定交換オプションを有効にします。

- **request**：設定交換要求を有効にします。
- **set**：設定交換要求セット オプションを有効にします。
- **accept**：設定交換要求セットを受け入れます。
- **send**：設定交換セットの送信を有効にします。

（注） デフォルトで、request オプションと set オプションが有効になります。

ステップ 9 **end**

例：

```
Device(config-ikev2-profile)# end
```

IKEv2 プロファイル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

IKEv2 名前分割の設定

このタスクを実行して、IKEv2名前分割を指定します。これを使用して認証要求の名前を生成し、AAA 事前共有キーを取得します。この名前は、リモート IKE ID または EAP ID の異なる形式の指定した部分から派生します。ここで指定した名前分割は、IKEv2プロファイルに結び付けられます。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ikev2 name-mangler** *mangler-name*
4. **dn** {**common-name** | **country** | **domain** | **locality** | **organization** | **organization-unit** | **state**}
5. **eap** {**all** | **dn** {**common-name** | **country** | **domain** | **locality** | **organization** | **organization-unit** | **state**} | **prefix** | **suffix** {**delimiter** {**.** | **@** | ****}}}
6. **email** {**all** | **domain** | **username**}
7. **fqdn** {**all** | **domain** | **hostname**}
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto ikev2 name-mangler** *mangler-name* 例： `Device(config)# crypto ikev2 name-mangler mangler1`	名前分割を定義し、IKEv2名前分割コンフィギュレーション モードを開始します。
ステップ 4	**dn** {**common-name** | **country** | **domain** | **locality** | **organization** | **organization-unit** | **state**} 例： `Device(config-ikev2-name-mangler)# dn state`	DN （識別名）タイプのリモートIDで、次のフィールドのいずれかから名前が派生します。 • **common-name** • **country** • **domain** • **locality** • **organization** • **organization-unit**

	コマンドまたはアクション	目的
		• **state**
ステップ 5	**eap** {**all** | **dn** {**common-name** | **country** | **domain** | **locality** | **organization** | **organization-unit** | **state**} | **prefix** | **suffix** {**delimiter** {**.** | **@** | \}}} 例： `Device(config-ikev2-name-mangler)# eap prefix delimiter @`	タイプが EAP（Extensible Authentication Protocol）のリモート ID から名前が派生します。 • **all**：EAP ID 全体から名前が派生します。 • **dn**：DN タイプのリモート EAP ID の次のフィールドのいずれかから名前が派生します。 • **common-name** • **country** • **domain** • **locality** • **organization** • **organization-unit** • **state** • **prefix**：EAP ID のプレフィックスから名前が派生します。 • **suffix**：EAP ID のサフィックスから名前が派生します。 • **delimiter** {**.** | **@** | \}：プレフィックスとサフィックスを分割する、EAP ID のデリミタを指定します。
ステップ 6	**email** {**all** | **domain** | **username**} 例： `Device(config-ikev2-name-mangler)# email username`	電子メール タイプのリモート ID から名前が派生します。 • **all**：電子メール タイプのリモート IKE ID 全体から名前が派生します。 • **domain**：リモート IKE ID のドメイン部分から名前が派生します。 • **username**：リモート IKE ID のユーザー名部分から名前が派生します。
ステップ 7	**fqdn** {**all** | **domain** | **hostname**} 例： `Device(config-ikev2-name-mangler)# fqdn domain`	タイプが FQDN（完全修飾ドメイン名）のリモート ID から名前が派生します。 • **all**：FQDN タイプのリモート IKE ID 全体から名前が派生します。 • **domain**：リモート IKE ID のドメイン部分から名前が派生します。

	コマンドまたはアクション	目的
		• **hostname**：リモート IKE ID のホスト名部分から名前が派生します。
ステップ 8	**end** 例： `Device(config-ikev2-name-mangler)# end`	IKEv2 名前分割コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

IKEv2 認証ポリシーの設定

このタスクを実行して、IKEv2 認証ポリシーを設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ikev2 authorization policy** *policy-name*
4. **aaa attribute list** *list-name*
5. **backup-gateway** *string*
6. **banner** *banner-text*
7. **configuration url** *url*
8. **configuration version** *version*
9. **def-domain** *domain-name*
10. **dhcp** { **giaddr** *ip-address* | **server** {*ip-address* | *hostname*} | **timeout** *seconds*}
11. [**ipv6**] **dns** *primary-server* [*secondary-server*]
12. **include-local-lan**
13. **ipsec flow-limit** *number*
14. **netmask** *mask*
15. **pfs**
16. [**ipv6**] **pool** *name*
17. **route set** { **interface** *interface* | **access-list** {*access-list-name* | *access-list-number* | **ipv6** *access-list-name*}}
18. **route accept any** [**tag** *value*] [**distance** *value*]
19. **route redistribute** *protocol* [**route-map** *map-name*]
20. **route set remote** { **ipv4** *ip-address mask* | **ipv6** *ip-address*/*mask*}
21. **smartcard-removal-disconnect**
22. **split-dns** *string*
23. **session-lifetime** *seconds*
24. **route set access-list** {*acl-number* | [**ipv6**] *acl-name*}
25. **wins** *primary-server* [*secondary-server*]
26. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto ikev2 authorization policy** *policy-name* 例： `Device(config)# crypto ikev2 authorization policy policy1`	IKEv2 認証ポリシーを指定して、IKEv2 認証ポリシー設定モードを開始します。
ステップ 4	**aaa attribute list** *list-name* 例： `Device(config-ikev2-author-policy)# aaa attribute list list1`	AAA 属性のリストを指定します。 （注） このコマンドで参照されている AAA 属性リストは、グローバル コンフィギュレーション モードで定義する必要があります。
ステップ 5	**backup-gateway** *string* 例： `Device(config-ikev2-author-policy)# backup-gateway gateway1`	最大 10 台のバックアップ サーバー名を指定できます。このパラメータは、非標準 Cisco Unity コンフィギュレーション属性によってクライアントにプッシュされます。このパラメータは、クライアントが使用可能なバックアップ サーバーを指定します。
ステップ 6	**banner** *banner-text* 例： `Device(config-ikev2-author-policy)# banner This is IKEv2`	バナーを指定します。このパラメータは、非標準 Cisco Unity コンフィギュレーション属性によってクライアントに送信されます。
ステップ 7	**configuration url** *url* 例： `Device(config-ikev2-author-policy)# configuration url http://www.cisco.com`	コンフィギュレーション URL を指定します。このパラメータは、非標準 Cisco FlexVPN コンフィギュレーション属性によってクライアントに送信されます。クライアントはこの URL を使用して、コンフィギュレーションをダウンロードできます。
ステップ 8	**configuration version** *version* 例： `Device(config-ikev2-author-policy)# configuration version 2.4`	コンフィギュレーションバージョンを指定します。このパラメータは、非標準 Cisco FlexVPN コンフィギュレーション属性によってクライアントに送信されます。このパラメータは、コンフィギュレーション URL と送信され、クライアントがダウンロードできるバージョンを指定します。

	コマンドまたはアクション	目的
ステップ 9	**def-domain** *domain-name* 例： `Device(config-ikev2-author-policy)# def-domain cisco`	デフォルト ドメインを指定します。このパラメータは、非標準 Cisco Unity コンフィギュレーション属性によってクライアントに送信されます。このパラメータは、クライアントが使用可能なデフォルトドメインを指定します。
ステップ 10	**dhcp** { **giaddr** *ip-address* | **server** {*ip-address* | *hostname*} | **timeout** *seconds*} 例： `Device(config-ikev2-author-policy)# dhcp giaddr 192.0.2.1`	リモート アクセス クライアントに割り当てられる IP アドレスをリースする DHCP サーバーを指定します。 • **giaddr** *ip-address*：ゲートウェイ IP アドレス（giaddr）を指定します。 • **server** {*ip-address* | *hostname*}：DHCP サーバーの IP アドレスまたはホスト名を指定します。ホスト名は、設定時に解決されます。 • **timeout** *seconds*：DHCP サーバーからの応答待ち時間を秒単位で指定します。 （注） 指定できる DHCP サーバーは 1 つのみです。DHCP サーバーはグローバル ルーティング テーブル経由で到達可能なことが前提であるため、DHCP パケットはグローバル ルーティング テーブルに転送されます。
ステップ 11	[**ipv6**] **dns** *primary-server* [*secondary-server*] 例： `Device(config-ikev2-author-policy)# dns 198.51.100.1 198.51.100.100`	設定応答でクライアントに送信される、プライマリおよびセカンダリ ドメイン名サービス（DNS）サーバーの IP アドレスを指定します。 • **ipv6**：（オプション）DNS サーバーの IPv6 アドレスを指定します。IPv4 アドレスを指定するには、このキーワードなしでコマンドを実行します。 • *primary-server*：プライマリ DNS サーバーの IP アドレス。 • *secondary-server*：（任意）セカンダリ DNS サーバーの IP アドレス。
ステップ 12	**include-local-lan** 例： `Device(config-ikev2-author-policy)# include-local-lan`	ローカル LAN を含めます。このパラメータは、非標準 Cisco Unity コンフィギュレーション属性によってクライアントに送信されます。

	コマンドまたはアクション	目的
ステップ 13	**ipsec flow-limit** *number* 例： `Device(config-ikev2-author-policy)# ipsec flow-limit 12500`	IKEv2 応答側の IKEv2 dVTI セッションが使用できる IPSec SAS の最大数を指定します。範囲は 0 ～ 50000 です。 デフォルトではコマンドは無効であり、dVTI セッションあたりの IPSec フローの数に制限はありません。値 0 では、IPSec SA は許可されません。
ステップ 14	**netmask** *mask* 例： `Device(config-ikev2-author-policy)# netmask 255.255.255.0`	クライアントに IP アドレスを割り当てるサブネットのネットマスクを指定します。 • *mask*：サブネット マスク アドレス。
ステップ 15	**pfs** 例： `Device(config-ikev2-author-policy)# pfs`	パスワード転送セキュリティ（PFS）を有効にします。このパラメータは、非標準 Cisco Unity コンフィギュレーション属性によってクライアントに送信されます。このパラメータは、クライアントで PFS を使用する必要性を指定します。
ステップ 16	[**ipv6**] **pool** *name* 例： `Device(config-ikev2-author-policy)# pool abc`	リモート アクセス クライアントに IP アドレスを割り当てるためのローカル IP アドレス プールを定義します。 • **ipv6**：（オプション）IPv6 アドレス プールを指定します。IPv4 アドレスを指定するには、このキーワードなしでコマンドを実行します。 • *name*：ローカル IP アドレス プールの名前。 （注） **ip local pool** コマンドを使用してすでに定義されているローカル IP アドレス プールを使用する必要があります。
ステップ 17	**route set** { **interface** *interface* | **access-list** {*access-list-name* | *access-list-number* | **ipv6** *access-list-name*}} 例： `Device(config-ikev2-author-policy)# route set interface`	コンフィギュレーションモードでピアに向かうルート設定パラメータを指定し、Border Gateway Protocol（BGP） over VPN などのルーティング プロトコルを実行できます。 • **interface**：ルート インターフェイスを指定します。 • **access-list**：ルート アクセス リストを指定します。 • *access-list-name*：アクセス リストの名前。 • *access-list-number*：標準のアクセス リスト番号。

	コマンドまたはアクション	目的
		• **ipv6**IPv6 アクセス リストを指定します。
ステップ 18	**route accept any** [**tag** *value*] [**distance** *value*] 例： `Device(config-ikev2-author-policy)# route accept any tag 10`	ピアから受信したルートをフィルタリングし、それらのルートをインストールするためにタグとメトリック値を指定します。 • **any**：ピアから受信したすべてのルートを受け入れます。 • **tag** *value*：（オプション）IKEv2 によって追加された静的ルートのタグ ID を指定します。範囲は 1 ～ 497777 です。 • **distance** *value*：（オプション）IKEv2 によって追加された静的ルートの距離を指定します。範囲は 1 ～ 255 です。
ステップ 19	**route redistribute** *protocol* [**route-map** *map-name*] 例： `Device(config-ikev2-author-policy)# route redistribute connected`	ピアから受信したルートをフィルタリングし、それらのルートをインストールするためにタグとメトリック値を指定します。 • *protocol*：ルートの再配布元のプロトコルです。connected または static のいずれかのキーワードを指定できます。 • **route-map** *map-name*：（オプション）ソース ルーティング プロトコルから別のルーティング プロトコルにルートをインポートするためにフィルタ処理する必要があるルートマップ。マップ名を指定しないと、すべてのルートが再配布されます。
ステップ 20	**route set remote** { **ipv4** *ip-address mask* | **ipv6** *ip-address/mask*} 例： `Device(config-ikev2-author-policy)# route set remote ipv6 2001:DB8::1/32`	内部ネットワークの IP アドレスを設定します。
ステップ 21	**smartcard-removal-disconnect** 例： `Device(config-ikev2-author-policy)# smartcard-removal-disconnect`	スマートカードの取り外しと切断を有効にします。このパラメータは、非標準 Cisco Unity コンフィギュレーション属性によってクライアントに送信されます。このパラメータでは、スマート カードが取り外された場合に、クライアントがセッションを停止する必要があることを指定します。

	コマンドまたはアクション	目的
ステップ 22	**split-dns** *string* 例： `Device(config-ikev2-author-policy)# split-dns abc1`	最大 10 台の分割ドメイン名を指定できます。このパラメータは、非標準Cisco Unityコンフィギュレーション属性によってクライアントに送信されます。このパラメータは、クライアントがプライベートネットワークに使用する必要があるドメイン名を指定します。
ステップ 23	**session-lifetime** *seconds* 例： `Device(config-ikev2-author-policy)# session-lifetime 1000`	IKEv2 セッションのライフタイムを指定します。 • **seconds** *seconds*：範囲は 120 ～ 25920000 で、2 分間～ 300 日間に変換されます。
ステップ 24	**route set access-list** {*acl-number* | [**ipv6**] *acl-name*} 例： `Device(config-ikev2-client-config-group)# route set access-list 110`	コンフィギュレーション モードを介してリモートピアにプッシュされるサブネットを指定します。 • *acl-number*：アクセス リスト番号（ACL）。ACL 番号は IPv4 ACL にのみ指定できます。 • **ipv6**：（オプション）IPv6アクセスコントロール リスト（ACL）を指定します。IPv4 属性を指定するには、このキーワードなしでコマンドを実行します。 • *acl-name*：アクセス リスト名。 （注） IPv4 アドレスに標準の、シンプルなアクセス リストのみを指定できます。
ステップ 25	**wins** *primary-server* [*secondary-server*] 例： `Device(config-ikev2-author-policy)# wins 203.0.113.1 203.0.113.115`	設定応答でクライアントに送信される、内部の Windows Internet Naming Service（WINS）サーバーアドレスを指定します。 • *primary-server*：プライマリ WINS サーバーの IP アドレス。 • *secondary-server*：（任意）セカンダリ WINS サーバーの IP アドレス。
ステップ 26	**end** 例： `Device(config-ikev2-author-policy)# end`	IKEv2 認証ポリシー設定モードを終了し、特権 EXEC モードに戻ります。

FlexVPN サーバーの構成例

例：FlexVPN サーバーの設定

例：EAP を使用してピアを認証するための FlexVPN サーバーの設定

この例では、EAPを使用してピアを認証するため、FlexVPNサーバーを設定する方法を示します。

```
aaa new-model
!
aaa group server radius eap-server
 server 192.168.2.1
!
aaa authentication login eap-list group eap-server
!
crypto pki trustpoint trustpoint1
 enrollment url http://192.168.3.1:80
 revocation-check crl
!
crypto ikev2 profile ikev2-profile1
 match identity remote address 0.0.0.0
 authentication local rsa-sig
 authentication remote eap query-identity
 pki trustpoint trustpoint1
 aaa authentication eap eap-list
 virtual-template 1
!
crypto ipsec transform-set transform1 esp-aes esp-sha-hmac
!
crypto ipsec profile ipsec-profile1
 set transform-set trans transform1
 set ikev2-profile ikev2-profile1
!
interface Ethernet0/0
 ip address 192.168.1.1 255.255.255.0
!
interface Virtual-Template1 type tunnel
 ip unnumbered Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile ipsec-profile1
!
radius-server host 192.168.2.1 key key1
!
```

例：グループ認証のための FlexVPN サーバーの設定（外部 AAA）

次の例は、グループ認証用に FlexVPN サーバーを設定する方法を示します。認証は RADIUS または TACACS サーバーである外部 AAA を通じて行います。

```
aaa new-model
!
aaa group server radius cisco-acs
 server 192.168.2.2
```

```
!
aaa authorization network group-author-list group cisco-acs
!
crypto pki trustpoint trustpoint1
 enrollment url http://192.168.3.1:80
 revocation-check crl
!
crypto pki certificate map certmap1 1
 subject-name co cisco
!
crypto ikev2 name-mangler group-author-mangler
 dn domain
!
crypto ikev2 profile ikev2-profile1
 match certificate certmap1
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint trustpoint1
 aaa authorization group cert list group-author-list name-mangler group-author-mangler
 virtual-template 1
!
crypto ipsec transform-set transform1 esp-aes esp-sha-hmac
!
crypto ipsec profile ipsec-profile1
 set transform-set trans transform1
 set ikev2-profile ikev2-profile1
!
interface Ethernet0/0
 ip address 192.168.1.1 255.255.255.0
!
interface Virtual-Template1 type tunnel
 ip unnumbered Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile ipsec-profile1
!
radius-server host 192.168.2.2 key key2
!
```

例：グループ認証のための FlexVPN サーバーの設定（ローカル AAA）

次の例は、グループ認証用に FlexVPN サーバーを設定する方法を示します。認証は、IKEv2 認証ポリシーを使用するローカル AAA を通じて行います。認証ポリシーでは、コンフィギュレーション モードでクライアントに送信する、標準の IPv4 および IPv6 属性、Cisco Unity、FlexVPN 属性を指定します。また、認証ポリシーは、ローカル使用に対して、**aaa attribute list** コマンドによってユーザー属性ごとに指定します。

```
aaa new-model
!
aaa authorization network local-group-author-list local
!
!
aaa attribute list attr-list1
 attribute type interface-config "ip mtu 1100"
 attribute type interface-config "tunnel key 10"
!

crypto pki trustpoint trustpoint1
 enrollment url http://192.168.3.1:80
 revocation-check crl
!
crypto pki certificate map certmap1 1
```

```
 subject-name co cisco
!
crypto ikev2 authorization policy author-policy1
 pool pool1
 dhcp server 192.168.4.1
 dhcp timeout 10
 dhcp giaddr 192.168.1.1
 dns 10.1.1.1 10.1.1.2
 route set access-list acl1
 wins 192.168.1.2 192.168.1.3
 netmask 255.0.0.0
 banner ^C flexvpn server ^C
 configuration url http://www.abc.com
 configuration version 10
 def-domain abc.com
 split-dns dns1
 split-dns dns2
 split-dns dns3
 backup-gateway gw1
 backup-gateway gw2
 backup-gateway gw3
 smartcard-removal-disconnect
 include-local-lan
 pfs
 aaa attribute list attr-list1
!
crypto ikev2 profile ikev2-profile1
 match certificate certmap1
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint trustpoint1
 aaa authorization group cert list local-group-author-list author-policy1
 virtual-template 1
!
crypto ipsec transform-set transform1 esp-aes esp-sha-hmac
!
crypto ipsec profile ipsec-profile1
 set transform-set trans transform1
 set ikev2-profile ikev2-profile1
!
interface Ethernet0/0
 ip address 192.168.1.1 255.255.255.0
!
interface Virtual-Template1 type tunnel
 ip unnumbered Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile ipsec-profile1
!
ip local pool pool11 192.168.2.10 192.168.2.100
!
ip access-list extended acl-1
 permit ip 192.168.3.10 192.168.4.100 any
 permit ip 192.168.10.1 192.168.10.100 any
!
```

例：ユーザー認証のための FlexVPN サーバーの設定

次の例は、ユーザー認証用に FlexVPN サーバーを設定する方法を示します。

```
aaa new-model
!
aaa group server radius cisco-acs
```

```
 server 192.168.2.2
!
aaa authorization network user-author-list group cisco-acs
!
crypto pki trustpoint trustpoint1
 enrollment url http:// 192.168.3.1:80
 revocation-check crl
!
crypto pki certificate map certmap1 1
 subject-name co cisco
!
crypto ikev2 name-mangler user-author-mangler
 dn common-name
!
crypto ikev2 profile ikev2-profile1
 match certificate certmap1
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint trustpoint1
 aaa authorization user cert list user-author-list name-mangler user-author-mangler
 virtual-template 1
!
crypto ipsec transform-set transform1 esp-aes esp-sha-hmac
!
crypto ipsec profile ipsec-profile1
 set transform-set trans transform1
 set ikev2-profile ikev2-profile1
!
interface Ethernet0/0
 ip address 192.168.1.1 255.255.255.0
!
interface Virtual-Template1 type tunnel
 ip unnumbered Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile ipsec-profile1
!
radius-server host 192.168.2.2 key key2
!
```

例：IPv6 設定属性による IPv6 セッション用の FlexVPN サーバーの設定

次の例に、IPv6 ダイナミック仮想トンネルインターフェイス（dVTI）セッション用に FlexVPN サーバーを設定する方法を示します。この例では、IKEv2 認証ポリシーを使用するローカル AAA グループ認証を使用します。IPv6 設定属性は、IKEv2 認証ポリシーの下で設定されます。

```
aaa new-model
!
aaa authorization network local-group-author-list local
!
crypto pki trustpoint trustpoint1
 enrollment url http://192.168.3.1:80
 revocation-check crl
!
crypto pki certificate map certmap1 1
 subject-name co cisco
!
crypto ikev2 authorization policy author-policy1
 ipv6 pool v6-pool
 ipv6 dns 2001:DB8:1::11 2001:DB8:1::12
 ipv6 subnet-acl v6-acl
!
crypto ikev2 profile ikev2-profile1
```

```
 match certificate certmap1
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint trustpoint1
 aaa authorization group cert list local-group-author-list author-policy1
 virtual-template 1
!
crypto ipsec transform-set transform1 esp-aes esp-sha-hmac
!
crypto ipsec profile ipsec-profile1
 set transform-set trans transform1
 set ikev2-profile ikev2-profile1
!
interface Ethernet0/0
 ipv6 address 2001:DB8:1::1/32
!
interface Virtual-Template1 type tunnel
 ipv6 unnumbered Ethernet0/0
 tunnel mode ipsec ipv6
 tunnel protection ipsec profile ipsec-profile1
!
ipv6 local pool v6-pool 2001:DB8:1::10/32 48
!
ipv6 access-list v6-acl
 permit ipv6 host 2001:DB8:1::20 any
 permit ipv6 host 2001:DB8:1::30 any
!
```

例：AnyConnect プロファイルのダウンロードの設定

次の例は、FlexVPN AnyConnectプロファイルのダウンロード機能を設定する方法を示します。

（注） AnyConnect クライアント マシン上のローカル ポリシー ファイルは変更しません。IKEv2 で AnyConnectプロファイルのダウンロード機能を設定すると、必要なXMLプロファイルがクライアント デバイスに自動的にダウンロードされます。

（注） プロファイルダウンロード機能に対して、HTTPS サーバー（ip http secure-server）または SSL ポリシー（crypto ssl policy）のいずれかを無効にする必要があります。これらの機能の両方が同時に有効になっている場合に、デバイスが着信 SSL VPN 接続を受信すると、デバイスがクラッシュする可能性があります。

```
no ip http secure-server
crypto ssl policy ssl-policy
  pki trustpoint CA1 sign
  ip address local 10.0.0.1 port 443
  no shutdown
crypto ssl profile ssl_prof
    match policy ssl-policy
crypto vpn anyconnect profile ANY-PROF bootflash:profile.xml
crypto ikev2 profile ikev2_profile
    anyconnect profile ANY-PROF
```

FlexVPN サーバーの設定に関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
セキュリティ コマンド	• 『Cisco IOS Security Command Reference Commands A to C』 • 『Cisco IOS Security Command Reference Commands D to L』 • 『Cisco IOS Security Command Reference Commands M to R』 • 『Cisco IOS Security Command Reference Commands S to Z』
Cisco AnyConnect Secure Mobility Client	https://www.cisco.com/c/en/us/support/security/anyconnect-secure-mobility-client/tsd-products-support-series-home.html
IPsec の設定	『*Configuring Security for VPNs with IPsec*』
推奨される暗号化アルゴリズム	『Next Generation Encryption』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

FlexVPN サーバーの設定の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだ

けを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *4 : FlexVPN* サーバーの設定の機能情報

機能名	リリース	機能情報
リモート アクセス クライアントの IKEv2 ヘッドエンド サポート	Cisco IOS XE Release 3.5S	この機能は、Anyconnect 3.0、FlexVPN ハードウェア クライアント、および VTI のマルチ SA サポートに対する IKEv2 をサポートします。 次のコマンドが導入または変更されました。 **aaa attribute list, backup-gateway, banner, config-mode set, configuration url, configuration version, def-domain, dhcp, dns, include-local-lan, max flow limit, pfs, pool, route accept, route set interface, smartcard-removal-disconnect, split-dns, subnet-acl.**

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。