IKEv2パケットオブディスコネクトの設定

IKEv2 リモート アクセス認可変更（CoA）のパケット オブ ディスコネクト機能は、シスコがサポートするデバイスのアクティブな暗号 IKEv2 セッションを停止します。

IKEv2 パケット オブ ディスコネクトに関する情報

切断要求

パケット オブ ディスコネクト（POD）は、RADIUS disconnect_request パケットで、認証エージェント サーバーで暗号化セッションを切断する必要がある場合に使用することを目的としています。

POD が必要な場合

パケット オブ ディスコネクトは、次の状況で必要になります。

- 再認証の実行：セッションが非常に長い期間接続されている場合、ネットワーク管理者として、FlexVPN サーバー上のユーザーを解除して強制的に再認証する必要がある場合があります。
- 新しいポリシーの適用：クライアントが再接続する場合、ネットワーク管理者として、アクティブな暗号化セッションを終了して新しいポリシーをセッションに適用する必要がある場合があります。
- リソースの解放：セッションを終了して、リソースを解放し、キー再生成を終了する必要がある場合があります。

IKEv2 パケット オブ ディスコネクト

IKEv2 リモート アクセスの認可変更（CoA）：パケット オブ ディスコネクト機能は、RADIUS パケット オブ ディスコネクト（POD）機能を使用して暗号化セッションを削除します。暗号化セッションは、VPN ユーザーを AAA サーバーの新しいユーザー ポリシーまたはグループ ポリシーに更新するために削除されます。

1. AAA は、RADIUS サーバーから提供される属性キー/値ペアのリストを IKEv2 に渡します。
2. IKEv2 はリストを解析して、キーとして監査セッション ID、Cisco AV ペアを検索し、ペア値を確認します。
3. IKEv2 はセッションを検索し、特定のセッションを削除します。
4. IKEv2 は AAA に通知し、AAA は RADIUS サーバーに通知します。
5. 監査セッション ID に関係するセッションは削除されます。

IKEv2 パケット オブ ディスコネクトのパラメータ

RFC 3576 は、IKEv2 パケット オブ ディスコネクトをサポートする次の POD コードを指定します。

- 40：切断要求
- 41：切断 ACK
- 42：切断 NAK

切断 ACK コードは、監査セッション ID 用にセッションが存在し、監査セッション ID に関係するセッションが正常に終了されたことを示します。切断 NACK コードは、監査セッション ID に対応するセッションがないことを示します。ゲートウェイに応答メッセージは送信されません。

IKEv2 パケット オブ ディスコネクトの設定方法

FlexVPN サーバーでの AAA の設定

IKEv2 リモート アクセス認可変更（CoA）のパケット オブ ディスコネクト機能に対して、FlexVPN サーバーに必要な IKEv2 独自の設定はありません。FlexVPN サーバーでは、認可、およびアカウンティング（AAA）のみを設定する必要があります。AAA の設定の詳細については、『』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** {*hostname* | *ip-address*} [**server-key** *string* | **vrf** *vrf-id*]
6. **port** *number*
7. **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	**aaa new-model** 例： `Device(config)# aaa new-model`	AAA をグローバルに有効にします。
ステップ 4	**aaa server radius dynamic-author** 例：	ローカル AAA サーバーでダイナミック認証サービスを設定し、ダイナミック認証ローカル サーバー コンフィギュレーション モードを開始します。 • このモードでは、RADIUS アプリケーション コマンドが設定されます。
ステップ 5	**client** {*hostname* | *ip-address*} [**server-key** *string* | **vrf** *vrf-id*] 例： `Device(config-locsvr-da-radius)# client 192.168.0.5 server-key cisco`	AAA サーバー クライアントの IP アドレスまたはホスト名を設定します。 • **server-key** キーワードと *string* 引数を使用して、クライアント レベルのサーバー キーを設定します。 （注） クライアント レベルでサーバー キーを設定すると、グローバル レベルで設定されたサーバー キーが上書きされます。
ステップ 6	**port** *number* 例： `Device(config-locsvr-da-radius)# port 1812`	UDP ポートを設定します。
ステップ 7	**end** 例： `Device(config-locsvr-da-radius)# end`	ダイナミック認証ローカル サーバー 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 パケット オブ ディスコネクトの設定例

例：IKEv2 セッションの終了

次に、**show aaa sessions** コマンドの出力例を示します。終了する IKEv2 セッションを特定するには、このコマンドを実行する必要があります。

```
Device# show aaa sessions

Total sessions since last reload: 32
Session Id: 3
   Unique Id: 14
   User Name: *not available*
   IP Address: 0.0.0.0
   Idle Time: 0
   CT Call Handle: 0
Session Id: 30
   Unique Id: 41
   User Name: pskuser2.g1.engdt.com
   IP Address: 0.0.0.0
   Idle Time: 0
   CT Call Handle: 0
Session Id: 32
   Unique Id: 43
   User Name: pskuser4.g2.engdt.com
   IP Address: 0.0.0.0
   Idle Time: 0
   CT Call Handle: 0
```

上記の出力では、ID 41 および 43 が IKEv2 セッションに関するものです。必要に応じて、**show aaa user** コマンドを実行して、セッションの詳細な情報を表示することができます。

```
Device# show aaa user 41

Unique id 41 is currently in use.
  No data for type 0
  No data for type EXEC
  No data for type CONN
  NET: Username=(n/a)
    Session Id=0000001E Unique Id=00000029
    Start Sent=0 Stop Only=N
    stop_has_been_sent=N
    Method List=0
    Attribute list:
      7FBD9783CCF0 0 00000001 session-id(408) 4 30(1E)
      7FBD9783CD30 0 00000001 start_time(418) 4 Nov 04 2014 00:20:23
--------
  No data for type CMD
  No data for type SYSTEM
  No data for type VRRS
  No data for type RM CALL
  No data for type RM VPDN
  No data for type AUTH PROXY
  No data for type DOT1X
  No data for type CALL
```

```
  No data for type VPDN-TUNNEL
  No data for type VPDN-TUNNEL-LINK
  IPSEC-TUNNEL: Username=pskuser2.g1.engdt.com
    Session Id=0000001E Unique Id=00000029
    Start Sent=1 Stop Only=N
    stop_has_been_sent=N
    Method List=7FBDA6E05A68 : Name = accnt_prof
    Attribute list:
      7FBD9783CCF0 0 00000001 session-id(408) 4 30(1E)
      7FBD9783CD30 0 00000001 start_time(418) 4 Nov 04 2014 00:20:23
      7FBD9783CD70 0 00000082 formatted-clid(37) 13 192.168.202.2
      7FBD9783CDB0 0 0000008A audit-session-id(819) 37
L2L433010101ZO2L4C0A8CA02ZH119404ZP37
      7FBD9783CDF0 0 00000081 isakmp-phase1-id(737) 21 pskuser2.g1.engdt.com
      7FBD9783BF80 0 00000002 isakmp-initator-ip(738) 4 192.168.202.2
--------
  No data for type MCAST
  No data for type RESOURCE
  No data for type SSG
  No data for type IDENTITY
  No data for type ConnectedApps
Accounting:
  log=0x400018041
  Events recorded :
    CALL START
    ATTR REPLACE
    INTERIM START
    INTERIM STOP
    IPSEC TNL UP
  update method(s) :
    NONE
  update interval = 0
  Outstanding Stop Records : 0
  Dynamic attribute list:
    7FBD9783BF80 0 00000001 connect-progress(75) 4 No Progress
    7FBD9783BFC0 0 00000001 pre-session-time(334) 4 0(0)
    7FBD9783C000 0 00000001 elapsed_time(414) 4 341(155)
    7FBD9783C040 0 00000001 bytes_in(146) 4 0(0)
    7FBD9783C080 0 00000001 bytes_out(311) 4 0(0)
    7FBD9783CCF0 0 00000001 pre-bytes-in(330) 4 0(0)
    7FBD9783CD30 0 00000001 pre-bytes-out(331) 4 0(0)
    7FBD9783CD70 0 00000001 paks_in(147) 4 0(0)
    7FBD9783CDB0 0 00000001 paks_out(312) 4 0(0)
    7FBD9783CDF0 0 00000001 pre-paks-in(332) 4 0(0)
    7FBD9783BA20 0 00000001 pre-paks-out(333) 4 0(0)
Debg: No data available
Radi: No data available
Interface:
  TTY Num = -1
  Stop Received = 0
  Byte/Packet Counts till Call Start:
    Start Bytes In = 0            Start Bytes Out = 0
    Start Paks  In = 0            Start Paks  Out = 0
  Byte/Packet Counts till Service Up:
    Pre Bytes In = 0            Pre Bytes Out = 0
    Pre Paks  In = 0            Pre Paks  Out = 0
  Cumulative Byte/Packet Counts :
    Bytes In = 0            Bytes Out = 0
    Paks  In = 0            Paks  Out = 0
  StartTime = 00:20:23 IST Nov 4 2014
  AuthenTime = 00:20:23 IST Nov 4 2014
  Component = VPN IPSEC
Authen: service=NONE type=NONE method=NONE
Kerb: No data available
```

```
Meth: No data available
Preauth: No Preauth data.
General:
  Unique Id = 00000029
  Session Id = 0000001E
  Session Server Key = 1771D693
  Attribute List:
PerU: No data available
Service Profile: No Service Profile data.
Unkn: No data available
Unkn: No data available
```

上記の出力では、audit-session-id、L2L433010101ZO2L4C0A8CA02ZH119404ZP37 に注意してください。次の出力例は、RADIUS サーバーで開始されるアカウンティングセッションの開始時に、FlexVPN サーバーに表示されます。

```
Nov  4 00:26:49.908 IST: RADIUS/ENCODE: Best Local IP-Address 192.168.202.1 for
Radius-Server 9.45.15.144
Nov  4 00:26:49.908 IST: RADIUS(0000002C): Send Accounting-Request to 9.45.15.144:1813
id 1646/231, len 288
Nov  4 00:26:49.908 IST: RADIUS:  authenticator 29 63 0C 79 C1 5E F2 0E - F3 CA 36 DD
A3 55 C1 DE
Nov  4 00:26:49.908 IST: RADIUS:  Acct-Session-Id     [44]  10  "00000021"
Nov  4 00:26:49.908 IST: RADIUS:  Calling-Station-Id  [31]  15  "192.168.202.2"
Nov  4 00:26:49.908 IST: RADIUS:  Vendor, Cisco       [26]  64
Nov  4 00:26:49.908 IST: RADIUS:   Cisco AVpair       [1]   58
"audit-session-id=L2L433010101ZO2L4C0A8CA02ZH11941194ZN3A"
Nov  4 00:26:49.908 IST: RADIUS:  Vendor, Cisco       [26]  46
Nov  4 00:26:49.908 IST: RADIUS:   Cisco AVpair       [1]   40
"isakmp-phase1-id=pskuser1.g1.engdt.com"
Nov  4 00:26:49.908 IST: RADIUS:  Vendor, Cisco       [26]  40
Nov  4 00:26:49.908 IST: RADIUS:   Cisco AVpair       [1]   34
"isakmp-initator-ip=192.168.202.2"
Nov  4 00:26:49.908 IST: RADIUS:  User-Name           [1]   23  "pskuser1.g1.engdt.com"
Nov  4 00:26:49.908 IST: RADIUS:  Vendor, Cisco       [26]  36
Nov  4 00:26:49.908 IST: RADIUS:   Cisco AVpair       [1]   30  "connect-progress=No
Progress"
Nov  4 00:26:49.908 IST: RADIUS:  Acct-Authentic      [45]  6   Local
   [2]
Nov  4 00:26:49.908 IST: RADIUS:  Acct-Status-Type    [40]  6   Start
   [1]
Nov  4 00:26:49.908 IST: RADIUS:  NAS-IP-Address      [4]   6   192.168.202.1

Nov  4 00:26:49.908 IST: RADIUS:  home-hl-prefix      [151] 10  "D33648D8"
Nov  4 00:26:49.908 IST: RADIUS:  Acct-Delay-Time     [41]  6   0

Nov  4 00:26:49.908 IST: RADIUS(0000002C): Sending a IPv4 Radius Packet
```

次の出力は、特定の audit-session-id のセッションを切断すると、FlexVPN サーバーに表示されます。セッション終了要求は RADIUS クライアント経由で RADIUS サーバーに送信されます。この例では、audit-session-ID が L2L433010101ZO2L4C0A8CA02ZH119404ZP37 のセッションは終了するため、出力には表示されません。

```
Nov  4 00:32:29.004 IST: RADIUS: POD  received from id 216 9.45.15.144:50567, POD Request,
 len 84
Nov  4 00:32:29.004 IST: POD: 9.45.15.144 request queued
Nov  4 00:32:29.004 IST:  ++++++ POD Attribute List ++++++
Nov  4 00:32:29.004 IST: 7FBD9783D3A8 0 00000089 audit-session-id(819) 39
L2L433010101ZO2L4C0A8CA02ZH11941194ZN3B
```

```
Nov  4 00:32:29.004 IST:
Nov  4 00:32:29.004 IST: POD: Sending ACK from port 1812 to 9.45.15.144/50567

Nov  4 00:32:29.005 IST: IKEv2:(SESSION ID = 59,SA ID = 2):Check for existing active SA
Nov  4 00:32:29.006 IST: IKEv2:in_octets 0, out_octets 0
Nov  4 00:32:29.006 IST: IKEv2:in_packets 0, out_packets 0
Nov  4 00:32:29.006 IST: IKEv2:(SA ID = 2):[IKEv2 -> AAA] Accounting stop request sent
successfully
Nov  4 00:32:29.006 IST: IKEv2:(SESSION ID = 59,SA ID = 2):Delete all IKE SAs
Nov  4 00:32:29.010 IST: RADIUS/ENCODE(0000002D):Orig. component type = VPN IPSEC
Nov  4 00:32:29.010 IST: RADIUS(0000002D): Config NAS IP: 0.0.0.0
Nov  4 00:32:29.010 IST: RADIUS(0000002D): Config NAS IPv6: ::
Nov  4 00:32:29.010 IST: RADIUS(0000002D): sending
Nov  4 00:32:29.011 IST: RADIUS/ENCODE: Best Local IP-Address 192.168.202.1 for
Radius-Server 9.45.15.144
Nov  4 00:32:29.011 IST: RADIUS(0000002D): Send Accounting-Request to 9.45.15.144:1813
id 1646/246, len 356
Nov  4 00:32:29.011 IST: RADIUS:  authenticator 52 88 5E CB 8B FA 1E C1 - CC EF 73 75
89 73 CA 95
Nov  4 00:32:29.011 IST: RADIUS:  Acct-Session-Id     [44]  10  "00000022"
Nov  4 00:32:29.011 IST: RADIUS:  Calling-Station-Id  [31]  15  "192.168.202.2"
Nov  4 00:32:29.011 IST: RADIUS:  Vendor, Cisco       [26]  64
Nov  4 00:32:29.011 IST: RADIUS:   Cisco AVpair       [1]   58
"audit-session-id=L2L433010101ZO2L4C0A8CA02ZH11941194ZN3B"
Nov  4 00:32:29.011 IST: RADIUS:  Vendor, Cisco       [26]  46
Nov  4 00:32:29.011 IST: RADIUS:   Cisco AVpair       [1]   40
"isakmp-phase1-id=pskuser1.g1.engdt.com"
Nov  4 00:32:29.011 IST: RADIUS:  Vendor, Cisco       [26]  40
Nov  4 00:32:29.011 IST: RADIUS:   Cisco AVpair       [1]   34
"isakmp-initator-ip=192.168.202.2"
Nov  4 00:32:29.011 IST: RADIUS:  User-Name           [1]   23  "pskuser1.g1.engdt.com"
Nov  4 00:32:29.011 IST: RADIUS:  Acct-Authentic      [45]  6   Local
   [2]
Nov  4 00:32:29.011 IST: RADIUS:  Vendor, Cisco       [26]  36
Nov  4 00:32:29.011 IST: RADIUS:   Cisco AVpair       [1]   30  "connect-progress=No
Progress"
Nov  4 00:32:29.011 IST: RADIUS:  Acct-Session-Time   [46]  6   56

Nov  4 00:32:29.011 IST: RADIUS:  Acct-Input-Octets   [42]  6   0

Nov  4 00:32:29.011 IST: RADIUS:  Acct-Output-Octets  [43]  6   0

Nov  4 00:32:29.011 IST: RADIUS:  Acct-Input-Packets  [47]  6   0

Nov  4 00:32:29.011 IST: RADIUS:  Acct-Output-Packets [48]  6   0

Nov  4 00:32:29.011 IST: RADIUS:  Acct-Terminate-Cause[49]  6   none
   [0]
Nov  4 00:32:29.011 IST: RADIUS:  Vendor, Cisco       [26]  32
Nov  4 00:32:29.011 IST: RADIUS:   Cisco AVpair      [1]   26  "disc-cause-ext=No Reason"
Nov  4 00:32:29.011 IST: RADIUS:  Acct-Status-Type    [40]  6   Stop
   [2]
Nov  4 00:32:29.011 IST: RADIUS:  NAS-IP-Address      [4]   6   192.168.202.1

Nov  4 00:32:29.011 IST: RADIUS:  home-hl-prefix      [151] 10  "E2F80C34"
Nov  4 00:32:29.011 IST: RADIUS:  Acct-Delay-Time     [41]  6   0

Nov  4 00:32:29.011 IST: RADIUS(0000002D): Sending a IPv4 Radius Packet
Nov  4 00:32:29.011 IST: RADIUS(0000002D): Started 5 sec timeout
```

次の出力は、特定の audit-session-ID で有効なセッションが存在しない場合に表示されます。これは、そのセッションがすでに終了していて、特定の audit-session-id に関連

するセッションが存在しない場合に発生します。FlexVPN サーバーに 送り返される
メッセージに注意してください。

```
Nov  4 00:30:31.905 IST: RADIUS: POD  received from id 131 9.45.15.144:52986, POD Request,
 len 84
Nov  4 00:30:31.905 IST: POD: 9.45.15.144 request queued
Nov  4 00:30:31.905 IST:  ++++++ POD Attribute List ++++++
Nov  4 00:30:31.905 IST: 7FBD9783BA20 0 00000089 audit-session-id(819) 39
L2L433010101ZO2L4C0A8CA02ZH11941194ZN3A
Nov  4 00:30:31.905 IST:
Nov  4 00:30:31.906 IST: POD: 9.45.15.144 Unsupported attribute type 26 for component
Nov  4 00:30:31.906 IST: POD: 9.45.15.144 user  0.0.0.0i sessid 0x0 key 0x0 DROPPED
Nov  4 00:30:31.906 IST: POD: Added Reply Message: No Matching Session
Nov  4 00:30:31.906 IST: POD: Added NACK Error Cause: Invalid Request
Nov  4 00:30:31.906 IST: POD: Sending NAK from port 1812 to 9.45.15.144/52986
Nov  4 00:30:31.906 IST: RADIUS:  18  21  4E6F204D61746368696E672053657373696F6E
Nov  4 00:30:31.906 IST: RADIUS:  101 6   00000194
```

IKEv2 パケット オブ ディスコネク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』
RADIUS パケット オブ ディスコネクト	『RADIUS Packet of Disconnect』 『RADIUS Packet of Disconnect』

標準および RFC

標準/RFC	タイトル
RFC 3576	*Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)*
RFC 5176	*Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)*

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 パケット オブ ディスコネクトの機能情報

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* パケット オブ ディスコネクトの機能情報

機能名	リリース	機能情報
IKEv2 リモート アクセス認可変更（CoA）のパケット オブ ディスコネクト		IKEv2 リモート アクセス認可変更（CoA）のパケット オブ ディスコネクト機能は、シスコがサポートするデバイスのアクティブな暗号 IKEv2 セッションを停止します。 この機能によって導入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。