IKEv2 パケット交換とプロトコル レベルのデバッグ

内容

概要

このドキュメントでは、最新バージョンのインターネットキーエクスチェンジ（IKE）のメリットと、バージョン 1 とバージョン 2 の相違点について説明します。

IKE は、IPsec プロトコル スイートでセキュリティ アソシエーション（SA）を設定するために使用するプロトコルです。IKEv2 は、IKE プロトコルの第 2 バージョンであり、最新バージョンです。このプロトコルは 2006 年から採用されています。IKE プロトコルの徹底的な見直しの必要性とその意図については、RFC 4306 の「*Internet Key Exchange (IKEv2) Protocol*」の付録 A を参照してください。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

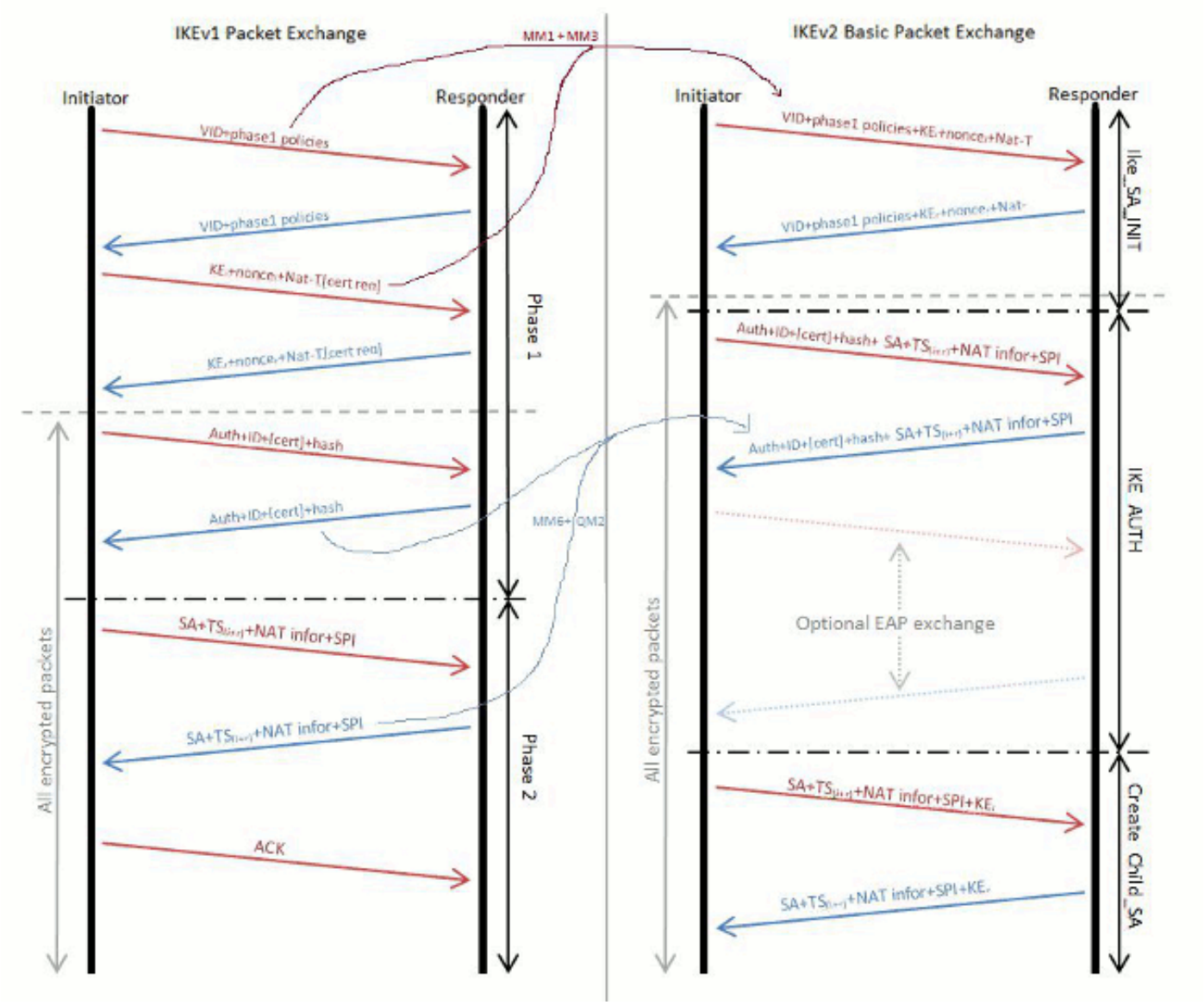
このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

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。

IKEv1 と IKEv2 の相違点

RFC 4306 の「*Internet Key Exchange (IKEv2) Protocol*」では、IKEv1 と比較した場合の IKEv2 の長所について詳しく説明されていますが、IKE の交換全体が徹底的に見直されたことに注意してください。次の図は、この 2 つの交換を比較したものです。



IKEv1 の場合は、境界が明確なフェーズ 1 交換があり、これには 6 個のパケットが含まれます。それに続くフェーズ 2 交換は 3 つのパケットで構成されます。IKEv2 の交換では変動します。最も良い場合は、パケットが 4 個しか交換されません。最も悪い場合は、認証の複雑さ、使用される Extensible Authentication Protocol（EAP）属性の数、形成される SA の数により、パケットが 30 個以上に増加することがあります。IKEv2 では、IKEv1 のフェーズ 2 の情報が IKE_AUTH 交換と組み合わされ、IKE_AUTH 交換が完了した後で、両方のピアに 1 つの SA が構築されてトラフィックを暗号化する準備が整います。この SA は、トリガー パケットと一致するプロキシ アイデンティティのみに構築されます。その後、他のプロキシIDと一致する後続のトラフィックがCREATE_CHILD_SA交換をトリガーします。これは、IKEv1のフェーズ2交換と同等です。アグレッシブモードまたはメインモードはありません。

IKEv2 交換の初期フェーズ

実質的に、IKEv2 には、ネゴシエーションの初期フェーズが 2 つしかありません。

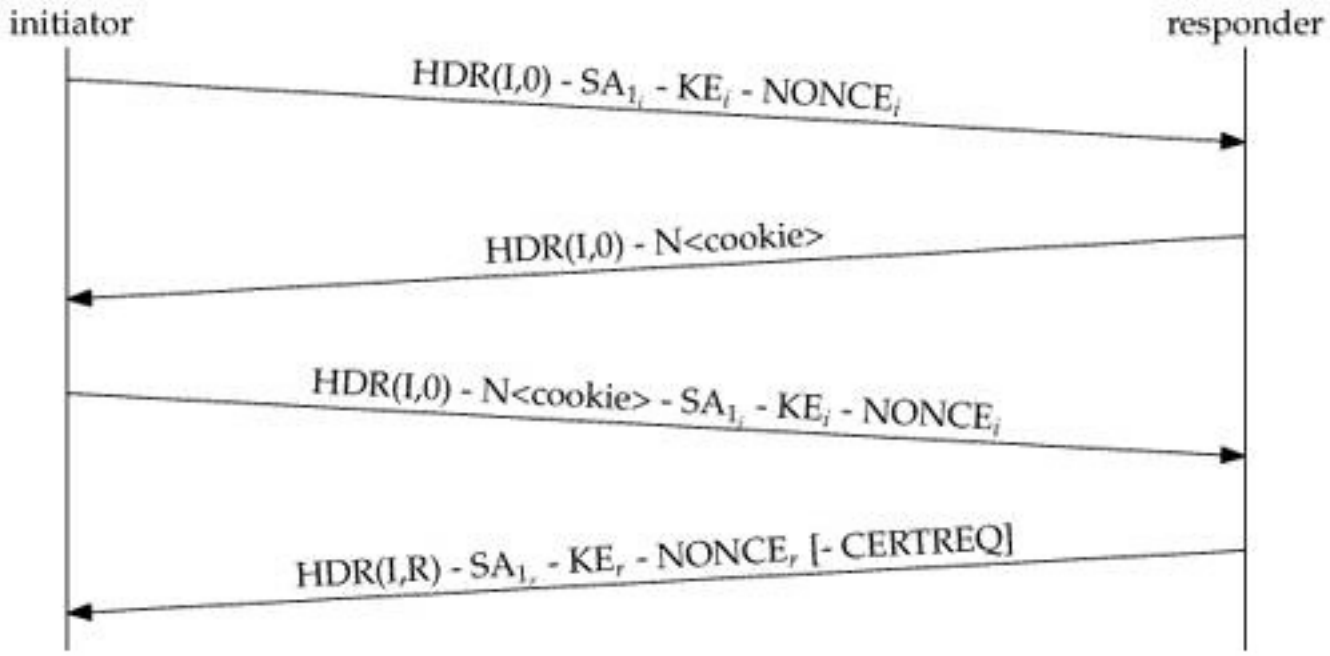
- IKE_SA_INIT 交換
- IKE_AUTH 交換

IKE_SA_INIT 交換

IKE_SA_INIT は初期交換であり、ピアが安全なチャネルを確立します。初期交換が完了すると、その後のすべての交換は暗号化されます。交換には2つのパケットしか含まれません。これは、IKEv1のMM1-4で通常交換されるすべての情報が結合されるためです。そのため、応答側はIKE_SA_INITパケットを処理するために計算的にコストがかかり、最初のパケットを処理するために残ることができます。これにより、プロトコルは、スプーフィングされたアドレスから DOS 攻撃を受けやすくなります。

この種の攻撃から保護するため、IKEv2 では、IKE_SA_INIT 内にオプションの交換があり、スプーフィング攻撃が防止されます。未完了セッションの特定のしきい値に達すると、応答側はパケットをそれ以上処理しなくなりますが、その代わりに Cookie を使用してイニシエータに応答を送信します。セッションを続けるには、イニシエータが IKE_SA_INIT パケットを再送信し、受信した Cookie を含める必要があります。

イニシエータは、元の交換がスプーフィングされていないことを証明する、応答側からの通知ペイロードとともに初期パケットを再送信します。以下は、Cookie チャレンジを含む IKE_SA_INIT 交換の図です。



IKE_AUTH 交換

IKE_SA_INIT 交換の完了後、IKEv2 SA は暗号化されます。ただし、リモート ピアは認証されていません。リモート ピアを認証して最初の IPsec SA を作成するには、IKE_AUTH 交換を使用します。

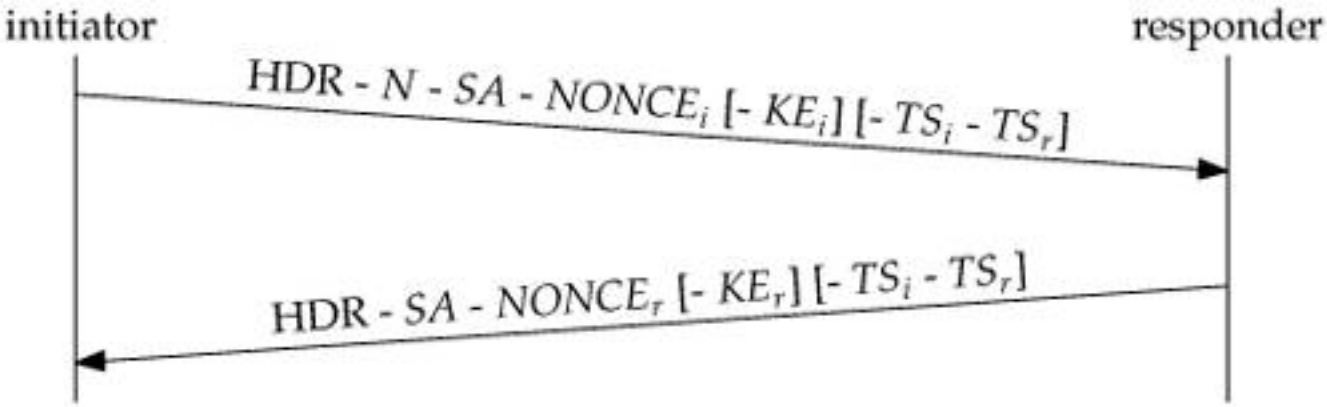
この交換には、Internet Security Association and Key Management Protocol（ISAKMP）ID および認証ペイロードが含まれます。認証ペイロードの内容は認証方式によって決まります。認証方式は、事前共有鍵（PSK）、RSA 証明書（RSA-SIG）、楕円曲線デジタル署名アルゴリズム証明書（ECDSA-SIG）、EAP のいずれかにすることができます。交換には、認証ペイロードに加えて、作成する IPsec SA について記述する SA ペイロードとトラフィック セレクタ ペイロードが

含まれます。

その後の IKEv2 交換

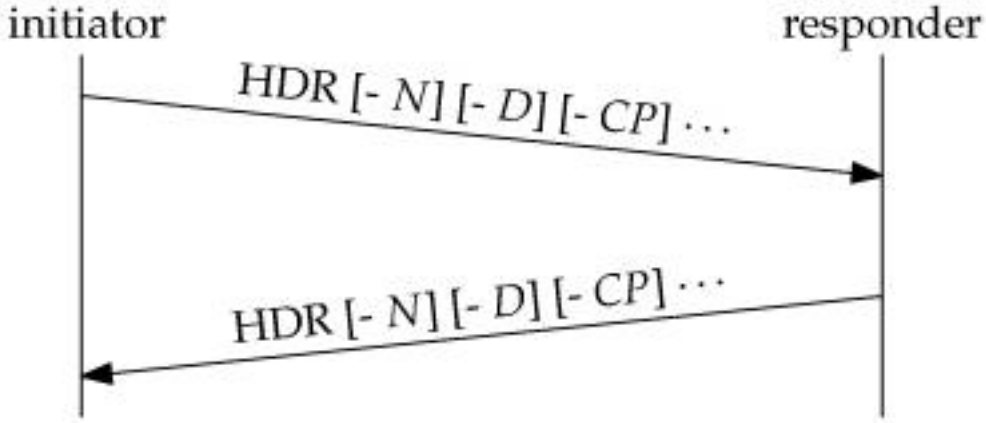
CREATE_CHILD_SA 交換

追加の子SAが必要な場合、またはIKE SAまたは子SAの1つを再鍵付けする必要がある場合は、IKEv1でクイックモード交換が実行するのと同じ機能を果たします。次の図に示すように、この交換には2つのパケットがあります。ただし、交換は鍵の再生成ごとまたは新しい SA ごとに繰り返されます。



INFORMATIONAL の交換

すべての IKEv2 交換と同じように、それぞれの INFORMATIONAL 交換要求では応答が期待されます。INFORMATIONAL 交換には、3 種類のペイロードが含まれることがあります。次の図で示すように、任意の数の任意の組み合わせのペイロードを含めることができます。



- 通知ペイロード (N) については、Cookie と合わせてすでに説明しました。その他にもいくつかの種類があります。IKEv1 と同じように、エラー情報とステータス情報が運ばれます。
- 削除ペイロード (D) は、送信側が 1 つ以上の着信 SA を削除したことをピアに通知します。応答側はその SA を削除することが期待され、通常、反対方向の対応する SA の削除ペイロードを応答メッセージに組み込みます。
- ピア間で設定データをネゴシエートするには、設定ペイロード (CP) を使用します。CP の重要な用途の 1 つは、セキュリティ ゲートウェイによって保護されているネットワークのアドレスを要求 (リクエスト) して割り当てる (応答する) ことです。一般的な状況では、モバイル ホストがホーム ネットワークでセキュリティ ゲートウェイを使用してバーチャル プライベート ネットワーク (VPN) を確立し、ホーム ネットワークで IP アドレスを取得する

ことを要求します。**注：これ**により、レイヤ2トンネリングプロトコル(L2TP)とIPsecの組み合わせで解決する問題の1つが解消されます。

関連情報

- PSK によるサイト間 VPN の ASA IKEv2 デバッグ テクニカルノート
- ASA IPsec および IKE のデバッグ (IKEv1 メイン モード) のトラブルシューティング テクニカルノート
- IOS IPSec および IKE のデバッグ (IKEv1 メイン モード) のトラブルシューティング テクニカルノート
- ASA IPSec および IKE デバッグ：IKEv1 アグレッシブ モード テクニカルノート
- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス
- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスのソフトウェア ダウンロード
- IPSec ネゴシエーション/IKE プロトコル
- Cisco IOS ファイアウォール
- Cisco IOS ソフトウェア
- セキュア シェル (SSH)
- IPSec ネゴシエーション/IKE プロトコル
- テクニカル サポートとドキュメント – Cisco Systems