Configuring IKEv2 Change of Authorization Support

The FlexVPN - IKEv2 CoA for QoS and ACL feature supports RADIUS Change of Authorization (CoA) on an active IKEv2 crypto session.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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

Prerequisites for IKEv2 Change of Authorization Support

- IKEv2 must be registered as a component, via a registry entry, on Cisco AAA component.

Restrictions for IKEv2 Change of Authorization Support

- This feature supports change of authorization (CoA) packets received from RADIUS-based AAA server only.

Information About IKEv2 Change of Authorization Support

RADIUS Change of Authorization

The RADIUS Change of Authorization (CoA) provides a mechanism to change the attributes of an authentication, authorization, and accounting (AAA) session after it is authenticated. When a policy changes for a user or user group in AAA, administrators can send the RADIUS CoA packets from the AAA server such as a Cisco Secure Access Control Server (ACS) to reinitialize authentication and apply the new policy.

A standard RADIUS interface is typically used in a pulled model, in which the request originates from a device attached to a network and the response is sent from the queried servers. Cisco software supports the RADIUS CoA request defined in RFC 5176 that is used in a pushed model, in which the request originates from the external server to the device attached to the network, and enables the dynamic reconfiguring of sessions from external authentication, authorization, and accounting (AAA) or policy servers.

Fore more information on RADIUS CoA, see *Authentication, Authorization, and Accounting Configuration Guide, Cisco IOS Release 15M&T* or *Authentication, Authorization, and Accounting Configuration Guide, Cisco IOS XE Release 3S*

Working of Change of Authorization on IKEv2

The FlexVPN - IKEv2 CoA for QoS and ACL feature allows to change attributes of an active IKEv2 crypto session to apply a new authorization attributes. The Cisco AAA component receives a Change of Authorization (CoA) packet from a AAA server and checks if the received CoA packet is meant for any of the components registered with it. If a component sees that the CoA packet is meant for itself, it processes it further. Based on the fields in the CoA packet, if the packet is relevant for a given component, such as IKEv2, the packet is consumed by that component. AAA will not forward the packet to the next component in the list.

In case of this feature, after IKEv2 receives a CoA packet, IKEv2 verifies the CoA packet for the Cisco (AV) pairs. IKEv2 identifies the session based on the audit-session-id which is already stored in the RADIUS server.

If the CoA packet contains attributes not supported by IKEv2, IKEv2 discards the packet and sends a CoA-NACK to AAA component.

Supported AV Pairs for IKEv2 Change of Authorization

The FlexVPN - IKEv2 CoA for QoS and ACL feature supports the following Cisco AV pairs:

- ip:interface-config
- ip:sub-policy-In
- ip:sub-policy-Out
- ip:sub-qos-policy-in
- ip:sub-qos-policy-out
- ipsec:inacl
- ipsec:outacl

How to Configure IKEv2 Change of Authorization Support

Configuring Change of Authorization on the FlexVPN Server

There is no IKEv2-specific configuration required for this feature. on the FlexVPN server for the IKEv2 Change of Authorization (CoA) Support feature. You only need to configure the RADIUS Change of Authorization on the FlexVPN server. For more information on AAA configuration, see the “RADIUS Change of Authorization” feature module in the *Authentication, Authorization, and Accounting Configuration Guide, Cisco IOS Release 15M&T*.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa server radius dynamic-author**
5. **client** {*ip-address* | *name* [**vrf** *vrf-name*]} **server-key** [**0** | **7**] *string*
6. **port** *port-number*
7. **auth-type** {**any** | **all** | **session-key**}
8. **ignore session-key**
9. **ignore server-key**
10. **exit**

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	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables authentication, authorization, and accounting (AAA) globally.
Step 4	**aaa server radius dynamic-author** **Example:** `Device(config)# aaa server radius dynamic-author`	Enters dynamic authorization local server configuration mode and specifies a RADIUS client from which a device accepts Change of Authorization (CoA) and disconnect requests. Configures the device as a AAA server to facilitate interaction with an external policy server.

	Command or Action	Purpose
Step 5	**client** {*ip-address* | *name* [**vrf** *vrf-name*]} **server-key** [**0** | **7**] *string* **Example:** `Device(config-locsvr-da-radius)# client 10.0.0.1`	Configures the RADIUS key to be shared between a device and RADIUS clients.
Step 6	**port** *port-number* **Example:** `Device(config-locsvr-da-radius)# port 3799`	Specifies the port on which a device listens for RADIUS requests from configured RADIUS clients. **Note** The default port for packet of disconnect is 1700. Port 3799 is required to interoperate with ACS 5.1.

Step 7	**auth-type** {**any** | **all** | **session-key**}
	Example:
	`Device(config-locsvr-da-radius)# auth-type all`
		Specifies the type of authorization that the device must use for RADIUS clients. The client must match the configured attributes for authorization.

Step 8	**ignore session-key** **Example:** `Device(config-locsvr-da-radius)# ignore session-key`	(Optional) Configures the device to ignore the session key.
Step 9	**ignore server-key** **Example:** `Device(config-locsvr-da-radius)# ignore server-key`	(Optional) Configures the device to ignore the server key.
Step 10	**exit** **Example:** `Device(config-locsvr-da-radius)# exit`	Returns to global configuration mode.

Verifying IKEv2 Change of Authorization Support on Cisco ASR 1000 Series Router

Use the following show commands to view the success of change of authorization (CoA) on Cisco ASR 1000 Series Aggregation Services Routers.

SUMMARY STEPS

1. **enable**
2. **show platform hardware qfp active feature qos all output all**
3. **show platform hardware qfp active feature qos all input all**

DETAILED STEPS

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **show platform hardware qfp active feature qos all output all**

Example:

```
Device# show platform hardware qfp active feature qos all output all

Interface: Virtual-Access1, QFP if_h: 14, Num Targets: 1
  Target: Out, Num UIDBs: 1
    UIDB #: 0
    Hierarchy level: 0, Num matching iftgts: 1
    Policy name: aaa-out-policy, Policy id: 9679472
    Parent Class Idx: 0, Parent Class ID: 0
      IF Tgt#: 0, ifh: 14, member_ifh: 0, link_idx: 0
        PSQD specifics:
          Target Index: 0, Num Classes: 1
            Class index: 0, Class object id: 1593, Match index: 0
            Class name: class-default, Policy name: aaa-out-policy
              psqd[0-3]: 0x00000000 0x00000000 0x00000001 0x00000000
        ISQD specifics:
          Target Index: 0, Num Classes: 1
            Class index: 0, Class object id: 1593
            Class name: class-default, Policy name: aaa-out-policy
              isqd[0-3]:  0x88e78ec0 0x00000000 0x00000000 0x00000000
              (cache) isqd[0-3]: 0x88e78ec0 0x00000000 0x00000000 0x00000000
        Police specifics:
          Target Index: 0, Num Classes: 1
            Class index: 0, Class object id: 1593
            Class name: class-default, Policy name: aaa-out-policy
              Policer id: 0x20000002
              hw_policer[0-3]:       0x4000047e 0x00163ac8 0x00000000 0x00000000
              cache hw_policer[0-3]: 0x4000047e 0x00163ac8 0x00000000 0x00000000
              conform stats (paks/octets): 0x0000000000000000, : 0x0000000000000000
              exceed stats  (paks/octets): 0x0000000000000000, : 0x0000000000000000
              violate stats (paks/octets): 0x0000000000000000, : 0x0000000000000000
              police_info:           0x00000000
              cache police_info:     0x00000000
        Queue specifics:
          Target Index: 0, Num Classes: 1
            Class index: 0, Class object id: 1593
            Class name: class-default, Policy name: aaa-out-policy
              No queue configured
        Schedule specifics:
          Target Index: 0, Num Classes: 1
            Class index: 0, Class object id: 1593
            Class name: class-default, Policy name: aaa-out-policy
              No schedule info (no queue configured)
```

Displays platform-specific information if CoA was successful.

Step 3 **show platform hardware qfp active feature qos all input all**

Example:

```
Device#  show platform hardware qfp active feature qos all input all

Interface: Virtual-Access1, QFP if_h: 14, Num Targets: 1
  Target: In, Num UIDBs: 1
    UIDB #: 0
```

```
Hierarchy level: 0, Num matching iftgts: 1
Policy name: aaa-in-policy, Policy id: 980784
Parent Class Idx: 0, Parent Class ID: 0
  IF Tgt#: 0, ifh: 14, member_ifh: 0, link_idx: 0
    PSQD specifics:
      Target Index: 0, Num Classes: 1
        Class index: 0, Class object id: 1593, Match index: 0
        Class name: class-default, Policy name: aaa-in-policy
          psqd[0-3]: 0x00000000 0x00000000 0x00000001 0x00000000
    ISQD specifics:
      Target Index: 0, Num Classes: 1
        Class index: 0, Class object id: 1593
        Class name: class-default, Policy name: aaa-in-policy
          isqd[0-3]:  0x88d49748 0x00000001 0x00000000 0x00000000
          (cache) isqd[0-3]: 0x88d49748 0x00000001 0x00000000 0x00000000
    Police specifics:
      Target Index: 0, Num Classes: 1
        Class index: 0, Class object id: 1593
        Class name: class-default, Policy name: aaa-in-policy
          Policer id: 0x20000003
          hw_policer[0-3]:       0x10000140 0x00113a29 0x00000000 0x00000000
          cache hw_policer[0-3]: 0x10000140 0x00113a29 0x00000000 0x00000000
          conform stats (paks/octets): 0x0000000000000000, : 0x0000000000000000
          exceed stats  (paks/octets): 0x0000000000000000, : 0x0000000000000000
          violate stats (paks/octets): 0x0000000000000000, : 0x0000000000000000
          police_info:           0x00000000
          cache police_info:     0x00000000
    Queue specifics:
      Target Index: 0, Num Classes: 1
        Class index: 0, Class object id: 1593
        Class name: class-default, Policy name: aaa-in-policy
          No queue configured
    Schedule specifics:
      Target Index: 0, Num Classes: 1
        Class index: 0, Class object id: 1593
        Class name: class-default, Policy name: aaa-in-policy
          No schedule info (no queue configured)
```

Displays the feature status.

Configuration Examples for IKEv2 Change of Authorization Support

Example: Triggering a Change of Authorization

The following sample output is displayed when an administrator triggers a change of authorization (CoA). The session is identified based on the audit-session-id, a dynamic string, which is an encoded form of 6 tuple information of a session with peer.

IKEv2 receives a change of authorization (CoA) packet from a RADIUS server. The session is identified based on audit-session-id.

```
*Oct  6 23:38:55.250: RADIUS: COA  received from id 125 10.106.210.176:58712, CoA Request,
 len 257
*Oct  6 23:38:55.251: COA: 10.106.210.176 request queued
```

```
*Oct  6 23:38:55.251: RADIUS:  authenticator BD 97 5E BA B2 EB C1 C5 - 1A 14 51 3D C2 C8
66 3F
*Oct  6 23:38:55.251: RADIUS:  Vendor, Cisco       [26]  62
*Oct  6 23:38:55.251: RADIUS:   Cisco AVpair       [1]   56
"audit-session-id=L2L44D010102ZO2L44D010101ZI1F401F4ZO2"
*Oct  6 23:38:55.251: RADIUS:  Vendor, Cisco       [26]  52
*Oct  6 23:38:55.251: RADIUS:   Cisco AVpair       [1]   46
"ip:interface-config=service-policy input pol"
*Oct  6 23:38:55.251: RADIUS:  Vendor, Cisco       [26]  35
*Oct  6 23:38:55.251: RADIUS:   Cisco AVpair       [1]   29  "ip:sub-qos-policy-out=2M-IN"
*Oct  6 23:38:55.251: RADIUS:  Vendor, Cisco       [26]  36
*Oct  6 23:38:55.251: RADIUS:   Cisco AVpair       [1]   30  "ip:sub-qos-policy-in=aaa-pol"
*Oct  6 23:38:55.251: RADIUS:  Vendor, Cisco       [26]  52
*Oct  6 23:38:55.251: RADIUS:   Cisco AVpair       [1]   46
"ip:interface-config=service-policy output 2M"
*Oct  6 23:38:55.251: COA: Message Authenticator missing or failed decode

*Oct  6 23:38:55.251:  ++++++ CoA Attribute List ++++++
*Oct  6 23:38:55.251: 421C9694 0 00000089 audit-session-id(819) 37
L2L44D010102ZO2L44D010101ZI1F401F4ZO2
*Oct  6 23:38:55.251: 421C9584 0 00000081 interface-config(222) 24 service-policy input pol
*Oct  6 23:38:55.251: 421C95B8 0 00000081 sub-qos-policy-out(423) 5 2M-IN
*Oct  6 23:38:55.251: 421C95EC 0 00000081 sub-qos-policy-in(421) 7 aaa-pol
*Oct  6 23:38:55.251: 421C9620 0 00000081 interface-config(222) 24 service-policy output
2M
*Oct  6 23:38:55.251:
*Oct  6 23:38:55.251: COA: Added NACK Error Cause: Success
```

Additional References for IKEv2 Change of Authorization Support

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 IKEv2 Change of Authorization Support

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 IKEv2 Change of Authorization Support

Feature Name	Releases	Feature Information
FlexVPN - IKEv2 CoA for QoS and ACL		The FlexVPN - IKEv2 CoA for QoS and ACL feature supports RADIUS Change of Authorization (CoA) on an active IKEv2 crypto session. No commands were modified or updated by this feature.