IPsec IKEv1 プロトコルについて

内容

はじめに

前提条件

- 要件
- 使用するコンポーネント
- 背景説明

IPSec

IKEプロトコル

- IKEフェーズ

IKEモード（フェーズ1）

- Main Mode
- アグレッシブ モード

IPsecモード（フェーズ2）

- Quick Mode

IKE用語集

メインモードパケット交換

- メインモード1(MM1)
- 2つの同時ネゴシエーションの識別
- メインモード2 (MM2)
- メインモード3および4(MM3-MM4)
- メインモード5および6(MM5-MM6)

クイックモード（QM1、QM2、およびQM3）

アグレッシブモードのパケット交換

メインモードとアグレッシブモード

IKEv2とIKEv1のパケット交換

ポリシーベースとルートベース

- ポリシーベースVPN
- ルートベースのVPN

VPN経由で受信しないトラフィックの一般的な問題

- ISPがUDP 500/4500をブロック
- ISPによるESPのブロック

関連情報

はじめに

このドキュメントでは、バーチャルプライベートネットワーク(VPN)を確立するためのインターネットキーエクスチェンジ(IKEv1)プロトコルプロセスについて説明します。

前提条件

要件

基本的なセキュリティの概念に関する知識があることが推奨されます。

- [Authentication]
- 機密保持
- 整合性
- IPSec

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。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

バーチャルプライベートネットワーク(VPN)を確立するためのインターネットキーエクスチェンジ(IKEv1)プロトコルプロセスは、IKEv1のあらゆる種類のインターネットプロトコルセキュリティ(IPsec)の問題のトラブルシューティングを簡略化するためのパケット交換を理解することが重要です。

IPSec

IPsecは、IP層でインターネット通信にセキュリティを提供するプロトコルスイートです。現在IPsecが最もよく使用されているのは、2つの場所の間（ゲートウェイ間）またはリモートユーザと企業ネットワークの間（ホストとゲートウェイ間）でバーチャルプライベートネットワーク(VPN)を提供する場合です。

IKEプロトコル

IPsecはIKEプロトコルを使用して、セキュリティ保護されたサイト間またはリモートアクセス仮想プライベートネットワーク(VPN)トンネルをネゴシエートおよび確立します。IKEプロトコルは、Internet Security Association and Key Management Protocol(ISAKMP)（シスコのみ）とも呼ばれます。

IKEには次の2つのバージョンがあります。

- IKEv1:RFC 2409、Internet Key Exchange(IKEv1)
- IKEバージョン2(IKEv2):RFC 4306、インターネットキーエクスチェンジ(IKEv2)プロトコル

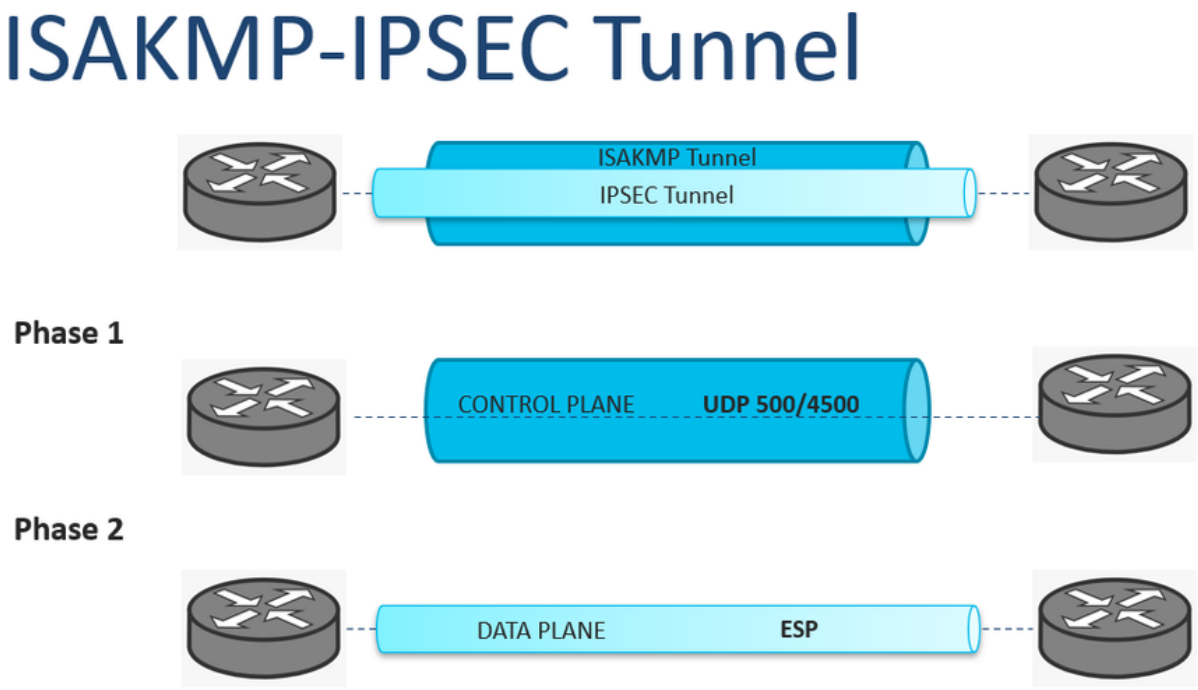
で定義

IKEフェーズ

ISAKMPはネゴシエーションを2つのフェーズに分けます。

- フェーズ1:2つのISAKMPピアがセキュアで認証済みのトンネルを確立し、ISAKMPネゴシエーションメッセージを保護します。このトンネルはISAKMP SAと呼ばれます。ISAKMPでは、メインモード(MM)とアグレッシブモードの2つのモードが定義されています。
- フェーズ2:IPSecトンネルを介して転送されるデータの暗号化(SA)に関する主要な資料とアルゴリズムをネゴシエートします。この段階をクイックモードと呼びます。

すべての抽象的な概念を具現化するために、フェーズ1トンネルは親トンネルであり、フェーズ2はサブトンネルです。次の図は、トンネルとしての2つのフェーズを示しています。



注：フェーズ1(ISAKMP)トンネルは、2つのゲートウェイ間のコントロールプレーンVPNトラフィックを保護します。コントロールプレーントラフィックには、ネゴシエーションパケット、情報パッケージ、DPD、キープアライブ、キー再生成などがあります。ISAKMPネゴシエーションでは、UDP 500および4500ポートを使用してセキュアなチャネルが確立されます。

注：フェーズ2(IPsec)トンネルは、2つのゲートウェイ間のVPNを通過するデータプレーントラフィックを保護します。データの保護に使用されるアルゴリズムはフェーズ2で設定され、フェーズ1で指定されたアルゴリズムとは独立しています。
これらのパケットのカプセル化と暗号化に使用されるプロトコルは、Encapsulation Security Payload(ESP)です。

IKEモード（フェーズ1）

Main Mode

イニシエータがレスポンダにプロポーザルを送信すると、IKEセッションが開始されます。ノード間の最初の交換によって基本的なセキュリティポリシーが確立され、イニシエータは使用する暗号化アルゴリズムと認証アルゴリズムを提示します。レスポンダは適切なプロポーザルを選択し（プロポーザルが選択されているとします）、そのプロポーザルをイニシエータに送信します。次の交換では、Diffie-Hellman(DH)公開キーとその他のデータが渡されます。以降のネゴシエーションはすべてIKE SA内で暗号化されます。3番目の交換は、ISAKMPセッションを認証します。IKE SAが確立されると、IPSecネゴシエーション（クイックモード）が開始されます。

アグレッシブ モード

アグレッシブモードでは、IKE SAネゴシエーションが3つのパケットに絞られ、SAに必要なすべてのデータがイニシエータから受け渡されます。レスポンダはプロポーザル、キーマテリアル、およびIDを送信し、次のパケットでセッションを認証します。イニシエータが応答し、セッションを認証します。ネゴシエーションが高速になり、発信側と応答側のIDがクリアテキストで渡されます。

IPsecモード（フェーズ2）

Quick Mode

IPSecネゴシエーション（クイックモード）はアグレッシブモードのIKEネゴシエーションに似ていますが、ネゴシエーションを除き、IKE SA内で保護する必要があります。クイックモードは、データ暗号化のSAをネゴシエートし、そのIPSec SAのキー交換を管理します。

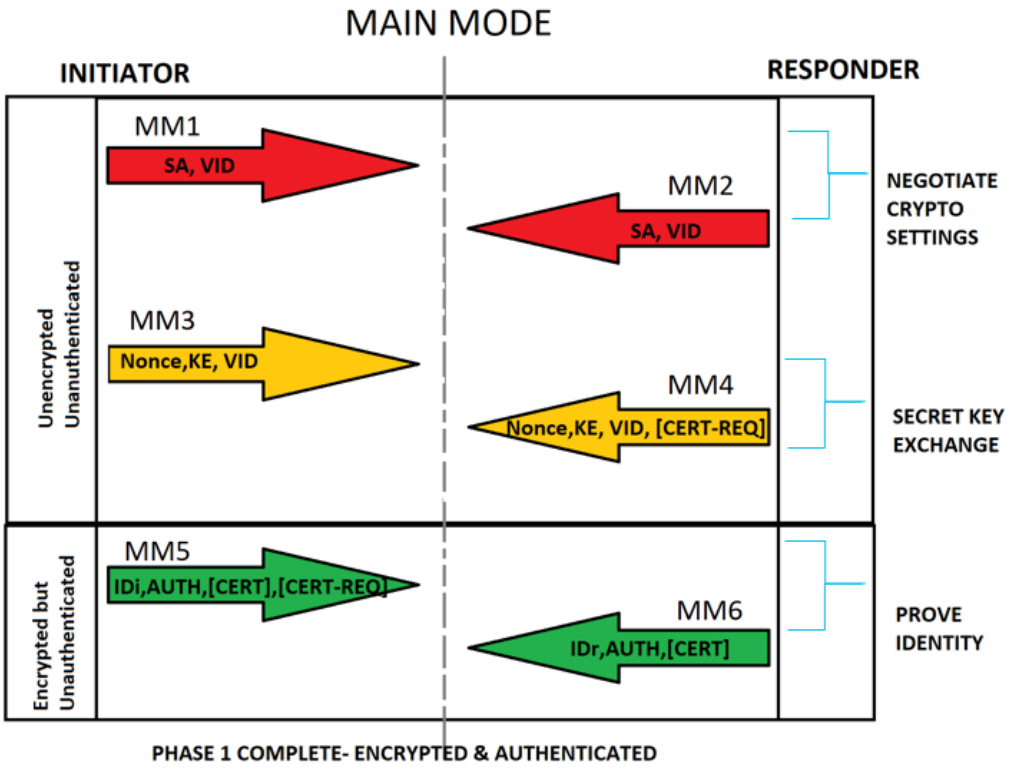
IKE用語集

- セキュリティアソシエーション(SA)は、セキュアな通信をサポートするために2つのネットワークエンティティ間で共有セキュリティ属性を確立することです。SAには、暗号化アルゴリズムとモード、トラフィック暗号化キー、接続を介して渡されるネットワークデータのパラメータなどの属性が含まれます。
- ベンダーID(VID)は、ピアがNATトラバーサル、デッドピア検出機能、フラグメンテーションなどをサポートしているかどうかを判断するために処理されます。
- ナンス：発信側が送信するランダムに生成された番号。このナンスは、合意したキーを使用して他の項目とともにハッシュされ、返送されます。イニシエータはcookieとナンスをチェックし、正しいナンスを持たないメッセージを拒否します。これにより、ランダムに生成されたナンスが何であるかをサードパーティが予測できないため、リプレイが防止されます。
- Diffie-Hellman(DH)セキュア鍵交換プロセスの鍵交換(KE)情報。
- IDイニシエータ/レスポンダ(IDi/IDr)は、ピアに認証情報を送信するために使用されます。この情報は、共通共有秘密の保護の下で送信されます。
- Diffie-Hellman(DH)キー交換は、パブリックチャネルを介して安全に暗号化アルゴリズムを交換する方法です。

- IPSec共有キーは、DHを再度使用して完全転送秘密(PFS)を確保するか、元のDH交換を以前取得した共有シークレットに更新することで取得できます。

メインモードパケット交換

各ISAKMPパケットには、トンネルを確立するためのペイロード情報が含まれています。IKE用語集では、次の図に示すように、メインモードでのパケット交換のペイロード内容の一部としてIKEの略語を説明しています。

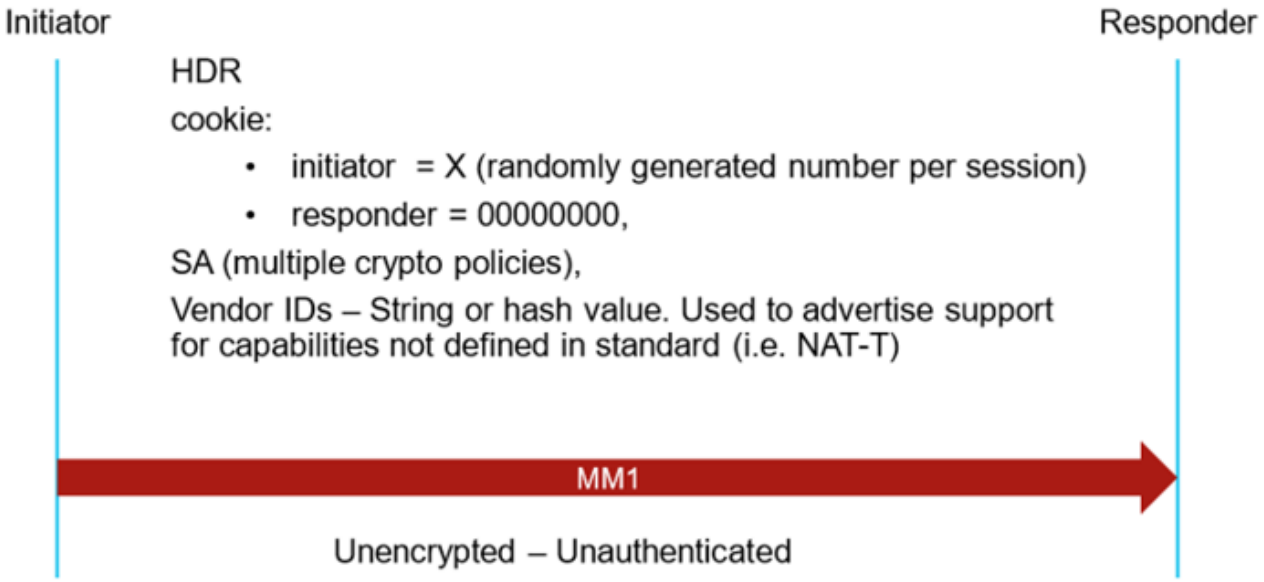


メインモード1(MM1)

ISAKMPネゴシエーションの条件を設定するには、次を含むISAKMPポリシーを作成します。

- ピアのIDを保証する認証方式。
- データを保護し、プライバシーを確保するための暗号化方式。
- 送信者の身元を確認し、メッセージが送信中に変更されていないことを保証するためのハッシュメッセージ認証コード(HMAC)方式。
- 暗号鍵決定アルゴリズムの強度を決定するDiffie-Hellmanグループ。セキュリティアプライアンスはこのアルゴリズムを使用して、暗号化キーとハッシュキーを取得します。
- セキュリティアプライアンスが交換される前に暗号キーを使用する時間の制限。

図に示すように、最初のパケットはIKEネゴシエーションのイニシエータによって送信されます。



注：メインモード1はIKEネゴシエーションの最初のパケットです。したがって、イニシエータSPIはランダムな値に設定され、レスポンダSPIは0に設定されます。2番目のパケット(MM2)では、応答側のSPIに新しい値で応答する必要があり、ネゴシエーション全体で同じSPI値が維持されます。

MM1がキャプチャされ、Wiresharkネットワークプロトコルアナライザが使用される場合、図に示すように、SPI値はInternet Security Association and Key Management Protocol(ISAKMP)の内容の範囲内です。

```
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 170.49.116.200, Dst: 209.134.162.150
> User Datagram Protocol, Src Port: 500, Dst Port: 500
v Internet Security Association and Key Management Protocol
    Initiator SPI: 6f80c0380ef6bdfd
    Responder SPI: 0000000000000000
    Next payload: Security Association (33)
```

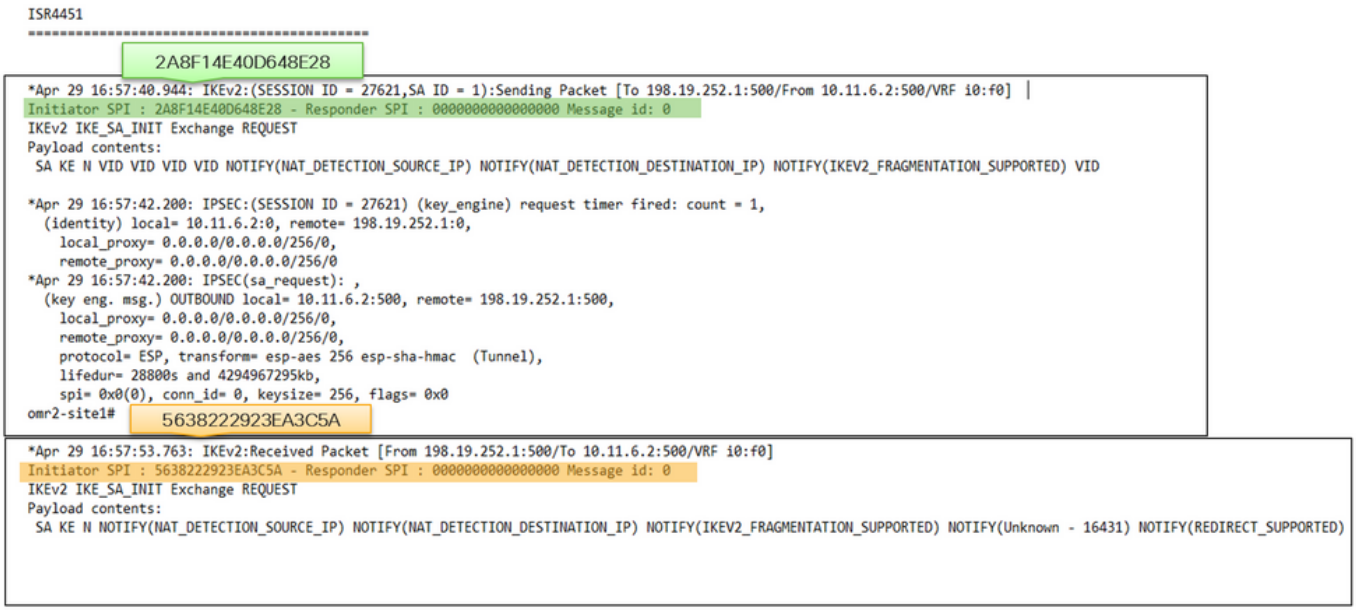
注：MM1パケットがパスで失われたり、MM2応答がない場合、IKEネゴシエーションでは最大再送信数に達するまでMM1の再送信が維持されます。この時点で、イニシエータは次のネゴシエーションが再びトリガーされるまで同じSPIを保持します。

ヒント：発信側および応答側のSPIの識別は、同じVPNの複数のネゴシエーションを識別し、ネゴシエーションの問題を絞り込むのに非常に役立ちます。

2つの同時ネゴシエーションの識別

Cisco IOS® XEプラットフォームでは、リモートIPアドレスが設定された条件を使用して、トンネルごとにデバッグをフィルタリングできます。ただし、同時ネゴシエーションはログに表示されるため、フィルタリングはできません。手動で行う必要があります。前述したように、ネゴシエーション全体で、発信側と応答側で同じSPI値が維持されます。同じピアIPアドレスからパケッ

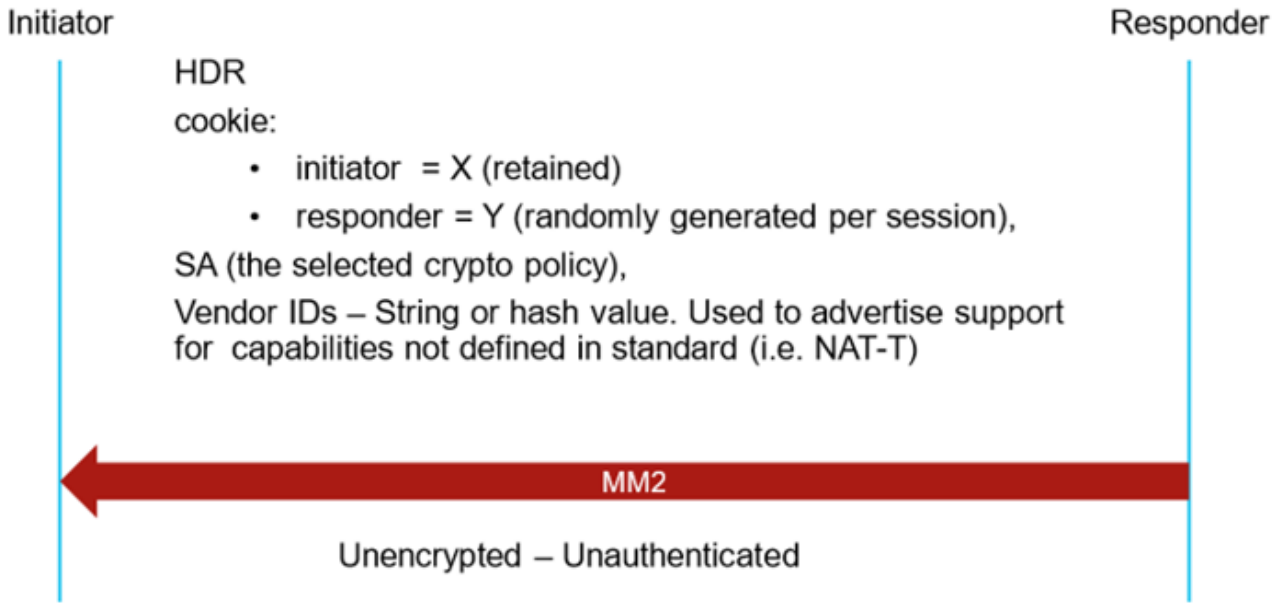
トを受信したが、ネゴシエーションが再送信の最大数に達する前に追跡された値とSPIが一致しない場合、図に示すように、同じピアの別のネゴシエーションです。



注：この例では、ネゴシエーション(MM1)の最初のパケットに対する同時ネゴシエーションを示しています。ただし、これは任意のネゴシエーションポイントで発生する可能性があります。後続のすべてのパケットには、応答側SPIの0とは異なる値を含める必要があります。

メインモード2 (MM2)

メインモード2パケットでは、レスポンダは一致したプロポーザルに対して選択したポリシーを送信し、レスポンダのSPIはランダムな値に設定されます。ネゴシエーション全体で同じSPI値が維持されます。図に示すように、MM2はMM1に応答し、SPI応答側は0とは異なる値に設定されます。



MM2がキャプチャされ、Wiresharkネットワークプロトコルアナライザが使用される場合、イニシエータSPIとレスポンダSPIの値は図に示すようにInternet Security Association and Key Management Protocol(ISAKMP)の内容の範囲内になります。

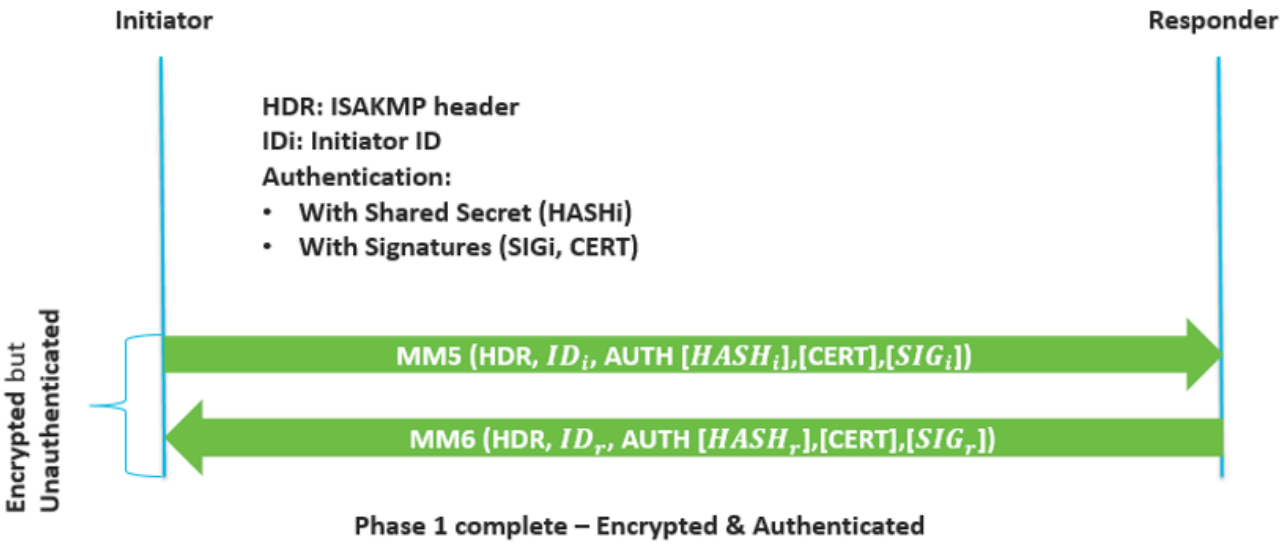
```
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 209.134.162.150, Dst: 170.49.116.200
> User Datagram Protocol, Src Port: 500, Dst Port: 500
v Internet Security Association and Key Management Protocol
    Initiator SPI: 6f80c0380ef6bdfd
    Responder SPI: 2bc06438c94e88dc
    Next payload: Security Association (33)
```

メインモード3および4(MM3-MM4)

MM3およびMM4パケットは暗号化および認証されておらず、秘密キーの交換が行われます。MM3とMM4が図に示されています。

メインモード5および6(MM5-MM6)

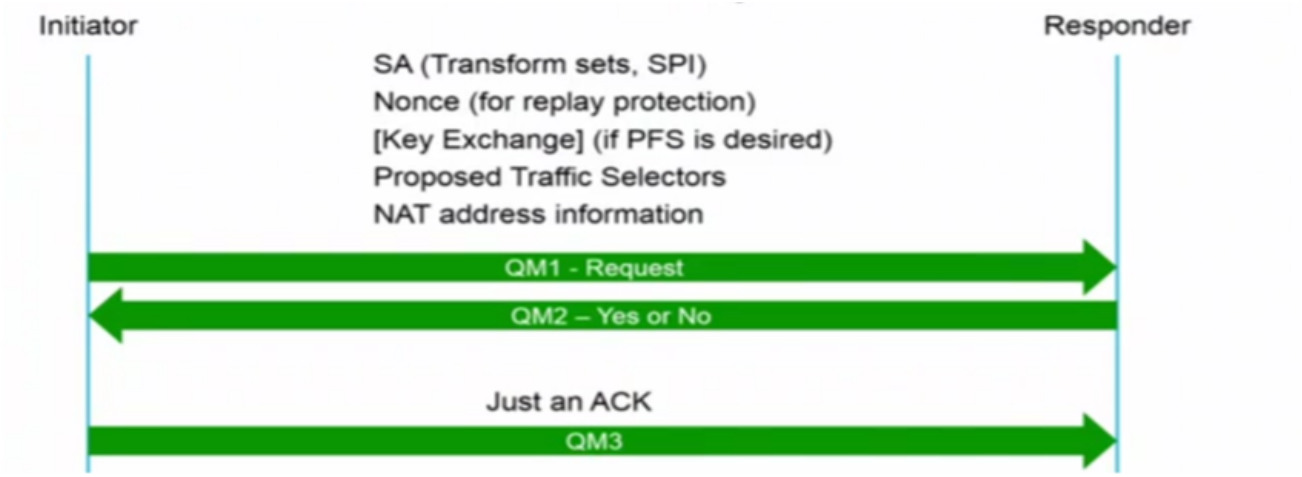
MM5およびMM6パケットはすでに暗号化されていますが、まだ認証されていません。これらのパケットでは、次の図に示すように認証が行われます。



クイックモード（QM1、QM2、およびQM3）

クイックモードは、メインモードとIKEがフェーズ1でセキュアトンネルを確立した後に実行されます。クイックモードは、IPSecセキュリティアルゴリズムの共有IPSecポリシーをネゴシエートし、IPSec SA確立のためのキー交換を管理します。ナンスは、新しい共有秘密キー情報を生成し、生成された偽のSAからのリプレイアタックを防ぐために使用されます。

図に示すように、このフェーズでは3つのパケットが交換されます。

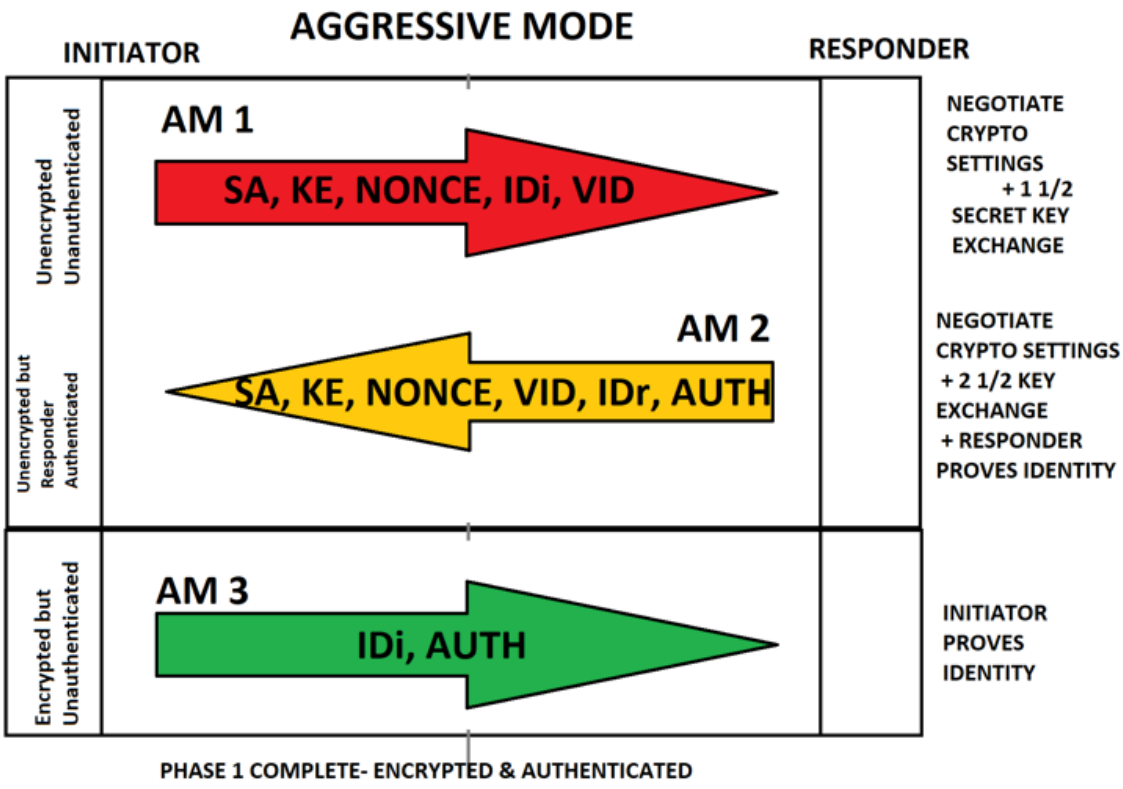


アグレッシブモードのパケット交換

アグレッシブモードでは、IKE SAネゴシエーションが3つのパケットに絞られ、SAに必要なすべてのデータがイニシエータから渡されます。

- レスポンダはプロポーザル、キーマテリアル、およびIDを送信し、次のパケットでセッションを認証します。
- イニシエータが応答し、セッションを認証します。
- ネゴシエーションが高速になり、発信側と応答側のIDがクリアテキストで渡されます。

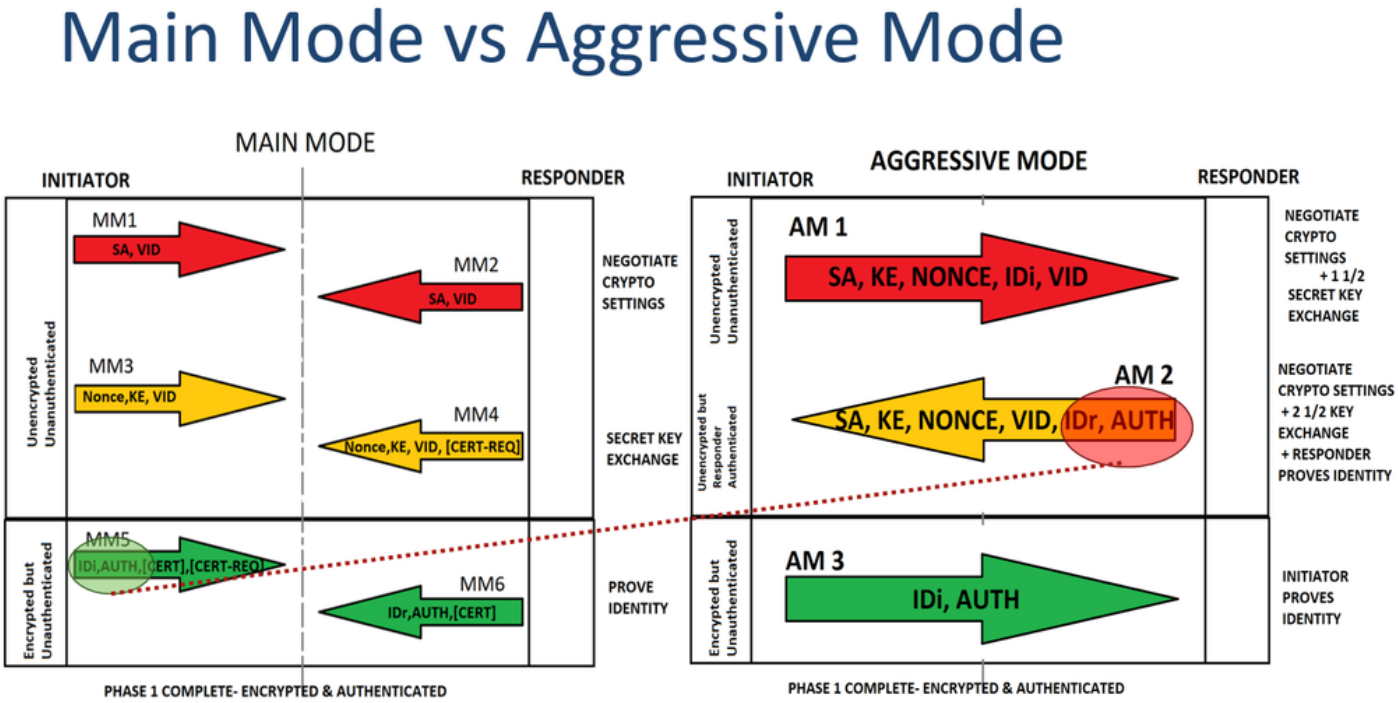
次の図は、アグレッシブモードで交換された3つのパケットのペイロードの内容を示しています。



メインモードとアグレッシブモード

メインモードと比較して、アグレッシブモードでは3つのパッケージがあります。

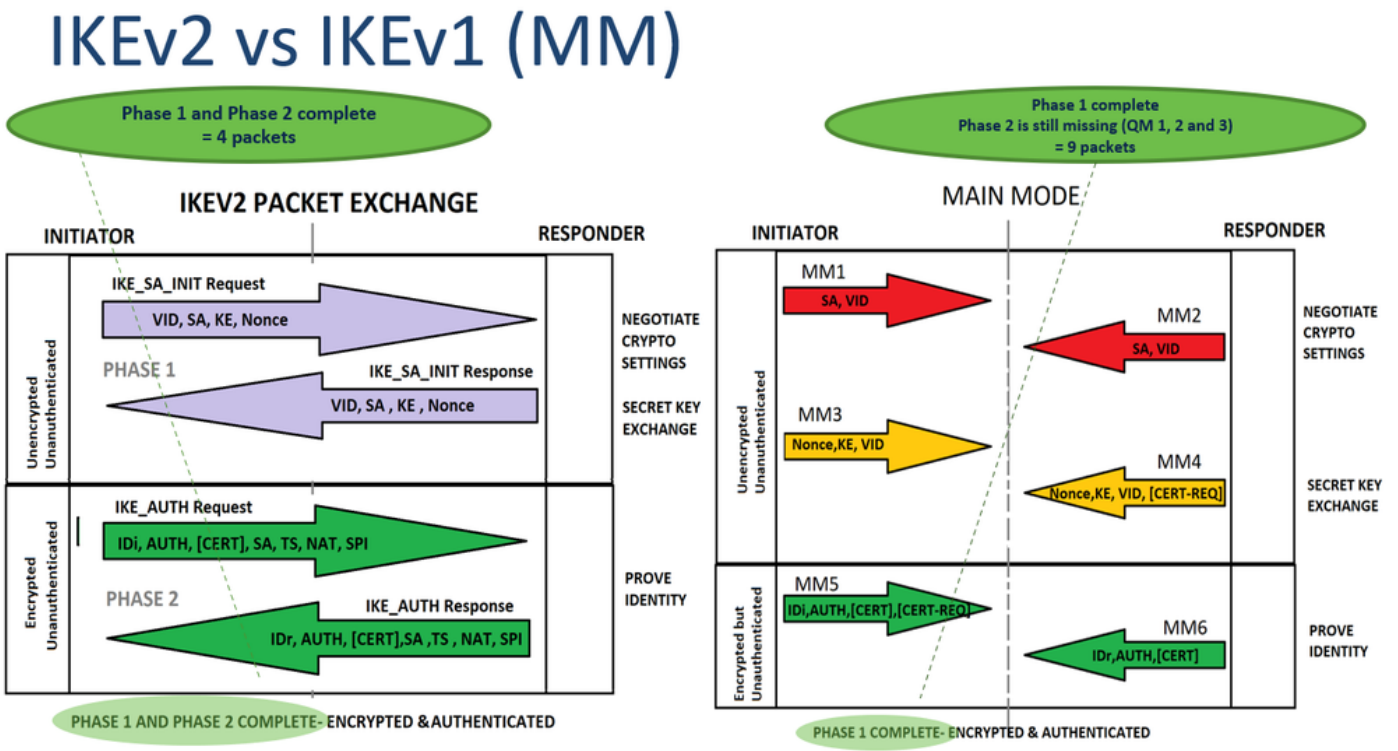
- AM1はMM1とMM3を吸収します。
- AM2は、MM2、MM4、およびMM6の一部を吸収する。ここで、アグレッシブモードの脆弱性が生じます。AM 2はIDrと認証を暗号化せずに構成します。メインモードとは異なり、この情報は暗号化されます。
- AM 3はIDiと認証を提供します。これらの値は暗号化されます。



IKEv2とIKEv1のパケット交換

IKEv2ネゴシエーションでは、トンネルを確立するために交換されるメッセージが少なくなります。IKEv2は4つのメッセージを使用します。IKEv1は6つのメッセージ（メインモード）または3つのメッセージ（アグレッシブモード）を使用します。

IKEv2メッセージタイプは、要求と応答のペアとして定義されます。次の図は、IKEv2とIKEv1のパケット比較およびペイロード内容を示しています。



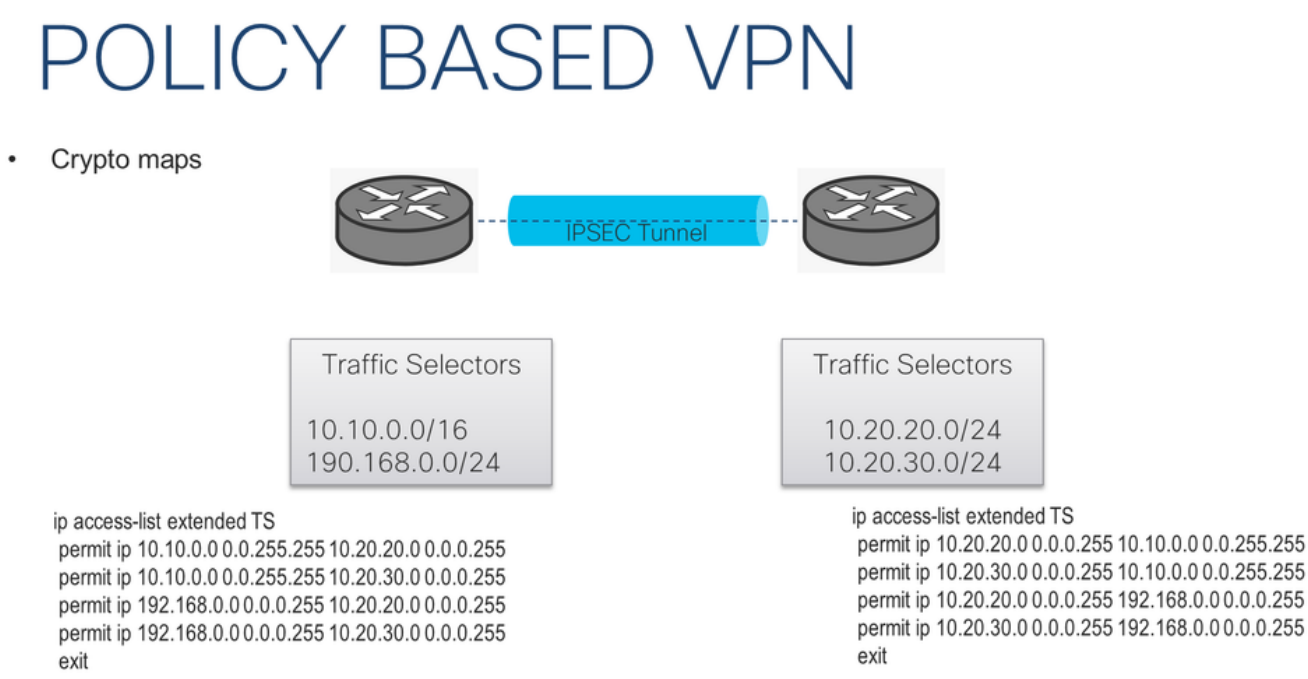
注：このドキュメントでは、IKEv2パケット交換については詳しく説明しません。詳細については、「IKEv2のパケット交換とプロトコルレベルデバッグ」を参照してください。

ポリシーベースとルートベース

ポリシーベースVPN

名前が示すように、ポリシーベースVPNは、ポリシーの一致基準を満たす中継トラフィック用のポリシーアクションを持つIPSec VPNトンネルです。シスコデバイスの場合、アクセスリスト(ACL)が設定され、VPNにリダイレクトされて暗号化されるトラフィックを指定するためにクリプトマップに接続されます。

トラフィックセレクタは、図に示すように、ポリシーで指定されたサブネットまたはホストです。

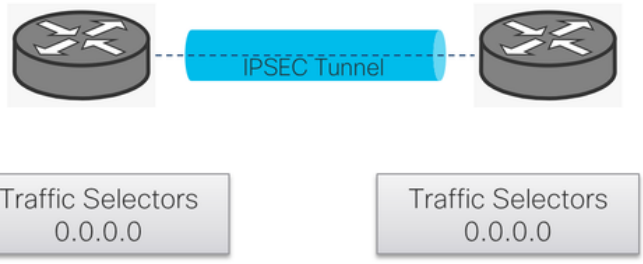


ルートベースのVPN

ポリシーは必要ありません。トラフィックはルートを使用してトンネルにリダイレクトされ、トンネルインターフェイスでのダイナミックルーティングをサポートします。図に示すように、トラフィックセレクタ（VPNで暗号化されたトラフィック）はデフォルトで0.0.0.0 ~ 0.0.0.0です。

ROUTE BASED VPN

- Supports dynamic routing over the tunnel interface.




```
interface: Tunnel100001
   Crypto map tag: Tunnel100001-head-0, local addr 10.0.21.17

  protected vrf: 1
  local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
```

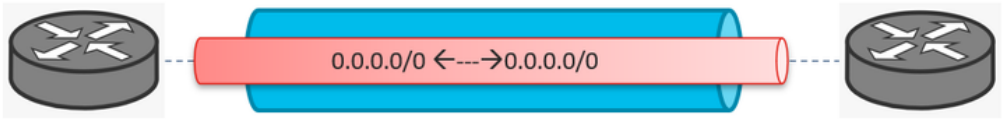
注：トラフィックセレクタが0.0.0.0であるため、すべてのホストまたはサブネットはに含まれます。したがって、SAは1つだけ作成されます。ダイナミックトンネルには例外があります。このドキュメントでは、ダイナミックトンネルについては説明しません。

ポリシーおよびルートベースのVPNは、図に示すように実現できます。

ISAKMP-IPSEC Tunnel

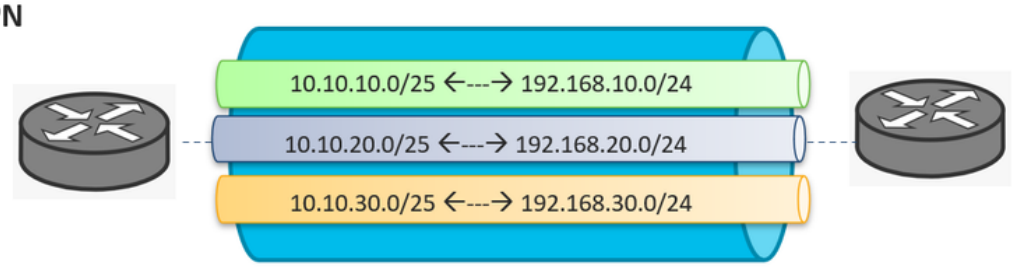
Route based VPN

*** Edges only support this.



Policy based VPN

- IOS - XE
- ASA
- FTD
- 3rd party devices



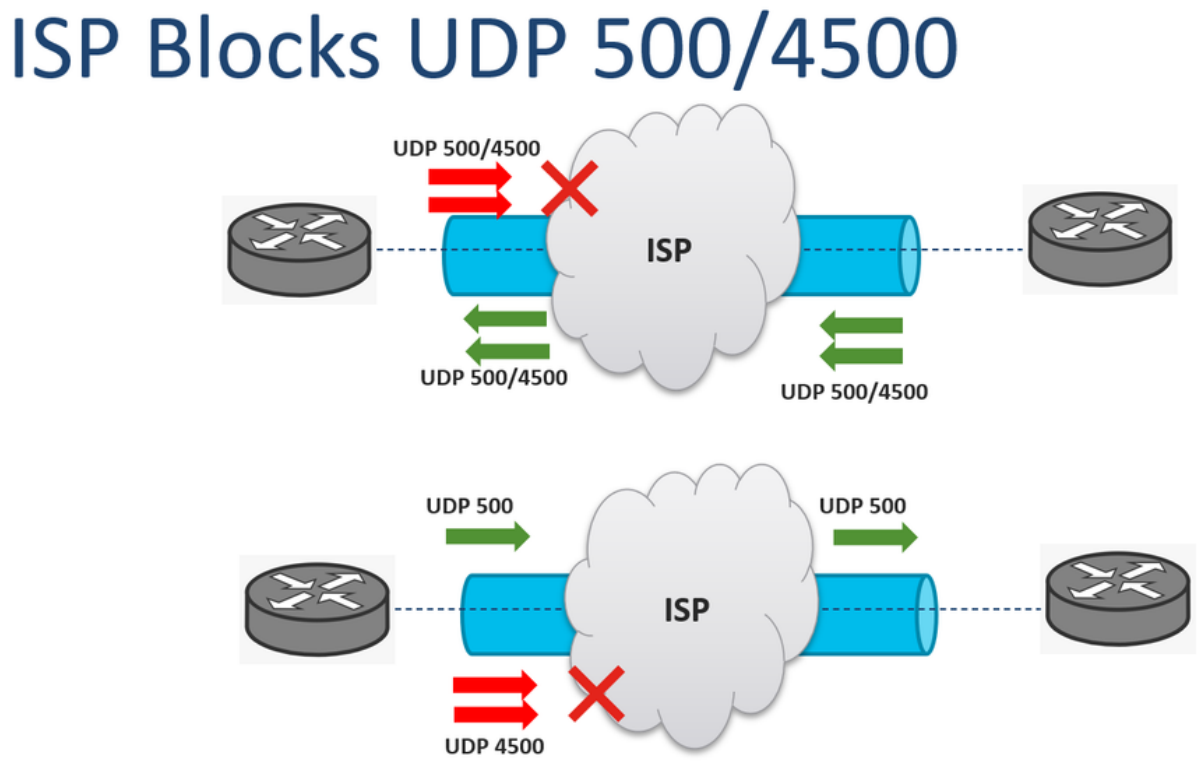
注：作成されたSAが1つだけのルートベースVPNとは異なり、ポリシーベースVPNは複数のSAを作成できます。ACLが設定されると、ACLの各ステートメントは（ステートメント間で異なる場合）、サブトンネルを作成します。

VPN経由で受信しないトラフィックの一般的な問題

ISPがUDP 500/4500をブロック

Internet Services Provider（ISP；インターネットサービスプロバイダー）がUDP 500/4500ポートをブロックする問題は非常に一般的です。IPSecトンネルを確立するには、2つの異なるISPを使用できます。一方はポートをブロックでき、もう一方はポートを許可します。

この図は、ISPが一方向でのみUDP 500/4500ポートをブロックできる2つのシナリオを示しています。

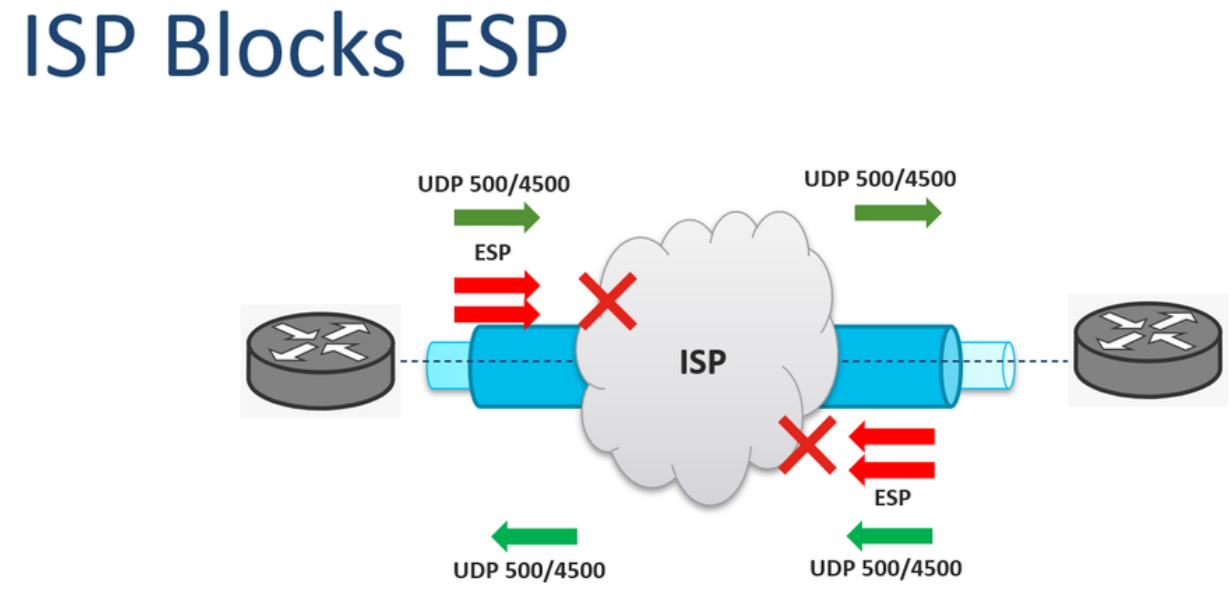


注：ポートUDP 500は、セキュアなVPNトンネルを確立するためにインターネットキーエクスチェンジ(IKE)によって使用されます。UDP 4500は、1つのVPNエンドポイントにNATが存在する場合に使用されます。

注:ISPがUDP 500/4500をブロックすると、IPSecトンネルの確立に影響を及ぼし、確立されません。

ISPによるESPのブロック

IPSecトンネルに関するもう1つの非常に一般的な問題は、ISPがESPトラフィックをブロックしているのに、UDP 500/4500ポートが許可されていることです。たとえば、UDP 500/4500ポートは双方向で許可されます。そのため、トンネルは正常に確立されますが、ESPパケットはISPまたはISPによって両方向でブロックされます。これにより、図に示すように、VPNを通過する暗号化されたトラフィックが失敗します。



注:ISPがESPパケットをブロックすると、IPSecトンネルは正常に確立されますが、暗号化されたトラフィックが影響を受けます。これはVPNアップ時に反映できますが、トラフィックはVPN上で動作しません。

ヒント:ESPトラフィックが一方向でのみブロックされるシナリオも存在する可能性があります。症状は同じですが、トンネル統計情報、カプセル化、カプセル化解除カウンタ、またはRXカウンタとTXカウンタを使用すると簡単に確認できます。

関連情報

- KEv2パケット交換とプロトコルレベルデバッグ
- インターネットキーエクスチェンジ(IKE):RFC 2409
- インターネットキーエクスチェンジ(IKEv2)プロトコル
- テクニカル サポートとドキュメント - Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。