Configuring Aggregate Authentication

The FlexVPN RA - Aggregate Auth Support for AnyConnect feature implements aggregate authentication method by extending support for Cisco AnyConnect client that uses the proprietary AnyConnect EAP authentication method to establish a secure tunnel over the Internet between Cisco AnyConnect client and FlexVPN server.

Prerequisites for Configuring Aggregate Authentication

- You must enable the BypassDownloader function in the AnyConnectLocalPolicy file by setting the <BypassDownloader> value to true. If your device does not support SSL, the BypassDownloader function will not work.You must disable the function manually by setting the <BypassDownloader> value to false, else the connection will fail.

Information for Configuring Aggregate Authentication

Cisco AnyConnect and FlexVPN

To establish a VPN connection, the VPN client must obtain user credentials using authentication methods such as, extensible authentication protocol (EAP), Extended Authentication (XAUTH), etc. and forward the user credentials to a hub, which contacts an access control server. The access control server sends an external database or active directory (AD) to validate the credentials.

FlexVPN server (as a hub) works with Cisco Secure Access Control Server to validate user credentials to establish VPN connections. However, Cisco AnyConnect uses EAP to obtain user credentials and does not support XAUTH. On the other hand, Cisco Secure Access Control Server does not support EAP-MD5 with external database (in this case AD). This leads to a scenario where either Cisco Secure Access Control Server must support EAP-MD5 or FlexVPN must authenticate the information from Cisco AnyConnect separately and connect separately with Cisco Secure Access Control Server. FlexVPN can use the Aggregate

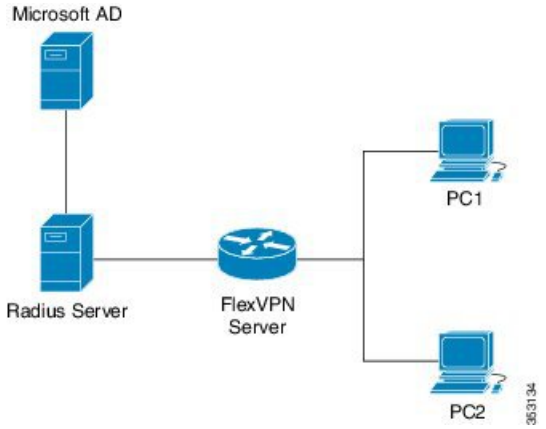
Authentication method to authentication information from Cisco AnyConnect. Implementing aggregate authentication method on FlexVPN server would provide a window to add more feature support on Cisco IOS software.

The FlexVPN RA - Aggregate Auth Support for AnyConnect feature implements aggregate authentication method by extending support for Cisco AnyConnect client that uses the proprietary AnyConnect EAP authentication method to establish a secure tunnel over the Internet using Cisco AnyConnect and FlexVPN server. This is a server-specific feature and works with Cisco AnyConnect.

How Aggregate Authentication Works

Internet Key Exchange Version 2 supports Cisco AnyConnect that uses the proprietary AnyConnect EAP authentication method by implementing basic aggregate authentication where authentication is performed via authentication, authorization, and accounting (AAA) using the remote RADIUS server. The following is an example of a network topology explains aggregate authentication implementation on Cisco IOS software.

Figure 1: FlexVPN Server Connected to RADIUS Server



In this diagram:

- Cisco Secure Access Control Server acts as a RADIUS server for authorization.
- The credentials are stored in Microsoft Active Directory, which acts as the active directory for authentication.

Note Microsoft Active Directory is referred for example purpose only. It does not matter where the credentials are stored.

- Cisco device acts as FlexVPN server.
- Windows 7 PC acts as Cisco AnyConnect client.

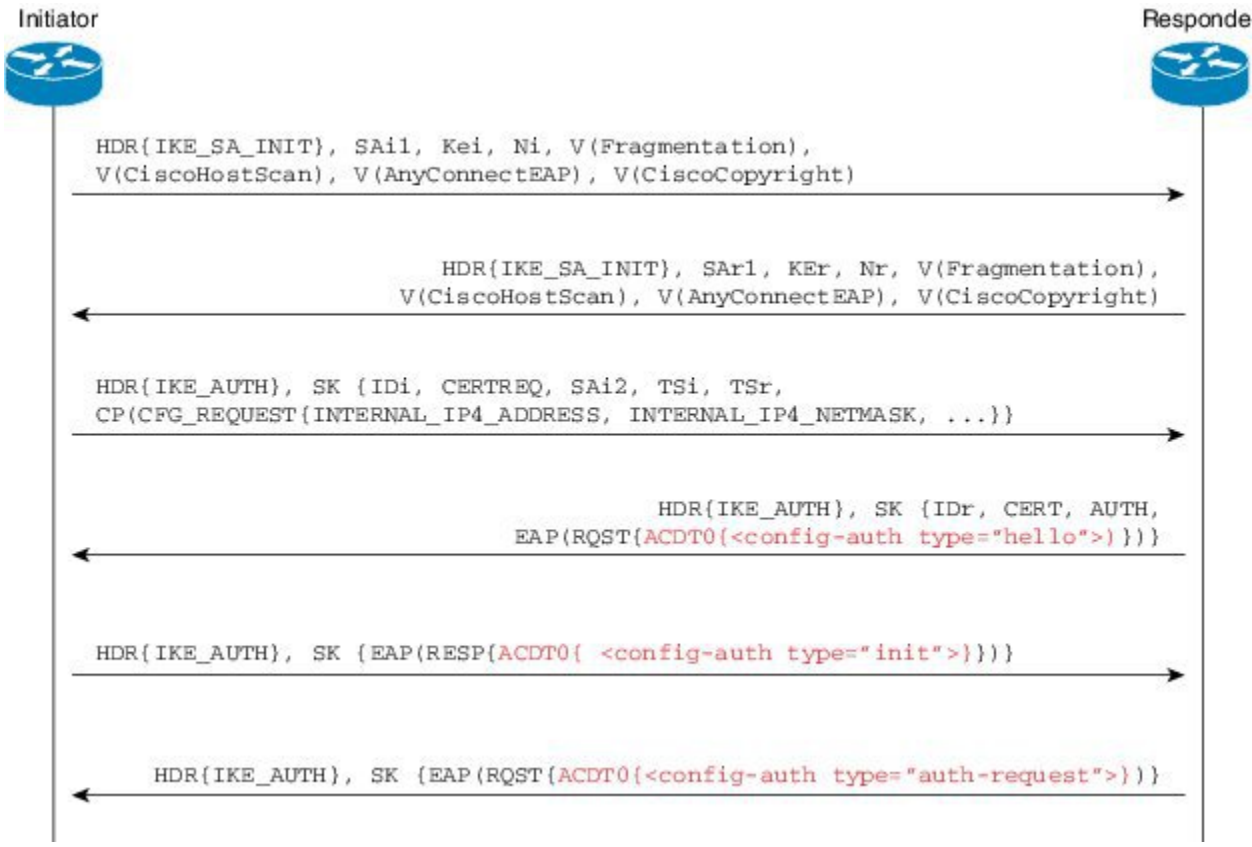
1. To initiate a VPN connection, Cisco AnyConnect client verifies a FlexVPN server using certifications.
2. After verifying the certificates, Cisco AnyConnect client sends Cisco AnyConnect EAP loaded message to FlexVPN server.

3. When FlexVPN server receives Cisco AnyConnect EAP loaded message from Cisco AnyConnect, FlexVPN server downloads the message and strips the message of EAP.
4. FlexVPN establishes a connection with RADIUS server for authorization and Microsoft Active Directory (AD) for authentication, and forwards the stripped message to verify the credentials provided by Cisco AnyConnect client.
5. When the credentials are verified and approved by RADIUS server and Microsoft Active Directory (AD), an appropriate reply is sent to FlexVPN server, which in turn replies to Cisco AnyConnect and a VPN connection is established.

IKE Exchanges Using Cisco AnyConnect EAP

Authentication in IKE using AnyConnect EAP is a variation of the standards EAP model as described in RFC 3748. When using AnyConnect EAP the public configuration or authentication XML is transported via EAP payloads. The following figure illustrates the typical message flow used by Cisco AnyConnect .

Figure 2: IKE Exchanges using AnyConnect EAP



1. Cisco AnyConnect client initiates IKE connection to FlexVPN server. The client sends vendor ID payloads to indicate support for Cisco AnyConnect EAP in addition to the typical IKE payloads. The client identifies itself as a Cisco product by including the Cisco copyright vendor ID.
2. The server gateway sends vendor ID payloads to indicate fragmentation and AnyConnect EAP support and identifies itself as a Cisco product by including the Cisco copyright vendor ID.

3. The configuration payload requests the tunnel configuration. The client indicates its desire to use Cisco AnyConnect EAP authentication by omitting the AUTH Payload from this message.
4. The Aggregate Authentication and Configuration protocol is carried over EAP
5. FlexVPN server sends a EAP success message.
6. Cisco AnyConnect client sends the AUTH payload.
7. FlexVPN server sends the AUTH payload and the tunnel configuration attributes that Cisco AnyConnect client requested.

Dual-Factor Authentication Support with IKEv2

The aggregate authentication implementation on Cisco IOS software can be extended for dual-factor authentication. Double authentication can be done by introducing new AnyConnect EAP exchange during Aggregate Authentication which exchange and validate the device certificate information. This mechanism of authenticating 'device' as well as 'user' is called 'Double Authentication'.

Note AnyConnect EAP is AnyConnect client specific authentication method and does not apply to any other client.

How to Configure Aggregate Authentication

Configuring the FlexVPN Server for Aggregate Authentication

Perform this task to configure aggregate authentication on the FlexVPN server.

SUMMARY STEPS

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**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**crypto ikev2 profile** *profile-name* **Example:** `Device(config)# crypto ikev2 profile profile1`	Defines an IKEv2 profile name and enters IKEv2 profile configuration mode.
Step 4	**aaa accounting anyconnect-eap** *list-name* **Example:** `Device(config-ikev2-profile)# aaa accounting anyconnect-eap list1`	Enables authentication, authorization, and accounting (AAA) accounting method lists when the IKEv2 remote authentication method is AnyConnect EAP.
Step 5	**match identity remote key-id** *opaque-string* **Example:** `Device(config-ikev2-profile)# match identity remote key-id aggauth_user3@abc.com`	Matches a profile based on the identity of the type remote key ID.
Step 6	**authentication remote anyconnect-eap aggregate** [**cert-request**] **Example:** `Device(config-ikev2-profile)# authentication remote anyconnect-eap aggregate cert-request`	Specifies aggregate authentication for Cisco AnyConnect EAP. • **cert-request** - requests certificate from Cisco AnyConnect client for double authentication.
Step 7	**authentication local rsa-sig** **Example:** `Device(config-ikev2-profile)# authentication local rsa-sig`	Specifies Rivest, Shamir, and Adelman (RSA) signature as the local authentication method.
Step 8	**pki trustpoint** *trustpoint-label* **Example:** `Device(config-ikev2-profile)# pki trustpoint CA1`	Specifies Public Key Infrastructure (PKI) trustpoints for use with the RSA signature authentication method.
Step 9	**aaa authentication anyconnect-eap** *list-name* **Example:** `Device(config-ikev2-profile)# aaa authentication anyconnect-eap list1`	Specifies authentication, authorization, and accounting (AAA) authentication list for Cisco AnyConnect EAP authentication. • **anyconnect-eap**—Specifies AAA AnyConnect EAP authentication. • *list-name*—The AAA authentication list name.

	Command or Action	Purpose
Step 10	**aaa authorization group anyconnect-eap list** *aaa-listname* **name-mangler** *mangler-name* **Example:** `Device(config-ikev2-profile)# aaa authorization group anyconnect-eap list list1 name-mangler mangler1`	Specifies the AAA authorization for each group policy when the remote authentication method is AnyConnect EAP and derives the name mangler.
Step 11	**aaa authorization user anyconnect-eap cached** **Example:** `Device(config-ikev2-profile)# aaa authorization user anyconnect-eap cached`	Specifies the AAA authorization for each user policy when the remote authentication method is AnyConnect EAP and uses cached attributes from the AnyConnect EAP authentication.
Step 12	**aaa authorization user anyconnect-eap list** *aaa-listname* **name-mangler** *mangler-name* **Example:** `Device(config-ikev2-profile)# aaa authorization user anyconnect-eap list list1 name-mangler mangler1`	Specifies the AAA method list for the remote authentication method and derives the name mangler.
Step 13	**end** **Example:** `Device(config-ikev2-profile)# end`	Exits IKEv2 profile configuration mode and returns to privileged EXEC mode.
Step 14	**show crypto ikev2 session detailed** **Example:** `Device# show crypto ikev2 session detailed`	Displays the status of active Internet Key Exchange Version 2 (IKEv2) sessions.

Configuration Examples for Aggregate Authentication

Example: Configuring Aggregate Authentication

The following example shows how to configure aggregate authentication on the FlexVPN server to enable the establishment of a secure tunnel between Cisco AnyConnect Client and FlexVPN server.

```
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
```

Additional References for Configuring Aggregate Authentication

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Security commands	• 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

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Configuring Aggregate Authentication

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for Configuring Aggregate Authentication

Feature Name	Releases	Feature Information
Dual-Factor Authentication support with IKEv2		Dual-Factor Authentication support with IKEv2 supports certificate request from Cisco AnyConnect client for double authentication. The following command was modified: **authentication (IKEv2 profile)**.
FlexVPN RA - Aggregate Auth Support for AnyConnect		The FlexVPN RA - Aggregate Auth Support for AnyConnect feature implements aggregate authentication method by extending support for Cisco AnyConnect client that uses the proprietary AnyConnect EAP authentication method to establish a secure tunnel over the Internet between Cisco AnyConnect client and FlexVPN server. The following commands were introduced or modified: **aaa accounting (IKEv2 profile)**, **aaa authentication (IKEv2 profile)**, **aaa authorization (IKEv2 profile)**, **authentication (IKEv2 profile)**, **show crypto ikev2 profile**, **show crypto ikev2 session**.