IKEv2 認可変更のサポートの設定

FlexVPN - QoS および ACL 用 IKEv2 CoA 機能は、アクティブな IKEv2 暗号セッションでの RADIUS 認可変更（CoA）をサポートしています。

IKEv2 認可変更のサポートの前提条件

- IKEv2 は、Cisco AAA コンポーネントのレジストリ エントリからコンポーネントとして登録する必要があります。

IKEv2 認可変更サポートの制限事項

- この機能では、RADIUS ベースの AAA サーバーから受信した認可変更（CoA）パケットのみをサポートしています。

IKEv2 認可変更サポートに関する情報

RADIUS 許可の変更

RADIUS 認可変更（CoA）機能は、認証、認可、およびアカウンティング（AAA）セッションの属性を、セッション認証後に変更するためのメカニズムを提供します。AAA でユーザー、またはユーザー グループのポリシーに変更がある場合、管理者は Cisco Secure Access Control

Server（ACS）などの AAA サーバーから RADIUS CoA パケットを送信して認証を再初期化し、新しいポリシーを適用することができます。

標準RADIUSインターフェイスは通常、ネットワークに接続しているデバイスから要求が送信され、クエリが送信されたサーバーが応答するプル モデルで使用されます。シスコのソフトウェアは、プッシュ モデルで使用される RFC 5176 で定義された RADIUS CoA 要求をサポートしています。このモデルでは、要求は外部サーバーからネットワークに接続されたデバイスへ発信され、外部の認証、認可、およびアカウンティング（AAA）またはポリシー サーバーからの動的なセッション再設定が可能になります。

RADIUS CoA の詳細については、『*Authentication, Authorization, and Accounting Configuration Guide, Cisco IOS Release 15M&T*』または『*Authentication, Authorization, and Accounting Configuration Guide, Cisco IOS XE Release 3S*』を参照してください。

IKEv2 認可変更の作業

FlexVPN - QoS および ACL 用 IKEv2 CoA 機能では、アクティブな IKEv2 暗号セッションの属性を変更して、新しい認証属性に適用できます。Cisco AAA コンポーネントは、AAA サーバーから認可変更（CoA）パケットを受信して、受信した CoA パケットがそれに登録された任意のコンポーネント用かどうかを確認します。CoA パケットがそれ自体のために作成されたとコンポーネントが確認した場合、以降の処理に進みます。CoA パケット内のフィールドに基づいて、パケットが IKEv2 などの任意のコンポーネントと関連している場合、そのパケットはそのコンポーネントによって使用されます。AAA はそのパケットを、リスト内の次のコンポーネントに転送しません。

この機能では、IKEv2 が CoA パケットを受信した後、IKEv2 では Cisco （AV）ペアに対してその CoA パケットを確認します。IKEv2 は、RADIUS サーバーにすでに保存されている audit-session-id に基づいてセッションを特定します。

CoA パケットに IKEv2 がサポートしていない属性が含まれる場合、IKEv2 はそのパケットを破棄し、CoA-NACK を AAA コンポーネントに送信します。

IKEv2 認可変更でサポートされる AV ペア

FlexVPN - QoS および ACL 用 IKEv2 CoA 機能は、次の Cisco AV ペアをサポートしています。

- 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

IKEv2 認可変更サポートの設定方法

FlexVPN サーバーでの認可変更の設定

IKEv2 認可変更（CoA）サポート機能に必要な、FlexVPN サーバーでの IKEv2 固有の設定はありません。FlexVPN サーバーでは、RADIUS 認可変更のみを設定する必要があります。AAA 設定の詳細については、『*Authentication, Authorization, and Accounting Configuration Guide, Cisco IOS Release 15M&T*』の「RADIUS Change of Authorization」機能モジュールを参照してください。

手順の概要

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**

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。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： `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	**aaa new-model** 例： `Device(config)# aaa new-model`	認証、認可、アカウンティング（AAA）をグローバルに有効化します。
ステップ 4	**aaa server radius dynamic-author** 例： `Device(config)# aaa server radius dynamic-author`	ダイナミック認可ローカル サーバー コンフィギュレーション モードを開始し、デバイスが認可変更（CoA）を受け入れ、要求を取り外す RADIUS クライアントを指定します。デバイスを AAA サー

	コマンドまたはアクション	目的
		バーとして設定し、外部ポリシー サーバーとの連携を可能にする。
ステップ 5	**client** {*ip-address* | *name* [**vrf** *vrf-name*]} **server-key** [**0** | **7**] *string* 例： `Device(config-locsvr-da-radius)# client 10.0.0.1`	RADIUS キーをデバイスと RADIUS クライアントとの間で共有されるように設定します。
ステップ 6	**port** *port-number* 例： `Device(config-locsvr-da-radius)# port 3799`	設定された RADIUS クライアントから RADIUS 要求をデバイスが受信するポートを指定します。 （注） パケットオブディスコネクトのデフォルト ポートは 1700 です。ACS 5.1 と相互運用するためには、ポート 3799 が必要です。
ステップ 7	**auth-type** {**any** | **all** | **session-key**} 例： `Device(config-locsvr-da-radius)# auth-type all`	デバイスが RADIUS クライアントに使用する認可のタイプを指定します。クライアントは、認可用に設定された属性と一致していなければなりません。
ステップ 8	**ignore session-key** 例： `Device(config-locsvr-da-radius)# ignore session-key`	（オプション）セッション キーを無視するようにデバイスを設定します。
ステップ 9	**ignore server-key** 例： `Device(config-locsvr-da-radius)# ignore server-key`	（オプション）サーバー キーを無視するようにデバイスを設定します。
ステップ 10	**exit** 例： `Device(config-locsvr-da-radius)# exit`	グローバル コンフィギュレーション モードに戻ります。

IKEv2 認可変更サポートの確認

次の show コマンドを使用して、Cisco デバイスでの認可変更（CoA）の成功を確認します。

手順の概要

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

手順の詳細

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 show platform hardware qfp active feature qos all output all

例：

```
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)
```

CoA が成功したかどうかのプラットフォーム固有情報が表示されます。

ステップ 3 show platform hardware qfp active feature qos all input all

例：

```
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)
```

機能のステータスが表示されます。

IKEv2 認可変更サポートの設定例

例：認可変更のトリガー

次の出力例は、管理者が認可変更（CoA）をトリガーすると表示されます。セッションは、audit-session-idに基づいて特定されます。このIDは動的文字列で、ピアとのセッションについて、6タプル情報の形式にエンコードされています。

IKEv2 は、RADIUS サーバーから認可変更（CoA）パケットを受信します。セッションは、audit-session-id に基づいて特定されます。

```
*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
```

IKEv2 認可変更サポートに関する追加情報

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

IKEv2 認可変更のサポートの機能情報

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 *1 : IKEv2* 認可変更のサポートの機能情報

機能名	リリース	機能情報
FlexVPN - QoS および ACL 用 IKEv2 CoA		FlexVPN - QoS および ACL 用 IKEv2 CoA 機能は、アクティブな IKEv2 暗号セッションでの RADIUS 認可変更（CoA）をサポートしています。 この機能によって変更または更新されたコマンドはありません。

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。