FlexVPN およびインターネット キー エクスチェンジ バージョン 2 コンフィギュレーション ガイド（Cisco IOS XE Gibraltar 16.10.x 向け）

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

目 次

第 1 章 最初にお読みください 1

第 2 章 FlexVPN の概要 3

インターネット キー エクスチェンジ バージョン 2（IKEv2）および FlexVPN リモート アクセスの設定 3

FlexVPN サーバの設定 4

FlexVPN クライアントの設定 4

IKEv2 ロード バランサの設定 4

IKEv2 フラグメンテーションの設定 4

IKEv2 再接続の設定 4

IKEv2 パケット オブ ディスコネクトの設定 4

IKEv2 認可変更のサポートの設定 5

集約認証の設定 5

付録：FlexVPN の RADIUS 属性 5

付録：IKEv2 およびレガシー VPN 5

第 3 章 インターネット キー エクスチェンジ バージョン 2 7

機能情報の確認 8

インターネット キー交換バージョン 2 の設定に関する前提条件 8

インターネット キー エクスチェンジ バージョン 2 の設定に関する制約事項 8

インターネット キー エクスチェンジ バージョン 2 に関する情報 9

IKEv2 のサポート対象規格 9

IKEv2 の利点 9

インターネット キー エクスチェンジ バージョン 2 CLI の構成 10

IKEv2 プロポーザル 10
IKEv2 ポリシー 11
IKEv2 プロファイル 11
IKEv2 キー リング 11
IKEv2 スマート デフォルト 11
IKEv2 Suite-B サポート 13
AES-GCM のサポート 13
IKEv2 での自動トンネル モードのサポート 14
インターネット キー交換バージョン 2 の設定方法 14
基本のインターネット キー エクスチェンジ バージョン 2 CLI 構造の設定 14
IKEv2 キーリングの設定 15
IKEv2 プロファイルの設定（基本） 17
高度なインターネット キー エクスチェンジ バージョン 2 CLI 構造の設定 22
グローバル IKEv2 オプションの設定 22
IKEv2 プロポーザルの設定 25
IKEv2 ポリシーの設定 28
インターネット キー エクスチェンジ バージョン 2 の設定例 30
基本のインターネット キー エクスチェンジ バージョン 2 CLI 構造の設定例 30
例：IKEv2 キー リングの設定 30
例：プロファイルの設定 33
例：証明書および IKEv2 スマート デフォルトを使用するダイナミック ルーティングによる FlexVPN の設定 34
高度なインターネット キー エクスチェンジ バージョン 2 CLI 構造の設定例 35
例：プロポーザルの設定 35
例：ポリシーの設定 36
次の作業 37
インターネット キー エクスチェンジ バージョン 2（IKEv2）のその他の関連資料 37
インターネット キー エクスチェンジ バージョン 2（IKEv2）の設定に関する機能情報 39

第 4 章 **FlexVPN サーバの設定** 41
機能情報の確認 41

FlexVPN サーバの制限事項 42
デュアルスタック トンネル インターフェイスおよび VRF 認識 IPsec 42
AnyConnect プロファイルのダウンロードの制約事項 43
FlexVPN サーバに関する情報 43
EAP を使用するピア認証 43
IKEv2 コンフィギュレーション モード 45
IKEv2 認証 48
IKEv2 認証ポリシー 49
IKEv2 名前分割 50
IKEv2 マルチ SA 50
IKEv2 ダイナミック ルーティング 50
AnyConnect プロファイルのダウンロード 51
サポートされる RADIUS 属性 51
サポートされるリモート アクセス クライアント 54
Microsoft Windows 7 IKEv2 クライアント 54
Cisco IKEv2 AnyConnect クライアント 55
FlexVPN サーバの設定方法 55
FlexVPN サーバの IKEv2 プロファイルの設定 55
IKEv2 名前分割の設定 60
IKEv2 認証ポリシーの設定 62
FlexVPN サーバの構成例 68
例：FlexVPN サーバの設定 68
例：EAP を使用してピアを認証するための FlexVPN サーバの設定 68
例：グループ認証のための FlexVPN サーバの設定（外部 AAA） 68
例：グループ認証のための FlexVPN サーバの設定（ローカル AAA） 69
例：ユーザ認証のための FlexVPN サーバの設定 70
例：IPv6 設定属性による IPv6 セッション用の FlexVPN サーバの設定 71
例：AnyConnect プロファイルのダウンロードの設定 72
FlexVPN サーバの設定に関する追加情報 73
FlexVPN サーバの設定の機能情報 74

第 5 章 FlexVPN クライアントの設定 75
機能情報の確認 75
FlexVPN クライアントの制限事項 76
ローカル認証方式としての EAP 76
デュアルスタック トンネル インターフェイスおよび VRF 認識 IPsec 76
FlexVPN クライアントに関する情報 77
IKEv2 FlexVPN クライアント 77
トンネル有効化 79
バックアップ機能 79
デュアル FlexVPN のサポート 82
スプリット DNS のサポート 82
NAT 82
FlexVPN クライアントのネットワーク リストの学習方法 83
WINS NBNS およびドメイン名 83
イベント トレース 84
ローカル認証方式としての Extensible Authentication Protocol 84
FlexVPN クライアントの設定方法 84
IKEv2 VPN クライアント プロファイルの設定 84
トンネル インターフェイスの設定 85
FlexVPN クライアントの設定 86
ローカル認証方式としての EAP の設定 88
FlexVPN クライアントの構成例 89
例：IKEv2 FlexVPN クライアント プロファイルの設定 89
例：ローカル認証方式としての EAP の設定 90
FlexVPN クライアントの設定に関する追加情報 90
FlexVPN クライアントの設定の機能情報 91

第 6 章 IKEv2 ロード バランサの設定 93
機能情報の確認 93
IKEv2 ロード バランサの前提条件 93

IKEv2 ロード バランサに関する情報 94
IKEv2 ロード バランサの概要 94
IKEv2 ロード バランサの利点 96
IKEv2 リダイレクト メカニズム 96
IKEv2 初期交換中のリダイレクト（SA 初期化） 96
IKE_AUTH 交換中のリダイレクト（SA 認証） 97
互換性および相互運用性 98
リダイレクト ループ処理 98
IKEv2 クラスタの再接続 98
IKEv2 ロード バランサの設定方法 99
サーバ クラスタの設定 99
ロード バランシングに対する HSRP グループの設定 99
負荷管理メカニズムの設定 100
サーバでの IKEv2 リダイレクト メカニズムの有効化 103
クライアントでの IKEv2 リダイレクト メカニズムの有効化 103
IKEv2 ロード バランサの設定例 104
例：ロード バランシングに対する HSRP グループの設定 104
例：負荷管理メカニズムの設定 104
例：リダイレクト メカニズムの設定 105
例：クラスタ再接続キーの設定 105
その他の参考資料 105
IKEv2 ロード バランサの機能情報 107

第 7 章 **IKEv2 フラグメンテーションの設定 109**
機能情報の確認 109
IKEv2 フラグメンテーションの設定に関する情報 109
IKEv2 フラグメンテーション 109
ピア間のネゴシエーション 110
以前のリリースのフラグメンテーション サポート 111
フラグメントの暗号化、複合化、および再送信 111
フラグメンテーションおよび暗号化 111

復号と最適化 112
再送信 112
フラグメンテーションの有効化 112
IPv6 のサポート 113
IKEv2 フラグメンテーションの設定方法 113
IKEv2 フラグメンテーションの設定 113
IKEv2 フラグメンテーションの設定例 114
例：設定された MTU の表示が有効な IETF フラグメンテーション 114
例：発信側で設定される IETF 標準フラグメンテーション方式 115
例：発信側で設定されない IETF 標準フラグメンテーション方式 117
例：フラグメンテーションの IPv6 サポート 117
IKEv2 フラグメンテーションの設定に関する追加情報 119
IKEv2 フラグメンテーションの機能情報 120

第 8 章 **IKEv2 再接続の設定 121**
機能情報の確認 121
IKEv2 再接続設定の前提条件 121
IKEv2 再接続設定の制限事項 122
設定された IKEv2 フラグメンテーションに関する情報 122
IKEv2 および Cisco AnyConnect クライアントの再接続機能 122
Cisco IOS ゲートウェイと Cisco AnyConnect 間のメッセージ交換 123
IKEv2 再接続の設定方法 123
IKEv2 再接続の有効化 123
IKEv2 再接続設定のトラブルシューティング 124
IKEv2 再接続の設定例 125
例：IKEv2 再接続の有効化 125
IKEv2 再接続の設定に関する追加情報 126
IKEv2 再接続の機能情報 126

第 9 章 **IKEv2 パケット オブ ディスコネクトの設定 129**
機能情報の確認 129

IKEv2 パケット オブ ディスコネクトに関する情報 129
切断要求 129
IKEv2 パケット オブ ディスコネクト 130
IKEv2 パケット オブ ディスコネクトの設定方法 131
FlexVPN サーバでの AAA の設定 131
IKEv2 パケット オブ ディスコネクトの設定例 132
例：IKEv2 セッションの終了 132
IKEv2 パケット オブ ディスコネクトに関する追加情報 136
IKEv2 パケット オブ ディスコネクトの機能情報 137

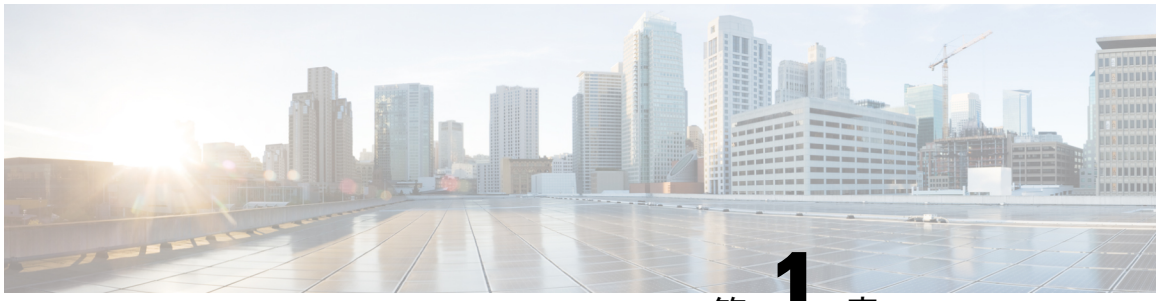
第 10 章 IKEv2 認可変更のサポートの設定 139
機能情報の確認 139
IKEv2 認可変更のサポートの前提条件 139
IKEv2 認可変更サポートの制限事項 140
IKEv2 認可変更サポートに関する情報 140
RADIUS 認可の変更 140
IKEv2 認可変更の作業 140
IKEv2 認可変更でサポートされる AV ペア 141
IKEv2 認可変更サポートの設定方法 141
FlexVPN サーバでの認可変更の設定 141
Cisco ASR 1000 シリーズ ルータでの IKEv2 認可変更サポートの確認 143
IKEv2 認可変更サポートの設定例 145
例：認可変更のトリガー 145
IKEv2 認可変更サポートに関する追加情報 146
IKEv2 認可変更のサポートの機能情報 146

第 11 章 集約認証の設定 149
機能情報の確認 149
集約認証の設定の前提条件 149
集約認証の設定に関する情報 150
Cisco AnyConnect および FlexVPN 150

集約認証の動作 150
Cisco AnyConnect EAP を使用する IKE 交換 152
IKEv2 でのデュアルファクタ認証のサポート 153
集約認証の設定方法 153
集約認証用の FlexVPN サーバの設定 153
集約認証の設定例 155
例：集約認証の設定 155
集約認証の設定に関する追加情報 156
集約認証の設定に関する機能情報 157

第 12 章 付録：**FlexVPN の RADIUS 属性** 159
FlexVPN RADIUS 属性 159

第 13 章 付録：**IKEv2 およびレガシー VPN** 173
例：事前共有キー認証方式を使用する暗号マップベースの IKEv2 ピアの設定 173
例：証明書認証方式を使用する暗号マップベースの IKEv2 ピアの設定 176
例：暗号マップ ベースおよび dVTI ベースの IKEv2 ピアの設定 180
例： sVTI ベース IKEv2 ピアを使用した IPSec の設定 182
例：DMVPN ネットワークでの IKEv2 の設定 185



第 1 章

最初にお読みください

Cisco IOS XE 16 に関する重要な情報

現行の Cisco IOS XE Release 3.7.0E（Catalyst スイッチング用）および Cisco IOS XE Release 3.17S（アクセスおよびエッジルーティング用）の 2 つのリリースは、単一バージョンのコンバージドリリース Cisco IOS XE 16 に進化（マージ）しました。これにより、スイッチングおよびルーティング ポートフォリオにおける広範なアクセス製品およびエッジ製品を 1 つのリリースでカバーします。

機能情報

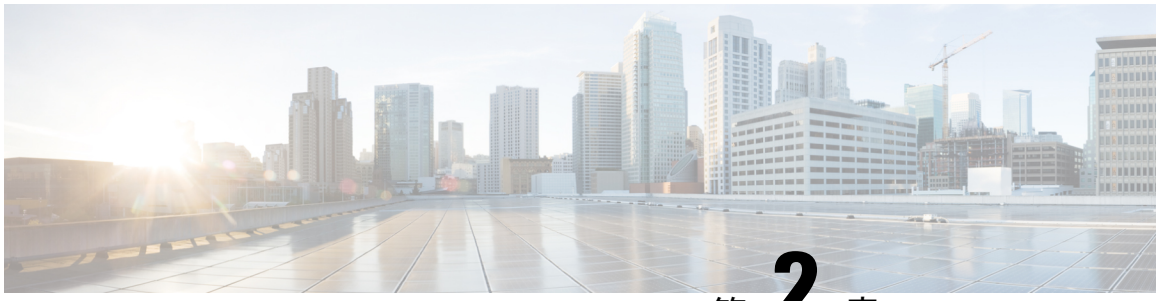
機能のサポート、プラットフォームのサポート、およびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco.com のアカウントは必要ありません。

参考資料

- 『Cisco IOS コマンド リファレンス』、すべてのリリース

マニュアルの入手方法およびテクニカル サポート

- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、シスコ サービスにアクセスしてください。
- サービス リクエストを送信するには、シスコ サポートにアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco Marketplace にアクセスしてください。
- 一般的なネットワーキング、トレーニング、認定関連の出版物を入手するには、Cisco Press にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder にアクセスしてください。



第 2 章

FlexVPN の概要

RFC 4306 に基づく次世代のキー管理プロトコルであるインターネット キー エクスチェンジ バージョン 2（IKEv2）は、IKE プロトコルの機能拡張です。IKEv2 は、相互認証を実行して SA を確立および管理するために使用します。

FlexVPN は、シスコによる IKEv2 標準の実装であり、サイト間アクセス、リモート アクセス、ハブ アンド スポーク トポロジ、および部分メッシュ（スポーク間ダイレクト）を組み合わせたユニファイド パラダイムと CLI を備えています。FlexVPN は、トンネル インターフェイス パラダイムを広範に使用し、かつ暗号マップを使用してレガシー VPN 実装との互換性を維持するシンプルなモジュラ フレームワークを提供します。

本書の構成は、次のとおりです。

- インターネット キー エクスチェンジ バージョン 2（IKEv2）および FlexVPN リモート アクセスの設定 （3 ページ）
- FlexVPN サーバの設定 （4 ページ）
- FlexVPN クライアントの設定 （4 ページ）
- IKEv2 ロード バランサの設定 （4 ページ）
- IKEv2 フラグメンテーションの設定 （4 ページ）
- IKEv2 再接続の設定 （4 ページ）
- IKEv2 パケット オブ ディスコネクトの設定 （4 ページ）
- IKEv2 認可変更のサポートの設定 （5 ページ）
- 集約認証の設定 （5 ページ）
- 付録：FlexVPN の RADIUS 属性 （5 ページ）
- 付録：IKEv2 およびレガシー VPN （5 ページ）

インターネット キー エクスチェンジ バージョン 2（IKEv2）および FlexVPN リモート アクセスの設定

このモジュールでは IKEv2 CLI について説明します。このモジュールは、基本セクションと高度なセクションに分かれています。

基本セクションでは、基本のIKEv2コマンドを紹介し、IKEv2スマートデフォルトとFlexVPNリモート アクセスに必要な必須の IKEv2 コマンドについて説明します。このモジュールは、後続の章を理解するための前提条件です。

高度なセクションでは、グローバル IKEv2 コマンドについて説明します。また、デフォルト IKEv2 コマンドをオーバーライドする方法についても説明します。

FlexVPN サーバの設定

このモジュールでは、FlexVPN サーバの機能、FlexVPN サーバの設定に必要な IKEv2 コマンド、リモート アクセス クライアント、およびサポートされる RADIUS 属性について説明します。

FlexVPN クライアントの設定

このモジュールでは、FlexVPN クライアント機能と FlexVPN クライアントに必要な IKEv2 コマンドについて説明します。

IKEv2 ロード バランサの設定

このモジュールでは、IKEv2 ロード バランサ サポート機能と、IKEv2 ロード バランサの設定に必要な IKEv2 コマンドについて説明します。

IKEv2 フラグメンテーションの設定

RFC 機能に準拠した IKE フラグメンテーションでは、IETF の **draft-ietf-ipsecme-ikev2-fragmentation-10** ドキュメントの提案に従って、インターネット キー エクスチェンジ バージョン 2 （IKEv2）パケットのフラグメンテーションを実装しました。

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 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 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。

集約認証の設定

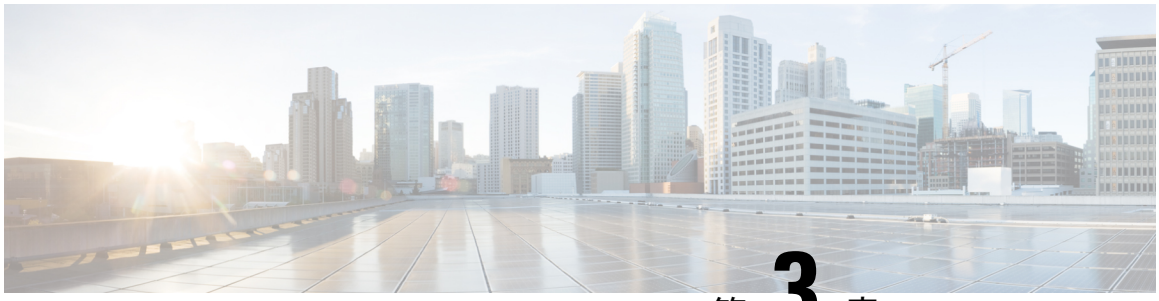
FlexVPN RA - Cisco AnyConnect クライアントのサポートを拡張することで、AnyConnect 機能の集約認証サポートは、集約認証方式を実装します。このクライアントでは、独自の AnyConnect EAP 認証方式を使用し、Cisco AnyConnect クライアントと FlexVPN サーバ間にインターネットを介したセキュア トンネルを確立します。

付録：FlexVPN の RADIUS 属性

このモジュールでは、FlexVPN サーバでサポートされる RADIUS 属性について説明します。

付録：IKEv2 およびレガシー VPN

このモジュールには、暗号化マップやインターネット キー エクスチェンジ バージョン 2（IKEv2）による DMVPN などのレガシー VPN の設定例が含まれています。



第 3 章

インターネット キー エクスチェンジ バージョン 2

このモジュールには、基本および高度なインターネット キー エクスチェンジ バージョン 2（IKEv2）の情報と設定手順が含まれています。このモジュールの IKEv2 のタスクおよび設定例は、次のように分類されます。

- 基本の IKEv2：基本の IKEv2 コマンド、IKEv2 スマート デフォルト、基本の IKEv2 プロファイル、および IKEv2 キー リングに関する情報が示されています。
- 高度な IKEv2：グローバルな IKEv2 コマンドに関する情報と、IKEv2 スマート デフォルトのオーバーライド方法が示されています。

（注） セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。最新のシスコの暗号化に関する推奨事項については、『Next Generation Encryption』（NGE）ホワイト ペーパーを参照してください。

- 機能情報の確認 （8 ページ）
- インターネット キー交換バージョン 2 の設定に関する前提条件 （8 ページ）
- インターネット キー エクスチェンジ バージョン 2 の設定に関する制約事項 （8 ページ）
- インターネット キー エクスチェンジ バージョン 2 に関する情報 （9 ページ）
- インターネット キー交換バージョン 2 の設定方法 （14 ページ）
- インターネット キー エクスチェンジ バージョン 2 の設定例 （30 ページ）
- 次の作業 （37 ページ）
- インターネット キー エクスチェンジ バージョン 2（IKEv2）のその他の関連資料 （37 ページ）
- インターネット キー エクスチェンジ バージョン 2（IKEv2）の設定に関する機能情報 （39 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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。

インターネット キー交換バージョン 2 の設定に関する前提条件

「Configuring Security for VPNs with IPsec」モジュールで説明している概念および作業を理解している必要があります。

インターネット キー エクスチェンジ バージョン 2 の設定に関する制約事項

特定のプラットフォーム上でサポートされないオプションを設定することはできません。たとえば、セキュリティ プロトコルでハードウェア クリプト エンジンの機能が重要である場合、エクスポート可能でないイメージ内で Triple Data Encryption Standard（3DES）または Advanced Encryption Standard（AES）の各タイプの暗号化トランスフォームを指定できず、暗号エンジンでサポートされない暗号化アルゴリズムを指定できません。

（注） IKEv2 は、統合サービス ルータ（ISR）G1 ではサポートしていません。

インターネット キー エクスチェンジ バージョン 2 に関する情報

IKEv2 のサポート対象規格

シスコでは、インターネット キー エクスチェンジ バージョン 2（IKEv2）で使用するための IP セキュリティ（IPsec）プロトコル規格を実装しています。

（注） DES または MD5（HMAC バリアントを含む）の使用は、現在推奨されていません。代わりに、AES および SHA-256 を使用してください。最新のシスコの暗号化の推奨事項の詳細については、『Next Generation Encryption』（NGE）のホワイト ペーパーを参照してください。

IKEv2 で実装されるコンポーネント技術は、次のとおりです。

- AES-CBC：高度暗号化規格暗号ブロック連鎖（AES-CBC）。
- SHA（HMAC バリアント）：セキュア ハッシュ アルゴリズム（SHA）。
- Diffie-Hellman：公開キー暗号法プロトコル。
- DES：データ暗号規格（現在は推奨されていません）。
- MD5（HMAC（ハッシュベースのメッセージ認証コード）バリアント）：メッセージ ダイジェスト アルゴリズム 5（現在は推奨されていません）。

サポートされる規格およびコンポーネント技術の詳細については、『*Internet Key Exchange for IPsec VPNs Configuration Guide*』の『Configuring Internet Key Exchange for IPsec VPNs』モジュールにある「Supported Standards for Use with IKE」の項を参照してください。

IKEv2 の利点

デッド ピア検出とネットワーク アドレス変換トラバーサル

インターネット キー エクスチェンジ バージョン 2（IKEv2）にはデッド ピア検出（DPD）とネットワーク アドレス変換トラバーサル（NAT-T）のサポートが組み込まれています。

証明書の URL

証明書は IKEv2 パケット内で送信されるのではなく URL とハッシュを通じて参照できるため、フラグメンテーションを回避できます。

DoS 攻撃の復元力

IKEv2 は、要求者を確認するまで要求を処理しません。これにより、偽の場所から大量の暗号化（高コスト）処理を実行するようにスプーフィングされる可能性がある IKEv1 でのサービス妨害（DoS）の問題にある程度対処しています。

EAP のサポート

IKEv2 では認証に Extensible Authentication Protocol（EAP）を使用できます。

複数の暗号エンジン

ネットワークに IPv4 と IPv6 の両方のトラフィックがあり、複数の暗号エンジンがある場合、次のいずれかの設定オプションを選択します。

- 1 つのエンジンで IPv4 トラフィックを処理し、他方のエンジンで IPv6 トラフィックを処理する。
- 1 つのエンジンで IPv4 と IPv6 の両方のトラフィックを処理する。

信頼性と状態管理（ウィンドウイング）

IKEv2 では、信頼性を提供するためにシーケンス番号と確認が使用され、エラー処理ロジスティックと共有状態管理が要求されます。

インターネット キー エクスチェンジ バージョン 2 CLI の構成

IKEv2 プロポーザル

インターネット キー エクスチェンジ バージョン 2（IKEv2）のプロポーザルは、IKE_SA_INIT 交換の一部としてインターネット キー エクスチェンジ（IKE）セキュリティ アソシエーション（SA）のネゴシエーションで使用されるトランスフォームのコレクションです。ネゴシエーションで使用されるトランスフォームのタイプは、次のとおりです。

- 暗号化アルゴリズム
- 整合性アルゴリズム
- Pseudo-Random Function（PRF）アルゴリズム
- デフィーヘルマン（DH）グループ

デフォルト IKEv2 プロポーザルについては、「IKEv2 スマート デフォルト」の項を参照してください。デフォルト IKEv2 プロポーザルをオーバーライドする方法および新しいプロポーザルを定義する方法については、高度な IKEv2 CLI 構造の設定に関する項を参照してください。

IKEv2 ポリシー

IKEv2 ポリシーには、IKE_SA_INIT 交換での暗号化、整合性、PRF アルゴリズム、および DH グループのネゴシエーションに使用されるプロポーザルが含まれています。これには match 文を含めることができ、ネゴシエーション時にポリシーを選択するための選択基準として使用されます。

デフォルト IKEv2 ポリシーについては、「IKEv2 スマート デフォルト」の項を参照してください。デフォルト IKEv2 ポリシーをオーバーライドする方法および新しいポリシーを定義する方法については、高度な IKEv2 CLI 構造の設定に関する項を参照してください。

IKEv2 プロファイル

IKEv2 プロファイルは、IKE SA のネゴシエーション可能でないパラメータ（ローカル ID またはリモート ID および認証方式）と、そのプロファイルと一致する認証相手が使用できるサービスのリポジトリです。IKEv2 プロファイルは、発信側の暗号マップまたは IPsec プロファイルのいずれかにアタッチされる必要があります。IKEv2 プロファイルは、応答側では必須ではありません。

IKEv2 キー リング

IKEv2 キー リングは対称および非対称の事前共有キーのリポジトリであり、IKEv1 キー リングとは無関係です。IKEv2 キー リングは 1 つの IKEv2 プロファイルと関連付けられるため、その IKEv2 プロファイルに一致する一連のピアをサポートします。IKEv2 キー リングは、関連付けられた IKEv2 プロファイルから VPN ルーティングおよび転送（VRF）コンテキストを取得します。

IKEv2 スマート デフォルト

IKEv2 スマート デフォルト機能は、ほとんどの使用例に対応することで FlexVPN 設定を最小化します。IKEv2 スマート デフォルトは特定の使用例向けにカスタマイズできますが、これはお勧めしません。

デフォルト IKEv2 構造を変更する方法については、高度な IKEv2 CLI 構造の設定に関する項を参照してください。

次のルールが IKEv2 スマート デフォルト機能に適用されます。

1. デフォルト設定は、**default** をキーワードとして指定して引数を指定しない、対応する **show** コマンドで表示されます。たとえば、**show crypto ikev2 proposal default** コマンドではデフォルト IKEv2 プロポーザルが表示され、**show crypto ikev2 proposal** コマンドではユーザ設定されたプロポーザルと共にデフォルト IKEv2 プロポーザルが表示されます。
2. デフォルト設定は、**show running-config all** コマンドで表示されます。**show running-config** コマンドでは表示されません。
3. **show running-config all** コマンドで表示されるデフォルト設定を変更できます。

4. コマンドの **no** 形式（**no crypto ikev2 proposal default** など）を使用して、デフォルト設定を無効にすることができます。無効化されたデフォルト設定はネゴシエーションで使用されませんが、設定は **show running-config** コマンドで表示されます。無効化されたデフォルト設定では、ユーザ変更が失われてシステム設定値が復元されます。
5. デフォルト設定は、コマンドのデフォルト形式（**default crypto ikev2 proposal** など）を使用すると再度有効にすることができ、システム設定値が復元されます。
6. デフォルト トランスフォーム セットのデフォルト モードは、トランスポートです。その他すべてのトランスフォーム セットのデフォルト モードは、トンネルです。

（注） MD5（HMAC バリアントを含む）や Diffie-Hellman（DH）グループ 1、2、および 5 の使用は、現在は推奨されていません。代わりに、SHA-256 および DH グループ 14 以降を使用してください。最新のシスコの暗号化の推奨事項の詳細については、『Next Generation Encryption』（NGE）のホワイト ペーパーを参照してください。

次の表に、IKEv2 スマート デフォルト機能によって有効化されるコマンドをデフォルト値と共に示します。

表 *1 : IKEv2* コマンドのデフォルト

コマンド名	デフォルト値

crypto ikev2 authorization policy	`Device# show crypto ikev2 authorization policy default`
	
	`IKEv2 Authorization policy: default`
	`route set interface`
	`route accept any tag: 1 distance: 2`

crypto ikev2 proposal	`Device# show crypto ikev2 proposal default`
	
	`IKEv2 proposal: default`
	`Encryption: AES-CBC-256 AES-CBC-192 AES-CBC-128`
	`Integrity: SHA512 SHA384 SHA256 SHA96 MD596`
	`PRF: SHA512 SHA384 SHA256 SHA1 MD5`
	`DH Group: DH_GROUP_1536_MODP/Group 5 DH_GROUP_1024_MODP/Group 2.`

crypto ikev2 policy	`Device# show crypto ikev2 policy default`
	
	`IKEv2 policy: default`
	`Match fvrf: any`
	`Match address local: any`
	`Proposal: default`

コマンド名	デフォルト値

crypto ipsec profile	Device# **show crypto ipsec profile default**
	
	IPSEC profile default
	Security association lifetime: 4608000 kilobytes/3600 seconds
	Responder-Only (Y/N): N
	PFS (Y/N): N
	Transform sets={
	default: { esp-aes esp-sha-hmac },
	}

crypto ipsec transform-set	Device# **show crypto ipsec transform-set default** Transform set default: { esp-aes esp-sha-hmac } will negotiate = { Tunnel, },

（注） デフォルト IPsec プロファイルを使用する前に、**tunnel protection ipsec profile default** コマンドを使用してトンネル インターフェイスで **crypto ipsec profile** コマンドを明示的に指定します。

IKEv2 Suite-B サポート

Suite-B は、暗号の近代化プログラムの一環として国家安全保障局によって交付された一連の暗号化アリゴリズムです。インターネット キー エクスチェンジ（IKE）および IPsec の Suite-B は、RFC 4869 で定義されます。Suite-B のコンポーネントは、次のとおりです。

- IKEv2 プロポーザルで設定された Advanced Encryption Standard（AES）の 128 ビット キーおよび 256 ビット キー。データ トラフィックの場合、AES は、IPsec トランスフォーム セットに設定されるガロア カウンタ モード（GCM）で使用する必要があります。
- IKEv2 プロファイルに設定された楕円曲線デジタル署名アルゴリズム（ECDSA）。
- IKEv2 プロポーザルおよび IPsec トランスフォーム セットに設定されたセキュア ハッシュ アルゴリズム 2（SHA-256 および SHA-384）。

Suite-B の要件は、IKE および IPSec で使用するために、暗号化アルゴリズムの 4 つのユーザ インターフェイス スイートで構成されています。各スイートは、暗号化アルゴリズム、デジタル署名アルゴリズム、キー合意アルゴリズム、ハッシュまたはメッセージ ダイジェスト アルゴリズムで構成されています。Cisco での Suite-B サポートに関する詳細については、『Configuring Security for VPNs with IPsec』機能モジュールを参照してください。

AES-GCM のサポート

認証済みの暗号化アルゴリズムは、暗号化と整合性の組み合わさった機能を提供します。このようなアルゴリズムは、連結モード アルゴリズムと呼ばれます。IOS 上における IKEv2 暗号としての AES-GCM サポート機能では、ガロア/カウンタ モードの Advanced Encryption Standard

（AES-GCM）を追加することによって、IKEv2 プロトコルの暗号化メッセージに認証済みの暗号化アルゴリズムを使用できます。AES-GCM は、128 ビットおよび 256 ビットのキー サイズ（AES-GCM-128 および AES-GCM-256）をサポートします。

（注） 暗号化アルゴリズムが AES-GCM のみの場合、整合性アルゴリズムをプロポーザルに追加することはできません。

IKEv2 での自動トンネル モードのサポート

複数ベンダー シナリオで VPN ヘッドエンドを設定する場合は、ピアまたはレスポンダの技術的な詳細を認識しておく必要があります。たとえば、一部のデバイスは IPsec トンネルを使用しているが、他のデバイスは Generic Routing Encapsulation（GRE）または IPsec トンネルを使用している場合やトンネルが IPv4 または IPv6 の場合があります。最後のケースでは、インターネット キー エクスチェンジ（IKE）プロファイルと仮想テンプレートを設定する必要があります。

トンネル モード自動選択機能は、設定を容易にし、レスポンダの詳細の入手を支援します。この機能は、IKE プロファイルから仮想アクセス インターフェイスが作成されるとすぐに、トンネリング プロトコル（GRE または IPsec）とトランスポート プロトコル（IPv4 または IPv6）を自動的に仮想テンプレートに適用します。この機能は、Cisco AnyConnect VPN Client や Microsoft Windows7 Client などのマルチベンダー リモート アクセスを集約しているデュアル スタック ハブ上で役に立ちます。

（注） トンネル モード自動選択機能は、レスポンダの設定のみを容易にします。トンネルはイニシエータに対して静的に設定する必要があります。

トンネル モードの自動選択機能は、IKEv2 プロファイル設定で **virtual-template** コマンドに **auto mode** キーワードを使用するとアクティブ化できます。

インターネット キー交換バージョン 2 の設定方法

基本のインターネット キー エクスチェンジ バージョン 2 CLI 構造の設定

暗号化インターフェイスで IKEv2 を有効にするには、インターネット キー エクスチェンジ バージョン 2（IKEv2）プロファイルをそのインターフェイスに適用される暗号マップまたは IPsec プロファイルにアタッチします。IKEv2 応答側では、この手順は任意です。

（注） IKEv1 と IKEv2 の違いは、IKEv1 はデバイス上のすべてのインターフェイスでグローバルに有効になっているため、個々のインターフェイスで IKEv1 を有効にする必要がないことです。

基本の IKEv2 構造を手動で設定するには、次のタスクを実行します。

IKEv2 キーリングの設定

このタスクは、ローカルまたはリモート認証方式が事前共有キーの場合に、IKEv2 キーリングを設定するために実行します。

IKEv2 キーリング キーは、ピア サブブロックを定義するピア コンフィギュレーション サブモードで設定する必要があります。IKEv2 キーリングには、複数のピア サブブロックを含めることができます。1 つのピア サブブロックには、ホスト名、ID、および IP アドレスの任意の組み合わせで識別される 1 つのピアまたはピア グループ用の単一の対称または非対称キー ペアが含まれています。

IKEv2 キーリングは IKEv1 キーリングと無関係です。主な違いは次のとおりです。

- IKEv2 キーリングは、対称事前共有キーと非対称事前共有キーをサポートします。
- IKEv2 キーリングは、Rivest、Shamir、および Adleman（RSA）公開キーをサポートしません。
- IKEv2 キーリングは、IKEv2 プロファイル内で指定され、ルックアップされないため、事前共有キー認証方式をネゴシエートするために MM1 の受信時にキーがルックアップされる IKEv1 とは異なります。IKEv2 では、認証方式がネゴシエートされません。
- IKEv2 キーリングは、設定時に VPN ルーティングおよび転送（VRF）と関連付けられません。IKEv2 キーリングの VRF は、そのキーリングを参照している IKEv2 プロファイルの VRF です。
- 複数のキー リングを指定できる IKEv1 プロファイルとは異なり、IKEv2 プロファイルでは 1 つのキー リングを指定できます。
- 同じキーが別々のプロファイルと一致するピア全体で共有されている場合は、1 つのキーリングを複数の IKEv2 プロファイルで指定できます。
- IKEv2 キーリングは 1 つ以上のピア サブブロックとして構造化されます。

IKEv2 イニシエータでは、ピアのホスト名またはアドレスを使用してその順に IKEv2 キーリング キー ルックアップが実行されます。IKEv2 レスポンダでは、ピアの IKEv2 ID またはアドレスを使用してその順にキー ルックアップが実行されます。

（注） 複数のピアで同じ ID を設定することはできません。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ikev2 keyring** *keyring-name*
4. **peer** *name*
5. **description** *line-of-description*
6. **hostname** *name*
7. **address** {*ipv4-address* [*mask*] | *ipv6-address prefix*}
8. **identity** {**address** {*ipv4-address* | *ipv6-address*} | **fqdn domain** *domain-name* | **email domain** *domain-name* | **key-id** *key-id*}
9. **pre-shared-key** {**local** | **remote**} [**0** | **6**] *line* **hex** *hexadecimal-string*
10. **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 keyring** *keyring-name* 例： `Device(config)# crypto ikev2 keyring kyr1`	IKEv2 キーリングを定義し、IKEv2 キーリング 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	**peer** *name* 例： `Device(config-ikev2-keyring)# peer peer1`	ピアまたはピア グループを定義し、IKEv2 キーリング コンフィギュレーション モードを開始します。
ステップ 5	**description** *line-of-description* 例： `Device(config-ikev2-keyring-peer)# description this is the first peer`	（任意）ピアまたはピア グループを記述します。
ステップ 6	**hostname** *name* 例： `Device(config-ikev2-keyring-peer)# hostname host1`	ホスト名を使用してピアを指定します。
ステップ 7	**address** {*ipv4-address* [*mask*]	*ipv6-address prefix*} 例：	ピアの IPv4 アドレス、IPv6 アドレス、または範囲を指定します。

	コマンドまたはアクション	目的
	`Device(config-ikev2-keyring-peer)# address 10.0.0.1 255.255.255.0`	（注） この IP アドレスが IKE エンドポイント アドレスであり、ID アドレスとは別個のものです。
ステップ 8	**identity** {**address** {*ipv4-address* | *ipv6-address*} | **fqdn domain** *domain-name* | **email domain** *domain-name* | **key-id** *key-id*} 例： `Device(config-ikev2-keyring-peer)# identity address 10.0.0.5`	次の ID を使用して IKEv2 ピアを特定します。 • 電子メール • 完全修飾ドメイン名（FQDN） • IPv4 アドレスまたは IPv6 アドレス • キー ID （注） ID は IKEv2 レスポンダ上のキー ルックアップにしか使用できません。
ステップ 9	**pre-shared-key** {**local** | **remote**} [**0** | **6**] *line* **hex** *hexadecimal-string* 例： `Device(config-ikev2-keyring-peer)# pre-shared-key local key1`	ピアの事前共有キーを指定します。
ステップ 10	**end** 例： `Device(config-ikev2-keyring-peer)# end`	IKEv2 キーリング ピア コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

次の作業

IKEv2 キー リングの設定後、IKEv2 プロファイルを設定します。詳細については、「IKEv2 プロファイルの設定（基本）」セクションを参照してください。

IKEv2 プロファイルの設定（基本）

このタスクは、IKEv2 プロファイル用の必須コマンドを設定するために実行します。

IKEv2 プロファイルは、IKE セキュリティ アソシエーション（SA）（ローカル ID またはリモート ID と認証方式など）のネゴシエーション不能パラメータと、そのプロファイルと一致する認証されたピアが使用可能なサービスのリポジトリです。IKEv2 プロファイルは、設定して、IKEv2 イニシエータ上のクリプト マップと IPSec プロファイルのどちらかに関連付ける必要があります。プロファイルを暗号マップまたは IPsec プロファイルに関連付けるには、**set ikev2-profile** *profile-name* コマンドを使用します。プロファイルの関連付けを解除するには、このコマンドの **no** 形式を使用します。

次のルールが match ステートメントに適用されます。

- IKEv2 プロファイルには、match identity ステートメントまたは match certificate ステートメントを含める必要があります。そうしないと、プロファイルが不完全と見なされ、使用さ

れません。IKEv2 プロファイルには、複数の match identity ステートメントまたは match certificate ステートメントを含めることができます。

- IKEv2 プロファイルには、単一の match Front Door VPN routing and forwarding (FVRF) ステートメントを含める必要があります。
- プロファイルを選択すると、同じタイプの複数の match ステートメントが論理的に OR され、違うタイプの複数の match ステートメントが論理的に AND されます。
- match identity ステートメントと match certificate ステートメントは、同じタイプのステートメントと見なされ、OR されます。
- 重複したプロファイルの設定は、設定ミスと見なされます。複数のプロファイルが一致した場合は、どのプロファイルも選択されません。

IKEv2 プロファイルを表示するには、**show crypto ikev2 profile** *profile-name* コマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ikev2 profile** *profile-name*
4. **description** *line-of-description*
5. **aaa accounting** {**psk** | **cert** | **eap**} *list-name*
6. **authentication** {**local** {**rsa-sig** | **pre-share** [**key** {**0** | **6**} *password*}] | **ecdsa-sig** | **eap** [**gtc** | **md5** | **ms-chapv2**] [**username** *username*] [**password** {**0** | **6**} *password*}]} | **remote** {**eap** [**query-identity** | **timeout** *seconds*] | **rsa-sig** | **pre-share** [**key** {**0** | **6**} *password*}] | **ecdsa-sig**}}
7. **dpd** *interval retry-interval* {**on-demand** | **periodic**}
8. **identity local** {**address** {*ipv4-address* | *ipv6-address*} | **dn** | **email** *email-string* | **fqdn** *fqdn-string* | **key-id** *opaque-string*}
9. **initial-contact force**
10. **ivrf** *name*
11. **keyring** {**local** *keyring-name* | **aaa** *list-name* [**name-mangler** *mangler-name* | **password** *password*] }
12. **lifetime** *seconds*
13. **match** {**address local** {*ipv4-address* | *ipv6-address* | **interface** *name*} | **certificate** *certificate-map* | **fvrf** {*fvrf-name* | **any**} | **identity remote address** {*ipv4-address* [*mask*] | *ipv6-address prefix*} | {**email** [*domain string*] | **fqdn** [*domain string*]} *string* | **key-id** *opaque-string*}
14. **nat keepalive** *seconds*
15. **pki trustpoint** *trustpoint-label* [**sign** | **verify**]
16. **virtual-template** *number* **mode auto**
17. **shutdown**
18. **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	**description** *line-of-description* 例： `Device(config-ikev2-profile)# description This is an IKEv2 profile`	（任意）プロファイルを記述します。
ステップ 5	**aaa accounting** {**psk** | **cert** | **eap**} *list-name* 例： `Device(config-ikev2-profile)# aaa accounting eap list1`	（任意）IPsec セッションの認証、認可、およびアカウンティング（AAA）アカウンティング方式リストを有効にします。 （注） **psk**、**cert**、または **eap** キーワードが指定されなかった場合は、ピア認証方式に関係なく、AAA アカウンティング方式リストが使用されます。
ステップ 6	**authentication** {**local** {**rsa-sig** | **pre-share** [**key** {**0** | **6**} *password*}] | **ecdsa-sig** | **eap** [**gtc** | **md5** | **ms-chapv2**] [**username** *username*] [**password** {**0** | **6**} *password*}]} | **remote** {**eap** [**query-identity** | **timeout** *seconds*] | **rsa-sig** | **pre-share** [**key** {**0** | **6**} *password*}] | **ecdsa-sig**}} 例： `Device(config-ikev2-profile)# authentication local ecdsa-sig`	ローカルまたはリモートの認証方式を指定します。 • **rsa-sig**：認証方式として RSA-sig を指定します。 • **pre-share**：認証方式として事前共有キーを指定します。 • **ecdsa-sig**：認証方式として ECDSA-sig を指定します。 • **eap**：リモート認証方式として EAP を指定します。 • **query-identity**：ピアに EAP ID を問い合わせます。 • **timeout** *seconds*：最初の IKE_AUTH 応答を返してから次の IKE_AUTH 要求を受け取るまでの期間を秒単位で指定します。

	コマンドまたはアクション	目的
		（注） ローカル認証方式は 1 つしか指定できませんが、リモート認証方式は複数指定できます。
ステップ 7	**dpd** *interval retry-interval* {**on-demand** | **periodic**} 例： `Device(config-ikev2-profile)# dpd 30 6 on-demand`	（任意）プロファイルと一致したピアのデッド ピア検出（DPD）をグローバルに設定します。 • Dead Peer Detection（DPD：デッドピア検出）はデフォルトでは無効化されています。 （注） この手順の例では、着信 ESP トラフィックがない場合、最初の DPD が 30 秒後に送信されます。6 秒間（指定された再試行間隔）待機した後、DPD 再試行が 6 秒間隔でアグレッシブに5回送信されます。そのため、合計 66 秒（30 + 6 + 6 X 5 = 66）が経過すると、DPD によって暗号化セッションが切断されます。
ステップ 8	**identity local** {**address** {*ipv4-address* | *ipv6-address*} | **dn** | **email** *email-string* | **fqdn** *fqdn-string* | **key-id** *opaque-string*} 例： `Device(config-ikev2-profile)# identity local email abc@example.com`	（任意）ローカル IKEv2 ID タイプを指定します。 （注） ローカル認証方式が事前共有キーの場合は、デフォルトのローカル ID が IP アドレスになります。ローカル認証方式が Rivest、Shamir、および Adleman（RSA）署名の場合は、デフォルトのローカル ID が識別名になります。
ステップ 9	**initial-contact force** 例： `Device(config-ikev2-profile)# initial-contact force`	初期連絡先通知が IKE_AUTH 交換で受信されなかった場合に、初期連絡先処理を強制します。
ステップ 10	**ivrf** *name* 例： `Device(config-ikev2-profile)# ivrf vrf1`	（任意）IKEv2 プロファイルがクリプト マップにアタッチされている場合に、ユーザ定義の VPN ルーティングおよび転送（VRF）またはグローバル VRF を指定します。 • IKEv2 プロファイルがトンネル保護に使用されている場合は、トンネル インターフェイス上で Inside VRF（IVRF）を設定する必要があります。 （注） IVRF は、クリア テキスト パケット用の VRF を指定します。IVRF のデフォルト値は FVRF です。

	コマンドまたはアクション	目的
ステップ 11	**keyring** {**local** *keyring-name* | **aaa** *list-name* [**name-mangler** *mangler-name* | **password** *password*] }	ローカルまたはリモートの事前共有キー認証方式で使用する必要があるローカルまたはAAAベースのキーリングを指定します。
	例： `Device(config-ikev2-profile)# keyring aaa keyring1 name-mangler mangler1`	（注） 1つのキーリングしか指定することができません。ローカル AAA は AAA ベースの事前共有キーに対してサポートされません。 （注） リリースによっては、**local** キーワードと **name-mangler** *mangler-name* キーワード引数ペアを使用する必要があります。 （注） AAAを使用する場合、Radiusアクセス要求のデフォルトパスワードは「cisco」です。パスワードを変更するには、**keyring** コマンド内で **password** キーワードを使用します。
ステップ 12	**lifetime** *seconds*	IKEv2 SA のライフタイムを秒単位で指定します。
	例： `Device(config-ikev2-profile)# lifetime 1000`	
ステップ 13	**match** {**address local** {*ipv4-address* | *ipv6-address* | **interface** *name*} | **certificate** *certificate-map* | **fvrf** {*fvrf-name* | **any**} | **identity remote address** {*ipv4-address* [*mask*] | *ipv6-address prefix*} | {**email** [*domain string*] | **fqdn** [*domain string*]} *string* | **key-id** *opaque-string*}	match ステートメントを使用して、ピア用の IKEv2 プロファイルを選択します。
	例： `Device(config-ikev2-profile)# match address local interface Ethernet 2/0`	
ステップ 14	**nat keepalive** *seconds*	（任意）NAT キープアライブを有効にして、その期間を秒単位で指定します。 • NAT はデフォルトで無効化されています。
	例： `Device(config-ikev2-profile)# nat keepalive 500`	
ステップ 15	**pki trustpoint** *trustpoint-label* [**sign** | **verify**]	RSA 署名認証方式で使用する Public Key Infrastructure（PKI）トラストポイントを指定します。
	例： `Device(config-ikev2-profile)# pki trustpoint tsp1 sign`	（注） **sign** または **verify** キーワードが指定されていない場合、トラストポイントは署名と検証に使用されます。

	コマンドまたはアクション	目的
		（注） IKEv1 とは対照的に、証明書ベースの認証を成功させるためにトラストポイントを IKEv2 プロファイル内で設定する必要があります。このコマンドが設定内に存在しない場合は、グローバルに設定されたトラストポイントのフォールバックが存在しません。トラストポイント設定は IKEv2 イニシエータおよびレスポンダに適用されます。
ステップ 16	**virtual-template** *number* **mode auto** 例： `Device(config-ikev2-profile)# virtual-template 1 mode auto`	（任意）仮想アクセス インターフェイス（VAI）の複製用の仮想テンプレートを指定します。 • **mode auto**：トンネル モード自動選択機能を有効にします。 （注） IPsec ダイナミック仮想トンネル インターフェイス（DVTI）では、仮想テンプレートを IKEv2 セッションが開始されない IKEv2 プロファイル内で指定する必要があります。
ステップ 17	**shutdown** 例： `Device(config-ikev2-profile)# shutdown`	（任意）IKEv2 プロファイルをシャット ダウンします。
ステップ 18	**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。

高度なインターネット キー エクスチェンジ バージョン 2 CLI 構造の設定

この項では、グローバル IKEv2 CLI 構造について説明します。また、IKEv2 のデフォルト CLI 構造をオーバーライドする方法についても説明します。IKEv2 スマート デフォルトは、ほとんどの使用例をサポートします。そのため、デフォルトで対応されない特定の使用例に必要な場合にのみ、デフォルトをオーバーライドすることをお勧めします。

高度な IKEv2 CLI 構造を設定するには、次のタスクを実行します。

グローバル IKEv2 オプションの設定

この作業は、ピアに依存しないグローバル IKEv2 オプションを設定するために実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ikev2 certificate-cache** *number-of-certificates*
4. **crypto ikev2 cookie-challenge** *number*
5. **crypto ikev2 diagnose error** *number*
6. **crypto ikev2 dpd** *interval retry-interval* {**on-demand** | **periodic**}
7. **crypto ikev2 http-url cert**
8. **crypto ikev2 limit** { **max-in-negotiation-sa** *limit* | **max-sa** *limit*}
9. **crypto ikev2 nat keepalive** *interval*
10. **crypto ikev2 window** *size*
11. **crypto logging ikev2**
12. **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 certificate-cache** *number-of-certificates* 例： `Device(config)# crypto ikev2 certificate-cache 750`	HTTP URL から取得した証明書を保存するためのキャッシュ サイズを定義します。
ステップ 4	**crypto ikev2 cookie-challenge** *number* 例： `Device(config)# crypto ikev2 cookie-challenge 450`	ハーフオープン セキュリティ アソシエーション（SA）の数が設定された値を超えた場合にだけ、IKEv2 cookie チャレンジを有効にします。 • Cookie チャレンジは、デフォルトで無効化されています。
ステップ 5	**crypto ikev2 diagnose error** *number* 例： `Device(config)# crypto ikev2 diagnose error 500`	IKEv2 エラーの診断を有効にして終了パス データベースのエントリ数を定義します。 • IKEv2エラー診断はデフォルトでは無効化されています。

	コマンドまたはアクション	目的
ステップ 6	**crypto ikev2 dpd** *interval retry-interval* {**on-demand** | **periodic**} 例： `Device(config)# crypto ikev2 dpd 30 6 on-demand`	ピアを次のようにライブでチェックできるようにします。 • Dead Peer Detection（DPD：デッドピア検出）はデフォルトでは無効化されています。 （注） この手順の例では、着信 ESP トラフィックがない場合、最初の DPD が 30 秒後に送信されます。6 秒間（指定された再試行間隔）待機した後、DPD 再試行が 6 秒間隔でアグレッシブに5回送信されます。そのため、合計 66 秒（30 + 6 + 6 X 5 = 66）が経過すると、DPD によって暗号化セッションが切断されます。
ステップ 7	**crypto ikev2 http-url cert** 例： `Device(config)# crypto ikev2 http-url cert`	HTTP CERT サポートを有効にします。 • HTTP CERT は、デフォルトで無効化されています。
ステップ 8	**crypto ikev2 limit** { **max-in-negotiation-sa** *limit* | **max-sa** *limit*} 例：	コネクション アドミッション制御（CAC）を有効にします。 • コネクション アドミッション制御はデフォルトで有効化されています。
ステップ 9	**crypto ikev2 nat keepalive** *interval* 例： `Device(config)# crypto ikev2 nat keepalive 500`	ネットワーク アドレス変換（NAT）のキープアライブを有効にして、インターネットキーエクスチェンジ（IKE）ピア間に NAT がある場合に、任意のトラフィックが欠けることによる NAT の削除を防ぎます。 • NAT キープアライブはデフォルトで無効化されています。
ステップ 10	**crypto ikev2 window** *size* 例： `Device(config)# crypto ikev2 window 15`	送信時に複数の IKEv2 要求と応答のピアを許可します。 • デフォルトのウィンドウ サイズは 5 です。
ステップ 11	**crypto logging ikev2** 例： `Device(config)# crypto logging ikev2`	IKEv2 Syslog メッセージを有効にします。 • デフォルトでは、IKEv2 syslog メッセージは無効化されています。

	コマンドまたはアクション	目的
ステップ 12	**end** 例： `Device(config)# end`	グローバル 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 プロポーザルの設定

デフォルトの IKEv2 プロポーザルについては、「IKEv2 スマート デフォルト」の項を参照してください。

このタスクは、デフォルト プロポーザルを使用しない場合に、デフォルト IKEv2 プロポーザルをオーバーライドするか、手動でプロポーザルを設定するために実行します。

IKEv2 プロポーザルは、IKE_SA_INIT 交換の一部として IKEv2 SA のネゴシエーションに使用されるトランスフォームのセットです。IKEv2 プロポーザルは、少なくとも 1 つの暗号化アルゴリズム、整合性アルゴリズム、および Diffie-Hellman（DH）グループが設定されている場合にのみ、完全であるとみなされます。プロポーザルが設定されておらず、IKEv2 ポリシーにアタッチされていない場合は、デフォルト IKEv2 ポリシー内のデフォルト プロポーザルがネゴシエーションで使用されます。

（注） セキュリティの脅威とそれに対抗するための暗号化技術は常に変化しています。最新のシスコの暗号化に関する推奨事項については、『Next Generation Encryption』（NGE）ホワイト ペーパーを参照してください。

IKEv2 プロポーザルは **crypto isakmp policy** コマンドに似ていますが、IKEv2 プロポーザルには次のような違いがあります。

- IKEv2 プロポーザルを使用すると、各トランスフォーム タイプに対して 1 つ以上のトランスフォームを設定できます。
- IKEv2 プロポーザルには関連付けられた優先順位はありません。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ikev2 proposal** *name*
4. **encryption** *encryption-type...*
5. **integrity** *integrity-type...*
6. **group** *group-type...*
7. **prf** *prf-algorithm*
8. **end**
9. **show crypto ikev2 proposal** [*name* | **default**]

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 proposal** *name* 例： `Device(config)# crypto ikev2 proposal proposal1`	デフォルト IKEv2 プロポーザルをオーバーライドして、IKEv2 プロポーザル名を定義し、IKEv2 プロポーザル 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	**encryption** *encryption-type...* 例： `Device(config-ikev2-proposal)# encryption aes-cbc-128 aes-cbc-192`	1 つまたは複数の暗号化タイプのトランスフォームを指定します。タイプは次のとおりです。 • **3des**（非推奨） • **aes-cbc-128** • **aes-cbc-192** • **aes-cbc-256** • **aes-gcm-128** • **aes-gcm-256**
ステップ 5	**integrity** *integrity-type...* 例： `Device(config-ikev2-proposal)# integrity sha1`	次のように、整合性アルゴリズム タイプの 1 つ以上のトランスフォームを指定します。 • **md5** キーワードは、ハッシュ アルゴリズムとして MD5（HMAC バリアント）を指定します。（非推奨） • **sha1** キーワードは、ハッシュ アルゴリズムとして SHA-1（HMAC バリアント）を指定します。 • **sha256** キーワードは、ハッシュ アルゴリズムとして SHA-2 ファミリ 256 ビット（HMAC バリアント）を指定します。 • **sha384** キーワードは、ハッシュ アルゴリズムとして SHA-2 ファミリ 384 ビット（HMAC バリアント）を指定します。 • **sha512** キーワードは、ハッシュ アルゴリズムとして SHA-2 ファミリ 512 ビット（HMAC バリアント）を指定します。

	コマンドまたはアクション	目的
		（注） 暗号化タイプとして Advanced Encryption Standard（AES）in Galois/Counter Mode（AES GCM）を指定した場合は、整合性アルゴリズム タイプを指定できません。
ステップ 6	**group** *group-type...* 例： `Device(config-ikev2-proposal)# group 14`	Diffie-Hellman（DH）グループ ID を指定します。 • デフォルトの DH グループ識別子は、IKEv2 プロポーザル内のグループ 2 および 5 です。 • **1**：768 ビット DH（非推奨）。 • **2**：1024 ビット DH（非推奨）。 • **5**：1536 ビット DH（非推奨）。 • **14**：2048 ビット DH グループを指定します。 • **15**：3072 ビット DH グループを指定します。 • **16**：4096 ビット DH グループを指定します。 • **19**：256 ビット Elliptic Curve DH（ECDH）グループを指定します。 • **20**：384 ビット ECDH グループを指定します。 • **24**：2048 ビット DH グループを指定します。 選択するグループは、ネゴシエーション中の IPsec キーを保護するため、十分強力（十分なビット数がある）である必要があります。一般に受け入れられているガイドラインでは、2013 年以降（2030 年まで）は 2048 ビット グループの使用が推奨されています。このガイドラインを満たすために、グループ 14 とグループ 24 のどちらかを選択できます。より寿命の長いセキュリティ方式が必要な場合でも、楕円曲線暗号の使用をお勧めしますが、グループ 15 とグループ 16 も検討してください。
ステップ 7	**prf** *prf-algorithm* 例： `Device(config-ikev2-proposal)# prf sha256 sha512`	次のように、1 つ以上の擬似ランダム関数（PRF）アルゴリズムを指定します。 • **md5** • **sha1** • **sha256** • **sha384** • **sha512**

	コマンドまたはアクション	目的
		（注） この手順は、暗号化タイプが AES-GCM：**aes-gmc-128** または **aes-gmc-256** の場合に必須です。暗号化アルゴリズムが AES-GCM でない場合は、PRF アルゴリズムが指定された整合性アルゴリズムと同じになります。ただし、必要に応じて、PRF アルゴリズムを指定できます。
ステップ 8	**end** 例： `Device(config-ikev2-proposal)# end`	IKEv2 プロポーザル 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。
ステップ 9	**show crypto ikev2 proposal** [*name* | **default**] 例： `Device# show crypto ikev2 proposal default`	（任意）IKEv2 プロポーザルを表示します。

次の作業

IKEv2 プロポーザルを作成した後、ポリシーと接続して、ネゴシエーションでプロポーザルを選択できるようにします。このタスクの完了について、詳細は「IKEv2 ポリシーの設定」セクションを参照してください。

IKEv2 ポリシーの設定

デフォルトの IKEv2 ポリシーについては、「IKEv2 スマート デフォルト」の項を参照してください。

このタスクは、デフォルト ポリシーを使用しない場合に、デフォルト IKEv2 ポリシーをオーバーライドするか、手動でポリシーを設定するために実行します。

IKEv2 ポリシーには、完全だと考えられる 1 つ以上のプロポーザルを含める必要があり、ネゴシエーション用のポリシーを選択するための選択基準として使用される match ステートメントを含めることができます。初期交換中に、ネゴシエートする SA のローカル アドレス（IPv4 または IPv6）と Front Door VRF（FVRF）がポリシーと照合され、プロポーザルが選択されます。

次のルールが match ステートメントに適用されます。

- match ステートメントを含まない IKEv2 ポリシーは、グローバル FVRF 内のすべてのピアと一致します。
- IKEv2 ポリシーには、match FVRF ステートメントを 1 つしか含めることができません。
- IKEv2 ポリシーには、match address local ステートメントを 1 つ以上含めることができます。
- ポリシーを選択すると、同じタイプの複数の match ステートメントが論理的に OR され、違うタイプの match ステートメントが論理的に AND されます。

- タイプが異なる match ステートメントの優先順位はありません。
- 重複したポリシーの設定は、設定ミスと見なされます。複数のポリシーが一致した場合は、最初のポリシーが選択されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ikev2 policy** *name*
4. **proposal** *name*
5. **match fvrf** {*fvrf-name* | **any**}
6. **match address local** {*ipv4-address* | *ipv6-address*}
7. **end**
8. **show crypto ikev2 policy** [*policy-name* | **default**]

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 policy** *name* 例： `Device(config)# crypto ikev2 policy policy1`	デフォルト IKEv2 ポリシーをオーバーライドして、IKEv2 ポリシー名を定義し、IKEv2 ポリシー 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	**proposal** *name* 例： `Device(config-ikev2-policy)# proposal proposal1`	このポリシーで使用する必要があるプロポーザルを指定します。 • プロポーザルは、一覧の順の優先順位になります。 （注） 少なくとも 1 つのプロポーザルを指定する必要があります。各プロポーザルを別々のステートメントに分けた追加のプロポーザルを指定できます。
ステップ 5	**match fvrf** {*fvrf-name*	**any**} 例： `Device(config-ikev2-policy)# match fvrf any`	（任意）ポリシーをユーザが設定した FVRF または任意の FVRF に基づいて照合します。 • デフォルトはグローバル FVRF です。

	コマンドまたはアクション	目的
		（注） 任意の VRF と一致させるには、**match fvrf any** コマンドを明示的に設定する必要があります。FVRF には、IKEv2 パケットのネゴシエーションを行う VRF を指定します。
ステップ 6	**match address local** {*ipv4-address* | *ipv6-address*} 例： `Device(config-ikev2-policy)# match address local 10.0.0.1`	（任意）ローカル IPv4 または IPv6 アドレスに基づいてポリシーを照合します。 • デフォルトは、設定済みの FVRF 内のすべてのアドレスと一致します。
ステップ 7	**end** 例： `Device(config-ikev2-policy)# end`	IKEv2 ポリシー 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。
ステップ 8	**show crypto ikev2 policy** [*policy-name* | **default**] 例： `Device# show crypto ikev2 policy policy1`	（任意）IKEv2 ポリシーを表示します。

インターネット キー エクスチェンジ バージョン 2 の設定例

基本のインターネット キー エクスチェンジ バージョン 2 CLI 構造の設定例

例：IKEv2 キー リングの設定

例：複数のピア サーバブロックを持つ IKEv2 キー リング

次の例は、複数のピア サブブロックを持つインターネット キー エクスチェンジ バージョン 2（IKEv2）キー リングを設定する方法を示します。

```
crypto ikev2 keyring keyring-1
 peer peer1
  description peer1
  address 209.165.200.225 255.255.255.224
  pre-shared-key key-1
 peer peer2
  description peer2
  hostname peer1.example.com
  pre-shared-key key-2
 peer peer3
```

```
 description peer3
 hostname peer3.example.com
 identity key-id abc
 address 209.165.200.228 255.255.255.224
 pre-shared-key key-3
```

例：IP アドレスに基づく対称型事前共有キーを使用した IKEv2 キー リング

次の例は、IP アドレスに基づく対称型事前共有キーを使用する IKEv2 キー リングの設定方法を示します。次は、発信側のキー リングです。

```
crypto ikev2 keyring keyring-1
 peer peer1
  description peer1
  address 209.165.200.225 255.255.255.224
  pre-shared-key key1
```

次は、応答側のキー リングです。

```
crypto ikev2 keyring keyring-1
 peer peer2
  description peer2
  address 209.165.200.228 255.255.255.224
  pre-shared-key key1
```

例：IP アドレスに基づく非対称型事前共有キーを使用した IKEv2 キー リング

次の例は、IP アドレスに基づく非対称型事前共有キーを使用する IKEv2 キー リングの設定方法を示します。次は、発信側のキー リングです。

```
crypto ikev2 keyring keyring-1
 peer peer1
  description peer1 with asymmetric keys
  address 209.165.200.225 255.255.255.224
  pre-shared-key local key1
  pre-shared-key remote key2
```

次は、応答側のキー リングです。

```
crypto ikev2 keyring keyring-1
 peer peer2
  description peer2 with asymmetric keys
  address 209.165.200.228 255.255.255.224
  pre-shared-key local key2
  pre-shared-key remote key1
```

例：ホスト名に基づく非対称型事前共有キーを使用した IKEv2 キー リング

次の例は、ホスト名に基づく非対称型事前共有キーを使用する IKEv2 キー リングの設定方法を示します。次は、発信側のキー リングです。

```
crypto ikev2 keyring keyring-1
 peer host1
  description host1 in example domain
  hostname host1.example.com
  pre-shared-key local key1
  pre-shared-key remote key2
```

次は、応答側のキー リングです。

```
crypto ikev2 keyring keyring-1
 peer host2
  description host2 in abc domain
  hostname host2.example.com
  pre-shared-key local key2
  pre-shared-key remote key1
```

例：アイデンティティに基づく対称型事前共有キーを使用した IKEv2 キー リング

次の例は、アイデンティティに基づく対称型事前共有キーを使用する IKEv2 キー リングの設定方法を示します。

```
crypto ikev2 keyring keyring-4
 peer abc
  description example domain
  identity fqdn example.com
  pre-shared-key abc-key-1
 peer user1
  description user1 in example domain
  identity email user1@example.com
  pre-shared-key abc-key-2
 peer user1-remote
  description user1 example remote users
  identity key-id example
  pre-shared-key example-key-3
```

例：ワイルドカード キーを使用した IKEv2 キー リング

次の例は、ワイルドカード キーを使用する IKEv2 キー リングの設定方法を示します。

```
crypto ikev2 keyring keyring-1
 peer cisco
  description example domain
  address 0.0.0.0 0.0.0.0
  pre-shared-key example-key
```

例：キー リングの照合

次の例は、キー リングの照合方法を示します。

```
crypto ikev2 keyring keyring-1
 peer cisco
  description example.com
  address 0.0.0.0 0.0.0.0
  pre-shared-key xyz-key
 peer peer1
  description abc.example.com
  address 10.0.0.0 255.255.0.0
  pre-shared-key abc-key
 peer host1
  description host1@abc.example.com
  address 10.0.0.1
  pre-shared-key host1-example-key
```

ここに示す例では、ピア 10.0.0.1 を照合するキーは最初にワイルドカード キー example-key と一致し、次にプレフィックス キー example-key と一致し、最後にホスト キー host1-example-key と一致します。最適な一致である host1-example-key が使用されます。

```
crypto ikev2 keyring keyring-2
 peer host1
 description host1 in abc.example.com sub-domain
 address 10.0.0.1
 pre-shared-key host1-example-key
 peer host2
  description example domain
  address 0.0.0.0 0.0.0.0
  pre-shared-key example-key
```

ここに示す例では、ピア 10.0.0.1 を照合するキーは最初にホスト キー host1-abc-key と一致します。これが固有の一致であることから、これ以上の照合は実行されません。

例：プロファイルの設定

例：リモート ID で照合する IKEv2 プロファイル

次のプロファイルは、完全修飾ドメイン名（FQDN）example.com を使用して自身を特定し、トラストポイントリモートを使用して RSA 署名で認証するピアをサポートします。ローカルノードは、keyring-1 を使用する事前共有キーでノード自体を認証します。

```
crypto ikev2 profile profile2
 match identity remote fqdn example.com
 identity local email router2@example.com
 authentication local pre-share
 authentication remote rsa-sig
 keyring keyring-1
 pki trustpoint trustpoint-remote verify
 lifetime 300
 dpd 10 5 on-demand
 virtual-template 1
```

例：2 つのピアをサポートする IKEv2 プロファイル

次の例は、異なる認証方式を使用する 2 つのピアがサポートする、IKEv2 プロファイルの設定方法を示します。

```
crypto ikev2 profile profile2
 match identity remote email user1@example.com
 match identity remote email user2@example.com
 identity local email router2@cisco.com
 authentication local rsa-sig
 authentication remote pre-share
 authentication remote rsa-sig
 keyring keyring-1
 pki trustpoint trustpoint-local sign
 pki trustpoint trustpoint-remote verify
 lifetime 300
 dpd 10 5 on-demand
 virtual-template 1
```

例：証明書および IKEv2 スマート デフォルトを使用するダイナミック ルーティングによる FlexVPN の設定

次の例に、トンネルを介したダイナミック ルーティングによるブランチデバイス（発信者側、スタティック仮想トンネルインターフェイス（sVTI）を使用）と中央デバイス（応答側、ダイナミック仮想トンネルインターフェイス（dVTI）を使用）との間の接続を示します。この例ではIKEv2スマートデフォルトを使用し、認証は証明書（RSA署名）を使用して実行されます。

（注） 推奨される RSA モジュラス サイズは 2048 です。

ピアは IKEv2 ID として FQDN を使用し、応答側の IKEv2 プロファイルは ID FQDN のドメインと一致します。

発信側（ブランチ デバイス）での設定は、次のとおりです。

```
hostname branch
ip domain name cisco.com
!
crypto ikev2 profile branch-to-central
 match identity remote fqdn central.cisco.com
 identity local fqdn branch.cisco.com
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint CA
!
crypto ipsec profile svti
 set ikev2-profile branch-to-central
!
interface Tunnel0
 ip address 172.16.0.101 255.255.255.0
 tunnel source Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel destination 10.0.0.100
 tunnel protection ipsec profile svti
!
interface Ethernet0/0
 ip address 10.0.0.101 255.255.255.0
!
interface Ethernet1/0
 ip address 192.168.101.1 255.255.255.0
!
router rip
 version 2
 passive-interface Ethernet1/0
 network 172.16.0.0
 network 192.168.101.0
 no auto-summary
```

応答側（中央ルータ）での設定は、次のとおりです。

```
hostname central
ip domain name cisco.com
!
crypto ikev2 profile central-to-branch
 match identity remote fqdn domain cisco.com
 identity local fqdn central.cisco.com
```

```
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint CA
 virtual-template 1
!
interface Loopback0
 ip address 172.16.0.100 255.255.255.0
!
interface Ethernet0/0
 ip address 10.0.0.100 255.255.255.0
!
interface Ethernet1/0
 ip address 192.168.100.1 255.255.255.0
!
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback0
 tunnel source Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile default
!
router rip
 version 2
 passive-interface Ethernet1/0
 network 172.16.0.0
 network 192.168.100.0
 no auto-summary
```

高度なインターネット キー エクスチェンジ バージョン 2 CLI 構造の設定例

例：プロポーザルの設定

例：各トランスフォーム タイプに対して 1 つのトランスフォームがある IKEv2 プロポーザル

次の例は、各トランスフォーム タイプに対して 1 つのトランスフォームがある IKEv2 プロポーザルの設定方法を示します。

```
crypto ikev2 proposal proposal-1
 encryption aes-cbc-128
 integrity sha1
 group 14
```

例：各トランスフォーム タイプに対して複数のトランスフォームがある IKEv2 プロポーザル

次の例は、各トランスフォーム タイプに対して複数のトランスフォームがある IKEv2 プロポーザルの設定方法を示します。

```
crypto ikev2 proposal proposal-2
 encryption aes-cbc-128 aes-cbc-192
 integrity sha1
 group 14
```

（注） シスコは現在、3DES、MD5（HMAC バリアント含む）、および Diffie-Hellman（DH）グループ 1、2、および 5 の使用は推奨していません。代わりに、AES、SHA-256、および DH グループ 14 以降を使用する必要があります。シスコの暗号化に関する最新の推奨事項の詳細は、『Next Generation Encryption』（NGE）ホワイト ペーパーを参照してください。

ここに示す IKEv2 プロポーザル proposal-2 では、次の組み合わせのトランスフォームの優先順位リストに変換されます。

- aes-cbc-128, sha1, 14
- aes-cbc-192, sha1, 14

例：発信側と応答側の IKEv2 プロポーザル

次の例は、発信側と応答側の IKEv2 プロポーザルの設定方法を示します。発信側のプロポーザルは次のとおりです。

```
crypto ikev2 proposal proposal-1
 encryption aes-cbc-192 aes-cbc-128
 integrity sha-256 sha1
 group 14 24
```

応答側のプロポーザルは次のとおりです。

```
crypto ikev2 proposal proposal-2
 encryption aes-cbc-128 aes-cbc-192
 peer
 integrity sha1 sha-256
 group 24 14
```

選択したプロポーザルは次のようになります。

```
encryption aes-cbc-128
integrity sha1
group 14
```

発信側と応答側に示されるプロポーザルでは、発信側と応答側では設定が競合します。この場合、発信側が応答側よりも優先されます。

例：ポリシーの設定

例：VRF およびローカル アドレスで照合する IKEv2 ポリシー

次の例は、IKEv2 ポリシーが VRF およびローカル アドレスで照合する方法を示します。

```
crypto ikev2 policy policy2
 match vrf vrf1
 match local address 10.0.0.1
 proposal proposal-1
```

例：グローバル VRF 内のすべてのピアを照合する複数のプロポーザルがある IKEv2 ポリシー

次の例は、複数のプロポーザルがある IKEv2 ポリシーがグローバル VRF 内のピアを照合する方法を示します。

```
crypto ikev2 policy policy2
 proposal proposal-A
 proposal proposal-B
 proposal proposal-B
```

例：任意の VRF 内のすべてのピアを照合する IKEv2 ポリシー

次の例は、任意の VRF 内のピアを照合する IKEv2 ポリシーの方法を示します。

```
crypto ikev2 policy policy2
 match vrf any
 proposal proposal-1
```

例：ポリシーの照合

重複するポリシーは設定しないでください。一致する複数の可能性がポリシーにある場合、次の例に示すように、最適な照合が使用されます。

```
crypto ikev2 policy policy1
 match fvrf fvrf1
crypto ikev2 policy policy2
 match fvrf fvff1
 match local address 10.0.0.1
```

vrf1 という FVRF のプロポーザルと 10.0.0.1 というローカル ピアは policy2 および policy2 と一致しますが、policy1 が最適な一致であるためにこちらが選択されます。

次の作業

IKEv2 の設定後、IPsec VPN の設定に進みます。詳細については、『Configuring Security for VPNs with IPsec』モジュールを参照してください。

インターネット キー エクスチェンジ バージョン 2（IKEv2）のその他の関連資料

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』、すべてのリリース

関連項目	マニュアル タイトル
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』
IPsec の設定	『Configuring Security for VPNs with IPsec』
Suite-B の ESP トランスフォーム	『Configuring Security for VPNs with IPsec』
Suite-B SHA-2 ファミリ（HMAC バリアント）および Elliptic Curve（EC）キーペアの設定	『Configuring Internet Key Exchange for IPsec VPNs』
IPsec SA ネゴシエーションでの Suite-B の Elliptic Curve Diffie-Hellman（ECDH）のサポート	『Configuring Internet Key Exchange for IPsec VPNs』
PKI の証明書登録のための Suite-B サポート	『Configuring Certificate Enrollment for a PKI』
IKE での使用にサポートされている標準	『Internet Key Exchange for IPsec VPNs Configuration Guide』
推奨される暗号化アルゴリズム	『Next Generation Encryption』

RFC

RFC	タイトル
RFC 4306	*Internet Key Exchange (IKEv2) Protocol*
RFC 4869	*Suite B Cryptographic Suites for IPsec*
RFC 5685	*Redirect Mechanism for the Internet Key Exchange Protocol Version 2 (IKEv2)*

シスコのテクニカル サポート

説明	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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

インターネット キー エクスチェンジ バージョン 2（IKEv2）の設定に関する機能情報

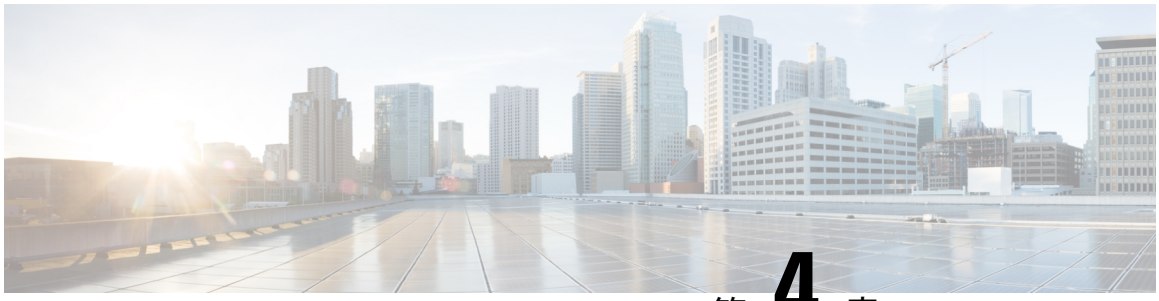
次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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 *2*：インターネット キー エクスチェンジ バージョン *2*（*IKEv2*）の設定に関する機能情報

機能名	リリース	機能情報
IPsec と IKEv2 に対する IPv6 のサポート		この機能によって、IPv6 アドレスを IPsec および IKEv2 プロトコルに追加できます。 次のコマンドが導入または変更されました。 **address (IKEv2 keyring), identity (IKEv2 keyring), identity local, match (IKEv2 policy), match (IKEv2 profile), show crypto ikev2 session, show crypto ikev2 sa, show crypto ikev2 profile, show crypto ikev2 policy, debug crypto condition, clear crypto ikev2 sa.**

機能名	リリース	機能情報
IOS ソフトウェア暗号での Suite-B のサポート		パケットデータの認証およびIKEv2プロポーザル設定の整合性確認メカニズムの検証に使用される SHA-2 ファミリ（HMAC バリアント）のハッシュアルゴリズムに、Suite-B のサポートが追加されました。HMACは、追加レベルのハッシュを提供するバリアントです。 Suite-B によって、RFC 4754 で定義されているように楕円曲線デジタル署名アルゴリズム（ECDSA）署名（ECDSA-sig）を IKEv2 の認証方式にすることもできます。 Suite-B の要件は、暗号化アルゴリズムの 4 つのユーザ インターフェイス スイートです。アルゴリズムは、RFC 4869 で説明されている IKE および IPSec で使用します。各スイートは、暗号化アルゴリズム、デジタル署名アルゴリズム、キー合意アルゴリズム、およびハッシュまたはメッセージダイジェストアルゴリズムで構成されています。Cisco IOS 上における Suite-B サポートの詳細については、『Configuring Security for VPNs with IPsec』モジュールを参照してください。 次のコマンドが導入または変更されました。 **authentication, group, identity (IKEv2 profile), integrity, match (IKEv2 profile).**
IOS 上における IKEv2 暗号としての AES-GCM のサポート		IKEv2 機能の AES-GCM サポートでは、Galois/カウンタ モードの Advanced Encryption Standard（AES-GCM）の使用方法を説明します。インターネット キー エクスチェンジ バージョン 2（IKEv2）プロトコルの暗号化ペイロードと共に認証済みの暗号化アルゴリズムを使用することについても説明します。 次のコマンドが導入または変更されました。 **encryption (IKEv2 proposal), prf, show crypto ikev2 proposal.**
トンネルモード自動選択		トンネルモード自動選択機能は、設定を容易にし、レスポンダの詳細の入手を支援します。この機能は、IKE プロファイルから仮想アクセスインターフェイスが作成されるとすぐに、トンネリング プロトコル（GRE または IPsec）とトランスポート プロトコル（IPv4 または IPv6）を自動的に仮想テンプレートに適用します。 次のコマンドが導入または変更されました。 **virtual-template (IKEv2 profile), show crypto ikev2 profile.**



第 4 章

FlexVPN サーバの設定

このモジュールでは、FlexVPN サーバの機能、FlexVPN サーバの設定に必要な IKEv2 コマンド、リモート アクセス クライアント、およびサポートされる RADIUS 属性について説明します。

（注） セキュリティに対する脅威は、そのような脅威からの保護に役立つ暗号化技術と同様に、絶え間なく変化しています。最新のシスコの暗号化の推奨事項の詳細については、『Next Generation Encryption』（NGE）のホワイト ペーパーを参照してください。

- 機能情報の確認 （41 ページ）
- FlexVPN サーバの制限事項 （42 ページ）
- FlexVPN サーバに関する情報 （43 ページ）
- FlexVPN サーバの設定方法 （55 ページ）
- FlexVPN サーバの構成例 （68 ページ）
- FlexVPN サーバの設定に関する追加情報 （73 ページ）
- FlexVPN サーバの設定の機能情報 （74 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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。

FlexVPN サーバの制限事項

デュアルスタック トンネル インターフェイスおよび VRF 認識 IPsec

VPN ルーティングおよび転送（VRF）認識 IPsec シナリオでデュアルスタック トンネル インターフェイスを設定する場合、**ip vrf forwarding** コマンドを使用して内部 VPN ルーティングおよび転送（IVRF）インスタンスを設定することはできません。これは有効な設定ではないためです。トンネル インターフェイスの IVRF を定義するには **vrf forwarding** *vrf-name* コマンドを使用します。ここで、*vrf-name* 引数は、定義内に IPv4 および IPv6 アドレス ファミリを指定した **vrf definition** コマンドを使用して定義されます。

SSO の制約事項

- Cisco ASR 1000 シリーズ ルータは、Embedded Services Processor（ESP）スイッチオーバーでステートフル IPSec セッションをサポートします。ESP スイッチオーバー中は、すべての IPSec セッションがアップ状態のままになるので、IPSec セッションを維持するためにユーザの操作は必要ありません。
- ESP をリロードした場合（スタンバイ ESP なし）、SA シーケンス番号は 0 から再開されます。ピアルータは、予期されたシーケンス番号を持たないパケットをドロップします。単一の ESP を使用するシステムで ESP のリロード後にこの問題を回避するには、IPSec セッションを明示的に再確立することが必要になる場合があります。このような場合、リロード中に IPSec セッションでトラフィックの中断が発生することがあります。
- Cisco ASR 1000 シリーズ ルータは、現在、ルート プロセッサ（RP）でのステートフル スイッチオーバー（SSO）の IPSec セッションをサポートしていません。IPSec セッションはスイッチオーバーの開始時にダウンしますが、新しい RP がアクティブになるとアップ状態に戻ります。ユーザの操作は必要ありません。セッションがアップ状態に戻るまでの間、スイッチオーバー中に IPSec セッションでトラフィックの中断が発生することがあります。
- Cisco ASR 1000 シリーズ ルータは、IPSec セッションのステートフル ISSU をサポートしていません。ISSU を実行する前に、既存のすべての IPSec セッションまたはトンネルを明示的に終了し、ISSU の実行後に再確立する必要があります。具体的には、ISSU を実行する前に、ハーフオープンまたは確立途中の IPSec トンネルが存在しないことを確認します。これを行うには、トンネル セットアップを開始する可能性のあるインターフェイス（トンネル セットアップを開始するルーティング プロトコルなど）、キープアライブが有効になっているインターフェイス、または IPSec セッションの自動トリガーが存在するインターフェイスの場合は、インターフェイスをシャットダウンすることをお勧めします。この場合、ISSU の実行中に IPSec セッションでトラフィックの中断が発生します。

AnyConnect プロファイルのダウンロードの制約事項

- FlexVPN AnyConnect プロファイルのダウンロード機能は、Cisco IOS XE デバイスをヘッドエンドおよび Cisco AnyConnect セキュア モビリティ クライアントとしてサポートします。
- Cisco AnyConnectプロファイル情報は、ブートフラッシュにのみ保存できます。TFTP ブートサーバなどのリモートロケーションからプロファイルをロードすることはできません。
- この機能は、リモート認証方式として AnyConnect EAP オプションを使用している場合に限り有効です。

FlexVPN サーバに関する情報

EAP を使用するピア認証

FlexVPN サーバは、Extensible Authentication Protocol（EAP：拡張可能認証プロトコル）を使用するピア認証をサポートし、クライアントとバックエンド EAP サーバ間で EAP メッセージを中継するパススルー オーセンティケータとして動作します。EAP バックエンド サーバは、通常、EAP 認証をサポートする RADIUS サーバです。

（注） FlexVPN クライアントはEAPを使用するFlexVPNクライアントを認証しますが、FlexVPNサーバは証明書を使用して認証を受ける必要があります。

FlexVPN サーバは、IKEv2 プロファイル設定モードの **authentication remote eap** コマンドによって、EAP を使用する FlexVPN クライアントを認証するよう設定されています。FlexVPN クライアントは、IKE_AUTH 要求内の AUTH ペイロードをスキップすることで、EAP を使用して認証します。

query-identity キーワードが設定されている場合、FlexVPN サーバはクライアントからの EAP ID をクエリします。それ以外は、FlexVPN クライアントの IKEv2 ID が EAP ID として使用されます。ただし、**query-identity** キーワードが設定されておらず、FlexVPN クライアントの IKEv2 ID が IPv4 または IPv6 アドレスの場合、IP アドレスを EAP ID として使用できないため、セッションは終了します。

FlexVPN サーバは、FlexVPN クライアントの EAP ID を EAP サーバに渡すことで、EAP 認証を開始します。その後、FlexVPN サーバは、認証が完了するまで、リモート アクセス（RA）クライアントと EAP サーバ間の EAP メッセージを中継します。認証が成功すると、EAP サーバでは、EAP 成功メッセージ内で認証された EAP の ID が FlexVPN サーバに返されることが予想されます。

EAP認証の後、IKEv2設定に使用されたEAP IDは、次の送信元から任意の順で取得されます。

- EAP 成功メッセージで EAP サーバから提供される EAP ID。

- **query-identity** キーワードの設定時にクライアントからクエリされる EAP ID。
- EAP ID として使用される FlexVPN クライアントの IKEv2 ID。

次の図は、**query-identity** キーワードなしの EAP 認証に対する IKEv2 交換を示します。

図 *1 : query-identity* キーワードなしの *IKEv2* 交換

IKEv2 RA client	IKEv2 RA server	RADIUS-EAP server
HDR, SAi1, KEi, Ni →		
	← HDR, SAr1, KEr, Nr, [CERTREQ]	
HDR, SK {IDi, [CERTREQ,] [IDr,] SAi2, TSi, TSr} →		
	RADIUS Access-Request/ EAP-Message/EAP-Response/(EAP-ID(IKEv2-ID)) →	
		← RADIUS Access-Challenge/EAP-Message/ EAP-Request/(EAP-method)
	← HDR, SK {IDr, [CERT,] AUTH, EAP(EAP-Request(EAP-method))}	
HDR, SK {EAP(EAP-Response(EAP-method)} →		
	RADIUS Access-Request/EAP-Message/EAP-Response/EAP-method) →	
		← RADIUS Access-Accept/EAP-Message/EAP-Success (other attributes))
	← HDR, SK {EAP (success)}	
HDR, SK {AUTH} →		
	← HDR, SK {AUTH, SAr2, TSi, TSr }	

209140

次の図は、**query-identity** キーワードありの EAP 認証に対する IKEv2 交換を示します。

図 *2 : query-identity* キーワードありの *IKEv2* 交換

IKEv2 RA client	IKEv2 RA server	RADIUS-EAP server
HDR, SAi1, KEi, Ni →		
	← HDR, SAr1, KEr, Nr, [CERTREQ]	
HDR, SK {IDi, [CERTREQ,] [IDr,] SAi2, TSi, TSr} →		
	← HDR, SK {IDr, [CERT,] AUTH, EAP (EAP-request (Identity)) }	
HDR, SK {EAP(EAP-Response(Identity)} →		
	RADIUS Access-Request/ EAP-Message/EAP-Response/(EAP-ID) →	
		← RADIUS Access-Challenge/EAP-Message/ EAP-Request/(EAP-method)
	← HDR, SK {IDr, [CERT,] AUTH, EAP(EAP-Request(EAP-method))}	
HDR, SK {EAP(EAP-Response(EAP-method)} →		
	RADIUS Access-Request/EAP-Message/EAP-Response/EAP-method) →	
		← RADIUS Access-Accept/EAP-Message/EAP-Success (EAP-identity) (other attributes))
	← HDR, SK {EAP (success)}	
HDR, SK {AUTH} →		
	← HDR, SK {AUTH, SAr2, TSi, TSr }	

209141

IKEv2 コンフィギュレーション モード

IKEv2 コンフィギュレーション モードで、IKE ピアは IP アドレスやルートなどの設定情報を交換できます。設定情報は、IKEv2 認証から取得されます。プル モデルとプッシュ モデルの両方がサポートされます。プル モデルには、設定要求と応答の交換が含まれます。プッシュ モデルには、設定セットと確認応答の交換が含まれます。

次の表に、発信側と応答側が異なる設定ペイロードタイプを送信するときの状況を示します。

表 *3:* 設定ペイロード タイプ

設定ペイロード タイプ	送信元...	属性...
CFG_REQUEST	発信側	発信側が FlexVPN クライアントの場合。または、**config-exchange request** コマンドが IKEv2 プロファイルで有効になっている場合。
CFG_REPLY	応答側	応答側が CFG_REQUEST を受信する場合。
CFG_SET	発信側と応答側	発信側：**config-exchange set send** コマンドが IKEv2 プロファイルで有効になっている場合。 応答側：CFG_REQUEST が受信されておらず、設定データを使用可能で、**config-exchange set send** コマンドが IKEv2 プロファイルで有効になっている場合。
CFG_ACK	発信側と応答側	発信側：**config-exchange set accept** コマンドが IKEv2 プロファイルで有効になっている場合。 応答側：**config-exchange set accept** コマンドが IKEv2 プロファイルで有効になっている場合。

（注） 設定要求と設定セットペイロードを送信するためのコマンドは、デフォルトで有効になっています。

ご使用のリリースに応じて、発信側が FlexVPN クライアントの場合に IKEv2 発信側がコンフィギュレーション モードをトリガーしたり、IKEv2 プロファイルで **config-mode** コマンドを有効にすることによって IKEv2 を発信するスタティック トンネル インターフェイスがコンフィギュレーション モードをトリガーすることができます。

IKEv2 FlexVPN サーバは、次の標準 IPv4 設定属性をサポートします。

- INTERNAL_IP4_ADDRESS
- INTERNAL_IP4_NETMASK
- INTERNAL_IP4_DNS
- INTERNAL_IP4_NBNS
- INTERNAL_IP4_SUBNET

IKEv2 FlexVPN サーバは、次の標準 IPv6 設定属性をサポートします。

- INTERNAL_IP6_ADDRESS
- INTERNAL_IP6_DNS
- INTERNAL_IP6_SUBNET

（注） IPv6 設定属性は、Microsoft Windows IKEv2 クライアントによってのみサポートされます。

IKEv2 認証ポリシーで **route set** コマンドと **aaa attribute list** コマンドによって制御されている INTERNAL_IP4_SUBNET および INTERNAL_IP6_SUBNET 設定属性は、SVTI（スタティック仮想トンネルインターフェイス）-to-SVTI トンネルを設定する場合はサポートされません。このような場合、IKEv2 ベースのルート交換の代わりにスタティック ルーティングまたはダイナミック ルーティングを使用する必要があります。

IKEv2 FlexVPN サーバは、次の標準共通設定属性をサポートします。

- APPLICATION_VERSION

（注） この属性は、Cisco AnyConnect および FlexVPN クライアントにのみ送信されます。

IKEv2 FlexVPN サーバは、次の Cisco Unity 設定属性をサポートします。

- MODECFG_BANNER
- MODECFG_DEFDOMAIN
- MODECFG_SPLITDNS_NAME
- MODECFG_BACKUPSERVERS
- MODECFG_PFS
- MODECFG_SMARTCARD_REMOVAL_DISCONNECT

（注） Cisco Unity 属性は、Cisco AnyConnect および FlexVPN クライアントにのみ送信されます。

IKEv2 FlexVPN サーバは、次の Cisco FlexVPN 設定属性をサポートします。

- MODECFG_CONFIG_URL
- MODECFG_CONFIG_VERSION

（注） Cisco FlexVPN 属性は、Cisco FlexVPN クライアントにのみ送信されます。

INTERNAL_IP4_ADDRESS 属性値は、指定された順序で次の送信元から取得されます。

- AAA ユーザ認証で受信した Framed-IP-Address 属性。
- ローカル IP アドレス プール。
- DHCP サーバ。

DHCP サーバ（設定されている場合）は、ローカル IP アドレス プールが設定されていない場合にのみアドレスを割り当てます。ただし、ローカル プールから IP アドレスを割り当てるとエラーが発生する場合、その次のアドレス送信元の DHCP サーバはアドレスの割り当てに使用されません。

INTERNAL_IP4_NETMASK 属性の値は、次から取得されます。

- IP アドレスが DHCP サーバから取得される場合、ネットマスクも DHCP サーバから取得されます。
- IP アドレスが AAA ユーザ認証の Framed-IP-Address 属性またはローカル IP アドレス プールのいずれかから取得される場合、ネットマスクはユーザ認証またはグループ認証で受信した IPv4 ネットマスク属性から取得されます。ネットマスクが使用できない場合、INTERNAL_IP4_NETMASK 属性は設定応答に含まれません。ネットマスクが使用可能な場合、INTERNAL_IP4_ADDRESS 属性が設定応答に含まれるときにのみ、INTERNAL_IP4_NETMASK 属性は含まれます。

IPv4アドレスは、クライアントがアドレスを要求する場合にのみ割り当てられ、応答に含まれます。クライアントが複数の IPv4 アドレスを要求した場合、応答で送信される IPv4 アドレスは1つのみです。可能な場合は、クライアントが要求しなくても残りの属性が応答に含まれます。クライアントが IPv4 アドレスを要求して、FlexVPN サーバがアドレスを割り当てることができない場合、INTERNAL_ADDRESS_FAILURE メッセージがクライアントに返されます。

ipv6 local pool 設定では常に、プレフィックス長に 128 を使用することをお勧めします。

たとえば、クライアント数が4の場合は、プレフィックス長として **ipv6 local pool pool1 afe0::/126 128** を設定する必要があります。クライアント数が16の場合は、プレフィックス長として **ipv6 local pool pool1 afe0::/124 128** を設定する必要があります。

IKEv2 認証

IKEv2 認証は、AAA を使用して認証されるセッションに対するポリシーを提供します。このポリシーは、ローカルに定義するかRADIUSサーバで定義できます。また、このポリシーにはローカルおよび/またはリモート属性が含まれています。認証用のユーザ名は、**name-mangler** キーワードを使用してピア ID から取得するか、コマンドで直接指定することができます。IKEv2 認証は、ピアがコンフィギュレーション モードを介して IP アドレスを要求する場合にのみ必要です。

IKEv2 認証タイプは、次のとおりです。

- ユーザ認証：ユーザ認証を有効にするには、IKEv2 プロファイルで **aaa authorization user** コマンドを使用します。ユーザ認証は、fqdn-hostname などのピア IKE ID のユーザ固有の部分に基づいています。ユーザ認証の属性は、ユーザ属性と呼ばれます。
- グループ認証：グループ認証を有効にするには、IKEv2 プロファイルで **aaa authorization group** コマンドを使用します。グループ認証は、fqdn-domain などのピア IKE ID の汎用部分に基づいています。グループ認証の属性は、グループ属性と呼ばれます。
- 暗黙的ユーザ認証：暗黙的ユーザ認証を有効にするには、IKEv2 プロファイルで **aaa authorization user cached** コマンドを使用します。暗黙的認証は、EAP 認証の一部として実行されるか、AAA 事前共有キーの取得時に実行されます。暗黙的ユーザ認証の属性は、キャッシュ属性と呼ばれます。

（注） ご使用のリリースに応じて、**aaa authorization user cached** コマンドが使用可能または使用不可能な場合があります。明示的ユーザ認証は、暗黙的ユーザ認証が属性を返さない場合または Framed-IP-Address 属性を持たない場合にのみ実行されます。

属性のマージおよびオーバーライド

異なる送信元からの属性は、使用前にマージされます。マージ属性の優先順位は、次のとおりです。

- 重複する属性をマージする場合、属性の送信元の優先順位が高くなります。
- ユーザ属性およびキャッシュ属性をマージする場合、ユーザ属性の優先順位が高くなります。
- マージ済みのユーザ属性およびグループ属性をマージする場合、デフォルトではマージ済みのユーザ属性の優先順位が高くなります。ただし、この優先順位は **aaa author group override** コマンドを使用して逆にすることができます。

IKEv2 認証ポリシー

IKEv2 認証ポリシーでは、ローカル認証ポリシーが定義され、ローカルおよび/またはリモート属性が含まれています。VPN ルーティングおよび転送（VRF）や QOS ポリシーなどのローカル属性は、ローカルに適用されます。ルートなどのリモート属性は、コンフィギュレーションモードでピアにプッシュされます。ローカルポリシーを定義するには、**crypto ikev2 authorization policy** コマンドを使用します。IKEv2 認証ポリシーは、**aaa authorization** コマンドによって IKEv2 プロファイルから示されます。

IKEv2 名前分割

IKEv2 名前分割は、IKEv2 認証用のユーザ名の取得およびピア IKE ID からの AAA 事前共有キーの取得に使用されます。

IKEv2 マルチ SA

IKEv2 マルチ SA 機能によって、IKEv2 応答側の IKEv2 ダイナミック仮想トンネル インターフェイス（DVTI）セッションは複数の IPsec セキュリティ アソシエーション（SA）をサポートできます。DVTI セッションあたりの IPSec SA の最大数は、AAA 認証から取得されるか IPsec プロファイルで設定されます。AAA からの値が優先されます。IPsec プロファイルでの *max-flow-limit* 引数への変更は現在のセッションには適用されませんが、後続のセッションに適用されます。IKEv2 マルチ SA 機能では、IPsec プロファイルでの IKEv2 プロファイルの設定は任意です。この任意設定によって、同じ仮想テンプレートを使用する IPsec DVTI セッションで異なる IKEv2 プロファイルを使用できるようになり、仮想テンプレート設定の数が削減されます。

（注） IKEv2 マルチ SA 機能では、非 any-any プロキシを持つ複数の IPsec SA が許可されます。ただし、IPSec SA プロキシが any-any の場合は 1 つの IPsec SA が許可されます。

詳細については、『*Security for VPNs with IPsec Configuration Guide*』の『Multi-SA Support for Dynamic Virtual Tunnel Interfaces for IKEv2』モジュールを参照してください。

IKEv2 ダイナミック ルーティング

IKEv2 スタティック ルーティングでは、最初のセッションの起動中にルート情報が交換されます。IKEv2 ダイナミック ルーティング サポート機能を使用すると、セッションが確立された後でもルート情報を交換できます。新しいルートやルートの追加または削除などのルーティング情報の変更は、FlexVPN クライアントから FlexVPN サーバに伝播できます。ルート情報は、IKEv2 情報交換メッセージに含まれています。

IKEv2 ダイナミック ルーティング サポート機能は、SVTI、FlexVPN クライアント、および FlexVPN スポークでサポートされています。詳細については、『*FlexVPN and Internet Key Exchange Version 2 Configuration Guide, Cisco IOS Release 15M&T*』の『Configuring the FlexVPN Client』モジュールにある「IKEv2 Dynamic Routing」の項を参照してください。この機能を FlexVPN クライアントで使用するには、FlexVPN サーバのソフトウェア リリースが Cisco IOS XE Everest 16.5.1 以降である必要があります。

（注） FlexVPN クライアントからの接続ルートの再配布のみがサポートされています。

AnyConnect プロファイルのダウンロード

FlexVPN AnyConnect プロファイルのダウンロード機能を使用すると、Cisco IOS XE ソフトウェアを実行しているデバイスが、Cisco AnyConnect セキュア モビリティ クライアントに IKEv2 プロトコルで接続してプロファイル情報をプッシュできます。

Cisco AnyConnect セキュア モビリティ クライアントには、VPN の設定に使用されるプロファイルが含まれています。このプロファイルは、手動で設定することも、ヘッドエンドからダウンロードすることもできます。ヘッドエンドは、Cisco AnyConnect セキュア モビリティ クライアントのすべてのユーザにプロファイルをグローバルに展開するように設定できます。

VPN プロファイルを IKEv2 プロファイルと照合するには、**anyconnect profile** コマンドを使用します。

（注） AnyConnect プロファイルのダウンロード機能を設定する際、crypto ssl profile は必須ではありません。

サポートされる RADIUS 属性

次のテーブルに、IKEv2 FlexVPN サーバがサポートする RADIUS 属性を示します。

- [Scope] フィールドは、属性の方向と、FlexVPN サーバまたはクライアントでの使用方法を定義します。
  - [Inbound]：FlexVPN サーバから RADIUS
  - [Outbound]：RADIUS から FlexVPN サーバ
  - [Local]：FlexVPN サーバによってローカルで使用される
  - [Remote]：FlexVPN サーバによってクライアントにプッシュされる
- [Local configuration] フィールドは、FlexVPN サーバでローカルに属性を設定するために使用される、IKEv2 認証ポリシー コマンドを指定します。
- Cisco AV ペアは、vendor-id が 9、vendor-type が 1 の Cisco ベンダー固有属性（VSA）です。VSA は、RADIUS IETF 属性 26 のベンダー固有でカプセル化されます。Cisco AV ペアは、文字列形式「protocol:attribute=value」で指定されます。

例：

```
cisco-avpair = “ipsec:ipv6-addr-pool=v6-pool”
```

次に、標準アクセス リストの Cisco AV ペアの例を示します。

```
cisco-avpair = "ipsec:route-set=access-list 99"
```

表 *4*：着信および双方向の *IETF RADIUS* 属性

属性	スコープ
User-Name	着信と発信（双方向）
User-Password	着信
Calling-Station-Id	着信
Service-Type	着信
EAP-Message	双方向
Message-Authenticator	双方向

表 *5*：発信 *IETF* および *Cisco AV* ペアの *RADIUS* 属性

属性	タイプ	スコープ	ローカル設定
Tunnel-Type	IETF	Local	該当なし
Tunnel-Medium-Type	IETF	Local	該当なし
Tunnel-Password	IETF	Local	該当なし
ipsec:ikev2-password-local	Cisco AV ペア	Local	該当なし
ipsec:ikev2-password-remote	Cisco AV ペア	Local	該当なし
ipsec:addr-pool	Cisco AV ペア	Local	pool
ipsec:group-dhcp-server	Cisco AV ペア	Local	dhcp server
ipsec:dhcp-giaddr	Cisco AV ペア	Local	dhcp giaddr
ipsec:dhcp-timeout	Cisco AV ペア	Local	dhcp timeout
ipsec:ipv6-addr-pool	Cisco AV ペア	Local	ipv6 pool
ipsec:route-set=interface	Cisco AV ペア	Local	route set interface

属性	タイプ	スコープ	ローカル設定
ipsec:route-set=prefix	Cisco AV ペア	Local	該当なし
ipsec:route-accept	Cisco AV ペア	Local	route accept any
ip:interface-config	Cisco AV ペア	Local	aaa attribute list
ipsec:ipsec-flow-limit	Cisco AV ペア	Local	ipsec flow-limit
Framed-IP-Address	IETF	Remote	該当なし
Framed-IP-Netmask	IETF	Remote	netmask
ipsec:dns-servers	Cisco AV ペア	Remote	DNS
ipsec:wins-servers	Cisco AV ペア	Remote	wins
ipsec:route-set=access-list （注 1 を参照）	Cisco AV ペア	Remote	route set access-list （注 1 を参照）
ipsec:addrv6	Cisco AV ペア	Remote	n/a
ipsec:prefix-len	Cisco AV ペア	Remote	n/a
ipsec:ipv6-dns-servers-addr	Cisco AV ペア	Remote	ipv6 dns
ipsec:route-set=access-list ipv6	Cisco AV ペア	Remote	route set access-list ipv6
ipsec:banner	Cisco AV ペア	Remote	banner
ipsec:default-domain	Cisco AV ペア	Remote	def-domain
ipsec:split-dns	Cisco AV ペア	Remote	split-dns

属性	タイプ	スコープ	ローカル設定
ipsec:ipsec-backup-gateway	Cisco AV ペア	Remote	backup-gateway
ipsec:pfs	Cisco AV ペア	Remote	pfs
ipsec:include-local-lan	Cisco AV ペア	Remote	include-local-lan
ipsec:smartcard-removal-disconnect	Cisco AV ペア	Remote	smartcard-removal- disconnect
ipsec:configuration-url	Cisco AV ペア	Remote	configuration url
ipsec:configuration-version	Cisco AV ペア	Remote	configuration version

（注）

- 1. IKEv2 FlexVPN サーバでアクセス リストを設定するための RADIUS 属性は、標準アクセス リストのみをサポートします。拡張アクセス リストはサポートされていません。

サポートされるリモート アクセス クライアント

FlexVPN サーバは、Microsoft 7 IKEv2 クライアント、Cisco IKEv2 AnyConnect クライアント、および Cisco FlexVPN クライアントと相互運用されます。

Microsoft Windows 7 IKEv2 クライアント

Microsoft Windows 7 IKEv2 クライアントは、インターネット キー エクスチェンジ（IKE）ID として IP アドレスを送信します。この ID は、Cisco IKEv2 FlexVPN サーバが IKE ID に基づいてリモート ユーザを分類するのを防ぎます。Windows 7 IKEv2 クライアントが電子メールアドレス（user@domain）を IKE ID として送信できるようにするには、KB975488（http://support.microsoft.com/kb/975488）に記載されたホットフィックスを Windows 7 に適用し、電子メールアドレスの文字列を、プロンプトが表示された場合は [Username] フィールドまたは証明書の [CommonName] フィールドに、認証方式に応じて指定します。

証明書ベースの認証の場合は、次のように、FlexVPN サーバと Microsoft Windows 7 クライアントの証明書に拡張キー使用法（EKU）フィールドが含まれている必要があります。

- クライアント証明書では、EKU フィールド = クライアント認証証明書です。
- サーバ証明書では、EKU フィールド = サーバ認証証明書です。

- 証明書は、Microsoft の証明書サーバまたは IOS CA サーバから取得できます。

EAP 認証の場合は、Microsoft Windows 7 IKEv2 クライアントが他の EAP 要求の前に EAP ID 要求を待ちます。クライアントに EAP ID 要求を送信するには、IKEv2 FlexVPN サーバ上の IKEv2 プロファイル内で **query-identity** キーワードが設定されていることを確認してください。

Cisco IKEv2 AnyConnect クライアント

証明書ベースの認証では、次のように FlexVPN サーバと AnyConnect クライアントの証明書に拡張キー使用法（EKU）フィールドが含まれている必要があります。

- クライアント証明書では、EKU フィールド = クライアント認証証明書です。
- サーバ証明書では、EKU フィールド = サーバ認証証明書です。

FlexVPN サーバが証明書を使用して AnyConnect クライアントを認証する場合、サーバの IP アドレスまたは完全修飾ドメイン名（FQDN）を含む FlexVPN サーバの証明書に SubjectAltName の拡張子が必要です。また、**no crypto ikev2 http-url cert** コマンドを使用して、HTTP 認証 URL を FlexVPN サーバで無効にしておく必要があります。

次の例では、AnyConnect クライアント プロファイルの IKEv2 セッションの EAP-MD5 認証に固有の XML タグを示します。

```
<PrimaryProtocol>IPsec
       <StandardAuthenticationOnly>true
           <AuthMethodDuringIKENegotiation>
               EAP-MD5
           </AuthMethodDuringIKENegotiation>
           <IKEIdentity>DEPT24</IKEIdentity>
       </StandardAuthenticationOnly>
</PrimaryProtocol>
```

詳細については、次のリンクで AnyConnect クライアント 3.0 のドキュメントを参照してください。
http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect30/release/notes/anyconnect30rn.html#wp1268255

FlexVPN サーバの設定方法

FlexVPN サーバの IKEv2 プロファイルの設定

このタスクでは、基本的な IKEv2 プロファイル コマンドに加えて、FlexVPN サーバの設定に必要な IKEv2 プロファイル コマンドについて説明します。基本的な IKEv2 プロファイルの設定方法については、『*Configuring Internet Key Exchange Version 2 (IKEv2)*』機能モジュールの「Configuring IKEv2 Profile (Basic)」タスクを参照してください。

このタスクは、FlexVPN サーバの IKEv2 プロファイルを設定するために実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ikev2 profile** *profile-name*
4. **aaa authentication eap** *list-name*
5. **authentication** {**local** {**rsa-sig** | **pre-share** [**key** {**0** | **6**} *password*}] | **ecdsa-sig** | **eap** [**gtc** | **md5** | **ms-chapv2**] [**username** *username*] [**password** {**0** | **6**} *password*}]} | **remote** {**eap** [**query-identity** | **timeout** *seconds*] | **rsa-sig** | **pre-share** [**key** {**0** | **6**} *password*}] | **ecdsa-sig**}}
6. 次のいずれかまたは両方を実行します。
   - **aaa authorization user** {**eap** | **psk**} {**cached** | **list** *aaa-listname* [*aaa-username* | **name-mangler** *mangler-name*]}
   - **aaa authorization user cert list** *aaa-listname* {*aaa-username* | **name-mangler** *mangler-name*}
7. 次のいずれかまたは両方を実行します。
   - **aaa authorization group** [**override**] {**eap** | **psk**} **list** *aaa-listname* [*aaa-username* | **name-mangler** *mangler-name*]
   - **aaa authorization group** [**override**] **cert list** *aaa-listname* {*aaa-username* | **name-mangler** *mangler-name*}
8. **crypto vpn anyconnect profile** *profile-name* **flash:***file-name*
9. **anyconnect profile** *profile-name*
10. **config-exchange** {**request** | **set** {**accept** | **send**}}
11. **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プロファイル名を定義し、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	**aaa authentication eap** *list-name* 例： `Device(config-ikev2-profile)# aaa authentication eap list1`	（任意）IKEv2 リモート アクセス サーバの実装中に EAP 認証用の AAA 認証リストを指定します。 • **eap**：外部 EAP サーバを指定します。 • *list-name*：AAA 認証リスト名。

	コマンドまたはアクション	目的
ステップ 5	**authentication** {**local** {**rsa-sig** | **pre-share** [**key** {**0** | **6**} *password*}] | **ecdsa-sig** | **eap** [**gtc** | **md5** | **ms-chapv2**] [**username** *username*] [**password** {**0** | **6**} *password*}]} | **remote** {**eap** [**query-identity** | **timeout** *seconds*] | **rsa-sig** | **pre-share** [**key** {**0** | **6**} *password*}] | **ecdsa-sig**}} 例： `Device(config-ikev2-profile)# authentication local ecdsa-sig`	ローカルまたはリモートの認証方式を指定します。 • **rsa-sig**：認証方式として RSA-sig を指定します。 • **pre-share**：認証方式として事前共有キーを指定します。 • **ecdsa-sig**：認証方式として ECDSA-sig を指定します。 • **eap**：リモート認証方式として EAP を指定します。 • **query-identity**：ピアに EAP ID を問い合わせます。 • **timeout** *seconds*：最初の IKE_AUTH 応答を返してから次の IKE_AUTH 要求を受け取るまでの期間を秒単位で指定します。 （注） ローカル認証方式は 1 つしか指定できませんが、リモート認証方式は複数指定できます。

ステップ 6	次のいずれかまたは両方を実行します。
	• **aaa authorization user** {**eap** | **psk**} {**cached** | **list** *aaa-listname* [*aaa-username* | **name-mangler** *mangler-name*]}
	• **aaa authorization user cert list** *aaa-listname* {*aaa-username* | **name-mangler** *mangler-name*}
	例：
	`Device(config-ikev2-profile)# aaa authorization user eap cached`
	例：
	`Device(config-ikev2-profile)# aaa authorization user cert list list1 name-mangler mangler1`
		ユーザ認可用の AAA 方式リストとユーザ名を指定します。
		• **user**：ユーザ認可を指定します。
		• **cert**：ピアは証明書を使用して認証を受ける必要があることを指定します。
		• **eap**：ピアは EAP を使用して認証を受ける必要があることを指定します。
		• **psk**：ピアは事前共有キーを使用して認証を受ける必要があることを指定します。
		• **cached**：EAP 認証中に受信した属性または AAA 事前共有キーから取得した属性をキャッシュする必要があることを指定します。
		• *aaa-listname*：AAA 方式リスト名。
		• *aaa-username*：AAA 認可要求で使用する必要があるユーザ名を指定します。
		• **name-mangler**：ピア ID から AAA 認可ユーザ名を抽出する name mangler を指定します。

	コマンドまたはアクション	目的
		• *mangler-name*：使用する name mangler。 （注） • **psk** 認証方式と **eap** 認証方式では、*aaa-username* 引数または **name-mangler** キーワードの指定は任意で、指定しなかった場合は、ピア ID がユーザ名として使用されます。 • **psk** 認証方式と **eap** 認証方式では、それぞれ、**cached** キーワードと **list** キーワードを使用して 2 つのユーザ認可用のバリアントを同時に設定できます。 • **cert** 認証ではタイプが識別名（DN）のピア ID を使用できないため、*aaa-username* 引数または **name-mangler** キーワードの指定が必須です。

ステップ 7	次のいずれかまたは両方を実行します。
	• **aaa authorization group** [**override**] {**eap** | **psk**} **list** *aaa-listname* [*aaa-username* | **name-mangler** *mangler-name*]
	• **aaa authorization group** [**override**] **cert list** *aaa-listname* {*aaa-username* | **name-mangler** *mangler-name*}
	例：
	`Device(config-ikev2-profile)# aaa authorization group override psk list list1`
	例：
	`Device(config-ikev2-profile)# aaa authorization group cert list list1 name-mangler mangler1`
		グループ認可用の AAA 方式リストとユーザ名を指定します。
		• **group**：グループ認可を指定します。
		• **override**：（任意）属性のマージ中はグループ認可からの属性を優先する必要があることを指定します。デフォルトでは、ユーザ属性が優先されます。
		• **cert**：ピアは証明書を使用して認証を受ける必要があることを指定します。
		• **eap**：ピアは EAP を使用して認証を受ける必要があることを指定します。
		• **psk**：ピアは事前共有キーを使用して認証を受ける必要があることを指定します。
		• *aaa-listname*：AAA 方式リスト名。
		• *aaa-username*：AAA 認可要求で使用する必要があるユーザ名。
		• **name-mangler**：ピア ID から AAA 認可ユーザ名を抽出する name mangler を指定します。
		• *mangler-name*：使用する name mangler。

	コマンドまたはアクション	目的
		（注） • **psk** 認証方式と **eap** 認証方式では、*aaa-username* 引数または **name-mangler** キーワードの指定は任意で、指定しなかった場合は、ピア ID がユーザ名として使用されます。 • **psk** 認証方式と **eap** 認証方式では、それぞれ、**cached** キーワードと **list** キーワードを使用して 2 つのユーザ認可用のバリアントを同時に設定できます。 • **cert** 認証ではタイプが識別名（DN）のピア ID を使用できないため、*aaa-username* 引数または **name-mangler** キーワードの指定が必須です。
ステップ 8	**crypto vpn anyconnect profile** *profile-name* **flash:***file-name* 例： `Device(config-ikev2-profile)# crypto vpn anyconnect profile vpn-profile flash:test1.xml`	AnyConnect プロファイルを定義します。
ステップ 9	**anyconnect profile** *profile-name* 例： `Device(config-ikev2-profile)# anyconnect profile vpn-profile`	Cisco AnyConnect プロファイルのダウンロードを有効にします。 （注） この手順で示したプロファイル名は、**crypto vpn anyconnect profile** *profile-name* **flash:***file-name* コマンドの Cisco AnyConnect プロファイルを参照する必要があります。
ステップ 10	**config-exchange** {**request** | **set** {**accept** | **send**}} 例： `Device(config-ikev2-profile)# config-exchange set accept`	（任意）設定交換オプションを有効にします。 • **request**：設定交換要求を有効にします。 • **set**：設定交換要求セット オプションを有効にします。 • **accept**：設定交換要求セットを受け入れます。 • **send**：設定交換セットの送信を有効にします。 （注） デフォルトで、request オプションと set オプションが有効になります。

	コマンドまたはアクション	目的
ステップ 11	**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 名前分割の設定

このタスクを実行して、IKEv2名前分割を指定します。これを使用して認証要求の名前を生成し、AAA 事前共有キーを取得します。この名前は、リモート IKE ID または EAP ID の異なる形式の指定した部分から派生します。ここで指定した名前分割は、IKEv2プロファイルに結び付けられます。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ikev2 name-mangler** *mangler-name*
4. **dn** {**common-name** | **country** | **domain** | **locality** | **organization** | **organization-unit** | **state**}
5. **eap** {**all** | **dn** {**common-name** | **country** | **domain** | **locality** | **organization** | **organization-unit** | **state**} | **prefix** | **suffix** {**delimiter** {**.** | **@** | \}}}
6. **email** {**all** | **domain** | **username**}
7. **fqdn** {**all** | **domain** | **hostname**}
8. **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 name-mangler** *mangler-name* 例： `Device(config)# crypto ikev2 name-mangler mangler1`	名前分割を定義し、IKEv2名前分割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	**dn** {**common-name**	**country**	**domain**	**locality**	**organization**	**organization-unit**	**state**} 例： `Device(config-ikev2-name-mangler)# dn state`	DN （識別名）タイプのリモートIDで、次のフィールドのいずれかから名前が派生します。 • **common-name** • **country**

	コマンドまたはアクション	目的
		• **domain** • **locality** • **organization** • **organization-unit** • **state**
ステップ 5	**eap** {**all** | **dn** {**common-name** | **country** | **domain** | **locality** | **organization** | **organization-unit** | **state**} | **prefix** | **suffix** {**delimiter** {**.** | **@** | \}}} 例： `Device(config-ikev2-name-mangler)# eap prefix delimiter @`	タイプが EAP（Extensible Authentication Protocol）のリモート ID から名前が派生します。 • **all**：EAP ID 全体から名前が派生します。 • **dn**：DN タイプのリモート EAP ID の次のフィールドのいずれかから名前が派生します。 • **common-name** • **country** • **domain** • **locality** • **organization** • **organization-unit** • **state** • **prefix**：EAP ID のプレフィックスから名前が派生します。 • **suffix**：EAP ID のサフィックスから名前が派生します。 • **delimiter** {**.** | **@** | \}：プレフィックスとサフィックスを分割する、EAP ID のデリミタを指定します。
ステップ 6	**email** {**all** | **domain** | **username**} 例： `Device(config-ikev2-name-mangler)# email username`	電子メール タイプのリモート ID から名前が派生します。 • **all**：電子メール タイプのリモート IKE ID 全体から名前が派生します。 • **domain**：リモート IKE ID のドメイン部分から名前が派生します。 • **username**：リモート IKE ID のユーザ名部分から名前が派生します。
ステップ 7	**fqdn** {**all** | **domain** | **hostname**} 例：	タイプが FQDN（完全修飾ドメイン名）のリモート ID から名前が派生します。

	コマンドまたはアクション	目的
	`Device(config-ikev2-name-mangler)# fqdn domain`	• **all**：FQDN タイプのリモート IKE ID 全体から名前が派生します。 • **domain**：リモート IKE ID のドメイン部分から名前が派生します。 • **hostname**：リモート IKE ID のホスト名部分から名前が派生します。
ステップ 8	**end** 例： `Device(config-ikev2-name-mangler)# end`	IKEv2 名前分割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 認証ポリシーの設定

このタスクを実行して、IKEv2 認証ポリシーを設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ikev2 authorization policy** *policy-name*
4. **aaa attribute list** *list-name*
5. **backup-gateway** *string*
6. **banner** *banner-text*
7. **configuration url** *url*
8. **configuration version** *version*
9. **def-domain** *domain-name*
10. **dhcp** { **giaddr** *ip-address* | **server** {*ip-address* | *hostname*} | **timeout** *seconds*}
11. [**ipv6**] **dns** *primary-server* [*secondary-server*]
12. **include-local-lan**
13. **ipsec flow-limit** *number*
14. **netmask** *mask*
15. **pfs**
16. [**ipv6**] **pool** *name*
17. **route set** { **interface** *interface* | **access-list** {*access-list-name* | *access-list-number* | **ipv6** *access-list-name*}}
18. **route accept any** [**tag** *value*] [**distance** *value*]
19. **route redistribute** *protocol* [**route-map** *map-name*]
20. **route set remote** { **ipv4** *ip-address mask* | **ipv6** *ip-address*/*mask*}
21. **smartcard-removal-disconnect**
22. **split-dns** *string*
23. **session-lifetime** *seconds*
24. **route set access-list** {*acl-number* | [**ipv6**] *acl-name*}

25. **wins** *primary-server* [*secondary-server*]
26. **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 authorization policy** *policy-name* 例： `Device(config)# crypto ikev2 authorization policy policy1`	IKEv2 認証ポリシーを指定して、IKEv2 認証ポリシー設定モードを開始します。
ステップ 4	**aaa attribute list** *list-name* 例： `Device(config-ikev2-author-policy)# aaa attribute list list1`	AAA 属性のリストを指定します。 （注） このコマンドで参照されている AAA 属性リストは、グローバル コンフィギュレーション モードで定義する必要があります。
ステップ 5	**backup-gateway** *string* 例： `Device(config-ikev2-author-policy)# backup-gateway gateway1`	最大 10 台のバックアップ サーバ名を指定できます。このパラメータは、非標準 Cisco Unity コンフィギュレーション属性によってクライアントにプッシュされます。このパラメータは、クライアントが使用可能なバックアップ サーバを指定します。
ステップ 6	**banner** *banner-text* 例： `Device(config-ikev2-author-policy)# banner This is IKEv2`	バナーを指定します。このパラメータは、非標準 Cisco Unity コンフィギュレーション属性によってクライアントに送信されます。
ステップ 7	**configuration url** *url* 例： `Device(config-ikev2-author-policy)# configuration url http://www.cisco.com`	コンフィギュレーション URL を指定します。このパラメータは、非標準 Cisco FlexVPN コンフィギュレーション属性によってクライアントに送信されます。クライアントはこの URL を使用して、コンフィギュレーションをダウンロードできます。
ステップ 8	**configuration version** *version* 例： `Device(config-ikev2-author-policy)# configuration version 2.4`	コンフィギュレーションバージョンを指定します。このパラメータは、非標準 Cisco FlexVPN コンフィギュレーション属性によってクライアントに送信されます。このパラメータは、コンフィギュレーショ

	コマンドまたはアクション	目的
		ン URL と送信され、クライアントがダウンロードできるバージョンを指定します。
ステップ 9	**def-domain** *domain-name* 例： `Device(config-ikev2-author-policy)# def-domain cisco`	デフォルト ドメインを指定します。このパラメータは、非標準 Cisco Unity コンフィギュレーション属性によってクライアントに送信されます。このパラメータは、クライアントが使用可能なデフォルトドメインを指定します。
ステップ 10	**dhcp** { **giaddr** *ip-address* | **server** {*ip-address* | *hostname*} | **timeout** *seconds*} 例： `Device(config-ikev2-author-policy)# dhcp giaddr 192.0.2.1`	リモート アクセス クライアントに割り当てられる IP アドレスをリースする DHCP サーバを指定します。 • **giaddr** *ip-address*：ゲートウェイ IP アドレス（giaddr）を指定します。 • **server** {*ip-address* | *hostname*}：DHCP サーバの IP アドレスまたはホスト名を指定します。ホスト名は、設定時に解決されます。 • **timeout** *seconds*：DHCP サーバからの応答待ち時間を秒単位で指定します。 （注） 指定できる DHCP サーバは 1 つのみです。DHCP サーバはグローバル ルーティング テーブル経由で到達可能なことが前提であるため、DHCP パケットはグローバルルーティングテーブルに転送されます。
ステップ 11	[**ipv6**] **dns** *primary-server* [*secondary-server*] 例： `Device(config-ikev2-author-policy)# dns 198.51.100.1 198.51.100.100`	設定応答でクライアントに送信される、プライマリおよびセカンダリ ドメイン名サービス（DNS）サーバの IP アドレスを指定します。 • **ipv6**：（オプション）DNS サーバの IPv6 アドレスを指定します。IPv4 アドレスを指定するには、このキーワードなしでコマンドを実行します。 • *primary-server*：プライマリ DNS サーバの IP アドレス。 • *secondary-server*：（任意）セカンダリ DNS サーバの IP アドレス。

	コマンドまたはアクション	目的
ステップ 12	**include-local-lan** 例： `Device(config-ikev2-author-policy)# include-local-lan`	ローカル LAN を含めます。このパラメータは、非標準 Cisco Unity コンフィギュレーション属性によってクライアントに送信されます。
ステップ 13	**ipsec flow-limit** *number* 例： `Device(config-ikev2-author-policy)# ipsec flow-limit 12500`	IKEv2 応答側の IKEv2 dVTI セッションが使用できる IPSec SAS の最大数を指定します。範囲は 0 ～ 50000 です。 デフォルトではコマンドは無効であり、dVTI セッションあたりの IPSec フローの数に制限はありません。値 0 では、IPSec SA は許可されません。
ステップ 14	**netmask** *mask* 例： `Device(config-ikev2-author-policy)# netmask 255.255.255.0`	クライアントに IP アドレスを割り当てるサブネットのネットマスクを指定します。 • *mask*：サブネット マスク アドレス。
ステップ 15	**pfs** 例： `Device(config-ikev2-author-policy)# pfs`	パスワード転送セキュリティ（PFS）を有効にします。このパラメータは、非標準 Cisco Unity コンフィギュレーション属性によってクライアントに送信されます。このパラメータは、クライアントで PFS を使用する必要性を指定します。
ステップ 16	[**ipv6**] **pool** *name* 例： `Device(config-ikev2-author-policy)# pool abc`	リモート アクセス クライアントに IP アドレスを割り当てるためのローカル IP アドレス プールを定義します。 • **ipv6**：（オプション）IPv6 アドレス プールを指定します。IPv4 アドレスを指定するには、このキーワードなしでコマンドを実行します。 • *name*：ローカル IP アドレス プールの名前。 （注） **ip local pool** コマンドを使用してすでに定義されているローカル IP アドレス プールを使用する必要があります。
ステップ 17	**route set** { **interface** *interface* | **access-list** {*access-list-name* | *access-list-number* | **ipv6** *access-list-name*}} 例： `Device(config-ikev2-author-policy)# route set interface`	コンフィギュレーション モードでピアに向かうルート設定パラメータを指定し、Border Gateway Protocol（BGP） over VPN などのルーティング プロトコルを実行できます。 • **interface**：ルート インターフェイスを指定します。

	コマンドまたはアクション	目的
		• **access-list**：ルート アクセス リストを指定します。 • *access-list-name*：アクセス リストの名前。 • *access-list-number*：標準のアクセス リスト番号。 • **ipv6**IPv6 アクセス リストを指定します。
ステップ 18	**route accept any** [**tag** *value*] [**distance** *value*] 例： `Device(config-ikev2-author-policy)# route accept any tag 10`	ピアから受信したルートをフィルタリングし、それらのルートをインストールするためにタグとメトリック値を指定します。 • **any**：ピアから受信したすべてのルートを受け入れます。 • **tag** *value*：（オプション）IKEv2 によって追加された静的ルートのタグ ID を指定します。範囲は 1 ～ 497777 です。 • **distance** *value*：（オプション）IKEv2 によって追加された静的ルートの距離を指定します。範囲は 1 ～ 255 です。
ステップ 19	**route redistribute** *protocol* [**route-map** *map-name*] 例： `Device(config-ikev2-author-policy)# route redistribute connected`	ピアから受信したルートをフィルタリングし、それらのルートをインストールするためにタグとメトリック値を指定します。 • *protocol*：ルートの再配布元のプロトコルです。connected または static のいずれかのキーワードを指定できます。 • **route-map** *map-name*：（オプション）ソース ルーティング プロトコルから別のルーティング プロトコルにルートをインポートするためにフィルタ処理する必要があるルートマップ。マップ名を指定しないと、すべてのルートが再配布されます。
ステップ 20	**route set remote** { **ipv4** *ip-address mask* | **ipv6** *ip-address*/*mask*} 例： `Device(config-ikev2-author-policy)# route set remote ipv6 2001:DB8::1/32`	内部ネットワークの IP アドレスを設定します。

	コマンドまたはアクション	目的
ステップ 21	**smartcard-removal-disconnect** 例： `Device(config-ikev2-author-policy)# smartcard-removal-disconnect`	スマートカードの取り外しと切断を有効にします。このパラメータは、非標準Cisco Unityコンフィギュレーション属性によってクライアントに送信されます。このパラメータでは、スマート カードが取り外された場合に、クライアントがセッションを停止する必要があることを指定します。
ステップ 22	**split-dns** *string* 例： `Device(config-ikev2-author-policy)# split-dns abc1`	最大 10 台の分割ドメイン名を指定できます。このパラメータは、非標準Cisco Unityコンフィギュレーション属性によってクライアントに送信されます。このパラメータは、クライアントがプライベート ネットワークに使用する必要があるドメイン名を指定します。
ステップ 23	**session-lifetime** *seconds* 例： `Device(config-ikev2-author-policy)# session-lifetime 1000`	IKEv2 セッションのライフタイムを指定します。 • **seconds** *seconds*：範囲は 120 ～ 25920000 で、2 分間～ 300 日間に変換されます。
ステップ 24	**route set access-list** {*acl-number* | [**ipv6**] *acl-name*} 例： `Device(config-ikev2-client-config-group)# route set access-list 110`	コンフィギュレーション モードを介してリモート ピアにプッシュされるサブネットを指定します。 • *acl-number*：アクセス リスト番号（ACL）。ACL 番号は IPv4 ACL にのみ指定できます。 • **ipv6**：（オプション）IPv6アクセス コントロール リスト（ACL）を指定します。IPv4 属性を指定するには、このキーワードなしでコマンドを実行します。 • *acl-name*：アクセス リスト名。 （注） IPv4 アドレスに標準の、シンプルなアクセス リストのみを指定できます。
ステップ 25	**wins** *primary-server* [*secondary-server*] 例： `Device(config-ikev2-author-policy)# wins 203.0.113.1 203.0.113.115`	設定応答でクライアントに送信される、内部の Windows Internet Naming Service（WINS）サーバ アドレスを指定します。 • *primary-server*：プライマリ WINS サーバの IP アドレス。 • *secondary-server*：（任意）セカンダリ WINS サーバの IP アドレス。
ステップ 26	**end** 例：	IKEv2 認証ポリシー設定モードを終了し、特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	Device(config-ikev2-author-policy)# end	

FlexVPN サーバの構成例

例：FlexVPN サーバの設定

例：EAP を使用してピアを認証するための FlexVPN サーバの設定

この例では、EAP を使用してピアを認証するため、FlexVPN サーバを設定する方法を示します。

```
aaa new-model
!
aaa group server radius eap-server
 server 192.168.2.1
!
aaa authentication login eap-list group eap-server
!
crypto pki trustpoint trustpoint1
 enrollment url http://192.168.3.1:80
 revocation-check crl
!
crypto ikev2 profile ikev2-profile1
 match identity remote address 0.0.0.0
 authentication local rsa-sig
 authentication remote eap query-identity
 pki trustpoint trustpoint1
 aaa authentication eap eap-list
 virtual-template 1
!
crypto ipsec transform-set transform1 esp-aes esp-sha-hmac
!
crypto ipsec profile ipsec-profile1
 set transform-set trans transform1
 set ikev2-profile ikev2-profile1
!
interface Ethernet0/0
 ip address 192.168.1.1 255.255.255.0
!
interface Virtual-Template1 type tunnel
 ip unnumbered Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile ipsec-profile1
!
radius-server host 192.168.2.1 key key1
!
```

例：グループ認証のための FlexVPN サーバの設定（外部 AAA）

次の例は、グループ認証用に FlexVPN サーバを設定する方法を示します。認証は RADIUS または TACACS サーバである外部 AAA を通じて行います。

```
aaa new-model
!
aaa group server radius cisco-acs
 server 192.168.2.2
!
aaa authorization network group-author-list group cisco-acs
!
crypto pki trustpoint trustpoint1
 enrollment url http://192.168.3.1:80
 revocation-check crl
!
crypto pki certificate map certmap1 1
 subject-name co cisco
!
crypto ikev2 name-mangler group-author-mangler
 dn domain
!
crypto ikev2 profile ikev2-profile1
 match certificate certmap1
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint trustpoint1
 aaa authorization group cert list group-author-list name-mangler group-author-mangler
 virtual-template 1
!
crypto ipsec transform-set transform1 esp-aes esp-sha-hmac
!
crypto ipsec profile ipsec-profile1
 set transform-set trans transform1
 set ikev2-profile ikev2-profile1
!
interface Ethernet0/0
 ip address 192.168.1.1 255.255.255.0
!
interface Virtual-Template1 type tunnel
 ip unnumbered Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile ipsec-profile1
!
radius-server host 192.168.2.2 key key2
!
```

例：グループ認証のための FlexVPN サーバの設定（ローカル AAA）

次の例は、グループ認証用にFlexVPNサーバを設定する方法を示します。認証は、IKEv2認証ポリシーを使用するローカル AAA を通じて行います。認証ポリシーでは、コンフィギュレーション モードでクライアントに送信する、標準のIPv4およびIPv6属性、Cisco Unity、FlexVPN属性を指定します。また、認証ポリシーは、ローカル使用に対して、**aaa attribute list** コマンドによってユーザ属性ごとに指定します。

```
aaa new-model
!
aaa authorization network local-group-author-list local
!
!
aaa attribute list attr-list1
 attribute type interface-config "ip mtu 1100"
 attribute type interface-config "tunnel key 10"
!
```

```
crypto pki trustpoint trustpoint1
 enrollment url http://192.168.3.1:80
 revocation-check crl
!
crypto pki certificate map certmap1 1
 subject-name co cisco
!
crypto ikev2 authorization policy author-policy1
 pool pool1
 dhcp server 192.168.4.1
 dhcp timeout 10
 dhcp giaddr 192.168.1.1
 dns 10.1.1.1 10.1.1.2
 route set access-list acl1
 wins 192.168.1.2 192.168.1.3
 netmask 255.0.0.0
 banner ^C flexvpn server ^C
 configuration url http://www.abc.com
 configuration version 10
 def-domain abc.com
 split-dns dns1
 split-dns dns2
 split-dns dns3
 backup-gateway gw1
 backup-gateway gw2
 backup-gateway gw3
 smartcard-removal-disconnect
 include-local-lan
 pfs
 aaa attribute list attr-list1
!
crypto ikev2 profile ikev2-profile1
 match certificate certmap1
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint trustpoint1
 aaa authorization group cert list local-group-author-list author-policy1
 virtual-template 1
!
crypto ipsec transform-set transform1 esp-aes esp-sha-hmac
!
crypto ipsec profile ipsec-profile1
 set transform-set trans transform1
 set ikev2-profile ikev2-profile1
!
interface Ethernet0/0
 ip address 192.168.1.1 255.255.255.0
!
interface Virtual-Template1 type tunnel
 ip unnumbered Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile ipsec-profile1
!
ip local pool pool11 192.168.2.10 192.168.2.100
!
ip access-list extended acl-1
 permit ip 192.168.3.10 192.168.4.100 any
 permit ip 192.168.10.1 192.168.10.100 any
!
```

例：ユーザ認証のための FlexVPN サーバの設定

次の例は、ユーザ認証用に FlexVPN サーバを設定する方法を示します。

```
aaa new-model
!
aaa group server radius cisco-acs
 server 192.168.2.2
!
aaa authorization network user-author-list group cisco-acs
!
crypto pki trustpoint trustpoint1
 enrollment url http:// 192.168.3.1:80
 revocation-check crl
!
crypto pki certificate map certmap1 1
 subject-name co cisco
!
crypto ikev2 name-mangler user-author-mangler
 dn common-name
!
crypto ikev2 profile ikev2-profile1
 match certificate certmap1
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint trustpoint1
 aaa authorization user cert list user-author-list name-mangler user-author-mangler
 virtual-template 1
!
crypto ipsec transform-set transform1 esp-aes esp-sha-hmac
!
crypto ipsec profile ipsec-profile1
 set transform-set trans transform1
 set ikev2-profile ikev2-profile1
!
interface Ethernet0/0
 ip address 192.168.1.1 255.255.255.0
!
interface Virtual-Template1 type tunnel
 ip unnumbered Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile ipsec-profile1
!
radius-server host 192.168.2.2 key key2
!
```

例：IPv6 設定属性による IPv6 セッション用の FlexVPN サーバの設定

次の例に、IPv6 ダイナミック仮想トンネルインターフェイス（dVTI）セッション用に FlexVPN サーバを設定する方法を示します。この例では、IKEv2 認証ポリシーを使用するローカル AAA グループ認証を使用します。IPv6 設定属性は、IKEv2 認証ポリシーの下で設定されます。

```
aaa new-model
!
aaa authorization network local-group-author-list local
!
crypto pki trustpoint trustpoint1
 enrollment url http://192.168.3.1:80
 revocation-check crl
!
crypto pki certificate map certmap1 1
 subject-name co cisco
!
crypto ikev2 authorization policy author-policy1
 ipv6 pool v6-pool
```

```
 ipv6 dns 2001:DB8:1::11 2001:DB8:1::12
 ipv6 subnet-acl v6-acl
!
crypto ikev2 profile ikev2-profile1
 match certificate certmap1
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint trustpoint1
 aaa authorization group cert list local-group-author-list author-policy1
 virtual-template 1
!
crypto ipsec transform-set transform1 esp-aes esp-sha-hmac
!
crypto ipsec profile ipsec-profile1
 set transform-set trans transform1
 set ikev2-profile ikev2-profile1
!
interface Ethernet0/0
 ipv6 address 2001:DB8:1::1/32
!
interface Virtual-Template1 type tunnel
 ipv6 unnumbered Ethernet0/0
 tunnel mode ipsec ipv6
 tunnel protection ipsec profile ipsec-profile1
!
ipv6 local pool v6-pool 2001:DB8:1::10/32 48
!
ipv6 access-list v6-acl
 permit ipv6 host 2001:DB8:1::20 any
 permit ipv6 host 2001:DB8:1::30 any
!
```

例：AnyConnect プロファイルのダウンロードの設定

次の例は、FlexVPN AnyConnectプロファイルのダウンロード機能を設定する方法を示します。

（注） AnyConnect クライアント マシン上のローカル ポリシー ファイルは変更しません。IKEv2 で AnyConnectプロファイルのダウンロード機能を設定すると、必要なXMLプロファイルがクライアント デバイスに自動的にダウンロードされます。

```
no ip http secure-server
crypto ssl policy ssl-policy
  pki trustpoint CA1 sign
  ip address local 10.0.0.1 port 443
  no shutdown
crypto ssl profile ssl_prof
    match policy ssl-policy
crypto vpn anyconnect profile ANY-PROF bootflash:profile.xml
crypto ikev2 profile ikev2_profile
    anyconnect profile ANY-PROF
```

FlexVPN サーバ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』、すべてのリリース
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』
Cisco AnyConnect Secure Mobility Client	https://www.cisco.com/c/en/us/support/security/anyconnect-secure-mobility-client/tsd-products-support-series-home.html
IPsec の設定	『*Configuring Security for VPNs with IPsec*』
推奨される暗号化アルゴリズム	『Next Generation Encryption』

シスコのテクニカル サポート

説明	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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

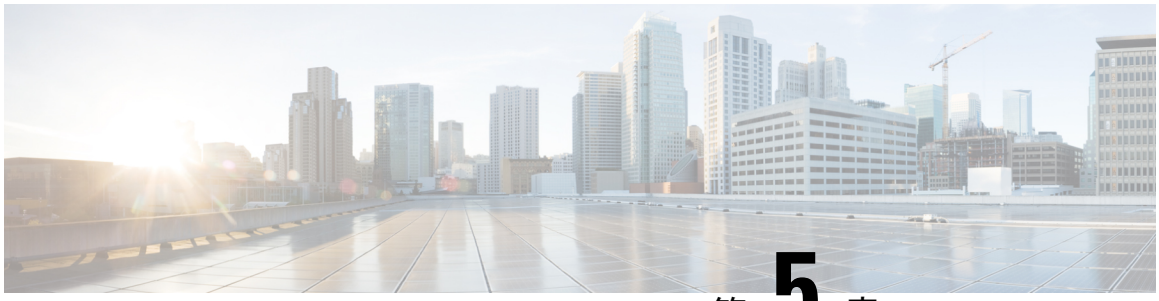
FlexVPN サーバの設定の機能情報

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 *6 : FlexVPN* サーバの設定の機能情報

機能名	リリース	機能情報
FlexVPN AnyConnect プロファイルのダウンロード	Cisco IOS XE Fuji 16.9.1	FlexVPN AnyConnect プロファイルのダウンロード機能を使用すると、Cisco IOS XE ソフトウェアを実行しているデバイスが、Cisco AnyConnect セキュア モビリティ クライアントに IKEv2 プロトコルで接続してプロファイル情報をプッシュできます。 次のコマンドが導入されました。**anyconnect profile**、**crypto vpn anyconnect profile**
リモート アクセス クライアントの IKEv2 ヘッドエンド サポート	Cisco IOS XE Release 3.5S	この機能は、Anyconnect 3.0、FlexVPN ハードウェア クライアント、および VTI のマルチ SA サポートに対する IKEv2 をサポートします。 次のコマンドが導入または変更されました。 **aaa attribute list, backup-gateway, banner, config-mode set, configuration url, configuration version, def-domain, dhcp, dns, include-local-lan, max flow limit, pfs, pool, route accept, route set interface, smartcard-removal-disconnect, split-dns, subnet-acl.**



第 5 章

FlexVPN クライアントの設定

このモジュールでは、FlexVPN クライアント機能と FlexVPN クライアントの設定に必要なインターネット キー エクスチェンジ バージョン 2（IKEv2）コマンドについて説明します。

（注） セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。最新のシスコの暗号化に関する推奨事項については、『Next Generation Encryption』（NGE）ホワイト ペーパーを参照してください。

- 機能情報の確認 （75 ページ）
- FlexVPN クライアントの制限事項 （76 ページ）
- FlexVPN クライアントに関する情報 （77 ページ）
- FlexVPN クライアントの設定方法 （84 ページ）
- FlexVPN クライアントの構成例 （89 ページ）
- FlexVPN クライアントの設定に関する追加情報 （90 ページ）
- FlexVPN クライアントの設定の機能情報 （91 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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。

FlexVPN クライアントの制限事項

ローカル認証方式としての EAP

- ローカル認証方式としての Extensible Authentication Protocol（EAP：拡張可能認証プロトコル）は、IKEv2 発信側でのみサポートされます。リモート認証としては、IKEv2 応答側でのみサポートされます。
- EAP がローカル認証方式として指定されている場合、リモート認証方式は証明書ベースである必要があります。
- FlexVPN サーバで **authentication remote eap query-identity** コマンドが設定されていないと、IP アドレスを EAP 認証方式のユーザ名として使用することはできないため、クライアントはローカル ID として IPv4 アドレスまたは IPv6 アドレスを持つことはできません。

デュアルスタック トンネル インターフェイスおよび VRF 認識 IPsec

VPN ルーティングおよび転送（VRF）認識 IPsec シナリオでデュアルスタック トンネル インターフェイスを設定する場合、**ip vrf forwarding** コマンドを使用して内部 VPN ルーティングおよび転送（IVRF）インスタンスを設定することはできません。これは有効な設定ではないためです。トンネル インターフェイスの IVRF を定義するには **vrf forwarding** *vrf-name* コマンドを使用します。ここで、*vrf-name* 引数は、定義内に IPv4 および IPv6 アドレス ファミリを指定した **vrf definition** コマンドを使用して定義されます。

SSO の制約事項

- Cisco ASR 1000 シリーズ ルータは、Embedded Services Processor（ESP）スイッチオーバーでステートフル IPSec セッションをサポートします。ESP スイッチオーバー中は、すべての IPSec セッションがアップ状態のままになるので、IPSec セッションを維持するためにユーザの操作は必要ありません。
- ESP をリロードした場合（スタンバイ ESP なし）、SA シーケンス番号は 0 から再開されます。ピアルータは、予期されたシーケンス番号を持たないパケットをドロップします。単一の ESP を使用するシステムで ESP のリロード後にこの問題を回避するには、IPSec セッションを明示的に再確立することが必要になる場合があります。このような場合、リロード中に IPSec セッションでトラフィックの中断が発生することがあります。
- Cisco ASR 1000 シリーズ ルータは、現在、ルート プロセッサ（RP）でのステートフル スイッチオーバー（SSO）の IPSec セッションをサポートしていません。IPSec セッションはスイッチオーバーの開始時にダウンしますが、新しい RP がアクティブになるとアップ状態に戻ります。ユーザの操作は必要ありません。セッションがアップ状態に戻るまでの間、スイッチオーバー中に IPSec セッションでトラフィックの中断が発生することがあります。

- Cisco ASR 1000 シリーズ ルータは、IPSec セッションのステートフル ISSU をサポートしていません。ISSU を実行する前に、既存のすべての IPSec セッションまたはトンネルを明示的に終了し、ISSU の実行後に再確立する必要があります。具体的には、ISSU を実行する前に、ハーフオープンまたは確立途中の IPSec トンネルが存在しないことを確認します。これを行うには、トンネル セットアップを開始する可能性のあるインターフェイス（トンネル セットアップを開始するルーティング プロトコルなど）、キープアライブが有効になっているインターフェイス、または IPSec セッションの自動トリガーが存在するインターフェイスの場合は、インターフェイスをシャットダウンすることをお勧めします。この場合、ISSU の実行中に IPSec セッションでトラフィックの中断が発生します。

FlexVPN クライアントに関する情報

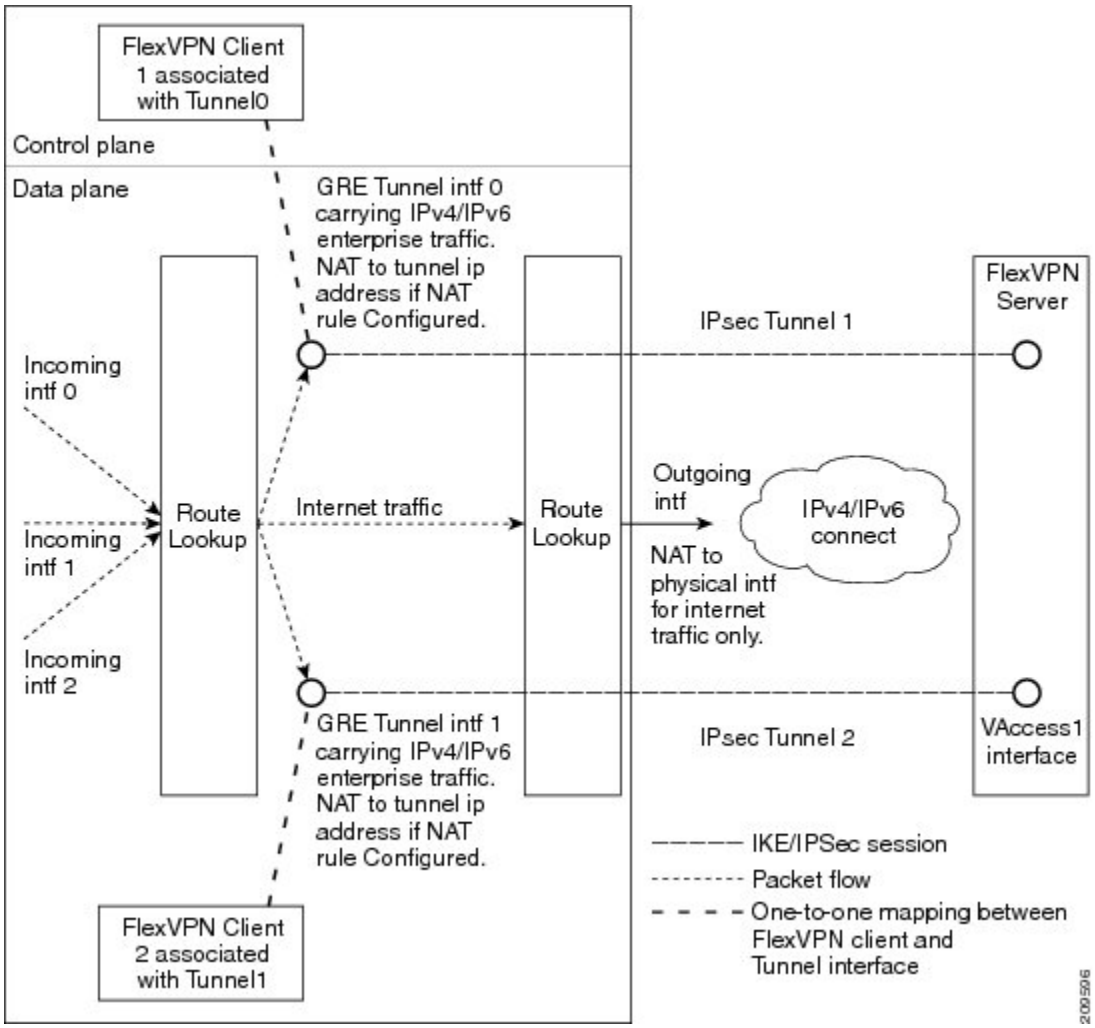
IKEv2 FlexVPN クライアント

IKEv2 FlexVPN クライアント機能は、FlexVPN クライアントと FlexVPN サーバの間にセキュアな IPsec VPN トンネルを確立します。IKEv2 FlexVPN クライアント機能の利点は、次のとおりです。

- トンネル インフラストラクチャの統合
- IPv4/IPv6 トランスポートを介した IPv4/IPv6 プロキシ サポート
- EasyVPN によってサポートされるいくつかの機能との下位互換性
- ダイナミック ルーティング プロトコルを実行するための柔軟性

各 FlexVPN クライアントは、一意のトンネル インターフェイスに関連付けられます。これは、特定の FlexVPN クライアントによって取得された IPsec セキュリティ アソシエーション（SA）がトンネル インターフェイスにバインドされていることを示します。次の図に、FlexVPN クライアントとトンネル インターフェイスとの間の関連付けを示します。

図 *3 : FlexVPN* クライアントとトンネル インターフェイスの関連付け



動作のシーケンスは、次のとおりです。

- ルーティング：FlexVPN サーバは、モード設定応答の一部としてネットワーク リストをプッシュします。クライアントは、これらのネットワークにトンネルインターフェイスのルートを追加します。コンフィギュレーションモード設定の一部として、クライアントはネットワークにルートを送信します。サーバがクライアント側ネットワークにルートを追加できるように、IP アドレスがトンネル インターフェイスに設定されます。
- NAT：ネットワーク アドレス変換（NAT）ルールは、ルート マップを使用して明示的に設定する必要があります。ルールが一致すると、FlexVPN クライアントの背後にあるホストはトンネルの IP アドレスに変換されます。この IP アドレスは、FlexVPN サーバによるモード設定時にプッシュされる属性の 1 つとして取得できます。
- カプセル化および暗号化：Generic Routing Encapsulation（GRE）および IPSec カプセル化モードがサポートされます。GRE は、IPv4 と IPv6 の両方のトラフィックをサポートします。トンネル インターフェイスに到達するトラフィックは、GRE ヘッダーでカプセル化

され、その後に IPSec 保護が実行されます。その後、暗号化されたトラフィックは発信インターフェイスにルーティングされます。

FlexVPN クライアントによってサポートされる機能について、次の項で説明します。

トンネル有効化

FlexVPN クライアントは、自動的にまたはユーザ操作によって手動で接続できます。FlexVPN 設定が完了すると、FlexVPN クライアントは、自動的にトンネルに接続します。トンネルでタイムアウトまたは障害が発生した場合、トンネルは自動的に再接続し、接続を無制限に再試行します。自動トンネル接続を設定するには、IKEv2 FlexVPN プロファイルで **connect** コマンドに **auto** キーワードを使用します。

手動接続では、FlexVPN クライアントは、接続を確立する前にコマンドを実行するユーザの操作を待ちます。クライアントがタイムアウトするか、接続に失敗すると、後続の接続ではユーザの操作が必要になります。手動接続を設定するには、特権 EXEC モードで、**crypto ikev2 client flexvpn connect** コマンドに *flexvpn-name* 引数を使用します。接続を終了するには、**clear crypto ikev2 client flexvpn connect** コマンドに *flexvpn-name* 引数を使用します。

追跡ベースのトンネル有効化

追跡ベースのトンネル有効化機能は、主にバックアップ シナリオで使用されます。FlexVPN クライアントは、オブジェクトの状態変更に関する通知を取得するため、追跡システムに登録されます。この通知はクライアントに、トンネル有効化のための適切なアクションを実行するよう要求します。**connect** コマンドの **track** キーワードによって、クライアントがオブジェクト番号で特定されるオブジェクトの追跡に関心があることを示す、追跡プロセスを通知します。次に、追跡プロセスはクライアントに、オブジェクトの状態がいつ変更されたかを通知します。

connect コマンドの **track** キーワードでトンネル有効化が設定されている場合、オブジェクトが起動すると、オブジェクトがアップ状態にあることを示す通知を受信したクライアントは、接続をトリガーします。**connect** コマンドの **track** キーワードでトンネル有効化が設定されている場合、オブジェクトが停止すると、オブジェクトがダウン状態にあることを示す通知を受信したクライアントは、接続をトリガーします。

バックアップ機能

FlexVPN クライアントは、事前に決定された順序で複数のピアまたはサーバに接続できます。ピアのリストはゲートウェイ リストまたはバックアップ ゲートウェイ リストと呼ばれ、次のリストを使用して作成されます。

- スタティック バックアップ ゲートウェイ リストまたはスタティック リスト
- ダウンロード バックアップ ゲートウェイ リストまたはダウンロード リスト

スタティック バックアップ ゲートウェイ リストは、シーケンス番号の付いたピアのリストを提供することによって FlexVPN プロファイルで設定されます。ダウンロード バックアップ ゲートウェイ リストは、動的にダウンロードされ、モード設定の応答時に取得されます。ダウンロード リストは、スタティック ゲートウェイ リストを補完してバックアップ ゲートウェイ

リストを作成します。ダウンロードリストは、リストがダウンロードされるピアの後に挿入されます。

ゲートウェイ リストのピアとの既存の接続がダウンすると、クライアントはゲートウェイ リストにある次のピアとの接続を確立しようとします。ダウンロード リストが使用可能でスタティック ピアとの接続に失敗すると、クライアントはダウンロード リストのピアと順番に接続しようとします。クライアントがダウンロードリストのすべてのピアとの接続の確立に失敗すると、クライアントはスタティック リストにある次のピアに接続を試みて、ダウンロードリストは削除されます。

バックアップ ゲートウェイ

バックアップ ゲートウェイ リストにピアを追加するには、**peer** コマンドを使用します。バックアップ ゲートウェイ リストを削除するには、**no peer** コマンドを使用します。

ピアは、優先順に並べられています。シーケンス番号が小さいほど、優先順位が高くなります。

新しいピアとの接続が確立され、そのピアがダウンロードリストに含まれていない場合、ピアはバックアップ ゲートウェイ リストにダウンロード リストを追加し、既存のバックアップ ゲートウェイ リストが新しいリストに置き換えられます。

スタティック ピアを設定して、トラック オブジェクトにアタッチすることができます。ピアのトラック オブジェクトがアップ状態の場合、ピアは「可能なピア」になります。

（注） ダウンロード リストのピアを含め、トラック オブジェクトにアタッチされていないピアは、これらのピアが常にアップ状態であるため「可能なピア」に分類されます。

ピアの選択プロセスは、次のように機能します。接続が確立されると、ゲートウェイ リストが検索され、最初の可能なピアが選択されます。ピアは次のルールに従って選択されます。スタティック ピアは、希望するステータス（アップまたはダウン）のトラック オブジェクトに関連付けることができます。トラック オブジェクトのステータスが設定されたステータスと一致すると、ピアは「可能なピア」と呼ばれます。

（注） ピアがドメイン ネーム サービス（DNS）の名前または完全修飾ドメイン名（FQDN）のいずれかによって識別される場合、名前は動的に解決されます。

ピアの選択プロセスの後に、新しいピアが選択されます。また、既存の条件が満たされない場合は、次のシナリオが発生します。

- アクティブなピアが、活性チェックに応答しなくなります。
- ピア名の DNS 解決が失敗します。
- ピアとの IKE ネゴシエーションが失敗します。
- ピアが「可能なピア」でなくなります（対応するトラック オブジェクトがダウンします）。

（注） 複数の FlexVPN ピアを FlexVPN クライアントで設定したり、プライマリ ピアで IKEv2 SA をクリアすると、そのクリアによってクライアントでの新しいピアの選択がトリガーされます。

プライマリ ピアの再アクティブ化

プライマリ ピアの再アクティブ化機能は、最高優先度のピアが常に接続されるようにします。最高優先度のピアのトラック オブジェクトがオブジェクト ステータスと一致する場合、優先度が低いピアがある既存の接続が切断され、最高優先度のピアへの接続が確立されます。この機能を有効にするには、**peer reactivate** コマンドを使用します。

（注） トラック オブジェクトは、静的に設定されたピアに関連付ける必要があります。

ダイヤル バックアップ（プライマリまたはバックアップ トンネル）

オブジェクトの状態の変化ついて通知を受けるように、FlexVPN クライアントを追跡システムに登録します。クライアントがオブジェクトを追跡したい追跡プロセス（オブジェクト番号で識別）について通知するには、**connect track** コマンドを使用します。追跡プロセスでは、このオブジェクトの状態が変わったときにクライアントに順番に通知されます。追跡しているオブジェクトの状態がアップまたはダウンの場合、この通知によってクライアントは、プライマリまたはバックアップ接続を開始または停止するために対処するよう促されます。

ダイヤル バックアップ機能は、次のように設定できます。

- プライマリおよびバックアップ トンネルの両方が FlexVPN トンネルの場合：
  - アクティブなトンネルは、一度に 1 つのみです。
  - 両方のクライアント プロファイルは **connect track** コマンドを使用して設定され、同じトラック オブジェクトを参照します。
  - オブジェクトがアップしているときにプライマリ トンネルがステータスを追跡する場合、セカンダリ トンネルはオブジェクトがダウンしているときにオブジェクトのステータスを追跡します。
- 1 つのトンネルが FlexVPN トンネルの場合：
  - 残りのトンネルは、セキュアな接続上に存在します。
  - プライマリ接続は FlexVPN ではなく、バックアップ接続が FlexVPN です。
  - クライアント プロファイルは、オブジェクトを指定した **connect track** コマンドを使用して設定され、プライマリ発信インターフェイスを介してプライマリ ピアに到達する能力をトレースします。

バックアップ グループ

バックアップ グループ機能によって、FlexVPN クライアントは、グループに属する FlexVPN クライアントが同じピアとのセッションを確立しているときにピアを省略することができま

す。グループに属している FlexVPN クライアントがピアとの接続を開始すると、FlexVPN クライアントは同じグループ内の別の FlexVPN クライアントが同じピアとのセッションを確立しているかどうかを確認します。接続が存在する場合、FlexVPN クライアントはこのピアを省いて、順番に次のピアを確認します。バックアップ グループを設定するには、*group-number* 引数を指定して **backup group** コマンドを使用します。

デュアル FlexVPN のサポート

デュアル FlexVPN サポート機能によって、同じ内部および外部インターフェイスを共有する 2 つの FlexVPN トンネルを設定することができます。2 つの FlexVPN トンネルは、ルート インジェクションを使用し、対応するトンネルインターフェイスを介して適切なトラフィックを送信します。トンネルがアップしているとき、トンネルはサーバからネットワーク リストを「学習」します。サーバがネットワーク リストを転送すると、FlexVPN は特定のルートをそのルーティング テーブル内の宛先ネットワークにインストールし、トンネル インターフェイスからこれらのネットワークにトラフィックを送信します。

（注） トンネル インターフェイスを介してデフォルト ルートと確立できる FlexVPN 接続は、1 つのみです。

スプリット DNS のサポート

スプリット DNS 機能では、FlexVPN クライアントはドメイン ネーム システム（DNS）プロキシとして動作できます。FlexVPN ネゴシエーションの間、DNS リストはモード設定中にダウンロードされます。このリストは、FlexVPN プロファイルと関連付けられた内部インターフェイスで、DNS ビュー リストとして設定されます。ビュー リストは、ドメイン名に基づいて要求と DNS クエリを照合し、一致した要求を DNS サーバに転送するために使用されます。他の DNS クエリは、デフォルト ビュー（グローバル DNS 設定）を照合するために使用され、ISP DNS に転送されます。

FlexVPN クライアント プロファイル内に 内部インターフェイスについての記載がない場合、DNS ビューはすべてのインターフェイスに適用されますが、設定されたすべてのプロファイルのトンネル インターフェイスとトンネル ソース インターフェイスを除きます。DNS クエリ要求が内部インターフェイスに受信されると、一致する DNS ビューが取得され、要求は DNS IP アドレスに転送されます。

NAT

FlexVPN のネットワーク アドレス変換（NAT）機能では、トラフィックがルーティングされるインターフェイスに基づいて、トラフィックを IP アドレスに変換できます。パケットが、**ip nat inside** コマンドで設定された 1 つのインターフェイスで受信され、**ip nat outside** コマンドで設定された別のインターフェイスに送信される場合、そのパケットは 2 番目のインターフェイスで設定された IP アドレスに変換されます。

サーバのネットワーク リスト

企業トラフィックのルートは、トンネルインターフェイスを使用して、クライアントによってダイナミックインストールされます。このトラフィックは、発信する物理インターフェイス経由でデフォルトのルートをたどります。企業トラフィックはトンネルIPアドレスに変換され、インターネット トラフィックは外部の発信インターフェイス IP アドレスに変換されます。

サーバからのデフォルト ルート リスト

デフォルト ルートは、トンネル インターフェイスを介してシーケンス番号がより高いデバイスで設定する必要があります。トンネル インターフェイスは **ip nat outside** コマンドで設定されます。また、トンネルインターフェイスのIPアドレスは、クライアントが送信したIPアドレスによって割り当てられます。内部インターフェイスからの企業トラフィックは、送信アドレスに変換されます。NAT は、ルート マップを使用して NAT ルールを設定することによって実現されます。ルートマップでは、発信インターフェイスに基づいてルールが定義されます。グローバルに設定された NAT ルールは、ルーティングに基づいて適用されます。

トンネル インターフェイスから送信された IPv4 トラフィックは、IPv4 送信アドレスに変換されます。

（注） NAT が不要な場合、トンネル インターフェイスに関連付けられた NAT ルールを設定する必要はありません。

FlexVPN クライアントのネットワーク リストの学習方法

FlexVPN クライアントは、次のいずれかの方法でピアの背後にあるネットワークのリストを学習します。

- モード設定プッシュ：FlexVPN サーバは、ネットワーク属性のリストをコンフィギュレーション モードのパラメータとしてクライアントに送信します。FlexVPN クライアントは、メトリックが最も高いトンネルインターフェイスを介してこれらのネットワークにルートをインストールします。クライアントは、サーバが仮想アクセスインターフェイスを介してそれらのルートを追加できるように、モード設定セットまたは確認応答（SET/ACK）の交換でサーバにそのネットワークを伝達します。
- ルーティング プロトコルの実行：FlexVPN クライアントおよびサーバはトンネルインターフェイスを介してルーティング プロトコルを実行し、ネットワーク ルートを確立します。これによって、クライアントおよびサーバは、既存のセッションを切断せずに柔軟にネットワークを追加または削除できます。トンネルアドレスは、ピアとのルートを確立するためにモード設定時に伝達されます。

WINS NBNS およびドメイン名

モード設定中、FlexVPN サーバはドメイン名、Windows Internet Naming Service（WINS）、またはNetBIOS ネーム サーバ（NBNS）属性をプッシュします。これらの属性は、FlexVPN クライアントで実行されている DHCP サーバに、動的に更新されます。

イベント トレース

イベント トレース機能は、デバッグのために使用されます。FlexVPN クライアントに通知されたイベントは記録され、その情報はデバッグに使用されます。イベント トレースは、バッファ領域に数バイトのトレース情報を記録する高速メカニズムと、デバッグ データを抽出および復号する表示メカニズムを組み合わせたものです。FlexVPN クライアントは、バッファを保持して、通常の動作時に有効にすることができます。

ローカル認証方式としての Extensible Authentication Protocol

FlexVPN クライアントは、ローカル認証方式として EAP をサポートします。サポートされる EAP 認証方式は、Microsoft Challenge Handshake Authentication Protocol Version 2（MSCHAPv2）、メッセージ ダイジェスト アルゴリズム 5（MD5）、および Generic Token Card（GTC：汎用トークン カード）です。EAP 認証プロセスは、次のとおりです。

- EAP を使用して FlexVPN クライアントを認証するには、IKEv2 プロファイル コンフィギュレーション モードで **authentication local eap** コマンドを使用します。
- FlexVPN クライアントがピアから IKE_AUTH 応答を受信した後、**crypto eap credentials** コマンドを入力します。
- EAP ID 要求を IKE_AUTH 応答で受信した場合、EAP ユーザ名とパスワードを指定する必要があります。
- EAP ID 要求を IKE_AUTH 応答で受信していない場合、ローカル IKEv2 ID をユーザ名として使用するため、パスワードのみを指定します。

（注） ローカル認証方式としての EAP は FlexVPN クライアントと一緒に使用する必要がありますが、IKEv2 発信側では EAP を使用することもできます。EAP サーバがサポートされていない認証方式を最初に指定すると、FlexVPN EAP 発信側は EAP 否定応答（NAK）パケットで応答し、希望の認証方式として EAP-MSCHAPv2、EAP-MD5、または EAP-GTC を要求します。FlexVPN EAP 応答側で、いずれかの認証方式を選択します。

FlexVPN クライアントの設定方法

IKEv2 VPN クライアント プロファイルの設定

このタスクでは、FlexVPN クライアントの設定に必要な IKEv2 コマンドと基本の IKEv2 コマンドについて説明します。基本の IKEv2 プロファイルの設定については、『*Configuring Internet Key Exchange Version 2 (IKEv2)*』モジュールの「Configuring Basic Internet Key Exchange Version 2 CLI Constructs」タスクを参照してください。

（注） IKEv2プロファイルの認証リストに入力ミスがある場合は、自動的にデフォルトのリストに戻ります。

FlexVPNサーバのIKEv2プロファイル設定については、「FlexVPNクライアントの設定方法」の項を参照してください。

トンネル インターフェイスの設定

このタスクを実行して、FlexVPN クライアントが参照するトンネル インターフェイスを設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface tunnel** *number*
4. **ip address** {*ipv4-address* | **negotiated**}
5. **tunnel mode gre ip**
6. **tunnel mode ipsec ipv4**
7. **tunnel source** {*ip-address* | *interface* | **dynamic**}
8. **tunnel destination dynamic**
9. **tunnel protection ipsec-profile** *profile-name*
10. **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	**interface tunnel** *number* 例： `Device(config)# interface tunnel 1`	トンネルインターフェイスを作成します。続いて、インターフェイス 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	**ip address** {*ipv4-address*	**negotiated**} 例： `Device(config-if)# ip address negotiated`	（オプション）IPv4 アドレスをトンネル インターフェイスに割り当てます。

	コマンドまたはアクション	目的
ステップ 5	**tunnel mode gre ip** 例： `Device(config-if)# tunnel mode gre ip`	（オプション）トンネル インターフェイスの Generic Route Encapsulation（GRE）モードを有効にします。
ステップ 6	**tunnel mode ipsec ipv4** 例： `Device(config-if)# tunnel mode ipsec ipv4`	（オプション）IPSec カプセル化を有効にします。
ステップ 7	**tunnel source** {*ip-address* | *interface* | **dynamic**} 例： `Device(config-if)# tunnel source 10.0.0.1`	トンネルインターフェイスの送信元を指定します。
ステップ 8	**tunnel destination dynamic** 例： `Device(config-if)# tunnel destination dynamic`	トンネル インターフェイスの宛先を指定します。
ステップ 9	**tunnel protection ipsec-profile** *profile-name* 例： `Device(config-if)# tunnel protection ipsec-profile ipsecprofile1`	トンネルインターフェイスを IPsec プロファイルに関連付けます。
ステップ 10	**end** 例： `Device(config-if)# end`	インターフェイス 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。

FlexVPN クライアントの設定

monitor event-trace flexvpn コマンドを使用して、イベント トレースを有効にします。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ikev2 client flexvpn** *client-name*
4. **peer** *sequence* {*ipv4-address* | *ipv6-address* | **fqdn** *fqdn-name* [**dynamic** | **ipv6**]} [**track** *track-number* [**up** | **down**]]
5. **connect** {**manual** | **auto** | **track** *track-number* [**up** | **down**]}
6. **client inside** *interface-type interface-number*
7. **client connect tunnel** *interface-number*
8. **source** *sequence-number interface-type interface-number* **track** *track-number*
9. **peer reactivate**
10. **backup group** {*group-number* | **default**}
11. **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 client flexvpn** *client-name* 例： `Device(config)# crypto ikev2 client flexvpn client1`	IKEv2 FlexVPN クライアント プロファイルを定義し、IKEv2 FlexVPN クライアント 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	**peer** *sequence* {*ipv4-address* | *ipv6-address* | **fqdn** *fqdn-name* [**dynamic** | **ipv6**]} [**track** *track-number* [**up** | **down**]] 例： `Device(config-ikev2-flexvpn)# peer 1 10.0.0.1`	IP アドレスまたはホスト名を使用して、静的ピアを定義します。
ステップ 5	**connect** {**manual** | **auto** | **track** *track-number* [**up** | **down**]} 例： `Device(config-ikev2-flexvpn)# connect track 10 up`	FlexVPN トンネルを接続します。 （注） このコマンドに変更を加えると、アクティブなセッションが終了します。
ステップ 6	**client inside** *interface-type interface-number* 例： `Device(config-ikev2-flexvpn)# client inside GigabitEthernet 0/1`	（オプション）内部インターフェイスを指定します。 • FlexVPN クライアント プロファイルには、複数の内部インターフェイスを指定できます。内部インターフェイスは、FlexVPN クライアント プロファイル全体で共有できます。 （注） このコマンドに変更を加えると、アクティブなセッションが終了します。
ステップ 7	**client connect tunnel** *interface-number* 例： `Device(config-ikev2-flexvpn)# client connect tunnel 1`	「トンネル インターフェイスの設定」タスクで作成したトンネル インターフェイスを、FlexVPN クライアントに割り当てます。 • FlexVPNクライアントプロファイルに対して、設定できるトンネル インターフェイスは 1 つのみです。

	コマンドまたはアクション	目的
		（注） このコマンドに変更を加えると、アクティブなセッションが終了します。
ステップ 8	**source** *sequence-number interface-type interface-number* **track** *track-number* 例： `Device(config-ikev2-flexvpn)# source 1 GigabitEthernet 0/1 track 11`	トンネルの送信元アドレスにシーケンス番号を追加します。 • トンネルの送信元アドレスには、トラック オブジェクト番号がアップ状態の最小シーケンス番号があります。 （注） このコマンドに変更を加えると、アクティブなセッションが終了します。
ステップ 9	**peer reactivate** 例： `Device(config-ikev2-flexvpn)# peer reactivate`	プライマリ ピア機能の再アクティベートを有効にします。
ステップ 10	**backup group** {*group-number* | **default**} 例： `Device(config-ikev2-flexvpn)# backup group default`	バックアップ グループにクライアントを割り当てます。 • デフォルトでは、すべてのクライアントがバックアップ グループ 0 に属しています。 （注） このコマンドに変更を加えると、アクティブなセッションが終了します。
ステップ 11	**end** 例： `Device(config-ikev2-flexvpn)# end`	IKEv2 FlexVPN クライアント 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。

ローカル認証方式としての EAP の設定

このタスクを実行して、FlexVPN クライアントのローカル認証方式として Extensible Authentication Protocol（EAP：拡張可能認証プロトコル）を設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ikev2 profile** *profile-name*
4. **authentication local eap**
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	**authentication local eap** 例： `Device(config-ikev2-profile)# authentication local eap`	ローカル認証方式として EAP を指定します。 （注） このコマンドは、IKEv2 の発信側でのみサポートされます。
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。

FlexVPN クライアントの構成例

例：IKEv2 FlexVPN クライアント プロファイルの設定

次の例は、IKEv2 FlexVPN クライアント プロファイルを設定する方法を示します。

```
crypto ikev2 client flexvpn flex
  peer 1 10.0.0.1
  connect manual
  client connect Tunnel0
!
crypto ikev2 authorization policy flex
 subnet-acl 199
 route set interface
 route accept any
!
crypto ikev2 keyring key
 peer dvti
  address 0.0.0.0 0.0.0.0
  pre-shared-key cisco
 !
crypto ikev2 profile prof
 match identity remote address 10.0.0.1 255.0.0.0
 authentication local pre-share
```

```
 authentication remote pre-share
 keyring key
 aaa authorization group psk list local-group-author-list flex
 config-mode set
!
crypto ipsec transform-set trans esp-aes
!
crypto ipsec profile ipsecprof
 set transform-set trans
 set pfs group2
 set ikev2-profile prof
!
interface Tunnel0
 ip address negotiated
 tunnel source Ethernet0/0
 tunnel destination dynamic
 tunnel mode ipsec ipv4
 tunnel protection ipsec-profile ipsecprof
!
interface Ethernet0/0
 ip address 172.16.0.1 255.240.0.0
 ip virtual-reassembly in
!
 ip route 0.0.0.0 0.0.0.0 2.2.2.2
access-list 199 permit ip 10.20.20.20 0.0.0.255 any
access-list 199 permit ip 10.30.30.30 0.0.0.255 any
```

例：ローカル認証方式としての EAP の設定

次の例は、EAP をローカル認証方式として設定する方法を示します。

```
crypto ikev2 profile profile1
 authentication remote rsa-sig
 authentication local eap
```

セッションが起動すると、次のように、EAP の認証情報を入力するプロンプトが表示されます。

```
Enter the command "crypto eap credentials profile1"
Device# crypto eap credentials profile1

Enter the Username for profile profile1: cisco
Enter the password for username cisco
```

FlexVPN クライアント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』、すべてのリリース

関連項目	マニュアル タイトル
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』
IPsec の設定	『*Configuring Security for VPNs with IPsec*』
推奨される暗号化アルゴリズム	『Next Generation Encryption』

シスコのテクニカル サポート

説明	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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

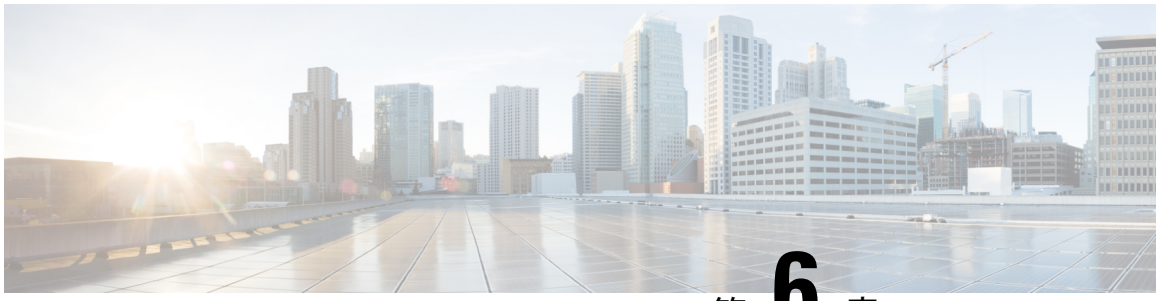
FlexVPN クライアントの設定の機能情報

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: FlexVPN* クライアントの設定の機能情報

機能名	リリース	機能情報
IKEv2 リモート アクセス ハードウェア クライアント		IKEv2 リモート アクセス ハードウェア クライアント機能は、モビリティ、NAT トラバーサル、およびサービス妨害（DoS）攻撃からの復元など、さまざまなソリューションのサポートに必要な、リモート アクセス接続と拡張機能をサポートします。 次のコマンドが導入または変更されました。 **backup group, client connect tunnel, client inside, connect, crypto ikev2 client flexvpn, interface, ip address, peer, peer reactivate, source tunnel destination, tunnel mode, tunnel protection, tunnel source.**
IPsec VPN の IPv6 リモート アクセス		IPsec VPN の IPv6 リモート アクセス機能は、IPv6 サポートと、IKEv2 FlexVPN クライアントのローカル認証方式としての EAP をサポートします。 次のコマンドが変更されました。 **authentication (IKEv2 profile), peer.**



第 6 章

IKEv2 ロード バランサの設定

IKEv2 ロードバランサ機能は、FlexVPN ゲートウェイのクラスタを有効にするためのサポートを提供し、FlexVPN ゲートウェイ間で受信インターネット キー エクスチェンジ バージョン 2（IKEv2）の接続要求を配信します。この機能は、システムおよび暗号の負荷率に基づいて最も負荷の小さい FlexVPN ゲートウェイに受信 FlexVPN または AnyConnect クライアントの要求をリダイレクトします。

- 機能情報の確認 （93 ページ）
- IKEv2 ロード バランサの前提条件 （93 ページ）
- IKEv2 ロード バランサに関する情報 （94 ページ）
- IKEv2 ロード バランサの設定方法 （99 ページ）
- IKEv2 ロード バランサの設定例 （104 ページ）
- その他の参考資料 （105 ページ）
- IKEv2 ロード バランサの機能情報 （107 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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。

IKEv2 ロード バランサの前提条件

- サーバ側の設定として、Hot Standby Router Protocol（HSRP）および FlexVPN サーバ（IKEv2 プロファイル）が設定されていること。

- クライアント側の設定として、FlexVPN クライアントが設定されていること。

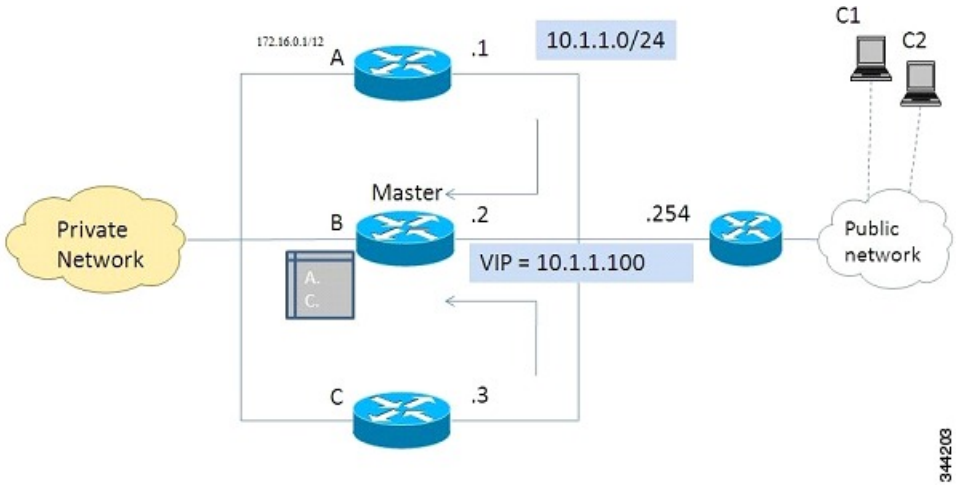
IKEv2 ロード バランサに関する情報

IKEv2 ロード バランサの概要

IKEv2 ロード バランサ サポート機能は、リモート アクセス クライアントからの要求を、Hot Standby Router Protocol（HSRP）グループまたはクラスタ内の最低負荷ゲートウェイ（LLG）にリダイレクトすることで、クラスタロードバランシング（CLB）ソリューションを提供します。HSRP クラスタは、LAN またはエンタープライズ ネットワーク内のゲートウェイまたは FlexVPN サーバのグループです。CLB ソリューションは、要求の HSRP クラスタ内 LLG へのリダイレクトにより、RFC 5685 で定義されたインターネット キー エクスチェンジ バージョン 2（IKEv2）リダイレクト メカニズムと連携します。

次の図は、IKEv2 クラスタのロード バランシング ソリューションの仕組みを示します。

図 *4 : IKEv2* クラスタのロード バランシング ソリューション



1. アクティブ HSRP ゲートウェイは、HSRP グループの「マスター」として選択され、グループの仮想 IP アドレス（VIP）の所有権を取得します。マスターはクラスタ内にゲートウェイのリストを保持して、各ゲートウェイの負荷を追跡し、FlexVPN クライアントの要求を LLG にリダイレクトします。
2. 残りのゲートウェイは「スレーブ」と呼ばれ、負荷の更新をマスターに定期的な感覚で送信します。
3. IKEv2 クライアントが HSRP VIP に接続すると、要求はまずマスターに到達し、クラスタ内の LLG に順番にリダイレクトされます。

CLB ソリューションのコンポーネントは次のとおりです。

- HSRP

- CLB マスター
- CLB スレーブ
- CLB 通信
- IKEv2 リダイレクト メカニズム

Hot Standby Router Protocol

Hot Standby Router Protocol（HSRP）は、HSRP マスターまたはアクティブ ルータ（AR）を選択するために使用されます。専用デバイスを選択する HSRP では、グループ内の 1 つのデバイスに VIP を設定する必要があります。このアドレスは、グループ内の他デバイスによって学習されます。マスターに割り当てられた IP アドレスは、グループの VIP として使用されます。HSRP アクティブ ルータ（CLB マスターとも呼ばれる）は IKEv2 要求を受信し、クラスタの LLG にこれらの要求をリダイレクトします。リダイレクトが IKEv2 プロトコル レベルで実行されると、以下を実行できるようになります。

- FlexVPN クライアントからのすべての要求は、VIP が FlexVPN クライアントで設定されると、HSRP マスターで受信される。FlexVPN クライアントが知る必要があるのは HSRP クラスタの VIP のみであるため、FlexVPN クライアントの設定は最小化される。
- CLB マスターは HSRP マスターと同じゲートウェイで実行されるため、すべての CLB スレーブの負荷情報が維持される。CLB マスターでは、要求の効率的なリダイレクトが可能なため、複数のリダイレクトやループを防ぐことができる。

CLB マスター

CLB マスターは、HSRP マスターまたはアクティブ ルータ（AR）で動作します。マスターは CLB スレーブから更新を受信し、その負荷条件に基づいてそれらをソートし、負荷が最小のゲートウェイ（LLG）を計算します。マスターは、LLG の IP アドレスを IKEv2（FlexVPN サーバ上）に送信します。IP アドレスは、LLG との IKEv2 セッションを開始した発信側（FlexVPN クライアント）に送信されます。マスターは受信する IKEv2 クライアント接続を LLG にリダイレクトします。詳細については、「IKEv2 リダイレクト メカニズム （96 ページ）」のセクションを参照してください。

（注） 「CLB ノード」は、CLB マスターと CLB スレーブを指定する必要がある場所で使用します。

CLB スレーブ

CLB スレーブは、アクティブ ルータ（AR）上を除いた、HSRP グループ内のすべてのデバイスで動作します。スレーブは、サーバに負荷更新を定期的に送信します。CLB スレーブは、CLB マスターに情報を提供する、フル機能の IKEv2 ゲートウェイです。更新以外にも、CLB スレーブは活動管理のメッセージを CLB マスターに送信します。

CLB 負荷管理メカニズム

CLB 負荷管理メカニズムは、CLB マスターと CLB スレーブ間で動作する、TCP ベースのプロトコルです。CLB 負荷管理メカニズムは、CLB マスターに CLB スレーブの負荷について情報を提供します。この情報に基づいて、CLB マスターは、新しく受信する各 IKEv2 接続のセッションを処理する LLG を選択します。

IKEv2 ロード バランサの利点

- IKEv2 ロード バランサ サポート機能は、設定が簡単でコスト効率に優れています。
- FlexVPN クライアントは、クラスタ内のすべてのゲートウェイの IP アドレスを知る必要はありません。クライアントが知っておく必要があるのは、クラスタの仮想 IP アドレスのみです。
- すべての暗号化セッションは、クラスタ内のノードにリダイレクトされます。

IKEv2 リダイレクト メカニズム

IKEv2 リダイレクト メカニズムによって、VPN ゲートウェイは負荷条件およびメンテナンス要件に基づいて FlexVPN クライアント要求を別の VPN ゲートウェイにリダイレクトできます。

IKEv2 リダイレクト メカニズムは、セキュリティ アソシエーション（SA）の初期化（IKE_SA_INIT）と SA 認証（IKE_AUTH）で実行されます。

IKEv2 初期交換中のリダイレクト（SA 初期化）

FlexVPN クライアントまたは AnyConnect クライアントは、最初の IKE_SA_INIT 要求に REDIRECT_SUPPORTED 通知メッセージを含めることで、インターネット キー エクスチェンジ バージョン 2（IKEv2）リダイレクト メカニズムのサポートを示します。**crypto ikev2 redirect client** コマンドを使用して、クライアントのリダイレクト メカニズムを有効にします。**crypto ikev2 redirect gateway init** コマンドを使用して、ゲートウェイの IKE_SA_INIT でのリダイレクトを有効にします。

IKEv2 要求を別の新しいゲートウェイにリダイレクトするには、IKE_SA_INIT 要求を受信するゲートウェイが、暗号ロードバランサ（CLB）モジュールのサポートによって、新しいゲートウェイ（この場合は LLG）の IP アドレスまたは完全修飾ドメイン名（FQDN）を選択します。このゲートウェイは、REDIRECT 通知メッセージを含む IKE_SA_INIT 応答で応答します。通知には、IKE_SA_INIT 要求内のペイロードからの新しいゲートウェイやナンス値などの情報が含まれます。IKE_SA_INIT 応答を受信したクライアントは、IKE_SA_INIT 要求で送信されたナンス値とリダイレクト通知で指定されたゲートウェイ情報を検証し、リダイレクト通知が設定のとおりかどうかを確認します。

（注） ナンス値が一致しない場合、クライアントはその応答を破棄して別の応答を待って、発信側のサービス妨害（DoS）攻撃を防ぎます。IKE_SA_INIT応答内に攻撃者が不正なリダイレクトペイロードが挿入すると、DoS 攻撃が発生する場合があります。

新しいゲートウェイとの IKE_SA_INIT 交換では、クライアント メッセージに REDIRECTED_FROM通知ペイロードが含まれます。REDIRECTED_FROM通知ペイロードは、クライアントにリダイレクトされる送信元 VPN ゲートウェイの IP アドレスで構成されています。IKEv2 交換は、送信元ゲートウェイでの処理と同じように処理されます。

（注） 新しいゲートウェイもクライアントの目的を果たせない場合、クライアントは新しいゲートウェイによって再度リダイレクトされることがあります。クライアントでは、リダイレクト後の新しいゲートウェイとの IKE_SA_INIT 交換に、REDIRECT_SUPPORTED ペイロードは再度含まれません。新しいゲートウェイとの IKE_SA_INIT 交換内に REDIRECTED_FROM 通知ペイロードが存在することは、クライアントが IKEv2 リダイレクト メカニズムをサポートすることを、新しいゲートウェイに示します。

IKE_AUTH 交換中のリダイレクト（SA 認証）

詳細なセキュリティ分析によって、IKE_AUTH 中のリダイレクトは IKE_INIT 中のリダイレクトと比較してより安全でも危険でもないことが示されました。ただし、パフォーマンスと拡張性の理由により、シスコは IKE_INIT 中のリダイレクトを推奨します。**crypto ikev2 redirect gateway auth** コマンドを使用して、ゲートウェイのリダイレクトメカニズムを有効にします。**redirect gateway auth** コマンドを使用して、選択した IKEv2 プロファイル認証時のリダイレクトを有効にします。

この方法では、クライアント認証ペイロードは、リダイレクト通知ペイロードを送信する前に検証されます。また、クライアントでも、リダイレクト通知に従って動作する前に、ゲートウェイ認証ペイロードが検証されます。任所ペイロードが交換され、正常に検証されると、IKEv2 セキュリティ アソシエーション（SA）が正常に検証され、要求のリダイレクトを決定する INITIAL_CONTACT が処理されます。リダイレクトが有効な場合、ゲートウェイでは IKE SA が作成され、リダイレクト通知で IKE_AUTH 応答が送信されます。

この方法では、子 SA は作成されません。IKE_AUTH には、子 SA に関連するペイロードは含まれません。IKE_AUTH応答を受信すると、クライアントは、ゲートウェイ認証ペイロードを検証し、削除通知を送信してそのゲートウェイがある IKEv2 SA を削除します。クライアントは、リダイレクト通知ペイロードに従って動作し、新しいゲートウェイとの接続を確立します。クライアントは、削除通知の確認応答を待たずに、新しいゲートウェイとの接続を確立します。IKE_AUTH 交換で Extensible Authentication Protocol（EAP：拡張可能認証プロトコル）認証が呼び出される場合、ゲートウェイでは、リダイレクトペイロードの送信を最初と最後の IKE_AUTH応答のどちらで送信するかを選択します。リダイレクトごとに認証情報を指定する必要がないため、EAP 認証は最初の IKE_AUTH 応答に含まれます。

互換性および相互運用性

IKEv2 リダイレクト メカニズムは、RFC 5685 に基づいています。ゲートウェイ（IKEv2 応答側）は、標準を実装するクライアント（IKEv2 発信側）と互換性があります。同様に、クライアント（発信者）の実装では、標準を実装しているサードパーティ製サーバ（応答側）との互換性が必要です。負荷管理メカニズムはCisco独自のもので、Cisco IOSデバイスでのみサポートされます。

リダイレクト ループ処理

クライアント要求は、正しくない設定またはサービス妨害（DoS）攻撃を理由として、順番に複数回リダイレクトできます。場合によっては、クライアントを他のゲートウェイにリダイレクトする複数のゲートウェイによってクライアントがループに入り、その結果クライアントへのサービスが拒否されることがあります。これを防ぐには、**max-redirects** *number* キーワード/引数ペアを指定して **crypto ikev2 redirect client** コマンドを使用し、特定の IKEv2 セキュリティ アソシエーション（SA）設定について特定数を超えるリダイレクトを受け入れないようにクライアントを設定します。

IKEv2 クラスタの再接続

IKEv2 クラスタの再接続機能によって、Cisco AnyConnect クライアントはクラスタ内のサーバに再接続できます。**crypto ikev2 reconnect key** は、クライアントにプッシュされた不明瞭なデータを暗号化するためにサーバに導入されています。障害を検出すると、クライアントは、認証クレデンシャルの入力を再度要求せずに新規または既存のサーバと再接続します。

キー インデックス値は 2 つのみ（1 および 2）です。いずれかの時点で、これを使用して設定されたキーの 1 つがアクティブになります。IOS サーバで再接続キーの CLI を使用して再接続キーが設定されている場合、Cisco IOS サーバは再接続データを復号できます。これは、キーがバックアップ キーのみの場合にも当てはまります。

この機能は、**authentication** コマンドで IKEv2 プロファイルの認証方式として **anyconnect-eap** キーワードを指定した場合にはサポートされません。

（注） この機能は、Cisco AnyConnect サーバとして動作するように設定された Cisco IOS デバイスで使用できます。この機能をサポートする AnyConnect クライアント ソフトウェア バージョンは、4.2 以降のリリースです。この機能は、新規導入にのみ適用できます。Cisco IOS サーバでこの機能が有効になると、以前のリリースのCisco AnyConnectクライアントはサポートされなくなります。

IKEv2 ロード バランサの設定方法

サーバ クラスタの設定

ロード バランシングに対する HSRP グループの設定

このタスクを実行して、単一の Hot Standby Router Protocol（HSRP）グループをクラスタ用に設定します。

Hot Standby Router Protocol（HSRP）は、HSRP マスターまたはアクティブ ルータ（AR）を選択するために使用されます。専用デバイスを選択する HSRP では、グループ内の 1 つのデバイスに VIP を設定する必要があります。このアドレスは、グループ内の他デバイスによって学習されます。マスターに割り当てられた IP アドレスは、グループの VIP として使用されます。HSRP アクティブ ルータ（CLB マスターとも呼ばれる）は IKEv2 要求を受信し、クラスタの LLG にこれらの要求をリダイレクトします。リダイレクトが IKEv2 プロトコル レベルで実行されると、以下を実行できるようになります。

- FlexVPN クライアントからのすべての要求は、VIP が FlexVPN クライアントで設定されると、HSRP マスターで受信される。FlexVPN クライアントが知る必要があるのは HSRP クラスタの VIP のみであるため、FlexVPN クライアントの設定は最小化される。
- CLB マスターは HSRP マスターと同じゲートウェイで実行されるため、すべての CLB スレーブの負荷情報が維持される。CLB マスターでは、要求の効率的なリダイレクトが可能なため、複数のリダイレクトやループを防ぐことができる。

（注） このタスクでは、ロードバランシングのため、HSRP グループの設定に必要な最小限のコマンドを説明します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask* [**secondary**]
5. **standby** [*group-number*] **priority** *priority*
6. **standby** *group-name*
7. **exit**
8. 手順 3 ～ 7 を繰り返して、別のクラスタに HSRP グループを設定します。

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	**interface** *type number* 例： `Device(config)# interface GigabitEthernet 0/0/0`	インターフェイス タイプを設定し、インターフェイス 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	**ip address** *ip-address mask* [**secondary**] 例： `Device(config-if)# ip address 10.0.0.1 255.255.255.0`	インターフェイスのプライマリ IP アドレスまたはセカンダリ IP アドレスを指定します。
ステップ 5	**standby** [*group-number*] **priority** *priority* 例： `Device(config-if)# standby 1 priority 110`	HSRP 優先度を設定します。
ステップ 6	**standby** *group-name* 例： `Device(config-if)# standby group1`	HSRP スタンバイ グループの名前を指定します。
ステップ 7	**exit** 例： `Device(config-if)# 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。
ステップ 8	手順 3 ～ 7 を繰り返して、別のクラスタに HSRP グループを設定します。	—

負荷管理メカニズムの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ikev2 cluster**
4. **holdtime** *milliseconds*
5. **master** { **overload-limit** *percent* | **weight** { **crypto-load** *weight-number* | **system-load** *weight-number*}}

6. **port** *port-number*
7. **slave** { **hello** *milliseconds* | **max-session** *number* | **priority** *number* | **update** *milliseconds*}
8. **standby-group** *group-name*
9. **shutdown**
10. **exit**
11. **crypto ikev2 reconnect key** *key index* **active** *name*
12. **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 cluster** 例： `Device(config)# crypto ikev2 cluster`	IKEv2 クラスタ ポリシーを定義し、IKEv2 クラスタ 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	**holdtime** *milliseconds* 例： `Device(config-ikev2-cluster)# holdtime 10000`	（オプション）ピアからのメッセージを受信する時間をミリ秒単位で指定します。 • 設定された時間内にメッセージを受信しない場合、ピアは「死んでいる」と宣言されます。
ステップ 5	**master** { **overload-limit** *percent* | **weight** { **crypto-load** *weight-number* | **system-load** *weight-number*}} 例： `Device(config-ikev2-cluster)# master weight crypto-load 10`	HSRP クラスタのマスターの設定を指定します。 • **overload-limit** *percent*：クラスタのしきい値負荷。デバイスがビジーなことを判断し、要求へのリダイレクトを無視するための負荷制限。 • **weight**：負荷属性の重みを指定します。範囲：0 ～ 100。デフォルトは 100 です。 • **crypto-load** *weight-number*：IKE と IPSec のセキュリティ アソシエーション（SA）の負荷。 • **system-load** *weight-number*：システムとメモリの負荷。
ステップ 6	**port** *port-number* 例： `Device(config-ikev2-cluster)# port 2000`	（オプション）クラスタ マスターのリッスン ポートを指定します。

	コマンドまたはアクション	目的
ステップ 7	**slave** { **hello** *milliseconds* | **max-session** *number* | **priority** *number* | **update** *milliseconds*} 例： `Device(config-ikev2-cluster)# slave max-session 90`	HSRP グループのスレーブ ゲートウェイ設定を指定します。 • **hello** *milliseconds*：ミリ秒単位のスレーブ ゲートウェイの Hello インターバル。 • **max-session** *number*：スレーブ上で許可される SA の最大数。このキーワードは必須であり、スキップできません。 • **priority** *number*：スレーブの優先度。 • **update** *milliseconds*：スレーブ ゲートウェイ用の更新メッセージ間の、ミリ秒単位のインターバル。
ステップ 8	**standby-group** *group-name* 例： `Device(config-ikev2-cluster)# standby-group group1`	スレーブが含まれている HSRP グループを定義します。 • *group-name*：グループ名は *group-name* 引数から派生します。これは、**standby name** コマンドで指定されます。
ステップ 9	**shutdown** 例： `Device(config-ikev2-cluster)# shutdown`	（オプション）IKEv2 クラスタ ポリシーを無効にします。
ステップ 10	**exit** 例： `Device(config-ikev2-cluster)# exit`	IKEv2 クラスタ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 11	**crypto ikev2 reconnect key** *key index* **active** *name* 例： `Device(config)# crypto ikev2 reconnect key 1 active test123`	セッション再接続の IKEv2 不透明型データ サポートを有効にします。 （注） IKEv2 クラスタの再接続機能は、**ikev2 reconnect key active** *name key-string* に **active** キーワードが含まれている場合にのみ、暗号化に対して有効になります。クラスタの再接続機能を有効にするには、**active** キーワードは必須です。**active** キーワードを指定せずに **ikev2 reconnect key** *key-name key-string* コマンドを使用すると、ヘッドエンドでは復号化のみが可能になります。

	コマンドまたはアクション	目的
ステップ 12	**end** 例： `Device(config-ikev2-cluster)# end`	IKEv2 クラスタ 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。

サーバでの IKEv2 リダイレクト メカニズムの有効化

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ikev2 redirect gateway init**
4. **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 redirect gateway init** 例： `Device(config)# crypto ikev2 redirect gateway init`	SA 開始中に、ゲートウェイで IKEv2 リダイレクト メカニズムを有効にします。
ステップ 4	**end** 例： `Device(config)# end`	グローバル 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。

クライアントでの IKEv2 リダイレクト メカニズムの有効化

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ikev2 redirect client** [**max-redirects** *number*]
4. **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 redirect client** [**max-redirects** *number*] 例： `Device(config)# crypto ikev2 redirect client max-redirects 15`	FlexVPN クライアントで IKEv2 リダイレクト メカニズムを有効にします。 • **max-redirects** *number*：（オプション）リダイレクト ループ検出に対して、FlexVPN クライアントで設定できるリダイレクトの最大数を指定します。
ステップ 4	**end** 例： `Device(config)# end`	グローバル 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 ロード バランサの設定例

例：ロード バランシングに対する HSRP グループの設定

次の例では、プライオリティ 110 で Hot Standby Router Protocol（HSRP）グループのアクティブ ルータとして設定された RouterA を示します。デフォルトのプライオリティ レベルは 100 です。この HSRP グループには、group1 のグループ名が割り当てられます。グループ名は、クラスタ ポリシーに記載されています。

```
Device(config)# hostname RouterA
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip address 10.0.0.1 255.255.255.0
Device(config-if)# standby 1 priority 110
Device(config-if)# standby group1
Device(config-if)# end
```

例：負荷管理メカニズムの設定

次の例は、IKEv2 で負荷管理メカニズムを設定する方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# crypto ikev2 cluster
Device(config-ikev2-cluster)# holdtime 10000
Device(config-ikev2-cluster)# master crypto-load 10
Device(config-ikev2-cluster)# port 2000
Device(config-ikev2-cluster)# slave priority 90
Device(config-ikev2-cluster)# standby-group group1
Device(config-ikev2-cluster)# shutdown
Device(config-ikev2-cluster)# end
```

例：リダイレクト メカニズムの設定

次の例は、クライアント上およびゲートウェイでの開始中にリダイレクト メカニズムを有効にする方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# crypto ikev2 redirect client
Device(config)# crypto ikev2 redirect gateway init
Device(config)# end
```

例：クラスタ再接続キーの設定

次の例は、サーバで再接続キーを有効にする方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# crypto ikev2 reconnect key 1 active key
Device(config)# crypto ikev2 reconnect key 2 test
Device(config)# end
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Master Command List』、すべてのリリース

関連項目	マニュアル タイトル
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』
HSRP コンフィギュレーション	『*Configuring HSRP*』
HSRP コマンド	『Cisco IOS First Hop Redundancy Protocols Command Reference』

標準および RFC

標準/RFC	タイトル
RFC 5685	*Redirect Mechanism for the Internet Key Exchange Protocol Version 2 (IKEv2)*

シスコのテクニカル サポート

説明	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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

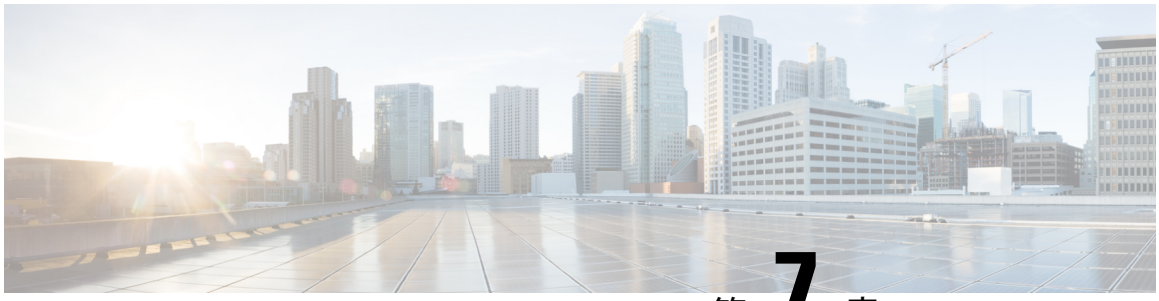
IKEv2 ロード バランサの機能情報

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 *8 : IKEv2* ロード バランサの機能情報

機能名	リリース	機能情報
AnyConnect のクラスタ再接続との IKEv2 高速コンバージェンス		AnyConnect のクラスタ再接続との IKEv2 高速コンバージェンス機能では、Cisco AnyConnect クライアントはクラスタ内の任意のサーバと再接続できます。 次のコマンドが導入または変更されました： **crypto ikev2 reconnect key**
IKEv2 ロード バランサのサポート		IKEv2 ロード バランサ サポート機能は、要求を最低負荷ゲートウェイにリダイレクトすることで、FlexVPN クライアントから受信する IKEv2 要求を、IKEv2 FlexVPN サーバ間またはゲートウェイ間で分散します。 次のコマンドが導入または変更されました。 **crypto ikev2 cluster, crypto ikev2 redirect, holdtime, master (IKEv2), port (IKEv2), redirect gateway, slave (IKEv2), standby-group, show crypto ikev2 cluster, show crypto ikev2 sa.**



第 7 章

IKEv2 フラグメンテーションの設定

RFC 機能に準拠した IKE フラグメンテーションでは、IETF の **draft-ietf-ipsecme-ikev2-fragmentation-10** ドキュメントの提案に従って、インターネット キー エクスチェンジ バージョン 2 （IKEv2）パケットのフラグメンテーションを実装しました。

- 機能情報の確認 （109 ページ）
- IKEv2 フラグメンテーションの設定に関する情報 （109 ページ）
- IKEv2 フラグメンテーションの設定方法 （113 ページ）
- IKEv2 フラグメンテーションの設定例 （114 ページ）
- IKEv2 フラグメンテーションの設定に関する追加情報 （119 ページ）
- IKEv2 フラグメンテーションの機能情報 （120 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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。

IKEv2 フラグメンテーションの設定に関する情報

IKEv2 フラグメンテーション

インターネット キー エクスチェンジ バージョン 2（IKEv2）フラグメンテーション プロトコルは、大きな IKEv2 メッセージを IKE フラグメント メッセージと呼ばれる一連の小さなメッセージに分割します。IKEv2 リモート アクセスのヘッドエンド機能によって Cisco IOS ソフト

ウェアに実装されたIKEv2フラグメンテーション方式は、シスコ独自の方法であり、シスコ以外のピアとの相互運用性は制限されます。フラグメンテーションは、暗号化されたIKEv2パケットでのみ実行されます。そのため、ピアがすべてのフラグメントを受信するまで、ピアはメッセージを復号したり認証することはできません。RFCに準拠したIKEフラグメンテーション機能は、フラグメンテーション後にパケットを暗号化することによってIETF **draft-ietf-ipsecme-ikev2-fragmentation-10** ドキュメントを実装し、シスコ独自のフラグメンテーション方式を引き続きサポートしながらシスコ以外のピアとの相互運用性を実現します。

ピア間のネゴシエーション

RFC 機能に準拠した IKE フラグメンテーションから有効。IETF 標準フラグメンテーション方式のサポートが通知ペイロードとして IKE_SA_INIT メッセージに追加されました。一方、シスコ独自のフラグメンテーション方式は、同じIKE_SA_INITメッセージ内で引き続きベンダーID ペイロードを使用します。フラグメンテーションが有効な場合、両方の方式が **show crypto ikev2 sa detail** コマンドで適切と表示されます。最大伝送ユニット（MTU）はローカルで設定され、メッセージ間のネゴシエーションも交換も行いません。INIT交換の後、いずれかの方式で設定されたネットワーク内のピアは、使用する必要がある認証方式と、AUTHメッセージをフラグメント化できるかどうかをを認識します。

次に、デバッグが有効で、INIT要求メッセージでのネゴシエーション機能を表している場合のデバイスからの出力例を示します。

```
*Oct 14 08:45:24.732: IKEv2:(SESSION ID = 0,SA ID = 1):Next payload: SA, version: 2.0
Exchange type: IKE_SA_INIT, flags: INITIATOR Message id: 0, length: 524
Payload contents:
SA Next payload: KE, reserved: 0x0, length: 144
…
Security protocol id: IKE, spi size: 0, type: NAT_DETECTION_DESTINATION_IP
NOTIFY(IKEV2_FRAGMENTATION_SUPPORTED) Next payload: VID, reserved: 0x0, length: 8
Security protocol id: Unknown - 0, spi size: 0, type: IKEV2_FRAGMENTATION_SUPPORTED
VID Next payload: NONE, reserved: 0x0, length: 20
```

上記の出力では、メッセージ内の IKEV2_FRAGMENTATION_SUPPORTED および VID 値によって、IETF 標準フラグメンテーション方式とシスコ独自のフラグメンテーション方式の両方をサポートすることを示す、発信側から応答側へのメッセージが INIT 要求に含まれます。

次に、デバッグが有効で、INIT応答メッセージでのネゴシエーション機能を表している場合のデバイスからの出力例を示します。

```
*Oct 14 08:45:24.732: IKEv2:(SESSION ID = 0,SA ID = 1):Next payload: SA, version: 2.0
Exchange type: IKE_SA_INIT, flags: INITIATOR Message id: 0, length: 524
Payload contents:
SA Next payload: KE, reserved: 0x0, length: 144
last proposal: 0x0, reserved: 0x0, length: 140
…
NOTIFY(IKEV2_FRAGMENTATION_SUPPORTED) Next payload: VID, reserved: 0x0, length: 8
Security protocol id: Unknown - 0, spi size: 0, type: IKEV2_FRAGMENTATION_SUPPORTED
<-------- Response, supporting both
VID Next payload: NONE, reserved: 0x0, length: 20 <-------- Response, supporting both
```

上記の出力では、メッセージ内の IKEV2_FRAGMENTATION_SUPPORTED および VID 値によって、IETF 標準フラグメンテーション方式とシスコ独自のフラグメンテーション方式の両方をサポートすることを示す、応答側から発信側へのメッセージが応答要求に含まれます。

以前のリリースのフラグメンテーション サポート

シスコ独自のフラグメンテーション方式を使用する以前のリリースのフラグメンテーションサポートを保証するために、IKEv2はIETF標準フラグメンテーション方式のIKEv2通知ペイロード タイプと共にベンダー ID を引き続き使用します。両方のフラグメンテーション方式がサポートされている場合、IKEv2 は IETF 標準フラグメンテーション方式を優先します。

次の表に、ピアの機能に基づいてフラグメンテーションのタイプを特定する方法を示します。CISCO はシスコ独自のフラグメンテーション方式を示し、STD は IETF 標準フラグメンテーション方式を示します。

ピア 1 の機能	ピア 2 の機能	セキュリティ アソシエーションでアクティブなフラグメンテーション タイプ
STD + CISCO	STD + CISCO	STD
STD	STD	STD
CISCO	CISCO	CISCO
CISCO	STD + CISCO	CISCO
STD	STD + CISCO	STD
STD	CISCO	なし
なし	なし、STD + CISCO、または STD または CISCO	なし

フラグメントの暗号化、複合化、および再送信

フラグメンテーションおよび暗号化

パケットは、**crypto ikev2 fragmentation** コマンドで指定された最大伝送ユニット（MTU）値またはデフォルトMTU値のいずれかに基づいてフラグメント化されます。暗号化されたペイロードのみを含む IKE メッセージがフラグメント化されます。アナウンス メッセージ内の新しいペイロードタイプ（暗号化および認証されたフラグメント）は、フラグメントの合計数以上のフラグメント番号を示します。このペイロードは SKF として注釈がつけられ、値は 53 です。

発信パケットを暗号化する前に、パケット長を確認します。確立済みのセキュリティ アソシエーションは、IETF標準フラグメント方式でSAが有効になっているかどうかも確認します。次に、フラグメント化されたパケットの伝送が表示されるデバイスからの出力例を示します。

```
*Oct 16 10:31:22.221: IKEv2:(SESSION ID = 0,SA ID = 3):Next payload: SKF, version: 2.0
Exchange type: INFORMATIONAL, flags: INITIATOR Message id: 1, length: 244
Payload contents:
SKF Next payload: COOP, reserved: 0x90, length: 216
SKF Fragment number: 1 OF Total Fragments: 3
*Oct 16 10:31:22.222: IKEv2:(SESSION ID = 0,SA ID = 3):Next payload: SKF, version: 2.0
Exchange type: INFORMATIONAL, flags: INITIATOR Message id: 1, length: 244
```

```
Payload contents:
SKF Next payload: COOP, reserved: 0x90, length: 216
SKF Fragment number: 2 OF Total Fragments: 3
*Oct 16 10:31:22.222: IKEv2:(SESSION ID = 0,SA ID = 3):Next payload: SKF, version: 2.0
Exchange type: INFORMATIONAL, flags: INITIATOR Message id: 1, length: 244
Payload contents:
SKF Next payload: COOP, reserved: 0x90, length: 216
SKF Fragment number: 3 OF Total Fragments: 3
```

「SKF Next payload: COOP, reserved: 0x90, length: 216」および「SKF Fragment number: 1 OF Total Fragments: 3」は、メッセージが 3 つのフラグメントにフラグメント化された協調キー サーバのアナウンスメント（ANN）パケットであることを示します。

復号と最適化

応答側で受信フラグメントが受信されると、各フラグメントは復号されて一時的に保存されます。復号（元のパックへのフラグメントのアセンブリ）時に、重複するフラグメント、フラグメントの合計数以上のフラグメント番号、およびまったく別のフラグメント番号を持つフラグメントはドロップされます。フラグメントは、受信した順ではなくフラグメント番号の昇順で追加されます。そのため、パケットアセンブリが高速化します。ただし、順序どおりではないフラグメントも許可され、処理されます。各フラグメントは、メッセージに関係するすべてのフラグメントが受信されていることを確認するために検証されます。すべてのフラグメントが受信されると、パケットはフラグメントからアセンブリされ、新しく受信したメッセージとして処理されます。確認応答（ACK）メッセージは、元のパケットがアセンブリされると送信されます。各フラグメントには送信されません。

再送信

IKEv2 再送信は、IKEv2 再送信タイマーから求められた場合に発生します。一度構成され最初に送信されたフラグメントは、リスト化され、再送信タイマーがトリガーされた場合に再送信できるよう準備されます。再送信要求を受信すると、IKEv2 は応答を再送信します。この応答は、最初のフラグメント（#1）再送信が受信されると、再送信されます。残りのフラグメント番号は無視されるため、応答のより短時間での処理が可能になります。

フラグメンテーションの有効化

セキュリティ アソシエーション（SA）ごとにフラグメンテーションをグローバルに有効にするには、**crypto ikev2 fragmentation** コマンドを使用します。両方のピアが各ピアでの INIT 交換の後に IKE_AUTH 交換に使用されるフラグメンテーションのサポートを示している場合、フラグメンテーションは SA で有効になっています。

（注） このコマンドは、IKEv2 リモート アクセス ヘッドエンド機能によって導入され、変更されていません。

mtu *mtu-size* キーワード/引数のペアを使用して、最大伝送ユニット（MTU）をバイト単位で指定できます。MTU サイズは、IP または UDP カプセル化済みの IKEv2 パケットを示します。

MTU の範囲は 68 ～ 1500 バイトです。デフォルトの MTU サイズは、IPv4 パケットでは 576 バイト、IPv6 パケットでは 1280 バイトです。

RFC 機能に準拠した IKE フラグメンテーションで有効な **crypto ikev2 fragmentation** コマンドは、次のように動作します。

- 将来の SA にのみ影響し、既存の古い SA には影響しません。
- シスコ独自のフラグメンテーション方式と IETF 標準のフラグメンテーション方式をサポートします。

show crypto ikev2 sa detail コマンドにより、以下の情報が表示されます。

- ピアで有効なフラグメンテーション方式。有効なフラグメンテーション方式が IETF 標準のフラグメンテーションの場合、出力には使用中の MTU が表示されます。
- フラグメンテーションが両方のピアで有効になっているか、ローカル ピアでのみ有効になっているか。

IPv6 のサポート

RFC 機能に準拠した IKE フラグメンテーションでは、IETF 標準フラグメンテーション方式を使用している場合の、IPv6 IKE エンドポイントでの IPv6 パケットの断片化のサポートを追加しました。デフォルトの MTU 値は 1280 バイトであり、**crypto ikev2 fragmentation** コマンドで MTU が指定されていない場合に使用されます。フラグメンテーションで使用される MTU は、**show crypto ikev2 sa detail** コマンドの出力に表示されます。

IKEv2 フラグメンテーションの設定方法

IKEv2 フラグメンテーションの設定

このタスクを実行して、大規模な IKEv2 パケットのラグメンテーションを有効にします。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ikev2 fragmentation** [**mtu** *mtu-size*]
4. **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：	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）。

	コマンドまたはアクション	目的
	`Device> enable`	
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 fragmentation** [**mtu** *mtu-size*] 例： `Device(config)# crypto ikev2 fragmentation mtu 100`	IKEv2 フラグメンテーションを設定します。 • MTU の範囲は 68 ～ 1500 バイトです。デフォルトの MTU サイズは、IPv4 パケットでは 576 バイト、IPv6 パケットでは 1280 バイトです。 （注） MTU のサイズは、IP または UDP でカプセル化された IKEv2 パケットを示します。
ステップ 4	**end** 例： `Device(config)# end`	グローバル 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 フラグメンテーションの設定例

例：設定された MTU の表示が有効な IETF フラグメンテーション

次は、IETF 標準フラグメンテーション方式が有効であることを示すサンプル出力です。このステートメントは、応答側が IETF 標準フラグメンテーション方式もサポートしている場合に表示されます。また、出力には、使用中の MTU も表示されます。

```
Device# show crypto ikev2 sa detail

IPv4 Crypto IKEv2 SA

Tunnel-id Local Remote fvrf/ivrf Status
1 10.0.8.3/848 10.0.9.4/848 none/none IN-NEG
Encr: Unknown - 0, PRF: Unknown - 0, Hash: None, DH Grp:0, Auth sign: Unknown - 0, Auth
 verify: Unknown - 0
Life/Active Time: 86400/0 sec
CE id: 0, Session-id: 0
Status Description: Initiator waiting for INIT response
Local spi: 2CD1BEADB7C20854 Remote spi: 0000000000000000
Local id: 10.0.8.3
Remote id:
Local req msg id: 0 Remote req msg id: 0
Local next msg id: 1 Remote next msg id: 0
Local req queued: 0 Remote req queued: 0
Local window: 1 Remote window: 1
DPD configured for 0 seconds, retry 0
IETF Std Fragmentation enabled.
IETF Std Fragmentation MTU in use: 272 bytes.
```

```
Extended Authentication not configured.
NAT-T is not detected
Cisco Trust Security SGT is disabled
Initiator of SA : Yes

IPv6 Crypto IKEv2 SA
```

例：発信側で設定される IETF 標準フラグメンテーション方式

次は、発信側で設定されたIETF標準フラグメンテーション方式を表示するサンプル出力です。応答側はシスコ独自のフラグメンテーション方式をサポートしています。

```
Device# show crypto ikev2 sa detail

IPv4 Crypto IKEv2 SA

Tunnel-id Local Remote fvrf/ivrf Status
1 10.0.8.3/848 10.0.9.4/848 none/none READY
Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth
verify: PSK
Life/Active Time: 86400/59 sec
CE id: 1001, Session-id: 1
Status Description: Negotiation done
Local spi: 84350219051DB9E3 Remote spi: 52A8BB3898E8B5CF
Local id: 10.0.8.3
Remote id: 10.0.9.4
Local req msg id: 4 Remote req msg id: 0
Local next msg id: 4 Remote next msg id: 0
Local req queued: 4 Remote req queued: 0
Local window: 5 Remote window: 5
DPD configured for 0 seconds, retry 0
IETF Std Fragmentation configured.
Extended Authentication not configured.
NAT-T is not detected
Cisco Trust Security SGT is disabled
Initiator of SA : Yes

IPv6 Crypto IKEv2 SA
```

次は、応答側の設定を表示するサンプル出力です。この出力では、シスコ独自のフラグメンテーション方式が構成されていますが、有効ではない点に注意してください。

```
Device# show crypto ikev2 sa detail

IPv4 Crypto IKEv2 SA

Tunnel-id Local Remote fvrf/ivrf Status
1 10.0.9.4/848 10.0.8.3/848 none/none READY
Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth
verify: PSK
Life/Active Time: 86400/52 sec
CE id: 1001, Session-id: 1
Status Description: Negotiation done
Local spi: 52A8BB3898E8B5CF Remote spi: 84350219051DB9E3
Local id: 10.0.9.4
Remote id: 10.0.8.3
Local req msg id: 0 Remote req msg id: 4
Local next msg id: 0 Remote next msg id: 4
Local req queued: 0 Remote req queued: 4
Local window: 5 Remote window: 5
```

```
DPD configured for 0 seconds, retry 0
Fragmentation configured.
Extended Authentication not configured.
NAT-T is not detected
Cisco Trust Security SGT is disabled
Initiator of SA : No

IPv6 Crypto IKEv2 SA
```

次は、発信側がIETF標準フラグメンテーション方式をサポートし、応答側はフラグメンテーションをサポートしていない例を示します。この出力は、IETF標準フラグメンテーション方式が構成されていますが、有効ではないことを示す点に注意してください。

```
Device# show crypto ikev2 sa detail
IPv4 Crypto IKEv2 SA

Tunnel-id Local Remote fvrf/ivrf Status
1 10.0.8.3/848 10.0.9.4/848 none/none READY
Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth
verify: PSK
Life/Active Time: 86400/44 sec
CE id: 1004, Session-id: 2
Status Description: Negotiation done
Local spi: 03534703287D9CA1 Remote spi: 146E1CFA68008A92
Local id: 10.0.8.3
Remote id: 10.0.9.4
Local req msg id: 4 Remote req msg id: 0
Local next msg id: 4 Remote next msg id: 0
Local req queued: 4 Remote req queued: 0
Local window: 5 Remote window: 5
DPD configured for 0 seconds, retry 0
IETF Std Fragmentation configured.
Extended Authentication not configured.
NAT-T is not detected
Cisco Trust Security SGT is disabled
Initiator of SA : Yes
```

次は、応答側の設定を表示するサンプル出力です。ステートメント「Fragmentation not configured.」に注意してください。

```
Device# show crypto ikev2 sa detail
IPv4 Crypto IKEv2 SA

Tunnel-id Local Remote fvrf/ivrf Status
1 10.0.9.4/848 10.0.8.3/848 none/none READY
Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth
verify: PSK
Life/Active Time: 86400/23 sec
CE id: 1004, Session-id: 4
Status Description: Negotiation done
Local spi: 146E1CFA68008A92 Remote spi: 03534703287D9CA1
Local id: 10.0.9.4
Remote id: 10.0.8.3
Local req msg id: 0 Remote req msg id: 3
Local next msg id: 0 Remote next msg id: 3
Local req queued: 0 Remote req queued: 3
Local window: 5 Remote window: 5
DPD configured for 0 seconds, retry 0
Fragmentation not configured.
Extended Authentication not configured.
NAT-T is not detected
```

```
Cisco Trust Security SGT is disabled
Initiator of SA : No
```

例：発信側で設定されない IETF 標準フラグメンテーション方式

次は、発信側で設定されるフラグメンテーション方式が表示されないサンプル出力です。

```
Device# show crypto ikev2 sa detail

IPv4 Crypto IKEv2 SA

Tunnel-id Local Remote fvrf/ivrf Status
2 10.0.8.3/848 10.0.9.4/848 none/none DELETE
Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth
verify: PSK
Life/Active Time: 86400/28 sec
CE id: 1001, Session-id: 1
Status Description: Deleting IKE SA
Local spi: 1A375C00C1D157CF Remote spi: DB50F1BC58814FFA
Local id: 10.0.8.3
Remote id: 10.0.9.4
Local req msg id: 2 Remote req msg id: 4
Local next msg id: 4 Remote next msg id: 5
Local req queued: 2 Remote req queued: 4
Local window: 5 Remote window: 5
DPD configured for 0 seconds, retry 0
Fragmentation not configured.
Extended Authentication not configured.
NAT-T is not detected
Cisco Trust Security SGT is disabled
Initiator of SA : No

IPv6 Crypto IKEv2 SA
```

例：フラグメンテーションの IPv6 サポート

次の例は、FlexVPN エンドポイント（ハブとスポーク）のフラグメンテーションを示します。次は、パケットのフラグメント化に 1300 の最大伝送ユニット（MTU）を設定したハブに関連する設定です。

```
Device# show crypto ikev2 sa detail

IPv4 Crypto IKEv2 SA

IPv6 Crypto IKEv2 SA

Tunnel-id fvrf/ivrf Status
1 none/none READY
Local 4001::2000:3/500
Remote 4001::2000:1/500
Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth
verify: PSK
Life/Active Time: 86400/64 sec
CE id: 1001, Session-id: 1
Status Description: Negotiation done
Local spi: 45BA0D30D0EB5FFF Remote spi: 8D7B5A8389CEB8B3
```

```
Local id: R2.cisco.com
Remote id: R1.cisco.com
Local req msg id: 3 Remote req msg id: 0
Local next msg id: 3 Remote next msg id: 0
Local req queued: 3 Remote req queued: 0
Local window: 5 Remote window: 5
DPD configured for 0 seconds, retry 0
IETF Std Fragmentation enabled.
IETF Std Fragmentation MTU in use: 1272 bytes.
Extended Authentication not configured.
NAT-T is not detected
Cisco Trust Security SGT is disabled
Initiator of SA : Yes
Remote subnets:
10.0.0.251 255.255.255.255
IPv6 Remote subnets:
3001::/112
5001::/64
```

次は、デフォルトの MTU を設定したスポークに関連する設定です。

```
Device# show crypto ikev2 sa detail

IPv4 Crypto IKEv2 SA

IPv6 Crypto IKEv2 SA

Tunnel-id fvrf/ivrf Status
1 none/none READY
Local 4001::2000:1/500
Remote 4001::2000:3/500
Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth
verify: PSK
Life/Active Time: 86400/58 sec
CE id: 1001, Session-id: 1
Status Description: Negotiation done
Local spi: 8D7B5A8389CEB8B3 Remote spi: 45BA0D30D0EB5FFF
Local id: R1.cisco.com
Remote id: R2.cisco.com
Local req msg id: 0 Remote req msg id: 3
Local next msg id: 0 Remote next msg id: 3
Local req queued: 0 Remote req queued: 3
Local window: 5 Remote window: 5
DPD configured for 0 seconds, retry 0
IETF Std Fragmentation enabled.
IETF Std Fragmentation MTU in use: 1232 bytes.
Extended Authentication not configured.
NAT-T is not detected
Cisco Trust Security SGT is disabled
Initiator of SA : No
Remote subnets:
10.0.0.3 255.255.255.255
```

IKEv2 フラグメンテーション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』、すべてのリリース
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』

標準および RFC

標準/RFC	タイトル
IKEv2 フラグメンテーション	*draft-ietf-ipsecme-ikev2-fragmentation-10*

シスコのテクニカル サポート

説明	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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

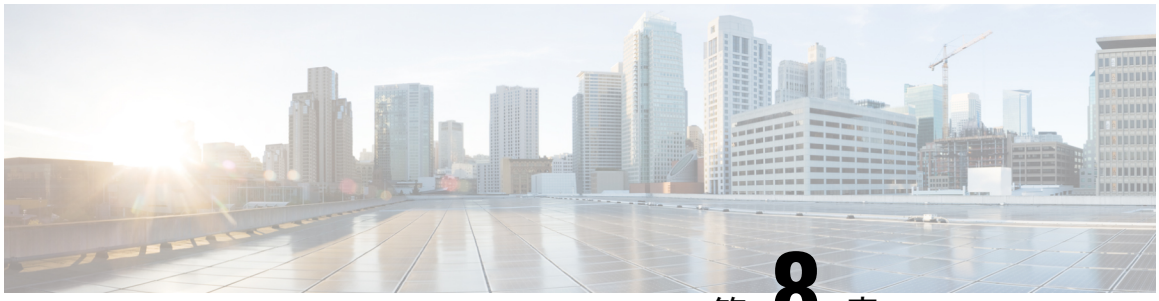
IKEv2 フラグメンテーションの機能情報

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 *9 : IKEv2* フラグメンテーションの機能情報

機能名	リリース	機能情報
RFC に準拠した IKEv2 フラグメンテーション		RFC 機能に準拠した IKE フラグメンテーションでは、IETF の **draft-ietf-ipsecme-ikev2-fragmentation-10** ドキュメントの提案に従って、インターネット キー エクスチェンジ バージョン 2 （IKEv2）パケットのフラグメンテーションを実装しました。 **show crypto ikev2 sa** コマンドが変更されました。



第 8 章

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。

- 機能情報の確認 （121 ページ）
- IKEv2 再接続設定の前提条件 （121 ページ）
- IKEv2 再接続設定の制限事項 （122 ページ）
- 設定された IKEv2 フラグメンテーションに関する情報 （122 ページ）
- IKEv2 再接続の設定方法 （123 ページ）
- IKEv2 再接続の設定例 （125 ページ）
- IKEv2 再接続の設定に関する追加情報 （126 ページ）
- IKEv2 再接続の機能情報 （126 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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。

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** および **clear crypto ikev2 sa reconnect** 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**
3. **clear 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
```

ステップ 3 **clear crypto ikev2 stats reconnect**

再接続の統計情報がクリアされます。

例：

```
Device# clear crypto ikev2 stats reconnect

Total incoming reconnect connection:        0
Success reconnect connection:               0
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*』、すべてのリリース
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*』
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
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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

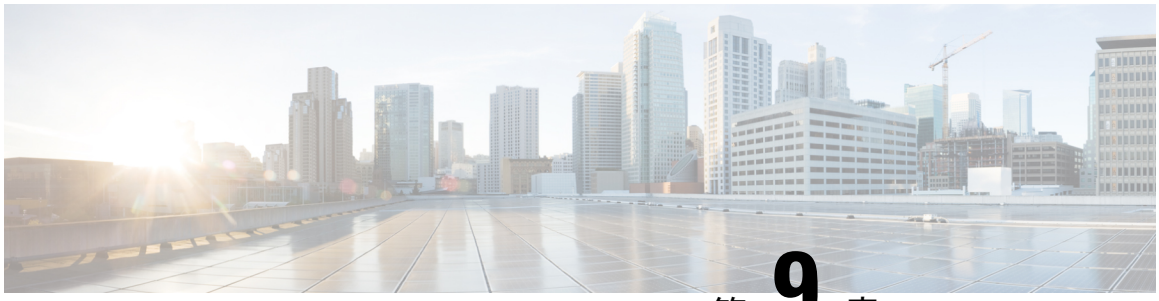
IKEv2 再接続の機能情報

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 *10 : 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.**



第 9 章

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。

- 機能情報の確認 （129 ページ）
- IKEv2 パケット オブ ディスコネクトに関する情報 （129 ページ）
- IKEv2 パケット オブ ディスコネクトの設定方法 （131 ページ）
- IKEv2 パケット オブ ディスコネクトの設定例 （132 ページ）
- IKEv2 パケット オブ ディスコネクトに関する追加情報 （136 ページ）
- IKEv2 パケット オブ ディスコネクトの機能情報 （137 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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。

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 サーバ上のユーザ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 ユーザを AAA サーバの新しいユーザ 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 サーバに必要な IKEv2 独自の設定はありません。FlexVPN サーバでは、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 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。

	コマンドまたはアクション	目的
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 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 キーを設定します。 （注） クライアント レベルでサーバ 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 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 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』、すべてのリリース

関連項目	マニュアル タイトル
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
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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

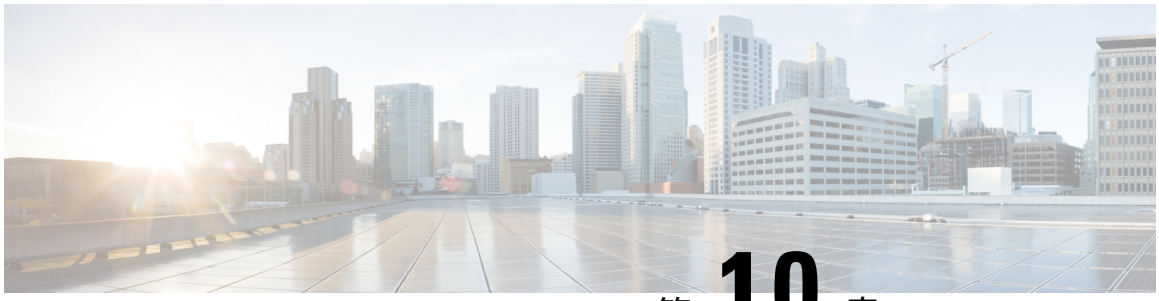
IKEv2 パケット オブ ディスコネクトの機能情報

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 *11 : 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。



第 10 章

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。

- 機能情報の確認 （139 ページ）
- IKEv2 認可変更のサポートの前提条件 （139 ページ）
- IKEv2 認可変更サポートの制限事項 （140 ページ）
- IKEv2 認可変更サポートに関する情報 （140 ページ）
- IKEv2 認可変更サポートの設定方法 （141 ページ）
- IKEv2 認可変更サポートの設定例 （145 ページ）
- IKEv2 認可変更サポートに関する追加情報 （146 ページ）
- IKEv2 認可変更のサポートの機能情報 （146 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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。

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 認可の変更

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、またはユーザ 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 サーバでの IKEv2 固有の設定はありません。FlexVPN サーバでは、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。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
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 サーバとして設定し、外部ポリシー サーバ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 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：	グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
	`Device(config-locsvr-da-radius)# exit`	

Cisco ASR 1000 シリーズ ルータでの IKEv2 認可変更サポートの確認

show コマンドを使用して、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータの認可変更（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』、すべてのリリース
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
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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 *12 : 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。

第 11 章

集約認証の設定

FlexVPN RA - Cisco AnyConnect クライアントのサポートを拡張することで、AnyConnect 機能の集約認証サポートは、集約認証方式を実装します。このクライアントでは、独自の AnyConnect EAP 認証方式を使用し、Cisco AnyConnect クライアントと FlexVPN サーバ間にインターネットを介したセキュア トンネルを確立します。

- 機能情報の確認 （149 ページ）
- 集約認証の設定の前提条件 （149 ページ）
- 集約認証の設定に関する情報 （150 ページ）
- 集約認証の設定方法 （153 ページ）
- 集約認証の設定例 （155 ページ）
- 集約認証の設定に関する追加情報 （156 ページ）
- 集約認証の設定に関する機能情報 （157 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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。

集約認証の設定の前提条件

- <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。

集約認証の設定に関する情報

Cisco AnyConnect および FlexVPN

VPN 接続を確立するには、VPN クライアントが Extensible Authentication Protocol（EAP：拡張可能認証プロトコル）、拡張認証（XAUTH）などの認証方式を使用してユーザ クレデンシャルを取得し、Access Control Server を接続するハブにユーザ クレデンシャルを転送する必要があります。Access Control Server は、外部データベースまたは Active Directory（AD）を送信してクレデンシャルを確認します。

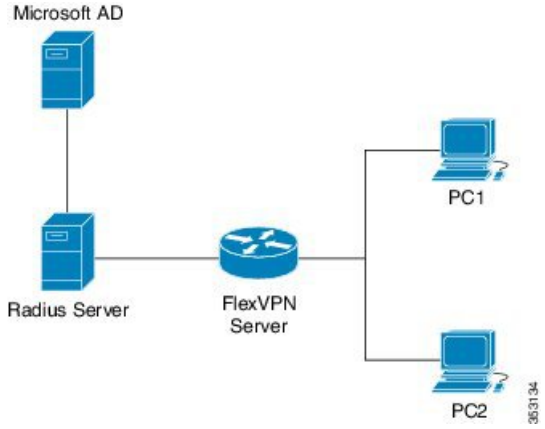
FlexVPN サーバは（ハブとして）Cisco Secure Access Control Server と連動してユーザ クレデンシャルを確認し、VPN 接続を確立します。ただし、Cisco AnyConnect は EAP を使用してユーザ クレデンシャルを取得し、XAUTH をサポートしません。一方、Cisco Secure Access Control Server は外部データベース（ここでは AD）を使用する EAP-MD5 をサポートしません。これによって、Cisco Secure Access Control Server が EAP-MD5 をサポートする必要があるシナリオ、または FlexVPN が Cisco AnyConnect からの情報を個別に認証して、Cisco Secure Access Control Server に個別に接続する必要があるシナリオが生じます。FlexVPN は、集約認証方式を使用して、Cisco AnyConnect からの情報を認証できます。FlexVPN サーバで集約認証方式を実装すると、Cisco IOS ソフトウェアにより多くの機能サポートを追加するためのウィンドウが提供されます。

FlexVPN RA：AnyConnect の集約認証サポート機能では、独自の AnyConnect EAP 認証方式を使用する Cisco AnyConnect クライアントのサポートを拡張することによって集約認証方式を実装し、Cisco AnyConnect サーバや FlexVPN サーバを使用してインターネット上にセキュアなトンネルを確立します。 これは、サーバ固有の機能で、Cisco AnyConnect と連動します。

集約認証の動作

インターネット キー エクスチェンジ バージョン 2 は、基本的な集約認証を実装することによって独自の AnyConnect EAP 認証方式を使用する Cisco AnyConnect をサポートします。ここでの認証は、リモート RADIUS サーバを使用する認証、認可、およびアカウンティング（AAA）を介して実行されます。次に、Cisco IOS ソフトウェアでの集約認証の実装を説明するネットワーク トポロジの例を示します。

図 *5 : RADIUS* サーバに接続された *FlexVPN* サーバ



この図は、次のことを示しています。

- Cisco Secure Access Control Server は、認証用の RADIUS サーバとして機能します。
- クレデンシャルは、認証用の Active Directory として機能する Microsoft Active Directory に格納されます。

（注） Microsoft Active Directory は、単なる例です。クレデンシャルの格納場所は重要ではありません。

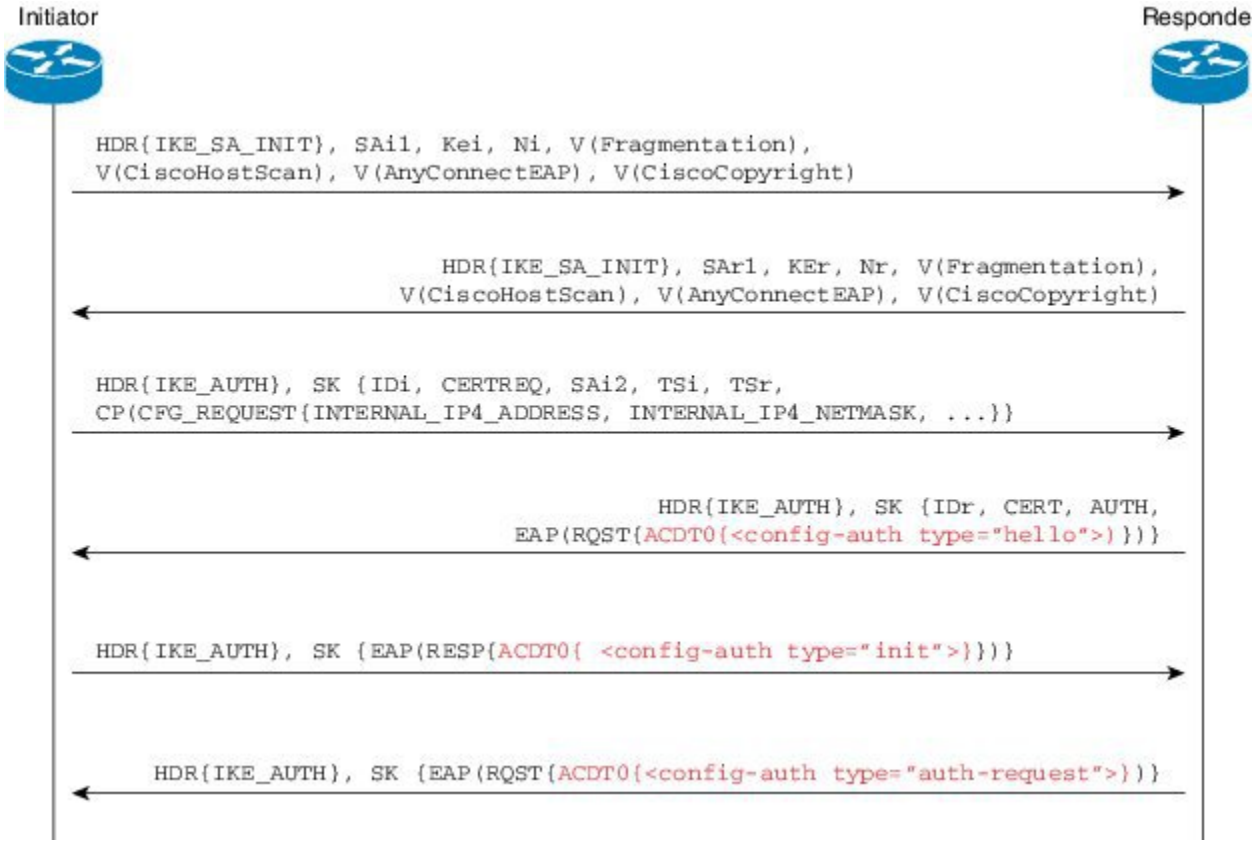
- シスコ デバイスは、FlexVPN サーバとして機能します。
- Windows 7 PC は、Cisco AnyConnect クライアントとして機能します。

1. VPN 接続を開始するために、Cisco AnyConnect クライアントは証明書を使用して FlexVPN サーバを確認します。
2. 証明書を確認した後、Cisco AnyConnect クライアントは Cisco AnyConnect EAP がロードしたメッセージを FlexVPN サーバに送信します。
3. FlexVPN サーバが Cisco AnyConnect から Cisco AnyConnect EAP がロードしたメッセージを受信すると、FlexVPN サーバはメッセージをダウンロードして EAP のメッセージを除去します。
4. FlexVPN は認証用の RADIUS サーバおよび認証用の Microsoft Active Directory（AD）との接続を確立して、除去されたメッセージを転送し、Cisco AnyConnect クライアントから提供されたクレデンシャルを確認します。
5. クレデンシャルが RADIUS サーバおよび Microsoft Active Directory（AD）によって確認されて承認されると、適切な応答が FlexVPN サーバに送信され、Cisco AnyConnect に応答し、VPN 接続が確立されます。

Cisco AnyConnect EAP を使用する IKE 交換

AnyConnect EAP を使用する IKE での認証は、RFC 3748 で説明されているように標準 EAP モデルのバリエーションです。AnyConnect EAP を使用すると、パブリック設定または認証 XML は EAP ペイロードを介して送信されます。次の図に、Cisco AnyConnect によって使用される一般的なメッセージ フローを示します。

図 *6 : AnyConnect EAP* を使用する *IKE* 交換



1. Cisco AnyConnect クライアントが、FlexVPN サーバへの IKE 接続を開始します。クライアントは、一般的な IKE ペイロードに加えて、Cisco AnyConnect EAP のサポートを示すためのベンダー ID ペイロードを送信します。クライアントは、シスコの著作権ベンダー ID を含めることによって自身をシスコ製品として識別します。
2. サーバ ゲートウェイが、フラグメンテーションおよび AnyConnect EAP サポートを示すためのベンダー ID ペイロードを送信し、シスコの著作権ベンダー ID を含めることによって自身をシスコ製品として識別します。
3. 設定ペイロードで、トンネル設定が要求されます。クライアントは、このメッセージから AUTH ペイロードを省略することによって、Cisco AnyConnect EAP 認証の使用を希望していることを示します。
4. 集約認証および設定プロトコルが、EAP を介して伝送されます。
5. FlexVPN サーバが、EAP の成功メッセージを送信します。
6. Cisco AnyConnect クライアントが、AUTH ペイロードを送信します。

7. FlexVPN サーバが、AUTH ペイロードと Cisco AnyConnect クライアントが要求したトンネル設定属性を送信します。

IKEv2 でのデュアルファクタ認証のサポート

Cisco IOS ソフトウェアでの集約認証の実装は、デュアルファクタ認証に拡張できます。二重認証は、デバイス証明書情報を交換し検証する集約認証中に、新しい AnyConnect EAP 交換を導入することで実行されます。「デバイス」と同様に「ユーザ」も認証するこのメカニズムは、「二重認証」と呼ばれます。

（注） AnyConnect EAP は、AnyConnect クライアント固有の認証方式であり、他クライアントには適用されません。

集約認証の設定方法

集約認証用の FlexVPN サーバの設定

このタスクを実行して、FlexVPN サーバの集約認証を設定します。

手順の概要

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**

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：	特権 EXEC モードを有効にします。

	コマンドまたはアクション	目的
	`Device> enable`	• 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プロファイル名を定義し、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	**aaa accounting anyconnect-eap** *list-name* 例： `Device(config-ikev2-profile)# aaa accounting anyconnect-eap list1`	IKEv2 リモート認証方式が AnyConnect EAP の場合、認証、認可、およびアカウンティング（AAA）のアカウンティング方式リストを有効にします。
ステップ 5	**match identity remote key-id** *opaque-string* 例： `Device(config-ikev2-profile)# match identity remote key-id aggauth_user3@abc.com`	リモート キー ID タイプの ID に基づいて、プロファイルを照合します。
ステップ 6	**authentication remote anyconnect-eap aggregate** [**cert-request**] 例： `Device(config-ikev2-profile)# authentication remote anyconnect-eap aggregate cert-request`	Cisco AnyConnect EAP に集約認証を指定します。 • **cert-request** ：二重認証用に Cisco AnyConnect クライアントに証明書を要求します。
ステップ 7	**authentication local rsa-sig** 例： `Device(config-ikev2-profile)# authentication local rsa-sig`	Rivest、Shamir、Adelman（RSA）署名をローカル認証方式として指定します。
ステップ 8	**pki trustpoint** *trustpoint-label* 例： `Device(config-ikev2-profile)# pki trustpoint CA1`	RSA 署名認証方式で使用する Public Key Infrastructure（PKI）トラストポイントを指定します。
ステップ 9	**aaa authentication anyconnect-eap** *list-name* 例： `Device(config-ikev2-profile)# aaa authentication anyconnect-eap list1`	Cisco AnyConnect EAP 認証用に、認証、認可、およびアカウンティング（AAA）認証リストを指定します。 • **anyconnect-eap**：AAA AnyConnect EAP 認証を指定します。 • *list-name*：AAA 認証リスト名。

	コマンドまたはアクション	目的
ステップ 10	**aaa authorization group anyconnect-eap list** *aaa-listname* **name-mangler** *mangler-name* 例： `Device(config-ikev2-profile)# aaa authorization group anyconnect-eap list list1 name-mangler mangler1`	リモート認証方式が AnyConnect EAP であり、名前分割が派生する場合、各グループ ポリシーに AAA 認証を指定します。
ステップ 11	**aaa authorization user anyconnect-eap cached** 例： `Device(config-ikev2-profile)# aaa authorization user anyconnect-eap cached`	リモート認証方式が AnyConnect EAP であり、AnyConnect EAP 認証からキャッシュした属性を使用する場合、各ユーザ ポリシーに AAA 認証を指定します。
ステップ 12	**aaa authorization user anyconnect-eap list** *aaa-listname* **name-mangler** *mangler-name* 例： `Device(config-ikev2-profile)# aaa authorization user anyconnect-eap list list1 name-mangler mangler1`	リモート認証方式に AAA 方式リストを指定し、名前分割が派生します。
ステップ 13	**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。
ステップ 14	**show crypto ikev2 session detailed** 例： `Device# show crypto ikev2 session detailed`	アクティブなインターネット キー エクスチェンジ バージョン 2（IKEv2）セッションのステータスを表示します。

集約認証の設定例

例：集約認証の設定

次の例は、FlexVPN サーバで集約認証を設定する方法を示します。これによって、Cisco AnyConnect クライアントと FlexVPN サーバ間のセキュア トンネルの確立を有効にします。

```
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
```

集約認証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』、すべてのリリース
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
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。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

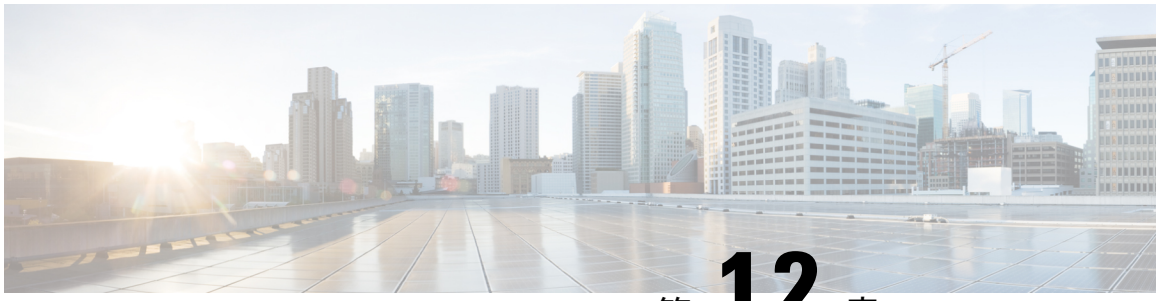
集約認証の設定に関する機能情報

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 *13 :* 集約認証の設定に関する機能情報

機能名	リリース	機能情報
IKEv2 でのデュアル ファクタ認証のサポート		IKEv2 でのデュアルファクタ認証のサポートは、二重認証への Cisco AnyConnect クライアントからの証明書要求をサポートします。 **authentication (IKEv2 profile)** コマンドが変更されました。
FlexVPN RA - AnyConnect の集約認証サポート		FlexVPN RA - Cisco AnyConnect クライアントのサポートを拡張することで、AnyConnect 機能の集約認証サポートは、集約認証方式を実装します。このクライアントでは、独自の AnyConnect EAP 認証方式を使用し、Cisco AnyConnect クライアントと FlexVPN サーバ間にインターネットを介したセキュア トンネルを確立します。 次のコマンドが導入または変更されました。**aaa accounting (IKEv2 profile)**、**aaa authentication (IKEv2 profile)**、**aaa authorization (IKEv2 profile)**、**authentication (IKEv2 profile)**、**show crypto ikev2 profile**、**show crypto ikev2 session**



第 12 章

付録：FlexVPN の RADIUS 属性

この章では、FlexVPN サーバでサポートされる RADIUS 属性について説明します。

• FlexVPN RADIUS 属性 （159 ページ）

FlexVPN RADIUS 属性

次に、FlexVPN サーバによって使用される RADIUS 属性カテゴリを示します。

- インバウンドおよび双方向 IETF RADIUS 属性
- アウトバウンド ローカル
- アウトバウンド リモート

（注） 次のリストに含まれていない FlexVPN サーバによって RADIUS に送信されるインバウンド属性では、値は AAA システムによって設定されます。

属性	User-Name
タイプ	IETF
書式	文字列
属性 ID	1

説明	この属性は、FlexVPN サーバによって RADIUS に送信され、次のように取得されます。 • AAA ベースの事前共有キー：ピア IKEv2 ID • EAP 認証：ピア EAP ID • ユーザ認証またはグループ認証：name mangler の出力または IKEv2 プロファイル認証コマンドで指定された文字列。 • アカウンティング：ピア EAP ID または IKEv2 ID。 この属性は、正常な EAP 認証後に Access-Accept で RADIUS から受信されることもあります。また、認証済みのピア EAP ID を指定します。

属性	User-Password
タイプ	IETF
書式	文字列
属性 ID	2
説明	この属性は、FlexVPN サーバによって RADIUS に送信され、次のように取得されます。 • AAA ベースの事前共有キー：「cisco」 • ユーザ/グループ認証：「cisco」

属性	Calling-Station-ID
タイプ	IETF
書式	文字列
属性 ID	31
説明	この属性は、FlexVPN サーバによって RADIUS に送信され、次のように取得されます。 • AAA ベースの事前共有キー：IKEv2 発信側アドレス • EAP 認証：IKEv2 発信側アドレス • ユーザ/グループ認証：IKEv2 発信側アドレス

属性	Service-Type

タイプ	IETF
書式	文字列
属性 ID	6
説明	この属性は、FlexVPN サーバによって EAP 認証に使用されており、この属性の値は「Login」に設定されています。

属性	EAP-Message
タイプ	IETF
書式	文字列
属性 ID	79
説明	この属性は、FlexVPN サーバによって EAP 認証に使用されており、EAP サーバとリモート アクセス クライアントの間で EAP パケットをリレーします。

属性	Message-Authenticator
タイプ	IETF
書式	文字列
属性 ID	80
説明	この属性は、FlexVPN サーバによって EAP 認証用に送信されます。この属性の値は、AAA サブシステムによって設定されます。

属性	Framed-Pool
タイプ	IETF
書式	文字列
属性 ID	88
ローカル設定	pool name
RADIUS 設定	Framed-Pool=*pool-name*

説明	FlexVPN サーバが IPv4 アドレスの割り当てに使用する IPv4 アドレス プールの名前を指定して、クライアントに割り当てます。割り当てられたアドレスは、IKEv2 標準設定属性の INTERNAL_IP4_ADDRESS を介してクライアントにプッシュされます。

属性	ipsec:group-dhcp-server
タイプ	Cisco AV ペア
書式	文字列
ローカル設定	dhcp server {*ipddr* | *host*}
RADIUS 設定	cisco-avpair="ipsec: group-dhcp-server=*ipaddr*"
説明	FlexVPN サーバが IPv4 アドレスのリースに使用する IPv4 DHCP サーバを指定して、クライアントに割り当てます。リースされたアドレスは、IKEv2 標準設定属性の INTERNAL_IP4_ADDRESS を介してクライアントにプッシュされます。

属性	ipsec:dhcp-giaddr
タイプ	Cisco AV ペア
書式	IPaddr
ローカル設定	dhcp giaddr ipaddr
RADIUS 設定	cisco-avpair="psec: dhcp-giaddr=*ipaddr*"
説明	FlexVPN サーバが DCHP サーバへの接続に使用する IPv4 DHCP ゲートウェイ IP アドレスを指定します。

属性	ipsec:dhcp-timeout
タイプ	Cisco AV ペア
書式	整数
ローカル設定	dhcp timeout *seconds*
RADIUS 設定	cisco-avpair="ipsec:dhcp-timeout=*seconds*"

説明	FlexVPN サーバが DHCP サーバからの応答をタイムアウトするのに使用する、IPv4 DHCP サーバからの応答の待機時間を指定します。

属性	ipsec:ipv6-addr-pool
タイプ	Cisco AV ペア
書式	文字列
ローカル設定	ipv6 *pool name*
RADIUS 設定	cisco-avpair="ipsec:ipv6-addr-pool=*pool-name*"
説明	FlexVPN サーバが IPv6 アドレスの割り当てに使用する IPv6 アドレス プールの名前を指定して、クライアントに割り当てます。割り当てられたアドレスは、IKEv2 標準設定属性の INTERNAL_IP6_ADDRESS を介してクライアントにプッシュされます。

属性	ipsec:route-set=prefix
タイプ	Cisco AV ペア
書式	文字列
ローカル設定	該当なし
RADIUS 設定	cisco-avpair="ipsec:route-set=prefix *prefix*/*length*"
例	ipsec:route-set=prefix 192.168.1.0/24
説明	FlexVPN サーバによって保護されるサブネットを指定します。これは、IKEv2 標準設定属性の INTERNAL_IP4_SUBNET を介してクライアントにプッシュされます。 （注） この AV ペアは、Cisco IOS リリース 15.2(2)T で導入されました。

属性	ipsec:route-set=interface
タイプ	Cisco AV ペア
書式	文字列
ローカル設定	route set interface

RADIUS 設定	cisco-avpair="ipsec:route-set=interface"
説明	この属性はローカルに使用され、IKEv2 標準設定属性の INTERNAL_IP4_SUBNET を介したピアへの VPN インターフェイス IP アドレスの送信を有効にします。これによって、BGP over VPN などのルーティング プロトコルが実行されます。 （注） Cisco IOS リリース 15.2(2)T で、「ipsec:route-set-interface」AV ペアからこの AV ペアに置き換えられました。

属性	ipsec:route-accept
タイプ	Cisco AV ペア
書式	文字列
ローカル設定	route accept any [tag *tag-id*] [distance *distance*]
RADIUS 設定	cisco-avpair="ipsec:route-accept=any [tag:*tag*] [distance:*distance*]"
例	ipsec:route-accept=any tag=100
説明	この属性はローカルに使用され、IKEv2 標準設定属性の INTERNAL_IP4_SUBNET を介してピアから受信されるサブネットのフィルタを指定します。この属性は、フィルタ処理されたサブネット用に IKEv2 よって追加されるルートのタグと距離も指定します。 （注） Cisco IOS リリース 15.2(2)T で、AV ペア「ipsec:route-accept=accept acl:any」から「ipsec:route-accept=any」に置き換えられ、AV ペア「ipsec:route-accept=deny」から「ipsec:route-accept=none」に置き換えられました。

属性	ipsec:ipsec-flow-limit
タイプ	Cisco AV ペア
書式	整数
ローカル設定	ipsec flow-limit *limit*
RADIUS 設定	cisco-avpair="ipsec:ipsec-flow-limit=*limit*"

説明	この属性はFlexVPNサーバによって使用され、IPSec dVTIセッションが使用可能なIPSec SAの最大数を指定します。デフォルトでは制限はありません。このパラメータは **crypto ipsec profile** コマンドおよび **set security-policy limit** コマンドと同様です。

属性	ip:interface-config
タイプ	Cisco AV ペア
書式	文字列
ローカル設定	aaa attribute list *list* attribute type interface-config *string*
RADIUS 設定	cisco-avpair="ip:interface-config=interface cmd string"
例	ip:interface-config=ip vrf forwarding red
説明	この属性はローカルに使用され、セッションの仮想アクセスインターフェイスに適用されるインターフェイス コンフィギュレーション モードのコマンド文字列を指定します。ローカル設定の場合、IKEv2認証ポリシーは、interface-config属性が必要な AAA 属性リストを示します。

属性	Tunnel-Type
タイプ	IETF
書式	整数
属性 ID	64
RADIUS 設定	Tunnel-Type=type
説明	この属性は、トンネルタイプ（ESP、AH、GREなど）を指定し、FlexVPNサーバがRADIUSサーバからセッションの事前共有キーを取得するときに受信されます。

属性	Tunnel-Medium-Type
タイプ	IETF
書式	整数
属性 ID	65、
RADIUS 設定	Tunnel-Medium-Type=type

説明	この属性は、トンネル転送タイプ（IPv4、IPv6 など）を指定し、FlexVPN サーバが RADIUS サーバからセッションの事前共有キーを取得するときに受信されます。

属性	Tunnel-Password
タイプ	IETF
書式	文字列
属性 ID	69
RADIUS 設定	Tunnel-Password=string
説明	この属性は、対称の事前共有キーを指定し、FlexVPN サーバが RADIUS サーバからセッションの事前共有キーを取得するときに受信されます。

属性	ipsec:ikev2-password-local
タイプ	Cisco AV ペア
書式	文字列
RADIUS 設定	cisco-avpair="ipsec:ikev2-password-local=*string*"
説明	この属性は、ローカルの事前共有キーを指定し、FlexVPN サーバが RADIUS サーバからセッションの事前共有キーを取得するときに受信されます。

属性	ipsec:ikev2-password-remote
タイプ	Cisco AV ペア
書式	文字列
RADIUS 設定	cisco-avpair="ipsec:ikev2-password-remote=*string*"
説明	この属性は、リモートの事前共有キーを指定し、FlexVPN サーバが RADIUS サーバからセッションの事前共有キーを取得するときに受信されます。

属性	Framed-IP-Address
タイプ	IETF
書式	IPaddr
属性 ID	8

RADIUS 設定	Framed-IP-Address=*ipaddr*
説明	クライアントに割り当てられるIPv4アドレスを指定します。これは、IKEv2標準設定属性の INTERNAL_IP4_ADDRESS を介してクライアントにプッシュされます。

属性	Framed-IP-Netmask
タイプ	IETF
書式	IPaddr
属性 ID	9
ローカル設定	netmask *mask*
RADIUS 設定	Framed-IP-Netmask=*mask*
説明	クライアントに割り当てられる IPv4 アドレスのサブネット マスクを指定します。これは、IKEv2 標準設定属性の INTERNAL_IP4_NETMASK を介してクライアントにプッシュされます。

属性	ipsec:dns-servers
タイプ	Cisco AV ペア
書式	文字列
ローカル設定	dns *primary* [*secondary*]
RADIUS 設定	cisco-avpair="ipsec:dns-servers=*primary secondary*"
説明	クライアントのプライマリ IPv4 DNS サーバおよびセカンダリ IPv4 DNS サーバを指定します。これは、IKEv2 標準設定属性の INTERNAL_IP4_DNS を介してクライアントにプッシュされます。

属性	ipsec:wins-servers
タイプ	Cisco AV ペア
書式	文字列
ローカル設定	wins *primary* [*secondary*]

RADIUS 設定	cisco-avpair="ipsec:wins-servers=*primary secondary*"
説明	クライアントのプライマリ IPv4 WINS サーバおよびセカンダリ IPv4 WINS サーバを指定します。これは、IKEv2 標準設定属性の INTERNAL_IP4_NBNS を介してクライアントにプッシュされます。

属性	ipsec:route-set=access-list
タイプ	Cisco AV ペア
書式	文字列
ローカル設定	route set access-list {*acl-name* | *acl-number*}
RADIUS 設定	cisco-avpair="ipsec:route-set=access-list {*acl-name* | *acl-number*}"
説明	FlexVPN サーバによって保護される IPv4 サブネットを指定します。これは、IKEv2 標準設定属性の INTERNAL_IP4_SUBNET を介してクライアントにプッシュされます。 （注） Cisco IOS リリース 15.2(2)T で、「ipsec:inacl」AV ペアからこの AV ペアに置き換えられました。

属性	ipsec:addrv6
タイプ	Cisco AV ペア
書式	文字列
RADIUS 設定	cisco-avpair="ipsec:addrv6=*ipv6-addr*"
説明	クライアントに割り当てられる IPv6 アドレスを指定します。これは、最初の 16 バイトで IKEv2 標準設定属性の INTERNAL_IP6_ADDRESS を介してクライアントにプッシュされます。

属性	ipsec:prefix-len
タイプ	Cisco AV ペア
書式	整数
ローカル設定	該当なし

RADIUS 設定	cisco-avpair="ipsec:prefix-len=*value*"
例	ipsec:prefix-len=24
説明	クライアントに割り当てられる IPv6 アドレスのプレフィックス長を指定します。これは、最後（17 番目）のバイトで IKEv2 標準設定属性の INTERNAL_IP6_ADDRESS を介してクライアントにプッシュされます。

属性	ipsec:ipv6-dns-servers-addr
タイプ	Cisco AV ペア
書式	文字列
ローカル設定	ipv6 dns *primary* [*secondary*]
RADIUS 設定	cisco-avpair="ipsec: ipv6-dns-servers-addr=ipaddr1 *ipaddr2"
説明	クライアントのプライマリ IPv6 DNS サーバおよびセカンダリ IPv6 DNS サーバを指定します。これは、IKEv2 標準設定属性の INTERNAL_IP6_DNS を介してクライアントにプッシュされます。

属性	ipsec:route-set=access-list ipv6
タイプ	Cisco AV ペア
書式	文字列
ローカル設定	route set access-list ipv6 acl-name
RADIUS 設定	cisco-avpair="ipsec:route-set=access-list ipv6 *acl-name*"
説明	FlexVPN サーバによって保護される IPv6 サブネットを指定します。これは、IKEv2 標準設定属性の INTERNAL_IP6_SUBNET を介してクライアントにプッシュされます。 （注） Cisco IOS リリース 15.2(2)T で、「ipsec:ipv6-subnet-acl」AV ペアからこの AV ペアに置き換えられました。

属性	ipsec:banner
タイプ	Cisco AV ペア
書式	文字列

ローカル設定	banner *text*
RADIUS 設定	cisco-avpair="ipsec:banner=*text*"
説明	バナーテキストを指定します。これは、Cisco Unity 属性の MODECFG_BANNER を介してクライアントにプッシュされます。

属性	ipsec:default-domain
タイプ	Cisco AV ペア
書式	文字列
ローカル設定	def-domain *name*
RADIUS 設定	cisco-avpair="ipsec:default-domain=*name*"
説明	デフォルト ドメインを指定します。これは、Cisco Unity 属性の MODECFG_DEFDOMAIN を介してクライアントにプッシュされます。

属性	ipsec:split-dns
タイプ	Cisco AV ペア
書式	文字列
ローカル設定	split-dns name
RADIUS 設定	cisco-avpair="ipsec:split-dns=name"
説明	スプリット DNS 名を指定します。これは、Cisco Unity 属性の MODECFG_SPLITDNS_NAME を介してクライアントにプッシュされます。最大 10 個のスプリット DNS 名を設定できます。

属性	ipsec:ipsec-backup-gateway
タイプ	Cisco AV ペア
書式	文字列
ローカル設定	backup-gateway *name*

RADIUS 設定	cisco-avpair="ipsec:ipsec-backup-gateway=*name*"
説明	バックアップ ゲートウェイを指定します。これは、Cisco Unity 属性の MODECFG_BACKUPSERVERS を介してクライアントにプッシュされます。最大 10 のバックアップ ゲートウェイを設定できます。

属性	ipsec:pfs
タイプ	Cisco AV ペア
書式	整数
ローカル設定	pfs
RADIUS 設定	cisco-avpair="ipsec:pfs=*value*"
説明	IPsec PFS（Perfect Forward Secrecy）の有効/無効を指定します。これは、Cisco Unity 属性の MODECFG_PFS を介してクライアントにプッシュされます。値は、無効の場合は 0、有効の場合は 1 にする必要があります。

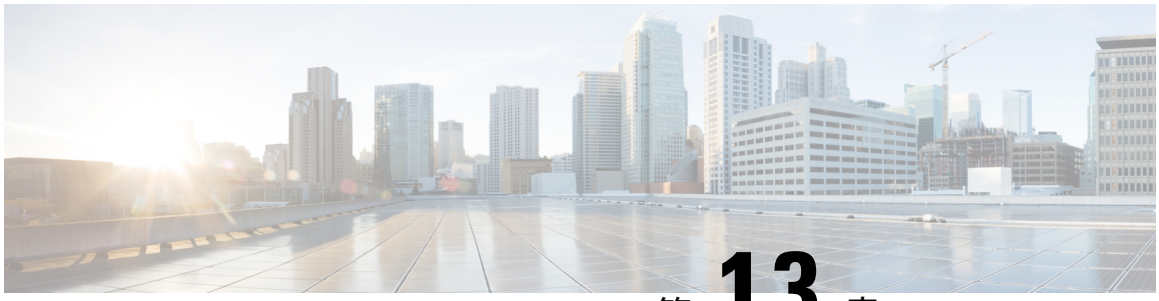
属性	ipsec:include-local-lan
タイプ	Cisco AV ペア
書式	整数
ローカル設定	include-local-lan
RADIUS 設定	cisco-avpair="ipsec:include-local-lan=*value*"
説明	ローカル LAN の包含を有効または無効にします。これは、Cisco Unity 属性の MODECFG_INCLUDE_LOCAL_LAN を介してクライアントにプッシュされます。値は、無効の場合は 0、有効の場合は 1 にする必要があります。

属性	ipsec:smartcard-removal-disconnect
タイプ	Cisco AV ペア
書式	整数
ローカル設定	smartcard-removal-disconnect

RADIUS 設定	cisco-avpair="ipsec:smartcard-removal-disconnect =*value*"
説明	スマートカードが取り外されたときの切断を有効または無効にします。これは、Cisco Unity 属性の MODECFG_SMARTCARD_REMOVAL_DISCONNECT を介してクライアントにプッシュされます。値は、無効の場合は 0、有効の場合は 1 にする必要があります。

属性	ipsec:configuration-url
タイプ	Cisco AV ペア
書式	文字列
ローカル設定	configuration url *url*
RADIUS 設定	cisco-avpair="ipsec:configuration-url=*url*"
説明	設定ダウンロードの URL を指定します。これは、Cisco FlexVPN 属性の MODECFG_CONFIG_URL を介してクライアントにプッシュされます。

属性	ipsec:configuration-version
タイプ	Cisco AV ペア
書式	整数
ローカル設定	configuration version *version*
RADIUS 設定	cisco-avpair="ipsec:configuration-version=*version*"
説明	ダウンロードする設定のバージョンを指定します。これは、Cisco FlexVPN 属性の MODECFG_CONFIG_VERSION を介してクライアントにプッシュされます。



第 13 章

付録：IKEv2 およびレガシー VPN

このモジュールでは、暗号マップ ベースの設定で IKEv2 を設定する例を示します。

（注） 暗号マップは、レガシー設定の構造と見なされます。既存の暗号マップ ベースの設定を移行して、トンネル保護および仮想インターフェイスを使用することをお勧めします。

- 例：事前共有キー認証方式を使用する暗号マップベースの IKEv2 ピアの設定 （173 ページ）
- 例：証明書認証方式を使用する暗号マップベースの IKEv2 ピアの設定 （176 ページ）
- 例：暗号マップ ベースおよび dVTI ベースの IKEv2 ピアの設定 （180 ページ）
- 例： sVTI ベース IKEv2 ピアを使用した IPSec の設定 （182 ページ）
- 例：DMVPN ネットワークでの IKEv2 の設定 （185 ページ）

例：事前共有キー認証方式を使用する暗号マップベースの IKEv2 ピアの設定

次の例に、スタティック暗号マップ IKEv2 発信側とダイナミック暗号マップ IKEv2 応答側との間で事前共有キー認証方式を使用して、暗号マップに基づく IKEv2 ピアを設定する方法を示します。発信側の設定は次のとおりです。

```
crypto ikev2 proposal prop-1
 encryption aes-cbc-128
 integrity sha1
 group 14
!
crypto ikev2 policy pol-1
 match fvrf any
 proposal prop-1
!
crypto ikev2 keyring v2-kr1
 peer abc
  address 209.165.200.231 255.255.255.224
  pre-shared-key abc
 !
```

```
!
!
crypto ikev2 profile prof
 match fvrf any
 match identity remote fqdn dmap-responder
 identity local fqdn smap-initiator
 authentication local pre-share
 authentication remote pre-share
 keyring v2-kr1
!
!
crypto ipsec transform-set trans esp-aes-cbc-128 esp-sha-hmac
!
crypto map cmap 1 ipsec-isakmp
 set peer 209.165.200.225
 set transform-set trans
 set ikev2-profile prof
 match address ikev2list
!
interface Loopback0
 ip address 209.165.200.226 255.255.255.224
!
interface Ethernet0/0
 ip address 209.165.200.227 255.255.255.224
 crypto map cmap
!
ip route 209.165.200.229 255.255.255.224 209.165.200.225
!
ip access-list extended ikev2list
 permit ip any any
!
```

応答側の設定は次のとおりです。

```
crypto ikev2 proposal prop-1
 encryption aes-cbc-128
 integrity sha1
 group 14
!
crypto ikev2 policy pol-1
 match fvrf any
 proposal prop-1
!
crypto ikev2 keyring v2-kr1
 peer abc
  address 209.165.200.228
  pre-shared-key abc
 !
!
!
crypto ikev2 profile prof
 match fvrf any
 match identity remote fqdn smap-initiator
 identity local fqdn dmap-responder
 authentication local pre-share
 authentication remote pre-share
 keyring v2-kr1
 ivrf global
!
!
crypto ipsec transform-set trans esp-aes-cbc-128 esp-sha-hmac
!
crypto dynamic-map dmap 1
 set transform-set trans
```

```
 set reverse-route tag 222
 set ikev2-profile prof
 match address ikev2list
!
crypto map cmap 1 ipsec-isakmp dynamic dmap
!
interface Loopback0
 ip address 209.165.200.230 255.255.255.224
!
interface Ethernet0/0
 ip address 209.165.200.231 255.255.255.224
 crypto map cmap
!
ip route 209.165.200.233 255.255.255.224 209.165.200.228
!
ip access-list extended ikev2list
 permit ip any any
!
```

発信側と応答側との接続を開始するには、発信側の CLI で次のコマンドを入力します。

```
ping 209.165.200.230 source 209.165.200.226
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.230, timeout is 2 seconds:
Packet sent with a source address of 209.165.200.226
%IKEV2-5-OSAL_INITIATE_TUNNEL: Received request to establish an IPsec tunnel; local
traffic selector = Address Range: 209.165.200.226-209.165.200.226 Protocol: 1 Port Range:
 0-65535; remote traffic selector = Address Range: 209.165.200.230-209.165.200.230
Protocol: 1 Port Range: 0-65535
%IKEV2-5-SA_UP: SA UP
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 8/11/12 ms
```

セッションの詳細を表示するには、次の **show** コマンドを入力します。

```
show crypto session
Crypto session current status
Interface: Ethernet0/0
Session status: UP-ACTIVE
Peer: 209.165.200.225 port 500
  IKEv2 SA: local 209.165.200.228/500 remote 209.165.200.231/500 Active
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map
show crypto ikev2 sa detail
Tunnel-id Local                 Remote                fvrf/ivrf            Status
1   209.165.200.228/500  209.165.200.231/500           (none)/(none)        READY
      Encr: AES-CBC, Keysize: 128, Hash: SHA96, DH Grp:14, Auth sign: PSK, Auth verify:
 PSK
      Life/Active Time: 86400/21 sec
      CE id: 1002, Session-id: 2
      Status Description: Negotiation done
      Local spi: 687752902752A6FD       Remote spi: C9DCCFC65493D14F
      Local id: smap-initiator
      Remote id: dmap-responder
      Local req msg id:  2              Remote req msg id:  0
      Local next msg id: 2              Remote next msg id: 0
      Local req queued:  2              Remote req queued:  0
      Local window:      5              Remote window:      5
      DPD configured for 0 seconds, retry 0
      NAT-T is not detected
```

例：証明書認証方式を使用する暗号マップベースのIKEv2 ピアの設定

次の例は、スタティック暗号マップ IKEv2 発信側、ダイナミック暗号マップ IKEv2 応答側、およびCA サーバの間で証明書認証方式を使用して、暗号マップに基づく IKEv2 ピアを設定する方法を示します。発信側の設定は次のとおりです。

```
crypto pki trustpoint ca-server
 enrollment url http://10.1.1.3:80
 revocation-check none
!
crypto pki certificate map cmap-1 1
 subject-name eq hostname = responder
!
!
crypto pki certificate chain ca-server
 certificate 02
  308201AF 30820118 A0030201 02020102 300D0609 2A864886 F70D0101 04050030
  14311230 10060355 04031309 63612D73 65727665 72301E17 0D313030 33313031
  32353132 355A170D 31313033 31303132 35313235 5A301A31 18301606 092A8648
  86F70D01 09021609 494E4954 4941544F 52305C30 0D06092A 864886F7 0D010101
  0500034B 00304802 4100A47E 8C58BA89 8CCDC5A4 5A63BD29 C331A2A5 393F4616
  6B43FD2E 5ED4C81A 913E3B13 33A9B2DC CFC30391 24BB0DC8 B28FD6F1 C008D101
  34C10062 30F88CF7 9D630203 010001A3 4F304D30 0B060355 1D0F0404 030205A0
  301F0603 551D2304 18301680 144871D9 002C66DF D85FACB8 45D1D25F EA357455
  91301D06 03551D0E 04160414 E77C74E7 183AB530 83DC531B 1DE3DA1D 914A925D
  300D0609 2A864886 F70D0101 04050003 81810042 21934B77 7E485E6F EE717D75
  6407B361 45190CEF E1A29CF2 6FA29E9A 5ECC1CEE B273533D 1453F6CE 1FDDA747
  7E701B4B 2A2AE53F D67C2345 952325BA 30950435 0706C5EE A7A8B414 CFEEB7A2
  9CD46F8F 3F663268 A20C4CCF E75D61EF 03FBA85D EDD6B26E 63653F09 F97DAFA6
  6C76E44E C9CA3FDC 6CD85D30 169A1D9E 4E870B
        quit
 certificate ca 01
  30820201 3082016A A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  14311230 10060355 04031309 63612D73 65727665 72301E17 0D313030 33313031
  32343933 385A170D 31333033 30393132 34393338 5A301431 12301006 03550403
  13096361 2D736572 76657230 819F300D 06092A86 4886F70D 01010105 0003818D
  00308189 02818100 DA4ECE09 B998F670 598F32C1 7E9FA920 1D217AC4 293B842E
  7563CE11 B2F0F822 23077930 636C8293 00F6CFDD F6C9B0F5 8348BE58 6478F631
  7D44152F 494AEBCC A507FA6B 408D6BBB FAAB0A7A 2E7546A8 CA70F9A6 0F7F6824
  554BD833 060D657D ABDF406C 69EEF449 7A4F9AFE 6F0852E7 05DEDAC1 D433191E
  712868C2 A94E642B 02030100 01A36330 61300F06 03551D13 0101FF04 05300301
  01FF300E 0603551D 0F0101FF 04040302 0186301F 0603551D 23041830 16801448
  71D9002C 66DFD85F ACB845D1 D25FEA35 74559130 1D060355 1D0E0416 04144871
  D9002C66 DFD85FAC B845D1D2 5FEA3574 5591300D 06092A86 4886F70D 01010405
  00038181 00AFC36B 8A917284 06BD51CB 83BDC4E8 9457A361 6CAAF416 3BBEF691
  04215AC5 EDBC5730 C071C2FB 8A6C90CF D6AB39C2 3BC2147F D35553D9 028B2155
  802E50DB 48CDE067 B3857447 89A1C733 D81EFEF7 1115480F 70ED2F22 F27E35A1
  F3BB597C 7C8F717B FAAD79D3 0F469702 DE9190E4 B1B0808E 46A118EB 887CEAEB
  DFE2900E D2
        quit
crypto ikev2 proposal prop-1
 encryption aes-cbc-128
 integrity sha1
 group 14
!
crypto ikev2 policy pol-1
 match fvrf any
```

```
 proposal prop-1
!
crypto ikev2 profile prof
 match fvrf any
 match certificate cmap-1
 identity local dn
 authentication local rsa-sig
 authentication remote pre-share
 authentication remote rsa-sig
 pki trustpoint ca-server
!
!
crypto ipsec transform-set trans esp-aes-cbc-128 esp-sha-hmac
!
crypto map cmap 1 ipsec-isakmp
 set peer 209.165.200.225
 set transform-set trans
 set ikev2-profile prof
 match address ikev2list
!
interface Loopback0
 ip address 209.165.200.226 255.255.255.224
!
interface Ethernet0/0
 ip address 209.165.200.227 255.255.255.224
 crypto map cmap
!
interface Ethernet1/0
 ip address 209.165.200.228 255.255.255.224
!
ip route 209.165.200.229 255.255.255.224 209.265.200.231
!
ip access-list extended ikev2list
 permit ip any any
!
```

応答側の設定は次のとおりです。

```
crypto pki trustpoint ca-server
 enrollment url http://10.1.1.3:80
 revocation-check none
!
!
!
crypto pki certificate map cmap-2 1
 subject-name eq hostname = initiator
!
crypto pki certificate chain ca-server
 certificate 03
  308201AF 30820118 A0030201 02020103 300D0609 2A864886 F70D0101 04050030
  14311230 10060355 04031309 63612D73 65727665 72301E17 0D313030 33313031
  32353231 325A170D 31313033 31303132 35323132 5A301A31 18301606 092A8648
  86F70D01 09021609 52455350 4F4E4445 52305C30 0D06092A 864886F7 0D010101
  0500034B 00304802 4100B517 EB8E64E1 B58CB014 07B3A6AF E6B69577 87486367
  9471B1DA BC66B847 DFA5073A 82121332 E787EA2D 3C433514 39033074 4095E7C7
  67A387A1 EBD24692 A76F0203 010001A3 4F304D30 0B060355 1D0F0404 030205A0
  301F0603 551D2304 18301680 144871D9 002C66DF D85FACB8 45D1D25F EA357455
  91301D06 03551D0E 04160414 DFF2401C 53276D96 89DE8C0A 786CCA71 C9EA792B
  300D0609 2A864886 F70D0101 04050003 8181002C 6E334273 CB832A95 3DDC6293
  669E416C A134D543 20952BC3 14A5C0B0 03AE011C 963AF523 C7C5C935 4FE9B2A5
  F24B3161 4D0D723A FA428BD1 85ADF172 B4007067 43C27D8A 1F74ED3D DEBE9F73
  1F515355 E77E766C AEACC303 39457991 29AB090C 99E21B5B 60DCB2C8 780B4479
  3EB3D46B B66C8C26 15311A7A B7A4ED97 32727C
        quit
```

```
 certificate ca 01
  30820201 3082016A A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  14311230 10060355 04031309 63612D73 65727665 72301E17 0D313030 33313031
  32343933 385A170D 31333033 30393132 34393338 5A301431 12301006 03550403
  13096361 2D736572 76657230 819F300D 06092A86 4886F70D 01010105 0003818D
  00308189 02818100 DA4ECE09 B998F670 598F32C1 7E9FA920 1D217AC4 293B842E
  7563CE11 B2F0F822 23077930 636C8293 00F6CFDD F6C9B0F5 8348BE58 6478F631
  7D44152F 494AEBCC A507FA6B 408D6BBB FAAB0A7A 2E7546A8 CA70F9A6 0F7F6824
  554BD833 060D657D ABDF406C 69EEF449 7A4F9AFE 6F0852E7 05DEDAC1 D433191E
  712868C2 A94E642B 02030100 01A36330 61300F06 03551D13 0101FF04 05300301
  01FF300E 0603551D 0F0101FF 04040302 0186301F 0603551D 23041830 16801448
  71D9002C 66DFD85F ACB845D1 D25FEA35 74559130 1D060355 1D0E0416 04144871
  D9002C66 DFD85FAC B845D1D2 5FEA3574 5591300D 06092A86 4886F70D 01010405
  00038181 00AFC36B 8A917284 06BD51CB 83BDC4E8 9457A361 6CAAF416 3BBEF691
  04215AC5 EDBC5730 C071C2FB 8A6C90CF D6AB39C2 3BC2147F D35553D9 028B2155
  802E50DB 48CDE067 B3857447 89A1C733 D81EFEF7 1115480F 70ED2F22 F27E35A1
  F3BB597C 7C8F717B FAAD79D3 0F469702 DE9190E4 B1B0808E 46A118EB 887CEAEB
  DFE2900E D2
        quit
crypto ikev2 proposal prop-1
 encryption aes-cbc-128
 integrity sha1
 group 14
!
crypto ikev2 policy pol-1
 match fvrf any
 proposal prop-1
!
!
crypto ikev2 profile prof
 match fvrf any
 match certificate cmap-2
 identity local dn
 authentication local rsa-sig
 authentication remote pre-share
 authentication remote rsa-sig
 pki trustpoint ca-server
!
!
crypto ipsec transform-set trans esp-aes-cbc-128 esp-sha-hmac
!
crypto dynamic-map dmap 1
 set transform-set trans
 set ikev2-profile prof
!
!
crypto map cmap 1 ipsec-isakmp dynamic dmap
interface Loopback0
 ip address 209.165.200.230 255.255.255.224
!
interface Ethernet0/0
 ip address 209.165.200.231 255.255.255.224
 crypto map cmap
!
interface Ethernet1/0
 ip address 209.165.200.232 255.255.255.224
!
ip route 209.165.200.233 255.255.255.224 209.165.200.228
!
ip access-list extended ikev2list
 permit ip host 209.165.200.231 host 209.165.200.228
```

CA サーバの設定は次のとおりです。

```
crypto pki server ca-server
 grant auto
!
crypto pki trustpoint ca-server
 revocation-check crl
 rsakeypair ca-server
!
!
crypto pki certificate chain ca-server
 certificate ca 01
  30820201 3082016A A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  14311230 10060355 04031309 63612D73 65727665 72301E17 0D303930 33303831
  36333335 395A170D 31323033 30373136 33333539 5A301431 12301006 03550403
  13096361 2D736572 76657230 819F300D 06092A86 4886F70D 01010105 0003818D
  00308189 02818100 99750598 EF4AF8B4 823DEF66 2F3BBA31 81C2DC5F D9B4040B
  99FB6020 22243CD6 B9F24C84 A543D7DB DD0B3018 2E36208C D0FD4015 EAF0DA69
  C1B0302B 87CEC34B 8646593F 0185AF02 0B86A3F3 5E5C3880 A992CD4A 79F13403
  411CC61F 07CEB4D9 0E967CB2 FAE0A899 5A3B6C87 73111F06 128465DA A45291F8
  F828C5DC 657487E7 02030100 01A36330 61300F06 03551D13 0101FF04 05300301
  01FF300E 0603551D 0F0101FF 04040302 0186301F 0603551D 23041830 1680147B
  D032BFB7 B3F70F1A 597B7C1E 1B42E472 5CCD6030 1D060355 1D0E0416 04147BD0
  32BFB7B3 F70F1A59 7B7C1E1B 42E4725C CD60300D 06092A86 4886F70D 01010405
  00038181 003838FA 628804EF E9FF69D9 3D5E299C 29074B2C AE33A563 8AF75976
  78FB68D4 5EF1E27B 04936FDF 78A09432 5348849D F79E17F5 70B233C9 2C1535D0
  506F0C35 99335012 84BBA3DC 050FD3C9 6E7B1D63 41ACC2B5 2B02432D BA2CC2CF
  E379DEA0 A9C208AC 0BEBB2D8 E6488815 EB12F1E0 19072D55 D5D11A49 739144D8
  271A842E ED
        quit
!
interface Ethernet1/0
 ip address 209.165.200.232 255.255.255.224
!
ip http server
```

CA およびデバイス証明書を取得するには、**crypto pki authenticate ca-server** コマンドおよび **crypto pki enroll ca-server** コマンドを入力します。発信側と応答側との接続を開始するには、発信側の CLI で次のコマンドを入力します。

```
ping 209.165.200.230 source 209.165.200.226
```

コマンドの出力は次のようになります。

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.230, timeout is 2 seconds:
Packet sent with a source address of 209.165.200.226
%IKEV2-5-OSAL_INITIATE_TUNNEL: Received request to establish an IPsec tunnel; local
traffic selector = Address Range: 209.165.200.226-209.165.200.226 Protocol: 1 Port Range:
 0-65535; remote traffic selector = Address Range: 209.165.200.230-209.165.200.230
Protocol: 1 Port Range: 0-65535
%IKEV2-5-SA_UP: SA UP
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 8/11/12 ms
```

セッションの詳細を表示するには、応答側の CLI に次の **show** コマンドを入力します。

```
show crypto session
Crypto session current status
Interface: Ethernet0/0
Session status: UP-ACTIVE
Peer: 1.1.1.1 port 500
```

```
  IKEv2 SA: local 209.165.200.231/500 remote 209.165.200.227/500 Active
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 host 209.165.200.226
        Active SAs: 2, origin: dynamic crypto map
show crypto ikev2 sa detailed
Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         209.165.200.231/500 209.165.200.227/500  (none)/(none)                  READY
      Encr: AES-CBC, Keysize: 128, Hash: SHA96, DH Grp:14, Auth sign: RSA, Auth verify:
 RSA
      Life/Active Time: 86400/846 sec
      CE id: 1001, Session-id: 1
      Status Description: Negotiation done
      Local spi: F79756E978ED41C7       Remote spi: 188FB9A119516D34
      Local id: hostname=RESPONDER
      Remote id: hostname=INITIATOR
      Local req msg id:  0              Remote req msg id:  2
      Local next msg id: 0              Remote next msg id: 2
      Local req queued:  0              Remote req queued:  2
      Local window:      5              Remote window:      5
      DPD configured for 0 seconds, retry 0
      NAT-T is not detected
```

例：暗号マップ ベースおよび dVTI ベースの IKEv2 ピアの設定

次の例は、スタティック クリプト マップ IKEv2 発信側と dVTI に基づく IKEv2 応答側との間に事前共有キー認証方式を使用し、クリプト マップと dVTI ベースの IKEv2 ピアを設定する方法を示します。発信側の設定は次のとおりです。

```
crypto ikev2 proposal prop-1
 encryption aes-cbc-128
 integrity sha1
 group 14
!
crypto ikev2 policy pol-1
 match fvrf any
 proposal prop-1
!
crypto ikev2 keyring v2-kr1
 peer abc
  address 0.0.0.0 0.0.0.0
  pre-shared-key abc
 !
!
!
crypto ikev2 profile prof
 match fvrf any
 match identity remote address 0.0.0.0
 authentication local pre-share
 authentication remote pre-share
 keyring v2-kr1
!
crypto ipsec transform-set trans esp-aes-cbc-128 esp-sha-hmac
!
crypto map cmap 1 ipsec-isakmp
 set peer 206.165.200.235
 set transform-set trans
 set ikev2-profile prof
 match address ikev2list
```

```
!
interface Loopback0
 ip address 206.165.200.226 255.255.255.224
!
interface Ethernet0/0
 ip address 206.165.200.227 255.255.255.224
 crypto map cmap
!
ip route 206.165.200.229 255.255.255.224 206.165.200.235
!
ip access-list extended ikev2list
 permit ip host 206.165.200.227 host 206.165.200.235
 permit ip 206.165.200.233 255.255.255.224 206.165.200.229 255.255.255.224
```

応答側の設定は次のとおりです。

```
crypto ikev2 proposal prop-1
 encryption aes-cbc-128
 integrity sha1
 group 14
!
crypto ikev2 policy pol-1
 match fvrf any
 proposal prop-1
!
crypto ikev2 keyring v2-kr1
 peer cisco
  address 0.0.0.0 0.0.0.0
  pre-shared-key cisco
 !
!
!
crypto ikev2 profile prof
 match fvrf any
 match identity remote address 0.0.0.0
 authentication local pre-share
 authentication remote pre-share
 keyring v2-kr1
 virtual-template 1
!
crypto ipsec transform-set set esp-aes-cbc-128 esp-sha-hmac
!
crypto ipsec profile vi
 set transform-set set
 set ikev2-profile prof
!
interface Loopback0
 ip address 206.165.200.230 255.255.255.224
!
interface Ethernet0/0
 ip address 206.165.200.235 255.255.255.224
!
interface Virtual-Template1 type tunnel
 ip unnumbered Ethernet0/0
 ip mtu 1000
 tunnel source Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile vi
!
```

発信側と応答側との接続を開始するには、発信側の CLI で次のコマンドを入力します。

```
ping 206.165.200.230 source 206.165.200.226
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 206.165.200.230, timeout is 2 seconds:
Packet sent with a source address of 206.165.200.226
%IKEV2-5-OSAL_INITIATE_TUNNEL: Received request to establish an IPsec tunnel; local
traffic selector = Address Range: 206.165.200.226-206.165.200.226 Protocol: 1 Port Range:
 0-65535; remote traffic selector = Address Range: 206.165.200.230-206.165.200.230
Protocol: 1 Port Range: 0-65535
%IKEV2-5-SA_UP: SA UP
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 8/11/12 ms
```

次の **show** コマンドを Easy VPN サーバに入力すると、セッションの詳細が表示されます。

```
show crypto session
Crypto session current status
Interface: Virtual-Access2
Session status: UP-ACTIVE
Peer: 206.165.200.227 port 500
  IKEv2 SA: local 206.165.200.235/500 remote 206.165.200.227/500 Active
  IPSEC FLOW: permit ip 206.165.200.229/255.255.255.224 206.165.200.233/255.255.255.224
        Active SAs: 2, origin: crypto map
show crypto ikev2 sa detail
Tunnel-id Local                 Remote                fvrf/ivrf            Status
1   206.165.200.235/500      206.165.200.227/500       (none)/(none)         READY
      Encr: AES-CBC, Keysize: 128, Hash: SHA96, DH Grp: 14, Auth sign: PSK, Auth verify:
 PSK
      Life/Active Time: 86400/8 sec
      CE id: 1001, Session-id: 1
      Status Description: Negotiation done
      Local spi: 305F610F57428834       Remote spi: D9D183B5689AEDCD
      Local id: 206.165.200.235
      Remote id: 206.165.200.227
      Local req msg id:  0              Remote req msg id:  2
      Local next msg id: 0              Remote next msg id: 2
      Local req queued:  0              Remote req queued:  2
      Local window:      5              Remote window:      5
      DPD configured for 0 seconds, retry 0
      NAT-T is not detected
show crypto route
VPN Routing Table: Shows RRI and VTI created routes
Codes: RRI - Reverse-Route, VTI- Virtual Tunnel Interface
        S - Static Map ACLs
Routes created in table GLOBAL DEFAULT
206.165.200.233/255.255.255.224 [1/0] via 206.165.200.227 tag 0
                                on Virtual-Access2 RRI
```

例： sVTI ベース IKEv2 ピアを使用した IPSec の設定

次の例は、sVTI IKEv2 発信側と sVTI IKEv2 応答側との間に事前共有キー認証方式を使用する IPsec の設定方法を示します。発信側の設定は次のとおりです。

```
crypto ikev2 proposal prop-1
 encryption aes-cbc-128
 integrity sha1
 group 14
!
crypto ikev2 policy pol-1
 match fvrf any
 proposal prop-1
```

```
!
crypto ikev2 keyring v2-kr1
 peer abc
  address 209.165.200.225
  pre-shared-key abc
 !
!
!
crypto ikev2 profile prof
 match fvrf any
 match identity remote address 209.165.200.231 255.255.255.224
 authentication local pre-share
 authentication remote pre-share
 keyring v2-kr1
!
!
crypto ipsec transform-set trans esp-aes-cbc-128 esp-sha-hmac
!
crypto ipsec profile ipsecprof
 set transform-set trans
 set ikev2-profile prof
!
interface Loopback0
 ip address 209.165.200.226 255.255.255.224
!
interface Tunnel0
 ip address 10.0.0.1 255.255.255.0
 tunnel source 209.165.200.231
 tunnel mode ipsec ipv4
 tunnel destination 209.165.200.225
 tunnel protection ipsec profile ipsecprof
!
interface Ethernet0/0
 ip address 209.165.200.231 255.255.255.224
!
ip route 209.165.200.229 255.255.255.224 Tunnel0
!
```

応答側の設定は次のとおりです。

```
crypto ikev2 proposal prop-1
 encryption aes-cbc-128
 integrity sha1
 group 14
!
crypto ikev2 policy pol-1
 match fvrf any
 proposal prop-1
!
crypto ikev2 keyring v2-kr1
 peer abc
  address 209.165.200.231
  pre-shared-key abc
 !
!
!
crypto ikev2 profile prof
 match fvrf any
 match identity remote address 209.165.200.231 255.255.255.224
 authentication local pre-share
 authentication remote pre-share
 keyring v2-kr1
!
!
```

```
crypto ipsec transform-set trans esp-aes-cbc-128 esp-sha-hmac
!
crypto ipsec profile ipsecprof
 set transform-set trans
 set ikev2-profile prof
!
crypto map cmap 1 ipsec-isakmp dynamic dmap
!
interface Loopback0
 ip address 209.165.200.230 255.255.255.224
!
interface Tunnel0
 ip address 10.0.0.2 255.255.255.0
 tunnel source 209.165.200.225
 tunnel mode ipsec ipv4
 tunnel destination 209.165.200.231
 tunnel protection ipsec profile ipsecprof
!
interface Ethernet0/0
 ip address 209.165.200.231 255.255.255.224
!
ip route 209.165.200.233 255.255.255.224 Tunnel0
```

IKEv2 ピアの sVTI では、セッションは sVTI インターフェイスが有効なときにだけ開始されます。つまり、セッションの開始のためにネットワーク トラフィックは必要ありません。発信側と応答側との間のトラフィックを確認するには、発信側の CLI で次のコマンドを入力します。

```
ping 209.165.200.230 source 209.165.200.226
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.230, timeout is 2 seconds:
Packet sent with a source address of 209.165.200.226
%IKEV2-5-OSAL_INITIATE_TUNNEL: Received request to establish an IPsec tunnel; local
traffic selector = Address Range: 209.165.200.226-209.165.200.226 Protocol: 1 Port Range:
 0-65535; remote traffic selector = Address Range: 209.165.200.230-209.165.200.23 Protocol:
 1 Port Range: 0-65535
%IKEV2-5-SA_UP: SA UP
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 8/11/12 ms
```

次の **show** コマンドを発信側の CLI に入力すると、セッションの詳細が表示されます。

```
show crypto session
Crypto session current status
Interface: Ethernet0/0
Session status: UP-ACTIVE
Peer: 209.165.200.225 port 500
  IKEv2 SA: local 209.165.200.231/500 remote 209.165.200.225/500 Active
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map
show crypto ikev2 sa detailed
Tunnel-id Local                 Remote                fvrf/ivrf            Status
1   209.165.200.231/500  209.165.200.225/500           (none)/(none)        READY
      Encr: AES-CBC, Keysize: 128, Hash: SHA96, DH Grp: 14, Auth sign: PSK, Auth verify:
 PSK
      Life/Active Time: 86400/21 sec
      CE id: 1002, Session-id: 2
      Status Description: Negotiation done
      Local spi: 687752902752A6FD       Remote spi: C9DCCFC65493D14F
      Local id: smap-initiator
      Remote id: dmap-responder
      Local req msg id:  2              Remote req msg id:  0
      Local next msg id: 2              Remote next msg id: 0
```

```
      Local req queued:  2              Remote req queued:  0
      Local window:      5              Remote window:      5
      DPD configured for 0 seconds, retry 0
      NAT-T is not detected
```

例：DMVPN ネットワークでの IKEv2 の設定

DMVPN は、IKEv1 と IKEv2 の間で同一のトンネル保護 CLI を使用します。DMVPN トンネルに適用される IPSec プロファイルは、IKEv2 プロファイルのみを参照します。DMVPN ハブの設定は次のとおりです。

```
crypto ikev2 keyring cisco-ikev2-keyring
 peer dmvpn-node
 description symmetric pre-shared key for the hub/spoke
 address 0.0.0.0 0.0.0.0
 pre-shared-key cisco123
crypto ikev2 profile cisco-ikev2-profile
 keyring cisco-ikev2-keyring
 authentication pre-shared
 match local address 0.0.0.0
crypto ipsec profile cisco-ipsec-ikev2
 set transform-set cisco-ts
 set ikev2-profile cisco-ikev2-profile
! interface Tunnel 0
 description This is the Legacy IKEv1 facing tunnel on the hub
 ip address 1.1.1.99 255.255.255.0
 no ip redirects
 ip nhrp map multicast dynamic
 ip nhrp network-id 99
 ip nhrp redirect
 no ip split-horizon eigrp 1
 tunnel source Ethernet0/0
 tunnel mode gre multipoint
 tunnel protection ipsec profile cisco-ipsec
 !
interface Tunnel1
 description This would be the new IKEv2 facing tunnel on the hub
 ip address 2.2.2.99 255.255.255.0
 no ip redirects
 ip nhrp map multicast dynamic
 ip nhrp network-id 100
 no ip split-horizon eigrp 1
 tunnel source Ethernet0/1
 tunnel mode gre multipoint
 tunnel protection ipsec profile cisco-ipsec-ikev2
```

IKEv2 の設定は次のとおりです。

```
crypto ikev2 profile cisco-ikev2-profile
 keyring cisco-ikev2-keyring
 authentication pre-shared
 match local address 0.0.0.0
crypto ipsec profile cisco-ipsec-ikev2
 set transform-set cisco-ts
 set ikev2-profile cisco-ikev2-profile
interface Tunnel1
 ip address 2.2.2.11 255.255.255.0
 no ip redirects
 ip nhrp map 2.2.2.99 22.22.22.99
```

```
ip nhrp map multicast 22.22.22.99
ip nhrp network-id 100 ? Keep this same for all IKEv2 spokes for clarity
ip nhrp nhs 2.2.2.99 ? This points to the hub's IKEv2 facing interface
tunnel source Ethernet0/1
tunnel mode gre multipoint
tunnel protection ipsec profile cisco-ipsec-ikev2
```