IKEv2 再接続の設定

AnyConnect 機能の AutoReconnect 機能の IOS IKEv2 サポートは、Cisco AnyConnect でユーザーが操作しない、IKEv2 ネゴシエーションの再確立に役立ちます。

IKEv2 再接続設定の前提条件

- <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。

IKEv2 再接続設定の制限事項

- 事前供給キー認証方式は、インターネット キー エクスチェンジ バージョン 2（IKEv2）プロファイルでは設定できません。AnyConnect 機能の AutoReconnect 機能に対する IOS IKEv2 サポートでも事前共有キー認証方式を使用するため、同じ IKEv2 プロファイル上の事前共有キーの設定によって混乱が生じる可能性があります。
- **authentication local pre-share**、**authentication remote pre-share**、**keyring**、**aaa authorization group psk**、および **aaa authorization user psk** コマンドは、IKEv2 プロファイルでは設定できません。

設定された IKEv2 フラグメンテーションに関する情報

IKEv2 および Cisco AnyConnect クライアントの再接続機能

Cisco AnyConnect クライアントの自動再接続機能によって、Cisco AnyConnect VPN クライアントは一定の期間セッションを記憶し、セキュアなチャネルの確立後に接続を再開することができます。Cisco AnyConnect クライアントはインターネット キー エクスチェンジ バージョン 2（IKEv2）と共に幅広く使用されるため、IKEv2 では Cisco IOS ソフトウェアでの自動再接続機能のサポートを AnyConnect の自動再接続機能に対する IOS IKEv2 サポートにまで拡大しています。

Cisco AnyConnect クライアントでの自動再接続は、次のシナリオで発生します。

- 中間ネットワークがダウンしています。Cisco AnyConnect クライアントは、中間ネットワークがアップするとセッションを再開しようとします。
- Cisco AnyConnect クライアント デバイスは、ネットワーク間で切り替わります。これによって送信元 IP またはポートが変わり、既存のセキュリティ アソシエーション（SA）がダウンします。そのため、Cisco AnyConnect クライアントは自動再接続機能を使用して SA を再開しようとします。
- Cisco AnyConnect クライアント デバイスは、スリープまたは休止モードから復帰した後に SA を再開しようとします。

自動再接続機能を使用する利点

- 元のセッションで使用されるコピー属性は、認証、認可、およびアカウンティング（AAA）サーバーに問い合わせることなく再使用されます。
- Cisco IOS ゲートウェイは、クライアントに再接続するために RADIUS サーバーに接続する必要はありません。
- セッションの再開時に、認証または認可のためのユーザーインタラクションは必要ありません。
- セッションを再接続する場合、認証方式は事前共有キーです。この認証方式は、他の認証方式（Rivest、Shamir、および Adelman（RSA）署名認証方式、楕円曲線デジタル署名アルゴリズム（ECDSA）署名（ECDSA-sig）認証方式、および Extensible Authentication Protocol（EAP）認証方式を含む）に比べて時間がかかりません。事前共有キー認証方式では、最小限のリソースで IOS ソフトウェアでセッションを再開できます。
- これによって、未使用のセキュリティアソシエーション（SA）が削除され、暗号化リソースが解放されます。

自動再接続および DPD

Dead Peer Detection（DPD：デッドピア検出）は、ピアにクエリを送信することによって送信されるピアの可用性を確認するように設定されます。ピアから応答がない場合、そのピアのために作成されたセキュリティアソシエーションは削除されます。両方の設定シナリオで目的は同じため、DPD が FlexVPN サーバーで設定された場合に再接続プロファイルに DPD を設定す

る必要はありません。ただし、機能が有効な場合、DPD は IKEv2 でオンデマンド DPD としてキューイングされ、SA の削除時にプラットフォーム固有のハンドルも格納します。

Cisco IOS ゲートウェイと Cisco AnyConnect 間のメッセージ交換

Cisco AnyConnect クライアントは、セキュリティ アソシエーション（SA）を確立するために、Cisco IOS ゲートウェイに問い合わせます。認証または AUTH 交換（IKE_AUTH 要求の CFGMODE_REQ ペイロード）中、IKEv2 は、**reconnect** コマンドを使用して、AnyConnect 機能の自動再接続機能に対する IOS IKEv2 サポートが IKEv2 プロファイルで有効かどうかを確認します。また、選択された IKEv2 プロファイルの IKEv2 ポリシーを選択し、セッション ID とセッション トークン属性を、IKE_AUTH 応答の CFGMODE_REPLY ペイロードで Cisco AnyConnect クライアントに送信します。認証方式は、SA 用のクライアントと Cisco IOS ソフトウェア間の事前共有キーです。

IKEv2 は、Dead Peer Detection（DPD：デッドピア検出）メッセージを Cisco AnyConnect クライアントに定期的に送信して、クライアントがアクティブかどうかを確認します。Cisco AnyConnect クライアントは、Cisco IOS ゲートウェイがアクティブ クライアントとして解釈し、そのクライアントとセキュリティ アソシエーション（SA）を作成する、DPD メッセージに応答します。ただし、クライアントがデフォルトの再接続タイムアウト期間である 30 分以内に再接続されない場合、Cisco IOS ゲートウェイはそのクライアントが非アクティブであるとみなし、そのクライアントの SA を削除します。Cisco AnyConnect クライアントは、新しい接続を開始する必要があります。

show crypto ikev2 stats reconnect コマンドを使用して接続の統計情報を表示し、**clear crypto ikev2 session** コマンドを使用してクライアントとの SA を削除します。

IKEv2 再接続の設定方法

IKEv2 再接続の有効化

このタスクを実行して、AnyConnect 機能の AutoReconnect 機能の IOS IKEv2 サポートを有効にします。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ikev2 profile** *profile-name*
4. **reconnect** [**timeout** *seconds*]
5. **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	**crypto ikev2 profile** *profile-name* 例： `Device(config)# crypto ikev2 profile profile1`	IKEv2 プロファイルを定義し、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	**reconnect** [**timeout** *seconds*] 例： `Device(config-ikev2-profile)# reconnect timeout 900`	自動再接続機能の IKEv2 サポートを有効にします。
ステップ 5	**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。

IKEv2 再接続設定のトラブルシューティング

AnyConnect 機能設定の AutoReconnect 機能の IOS IKEv2 サポートを確認またはクリアするには、次のコマンドを使用します。

手順の概要

1. **enable**
2. **show crypto ikev2 stats reconnect**

手順の詳細

ステップ 1 **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）。

例：

```
Device> enable
```

ステップ 2 **show crypto ikev2 stats reconnect**

再接続の統計情報が表示されます。

例：

```
Device# show crypto ikev2 stats reconnect

Total incoming reconnect connection:        10
Success reconnect connection:               10
Failed reconnect connection:                0
Reconnect capable active session count:     4
Reconnect capable inactive session count:   6
```

IKEv2 再接続の設定例

例：IKEv2 再接続の有効化

次の例は、AnyConnect 機能の AutoReconnect 機能の IOS IKEv2 サポートを有効にする方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# crypto ikev2 profile profile1
Device(config-ikev2-profile)# reconnect timeout 600
Device(config-ikev2-profile)# end
```

IKEv2 再接続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*』

関連項目	マニュアル タイトル
Cisco AnyConnect VPN クライアントに関する情報	『*Cisco AnyConnect VPN Client Administrator Guide, Release 2.4*』

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 再接続の機能情報

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* 再接続の機能情報

機能名	リリース	機能情報
AnyConnect の AutoReconnect 機能の IOS IKEv2 サポート		AnyConnect 機能の AutoReconnect 機能の IOS IKEv2 サポートは、Cisco AnyConnect でユーザーが操作しない、IKEv2 ネゴシエーションの再確立に役立ちます。 次のコマンドが導入または変更されました。 **clear crypto ikev2 stats, reconnect, show crypto ikev2 stats.**

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。