集約認証の設定

FlexVPN RA - Cisco AnyConnect クライアントのサポートを拡張することで、AnyConnect 機能の集約認証サポートは、集約認証方式を実装します。このクライアントでは、独自の AnyConnect EAP 認証方式を使用し、Cisco AnyConnect クライアントと FlexVPN サーバー間にインターネットを介したセキュア トンネルを確立します。

集約認証の設定の前提条件

- <BypassDownloader> 値を true に設定して、AnyConnectLocalPolicy ファイルで BypassDownloader 関数を有効にする必要があります。デバイスで SSL がサポートされていない場合、BypassDownloader 関数は動作しないため、<BypassDownloader> 値を false に設定して、この関数を無効にする必要があります。そうしないと、接続が失敗します。

集約認証の設定に関する情報

Cisco AnyConnect および FlexVPN

VPN 接続を確立するには、VPN クライアントが Extensible Authentication Protocol（EAP：拡張可能認証プロトコル）、拡張認証（XAUTH）などの認証方式を使用してユーザー クレデンシャルを取得し、Access Control Server を接続するハブにユーザー クレデンシャルを転送する必要があります。Access Control Server は、外部データベースまたは Active Directory（AD）を送信してクレデンシャルを確認します。

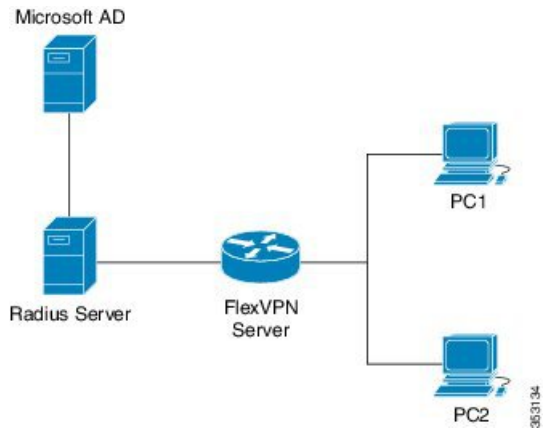
FlexVPN サーバーは（ハブとして）Cisco Secure Access Control Server と連動してユーザー クレデンシャルを確認し、VPN 接続を確立します。ただし、Cisco AnyConnect は EAP を使用してユーザー クレデンシャルを取得し、XAUTH をサポートしません。一方、Cisco Secure Access Control Server は外部データベース（ここでは AD）を使用する EAP-MD5 をサポートしません。これによって、Cisco Secure Access Control Server が EAP-MD5 をサポートする必要があるシナリオ、または FlexVPN が Cisco AnyConnect からの情報を個別に認証して、Cisco Secure Access Control Server に個別に接続する必要があるシナリオが生じます。FlexVPN は、集約認証方式を使用して、Cisco AnyConnect からの情報を認証できます。FlexVPN サーバーで集約認証方式を実装すると、Cisco IOS ソフトウェアにより多くの機能サポートを追加するためのウィンドウが提供されます。

FlexVPN RA：AnyConnect の集約認証サポート機能では、独自の AnyConnect EAP 認証方式を使用する Cisco AnyConnect クライアントのサポートを拡張することによって集約認証方式を実装し、Cisco AnyConnect サーバーや FlexVPN サーバーを使用してインターネット上にセキュアなトンネルを確立します。 これは、サーバー固有の機能で、Cisco AnyConnect と連動します。

集約認証の動作

インターネット キー エクスチェンジ バージョン 2 は、基本的な集約認証を実装することによって独自の AnyConnect EAP 認証方式を使用する Cisco AnyConnect をサポートします。ここでの認証は、リモート RADIUS サーバーを使用する認証、認可、およびアカウンティング（AAA）を介して実行されます。次に、Cisco IOS ソフトウェアでの集約認証の実装を説明するネットワーク トポロジの例を示します。

図 *1 : RADIUS* サーバーに接続された *FlexVPN* サーバー



この図は、次のことを示しています。

- Cisco Secure Access Control Server は、認証用の RADIUS サーバーとして機能します。
- クレデンシャルは、認証用の Active Directory として機能する Microsoft Active Directory に格納されます。

（注） Microsoft Active Directory は、単なる例です。クレデンシャルの格納場所は重要ではありません。

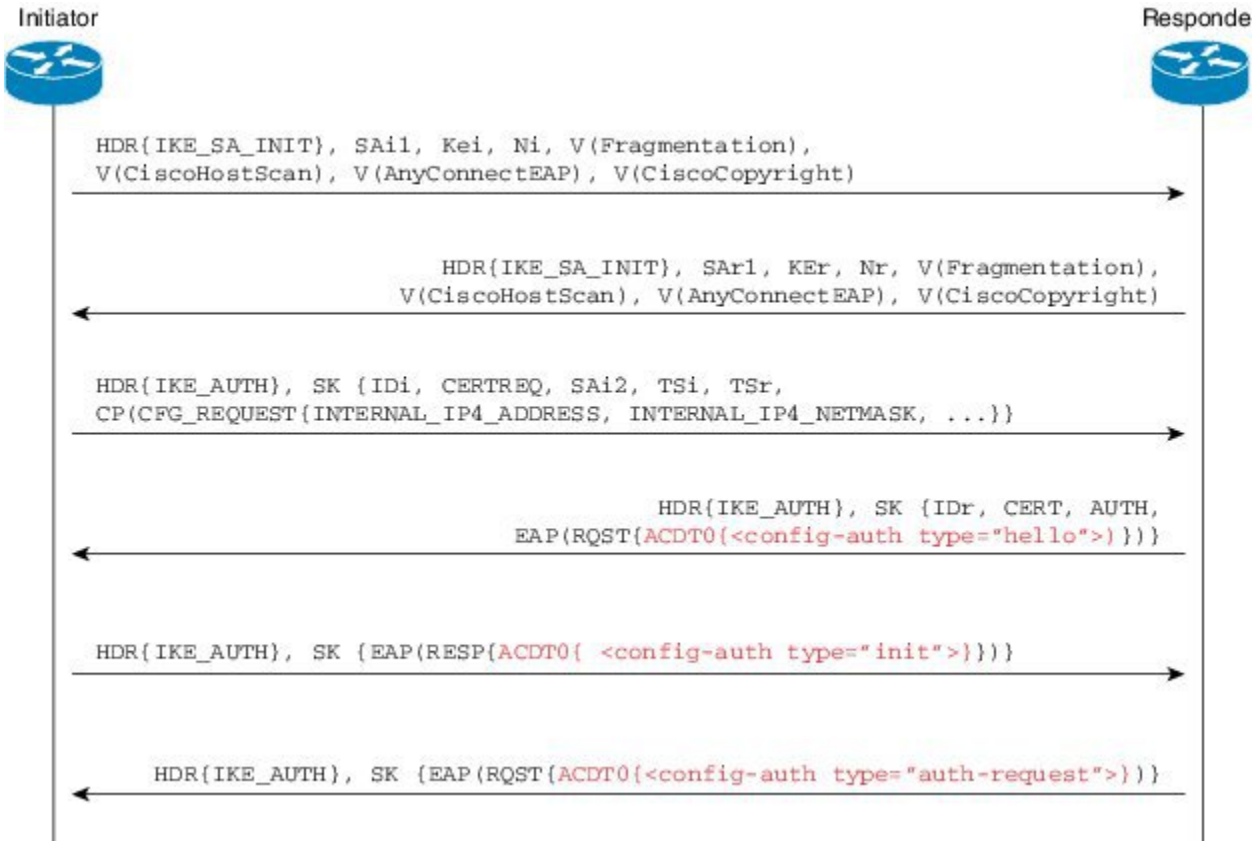
- シスコ デバイスは、FlexVPN サーバーとして機能します。
- Windows 7 PC は、Cisco AnyConnect クライアントとして機能します。

1. VPN 接続を開始するために、Cisco AnyConnect クライアントは証明書を使用して FlexVPN サーバーを確認します。
2. 証明書を確認した後、Cisco AnyConnect クライアントは Cisco AnyConnect EAP がロードしたメッセージを FlexVPN サーバーに送信します。
3. FlexVPN サーバーが Cisco AnyConnect から Cisco AnyConnect EAP がロードしたメッセージを受信すると、FlexVPN サーバーはメッセージをダウンロードして EAP のメッセージを除去します。
4. FlexVPN は認証用の RADIUS サーバーおよび認証用の Microsoft Active Directory（AD）との接続を確立して、除去されたメッセージを転送し、Cisco AnyConnect クライアントから提供されたクレデンシャルを確認します。
5. クレデンシャルが RADIUS サーバーおよび Microsoft Active Directory（AD）によって確認されて承認されると、適切な応答が FlexVPN サーバーに送信され、Cisco AnyConnect に応答し、VPN 接続が確立されます。

Cisco AnyConnect EAP を使用する IKE 交換

AnyConnect EAP を使用する IKE での認証は、RFC 3748 で説明されているように標準 EAP モデルのバリエーションです。AnyConnect EAP を使用すると、パブリック設定または認証 XML は EAP ペイロードを介して送信されます。次の図に、Cisco AnyConnect によって使用される一般的なメッセージ フローを示します。

図 *2 : AnyConnect EAP* を使用する *IKE* 交換



1. Cisco AnyConnect クライアントが、FlexVPN サーバーへの IKE 接続を開始します。クライアントは、一般的な IKE ペイロードに加えて、Cisco AnyConnect EAP のサポートを示すためのベンダー ID ペイロードを送信します。クライアントは、シスコの著作権ベンダー ID を含めることによって自身をシスコ製品として識別します。
2. サーバー ゲートウェイが、フラグメンテーションおよび AnyConnect EAP サポートを示すためのベンダー ID ペイロードを送信し、シスコの著作権ベンダー ID を含めることによって自身をシスコ製品として識別します。
3. 設定ペイロードで、トンネル設定が要求されます。クライアントは、このメッセージから AUTH ペイロードを省略することによって、Cisco AnyConnect EAP 認証の使用を希望していることを示します。
4. 集約認証および設定プロトコルが、EAP を介して伝送されます。
5. FlexVPN サーバーが、EAP の成功メッセージを送信します。
6. Cisco AnyConnect クライアントが、AUTH ペイロードを送信します。
7. FlexVPN サーバーが、AUTH ペイロードと Cisco AnyConnect クライアントが要求したトンネル設定属性を送信します。

IKEv2 でのデュアルファクタ認証のサポート

Cisco IOS ソフトウェアでの集約認証の実装は、デュアルファクタ認証に拡張できます。二重認証は、デバイス証明書情報を交換し検証する集約認証中に、新しい AnyConnect EAP 交換を導入することで実行されます。「デバイス」と同様に「ユーザー」も認証するこのメカニズムは、「二重認証」と呼ばれます。

（注） AnyConnect EAP は、AnyConnect クライアント固有の認証方式であり、他クライアントには適用されません。

集約認証の設定方法

集約認証用の FlexVPN サーバーの設定

このタスクを実行して、FlexVPN サーバーの集約認証を設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ikev2 profile** *profile-name*
4. **aaa accounting anyconnect-eap** *list-name*
5. **match identity remote key-id** *opaque-string*
6. **authentication remote anyconnect-eap aggregate** [**cert-request**]
7. **authentication local rsa-sig**
8. **pki trustpoint** *trustpoint-label*
9. **aaa authentication anyconnect-eap** *list-name*
10. **aaa authorization group anyconnect-eap list** *aaa-listname* **name-mangler** *mangler-name*
11. **aaa authorization user anyconnect-eap cached**
12. **aaa authorization user anyconnect-eap list** *aaa-listname* **name-mangler** *mangler-name*
13. **end**
14. **show crypto ikev2 session detailed**

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）。

	コマンドまたはアクション	目的
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 profile** *profile-name* 例： `Device(config)# crypto ikev2 profile profile1`	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。
ステップ 4	**aaa accounting anyconnect-eap** *list-name* 例： `Device(config-ikev2-profile)# aaa accounting anyconnect-eap list1`	IKEv2 リモート認証方式が AnyConnect EAP の場合、認証、認可、およびアカウンティング（AAA）のアカウンティング方式リストを有効にします。
ステップ 5	**match identity remote key-id** *opaque-string* 例： `Device(config-ikev2-profile)# match identity remote key-id aggauth_user3@abc.com`	リモート キー ID タイプの ID に基づいて、プロファイルを照合します。
ステップ 6	**authentication remote anyconnect-eap aggregate** [**cert-request**] 例： `Device(config-ikev2-profile)# authentication remote anyconnect-eap aggregate cert-request`	Cisco AnyConnect EAP に集約認証を指定します。 • **cert-request** ：二重認証用に Cisco AnyConnect クライアントに証明書を要求します。
ステップ 7	**authentication local rsa-sig** 例： `Device(config-ikev2-profile)# authentication local rsa-sig`	Rivest、Shamir、Adelman（RSA）署名をローカル認証方式として指定します。
ステップ 8	**pki trustpoint** *trustpoint-label* 例： `Device(config-ikev2-profile)# pki trustpoint CA1`	RSA 署名認証方式で使用する Public Key Infrastructure（PKI）トラストポイントを指定します。
ステップ 9	**aaa authentication anyconnect-eap** *list-name* 例： `Device(config-ikev2-profile)# aaa authentication anyconnect-eap list1`	Cisco AnyConnect EAP 認証用に、認証、認可、およびアカウンティング（AAA）認証リストを指定します。 • **anyconnect-eap**：AAA AnyConnect EAP 認証を指定します。 • *list-name*：AAA 認証リスト名。
ステップ 10	**aaa authorization group anyconnect-eap list** *aaa-listname* **name-mangler** *mangler-name* 例：	リモート認証方式が AnyConnect EAP であり、名前分割が派生する場合、各グループ ポリシーに AAA 認証を指定します。

	コマンドまたはアクション	目的
	`Device(config-ikev2-profile)# aaa authorization group anyconnect-eap list list1 name-mangler mangler1`	
ステップ 11	**aaa authorization user anyconnect-eap cached** 例： `Device(config-ikev2-profile)# aaa authorization user anyconnect-eap cached`	リモート認証方式が AnyConnect EAP であり、AnyConnect EAP 認証からキャッシュした属性を使用する場合、各ユーザーポリシーにAAA認証を指定します。
ステップ 12	**aaa authorization user anyconnect-eap list** *aaa-listname* **name-mangler** *mangler-name* 例： `Device(config-ikev2-profile)# aaa authorization user anyconnect-eap list list1 name-mangler mangler1`	リモート認証方式に AAA 方式リストを指定し、名前分割が派生します。
ステップ 13	**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。
ステップ 14	**show crypto ikev2 session detailed** 例： `Device# show crypto ikev2 session detailed`	アクティブなインターネット キー エクスチェンジ バージョン 2（IKEv2）セッションのステータスを表示します。

集約認証の設定例

例：集約認証の設定

次の例は、FlexVPN サーバーで集約認証を設定する方法を示します。これによって、Cisco AnyConnect クライアントと FlexVPN サーバー間のセキュア トンネルの確立を有効にします。

```
Device> enable
Device# configure terminal
Device(config)# crypto ikev2 profile profile1
Device(config-ikev2-profile)# aaa accounting anyconnect-eap list1
Device(config-ikev2-profile)# match identity remote key-id aggauth_user1@example.com
Device(config-ikev2-profile)# authentication remote anyconnect-eap aggregate cert-request
Device(config-ikev2-profile)# authentication local rsa-sig
Device(config-ikev2-profile)# pki trustpoint CA1
Device(config-ikev2-profile)# aaa authentication anyconnect-eap list1
Device(config-ikev2-profile)# aaa authorization group anyconnect-eap list list1
name-mangler mangler1
Device(config-ikev2-profile)# aaa authorization user anyconnect-eap cached
Device(config-ikev2-profile)# aaa authorization user anyconnect-eap list list1 name-mangler
 mangler1
Device(config-ikev2-profile)# end
```

集約認証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』

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

集約認証の設定に関する機能情報

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 *1*：集約認証の設定に関する機能情報

機能名	リリース	機能情報
IKEv2 でのデュアルファクタ認証のサポート		IKEv2 でのデュアルファクタ認証のサポートは、二重認証への Cisco AnyConnect クライアントからの証明書要求をサポートします。 **authentication (IKEv2 profile)** コマンドが変更されました。
FlexVPN RA - AnyConnect の集約認証サポート		FlexVPN RA - Cisco AnyConnect クライアントのサポートを拡張することで、AnyConnect 機能の集約認証サポートは、集約認証方式を実装します。このクライアントでは、独自の AnyConnect EAP 認証方式を使用し、Cisco AnyConnect クライアントと FlexVPN サーバー間にインターネットを介したセキュア トンネルを確立します。 次のコマンドが導入または変更されました。**aaa accounting (IKEv2 profile)**、**aaa authentication (IKEv2 profile)**、**aaa authorization (IKEv2 profile)**、**authentication (IKEv2 profile)**、**show crypto ikev2 profile**、**show crypto ikev2 session**

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。