

Cisco VPN 5000 Concentrator シリーズのための 仮想プライベートネットワークおよびインター ネット鍵交換

目次

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[IKE タスク](#)

[認証](#)

[セッション ネゴシエーション](#)

[キー交換](#)

[IPSec トンネル ネゴシエーションおよび設定](#)

[VPN 5000 コンセントレータの IKE 拡張](#)

[ISAKMP およびOakley](#)

[STEP およびSTAMP](#)

[関連情報](#)

[はじめに](#)

インターネット キー交換 (IKE) は、安全で認証された通信の基盤となる標準的な方法です。Cisco VPN 5000 コンセントレータは IKE を使用して、IPSec トンネルを設定します。それらの IPSec トンネルが、この製品のバックボーンです。

[前提条件](#)

[要件](#)

このドキュメントに関しては個別の要件はありません。

[使用するコンポーネント](#)

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- VPN 5000 シリーズ コンセントレータ

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してくだ

さい。

表記法

ドキュメント表記の詳細は、『[シスコ テクニカル ティップスの表記法](#)』を参照してください。

IKE タスク

IKE は、次のタスクを処理します。

- [認証](#)
- [セッション ネゴシエーション](#)
- [キー交換](#)
- [IPSec トンネル ネゴシエーションおよび設定](#)

認証

認証は、IKE が実現する、最も複雑で重要な作業です。ネゴシエートするときは常に、ネゴシエートする相手がわかっていることが重要です。IKE は、複数の方式の 1 つを使用して、交渉の当事者が相互に認証するようにします。

- **共有キー**：IKE はハッシュ技術を使用して、同じキーを持つユーザだけが IKE パケットを送信できるようにします。
- **デジタル署名規格 (DSS) または Rivest, Shamir, Adelman (RSA) デジタル署名**：IKE は公開キー デジタル署名暗号化を使用して、各当事者が示している自身の識別情報を確認します。
- **RSA 暗号化**：IKE は、2 つの方法のいずれかを使用してネゴシエーションに十分な暗号化を行い、正しい秘密キーを持つ当事者だけがネゴシエーションを続行できるようにします。

セッション ネゴシエーション

セッション ネゴシエーション中に IKE は、当事者が認証を行う方法と、将来のネゴシエーション (つまり、IPSec トンネル ネゴシエーション) を保護する方法をネゴシエートすることを許可します。次の項目が、ネゴシエートされます。

- **認証方式**：これは、このドキュメントの「[認証](#)」の項に記載されている方法の 1 つです。
- **キー交換アルゴリズム**：これは、公衆メディア (Diffie-Hellman) 上で安全に暗号キーを交換するための数学的技術です。キーは、暗号化およびパケット署名アルゴリズムで使用されます。
- **暗号化アルゴリズム**：データ暗号規格 (DES) またはトリプル DES (3DES) 。
- **パケット署名アルゴリズム**：Message Digest 5 (MD5) および Secure Hash Algorithm 1 (SHA-1) 。

キー交換

IKE は、ネゴシエートされたキー交換方法 (このドキュメントの「[セッション ネゴシエーション](#)」の項を参照) を使用して、暗号化キー関連情報の十分なビットを作成し、将来のトランザクションを保護します。この方式により、各 IKE セッションが新しい安全なキーのセットで確実に保

護されます。

認証、セッション ネゴシエーション、およびキー交換で、IKE ネゴシエーションのフェーズ 1 が構成されます。VPN 5000 コンセントレータでは、これらのプロパティが、Protection キーワードを使用して [IKE Policy] セクションで設定されます。このキーワードは、認証アルゴリズム、暗号化アルゴリズム、キー交換アルゴリズムという 3 つ要素を持つラベルです。これらの要素はアンダースコアで区切られています。ラベル MD5_DES_G1 は、IKE パケット認証に MD5 を、IKE パケット暗号化に DES を、キー交換に Diffie-Hellman グループ 1 を使用することを意味します。詳細については、「[IPSec トンネル セキュリティの IKE ポリシーの設定](#)」を参照してください。

[IPSec トンネル ネゴシエーションおよび設定](#)

IKE は、情報を交換するための安全な方法のネゴシエートを完了した (フェーズ 1) 後、IPsec トンネルをネゴシエートするために使用されます。これは、IKE フェーズ 2 を使用して行われます。この交換では、使用する IPsec トンネルの新しいキー関連情報を IKE が (ベースとして IKE フェーズ 1 キーを使用して、または新しいキー交換を実行して) 作成します。このトンネルの暗号化と認証のアルゴリズムも、ネゴシエートされます。

IPsec トンネルは、VPN Client トンネルの VPN グループ (以前の Secure Tunnel Establishment Protocol (STEP) クライアント) セクションと、LAN-to-LAN トンネルのトンネル パートナー セクションを使用して設定されます。各ユーザの認証方式が格納されるのは、VPN Users セクションです。これらのセクションについては、「[IPSec トンネル セキュリティの IKE ポリシーの設定](#)」で説明しています。

[VPN 5000 コンセントレータの IKE 拡張](#)

- **RADIUS** : IKE は、RADIUS 認証をサポートしていません。RADIUS 認証は、VPN Client からの最初の IKE パケットの後に発生する特別な情報交換で実行されます。パスワード認証プロトコル (PAP) が必要な場合は、特別な RADIUS 認証のシークレットが必要です。詳細については、「[IPSec トンネル セキュリティの IKE ポリシーの設定](#)」にある、NoCHAP と PAPAuthSecret の説明を参照してください。RADIUS 認証は、認証され、暗号化されます。PAP 交換は PAPAuthSecret によって保護されます。ただし、このようなシークレットがあるのは、IntraPort 全体で 1 つだけであるため、保護は、共有パスワードと同様に脆弱です。
- **SecurID** : IKE は、現時点では SecurID 認証をサポートしていません。SecurID 認証は、フェーズ 1 とフェーズ 2 の間の特別な情報交換で実行されます。この交換は、フェーズ 1 でネゴシエートされる IKE セキュリティ アソシエーション (SA) によって完全に保護されます。
- **Secure Tunnel Access Management Protocol (STAMP)** : VPN Client が IKE プロセス中に IntraPort と接続情報を交換します。シークレットを保存してもよいかどうか、どの IP ネットワークをトンネリングするか、Internetwork Packet Exchange (IPX) トラフィックをトンネリングするかどうかなどの情報が、最後の 2 個の IKE パケット中のプライベートペイロードで送信されます。これらのペイロードは、互換性のある VPN Client にだけ送信されます。

[ISAKMP およびOakley](#)

Internet Security Association and Key Management Protocol (ISAKMP) は、インターネット上でネゴシエーションを行う (IP プロトコルを使用して、など) ために使用される言語です。

Oakley とは、暗号キー関連情報の認証済み交換の実行方法です。IKE は、この 2 つを 1 個のパッケージにまとめ、安全ではないインターネット経由で安全な接続を確立できるようにします。

STEP および STAMP

Secure Tunnel Establishment Protocol (STEP) は、VPN システムの以前の名前です。IKE が使用される前は、STAMP を使用して IPSec 接続をネゴシエートしていました。3.0 より前の VPN Client バージョンは、STAMP を使用して、IntraPort との接続を確立します。

関連情報

- [Cisco VPN 5000 シリーズ コンセントレータの販売終了の発表](#)
- [ルータおよび VPN 5000 シリーズ コンセントレータ LAN-to-LAN トンネル設定](#)
- [Cisco VPN 5000 コンセントレータ製品に関するサポート ページ](#)
- [Cisco VPN 5000 クライアント製品に関するサポート ページ](#)
- [IPSec ネゴシエーション/IKE プロトコル テクノロジーに関するサポート](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)