

Cisco ネットワークレイヤの暗号化の設定とトラブルシューティング：IPSec と ISAKMP - 第 2 部

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[ネットワークレイヤ暗号化の背景情報と設定](#)

[定義](#)

[IPSec と ISAKMP](#)

[IPSec プロトコル](#)

[ISAKMP/Oakley](#)

[IPSec と ISAKMP の Cisco IOS ネットワークレイヤの暗号化の設定](#)

[例 1：ISAKMP 事前共有キー](#)

[例 2：ISAKMP：RSA 暗号化された認証](#)

[例 3：ISAKMP：RSA-SIG 認証/CA](#)

[IPSec と ISAKMP のトラブルシューティング](#)

[関連情報](#)

概要

このテクニカル レポートの [第 1 部](#) では、ネットワークレイヤ暗号化の背景情報と基本的なネットワークレイヤ暗号化の設定を取り上げました。このドキュメントの第 2 部では、IP Security (IPSec) および Internet Security Association and Key Management Protocol (ISAKMP) を取り上げています。

IPSec は Cisco IOS® ソフトウェア リリース 11.3T で導入されました。この機能は安全なデータ送信のためのメカニズムを提供するもので、ISAKMP/Oakley と IPSec で構成されています。

前提条件

要件

このドキュメントに関する固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。

- Cisco IOS ソフトウェア リリース 11.3(T) 以降

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、クリアな（デフォルト）設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

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。

ネットワークレイヤ暗号化の背景情報と設定

定義

このセクションでは、このドキュメントで使用される関連用語を定義しています。

- **認証**：受信したデータが実際にそこに示されている送信者から送られたものであることを知る手段。
- **Confidentiality (機密性)**：意図した受信者には内容がわかるがそれ以外のものにはわからないようにする通信の属性。
- **Data Encryption Standard (DES; データ暗号標準)**：DESでは、秘密鍵方式とも呼ばれる対称鍵方式が使用されています。これは、キーを使用してデータのブロックを暗号化した場合、同じキーを使用して復号化する必要があることを意味し、したがって暗号化と復号化で同じキーを使用する必要があります。この暗号化方式は周知のもので広く公開されていますが、一般に知られている最善の攻撃方法は力づくの手段によるものになります。暗号化されたブロックに対して逐一キーを試し、正しく解読できるかどうかを調べるものです。プロセッサが強力になってきたことで、DESの寿命は終わろうとしています。たとえば、インターネット上の何千台ものコンピュータの余剰処理能力を利用した組織的な作業により、DESで符号化されたメッセージに対する56ビットのキーを21日間で発見できます。DESは、米国政府の目的に適合するように、5年ごとにUS National Security Agency (NSA; 米国安全保障局)によって見直されています。現在の承認は1998年に切れることになっており、NSAはDESを再認定しないことを表明しています。DESの後継としては、力づくの攻撃以外に弱点が知られていない他の暗号化アルゴリズムが他にも存在します。追加情報については、[National Institute of Standards and Technology \(NIST; 国立標準技術研究所\)](#)によるDES FIPS 46-2を参照してください。
- **Decryption (復号化)**：暗号化されたデータに対して暗号アルゴリズムを逆に適用することで、データを暗号化されていない元の状態に戻すこと。
- **DSS および Digital Signature Algorithm (DSA; デジタル署名アルゴリズム)**：DSAは、NISTがDigital Signature Standard (DSS; デジタルシグニチャ規格)において公開したもので、米国政府のCapstoneプロジェクトの一部です。NISTとNSAは、米国政府のデジタル認証標準としてDSSを選択しました。この標準は1994年5月19日に公開されています。
- **Encryption (暗号化)**：特定のアルゴリズムをデータに適用して、データの外見を変更し、情報を見ることを許可されていない者がデータを理解できないようにすること。
- **Integrity (整合性)**：送信元から宛先まで、検出できない変更が加えられることなく、データが伝送されることを保証する属性。

- **Non-repudiation (否認防止)** : データを送信したことを送信者が後で拒否しようとする場合でも、データがその送信者によって実際に送信されたことを受信者が証明できる属性。
- **Public Key Cryptography (公開キー暗号方式)** : 従来の暗号法は、メッセージの送信者と受信者が同じ秘密キーを知っていて、それを使用することに基づくものです。送信者は秘密キーを使用してメッセージを暗号化し、受信者は同じ秘密キーを使用してメッセージを復号化します。この方式は、「秘密鍵」または「対称暗号方式」と呼ばれます。最大の問題は、他人に知られないように送信者と受信者が秘密鍵に合意することです。送信者と受信者が物理的に異なる場所にいる場合、配達人や電話システムや他の伝達手段による伝達の過程で秘密キーが暴露されないということを信頼する必要があります。移動中のキーを傍受する者は、後で、そのキーを使用して暗号化や認証が行われたメッセージを読んだり、変更したり、偽造したりできます。キーの生成、伝達、保管は鍵管理と呼ばれます。すべての暗号システムは鍵管理の問題に対処する必要があります。秘密キーの暗号システムではすべてのキーを秘密に保つ必要があるため、秘密キーの暗号法では、安全なキー管理を行うことが困難な場合がよくあります。特に、多数のユーザがいるオープンシステムではそのことが言えます。公開鍵暗号法は、鍵管理の問題を解決するために、Whitfield Diffie と Martin Hellman によって 1976 年に考案されました。この概念では、各ユーザは、公開キーおよび秘密キーと呼ばれる一対のキーを受け取ります。各ユーザの公開キーは公開されますが、秘密キーは秘密に保たれます。送信者と受信者が秘密の情報を共有する必要がなくなり、すべての通信に含まれるのは公開キーだけで、秘密キーが送信や共有されることはありません。通信の各経路が手段が盗聴や暴露に対してセキュアであると信じる必要がなくなります。ただ 1 つ必要なことは、公開キーをそのユーザと信頼できる (認証された) 方法 (信頼できるディレクトリなど) で関連付けることだけです。公開されている情報を使用してだれでも簡単に機密メッセージを送信できますが、メッセージを復号化できるのは、意図された受信者だけが所有する秘密キーを使用した場合だけです。さらに、公開キー暗号法は、プライバシー (暗号化) だけでなく、認証 (デジタル署名) にも使用できます。
- **Public Key Digital Signatures (公開キー デジタル署名)** : メッセージに署名するには、秘密キーとメッセージ自体を含む計算を実行します。出力はデジタル署名と呼ばれ、メッセージに添付された後、メッセージと一緒に送信されます。受信者は、メッセージ、署名とされているもの、送信者の公開鍵を使用して計算を実行し、署名を検証します。結果が簡単な数学的関係を正しく保持している場合、署名は本物と確認されます。それ以外の場合は、署名が正しくないか、またはメッセージが改ざんされている可能性があります。
- **Public Key Encryption (公開キー暗号化)** : 秘密のメッセージの送信者は、ディレクトリ内で受信者の公開キーを探し、それを使ってメッセージを暗号化して送信します。受信者は、自分の秘密キーを使用してメッセージを復号化して、これを読み取ります。だれかがメッセージを盗聴しても復号化することはできません。だれでも暗号化されたメッセージを送信することはできますが、メッセージを読むことができるのは受信者だけです。明らかですが、1 つ必要なのは、対応する公開鍵から秘密鍵を突きとめることができないということです。
- **Traffic Analysis (トラフィック分析)** : 相手について役に立つ情報を推定するためのネットワークのトラフィックフローを分析すること。このような情報としては、たとえば、送信の頻度、相手の ID、パケットのサイズ、使用されているフロー ID などがあります。

IPSec と ISAKMP

このドキュメントの第 2 部では、IPSec と ISAKMP について説明しています。

IPSec は、Cisco IOS ソフトウェア リリース 11.3T で導入されました。この機能は安全なデータ

送信のためのメカニズムを提供するもので、ISAKMP/Oakley と IPsec で構成されています。

IPsec プロトコル

IPsec プロトコル ([RFC 1825](#)) では、IP ネットワークレイヤの暗号化が提供され、IP データグラムへ追加される新しいヘッダー セットが定義されています。 これらの新しいヘッダーは、IP ヘッダーの後かつレイヤ 4 プロトコル (一般的には TCP または UDP) の前に配置されます。このヘッダーでは、次のような IP パケットのペイロードを安全にするための情報が提供されます。

大部分のアプリケーションにはどちらか 1 つだけの使用で十分ですが、Authentication Header (AH; 認証ヘッダー) および Encapsulating Security Payload (ESP) は単独または組み合わせて使用することができます。これら両方のプロトコルに関して、IPsec では使用する具体的なセキュリティアルゴリズムが定義されていません。その代わりに、業界標準のアルゴリズムを実装するためのオープンなフレームワークが用意されています。まず、IPsec の大部分の実装では、整合性と認証について米国政府によって定義されたとおり、RSA Data Security または Secure Hash Algorithm (SHA) からの MD5 がサポートされます。IDEA、Blowfish、および RC4 など、他の多くの暗号化システムを使用する方法を定義する RFC も使用可能ですが、現在のところは DES が最も一般的に提供されるバルク暗号化アルゴリズムです。

- **AH** ([RFC 1826](#) を参照) AH は、IP データグラムに強固な整合性と認証を提供するメカニズムです。また、使用される暗号アルゴリズムと鍵入力の実行方法によっては、否認防止も提供できます。たとえば、RSA などの非対称デジタル署名アルゴリズムを使用すると、否認防止を提供できます。AH では、トラフィック分析からの機密保持および保護は提供されません。機密保持が必要なユーザは、AH の代わりに、または AH と組み合わせて、IP ESP の使用を検討する必要があります。AH は、各ホップで検査される他の任意のヘッダーの後かつ中間ホップで検査されない他の任意のヘッダーの前に配置される可能性があります。AH 直前の IPv4 または IPv6 ヘッダーは、その Next Header (または Protocol) フィールドに値 51 を含みます。
- **ESP** ([RFC 1827](#) を参照) ESP は、IP ヘッダーの後かつ最終の転送レイヤ プロトコルの前の任意の場所に配置できます。Internet Assigned Numbers Authority (IANA; インターネット割り当て番号局) では、ESP にプロトコル番号 50 を割り当てています。ESP 直前のヘッダーは、常にその Next Header (IPv6) または Protocol (IPv4) フィールドに値 50 を含みます。ESP は、暗号化されていないヘッダーとそれに続く暗号化されたデータで構成されます。暗号化されたデータには、保護されている ESP ヘッダー フィールドと、全 IP データグラムまたは上位層プロトコル フレーム (TCP または UDP など) のどちらかである保護されたユーザデータの両方が含まれています。IP ESP は、保護を目的としてデータを暗号化し、暗号化されたデータを IP ESP のデータ部分に配置することで、機密保持と整合性を提供しています。ユーザのセキュリティ要件によっては、トランスポート層セグメント (TCP、UDP、ICMP、IGMP など) または IP データグラム全体を暗号化するためにこのメカニズムを使用できます。保護されたデータのカプセル化は、元のデータグラム全体に機密保持を提供するために必要です。この仕様を使用すると、参加しているシステムにおいて IP プロトコルの処理コストが増大し、通信の遅延も拡大します。遅延の拡大は、主に ESP を含んでいる各 IP データグラムに必要な暗号化と復号化によるものです。トンネルモード ESP では、元の IP データグラムは ESP の暗号化された部分に配置され、ESP フレーム全体が暗号化されていない IP ヘッダーが含まれるデータグラム内部に配置されます。暗号化されていない IP ヘッダー内の情報は、セキュアなデータグラムを起点から宛先へルーティングするために使用されます。暗号化されていない IP ルーティング ヘッダーが、IP ヘッダーと ESP の間に含まれる場合があります。このモードを使用すると、ルータなどのネットワーク デバイスが IPsec プロキシとして動作できます。つまり、ホストの代わりにルータによって暗号化が実

行されます。発信元のルータによってパケットが暗号化され、IPSec トンネルに沿ってこれらのパケットが転送されます。宛先のルータでは、元の IP データグラムが復号化され、宛先のシステムへ転送されます。トンネル モードの主な利点は、IP Security の利点を活用するためにエンドシステムを変更する必要がないことです。また、トンネル モードを使用すると、トラフィック分析に対しても保護されます。トンネル モードを使用した場合、攻撃者は、トンネルのエンドポイントだけを特定できます。トンネルを通過するパケットの送信元と宛先がトンネルのエンドポイントと同じである場合でも、攻撃者はそのパケットの実際の送信元と宛先を特定できません。IETF によって定義されるとおり、IPSec トランスポート モードは、送信元と宛先のどちらのシステムでも IPSec が認識されている場合にだけ使用できます。ほとんどの場合、IPSec はトンネル モードで展開します。こうすることで、ユーザの PC、サーバ、およびホスト上のオペレーティング システムやどのアプリケーションも変更することなく、IPSec をネットワーク アーキテクチャ内に実装できます。トランスポート モード ESP では、ESP ヘッダーがトランスポート層プロトコルヘッダー (TCP、UDP、または ICMP など) の直前の IP データグラムに挿入されます。このモードでは、暗号化された IP ヘッダーまたは IP オプションが存在しないため、帯域幅が節約されます。IP ペイロードだけが暗号化され、元の IP ヘッダーはそのままになります。このモードでは、各パケットに追加されるのが数バイトだけという利点があります。また、このモードによって、パブリック ネットワーク上のデバイスは、パケットの最終的な発信元と宛先を認識できるようになります。この機能を使用すると、IP ヘッダーの情報に基づく中継ネットワークでの特殊な処理 (たとえば Quality Of Service など) を有効にすることができるようになります。ただし、レイヤ 4 ヘッダーが暗号化され、パケットの検査が制限されます。残念ながら、クリアテキストによる IP ヘッダーの受け渡しによって、トランスポート モードでは、攻撃者がなんらかのトラフィック分析を行えます。たとえば、攻撃者は、ある CEO から他の CEO に多数のパケットが送信されたことが把握できます。ただし、攻撃者が把握するのは、IP パケットが送信されたことだけです。攻撃者はこれらが電子メールだったのか、または別のアプリケーションだったのかを判断することはできません。

[ISAKMP/Oakley](#)

IPSec が IP データグラムを保護する実際のプロトコルである一方、ISAKMP はポリシーをネゴシエートし、IPSec ピア間で共有される鍵を生成するための共通フレームワークを提供するプロトコルです。ISAKMP では鍵管理または鍵交換の詳細は指定されず、鍵生成の技術にはバインドされません。ISAKMP の内部では、Cisco は鍵交換プロトコルに Oakley を使用しています。Oakley を使用すると、「well-known」グループ間での選択が可能です。Cisco IOS では、グループ 1 (768 ビット鍵) およびグループ 2 (1024 ビット鍵) がサポートされています。グループ 5 (1536 ビット鍵) のサポートは、Cisco IOS ソフトウェア リリース 12.1(3)T で導入されています。

ISAKMP/Oakley では、2 つのエンティティ間に認証済みで安全なトンネルが作成されてから、IPSec のセキュリティ アソシエーションがネゴシエートされます。このプロセスでは、2 つのエンティティが相互にエンティティ自体を認証し、共有鍵を構築する必要があります。

どちらのパーティも相互に認証される必要があります。ISAKMP/Oakley では、複数の認証方式がサポートされています。2 つのエンティティは、RSA 署名、RSA 暗号化ナンス、または事前共有鍵を使用して、ネゴシエーション プロセスを介して共通の認証プロトコルに合意する必要があります。

ISAKMP/Oakley トンネルを暗号化するには、どちらのパーティも共有セッション鍵を所持している必要があります。デフィーヘルマン プロトコルは、共通のセッション鍵に合意するために使用されます。この交換は、「man-in-the-middle (中間者)」攻撃から保護するために、上述のよう

に認証されます。

これらの2つの手順（認証と鍵交換）によって、2つのデバイス間の安全なトンネルである ISAKMP/Oakley session association (SA; セッション アソシエーション) が作成されます。トンネルの一方の側がアルゴリズムのセットを提供します。もう一方の側は、いずれかのアルゴリズムを受け入れるか、または接続全体を拒否する必要があります。使用するアルゴリズムについて両側で合意されると、AH、ESP、または両方で IPsec に使用する鍵関連情報を取得する必要があります。

IPsec では、ISAKMP/Oakley とは異なる共有鍵が使用されます。IPsec 共有鍵は、完全転送秘密を確実にするためにデフィーヘルマンを再度使用するか、または擬似ランダム番号（ナンズ）を使用したハッシュにより ISAKMP/Oakley SA を生成した元のデフィーヘルマン交換から取得された共有秘密鍵を更新することで取得できます。1つ目の方法では優れたセキュリティが提供されますが、低速です。大部分の実装では、2つの方法の組み合わせが使用されます。つまり、デフィーヘルマンが最初の鍵交換に使用されてから、ローカル ポリシーによってデフィーヘルマンを使用する状況または単に鍵更新を行う状況が規定されます。この完了後、IPsec SA が確立されます。

RSA 署名および RSA 暗号化ナンズのどちらにもリモート ピアの公開鍵が必要であり、ユーザのローカル公開鍵がリモート ピアで認識されていることも必要になります。公開鍵は、証明書の形式で ISAKMP 内で交換されます。これらの証明書は、Certificate Authority (CA; 認証局) に登録することで取得されます。現在、ルータ内に証明書が存在しない場合、ISAKMP では保護スイート RSA 署名をネゴシエートしません。

Cisco ルータでは、証明書を作成しません。ルータでは鍵が作成され、これらの鍵用の証明書が要求されます。ルータの鍵をそれらの ID にバインドする証明書は、認証局によって作成され署名されます。これは管理機能であり、認証局はユーザが主張している身元の正当性に対する何らかの証明を常に要求します。これは新しい証明書をただちに作成できないことを意味します。

通信しているマシンでは、認証局から取得された既存の証明書が交換されます。証明書自体は公開されている情報ですが、対応する秘密鍵は、ID を証明するために証明書を使用するどのユーザも利用できる必要があります。ただし、その ID を使用する必要のないユーザには、秘密にしておく必要もあります。

証明書によって、ユーザまたはマシンが識別される場合があります。これは実装によって異なります。初期の大部分のシステムでは、マシンを識別するために証明書を使用している可能性があります。証明書によってユーザが識別されると、その証明書に対応している秘密鍵は、同じマシン上の別のユーザがその秘密鍵を使用できないような方法で格納される必要があります。このことは一般的に、鍵が暗号化されたままであるか、または鍵がスマート カードで保持されることを意味します。初期の実装では、暗号化された鍵がより一般的である可能性があります。どちらの場合も、一般的には鍵がアクティブになるたびにユーザがパスワードを入力する必要があります。

注: ISAKMP/Oakley ではネゴシエーションに UDP ポート 500 が使用されます。AH では Protocol フィールドに 51 が含まれ、ESP では Protocol フィールドに 50 が含まれます。これらをフィルタリングしていないことを確認してください。

このテクニカル レポートで使用される用語の詳細は、「[定義](#)」セクションを参照してください。

[IPsec と ISAKMP の Cisco IOS ネットワークレイヤの暗号化の設定](#)

このドキュメントで示す Cisco IOS 設定の実稼働サンプルは、ラボのルータのものをそのまま使用しています。変更点は、関係のないインターフェイスの設定を省略したことだけです。ここで示す資料はすべて、インターネットまたはこのドキュメントの最後の「[関連情報](#)」のセクションで示されているリソースから無料で公開されています。

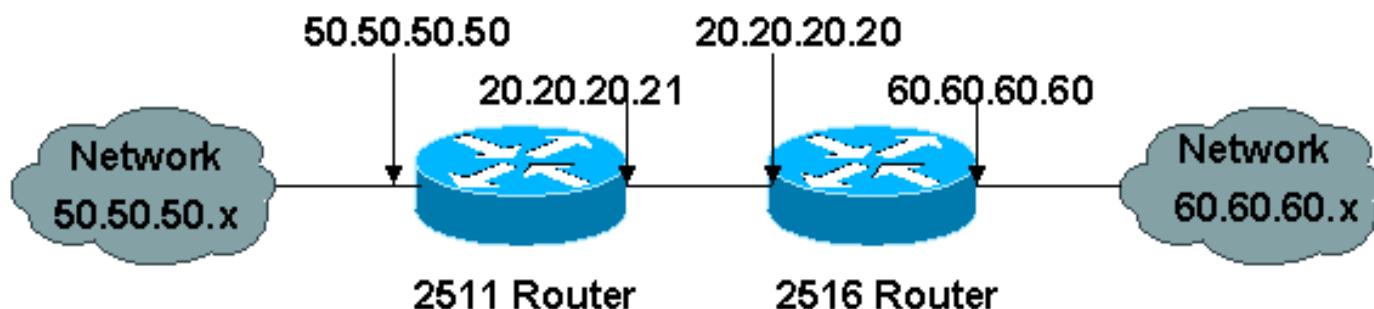
例 1 : ISAKMP 事前共有キー

事前共有鍵を介した認証は、非公開鍵の代替です。この方式を使用すると、アウトオブバンドで交換され、ルータに設定された秘密鍵が各ピアで共有されます。(明示的に言及することなく)それぞれの側でこの秘密鍵に対する認識を示す機能によって、交換が認証されます。この方式は、小規模なインストールには適切ですが、スケーリングの問題を含んでいます。「sharedkey」の事前共有鍵が次に使用されています。ホストでアドレスベースの事前共有鍵が共有される場合、それらのアドレスを ID として使用する必要があります。これは Cisco IOS ソフトウェアではデフォルト動作のため、以下のコマンドは設定には出力されません。

```
crypto isakmp identity address
```

注: ISAKMP によって IPsec のポリシーおよび鍵を確立できない状況があります。ルータで定義された証明書が存在せず、ISAKMP ポリシー内に公開鍵ベースの認証方式だけが存在する場合、または(アドレスまたはそのアドレスを使用して設定されたホスト名によって直接共有される)ピア用の証明書と事前共有鍵が存在しない場合、ISAKMP ではピアとネゴシエートできず、IPsec は機能しません。

次の図は、この構成のネットワーク ダイアグラムを示しています。



事前共有鍵に基づいて IPsec および ISAKMP 認証を行っているバックツールバックの 2 台のルータ (Cisco 2511 および Cisco 2516) の設定は次のとおりです。コメント行は冒頭の感嘆符によって示してあり、ルータに入力される場合は無視されます。次の設定では、一部の設定行を説明するために、それらの直前にコメントが付けられています。

Cisco 2511 の設定

```
cl-2513-2A#write terminal Building configuration...
Current configuration: ! version 11.3 service timestamps
debug uptime service timestamps log uptime no service
password-encryption ! hostname cl-2513-2A ! !---
Override the default policy and use !--- preshared keys
for authentication. crypto isakmp policy 1
authentication pre-share group 2 ! !--- Define our
secret shared key so !--- you do not have to use RSA
keys. crypto isakmp key sharedkey address 20.20.20.20 !
!--- These are the authentication and encryption !---
settings defined for "auth2", !--- which is later
applied to the crypto map. crypto ipsec transform-set
auth2 esp-des esp-sha-hmac ! !--- The crypto map where
you define your peer, !--- transform auth2, and your
```

```

access list. crypto map test 10 ipsec-isakmp set peer
20.20.20.20 set transform-set auth2 match address 133 !
interface Ethernet0 ip address 50.50.50.50 255.255.255.0
! interface Serial0 ip address 20.20.20.21 255.255.255.0
no ip route-cache no ip mroute-cache !--- Nothing
happens unless you apply !--- the crypto map to an
interface. crypto map test ! ip route 0.0.0.0 0.0.0.0
20.20.20.20 ! !--- This is the access list referenced !-
-- in the crypto map; never use "any". !--- You are
encrypting traffic between !--- the remote Ethernet
LANs. access-list 133 permit ip 50.50.50.0 0.0.0.255
60.60.60.0 0.0.0.255 ! line con 0 line aux 0 line vty 0
4 login ! end

```

Cisco 2516 の設定

```

cl-2513-2B#show run Building configuration... Current
configuration: ! version 11.3 service timestamps debug
uptime service timestamps log uptime no service
password-encryption ! hostname cl-2513-2B ! ip subnet-
zero ! !--- Override the default policy and use !---
preshared keys for authentication. crypto isakmp policy
1 authentication pre-share group 2 !--- Define the
secret shared key so you !--- do not have to use RSA
keys. crypto isakmp key sharedkey address 20.20.20.21 !-
-- These are the authentication and encryption !---
settings defined for "auth2," !--- which is later
applied to the crypto map. crypto ipsec transform-set
auth2 esp-des esp-sha-hmac !--- The crypto map where you
define the peer, !--- transform auth2, and the access
list. crypto map test 10 ipsec-isakmp set peer
20.20.20.21 set transform-set auth2 match address 144 !
interface Ethernet0 ip address 60.60.60.60 255.255.255.0
no ip directed-broadcast ! !--- Nothing happens unless
you apply !--- the crypto map to an interface. interface
Serial0 ip address 20.20.20.20 255.255.255.0 no ip
directed-broadcast no ip route-cache no ip mroute-cache
clockrate 800000 crypto map test ! ip classless ip route
0.0.0.0 0.0.0.0 20.20.20.21 ! !--- This is the access
list referenced !--- in the crypto map; never use "any".
!--- You are encrypting traffic between !--- the remote
Ethernet LANs. access-list 144 permit ip 60.60.60.0
0.0.0.255 50.50.50.0 0.0.0.255 ! line con 0 transport
input none line aux 0 line vty 0 4 login ! end

```

debug コマンド出力を次に示します。

```

----- Preshare with RSA key defined
(need to remove RSA keys) -----

*Mar  1 00:14:48.579: ISAKMP (10): incorrect policy settings.
Unable to initiate.
*Mar  1 00:14:48.587: ISAKMP (11): incorrect policy settings.
Unable to initiate.....

----- Preshare, wrong hostname -----

ISAKMP: no pre-shared key based on hostname wan-2511.cisco.com!
%CRYPTO-6-IKMP_MODE_FAILURE: Processing of Aggressive mode
failed with peer at
20.20.20.21
----- Preshare, incompatable policy -----
wan2511#
*Mar  1 00:33:34.839: ISAKMP (17): processing SA payload. message ID = 0

```



```
*Mar 1 00:33:34.843: ISAKMP (17): Checking ISAKMP transform 1
against priority 1 policy
*Mar 1 00:33:34.843: ISAKMP: encryption DES-CBC
*Mar 1 00:33:34.843: ISAKMP: hash SHA
*Mar 1 00:33:34.847: ISAKMP: default group 2
*Mar 1 00:33:34.847: ISAKMP: auth pre-share
*Mar 1 00:33:34.847: ISAKMP: life type in seconds
*Mar 1 00:33:34.851: ISAKMP: life duration (basic) of 240
*Mar 1 00:33:34.851: ISAKMP (17): atts are acceptable.
Next payload is 0
*Mar 1 00:33:43.735: ISAKMP (17): processing KE payload.
message ID = 0
*Mar 1 00:33:54.307: ISAKMP (17): processing NONCE payload.
message ID = 0
*Mar 1 00:33:54.311: ISAKMP (17): processing ID payload.
message ID = 0
*Mar 1 00:33:54.331: ISAKMP (17): SKEYID state generated
*Mar 1 00:34:04.867: ISAKMP (17): processing HASH payload.
message ID = 0
*Mar 1 00:34:04.879: ISAKMP (17): SA has been authenticated
*Mar 1 00:34:06.151: ISAKMP (17): processing SA payload.
message ID = -1357683133
*Mar 1 00:34:06.155: ISAKMP (17): Checking IPsec proposal 1
*Mar 1 00:34:06.155: ISAKMP: transform 1, AH_MD5_HMAC
*Mar 1 00:34:06.159: ISAKMP: attributes in transform:
*Mar 1 00:34:06.159: ISAKMP: encaps is 1
*Mar 1 00:34:06.159: ISAKMP: SA life type in seconds
*Mar 1 00:34:06.163: ISAKMP: SA life duration (basic) of 3600
*Mar 1 00:34:06.163: ISAKMP: SA life type in kilobytes
*Mar 1 00:34:06.163: ISAKMP: SA life duration (VPI) of
0x0 0x46 0x50 0x0
*Mar 1 00:34:06.167: ISAKMP (17): atts not acceptable.
Next payload is 0
*Mar 1 00:34:06.171: ISAKMP (17): Checking IPsec proposal 1
*Mar 1 00:34:06.171: ISAKMP: transform 1, ESP_DES
*Mar 1 00:34:06.171: ISAKMP: attributes in transform:
*Mar 1 00:34:06.175: ISAKMP: encaps is 1
*Mar 1 00:34:06.175: ISAKMP: SA life type in seconds
*Mar 1 00:34:06.175: ISAKMP: SA life duration (basic) of 3600
*Mar 1 00:34:06.179: ISAKMP: SA life type in kilobytes
*Mar 1 00:34:06.179: ISAKMP: SA life duration (VPI) of
0x0 0x46 0x50 0x0
*Mar 1 00:34:06.183: ISAKMP: HMAC algorithm is SHA
*Mar 1 00:34:06.183: ISAKMP (17): atts are acceptable.
*Mar 1 00:34:06.187: ISAKMP (17): SA not acceptable!
%CRYPTO-6-IKMP_MODE_FAILURE: Processing of Quick mode failed
with peer at 20.20.20.20
wan2511#
```

```
----- preshare, debug isakmp -----
```

```
wan2511#
*Mar 1 00:06:54.179: ISAKMP (1): processing SA payload.
message ID = 0
*Mar 1 00:06:54.179: ISAKMP (1): Checking ISAKMP transform 1
against priority 1 policy
*Mar 1 00:06:54.183: ISAKMP: encryption DES-CBC
*Mar 1 00:06:54.183: ISAKMP: hash SHA
*Mar 1 00:06:54.183: ISAKMP: default group 2
*Mar 1 00:06:54.187: ISAKMP: auth pre-share
*Mar 1 00:06:54.187: ISAKMP: life type in seconds
*Mar 1 00:06:54.187: ISAKMP: life duration (basic) of 240
*Mar 1 00:06:54.191: ISAKMP (1): atts are acceptable.
Next payload is 0
```

*Mar 1 00:07:02.955: ISAKMP (1): processing KE payload.
message ID = 0

*Mar 1 00:07:13.411: ISAKMP (1): processing NONCE payload.
message ID = 0

*Mar 1 00:07:13.415: ISAKMP (1): processing ID payload.
message ID = 0

*Mar 1 00:07:13.435: ISAKMP (1): SKEYID state generated

*Mar 1 00:07:23.903: ISAKMP (1): processing HASH payload.
message ID = 0

*Mar 1 00:07:23.915: ISAKMP (1): SA has been authenticated

*Mar 1 00:07:25.187: ISAKMP (1): processing SA payload.
message ID = 1435594195

*Mar 1 00:07:25.187: ISAKMP (1): Checking IPsec proposal 1

*Mar 1 00:07:25.191: ISAKMP: transform 1, AH_SHA_HMAC

*Mar 1 00:07:25.191: ISAKMP: attributes in transform:

*Mar 1 00:07:25.191: ISAKMP: encaps is 1

*Mar 1 00:07:25.195: ISAKMP: SA life type in seconds

*Mar 1 00:07:25.195: ISAKMP: SA life duration (basic) of 3600

*Mar 1 00:07:25.195: ISAKMP: SA life type in kilobytes

*Mar 1 00:07:25.199: ISAKMP: SA life duration (VPI) of
0x0 0x46 0x50 0x0

*Mar 1 00:07:25.203: ISAKMP (1): atts are acceptable.

*Mar 1 00:07:25.203: ISAKMP (1): Checking IPsec proposal 1

*Mar 1 00:07:25.207: ISAKMP: transform 1, ESP_DES

*Mar 1 00:07:25.207: ISAKMP: attributes in transform:

*Mar 1 00:07:25.207: ISAKMP: encaps is 1

*Mar 1 00:07:25.211: ISAKMP: SA life type in seconds

*Mar 1 00:07:25.211: ISAKMP: SA life duration (basic) of 3600

*Mar 1 00:07:25.211: ISAKMP: SA life type in kilobytes

*Mar 1 00:07:25.215: ISAKMP: SA life duration (VPI) of
0x0 0x46 0x50 0x0

*Mar 1 00:07:25.215: ISAKMP: HMAC algorithm is SHA

*Mar 1 00:07:25.219: ISAKMP (1): atts are acceptable.

*Mar 1 00:07:25.223: ISAKMP (1): processing NONCE payload.
message ID = 1435594195

*Mar 1 00:07:25.227: ISAKMP (1): processing ID payload.
message ID = 1435594195

*Mar 1 00:07:25.227: ISAKMP (1): processing ID payload.
message ID = 1435594195

*Mar 1 00:07:25.639: ISAKMP (1): Creating IPsec SAs

*Mar 1 00:07:25.643: inbound SA from 20.20.20.20
to 20.20.20.21
(proxy 60.60.60.0 to 50.50.50.0)

*Mar 1 00:07:25.647: has spi 85067251 and
conn_id 3 and flags 4

*Mar 1 00:07:25.647: lifetime of 3600 seconds

*Mar 1 00:07:25.647: lifetime of 4608000 kilobytes

*Mar 1 00:07:25.651: outbound SA from 20.20.20.21
to 20.20.20.20
(proxy 50.50.50.0 to 60.60.60.0)

*Mar 1 00:07:25.655: has spi 57872298 and
conn_id 4 and flags 4

*Mar 1 00:07:25.655: lifetime of 3600 seconds

*Mar 1 00:07:25.655: lifetime of 4608000 kilobytes

*Mar 1 00:07:25.659: ISAKMP (1): Creating IPsec SAs

*Mar 1 00:07:25.659: inbound SA from 20.20.20.20
to 20.20.20.21
(proxy 60.60.60.0 to 50.50.50.0)

*Mar 1 00:07:25.663: has spi 538316566 and
conn_id 5 and flags 4

*Mar 1 00:07:25.663: lifetime of 3600 seconds

*Mar 1 00:07:25.667: lifetime of 4608000 kilobytes

*Mar 1 00:07:25.667: outbound SA from 20.20.20.21
to 20.20.20.20

```
(proxy 50.50.50.0      to 60.60.60.0      )
*Mar 1 00:07:25.671:      has spi 356000275 and
conn_id 6 and flags 4
*Mar 1 00:07:25.671:      lifetime of 3600 seconds
*Mar 1 00:07:25.675:      lifetime of 4608000 kilobytes
wan2511#

----- preshare debug ipsec -----
wan2511#
*Mar 1 00:05:26.947: IPSEC(validate_proposal_request):
proposal part #1,
(key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20,
dest_proxy= 50.50.50.0/0.0.0.0/0/0,
src_proxy= 60.60.60.0/0.0.0.16/0/0,
protocol= AH, transform= ah-sha-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
*Mar 1 00:05:26.955: IPSEC(validate_proposal_request):
proposal part #2,
(key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20,
dest_proxy= 50.50.50.0/0.0.0.0/0/0,
src_proxy= 60.60.60.0/0.0.0.16/0/0,
protocol= ESP, transform= esp-des esp-sha-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
*Mar 1 00:05:26.967: IPSEC(key_engine): got a queue event...
*Mar 1 00:05:26.971: IPSEC(spi_response): getting
spi 203563166 for SA
from 20.20.20.20      to 20.20.20.21      for prot 2
*Mar 1 00:05:26.975: IPSEC(spi_response): getting
spi 194838793 for SA
from 20.20.20.20      to 20.20.20.21      for prot 3
*Mar 1 00:05:27.379: IPSEC(key_engine): got a queue event...
*Mar 1 00:05:27.379: IPSEC(initialize_sas): ,
(key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20,
dest_proxy= 50.50.50.0/255.255.255.0/0/0,
src_proxy= 60.60.60.0/255.255.255.0/0/0,
protocol= AH, transform= ah-sha-hmac ,
lifedur= 3600s and 4608000kb,
spi= 0xC22209E(203563166), conn_id= 3, keysize= 0, flags= 0x4
*Mar 1 00:05:27.387: IPSEC(initialize_sas): ,
(key eng. msg.) SRC= 20.20.20.21, dest= 20.20.20.20,
src_proxy= 50.50.50.0/255.255.255.0/0/0,
dest_proxy= 60.60.60.0/255.255.255.0/0/0,
protocol= AH, transform= ah-sha-hmac ,
lifedur= 3600s and 4608000kb,
spi= 0x15E010D(22937869), conn_id= 4, keysize= 0, flags= 0x4
*Mar 1 00:05:27.395: IPSEC(initialize_sas): ,
(key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20,
dest_proxy= 50.50.50.0/255.255.255.0/0/0,
src_proxy= 60.60.60.0/255.255.255.0/0/0,
protocol= ESP, transform= esp-des esp-sha-hmac ,
lifedur= 3600s and 4608000kb,
spi= 0xB9D0109(194838793), conn_id= 5, keysize= 0, flags= 0x4
*Mar 1 00:05:27.403: IPSEC(initialize_sas): ,
(key eng. msg.) SRC= 20.20.20.21, dest= 20.20.20.20,
src_proxy= 50.50.50.0/255.255.255.0/0/0,
dest_proxy= 60.60.60.0/255.255.255.0/0/0,
protocol= ESP, transform= esp-des esp-sha-hmac ,
lifedur= 3600s and 4608000kb,
spi= 0xDEDOAB4(233638580), conn_id= 6, keysize= 0, flags= 0x4
*Mar 1 00:05:27.415: IPSEC(create_sa): sa created,
(sa) sa_dest= 20.20.20.21, sa_prot= 51,
sa_spi= 0xC22209E(203563166),
```

```
sa_trans= ah-sha-hmac , sa_conn_id= 3
*Mar 1 00:05:27.419: IPSEC(create_sa): sa created,
(sa) sa_dest= 20.20.20.20, sa_prot= 51,
sa_spi= 0x15E010D(22937869),
sa_trans= ah-sha-hmac , sa_conn_id= 4
*Mar 1 00:05:27.423: IPSEC(create_sa): sa created,
(sa) sa_dest= 20.20.20.21, sa_prot= 50,
sa_spi= 0xB9D0109(194838793),
sa_trans= esp-des esp-sha-hmac , sa_conn_id= 5
*Mar 1 00:05:27.427: IPSEC(create_sa): sa created,
(sa) sa_dest= 20.20.20.20, sa_prot= 50,
sa_spi= 0xDEDOAB4(233638580),
sa_trans= esp-des esp-sha-hmac , sa_conn_id= 6
wan2511#
```

```
----- Preshare, good connection -----
wan2511#
```

```
*Mar 1 00:09:45.095: ISAKMP (1): processing SA payload.
message ID = 0
*Mar 1 00:09:45.099: ISAKMP (1): Checking ISAKMP transform
1 against priority 1 policy
*Mar 1 00:09:45.099: ISAKMP: encryption DES-CBC
*Mar 1 00:09:45.103: ISAKMP: hash SHA
*Mar 1 00:09:45.103: ISAKMP: default group 2
*Mar 1 00:09:45.103: ISAKMP: auth pre-share
*Mar 1 00:09:45.107: ISAKMP: life type in seconds
*Mar 1 00:09:45.107: ISAKMP: life duration (basic) of 240
*Mar 1 00:09:45.107: ISAKMP (1): atts are acceptable.
Next payload is 0
*Mar 1 00:09:53.867: ISAKMP (1): processing KE payload.
message ID = 0
*Mar 1 00:10:04.323: ISAKMP (1): processing NONCE payload.
message ID = 0
*Mar 1 00:10:04.327: ISAKMP (1): processing ID payload.
message ID = 0
*Mar 1 00:10:04.347: ISAKMP (1): SKEYID state generated
*Mar 1 00:10:15.103: ISAKMP (1): processing HASH payload.
message ID = 0
*Mar 1 00:10:15.115: ISAKMP (1): SA has been authenticated
*Mar 1 00:10:16.391: ISAKMP (1): processing SA payload.
message ID = 800032287
*Mar 1 00:10:16.391: ISAKMP (1): Checking IPsec proposal 1
*Mar 1 00:10:16.395: ISAKMP: transform 1, AH_SHA_HMAC
*Mar 1 00:10:16.395: ISAKMP: attributes in transform:
*Mar 1 00:10:16.395: ISAKMP: encaps is 1
*Mar 1 00:10:16.399: ISAKMP: SA life type in seconds
*Mar 1 00:10:16.399: ISAKMP: SA life duration (basic) of 3600
*Mar 1 00:10:16.399: ISAKMP: SA life type in kilobytes
*Mar 1 00:10:16.403: ISAKMP: SA life duration (VPI) of
0x0 0x46 0x50 0x0
*Mar 1 00:10:16.407: ISAKMP (1): atts are acceptable.
*Mar 1 00:10:16.407: ISAKMP (1): Checking IPsec proposal 1
*Mar 1 00:10:16.411: ISAKMP: transform 1, ESP_DES
*Mar 1 00:10:16.411: ISAKMP: attributes in transform:
*Mar 1 00:10:16.411: ISAKMP: encaps is 1
*Mar 1 00:10:16.415: ISAKMP: SA life type in seconds
*Mar 1 00:10:16.415: ISAKMP: SA life duration (basic) of 3600
*Mar 1 00:10:16.415: ISAKMP: SA life type in kilobytes
*Mar 1 00:10:16.419: ISAKMP: SA life duration (VPI) of
0x0 0x46 0x50 0x0
*Mar 1 00:10:16.419: ISAKMP: HMAC algorithm is SHA
*Mar 1 00:10:16.423: ISAKMP (1): atts are acceptable.
*Mar 1 00:10:16.427: IPSEC(validate_proposal_request):
proposal part #1,
```

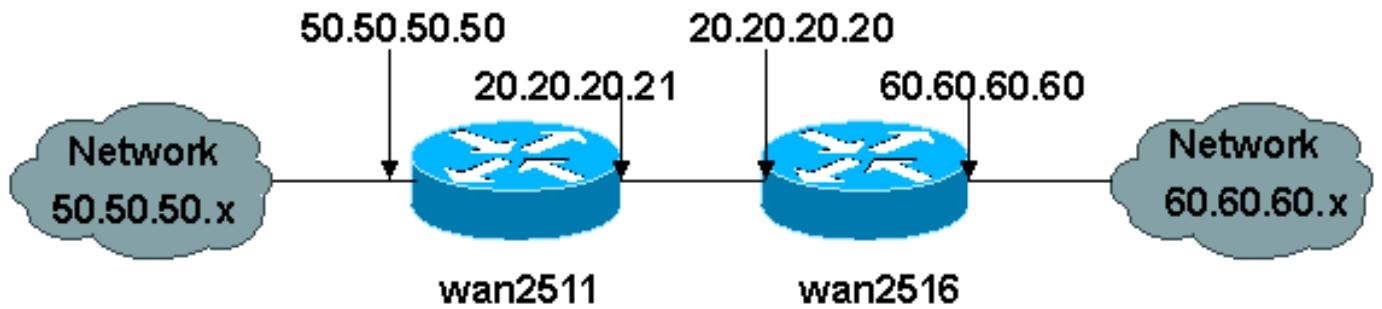
```
(key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20,
dest_proxy= 50.50.50.0/0.0.0.0/0/0,
src_proxy= 60.60.60.0/0.0.0.16/0/0,
protocol= AH, transform= ah-sha-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
*Mar 1 00:10:16.435: IPSEC(validate_proposal_request):
proposal part #2,
(key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20,
dest_proxy= 50.50.50.0/0.0.0.0/0/0,
src_proxy= 60.60.60.0/0.0.0.16/0/0,
protocol= ESP, transform= esp-des esp-sha-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
*Mar 1 00:10:16.443: ISAKMP (1): processing NONCE payload.
message ID = 800032287
*Mar 1 00:10:16.443: ISAKMP (1): processing ID payload.
message ID = 800032287
*Mar 1 00:10:16.447: ISAKMP (1): processing ID payload.
message ID = 800032287
*Mar 1 00:10:16.451: IPSEC(key_engine): got a queue event...
*Mar 1 00:10:16.455: IPSEC(spi_response): getting
spi 16457800 for SA
    from 20.20.20.20    to 20.20.20.21    for prot 2
*Mar 1 00:10:16.459: IPSEC(spi_response): getting
spi 305534655 for SA
    from 20.20.20.20    to 20.20.20.21    for prot 3
*Mar 1 00:10:17.095: ISAKMP (1): Creating IPsec SAs
*Mar 1 00:10:17.095:    inbound SA from 20.20.20.20
to 20.20.20.21
    (proxy 60.60.60.0    to 50.50.50.0    )
*Mar 1 00:10:17.099:    has spi 16457800 and conn_id 3
and flags 4
*Mar 1 00:10:17.103:    lifetime of 3600 seconds
*Mar 1 00:10:17.103:    lifetime of 4608000 kilobytes
*Mar 1 00:10:17.103:    outbound SA from 20.20.20.21
to 20.20.20.20
    (proxy 50.50.50.0    to 60.60.60.0    )
*Mar 1 00:10:17.107:    has spi 507120385 and conn_id 4
and flags 4
*Mar 1 00:10:17.111:    lifetime of 3600 seconds
*Mar 1 00:10:17.111:    lifetime of 4608000 kilobytes
*Mar 1 00:10:17.115: ISAKMP (1): Creating IPsec SAs
*Mar 1 00:10:17.115:    inbound SA from 20.20.20.20
to 20.20.20.21
    (proxy 60.60.60.0    to 50.50.50.0    )
*Mar 1 00:10:17.119:    has spi 305534655 and
conn_id 5 and flags 4
*Mar 1 00:10:17.119:    lifetime of 3600 seconds
*Mar 1 00:10:17.123:    lifetime of 4608000 kilobytes
*Mar 1 00:10:17.123:    outbound SA from 20.20.20.21
to 20.20.20.20
    (proxy 50.50.50.0    to 60.60.60.0    )
*Mar 1 00:10:17.127:    has spi 554175376 and
conn_id 6 and flags 4
*Mar 1 00:10:17.127:    lifetime of 3600 seconds
*Mar 1 00:10:17.131:    lifetime of 4608000 kilobytes
*Mar 1 00:10:17.139: IPSEC(key_engine): got a queue event...
*Mar 1 00:10:17.143: IPSEC(initialize_sas): ,
(key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20,
dest_proxy= 50.50.50.0/255.255.255.0/0/0,
src_proxy= 60.60.60.0/255.255.255.0/0/0,
protocol= AH, transform= ah-sha-hmac ,
lifedur= 3600s and 4608000kb,
```

```
spi= 0xFB2048(16457800), conn_id= 3, keysize= 0,
flags= 0x4
*Mar 1 00:10:17.151: IPSEC(initialize_sas): ,
(key eng. msg.) SRC= 20.20.20.21, dest= 20.20.20.20,
src_proxy= 50.50.50.0/255.255.255.0/0/0,
dest_proxy= 60.60.60.0/255.255.255.0/0/0,
protocol= AH, transform= ah-sha-hmac ,
lifedur= 3600s and 4608000kb,
spi= 0x1E3A0B01(507120385), conn_id= 4, keysize= 0,
flags= 0x4
*Mar 1 00:10:17.159: IPSEC(initialize_sas): ,
(key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20,
dest_proxy= 50.50.50.0/255.255.255.0/0/0,
src_proxy= 60.60.60.0/255.255.255.0/0/0,
protocol= ESP, transform= esp-des esp-sha-hmac ,
lifedur= 3600s and 4608000kb,
spi= 0x123616BF(305534655), conn_id= 5, keysize= 0,
flags= 0x4
*Mar 1 00:10:17.167: IPSEC(initialize_sas): ,
(key eng. msg.) SRC= 20.20.20.21, dest= 20.20.20.20,
src_proxy= 50.50.50.0/255.255.255.0/0/0,
dest_proxy= 60.60.60.0/255.255.255.0/0/0,
protocol= ESP, transform= esp-des esp-sha-hmac ,
lifedur= 3600s and 4608000kb,
spi= 0x21080B90(554175376), conn_id= 6, keysize= 0,
flags= 0x4
*Mar 1 00:10:17.175: IPSEC(create_sa): sa created,
(sa) sa_dest= 20.20.20.21, sa_prot= 51,
sa_spi= 0xFB2048(16457800),
sa_trans= ah-sha-hmac , sa_conn_id= 3
*Mar 1 00:10:17.179: IPSEC(create_sa): sa created,
(sa) sa_dest= 20.20.20.20, sa_prot= 51,
sa_spi= 0x1E3A0B01(507120385),
sa_trans= ah-sha-hmac , sa_conn_id= 4
*Mar 1 00:10:17.183: IPSEC(create_sa): sa created,
(sa) sa_dest= 20.20.20.21, sa_prot= 50,
sa_spi= 0x123616BF(305534655),
sa_trans= esp-des esp-sha-hmac , sa_conn_id= 5
*Mar 1 00:10:17.187: IPSEC(create_sa): sa created,
(sa) sa_dest= 20.20.20.20, sa_prot= 50,
sa_spi= 0x21080B90(554175376),
sa_trans= esp-des esp-sha-hmac , sa_conn_id= 6
*Mar 1 00:10:36.583: ISADB: reaper checking SA, conn_id = 1
wan2511#
```

例 2 : ISAKMP : RSA 暗号化された認証

このシナリオでは、共有秘密鍵は作成されません。それぞれのルータによってその独自の RSA 鍵が生成されます。次に、それぞれのルータではピアの RSA 公開鍵を設定する必要があります。これは手動のプロセスであるため、スケーリングの制限が明確に存在します。つまり、ルータには、セキュリティ アソシエーションを設定する必要がある各ピアの公開 RSA 鍵を含める必要があります。

次のドキュメントは、この設定例のネットワーク ダイアグラムを示しています。



この例では、各ルータによって RSA 鍵ペアが生成され (生成する RSA 秘密鍵は表示されません)、リモートピアの公開 RSA 鍵が設定されています。

```
wan2511(config)#crypto key generate rsa The name for the keys will be: wan2511.cisco.com Choose
the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing
a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]:
Generating RSA keys ... [OK] wan2511(config)#^Z wan2511# wan2511#show crypto key mypubkey rsa %
Key pair was generated at: 00:09:04 UTC Mar 1 1993 Key name: wan2511.cisco.com Usage: General
Purpose Key Key Data: 305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00E9007B E5CD7DC8
6E1C0423 92044254 92C972AD 0CCE9796 86797EAA B6C4EFF0 0F0A5378 6AFAE43B 3A2BD92F 98039DAC
08741E82 5D9053C4 D9CFABC1 AB54E0E2 BB020301 0001 wan2511# wan2511(config)#crypto key pubkey-
chain rsa wan2511(config-pubkey-chain)#named-key wan2516.cisco.com wan2511(config-pubkey-
key)#key-string Enter a public key as a hexadecimal number ... wan2511(config-pubkey)#$86F70D
01010105 00034B00 30480241 00DC3DDC 59885F14 wan2511(config-pubkey)#$D918DE FC7ADB76 B0B9DD1A
ABAF4884 009E758C 4064C699 wan2511(config-pubkey)#$220CB9 31E267F8 0259C640 F8DE4169 1F020301
0001 wan2511(config-pubkey)#quit wan2511(config-pubkey-key)#^Z wan2511# wan2511#show crypto key
pubkey-chain rsa Key name: wan2516.cisco.com Key usage: general purpose Key source: manually
entered Key data: 305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00DC3DDC 59885F14
1AB30DCB 794AB5C7 82D918DE FC7ADB76 B0B9DD1A ABAF4884 009E758C 4064C699 3BC9D17E C47581DC
50220CB9 31E267F8 0259C640 F8DE4169 1F020301 0001 wan2511# wan2511#write terminal Building
configuration... Current configuration: ! version 11.3 service timestamps debug datetime msec no
service password-encryption ! hostname wan2511 ! enable password ww ! no ip domain-lookup ip
host wan2516.cisco.com 20.20.20.20 ip domain-name cisco.com ! crypto isakmp policy 1
authentication rsa-encr group 2 lifetime 240 crypto isakmp identity hostname ! crypto ipsec
transform-set auth2 ah-sha-hmac esp-des esp-sha-hmac ! crypto map test 10 ipsec-isakmp set peer
20.20.20.20 set transform-set auth2 match address 133 ! crypto key pubkey-chain rsa named-key
wan2516.cisco.com key-string 305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00DC3DDC
59885F14 1AB30DCB 794AB5C7 82D918DE FC7ADB76 B0B9DD1A ABAF4884 009E758C 4064C699 3BC9D17E
C47581DC 50220CB9 31E267F8 0259C640 F8DE4169 1F020301 0001 quit ! interface Ethernet0 ip address
50.50.50.50 255.255.255.0 ! interface Serial0 ip address 20.20.20.21 255.255.255.0 encapsulation
ppp no ip mroute-cache crypto map test ! interface Serial1 no ip address shutdown ! ip classless
ip route 0.0.0.0 0.0.0.0 10.11.19.254 ip route 60.0.0.0 255.0.0.0 20.20.20.20 access-list 133
permit ip 50.50.50.0 0.0.0.255 60.60.60.0 0.0.0.255 ! line con 0 exec-timeout 0 0 password ww
login line 1 6 modem InOut transport input all speed 115200 flowcontrol hardware line 7 16
autoselect ppp modem InOut transport input all speed 115200 flowcontrol hardware line aux 0
login local modem InOut transport input all flowcontrol hardware line vty 0 4 password ww login
! end wan2511# ----- wan2516(config)#crypto key generate rsa The name for the keys
will be: wan2516.cisco.com Choose the size of the key modulus in the range of 360 to 2048 for
your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes. How
many bits in the modulus [512]: Generating RSA keys ... [OK] wan2516#show crypto key mypubkey
rsa % Key pair was generated at: 00:06:35 UTC Mar 1 1993 Key name: wan2516.cisco.com Usage:
General Purpose Key Key Data: 305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00DC3DDC
59885F14 1AB30DCB 794AB5C7 82D918DE FC7ADB76 B0B9DD1A ABAF4884 009E758C 4064C699 3BC9D17E
C47581DC 50220CB9 31E267F8 0259C640 F8DE4169 1F020301 0001 wan2516# -----
wan2516(config)#crypto key exchange ? dss Exchange DSS keys ----- wan2516(config)#crypto key
pubkey-chain rsa wan2516(config-pubkey-chain)#named-key wan2511.cisco.com wan2516(config-pubkey-
key)#key-string Enter a public key as a hexadecimal number ... wan2516(config-pubkey)#$86F70D
01010105 00034B00 30480241 00E9007B E5CD7DC8 wan2516(config-pubkey)#$C972AD 0CCE9796 86797EAA
B6C4EFF0 0F0A5378 6AFAE43B wan2516(config-pubkey)#$741E82 5D9053C4 D9CFABC1 AB54E0E2 BB020301
0001 wan2516(config-pubkey)#quit wan2516(config-pubkey-key)#^Z wan2516#show crypto key pubkey
rsa Key name: wan2511.cisco.com Key usage: general purpose Key source: manually entered Key
```

data: 305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00E9007B E5CD7DC8 6E1C0423 92044254
92C972AD 0CCE9796 86797EAA B6C4EFF0 0F0A5378 6AFAE43B 3A2BD92F 98039DAC 08741E82 5D9053C4
D9CFABC1 AB54E0E2 BB020301 0001 wan2516# ----- wan2516#**write terminal**
Building configuration... Current configuration: ! version 11.3 no service pad service
timestamps debug datetime msec no service password-encryption service udp-small-servers service
tcp-small-servers ! hostname wan2516 ! enable password ww ! no ip domain-lookup ip host
wan2511.cisco.com 20.20.20.21 ip domain-name cisco.com ! crypto isakmp policy 1 authentication
rsa-encr group 2 lifetime 240 crypto isakmp identity hostname ! crypto ipsec transform-set auth2
ah-sha-hmac esp-des esp-sha-hmac ! crypto map test 10 ipsec-isakmp set peer 20.20.20.21 set
transform-set auth2 match address 144 ! crypto key pubkey-chain rsa named-key wan2511.cisco.com
key-string 305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00E9007B E5CD7DC8 6E1C0423
92044254 92C972AD 0CCE9796 86797EAA B6C4EFF0 0F0A5378 6AFAE43B 3A2BD92F 98039DAC 08741E82
5D9053C4 D9CFABC1 AB54E0E2 BB020301 0001 quit ! hub ether 0 1 link-test auto-polarity !
interface Loopback0 ip address 70.70.70.1 255.255.255.0 no ip route-cache no ip mroute-cache !
interface Ethernet0 ip address 60.60.60.60 255.255.255.0 ! interface Serial0 ip address
20.20.20.20 255.255.255.0 encapsulation ppp clockrate 2000000 crypto map test ! interface
Serial1 no ip address no ip route-cache no ip mroute-cache shutdown ! interface BRI0 no ip
address no ip route-cache no ip mroute-cache shutdown ! ip default-gateway 20.20.20.21 ip
classless ip route 0.0.0.0 0.0.0.0 20.20.20.21 access-list 144 permit ip 60.60.60.0 0.0.0.255
50.50.50.0 0.0.0.255 ! line con 0 exec-timeout 0 0 password ww login line aux 0 password ww
login modem InOut transport input all flowcontrol hardware line vty 0 4 password ww login ! end
wan2516# ----- RSA-enc missing RSA Keys ----- *Mar 1 00:02:51.147: ISAKMP: No
cert, and no keys (public or pre-shared) with remote peer 20.20.20.21 *Mar 1 00:02:51.151:
ISAKMP: No cert, and no keys (public or pre-shared) with remote peer 20.20.20.21 -----
RSA-enc good connection ----- wan2511# *Mar 1 00:21:46.375: ISAKMP (1): processing
SA payload. message ID = 0 *Mar 1 00:21:46.379: ISAKMP (1): Checking ISAKMP transform 1 against
priority 1 policy *Mar 1 00:21:46.379: ISAKMP: encryption DES-CBC *Mar 1 00:21:46.379: ISAKMP:
hash SHA *Mar 1 00:21:46.383: ISAKMP: default group 2 *Mar 1 00:21:46.383: ISAKMP: auth RSA encr
*Mar 1 00:21:46.383: ISAKMP: life type in seconds *Mar 1 00:21:46.387: ISAKMP: life duration
(basic) of 240 *Mar 1 00:21:46.387: ISAKMP (1): atts are acceptable. Next payload is 0 *Mar 1
00:21:46.391: Crypto engine 0: generate alg param *Mar 1 00:21:55.159: CRYPTO_ENGINE: Dh phase 1
status: 0 *Mar 1 00:21:55.163: CRYPTO: DH gen phase 1 status for conn_id 1 slot 0:OK *Mar 1
00:21:55.167: ISAKMP (1): Unable to get router cert to find DN! *Mar 1 00:21:55.171: ISAKMP (1):
SA is doing RSA encryption authentication *Mar 1 00:22:04.351: ISAKMP (1): processing KE
payload. message ID = 0 *Mar 1 00:22:04.351: Crypto engine 0: generate alg param *Mar 1
00:22:14.767: CRYPTO: DH gen phase 2 status for conn_id 1 slot 0:OK *Mar 1 00:22:14.771: ISAKMP
(1): processing ID payload. message ID = 0 *Mar 1 00:22:14.775: Crypto engine 0: RSA decrypt
with private key *Mar 1 00:22:15.967: CRYPTO_ENGINE: key process suspended and continued *Mar 1
00:22:16.167: CRYPTO_ENGINE: key process suspended and continued *Mar 1 00:22:16.367:
CRYPTO_ENGINE: key process suspended and continued *Mar 1 00:22:16.579: CRYPTO_ENGINE: key
process suspended and continued *Mar 1 00:22:16.787: CRYPTO_ENGINE: key process suspended and
continued *Mar 1 00:22:16.987: CRYPTO_ENGINE: key process suspended and continued *Mar 1
00:22:17.215: CRYPTO_ENGINE: key process suspended and continued *Mar 1 00:22:17.431:
CRYPTO_ENGINE: key process suspended and continued *Mar 1 00:22:17.539: CRYPTO: RSA private
decrypt finished with status=OK *Mar 1 00:22:17.543: ISAKMP (1): processing NONCE payload.
message ID = 0 *Mar 1 00:22:17.543: Crypto engine 0: RSA decrypt with private key *Mar 1
00:22:18.735: CRYPTO_ENGINE: key process suspended and continued *Mar 1 00:22:18.947:
CRYPTO_ENGINE: key process suspended and continued *Mar 1 00:22:19.155: CRYPTO_ENGINE: key
process suspended and continued *Mar 1 00:22:19.359: CRYPTO_ENGINE: key process suspended and
continued *Mar 1 00:22:19.567: CRYPTO_ENGINE: key process suspended and continued *Mar 1
00:22:19.767: CRYPTO_ENGINE: key process suspended and continued *Mar 1 00:22:19.975:
CRYPTO_ENGINE: key process suspended and continued *Mar 1 00:22:20.223: CRYPTO_ENGINE: key
process suspended and continued *Mar 1 00:22:20.335: CRYPTO: RSA private decrypt finished with
status=OK *Mar 1 00:22:20.347: Crypto engine 0: create ISAKMP SKEYID for conn id 1 *Mar 1
00:22:20.363: ISAKMP (1): SKEYID state generated *Mar 1 00:22:20.367: Crypto engine 0: RSA
encrypt with public key *Mar 1 00:22:20.567: CRYPTO: RSA public encrypt finished with status=OK
*Mar 1 00:22:20.571: Crypto engine 0: RSA encrypt with public key *Mar 1 00:22:20.767: CRYPTO:
RSA public encrypt finished with status=OK *Mar 1 00:22:20.775: ISAKMP (1): processing KE
payload. message ID = 0 *Mar 1 00:22:20.775: ISAKMP (1): processing ID payload. message ID = 0
*Mar 1 00:22:20.779: Crypto engine 0: RSA decrypt with private key *Mar 1 00:22:21.959:
CRYPTO_ENGINE: key process suspended and continued *Mar 1 00:22:22.187: CRYPTO_ENGINE: key
process suspended and continued *Mar 1 00:22:22.399: CRYPTO_ENGINE: key process suspended and
continued *Mar 1 00:22:22.599: CRYPTO_ENGINE: key process suspended and continued *Mar 1
00:22:22.811: CRYPTO_ENGINE: key process suspended and continued *Mar 1 00:22:23.019:

CRYPTO_ENGINE: key process suspended and continued *Mar 1 00:22:23.223: CRYPTO_ENGINE: key process suspended and continued *Mar 1 00:22:23.471: CRYPTO_ENGINE: key process suspended and continued *Mar 1 00:22:23.583: CRYPTO: RSA private decrypt finished with status=OK *Mar 1 00:22:23.583: ISAKMP (1): processing NONCE payload. message ID = 0 %CRYPTO-6-IKMP_AUTH_FAIL: Authentication method 4 failed with host 20.20.20.20 %CRYPTO-6-IKMP_MODE_FAILURE: Processing of Main mode failed with peer at 20.20.20.20 *Mar 1 00:22:36.955: ISAKMP (1): processing HASH payload. message ID = 0 *Mar 1 00:22:36.959: generate hmac context for conn id 1 *Mar 1 00:22:36.971: ISAKMP (1): SA has been authenticated *Mar 1 00:22:36.975: generate hmac context for conn id 1 *Mar 1 00:22:37.311: generate hmac context for conn id 1 *Mar 1 00:22:37.319: ISAKMP (1): processing SA payload. message ID = -114148384 *Mar 1 00:22:37.319: ISAKMP (1): Checking IPsec proposal 1 *Mar 1 00:22:37.323: ISAKMP: transform 1, AH_SHA_HMAC *Mar 1 00:22:37.323: ISAKMP: attributes in transform: *Mar 1 00:22:37.327: ISAKMP: encaps is 1 *Mar 1 00:22:37.327: ISAKMP: SA life type in seconds *Mar 1 00:22:37.327: ISAKMP: SA life duration (basic) of 3600 *Mar 1 00:22:37.331: ISAKMP: SA life type in kilobytes *Mar 1 00:22:37.331: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 *Mar 1 00:22:37.335: ISAKMP (1): atts are acceptable. *Mar 1 00:22:37.335: ISAKMP (1): Checking IPsec proposal 1 *Mar 1 00:22:37.339: ISAKMP: transform 1, ESP_DES *Mar 1 00:22:37.339: ISAKMP: attributes in transform: *Mar 1 00:22:37.339: ISAKMP: encaps is 1 *Mar 1 00:22:37.343: ISAKMP: SA life type in seconds *Mar 1 00:22:37.343: ISAKMP: SA life duration (basic) of 3600 *Mar 1 00:22:37.347: ISAKMP: SA life type in kilobytes *Mar 1 00:22:37.347: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 *Mar 1 00:22:37.351: ISAKMP: HMAC algorithm is SHA *Mar 1 00:22:37.351: ISAKMP (1): atts are acceptable. *Mar 1 00:22:37.355: IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20, dest_proxy= 50.50.50.0/0.0.0.0/0/0, src_proxy= 60.60.60.0/0.0.0.16/0/0, protocol= AH, transform= ah-sha-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4 *Mar 1 00:22:37.363: IPSEC(validate_proposal_request): proposal part #2, (key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20, dest_proxy= 50.50.50.0/0.0.0.0/0/0, src_proxy= 60.60.60.0/0.0.0.16/0/0, protocol= ESP, transform= esp-des esp-sha-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4 *Mar 1 00:22:37.371: ISAKMP (1): processing NONCE payload. message ID = -114148384 *Mar 1 00:22:37.375: ISAKMP (1): processing ID payload. message ID = -114148384 *Mar 1 00:22:37.375: ISAKMP (1): processing ID payload. message ID = -114148384 *Mar 1 00:22:37.379: IPSEC(key_engine): got a queue event... *Mar 1 00:22:37.383: IPSEC(spi_response): getting spi 531040311 for SA from 20.20.20.20 to 20.20.20.21 for prot 2 *Mar 1 00:22:37.387: IPSEC(spi_response): getting spi 220210147 for SA from 20.20.20.20 to 20.20.20.21 for prot 3 *Mar 1 00:22:37.639: generate hmac context for conn id 1 *Mar 1 00:22:37.931: generate hmac context for conn id 1 *Mar 1 00:22:37.975: ISAKMP (1): Creating IPsec SAs *Mar 1 00:22:37.975: inbound SA from 20.20.20.20 to 20.20.20.21 (proxy 60.60.60.0 to 50.50.50.0) *Mar 1 00:22:37.979: has spi 531040311 and conn_id 2 and flags 4 *Mar 1 00:22:37.979: lifetime of 3600 seconds *Mar 1 00:22:37.983: lifetime of 4608000 kilobytes *Mar 1 00:22:37.983: outbound SA from 20.20.20.21 to 20.20.20.20 (proxy 50.50.50.0 to 60.60.60.0) *Mar 1 00:22:37.987: has spi 125043658 and conn_id 3 and flags 4 *Mar 1 00:22:37.987: lifetime of 3600 seconds *Mar 1 00:22:37.991: lifetime of 4608000 kilobytes *Mar 1 00:22:37.991: ISAKMP (1): Creating IPsec SAs *Mar 1 00:22:37.991: inbound SA from 20.20.20.20 to 20.20.20.21 (proxy 60.60.60.0 to 50.50.50.0) *Mar 1 00:22:37.995: has spi 220210147 and conn_id 4 and flags 4 *Mar 1 00:22:37.999: lifetime of 3600 seconds *Mar 1 00:22:37.999: lifetime of 4608000 kilobytes *Mar 1 00:22:38.003: outbound SA from 20.20.20.21 to 20.20.20.20 (proxy 50.50.50.0 to 60.60.60.0) *Mar 1 00:22:38.003: has spi 299247102 and conn_id 5 and flags 4 *Mar 1 00:22:38.007: lifetime of 3600 seconds *Mar 1 00:22:38.007: lifetime of 4608000 kilobytes *Mar 1 00:22:38.011: IPSEC(key_engine): got a queue event... *Mar 1 00:22:38.015: IPSEC(initialize_sas): , (key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20, dest_proxy= 50.50.50.0/255.255.255.0/0/0, src_proxy= 60.60.60.0/255.255.255.0/0/0, protocol= AH, transform= ah-sha-hmac , lifedur= 3600s and 4608000kb, spi= 0x1FA70837(531040311), conn_id= 2, keysize= 0, flags= 0x4 *Mar 1 00:22:38.023: IPSEC(initialize_sas): , (key eng. msg.) SRC= 20.20.20.21, dest= 20.20.20.20, src_proxy= 50.50.50.0/255.255.255.0/0/0, dest_proxy= 60.60.60.0/255.255.255.0/0/0, protocol= AH, transform= ah-sha-hmac , lifedur= 3600s and 4608000kb, spi= 0x77403CA(125043658), conn_id= 3, keysize= 0, flags= 0x4 *Mar 1 00:22:38.031: IPSEC(initialize_sas): , (key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20, dest_proxy= 50.50.50.0/255.255.255.0/0/0, src_proxy= 60.60.60.0/255.255.255.0/0/0, protocol= ESP, transform= esp-des esp-sha-hmac , lifedur= 3600s and 4608000kb, spi= 0xD2023E3(220210147), conn_id= 4, keysize= 0, flags= 0x4 *Mar 1 00:22:38.039: IPSEC(initialize_sas): , (key eng. msg.) SRC= 20.20.20.21, dest= 20.20.20.20, src_proxy= 50.50.50.0/255.255.255.0/0/0, dest_proxy= 60.60.60.0/255.255.255.0/0/0, protocol= ESP, transform= esp-des esp-sha-hmac , lifedur= 3600s and 4608000kb, spi= 0x11D625FE(299247102), conn_id= 5, keysize= 0, flags= 0x4 *Mar 1 00:22:38.047: IPSEC(create_sa): sa created, (sa) sa_dest= 20.20.20.21, sa_prot= 51, sa_spi= 0x1FA70837(531040311), sa_trans= ah-sha-hmac , sa_conn_id= 2 *Mar 1 00:22:38.051:

IPSEC(create_sa): sa created, (sa) sa_dest= 20.20.20.20, sa_prot= 51, sa_spi= 0x77403CA(125043658), sa_trans= ah-sha-hmac , sa_conn_id= 3 *Mar 1 00:22:38.055:
IPSEC(create_sa): sa created, (sa) sa_dest= 20.20.20.21, sa_prot= 50, sa_spi= 0xD2023E3(220210147), sa_trans= esp-des esp-sha-hmac , sa_conn_id= 4 *Mar 1 00:22:38.063:
IPSEC(create_sa): sa created, (sa) sa_dest= 20.20.20.20, sa_prot= 50, sa_spi= 0x11D625FE(299247102), sa_trans= esp-des esp-sha-hmac , sa_conn_id= 5 wan2511# ----- RSA-
ENC ISAKMP debugs good connection --- wan2511# *Mar 1 00:27:23.279: ISAKMP (6): processing SA
payload. message ID = 0 *Mar 1 00:27:23.279: ISAKMP (6): Checking ISAKMP transform 1 against
priority 1 policy *Mar 1 00:27:23.283: ISAKMP: encryption DES-CBC *Mar 1 00:27:23.283: ISAKMP:
hash SHA *Mar 1 00:27:23.283: ISAKMP: default group 2 *Mar 1 00:27:23.287: ISAKMP: auth RSA encr
*Mar 1 00:27:23.287: ISAKMP: life type in seconds *Mar 1 00:27:23.287: ISAKMP: life duration
(basic) of 240 *Mar 1 00:27:23.291: ISAKMP (6): atts are acceptable. Next payload is 0 *Mar 1
00:27:32.055: ISAKMP (6): Unable to get router cert to find DN! *Mar 1 00:27:32.055: ISAKMP (6):
SA is doing RSA encryption authentication *Mar 1 00:27:41.183: ISAKMP (6): processing KE
payload. message ID = 0 *Mar 1 00:27:51.779: ISAKMP (6): processing ID payload. message ID = 0
*Mar 1 00:27:54.507: ISAKMP (6): processing NONCE payload. message ID = 0 *Mar 1 00:27:57.239:
ISAKMP (6): SKEYID state generated *Mar 1 00:27:57.627: ISAKMP (6): processing KE payload.
message ID = 0 *Mar 1 00:27:57.631: ISAKMP (6): processing ID payload. message ID = 0 *Mar 1
00:28:00.371: ISAKMP (6): processing NONCE payload. message ID = 0 %CRYPTO-6-IKMP_AUTH_FAIL:
Authentication method 4 failed with host 20.20.20.20 %CRYPTO-6-IKMP_MODE_FAILURE: Processing of
Main mode failed with peer at 20.20.20.20 *Mar 1 00:28:13.587: ISAKMP (6): processing HASH
payload. message ID = 0 *Mar 1 00:28:13.599: ISAKMP (6): SA has been authenticated *Mar 1
00:28:13.939: ISAKMP (6): processing SA payload. message ID = -161552401 *Mar 1 00:28:13.943:
ISAKMP (6): Checking IPsec proposal 1 *Mar 1 00:28:13.943: ISAKMP: transform 1, AH_SHA_HMAC *Mar
1 00:28:13.943: ISAKMP: attributes in transform: *Mar 1 00:28:13.947: ISAKMP: encaps is 1 *Mar 1
00:28:13.947: ISAKMP: SA life type in seconds *Mar 1 00:28:13.947: ISAKMP: SA life duration
(basic) of 3600 *Mar 1 00:28:13.951: ISAKMP: SA life type in kilobytes *Mar 1 00:28:13.951:
ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 *Mar 1 00:28:13.955: ISAKMP (6): atts are
acceptable. *Mar 1 00:28:13.959: ISAKMP (6): Checking IPsec proposal 1 *Mar 1 00:28:13.959:
ISAKMP: transform 1, ESP_DES *Mar 1 00:28:13.959: ISAKMP: attributes in transform: *Mar 1
00:28:13.963: ISAKMP: encaps is 1 *Mar 1 00:28:13.963: ISAKMP: SA life type in seconds *Mar 1
00:28:13.963: ISAKMP: SA life duration (basic) of 3600 *Mar 1 00:28:13.967: ISAKMP: SA life type
in kilobytes *Mar 1 00:28:13.967: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 *Mar 1
00:28:13.971: ISAKMP: HMAC algorithm is SHA *Mar 1 00:28:13.971: ISAKMP (6): atts are
acceptable. *Mar 1 00:28:13.975: ISAKMP (6): processing NONCE payload. message ID = -161552401
*Mar 1 00:28:13.979: ISAKMP (6): processing ID payload. message ID = -161552401 *Mar 1
00:28:13.979: ISAKMP (6): processing ID payload. message ID = -161552401 *Mar 1 00:28:14.391:
ISAKMP (6): Creating IPsec SAs *Mar 1 00:28:14.391: inbound SA from 20.20.20.20 to 20.20.20.21
(proxy 60.60.60.0 to 50.50.50.0) *Mar 1 00:28:14.395: has spi 437593758 and conn_id 7 and flags
4 *Mar 1 00:28:14.399: lifetime of 3600 seconds *Mar 1 00:28:14.399: lifetime of 4608000
kilobytes *Mar 1 00:28:14.403: outbound SA from 20.20.20.21 to 20.20.20.20 (proxy 50.50.50.0 to
60.60.60.0) *Mar 1 00:28:14.403: has spi 411835612 and conn_id 8 and flags 4 *Mar 1
00:28:14.407: lifetime of 3600 seconds *Mar 1 00:28:14.407: lifetime of 4608000 kilobytes *Mar 1
00:28:14.411: ISAKMP (6): Creating IPsec SAs *Mar 1 00:28:14.411: inbound SA from 20.20.20.20 to
20.20.20.21 (proxy 60.60.60.0 to 50.50.50.0) *Mar 1 00:28:14.415: has spi 216990519 and conn_id
9 and flags 4 *Mar 1 00:28:14.415: lifetime of 3600 seconds *Mar 1 00:28:14.419: lifetime of
4608000 kilobytes *Mar 1 00:28:14.419: outbound SA from 20.20.20.21 to 20.20.20.20 (proxy
50.50.50.0 to 60.60.60.0) *Mar 1 00:28:14.423: has spi 108733569 and conn_id 10 and flags 4
*Mar 1 00:28:14.423: lifetime of 3600 seconds *Mar 1 00:28:14.427: lifetime of 4608000 kilobytes
wan2511# ----- RSA-enc IPSEC debug ----- wan2511# *Mar 1 00:30:32.155:
ISAKMP (11): Unable to get router cert to find DN! wan2511#**show debug** Cryptographic Subsystem:
Crypto IPSEC debugging is on wan2511# wan2511# wan2511# wan2511# %CRYPTO-6-IKMP_AUTH_FAIL:
Authentication method 4 failed with host 20.20.20.20 %CRYPTO-6-IKMP_MODE_FAILURE: Processing of
Main mode failed with peer at 20.20.20.20 *Mar 1 00:31:13.931: IPSEC(validate_proposal_request):
proposal part #1, (key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20, dest_proxy=
50.50.50.0/0.0.0.0/0/0, src_proxy= 60.60.60.0/0.0.0.16/0/0, protocol= AH, transform= ah-sha-hmac
, lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4 *Mar 1 00:31:13.935:
IPSEC(validate_proposal_request): proposal part #2, (key eng. msg.) dest= 20.20.20.21, SRC=
20.20.20.20, dest_proxy= 50.50.50.0/0.0.0.0/0/0, src_proxy= 60.60.60.0/0.0.0.16/0/0, protocol=
ESP, transform= esp-des esp-sha-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0,
flags= 0x4 *Mar 1 00:31:13.947: IPSEC(key_engine): got a queue event... *Mar 1 00:31:13.951:
IPSEC(spi_response): getting spi 436869446 for SA from 20.20.20.20 to 20.20.20.21 for prot 2
*Mar 1 00:31:13.955: IPSEC(spi_response): getting spi 285609740 for SA from 20.20.20.20 to
20.20.20.21 for prot 3 *Mar 1 00:31:14.367: IPSEC(key_engine): got a queue event... *Mar 1

```

00:31:14.367: IPSEC(initialize_sas): , (key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20,
dest_proxy= 50.50.50.0/255.255.255.0/0/0, src_proxy= 60.60.60.0/255.255.255.0/0/0, protocol= AH,
transform= ah-sha-hmac , lifedur= 3600s and 4608000kb, spi= 0x1A0A1946(436869446), conn_id= 12,
keysize= 0, flags= 0x4 *Mar 1 00:31:14.375: IPSEC(initialize_sas): , (key eng. msg.) SRC=
20.20.20.21, dest= 20.20.20.20, src_proxy= 50.50.50.0/255.255.255.0/0/0, dest_proxy=
60.60.60.0/255.255.255.0/0/0, protocol= AH, transform= ah-sha-hmac , lifedur= 3600s and
4608000kb, spi= 0x2C40706(46401286), conn_id= 13, keysizes= 0, flags= 0x4 *Mar 1 00:31:14.383:
IPSEC(initialize_sas): , (key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20, dest_proxy=
50.50.50.0/255.255.255.0/0/0, src_proxy= 60.60.60.0/255.255.255.0/0/0, protocol= ESP, transform=
esp-des esp-sha-hmac , lifedur= 3600s and 4608000kb, spi= 0x11060F0C(285609740), conn_id= 14,
keysize= 0, flags= 0x4 *Mar 1 00:31:14.391: IPSEC(initialize_sas): , (key eng. msg.) SRC=
20.20.20.21, dest= 20.20.20.20, src_proxy= 50.50.50.0/255.255.255.0/0/0, dest_proxy=
60.60.60.0/255.255.255.0/0/0, protocol= ESP, transform= esp-des esp-sha-hmac , lifedur= 3600s
and 4608000kb, spi= 0x12881335(310907701), conn_id= 15, keysizes= 0, flags= 0x4 *Mar 1
00:31:14.399: IPSEC(create_sa): sa created, (sa) sa_dest= 20.20.20.21, sa_prot= 51, sa_spi=
0x1A0A1946(436869446), sa_trans= ah-sha-hmac , sa_conn_id= 12 *Mar 1 00:31:14.407:
IPSEC(create_sa): sa created, (sa) sa_dest= 20.20.20.20, sa_prot= 51, sa_spi=
0x2C40706(46401286), sa_trans= ah-sha-hmac , sa_conn_id= 13 *Mar 1 00:31:14.411:
IPSEC(create_sa): sa created, (sa) sa_dest= 20.20.20.21, sa_prot= 50, sa_spi=
0x11060F0C(285609740), sa_trans= esp-des esp-sha-hmac , sa_conn_id= 14 *Mar 1 00:31:14.415:
IPSEC(create_sa): sa created, (sa) sa_dest= 20.20.20.20, sa_prot= 50, sa_spi=
0x12881335(310907701), sa_trans= esp-des esp-sha-hmac , sa_conn_id= 15 wan2511#

```

例 3 : ISAKMP : RSA-SIG 認証/CA

この例では、CA サーバの使用を必要とする RSA 署名が使用されています。それぞれのピアでは、証明書が CA サーバ (通常これは証明書を発行するように設定されたワークステーションです) から取得されます。両方のピアで有効な CA 証明書が取得されたら、ISAKMP ネゴシエーションの一環で、自動的に RSA 公開鍵が相互に交換されます。このシナリオで唯一必要なことは、それぞれのピアが CA に登録済みであり、証明書を取得していることです。ピアでは、ネットワーク内のすべてのピアの公開 RSA 鍵を保持する必要はなくなります。

また、次に示すデフォルト ポリシーを使用しているため、ISAKMP ポリシーが指定されていないことにも注意してください。

```

lab-isdn1#show crypto isakmp policy Default protection suite encryption algorithm: DES - Data
Encryption Standard (56 bit keys). hash algorithm: Secure Hash Standard authentication method:
Rivest-Shamir-Adleman Signature Diffie-Hellman group: #1 (768 bit) lifetime: 86400 seconds, no
volume limit

```

まず、CA サーバのホスト名を定義し、RSA 鍵を生成します。

```

test1-isdn(config)#ip host cert-author 10.19.54.46 test1-isdn(config)#crypto key gen rsa usage
The name for the keys will be: test1-isdn.cisco.com Choose the size of the key modulus in the
range of 360 to 2048 for your Signature Keys. Choosing a key modulus greater than 512 may take a
few minutes. How many bits in the modulus [512]: Generating RSA keys ... [OK] Choose the size of
the key modulus in the range of 360 to 2048 for your Encryption Keys. Choosing a key modulus
greater than 512 may take a few minutes. How many bits in the modulus [512]: Generating RSA keys
... [OK]

```

次に、「test1-isdn-ultra」と呼ばれるタグを使用して CA 設定が定義され、CA 名 URL を定義します。CA サーバを使用して認証し、証明書を取得します。最後に、使用するのに「利用可能な」証明書を受け取ったことを確認するためにチェックを続けます。

```

test1-isdn(config)#crypto ca identity test1-isdn-ultra test1-isdn(ca-identity)#enrollment url
http://cert-author test1-isdn(ca-identity)#crl optional test1-isdn(ca-identity)#exit -----
----- test1-isdn(config)#crypto ca authenticate test1-isdn-ultra Certificate
has the following attributes: Fingerprint: 71CA5A98 78828EF8 4987BA95 57830E5F % Do you accept
this certificate? [yes/no]: yes Apr 3 14:08:56.329: CRYPTO_PKI: http connection opened Apr 3
14:08:56.595: CRYPTO__PKI: All enrollment requests completed. Apr 3 14:08:56.599: CRYPTO_PKI:
transaction GetCACert completed Apr 3 14:08:56.599: CRYPTO_PKI: CA certificate received test1-
isdn(config)# ----- test1-isdn(config)#crypto ca enroll test1-

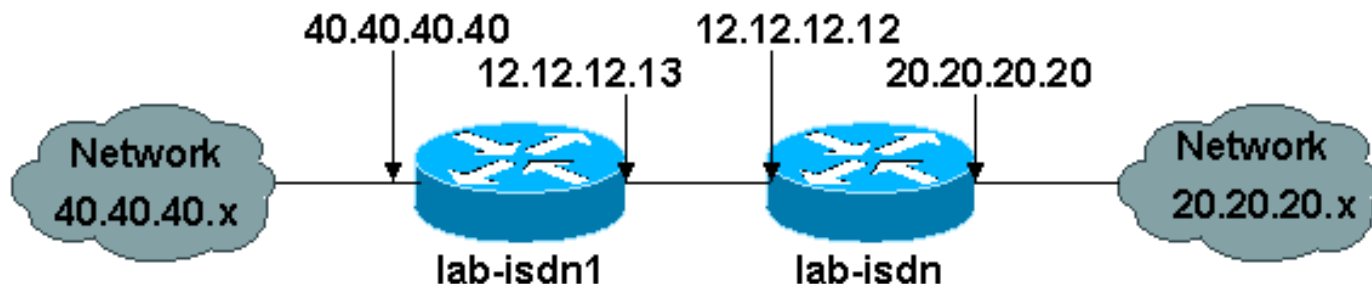
```

```

isdn-ultra % Start certificate enrollment .. % Create a challenge password. You will need to
verbally provide this password to the CA Administrator in order to revoke your certificate. For
security reasons your password will not be saved in the configuration. Please make a note of it.
Password: Re-enter password: % The subject name in the certificate will be: test1-isdn.cisco.com
% Include the router serial number in the subject name? [yes/no]: yes % The serial number in the
certificate will be: 04922418 % Include an IP address in the subject name? [yes/no]: yes
Interface: bri0 Request certificate from CA? [yes/no]: yes % Certificate request sent to
Certificate Authority % The certificate request fingerprint will be displayed. % The 'show
crypto ca certificate' command will also show the fingerprint. ----- status: pending
----- test1-isdn#show crypto ca certificate CA Certificate Status: Available
Certificate Serial Number: 3051DF7169BEE31B821DFE4B3A338E5F Key Usage: Not Set Certificate
Subject Name Name: test1-isdn.cisco.com IP Address: 10.18.117.189 Serial Number: 04922418
Status: Pending Key Usage: Signature Fingerprint: B1566229 472B1DDB 01A072C0 8202A985 00000000
Certificate Subject Name Name: test1-isdn.cisco.com IP Address: 10.18.117.189 Serial Number:
04922418 Status: Pending Key Usage: Encryption Fingerprint: 1EA39C07 D1B26FC7 7AD08BF4 ACA3AABD
00000000 ----- status: available ----- test1-isdn#show crypto ca
certificate Certificate Subject Name Name: test1-isdn.cisco.com Serial Number: 04922418 Status:
Available Certificate Serial Number: 1BAFCBCA71F0434B59D192FAFB37D376 Key Usage: Encryption CA
Certificate Status: Available Certificate Serial Number: 3051DF7169BEE31B821DFE4B3A338E5F Key
Usage: Not Set Certificate Subject Name Name: test1-isdn.cisco.com Serial Number: 04922418
Status: Available Certificate Serial Number: 4B39EE2866814279CBA7534496DE1D99 Key Usage:
Signature test1-isdn#

```

次の図は、この設定例のネットワークダイアグラムを表しています。



次の設定例は、(上に示すように) CA 証明書を取得済みで、認証ポリシーとして「rsa-sig」を使用して ISAKMP を実行しようとする 2 台の Cisco 1600 ルータからのものです。暗号化されるのは、2 つのリモートイーサネット LAN 間のトラフィックだけです。

```

lab-isdn1#write terminal Building configuration... Current configuration: ! version 11.3 service
timestamps debug datetime msec no service password-encryption service udp-small-servers service
tcp-small-servers ! hostname lab-isdn1 ! enable secret 5 $1$VdPY$uA/BIVeEm9UAFEm.PPJFc. !
username lab-isdn password 0 cisco ip host ciscoca-ultra 171.69.54.46 ip host lab-isdn
12.12.12.12 ip domain-name cisco.com ip name-server 171.68.10.70 ip name-server 171.68.122.99
isdn switch-type basic-nil ! crypto ipsec transform-set mypolicy ah-sha-hmac esp-des esp-sha-
hmac ! crypto map test 10 ipsec-isakmp set peer 12.12.12.12 set transform-set mypolicy match
address 144 ! crypto ca identity bubba enrollment url http://ciscoca-ultra.crl optional crypto
ca certificate chain bubba certificate 3E1ED472BDA2CE0163FB6B0B004E5EEE 308201BC 30820166
A0030201 0202103E 1ED472BD A2CE0163 FB6B0B00 4E5EEE30 0D06092A 864886F7 0D010104 05003042
31163014 06035504 0A130D43 6973636F 20537973 74656D73 3110300E 06035504 0B130744 65767465
73743116 30140603 55040313 0D434953 434F4341 2D554C54 5241301E 170D3938 30343038 30303030
30305A17 0D393930 34303832 33353935 395A303B 31273025 06092A86 4886F70D 01090216 18737461
6E6E6F75 732D6973 646E312E 63697363 6F2E636F 6D311030 0E060355 04051307 35363739 39383730
5C300D06 092A8648 86F70D01 01010500 034B0030 48024100 D2D125FF BBFC6E56 93CB4385 5473C165
BC7CCAF6 45C35BED 554BAA0B 119AFA6F 0853F574 5E0B8492 2E39B5FA 84C4DD05 C19AA625 8184395C
6CBC7FA4 614F6177 02030100 01A33F30 3D300B06 03551D0F 04040302 05203023 0603551D 11041C30
1A821873 74616E6E 6F75732D 6973646E 312E6369 73636F2E 636F6D30 09060355 1D130402 3000300D
06092A86 4886F70D 01010405 00034100 04AF83B8 FE95F5D9 9C07C105 F1E88F1A 9320CE7D 0FA540CF
44C77829 FC85C94B 8CB4CA32 85FF9655 8E47AC9A B9D6BF1A 0C4846DE 5CB07C8E A32038EC 8AFD161A quit
certificate ca 3051DF7169BEE31B821DFE4B3A338E5F 30820182 3082012C A0030201 02021030 51DF7169
BEE31B82 1DFE4B3A 338E5F30 0D06092A 864886F7 0D010104 05003042 31163014 06035504 0A130D43
6973636F 20537973 74656D73 3110300E 06035504 0B130744 65767465 73743116 30140603 55040313
0D434953 434F4341 2D554C54 5241301E 170D3937 31323032 30313036 32385A17 0D393831 32303230

```

```
31303632 385A3042 31163014 06035504 0A130D43 6973636F 20537973 74656D73 3110300E 06035504
0B130744 65767465 73743116 30140603 55040313 0D434953 434F4341 2D554C54 5241305C 300D0609
2A864886 F70D0101 01050003 4B003048 024100C1 B69D7BF6 34E4EE28 A84E0DC6 FCA4DEA8 04D89E50
C5EBE862 39D51890 D0D4B732 678BDBF2 80801430 E5E56E7C C126E2DD DBE9695A DF8E5BA7 E67BAE87
29375302 03010001 300D0609 2A864886 F70D0101 04050003 410035AA 82B5A406 32489413 A7FF9A9A
E349E5B4 74615E05 058BA3CE 7C5F00B4 019552A5 E892D2A3 86763A1F 2852297F C68EECE1 F41E9A7B
2F38D02A B1D2F817 3F7B quit certificate 503968D890F7D409475B7280162754D2 308201BC 30820166
A0030201 02021050 3968D890 F7D40947 5B728016 2754D230 0D06092A 864886F7 0D010104 05003042
31163014 06035504 0A130D43 6973636F 20537973 74656D73 3110300E 06035504 0B130744 65767465
73743116 30140603 55040313 0D434953 434F4341 2D554C54 5241301E 170D3938 30343038 30303030
30305A17 0D393930 34303832 33353935 395A303B 31273025 06092A86 4886F70D 01090216 18737461
6E6E6F75 732D6973 646E312E 63697363 6F2E636F 6D311030 0E060355 04051307 35363739 39383730
5C300D06 092A8648 86F70D01 01010500 034B0030 48024100 BECE2D8C B32E6B09 0ADE0D46 AF8D4A1F
37850034 35D0C729 3BF91518 0C9E4CF8 1A6A43AE E4F04687 B8E2859D 33D5CE04 2E5DDEA6 3DA54A31
2AD4255A 756014CB 02030100 01A33F30 3D300B06 03551D0F 04040302 07803023 0603551D 11041C30
1A821873 74616E6E 6F75732D 6973646E 312E6369 73636F2E 636F6D30 09060355 1D130402 3000300D
06092A86 4886F70D 01010405 00034100 B3AF6E71 CBD9AEDD A4711B71 6897F2CE D669A23A EE47B92B
B2BE942A 422DF4A5 7ACB9433 BD17EC7A BB3721EC E7D1175F 5C62BC58 C409F805 19691FBD FD925138 quit !
interface Ethernet0 ip address 40.40.40.40 255.255.255.0 no ip mroute-cache ! interface BRI0 ip
address 12.12.12.13 255.255.255.0 encapsulation ppp no ip mroute-cache dialer idle-timeout 99999
dialer map ip 12.12.12.12 name lab-isdn 4724171 dialer hold-queue 40 dialer-group 1 isdn spid1
919472411800 4724118 isdn spid2 919472411901 4724119 ppp authentication chap crypto map test !
ip classless ip route 0.0.0.0 0.0.0.0 12.12.12.12 access-list 144 permit ip 40.40.40.0 0.0.0.255
20.20.20.0 0.0.0.255 dialer-list 1 protocol ip permit ! line con 0 exec-timeout 0 0 line vty 0 4
password ww login ! end lab-isdn1# ----- lab-isdn#write terminal Building
configuration... Current configuration: ! version 11.3 service timestamps debug datetime msec no
service password-encryption service udp-small-servers service tcp-small-servers ! hostname lab-
isdn ! enable secret 5 $!$0Ne1$wDbhBdN6x9Y5gfuMjqh10 ! username lab-isdn1 password 0 cisco ip
host ciscoca-ultra 171.69.54.46 ip host lab-isdn1 12.12.12.13 ip domain-name cisco.com ip name-
server 171.68.10.70 ip name-server 171.68.122.99 isdn switch-type basic-nil ! crypto ipsec
transform-set mypolicy ah-sha-hmac esp-des esp-sha-hmac ! crypto map test 10 ipsec-isakmp set
peer 12.12.12.13 set transform-set mypolicy match address 133 ! crypto ca identity lab
enrollment url http://ciscoca-ultra crl optional crypto ca certificate chain lab certificate
44FC6C531FC3446927E4EE307A806B20 308201E0 3082018A A0030201 02021044 FC6C531F C3446927 E4EE307A
806B2030 0D06092A 864886F7 0D010104 05003042 31163014 06035504 0A130D43 6973636F 20537973
74656D73 3110300E 06035504 0B130744 65767465 73743116 30140603 55040313 0D434953 434F4341
2D554C54 5241301E 170D3938 30343038 30303030 30305A17 0D393930 34303832 33353935 395A305A
31263024 06092A86 4886F70D 01090216 17737461 6E6E6F75 732D6973 646E2E63 6973636F 2E636F6D
311E301C 060A2B06 0104012A 020B0201 130E3137 312E3638 2E313137 2E313839 3110300E 06035504
05130735 36373939 3139305C 300D0609 2A864886 F70D0101 01050003 4B003048 024100B8 F4A17A70
FAB5C2E3 39186513 486779C7 61EF0AC1 3B6CFF83 810E6D28 B3E4C034 CD803CFF 5158C270 28FEBEDE
CB6EF2D4 83BDD9B3 EAF915DB 78266E96 500CD702 03010001 A3443042 300B0603 551D0F04 04030205
20302806 03551D11 0421301F 82177374 616E6E6F 75732D69 73646E2E 63697363 6F2E636F 6D8704AB
4475BD30 09060355 1D130402 3000300D 06092A86 4886F70D 01010405 00034100 BF65B931 0F960195
ABDD41D5 622743D9 C12B5499 B3A8EB30 5005E6CC 7FDF7C5B 51D13EB8 D46187E5 A1E7F711 AEB7B33B
AA4C6728 7A4BA692 00A44A05 C5CF973F quit certificate ca 3051DF7169BEE31B821DFE4B3A338E5F
30820182 3082012C A0030201 02021030 51DF7169 BEE31B82 1DFE4B3A 338E5F30 0D06092A 864886F7
0D010104 05003042 31163014 06035504 0A130D43 6973636F 20537973 74656D73 3110300E 06035504
0B130744 65767465 73743116 30140603 55040313 0D434953 434F4341 2D554C54 5241301E 170D3937
31323032 30313036 32385A17 0D393831 32303230 31303632 385A3042 31163014 06035504 0A130D43
6973636F 20537973 74656D73 3110300E 06035504 0B130744 65767465 73743116 30140603 55040313
0D434953 434F4341 2D554C54 5241305C 300D0609 2A864886 F70D0101 01050003 4B003048 024100C1
B69D7BF6 34E4EE28 A84E0DC6 FCA4DEA8 04D89E50 C5EBE862 39D51890 D0D4B732 678BDBF2 80801430
E5E56E7C C126E2DD DBE9695A DF8E5BA7 E67BAE87 29375302 03010001 300D0609 2A864886 F70D0101
04050003 410035AA 82B5A406 32489413 A7FF9A9A E349E5B4 74615E05 058BA3CE 7C5F00B4 019552A5
E892D2A3 86763A1F 2852297F C68EECE1 F41E9A7B 2F38D02A B1D2F817 3F7B quit certificate
52A46D5D10B18A6F51E6BC735A36508C 308201E0 3082018A A0030201 02021052 A46D5D10 B18A6F51 E6BC735A
36508C30 0D06092A 864886F7 0D010104 05003042 31163014 06035504 0A130D43 6973636F 20537973
74656D73 3110300E 06035504 0B130744 65767465 73743116 30140603 55040313 0D434953 434F4341
2D554C54 5241301E 170D3938 30343038 30303030 30305A17 0D393930 34303832 33353935 395A305A
31263024 06092A86 4886F70D 01090216 17737461 6E6E6F75 732D6973 646E2E63 6973636F 2E636F6D
311E301C 060A2B06 0104012A 020B0201 130E3137 312E3638 2E313137 2E313839 3110300E 06035504
05130735 36373939 3139305C 300D0609 2A864886 F70D0101 01050003 4B003048 024100D7 71AD5672
B487A019 5ECD1954 6F919A3A 6270102E 5A9FF4DC 7A608480 FB27A181 715335F4 399D3E57 7F72B323
```

```
BF0620AB 60C371CF 4389BA4F C60EE6EA 21E06302 03010001 A3443042 300B0603 551D0F04 04030207
80302806 03551D11 0421301F 82177374 616E6E6F 75732D69 73646E2E 63697363 6F2E636F 6D8704AB
4475BD30 09060355 1D130402 3000300D 06092A86 4886F70D 01010405 00034100 8AD45375 54803CF3
013829A8 8DB225A8 25342160 94546F3C 4094BBA3 F2F5A378 97E2F06F DCFFC509 A07B930A FBE6C3CA
E1FC7FD9 1E69B872 C402E62A A8814C09 quit ! interface Ethernet0 ip address 20.20.20.20
255.255.255.0 ! interface BRI0 description bri to rtp ip address 12.12.12.12 255.255.255.0 no ip
proxy-arp encapsulation ppp no ip mroute-cache bandwidth 128 load-interval 30 dialer idle-
timeout 99999 dialer hold-queue 40 dialer-group 1 isdn spid1 919472417100 4724171 isdn spid2
919472417201 4724172 ppp authentication chap crypto map test ! ip classless ip route 0.0.0.0
0.0.0.0 12.12.12.13 access-list 133 permit ip 20.20.20.0 0.0.0.255 40.40.40.0 0.0.0.255 dialer-
list 1 protocol ip permit ! line con 0 exec-timeout 0 0 line vty 0 4 password ww login ! end
lab-isdn# ----- RSA-sig ----- lab-isdn#show debug
Cryptographic Subsystem: Crypto ISAKMP debugging is on Crypto Engine debugging is on Crypto
IPSEC debugging is on lab-isdn# lab-isdn# *Mar 21 20:16:50.871: ISAKMP (4): processing SA
payload. message ID = 0 *Mar 21 20:16:50.871: ISAKMP (4): Checking ISAKMP transform 1 against
priority 65535 policy *Mar 21 20:16:50.875: ISAKMP: encryption DES-CBC *Mar 21 20:16:50.875:
ISAKMP: hash SHA *Mar 21 20:16:50.875: ISAKMP: default group 1 *Mar 21 20:16:50.875: ISAKMP:
auth RSA sig *Mar 21 20:16:50.879: ISAKMP (4): atts are acceptable. Next payload is 0 *Mar 21
20:16:50.879: Crypto engine 0: generate alg param *Mar 21 20:16:54.070: CRYPTO_ENGINE: Dh phase
1 status: 0 *Mar 21 20:16:54.090: ISAKMP (4): SA is doing RSA signature authentication *Mar 21
20:16:57.343: ISAKMP (4): processing KE payload. message ID = 0 *Mar 21 20:16:57.347: Crypto
engine 0: generate alg param *Mar 21 20:17:01.168: ISAKMP (4): processing NONCE payload. message
ID = 0 *Mar 21 20:17:01.176: Crypto engine 0: create ISAKMP SKEYID for conn id 4 *Mar 21
20:17:01.188: ISAKMP (4): SKEYID state generated *Mar 21 20:17:07.331: ISAKMP (4): processing ID
payload. message ID = 0 *Mar 21 20:17:07.331: ISAKMP (4): processing CERT payload. message ID =
0 *Mar 21 20:17:07.497: ISAKMP (4): cert approved with warning *Mar 21 20:17:07.600: ISAKMP (4):
processing SIG payload. message ID = 0 *Mar 21 20:17:07.608: Crypto engine 0: RSA decrypt with
public key *Mar 21 20:17:07.759: generate hmac context for conn id 4 *Mar 21 20:17:07.767:
ISAKMP (4): SA has been authenticated *Mar 21 20:17:07.775: generate hmac context for conn id 4
*Mar 21 20:17:07.783: Crypto engine 0: RSA encrypt with private key *Mar 21 20:17:08.672:
CRYPTO_ENGINE: key process suspended and continued *Mar 21 20:17:08.878: CRYPTO_ENGINE: key
process suspended and continued *Mar 21 20:17:09.088: CRYPTO_ENGINE: key process suspended and
continued *Mar 21 20:17:09.291: CRYPTO_ENGINE: key process suspended and continued *Mar 21
20:17:09.493: CRYPTO_ENGINE: key process suspended and continued *Mar 21 20:17:09.795:
CRYPTO_ENGINE: key process suspended and continued *Mar 21 20:17:10.973: generate hmac context
for conn id 4 *Mar 21 20:17:10.981: ISAKMP (4): processing SA payload. message ID = -538880964
*Mar 21 20:17:10.981: ISAKMP (4): Checking IPsec proposal 1 *Mar 21 20:17:10.981: ISAKMP:
transform 1, AH_SHA_HMAC *Mar 21 20:17:10.985: ISAKMP: attributes in transform: *Mar 21
20:17:10.985: ISAKMP: encaps is 1 *Mar 21 20:17:10.985: ISAKMP: SA life type in seconds *Mar 21
20:17:10.985: ISAKMP: SA life duration (basic) of 3600 *Mar 21 20:17:10.989: ISAKMP: SA life
type in kilobytes *Mar 21 20:17:10.989: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 *Mar
21 20:17:10.993: ISAKMP (4): atts are acceptable. *Mar 21 20:17:10.993: ISAKMP (4): Checking
IPsec proposal 1 *Mar 21 20:17:10.993: ISAKMP: transform 1, ESP_DES *Mar 21 20:17:10.997:
ISAKMP: attributes in transform: *Mar 21 20:17:10.997: ISAKMP: encaps is 1 *Mar 21 20:17:10.997:
ISAKMP: SA life type in seconds *Mar 21 20:17:10.997: ISAKMP: SA life duration (basic) of 3600
*Mar 21 20:17:11.001: ISAKMP: SA life type in kilobytes *Mar 21 20:17:11.001: ISAKMP: SA life
duration (VPI) of 0x0 0x46 0x50 0x0 *Mar 21 20:17:11.001: ISAKMP: HMAC algorithm is SHA *Mar 21
20:17:11.005: ISAKMP (4): atts are acceptable. *Mar 21 20:17:11.005:
IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) dest= 12.12.12.12, SRC=
12.12.12.13, dest_proxy= 20.20.20.0/0.0.0.0/0/0, src_proxy= 40.40.40.0/0.0.0.16/0/0, protocol=
AH, transform= ah-sha-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags=
0x4 *Mar 21 20:17:11.013: IPSEC(validate_proposal_request): proposal part #2, (key eng. msg.)
dest= 12.12.12.12, SRC= 12.12.12.13, dest_proxy= 20.20.20.0/0.0.0.0/0/0, src_proxy=
40.40.40.0/0.0.0.16/0/0, protocol= ESP, transform= esp-des esp-sha-hmac , lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4 *Mar 21 20:17:11.021: ISAKMP (4): processing
NONCE payload. message ID = -538880964 *Mar 21 20:17:11.021: ISAKMP (4): processing ID payload.
message ID = -538880964 *Mar 21 20:17:11.021: ISAKMP (4): processing ID payload. message ID = -
538880964 *Mar 21 20:17:11.025: IPSEC(key_engine): got a queue event... *Mar 21 20:17:11.029:
IPSEC(spi_response): getting spi 112207019 for SA from 12.12.12.13 to 12.12.12.12 for prot 2
*Mar 21 20:17:11.033: IPSEC(spi_response): getting spi 425268832 for SA from 12.12.12.13 to
12.12.12.12 for prot 3 *Mar 21 20:17:11.279: generate hmac context for conn id 4 *Mar 21
20:17:11.612: generate hmac context for conn id 4 *Mar 21 20:17:11.644: ISAKMP (4): Creating
IPsec SAs *Mar 21 20:17:11.644: inbound SA from 12.12.12.13 to 12.12.12.12 (proxy 40.40.40.0 to
20.20.20.0 ) *Mar 21 20:17:11.648: has spi 112207019 and conn_id 5 and flags 4 *Mar 21
```

```

20:17:11.648: lifetime of 3600 seconds *Mar 21 20:17:11.648: lifetime of 4608000 kilobytes *Mar
21 20:17:11.652: outbound SA from 12.12.12.12 to 12.12.12.13 (proxy 20.20.20.0 to 40.40.40.0 )
*Mar 21 20:17:11.652: has spi 83231845 and conn_id 6 and flags 4 *Mar 21 20:17:11.656: lifetime
of 3600 seconds *Mar 21 20:17:11.656: lifetime of 4608000 kilobytes *Mar 21 20:17:11.656: ISAKMP
(4): Creating IPsec SAs *Mar 21 20:17:11.656: inbound SA from 12.12.12.13 to 12.12.12.12 (proxy
40.40.40.0 to 20.20.20.0 ) *Mar 21 20:17:11.660: has spi 425268832 and conn_id 7 and flags 4
*Mar 21 20:17:11.660: lifetime of 3600 seconds *Mar 21 20:17:11.664: lifetime of 4608000
kilobytes *Mar 21 20:17:11.664: outbound SA from 12.12.12.12 to 12.12.12.13 (proxy 20.20.20.0 to
40.40.40.0 ) *Mar 21 20:17:11.668: has spi 556010247 and conn_id 8 and flags 4 *Mar 21
20:17:11.668: lifetime of 3600 seconds *Mar 21 20:17:11.668: lifetime of 4608000 kilobytes *Mar
21 20:17:11.676: IPSEC(key_engine): got a queue event... *Mar 21 20:17:11.676:
IPSEC(initialize_sas): , (key eng. msg.) dest= 12.12.12.12, SRC= 12.12.12.13, dest_proxy=
20.20.20.0/255.255.255.0/0/0, src_proxy= 40.40.40.0/255.255.255.0/0/0, protocol= AH, transform=
ah-sha-hmac , lifedur= 3600s and 4608000kb, spi= 0x6B024AB(112207019), conn_id= 5, keysize= 0,
flags= 0x4 *Mar 21 20:17:11.680: IPSEC(initialize_sas): , (key eng. msg.) SRC= 12.12.12.12,
dest= 12.12.12.13, src_proxy= 20.20.20.0/255.255.255.0/0/0, dest_proxy=
40.40.40.0/255.255.255.0/0/0, protocol= AH, transform= ah-sha-hmac , lifedur= 3600s and
4608000kb, spi= 0x4F60465(83231845), conn_id= 6, keysize= 0, flags= 0x4 *Mar 21 20:17:11.687:
IPSEC(initialize_sas): , (key eng. msg.) dest= 12.12.12.12, SRC= 12.12.12.13, dest_proxy=
20.20.20.0/255.255.255.0/0/0, src_proxy= 40.40.40.0/255.255.255.0/0/0, protocol= ESP, transform=
esp-des esp-sha-hmac , lifedur= 3600s and 4608000kb, spi= 0x19591660(425268832), conn_id= 7,
keysize= 0, flags= 0x4 *Mar 21 20:17:11.691: IPSEC(initialize_sas): , (key eng. msg.) SRC=
12.12.12.12, dest= 12.12.12.13, src_proxy= 20.20.20.0/255.255.255.0/0/0, dest_proxy=
40.40.40.0/255.255.255.0/0/0, protocol= ESP, transform= esp-des esp-sha-hmac , lifedur= 3600s
and 4608000kb, spi= 0x21240B07(556010247), conn_id= 8, keysize= 0, flags= 0x4 *Mar 21
20:17:11.699: IPSEC(create_sa): sa created, (sa) sa_dest= 12.12.12.12, sa_prot= 51, sa_spi=
0x6B024AB(112207019), sa_trans= ah-sha-hmac , sa_conn_id= 5 *Mar 21 20:17:11.703:
IPSEC(create_sa): sa created, (sa) sa_dest= 12.12.12.13, sa_prot= 51, sa_spi=
0x4F60465(83231845), sa_trans= ah-sha-hmac , sa_conn_id= 6 *Mar 21 20:17:11.707:
IPSEC(create_sa): sa created, (sa) sa_dest= 12.12.12.12, sa_prot= 50, sa_spi=
0x19591660(425268832), sa_trans= esp-des esp-sha-hmac , sa_conn_id= 7 *Mar 21 20:17:11.707:
IPSEC(create_sa): sa created, (sa) sa_dest= 12.12.12.13, sa_prot= 50, sa_spi=
0x21240B07(556010247), sa_trans= esp-des esp-sha-hmac , sa_conn_id= 8 *Mar 21 20:18:06.767:
ISADB: reaper checking SA, conn_id = 4 lab-isdn#

```

IPSec と ISAKMP のトラブルシューティング

一般に、次のコマンドを使用して情報を収集することが、個々のトラブルシューティング セッションを開始する最善の方法です。アスタリスク (*) は特に役に立つコマンドを示しています。詳細情報については、「[IP Security のトラブルシューティング - debug コマンドの理解と使用](#)」を参照してください。

特定の show コマンドは、[Output Interpreter Tool](#) ([登録ユーザ専用](#)) によってサポートされています。このツールを使用すると、show コマンド出力の分析を表示できます。

注: debug コマンドを使用する前に、「[debug コマンドに関する重要な情報](#)」を参照してください。

コマンド	
debug crypto pki trans	* debug crypto ipsec
* debug crypto isakmp	debug crypto key
debug crypto sess	debug crypto engine
show crypto engine connections active	show crypto engine connections dropped-packet
show crypto engine configuration	* show crypto ca certificates
* show crypto key	* show crypto key pubkey-

mypubkey rsa	chain rsa
show crypto isakmp policy	show crypto isakmp sa
show crypto ipsec sa	show crypto ipsec session-key
show crypto ipsec transform-proposal	show crypto map interface bri 0
show crypto map tag test	clear crypto connection <connection id of SA>
* clear crypto isakmp	* clear crypto sa
clear crypto sa counters	clear crypto sa map
clear crypto sa peer	clear crypto sa spi
clear crypto sa counters	

次に、これらのコマンドの一部の出力例を示します。

```
wan2511#show crypto engine connections active ID Interface IP-Address State Algorithm Encrypt
Decrypt 9 Serial0 20.20.20.21 set HMAC_SHA 0 240 10 Serial0 20.20.20.21 set HMAC_SHA 240 0
wan2511#show crypto engine connections dropped-packet Interface IP-Address Drop Count
wan2511#show crypto engine configuration slot: 0 engine name: unknown engine type: software
serial number: 01496536 platform: rp crypto engine crypto lib version: 10.0.0 Encryption Process
Info: input queue top: 140 input queue bot: 140 input queue count: 0 wan2511#show crypto key
mypubkey rsa % Key pair was generated at: 00:09:04 UTC Mar 1 1993 Key name: wan2511.cisco.com
Usage: General Purpose Key Key Data: 305C300D 06092A86 4886F70D 01010105 00034B00 30480241
00E9007B E5CD7DC8 6E1C0423 92044254 92C972AD 0CCE9796 86797EAA B6C4EFF0 0F0A5378 6AFAE43B
3A2BD92F 98039DAC 08741E82 5D9053C4 D9CFABC1 AB54E0E2 BB020301 0001 wan2511#show crypto key
pubkey-chain rsa wan2511# wan2511#show crypto isakmp policy Protection suite of priority 1
encryption algorithm: DES - Data Encryption Standard (56 bit keys). hash algorithm: Secure Hash
Standard authentication method: Pre-Shared Key Diffie-Hellman group: #2 (1024 bit) lifetime: 240
seconds, no volume limit Default protection suite encryption algorithm: DES - Data Encryption
Standard (56 bit keys). hash algorithm: Secure Hash Standard authentication method: Rivest-
Shamir-Adleman Signature Diffie-Hellman group: #1 (768 bit) lifetime: 86400 seconds, no volume
limit wan2511#show crypto isakmp sa dst src state conn-id slot 20.20.20.21 20.20.20.20 QM_IDLE 7
0 wan2511# wan2511#show crypto ipsec sa interface: Serial0 Crypto map tag: test, local addr.
20.20.20.21 local ident (addr/mask/prot/port): (50.50.50.0/255.255.255.0/0/0) remote ident
(addr/mask/prot/port): (60.60.60.0/255.255.255.0/0/0) current_peer: 20.20.20.20 PERMIT,
flags={origin_is_acl,ident_is_ipsec,} #pkts encaps: 320, #pkts encrypt: 320, #pkts digest 320
#pkts decaps: 320, #pkts decrypt: 320, #pkts verify 320 #send errors 0, #recv errors 0 local
crypto endpt.: 20.20.20.21, remote crypto endpt.: 20.20.20.20 path mtu 1500, media mtu 1500
current outbound spi: 6625CD inbound esp sas: spi: 0x1925112F(421859631) transform: esp-des esp-
sha-hmac , in use settings = {Tunnel, } slot: 0, conn id: 11, crypto map: test sa timing:
remaining key lifetime (k/sec): (4607971/3354) IV size: 8 bytes replay detection support: Y
inbound ah sas: spi: 0x12050DD2(302321106) transform: ah-sha-hmac , in use settings = {Tunnel, }
slot: 0, conn id: 9, crypto map: test sa timing: remaining key lifetime (k/sec): (4607958/3354)
replay detection support: Y outbound esp sas: spi: 0x3262313(52830995) transform: esp-des esp-
sha-hmac , in use settings = {Tunnel, } slot: 0, conn id: 12, crypto map: test sa timing:
remaining key lifetime (k/sec): (4607971/3354) IV size: 8 bytes replay detection support: Y
outbound ah sas: spi: 0x6625CD(6694349) transform: ah-sha-hmac , in use settings = {Tunnel, }
slot: 0, conn id: 10, crypto map: test sa timing: remaining key lifetime (k/sec): (4607958/3354)
replay detection support: Y wan2511#show crypto ipsec session-key Session key lifetime: 4608000
kilobytes/3600 seconds wan2511#show crypto ipsec transform-proposal Transform proposal auth2: {
ah-sha-hmac } supported settings = { Tunnel, }, default settings = { Tunnel, }, will negotiate =
{ Tunnel, }, { esp-des esp-sha-hmac } supported settings = { Tunnel, }, default settings = {
Tunnel, }, will negotiate = { Tunnel, }, wan2511#show crypto map interface serial 0 Crypto Map
"test" 10 ipsec-isakmp Peer = 20.20.20.20 Extended IP access list 133 access-list 133 permit ip
source: addr = 50.50.50.0/0.0.0.255 dest: addr = 60.60.60.0/0.0.0.255 Current peer: 20.20.20.20
Session key lifetime: 4608000 kilobytes/3600 seconds PFS (Y/N): N Transform proposals={ auth2, }
wan2511#show crypto map tag test Crypto Map "test" 10 ipsec-isakmp Peer = 20.20.20.20 Extended
IP access list 133 access-list 133 permit ip source: addr = 50.50.50.0/0.0.0.255 dest: addr =
```


60.60.60.0/0.0.0.255 Current peer: 20.20.20.20 Session key lifetime: 4608000 kilobytes/3600 seconds PFS (Y/N): N Transform proposals={ auth2, } wan2511# ----- lab-isdnl#show crypto engine connections active ID Interface IP-Address State Algorithm Encrypt Decrypt 5 BRI0 12.12.12.13 set HMAC_SHA 0 89 6 BRI0 12.12.12.13 set HMAC_SHA 89 0 lab-isdnl#show crypto engine connections dropped-packet Interface IP-Address Drop Count BRI0 12.12.12.13 4 lab-isdnl#show crypto engine configuration slot: 0 engine name: unknown engine type: software serial number: 05679987 platform: rp crypto engine crypto lib version: 10.0.0 Encryption Process Info: input queue top: 243 input queue bot: 243 input queue count: 0 lab-isdnl#show crypto ca cert Certificate Subject Name Name: lab-isdnl.cisco.com Serial Number: 05679987 Status: Available Certificate Serial Number: 3E1ED472BDA2CE0163FB6B0B004E5EEE Key Usage: Encryption CA Certificate Status: Available Certificate Serial Number: 3051DF7169BEE31B821DFE4B3A338E5F Key Usage: Not Set Certificate Subject Name Name: lab-isdnl.cisco.com Serial Number: 05679987 Status: Available Certificate Serial Number: 503968D890F7D409475B7280162754D2 Key Usage: Signature lab-isdnl#show crypto key mypubkey rsa % Key pair was generated at: 03:10:23 UTC Mar 21 1993 Key name: lab-isdnl.cisco.com Usage: Signature Key Key Data: 305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00BECE2D 8CB32E6B 090ADE0D 46AF8D4A 1F378500 3435D0C7 293BF915 180C9E4C F81A6A43 AEE4F046 87B8E285 9D33D5CE 042E5DDE A63DA54A 312AD425 5A756014 CB020301 0001 % Key pair was generated at: 03:11:17 UTC Mar 21 1993 Key name: lab-isdnl.cisco.com Usage: Encryption Key Key Data: 305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00D2D125 FFBBFC6E 5693CB43 855473C1 65BC7CCA F645C35B ED554BAA 0B119AFA 6F0853F5 745E0B84 922E39B5 FA84C4DD 05C19AA6 25818439 5C6CBC7F A4614F61 77020301 0001 lab-isdnl#show crypto key pubkey-chain rsa Key name: Cisco SystemsDevtestCISCOCA-ULTRA Key serial number: C7040262 Key usage: signatures only Key source: certificate Key data: 305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00C1B69D 7BF634E4 EE28A84E 0DC6FCA4 DEA804D8 9E50C5EB E86239D5 1890D0D4 B732678B DBF28080 1430E5E5 6E7CC126 E2DDDBE9 695ADF8E 5BA7E67B AE872937 53020301 0001 Key name: lab-isdnl.cisco.com Key address: 171.68.117.189 Key serial number: 05679919 Key usage: general purpose Key source: certificate Key data: 305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00D771AD 5672B487 A0195ECD 19546F91 9A3A6270 102E5A9F F4DC7A60 8480FB27 A1817153 35F4399D 3E577F72 B323BF06 20AB60C3 71CF4389 BA4FC60E E6EA21E0 63020301 0001 lab-isdnl#show crypto isakmp policy Default protection suite encryption algorithm: DES - Data Encryption Standard (56 bit keys). hash algorithm: Secure Hash Standard authentication method: Rivest-Shamir-Adleman Signature Diffie-Hellman group: #1 (768 bit) lifetime: 86400 seconds, no volume limit lab-isdnl#show crypto isakmp sa dst src state conn-id slot 12.12.12.12 12.12.12.13 QM_IDLE 4 0 lab-isdnl#show crypto ipsec sa interface: BRI0 Crypto map tag: test, local addr. 12.12.12.13 local ident (addr/mask/prot/port): (40.40.40.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port): (20.20.20.0/255.255.255.0/0/0) current_peer: 12.12.12.12 PERMIT, flags={origin_is_acl,ident_is_ipsec,} #pkts encaps: 89, #pkts encrypt: 89, #pkts digest 89 #pkts decaps: 89, #pkts decrypt: 89, #pkts verify 89 #send errors 11, #recv errors 0 local crypto endpt.: 12.12.12.13, remote crypto endpt.: 12.12.12.12 path mtu 1500, media mtu 1500 current outbound spi: 6B024AB inbound esp sas: spi: 0x21240B07(556010247) transform: esp-des esp-sha-hmac , in use settings = {Tunnel, } slot: 0, conn id: 7, crypto map: test sa timing: remaining key lifetime (k/sec): (4607989/3062) IV size: 8 bytes replay detection support: Y inbound ah sas: spi: 0x4F60465(83231845) transform: ah-sha-hmac , in use settings = {Tunnel, } slot: 0, conn id: 5, crypto map: test sa timing: remaining key lifetime (k/sec): (4607984/3062) replay detection support: Y outbound esp sas: spi: 0x19591660(425268832) transform: esp-des esp-sha-hmac , in use settings = {Tunnel, } slot: 0, conn id: 8, crypto map: test sa timing: remaining key lifetime (k/sec): (4607989/3062) IV size: 8 bytes replay detection support: Y outbound ah sas: spi: 0x6B024AB(112207019) transform: ah-sha-hmac , in use settings = {Tunnel, } slot: 0, conn id: 6, crypto map: test sa timing: remaining key lifetime (k/sec): (4607984/3062) replay detection support: Y lab-isdnl#show crypto ipsec session-key Session key lifetime: 4608000 kilobytes/3600 seconds lab-isdnl#show crypto ipsec transform-proposal Transform proposal mypolicy: { ah-sha-hmac } supported settings = { Tunnel, }, default settings = { Tunnel, }, will negotiate = { Tunnel, }, { esp-des esp-sha-hmac } supported settings = { Tunnel, }, default settings = { Tunnel, }, will negotiate = { Tunnel, }, lab-isdnl#show crypto map interface bri 0 Crypto Map "test" 10 ipsec-isakmp Peer = 12.12.12.12 Extended IP access list 144 access-list 144 permit ip source: addr = 40.40.40.0/0.0.0.255 dest: addr = 20.20.20.0/0.0.0.255 Current peer: 12.12.12.12 Session key lifetime: 4608000 kilobytes/3600 seconds PFS (Y/N): N Transform proposals={ mypolicy, } lab-isdnl#show crypto map tag test Crypto Map "test" 10 ipsec-isakmp Peer = 12.12.12.12 Extended IP access list 144 access-list 144 permit ip source: addr = 40.40.40.0/0.0.0.255 dest: addr = 20.20.20.0/0.0.0.255 Current peer: 12.12.12.12 Session key lifetime: 4608000 kilobytes/3600 seconds PFS (Y/N): N Transform proposals={ mypolicy, } lab-isdnl# ----- lab-isdnl#clear crypto isakmp lab-isdnl# *Mar 21 20:58:34.503: ISADB: reaper checking SA, conn_id = 4 DELETE IT! *Mar 21 20:58:34.507: generate hmac context for conn id 4 *Mar 21 20:58:34.519: CRYPTO(epa_release_crypto_conn_entry): released

```
conn 4 lab-isdn1# lab-isdn1#clear crypto sa lab-isdn1# *Mar 21 20:58:42.495: IPSEC(delete_sa): deleting SA, (sa) sa_dest= 12.12.12.13, sa_prot= 51, sa_spi= 0x4F60465(83231845), sa_trans= ah-sha-hmac , sa_conn_id= 5 *Mar 21 20:58:42.499: CRYPTO(epa_release_crypto_conn_entry): released conn 5 *Mar 21 20:58:42.499: IPSEC(delete_sa): deleting SA, (sa) sa_dest= 12.12.12.12, sa_prot= 51, sa_spi= 0x6B024AB(112207019), sa_trans= ah-sha-hmac , sa_conn_id= 6 *Mar 21 20:58:42.503: CRYPTO(epa_release_crypto_conn_entry): released conn 6 *Mar 21 20:58:42.503: IPSEC(delete_sa): deleting SA, (sa) sa_dest= 12.12.12.13, sa_prot= 50, sa_spi= 0x21240B07(556010247), sa_trans= esp-des esp-sha-hmac , sa_conn_id= 7 *Mar 21 20:58:42.507: CRYPTO(epa_release_crypto_conn_entry): released conn 7 *Mar 21 20:58:42.507: IPSEC(delete_sa): deleting SA, (sa) sa_dest= 12.12.12.12, sa_prot= 50, sa_spi= 0x19591660(425268832), sa_trans= esp-des esp-sha-hmac , sa_conn_id= 8 *Mar 21 20:58:42.511: CRYPTO(epa_release_crypto_conn_entry): released conn 8 lab-isdn1#
```

関連情報

- [Cisco ネットワークレイヤの暗号化の設定とトラブルシューティング：背景説明 - 第 1 部](#)
- [DES FIPS 46-2 at National Institute of Standards and Technology \(NIST\)](#)
- [DSS FIPS 186 at National Institute of Standards and Technology \(NIST\)](#)
- [RSA Laboratories' Frequently Asked Questions About Today's Cryptography](#)
- [IETF Security Standards](#)
- [インターネット キー交換セキュリティ プロトコルの設定](#)
- [IPsec ネットワーク セキュリティの設定](#)
- [IPSec に関するサポート ページ](#)
- [テクニカルサポート - Cisco Systems](#)