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

目次

概要

このドキュメントでは、IPSec および Internet Security Association and Key Management Protocol (ISAKMP) によるシスコのネットワークレイヤ暗号化の設定とトラブルシューティングを解説し、ネットワークレイヤ暗号化の背景情報および IPSec と ISAKMP に関する基本的な設定について説明します。

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 11.2 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

ネットワークレイヤ暗号化 機能は Cisco IOS® ソフトウェア リリース 11.2 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、次の 2 つのコンポーネントで構成されています。

- **ルータ認証：** 暗号化されたトラフィックを渡す前に、2 つのルータが、Digital Signature Standard（DSS; デジタル シグニチャ規格）の公開キーを使用した 1 回限りの双方向認証を行い、ランダムなチャレンジにサインします。
- **ネットワークレイヤ暗号化：** IP ペイロード暗号化の場合、ルータは、Diffie-Hellman キー交換を使用して、DES（40 または 56 ビット セッション キー）、Triple DES - 3DES（168 ビット）、または 12.2(13)T で導入されたさらに新しい Advanced Encryption Standard - AES（128 ビット（デフォルト）、192 ビット、または 256 ビット キー）を安全に生成します。 新しいセッション キーは、設定可能な基盤上に生成されます。 暗号化ポリシーは crypto map によって設定され、crypto map は拡張 IP アクセスを使用して、ルータにおいて暗号化するネットワーク、サブネット、ホスト、またはプロトコルのペアを定義します。

暗号化の背景説明

暗号化の分野では、通信の秘守に観点が置かれています。 機密性の高い通信の保護は、暗号の歴史のほとんどで中心的なテーマでした。 暗号化とは、データを何らかの不可読な形式に変換することです。 暗号化の目的は、関係のない者が暗号化されたデータを見ることができたとしても内容がわからないように情報を隠して、プライバシを守ることです。 復号化は暗号化の反転です: それはわかりやすい形式に再び暗号化されたデータの変換です。

暗号化と復号化には何らかの秘密の情報を使用する必要があり、通常は「キー」と呼ばれます。 使用される暗号化メカニズムによっては同じキーは暗号化および復号化両方に使用するかもしれません; 他のメカニズムのために、暗号化に使用するキーおよび復号化は異なるかもしれません間。

デジタル署名は特定のキーの所有者にドキュメントを結び付け、デジタル タイムスタンプは特定の時刻の作成にドキュメントを結び付けます。 これらの暗号化メカニズムを使用して、共有ディスク ドライブ、高度なセキュリティのインストール、ペイパービュー（PPV; pay-per-view）のテレビ チャンネルなどに対するアクセスを制御できます。

最新の暗号化技術は多岐に渡り進歩を続けていますが、根本的に解決の困難な問題があります。問題が困難である理由は、暗号化されたメッセージの復号化や、デジタル文書への署名など、解決にはキーを知る必要があるためです。 また、特定のハッシュ値を生成するメッセージの検索など、達成するのが本質的に困難であることも理由です。

暗号化の分野が進歩するのに伴い、暗号化と呼べるものと呼べないものを区別する線はあいまいになっています。 今日の暗号技術には、解決困難な数学的問題の存在に依存する技法と応用の研究が統合されています。 暗号解読者は暗号メカニズムを破ろうとしており、暗号研究は暗号と暗号解読が組み合わさった分野です。

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ず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、力ず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ので、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。公開鍵暗号法の概念は、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（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。 明らかなことですが、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。

予備情報

このセクションでは、ネットワークレイヤ暗号化の基本的な概念について解説します。 ここでは、ユーザが注意する必要のある暗号化の側面が含まれています。 これらの問題は最初はあまり意味がないかもしれませんが、何か月か暗号化に関わる作業をしていれば重要なものになるので、今の時点で目を通して認識しておくことをお勧めします。

- 暗号化はインターフェイスの出力でだけ発生し、復号化はインターフェイスへの入力でだけ行われるということを覚えておくことが重要です。 これは、ポリシーを計画するときに重要になります。 暗号化と複合化に対するポリシーは対称的です。 つまり、一方を定義すると、もう一方も自動的に定義されます。 crypto map と関連する拡張アクセス リストを使用すると、暗号化ポリシーだけが明示的に定義されます。復号化ポリシーは同じ情報を使用します

が、パケットを照合するときには、送信元と宛先のアドレスとポートを逆にします。 このようにすることで、デュプレックス接続の両方向でデータが保護されます。 crypto map コマンドの match address x ステートメントは、インターフェイスから送信されるパケットを記述するために使用します。 つまり、パケットの暗号化を記述しています。 一方、パケットは、インターフェイスに入るときには、復号化に対して照合される必要もあります。 これは、送信元と宛先のアドレスとポートのアクセス リストを逆に経由することで、自動的に行われます。 これにより、接続は対称的になります。 crypto map が指し示すアクセス リストでは、1 方向（発信）だけのトラフィックを記述する必要があります。 定義されているアクセス リストと一致しない IP パケットは、送信はされますが暗号化されません。 アクセス リスト内の「deny」は、そのホストは一致しないことを示し、そのホストについては暗号化されません。 この場合の「deny」は、パケットを廃棄するという意味ではありません。

- 拡張アクセス リストで「any」という言葉を使用するときには十分注意する必要があります。 「any」を使用すると、一致する「非暗号化」インターフェイスに対するものでないトラフィックは廃棄されます。 さらに、Cisco IOS ソフトウェア リリース 11.3(3)T の IPSec では、「any」は認められていません。
- 送信元や宛先のアドレスを指定するために「any」キーワードを使用することは推奨されません。 「any」を指定すると、受信したルータではそのパケットが通知なしに廃棄されるので、ルーティング プロトコル、Network Time Protocol（NTP; ネットワーク タイム プロトコル）、エコー、エコー応答、およびマルチキャスト トラフィックで問題が発生する可能性があります。 「any」を使用する場合は、「ntp」のような暗号化しないトラフィックについては、前に「deny」文を付けておく必要があります。
- 時間を節約するために、暗号化アソシエーションを確立しようとするピア ルータに対して ping を実行できることを確認してください。 また、先に（トラフィックを暗号化することに依存する）エンド デバイス間で ping を実行しておくと、見当はずれの問題のトラブルシューティングで時間を無駄にしなくて済みます。 つまり、crypto を実行する前にルーティングが機能することを確認してください。 リモート ピアが出力インターフェイスに対するルートを持たないことがあり、その場合、そのピアとは暗号化セッションを持つことができません（そのようなシリアル インターフェイスでは、ip unnumbered を使用できる場合があります）。
- WAN の多くのポイントツーポイント リンクではルーティング不能な IP アドレスが使用されており、Cisco IOS ソフトウェア リリース 11.2 の暗号化は、Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）に依存しています（つまり、ICMP 用の出力シリアル インターフェイスの IP アドレスを使用します）。 このため、WAN インターフェイスでは ip unnumbered を使用することが必要になる場合があります。 常に ping と traceroute コマンドを実行して、ピアを形成する（暗号化/復号化を行う）2 つのルータでルーティングが行われていることを確認してください。
- Diffie-Hellman セッション キーを共有できるのは、2 つのルータだけです。 すなわち、1 つのルータは同じセッションキーを使用して 2 同位に暗号化されたパケットを交換できません; ルータの各ペアはその間の Diffie-Hellman交換の結果であるセッションキーがなければなりません。
- 暗号化エンジンは、Cisco IOS、VIP2 Cisco IOS、またはハードウェアでは VIP2 の Encryption services adapter（ESA; 暗号化サービス アダプタ）に存在します。 VIP2 がない場合、Cisco IOS 暗号化エンジンがすべてのポートの暗号化ポリシーを管理します。 VIP2 を使用してプラットフォームで、複数の暗号化エンジンがあります: Cisco IOS の 1 つ、および各 VIP2 の 1。 VIP2 の暗号化エンジンは、ボード上に存在するポートでの暗号化を管理します。
- 必ず、暗号化用に準備されているインターフェイスにトラフィックが到着するよう設定してください。 crypto map が適用されたもの以外のインターフェイスに到着したトラフィックは

、通知なしに廃棄されます。
- それは鍵交換をするとき両方のルータにコンソール（か交替）アクセスがあるのを助けます; キーを待っている間ハングするために受動側を得ることは可能性のあるです。
- CPU の負荷に関しては、cfb-8 より cfb-64 の方が処理効率が優っています。
- ルータは使用したいと思う cipher-feedback （CFB）モードでの使用したいと思うアルゴリズムを実行する必要があります; 各イメージのためのデフォルトは **cfb-64** のイメージ名（"56" のような）です。
- キータイムアウトの変更を検討します。 デフォルトの 30 分では短すぎます。 1 日（1,440 分）まで増やしてみてください。
- キーの有効期限が切れるたびに行われるキーの再ネゴシエーションの間、IP トラフィックは廃棄されます。
- ほんとうに暗号化する必要のあるトラフィックだけを選択します（CPU サイクルを節約できます）。
- Dial-on-Demand Routing（DDR; ダイヤルオンデマンド ルーティング）で、ICMP を対象にします。そうしないとダイヤル アウトされません。
- IP 以外のトラフィックを暗号化する場合は、トンネルを使用します。 トンネルを使用すると、物理インターフェイスとトンネル インターフェイスの両方に対して、crypto map が適用されます。 サンプル 5 を参照して下さい: 詳細については IPトンネルの IPXトラフィックの暗号化。
- 2 つの暗号化ピア ルータを直接接続する必要はありません。
- ローエンドのルータでは、「CPU hog」メッセージが発生する場合があります。 このメッセージは、暗号化処理が大量の CPU リソースを使用していることを伝えるものなので、無視してかまいません。
- 暗号化を行うルータを冗長に配置しないでください。トラフィックの復号化と再暗号化で CPU が浪費されます。 2 つのエンドポイントだけで暗号化を行います。 サンプル 3 を参照して下さい: 詳細についてはルータへのおよびを通した暗号化。
- 現時点では、ブロードキャストとマルチキャストのパケットの暗号化はサポートされていません。 「セキュアな」ルーティング アップデートがネットワークの設計にとって重要である場合は、Enhanced Interior Gateway Routing Protocol（EIGRP）、Open Shortest Path First（OSPF）、Routing Information Protocol バージョン 2（RIPv2）などの認証が組み込まれたプロトコルを使用して、アップデートの整合性を保証する必要があります。

警告

注: 次に示す注意はすべて解決済です。

- 暗号化に ESA を使用する Cisco 7200 ルータは、あるセッション キーでパケットを復号化した後、別のセッション キーで同じパケットを再暗号化することはできません。 Cisco Bug ID CSCdj82613（登録ユーザ専用）を参照してください。
- 2 つのルータが暗号化された専用回線と ISDN バックアップ回線で接続されている場合、専用回線が切断されると、ISDN リンクが有効になります。 ところが、専用回線が復旧すると、ISDN のコールを処理中のルータがクラッシュします。 Cisco Bug ID CSCdj00310（登録ユーザ専用）を参照してください。
- 複数の VIP を備える Cisco 7500 シリーズ ルータの場合、いずれかの VIP の 1 つのインターフェイスで crypto map が適用されると、1 つあるいは複数の VIP でクラッシュが発生します。 Cisco Bug ID CSCdi88459（登録ユーザ専用）を参照してください。
- VIP2 と ESA を備える Cisco 7500 シリーズ ルータの場合、ユーザがコンソール ポートを使用していないと、show crypto card コマンドの出力が表示されません。 Cisco Bug ID

CSCdj89070（登録ユーザ専用）を参照してください。

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。

このドキュメントのサンプル設定はすべて、Cisco IOS ソフトウェア リリース 11.3 のものです。次に示すキーワードが追加されたことなど、Cisco IOS ソフトウェア リリース 11.2 のコマンドからは若干の変更があります。

- 一部のキー設定コマンドでの dss。
- 一部の show コマンドと crypto map コマンドでの cisco。これは、シスコ固有の暗号化（Cisco IOS ソフトウェア リリース 11.2 以降に含まれるもの）と Cisco IOS ソフトウェア リリース 11.3(2)T の IPSec を区別するためのものです。

注: これらの設定例で使用されている IP アドレスは、シスコのラボでランダムに選択されたもので、完全な汎用性を目的としたものです。

ステップ 1： 手動で 生成する DSS キーペア

DSS キー ペア（公開キーと秘密キー）は、暗号化セッションに参加するルータごとに手動で生成する必要があります。 つまり、暗号化セッションに参加するすべてのルータに、独自の DSS キーが備わっている必要があります。 暗号化エンジンは、エンジンを一意に識別する DSS キーを 1 つだけ持つことができます。 DSS キーと RSA キーを区別するため、Cisco IOS ソフトウェア リリース 11.3 ではキーワード「dss」が追加されました。 ルータ独自の DSS キーには、任意の名前を指定できます（ただし、ルータのホスト名を使用することをお勧めします）。 処理能力の低い CPU（Cisco 2500 シリーズなど）では、キー ペアの生成に最大で 5 秒程度かかります。

ルータは、次に示すキーのペアを生成します。

- 公開キー（後で、暗号化セッションに参加するルータに送信されます）。
- （誰でもと参照されなかったり交換されないプライベートキー; 実際、それは表示することができない） NVRAM の別のセクションで保存されます。

生成されたルータの DSS キー ペアは、そのルータの暗号化エンジンと一意的に関連付けられます。 次のコマンド出力の例は、キー ペアの生成を示したものです。

```
dial-5(config)#crypto key generate dss dial5 Generating DSS keys .... [OK] dial-5#show crypto key mypubkey dss crypto public-key dial5 05679919 160AA490 5B9B1824 24769FCD EE5E0F46 1ABBD343 4C0C4A03 4B279D6B 0EE5F65F F64665D4 1036875A 8CF93691 BDF81722 064B51C9 58D72E12 3E1894B6 64B1D145 quit dial-5#show crypto engine configuration slot: 0 engine name: dial5 engine type: software serial number: 05679919 platform: rp crypto engine crypto lib version: 10.0.0 Encryption Process Info: input queue top: 43 input queue bot: 43 input queue count: 0 dial-5#
```

ルータを識別するキー ペアは 1 つしか生成できないので、元のキーを上書きしたら、暗号化アソシエーション内のすべてのルータに公開キーを送信し直す必要があります。 次のコマンド出力例は、これを示したものです。

```
StHelen(config)#crypto key generate dss barney % Generating new DSS keys will require re-exchanging public keys with peers who already have the public key named barney! Generate new DSS keys? [yes/no]: yes Generating DSS keys .... [OK] StHelen(config)# Mar 16 12:13:12.851: Crypto engine 0: create key pairs.
```

ステップ 2： DSS 公開キーをピアと手動で交換する (アウト・オブ・バンド)

暗号化セッションのアソシエーションを確立する最初のステップは、ルータ独自の DSS キー ペアを生成することでした。 次のステップでは、他のすべてのルータと公開キーを交換します。 最初に show crypto mypubkey コマンドを入力してルータの DSS 公開キーを表示することで、公開キーを手動で入力できます。 その後、公開キーを交換し（電子メールなどで）、crypto key pubkey-chain dss コマンドを使用して、ピア ルータの公開キーをルータにカット アンド ペースト します。

または、crypto key exchange dss コマンドを使用して、ルータに公開キーを自動的に交換させることもできます。 自動的な方法を使用する場合は、キー交換に使用するインターフェイスに crypto map ステートメントがないことを確認してください。 ここでは debug crypto key が役に立ちます。

注: 注：キーを交換する前に、ピアに対して ping を実行することをお勧めします。

```
Loser#ping 19.19.19.20 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to
19.19.19.20, timeout is 2 seconds: !!!!! Loser(config)#crypto key exchange dss passive Enter
escape character to abort if connection does not complete. Wait for connection from
peer[confirm] Waiting .... StHelen(config)#crypto key exchange dss 19.19.19.19 barney Public key
for barney: Serial Number 05694352 Fingerprint 309E D1DE B6DA 5145 D034 Wait for peer to send a
key[confirm] Public key for barney: Serial Number 05694352 Fingerprint 309E D1DE B6DA 5145 D034
Add this public key to the configuration? [yes/no]:yes Mar 16 12:16:55.343: CRYPTO-KE: Sent 2
bytes. Mar 16 12:16:55.343: CRYPTO-KE: Sent 4 bytes. Mar 16 12:16:55.343: CRYPTO-KE: Sent 2
bytes. Mar 16 12:16:55.347: CRYPTO-KE: Sent 64 bytes. Mar 16 12:16:45.099: CRYPTO-KE: Received 4
bytes. Mar 16 12:16:45.099: CRYPTO-KE: Received 2 bytes. Mar 16 12:16:45.103: CRYPTO-KE:
Received 6 bytes. Mar 16 12:16:45.103: CRYPTO-KE: Received 2 bytes. Mar 16 12:16:45.107: CRYPTO-
KE: Received 50 bytes. Mar 16 12:16:45.111: CRYPTO-KE: Received 14 bytes. Send peer a key in
return[confirm] Which one? fred? [yes]: Public key for fred: Serial Number 02802219 Fingerprint
2963 05F9 ED55 576D CF9D Waiting .... Public key for fred: Serial Number 02802219 Fingerprint
2963 05F9 ED55 576D CF9D Add this public key to the configuration? [yes/no]: Loser(config)# Mar
16 12:16:55.339: CRYPTO-KE: Sent 4 bytes. Mar 16 12:16:55.343: CRYPTO-KE: Sent 2 bytes. Mar 16
12:16:55.343: CRYPTO-KE: Sent 4 bytes. Mar 16 12:16:55.343: CRYPTO-KE: Sent 2 bytes. Mar 16
12:16:55.347: CRYPTO-KE: Sent 64 bytes. Loser(config)# Mar 16 12:16:56.083: CRYPTO-KE: Received
4 bytes. Mar 16 12:16:56.087: CRYPTO-KE: Received 2 bytes. Mar 16 12:16:56.087: CRYPTO-KE:
Received 4 bytes. Mar 16 12:16:56.091: CRYPTO-KE: Received 2 bytes. Mar 16 12:16:56.091: CRYPTO-
KE: Received 52 bytes. Mar 16 12:16:56.095: CRYPTO-KE: Received 12 bytes. Add this public key to
the configuration? [yes/no]: yes StHelen(config)#^Z StHelen#
```

公開 DSS キーの交換が済んだので、次のコマンド出力で示すようにして、両方のルータに相手側の公開キーがあり、それらが一致することを確認します。

```
Loser#show crypto key mypubkey dss crypto public-key fred 02802219 79CED212 AF191D29 702A9301
B3E06602 D4FB26B3 316E58C8 05D4930C CE891810 C0064492 5F6684CD 3FC326E5 679BCA46 BB155402
D443F68D 93487F7E 5ABE182E quit Loser#show crypto key pubkey-chain dss crypto public-key barney
05694352 B407A360 204CBFA3 F9A0C0B0 15D6185D 91FD7D3A 3232EBA2 F2D31D21 53AE24ED 732EA43D
484DEB22 6E91515C 234B4019 38E51D64 04CB9F59 EE357477 91810341 quit -------- StHelen#show crypto
key mypubkey dss crypto public-key barney 05694352 B407A360 204CBFA3 F9A0C0B0 15D6185D 91FD7D3A
3232EBA2 F2D31D21 53AE24ED 732EA43D 484DEB22 6E91515C 234B4019 38E51D64 04CB9F59 EE357477
91810341 quit StHelen#show crypto key pubkey-chain dss crypto public-key fred 02802219 79CED212
AF191D29 702A9301 B3E06602 D4FB26B3 316E58C8 05D4930C CE891810 C0064492 5F6684CD 3FC326E5
679BCA46 BB155402 D443F68D 93487F7E 5ABE182E quit
```

例 1： 専用 リンクのための Cisco IOSコンフィギュレーション

各ルータで DSS キーを生成し、DSS 公開キーを交換した後、インターフェイスに crypto map コマンドを適用できます。 crypto map で使用されているアクセス リストと一致するトラフィックを生成することで、暗号化セッションが開始します。

```
Loser#write terminal Building configuration... Current configuration: ! ! Last configuration
change at 13:01:18 UTC Mon Mar 16 1998 ! NVRAM config last updated at 13:03:02 UTC Mon Mar 16
1998 ! version 11.3 service timestamps debug datetime msec no service password-encryption !
hostname Loser ! enable secret 5 $1$AeuFSMx7O/DhpqjLKc2VQVbeC0 ! ip subnet-zero no ip domain-
lookup crypto map oldstyle 10 set peer barney match address 133 ! crypto key pubkey-chain dss
named-key barney serial-number 05694352 key-string B407A360 204CBFA3 F9A0C0B0 15D6185D 91FD7D3A
3232EBA2 F2D31D21 53AE24ED 732EA43D 484DEB22 6E91515C 234B4019 38E51D64 04CB9F59 EE357477
91810341 quit ! interface Ethernet0 ip address 40.40.40.41 255.255.255.0 no ip mroute-cache !
interface Serial0 ip address 18.18.18.18 255.255.255.0 encapsulation ppp no ip mroute-cache
shutdown ! interface Serial1 ip address 19.19.19.19 255.255.255.0 encapsulation ppp no ip
mroute-cache clockrate 2400 no cdp enable crypto map oldstyle ! ip default-gateway 10.11.19.254
ip classless ip route 0.0.0.0 0.0.0.0 19.19.19.20 access-list 133 permit ip 40.40.40.0 0.0.0.255
30.30.30.0 0.0.0.255 ! line con 0 exec-timeout 0 0 line aux 0 no exec transport input all line
vty 0 4 password ww login ! end Loser# ------------------------- StHelen#write terminal
Building configuration... Current configuration: ! ! Last configuration change at 13:03:05 UTC
Mon Mar 16 1998 ! NVRAM config last updated at 13:03:07 UTC Mon Mar 16 1998 ! version 11.3
service timestamps debug datetime msec no service password-encryption ! hostname StHelen ! boot
system flash c2500-is56-l enable password ww ! partition flash 2 8 8 ! no ip domain-lookup
crypto map oldstyle 10 set peer fred match address 144 ! crypto key pubkey-chain dss named-key
fred serial-number 02802219 key-string 79CED212 AF191D29 702A9301 B3E06602 D4FB26B3 316E58C8
05D4930C CE891810 C0064492 5F6684CD 3FC326E5 679BCA46 BB155402 D443F68D 93487F7E 5ABE182E quit !
! interface Ethernet0 ip address 30.30.30.31 255.255.255.0 ! interface Ethernet1 no ip address
shutdown ! interface Serial0 no ip address encapsulation x25 no ip mroute-cache shutdown !
interface Serial1 ip address 19.19.19.20 255.255.255.0 encapsulation ppp no ip mroute-cache
load-interval 30 compress stac no cdp enable crypto map oldstyle ! ip default-gateway
10.11.19.254 ip classless ip route 0.0.0.0 0.0.0.0 19.19.19.19 access-list 144 permit ip
30.30.30.0 0.0.0.255 40.40.40.0 0.0.0.255 ! line con 0 exec-timeout 0 0 line aux 0 transport
input all line vty 0 4 password ww login ! end StHelen#
```

例 2： マルチポイントフレームリレーのための Cisco IOSコンフィギュレーション

次のコマンド出力例は、HUB ルータからのものです。

```
Loser#write terminal Building configuration... Current configuration: ! ! Last configuration
change at 10:45:20 UTC Wed Mar 11 1998 ! NVRAM config last updated at 18:28:27 UTC Tue Mar 10
1998 ! version 11.3 service timestamps debug datetime msec no service password-encryption !
hostname Loser ! enable secret 5 $1$AeuFSMx7O/DhpqjLKc2VQVbeC0 ! ip subnet-zero no ip domain-
lookup ! crypto map oldstuff 10 set peer barney match address 133 crypto map oldstuff 20 set
peer wilma match address 144 ! crypto key pubkey-chain dss named-key barney serial-number
05694352 key-string 1D460DC3 BDC73312 93B7E220 1861D55C E00DA5D8 DB2B04CD FABD297C 899D40E7
D284F07D 6EEC83B8 E3676EC2 D813F7C8 F532DC7F 0A9913E7 8A6CB7E9 BE18790D quit named-key wilma
serial-number 01496536 key-string C26CB3DD 2A56DD50 CC2116C9 2697CE93 6DBFD824 1889F791 9BF36E70
7B29279C E343C56F 32266443 989B4528 1CF32C2D 9E3F2447 A5DBE054 879487F6 26A55939 quit ! crypto
cisco pregen-dh-pairs 5 ! crypto cisco key-timeout 1440 ! interface Ethernet0 ip address
190.190.190.190 255.255.255.0 no ip mroute-cache ! interface Serial1 ip address 19.19.19.19
255.255.255.0 encapsulation frame-relay no ip mroute-cache clockrate 500000 crypto map oldstuff
! ! ip default-gateway 10.11.19.254 ip classless ip route 200.200.200.0 255.255.255.0
19.19.19.20 ip route 210.210.210.0 255.255.255.0 19.19.19.21 access-list 133 permit ip
190.190.190.0 0.0.0.255 200.200.200.0 0.0.0.255 access-list 144 permit ip 190.190.190.0
0.0.0.255 210.210.210.0 0.0.0.255 ! line con 0 exec-timeout 0 0 line aux 0 no exec transport
input all line vty 0 4 password ww login ! end Loser#
```

次のコマンド出力例は、リモート サイト A からのものです。

```
WAN-2511a#write terminal Building configuration... Current configuration: ! version 11.3 no
service password-encryption ! hostname WAN-2511a ! enable password ww ! no ip domain-lookup !
crypto map mymap 10 set peer fred match address 133 ! crypto key pubkey-chain dss named-key fred
serial-number 02802219 key-string 56841777 4F27A574 5005E0F0 CF3C33F5 C6AAD000 5518A8FF 7422C592
021B295D D95AAB73 01235FD8 40D70284 3A63A38E 216582E8 EC1F8B0D 0256EFF5 0EE89436 quit !
interface Ethernet0 ip address 210.210.210.210 255.255.255.0 shutdown ! interface Serial0 ip
address 19.19.19.21 255.255.255.0 encapsulation frame-relay no fair-queue crypto map mymap ! ip
default-gateway 10.11.19.254 ip classless ip route 190.190.190.0 255.255.255.0 19.19.19.19
access-list 133 permit ip 210.210.210.0 0.0.0.255 190.190.190.0 0.0.0.255 ! line con 0 exec-
timeout 0 0 line 1 no exec transport input all line 2 16 no exec line aux 0 line vty 0 4
```

```
password ww login ! end WAN-2511a#
```

次のコマンド出力例は、リモート サイト B からのものです。

```
StHelen#write terminal Building configuration... Current configuration: ! ! Last configuration
change at 19:00:34 UTC Tue Mar 10 1998 ! NVRAM config last updated at 18:48:39 UTC Tue Mar 10
1998 ! version 11.3 service timestamps debug datetime msec no service password-encryption !
hostname StHelen ! boot system flash c2500-is56-l enable password ww ! partition flash 2 8 8 !
no ip domain-lookup ! crypto map wabba 10 set peer fred match address 144 ! crypto key pubkey-
chain dss named-key fred serial-number 02802219 key-string 56841777 4F27A574 5005E0F0 CF3C33F5
C6AAD000 5518A8FF 7422C592 021B295D D95AAB73 01235FD8 40D70284 3A63A38E 216582E8 EC1F8B0D
0256EFF5 0EE89436 quit ! interface Ethernet0 ip address 200.200.200.200 255.255.255.0 !
interface Serial1 ip address 19.19.19.20 255.255.255.0 encapsulation frame-relay no ip mroute-
cache crypto map wabba ! ip default-gateway 10.11.19.254 ip classless ip route 190.190.190.0
255.255.255.0 19.19.19.19 access-list 144 permit ip 200.200.200.0 0.0.0.255 190.190.190.0
0.0.0.255 ! line con 0 exec-timeout 0 0 line aux 0 transport input all line vty 0 4 password ww
login ! end StHelen#
```

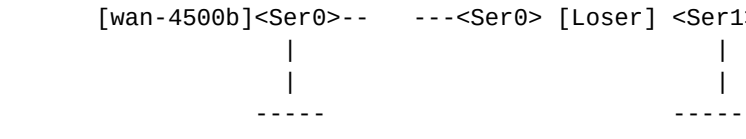
次のコマンド出力例は、フレーム リレー スイッチからのものです。

```
Current configuration:
!
version 11.2
no service password-encryption
no service udp-small-servers
no service tcp-small-servers
!
hostname wan-4700a
!
enable password ww
!
no ip domain-lookup
frame-relay switching
!
interface Serial0
 no ip address
 encapsulation frame-relay
 clockrate 500000
 frame-relay intf-type dce
 frame-relay route 200 interface Serial1 100
!
interface Serial1
 no ip address
 encapsulation frame-relay
 frame-relay intf-type dce
 frame-relay route 100 interface Serial0 200
 frame-relay route 300 interface Serial2 200
!
interface Serial2
 no ip address
 encapsulation frame-relay
 clockrate 500000
 frame-relay intf-type dce
 frame-relay route 200 interface Serial1 300
!
```

例 3： ルータを介した暗号化

ピア ルータとの距離は、1 ホップである必要はありません。 リモート ルータとピアリング セッションを作成することもできます。 次の例では、180.180.180.0/24 と 40.40.40.0/24 の間、および 180.180.180.0/24 と 30.30.30.0/24 の間のすべてのネットワーク トラフィックを暗号化することが目的です。 40.40.40.0/24 と 30.30.30.0/24 の間のトラフィックは暗号化しません。

ルータ wan-4500b では Loser との間、および StHelen との間に暗号化セッション アソシエーションがあります。 wan-4500b のイーサネット セグメントから StHelen のイーサネット セグメントまでのトラフィックを暗号化することで、Loser での無用な復号化ステップを回避できます。 Loser は暗号化されたトラフィックを単純に StHelen のシリアル インターフェイスに渡し、トラフィックはそこで復号化されます。 これにより、Loser ルータでの IP パケットに対するトラフィック遅延と CPU サイクルが減少します。 さらに重要なこととして、Loser に盗聴者がいてもトラフィックを読み取ることができないので、システムのセキュリティが大幅に向上します。 Loser がトラフィックを復号化すると、復号化されたデータを悪用される可能性があります。



wan-4500b#**write terminal** Building configuration... Current configuration: ! version 11.3 no service password-encryption ! hostname wan-4500b ! enable password 7 111E0E ! username cse password 0 ww no ip domain-lookup ! crypto map toworld 10 set peer loser match address 133 crypto map toworld 20 set peer sthelen match address 144 ! crypto key pubkey-chain dss named-key loser serial-number 02802219 key-string F0BE2128 752D1A24 F394B355 3216BA9B 7C4E8677 29C176F9 A047B7D9 7D03BDA4 6B7AFDC2 2DAEF3AB 393EE7C7 802C1A95 B40031D1 908004F9 8A33A352 FF19BC24 quit named-key sthelen serial-number 05694352 key-string 5C401002 404DC5A9 EAED2360 D7007E51 4A4BB8F8 6F9B1554 51D8ACBB D3964C10 A23848CA 46003A94 2FC8C7D6 0B57AE07 9EB5EF3A BD71482B 052CF06B 90C3C618 quit ! interface Ethernet0 ip address 180.180.180.180 255.255.255.0 ! interface Serial0 ip address 18.18.18.19 255.255.255.0 encapsulation ppp crypto map toworld ! router rip network 18.0.0.0 network 180.180.0.0 ! ip classless ip route 0.0.0.0 0.0.0.0 30.30.30.31 ip route 171.68.118.0 255.255.255.0 10.11.19.254 access-list 133 permit ip 180.180.180.0 0.0.0.255 40.40.40.0 0.0.0.255 access-list 144 permit ip 180.180.180.0 0.0.0.255 30.30.30.0 0.0.0.255 ! line con 0 exec-timeout 0 0 line aux 0 password 7 044C1C line vty 0 4 login local ! end wan-4500b# ---------- Loser#**write terminal** Building configuration... Current configuration: ! ! Last configuration change at 11:01:54 UTC Wed Mar 18 1998 ! NVRAM config last updated at 11:09:59 UTC Wed Mar 18 1998 ! version 11.3 service timestamps debug datetime msec no service password-encryption ! hostname Loser ! enable secret 5 1AeuFSMx7O/DhpqjLKc2VQVbeC0 ! ip subnet-zero no ip domain-lookup ip host StHelen.cisco.com 19.19.19.20 ip domain-name cisco.com ! crypto map towan 10 set peer wan match address 133 ! crypto key pubkey-chain dss named-key wan serial-number 07365004 key-string A547B701 4312035D 2FC7D0F4 56BC304A 59FA76C3 B9762E4A F86DED86 3830E66F 2ED5C476 CFF234D3 3842BC98 3CA4A5FB 9089556C 7464D2B4 AF7E6AEB 86269A5B quit ! interface Ethernet0 ip address 40.40.40.40 255.255.255.0 no ip mroute-cache ! interface Serial0 ip address 18.18.18.18 255.255.255.0 encapsulation ppp no ip mroute-cache clockrate 64000 crypto map towan ! interface Serial1 ip address 19.19.19.19 255.255.255.0 encapsulation ppp no ip mroute-cache priority-group 1 clockrate 64000 ! ! router rip network 19.0.0.0 network 18.0.0.0 network 40.0.0.0 ! ip default-gateway 10.11.19.254 ip classless access-list 133 permit ip 40.40.40.0 0.0.0.255 180.180.180.0 0.0.0.255 ! line con 0 exec-timeout 0 0 line aux 0 no exec transport input all line vty 0 4 password ww login ! end Loser# ---------- StHelen#**write terminal** Building configuration... Current configuration: ! ! Last configuration change at 11:13:18 UTC Wed Mar 18 1998 ! NVRAM config last updated at 11:21:30 UTC Wed Mar 18 1998 ! version 11.3 service timestamps debug datetime msec no service password-encryption ! hostname StHelen ! boot system flash c2500-is56-l enable password ww ! partition flash 2 8 8 ! no ip domain-lookup ! crypto map towan 10 set peer wan match address 144 ! crypto key pubkey-chain dss named-key wan serial-number 07365004 key-string A547B701 4312035D 2FC7D0F4 56BC304A 59FA76C3 B9762E4A F86DED86 3830E66F 2ED5C476 CFF234D3 3842BC98 3CA4A5FB 9089556C 7464D2B4 AF7E6AEB 86269A5B quit ! interface Ethernet0 no ip address ! interface Ethernet1 ip address 30.30.30.30 255.255.255.0 ! interface Serial1 ip address 19.19.19.20 255.255.255.0 encapsulation ppp no ip mroute-cache load-interval 30 crypto map towan ! router rip network 30.0.0.0 network 19.0.0.0 ! ip default-gateway 10.11.19.254 ip classless access-list 144 permit ip 30.30.30.0 0.0.0.255 180.180.180.0 0.0.0.255 ! line con 0 exec-timeout 0 0 line aux 0 transport input all line vty 0 4 password ww login ! end StHelen# ---------- wan-4500b#**show crypto cisco algorithms** des cfb-64 40-bit-des cfb-64 wan-4500b#**show crypto cisco key-timeout** Session keys will be re-negotiated every 30 minutes wan-4500b#**show crypto cisco pregen-dh-pairs** Number of pregenerated DH pairs: 0 wan-4500b#**show crypto engine connections active** ID Interface IP-Address State Algorithm Encrypt Decrypt 1 Serial0 18.18.18.19 set DES_56_CFB64 1683 1682 5 Serial0 18.18.18.19 set DES_56_CFB64 1693 1693 wan-4500b#**show crypto engine connections dropped-packet** Interface IP-Address Drop Count Serial0 18.18.18.19 52 wan-4500b#**show crypto engine**

configuration slot: 0 engine name: wan engine type: software serial number: 07365004 platform: rp crypto engine crypto lib version: 10.0.0 Encryption Process Info: input queue top: 303 input queue bot: 303 input queue count: 0 wan-4500b#**show crypto key mypubkey dss** crypto public-key wan 07365004 A547B701 4312035D 2FC7D0F4 56BC304A 59FA76C3 B9762E4A F86DED86 3830E66F 2ED5C476 CFF234D3 3842BC98 3CA4A5FB 9089556C 7464D2B4 AF7E6AEB 86269A5B quit wan-4500b#**show crypto key pubkey-chain dss** crypto public-key loser 02802219 F0BE2128 752D1A24 F394B355 3216BA9B 7C4E8677 29C176F9 A047B7D9 7D03BDA4 6B7AFDC2 2DAEF3AB 393EE7C7 802C1A95 B40031D1 908004F9 8A33A352 FF19BC24 quit crypto public-key sthelen 05694352 5C401002 404DC5A9 EAED2360 D7007E51 4A4BB8F8 6F9B1554 51D8ACBB D3964C10 A23848CA 46003A94 2FC8C7D6 0B57AE07 9EB5EF3A BD71482B 052CF06B 90C3C618 quit wan-4500b#**show crypto map interface serial 1** No crypto maps found. wan-4500b#**show crypto map** Crypto Map "toworld" 10 cisco Connection Id = 1 (1 established, 0 failed) Peer = loser PE = 180.180.180.0 UPE = 40.40.40.0 Extended IP access list 133 access-list 133 permit ip source: addr = 180.180.180.0/0.0.0.255 dest: addr = 40.40.40.0/0.0.0.255 Crypto Map "toworld" 20 cisco Connection Id = 5 (1 established, 0 failed) Peer = sthelen PE = 180.180.180.0 UPE = 30.30.30.0 Extended IP access list 144 access-list 144 permit ip source: addr = 180.180.180.0/0.0.0.255 dest: addr = 30.30.30.0/0.0.0.255 wan-4500b# ---------- Loser#**show crypto cisco algorithms** des cfb-64 des cfb-8 40-bit-des cfb-64 40-bit-des cfb-8 Loser#**show crypto cisco key-timeout** Session keys will be re-negotiated every 30 minutes Loser#**show crypto cisco pregen-dh-pairs** Number of pregenerated DH pairs: 10 Loser#**show crypto engine connections active** ID Interface IP-Address State Algorithm Encrypt Decrypt 61 Serial0 18.18.18.18 set DES_56_CFB64 1683 1682 Loser#**show crypto engine connections dropped-packet** Interface IP-Address Drop Count Serial0 18.18.18.18 1 Serial1 19.19.19.19 90 Loser#**show crypto engine configuration** slot: 0 engine name: loser engine type: software serial number: 02802219 platform: rp crypto engine crypto lib version: 10.0.0 Encryption Process Info: input queue top: 235 input queue bot: 235 input queue count: 0 Loser#**show crypto key mypubkey dss** crypto public-key loser 02802219 F0BE2128 752D1A24 F394B355 3216BA9B 7C4E8677 29C176F9 A047B7D9 7D03BDA4 6B7AFDC2 2DAEF3AB 393EE7C7 802C1A95 B40031D1 908004F9 8A33A352 FF19BC24 quit Loser#**show crypto key pubkey-chain dss** crypto public-key wan 07365004 A547B701 4312035D 2FC7D0F4 56BC304A 59FA76C3 B9762E4A F86DED86 3830E66F 2ED5C476 CFF234D3 3842BC98 3CA4A5FB 9089556C 7464D2B4 AF7E6AEB 86269A5B quit Loser#**show crypto map interface serial 1** No crypto maps found. Loser#**show crypto map** Crypto Map "towan" 10 cisco Connection Id = 61 (0 established, 0 failed) Peer = wan PE = 40.40.40.0 UPE = 180.180.180.0 Extended IP access list 133 access-list 133 permit ip source: addr = 40.40.40.0/0.0.0.255 dest: addr = 180.180.180.0/0.0.0.255 Loser# ---------- ---------- StHelen#**show crypto cisco algorithms** des cfb-64 StHelen#**show crypto cisco key-timeout** Session keys will be re-negotiated every 30 minutes StHelen#**show crypto cisco pregen-dh-pairs** Number of pregenerated DH pairs: 10 StHelen#**show crypto engine connections active** ID Interface IP-Address State Algorithm Encrypt Decrypt 58 Serial1 19.19.19.20 set DES_56_CFB64 1694 1693 StHelen#**show crypto engine connections dropped-packet** Interface IP-Address Drop Count Ethernet0 0.0.0.0 1 Serial1 19.19.19.20 80 StHelen#**show crypto engine configuration** slot: 0 engine name: sthelen engine type: software serial number: 05694352 platform: rp crypto engine crypto lib version: 10.0.0 Encryption Process Info: input queue top: 220 input queue bot: 220 input queue count: 0 StHelen#**show crypto key mypubkey dss** crypto public-key sthelen 05694352 5C401002 404DC5A9 EAED2360 D7007E51 4A4BB8F8 6F9B1554 51D8ACBB D3964C10 A23848CA 46003A94 2FC8C7D6 0B57AE07 9EB5EF3A BD71482B 052CF06B 90C3C618 quit StHelen#**show crypto key pubkey-chain dss** crypto public-key wan 07365004 A547B701 4312035D 2FC7D0F4 56BC304A 59FA76C3 B9762E4A F86DED86 3830E66F 2ED5C476 CFF234D3 3842BC98 3CA4A5FB 9089556C 7464D2B4 AF7E6AEB 86269A5B quit StHelen#**show crypto map interface serial 1** Crypto Map "towan" 10 cisco Connection Id = 58 (1 established, 0 failed) Peer = wan PE = 30.30.30.0 UPE = 180.180.180.0 Extended IP access list 144 access-list 144 permit ip source: addr = 30.30.30.0/0.0.0.255 dest: addr = 180.180.180.0/0.0.0.255 StHelen#**show crypto map** Crypto Map "towan" 10 cisco Connection Id = 58 (1 established, 0 failed) Peer = wan PE = 30.30.30.0 UPE = 180.180.180.0 Extended IP access list 144 access-list 144 permit ip source: addr = 30.30.30.0/0.0.0.255 dest: addr = 180.180.180.0/0.0.0.255 StHelen#

サンプル 4: DDR との暗号

Cisco IOS は ICMP を利用して暗号化セッションを確立するので、DDR リンクで暗号化を行う場合は、ダイヤラ リストで ICMP トラフィックを「対象」として分類する必要があります。

注: Cisco IOS ソフトウェア リリース 11.3 では圧縮を行うことができますが、暗号化されたデータにはあまり役に立ちません。 暗号化されたデータは見かけが非常にランダムになるので、圧縮を行っても処理が遅くなるだけです。 ただし、暗号化されていないトラフィックに対しては圧縮

を有効にしておいてかまいません。

状況によっては、同じルータに対するダイヤル バックアップが必要になります。 たとえば、WAN ネットワークでの特定のリンクの障害に対する保護として有効です。 同じピアに対して 2 つのインターフェイスがある場合は、両方のインターフェイスで同じ crypto map を使用できます。 この機能が正しく動作するためには、バックアップ インターフェイスを使用する必要があります。 バックアップの設計でルータが別のボックスにダイヤルする場合は、別の crypto map を作成し、それに従ってピアを設定する必要があります。 ここでも、backup interface コマンドを使用する必要があります。

```
dial-5#write terminal Building configuration... Current configuration: ! version 11.3 no service
password-encryption service udp-small-servers service tcp-small-servers ! hostname dial-5 ! boot
system c1600-sy56-l 171.68.118.83 enable secret 5 $1$oNe1wDbhBdcN6x9Y5gfuMjqh10 ! username dial-
6 password 0 cisco isdn switch-type basic-ni1 ! crypto map dial6 10 set peer dial6 match address
133 ! crypto key pubkey-chain dss named-key dial6 serial-number 05679987 key-string 753F71AB
E5305AD4 3FCDFB6D 47AA2BB5 656BFCAA 53DBE37F 07465189 06E91A82 2BC91236 13DC4AA8 7EC5B48C
D276E5FE 0D093014 6D3061C5 03158820 B609CA7C quit ! interface Ethernet0 ip address 20.20.20.20
255.255.255.0 ! interface BRI0 ip address 10.10.10.11 255.255.255.0 encapsulation ppp no ip
mroute-cache load-interval 30 dialer idle-timeout 9000 dialer map ip 10.10.10.10 name dial-6
4724118 dialer hold-queue 40 dialer-group 1 isdn spid1 919472417100 4724171 isdn spid2
919472417201 4724172 compress stac ppp authentication chap ppp multilink crypto map dial6 ! ip
classless ip route 40.40.40.0 255.255.255.0 10.10.10.10 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 dial-5# ----------------------- dial-6#write terminal
Building configuration... Current configuration: ! version 11.3 no service password-encryption
service udp-small-servers service tcp-small-servers ! hostname dial-6 ! boot system c1600-sy56-l
171.68.118.83 enable secret 5 $1$VdPYuA/BIVeEm9UAFEm.PPJFc. ! username dial-5 password 0 cisco
no ip domain-lookup isdn switch-type basic-ni1 ! crypto map dial5 10 set peer dial5 match
address 144 ! crypto key pubkey-chain dss named-key dial5 serial-number 05679919 key-string
160AA490 5B9B1824 24769FCD EE5E0F46 1ABBD343 4C0C4A03 4B279D6B 0EE5F65F F64665D4 1036875A
8CF93691 BDF81722 064B51C9 58D72E12 3E1894B6 64B1D145 quit ! ! interface Ethernet0 ip address
40.40.40.40 255.255.255.0 ! interface BRI0 ip address 10.10.10.10 255.255.255.0 encapsulation
ppp no ip mroute-cache dialer idle-timeout 9000 dialer map ip 10.10.10.11 name dial-5 4724171
dialer hold-queue 40 dialer load-threshold 5 outbound dialer-group 1 isdn spid1 919472411800
4724118 isdn spid2 919472411901 4724119 compress stac ppp authentication chap ppp multilink
crypto map dial5 ! ip classless ip route 20.20.20.0 255.255.255.0 10.10.10.11 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 dial-6#
```

サンプル 5: IPトンネルにおけるIPXトラフィックの暗号化

この例では、IP トンネル内の IPX トラフィックを暗号化します。

注: 暗号化されるのは、このトンネル（IPX）内のトラフィックだけです。 その他すべての IP トラフィックは暗号化されません。

```
WAN-2511a#write terminal Building configuration... Current configuration: ! version 11.2 no
service password-encryption no service udp-small-servers no service tcp-small-servers ! hostname
WAN-2511a ! enable password ww ! no ip domain-lookup ipx routing 0000.0c34.aa6a ! crypto public-
key wan2516 01698232 B1C127B0 78D79CAA 67ECAD80 03D354B1 9012C80E 0C1266BE 25AEDE60 37A192A2
B066D299 77174D48 7FBAB5FC 2B60893A 37E5CB7B 62F6D902 9495733B 98046962 quit ! crypto map
wan2516 10 set peer wan2516 match address 133 ! ! interface Loopback1 ip address 50.50.50.50
255.255.255.0 ! interface Tunnel1 no ip address ipx network 100 tunnel source 50.50.50.50 tunnel
destination 60.60.60.60 crypto map wan2516 ! interface Ethernet0 ip address 40.40.40.40
255.255.255.0 ipx network 600 ! interface Serial0 ip address 20.20.20.21 255.255.255.0
encapsulation ppp no ip mroute-cache crypto map wan2516 ! interface Serial1 no ip address
shutdown ! ip default-gateway 10.11.19.254 ip classless ip route 0.0.0.0 0.0.0.0 20.20.20.20
access-list 133 permit ip host 50.50.50.50 host 60.60.60.60 ! line con 0 exec-timeout 0 0
password ww login line 1 16 line aux 0 password ww login line vty 0 4 password ww login ! end
WAN-2511a# ----------------------- WAN-2516a#write terminal Building configuration... Current
configuration: ! version 11.2 no service pad no service password-encryption service udp-small-
```

```
servers service tcp-small-servers ! hostname WAN-2516a ! enable password ww ! no ip domain-
lookup ipx routing 0000.0c3b.cc1e ! crypto public-key wan2511 01496536 C8EA7C21 DF3E48F5
C6C069DB 3A5E1B08 8B830AD4 4F1DABCE D62F5F46 ED08C81D 5646DC78 DDC77EFC 823F302A F112AF97
668E39A1 E2FCDC05 545E0529 9B3C9553 quit ! crypto map wan2511 10 set peer wan2511 match address
144 ! ! hub ether 0 1 link-test auto-polarity ! ! <other hub interfaces snipped> ! hub ether 0
14 link-test auto-polarity ! interface Loopback1 ip address 60.60.60.60 255.255.255.0 !
interface Tunnel1 no ip address ipx network 100 tunnel source 60.60.60.60 tunnel destination
50.50.50.50 crypto map wan2511 ! interface Ethernet0 ip address 30.30.30.30 255.255.255.0 ipx
network 400 ! interface Serial0 ip address 20.20.20.20 255.255.255.0 encapsulation ppp clockrate
2000000 crypto map wan2511 ! interface Serial1 no ip address shutdown ! interface BRI0 no ip
address 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 host 60.60.60.60 host 50.50.50.50 access-list 188 permit
gre any any ! 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 WAN-2516a# -
---------- WAN-2511a#show ipx route Codes: C - Connected primary network, c -
Connected secondary network S - Static, F - Floating static, L - Local (internal), W - IPXWAN R
- RIP, E - EIGRP, N - NLSP, X - External, A - Aggregate s - seconds, u - uses 3 Total IPX
routes. Up to 1 parallel paths and 16 hops allowed. No default route known. C 100 (TUNNEL), Tu1
C 600 (NOVELL-ETHER), Et0 R 400 [151/01] via 100.0000.0c3b.cc1e, 24s, Tu1 WAN-2511a#show crypto
engine connections active ID Interface IP-Address State Algorithm Encrypt Decrypt 1 Serial0
20.20.20.21 set DES_56_CFB64 207 207 WAN-2511a#ping 400.0000.0c3b.cc1e Translating
"400.0000.0c3b.cc1e" Type escape sequence to abort. Sending 5, 100-byte IPX cisco Echoes to
400.0000.0c3b.cc1e, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip
min/avg/max = 32/35/48 ms WAN-2511a#show crypto engine connections active ID Interface IP-
Address State Algorithm Encrypt Decrypt 1 Serial0 20.20.20.21 set DES_56_CFB64 212 212 WAN-
2511a#ping 30.30.30.30 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to
30.30.30.30, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip
min/avg/max = 4/5/8 ms WAN-2511a#show crypto engine connections active ID Interface IP-Address
State Algorithm Encrypt Decrypt 1 Serial0 20.20.20.21 set DES_56_CFB64 212 212 WAN-2511a#
```

サンプル 6: L2F トンネルの暗号化

この例では、ダイヤルインするユーザのための L2F トラフィックだけに暗号化を試みています。user@cisco.com が市内にある「DEMO2」という名前のローカルな Network Access Server (NAS; ネットワーク アクセス サーバ) を呼び出して、ホーム ゲートウェイ CD に対するトンネルを確立します。 すべての DEMO2 トラフィックは (他の L2F 通話者のトラフィックと同様に) 暗号化されます。 L2F は UDP ポート 1701 を使用するので、ここで示すような方法でアクセス リストを作成し、これにより暗号化するトラフィックが決まります。

注: 暗号化アソシエーションがまだセットアップされていない場合、つまりその通話者が電話をかけて L2F トンネルを作成する最初の通話者である場合は、暗号化アソシエーションをセットアップする遅延のために、この通話者は廃棄される可能性があります。 十分な処理能力の CPU を備えたルータでは、このようなことは発生しません。 また、暗号化のセットアップとティアダウンがオフピークの時間中にだけ行われるよう、keytimeout の値を大きくすることもできます。

次のコマンド出力例は、リモートの NAS からのものです。

```
DEMO2#write terminal Building configuration... Current configuration: ! version 11.2 no service
password-encryption no service udp-small-servers no service tcp-small-servers ! hostname DEMO2 !
enable password ww ! username NAS1 password 0 SECRET username HomeGateway password 0 SECRET no
ip domain-lookup vpdn enable vpdn outgoing cisco.com NAS1 ip 20.20.20.20 ! crypto public-key
wan2516 01698232 B1C127B0 78D79CAA 67ECAD80 03D354B1 9012C80E 0C1266BE 25AEDE60 37A192A2
B066D299 77174D48 7FBAB5FC 2B60893A 37E5CB7B 62F6D902 9495733B 98046962 quit ! crypto map vpdn
10 set peer wan2516 match address 133 ! crypto key-timeout 1440 ! interface Ethernet0 ip address
40.40.40.40 255.255.255.0 ! interface Serial0 ip address 20.20.20.21 255.255.255.0 encapsulation
ppp no ip mroute-cache crypto map vpdn ! interface Serial1 no ip address shutdown ! interface
Group-Async1 no ip address encapsulation ppp async mode dedicated no peer default ip address no
cdp enable ppp authentication chap pap group-range 1 16 ! ip default-gateway 10.11.19.254 ip
classless ip route 0.0.0.0 0.0.0.0 20.20.20.20 access-list 133 permit udp host 20.20.20.21 eq
1701 host 20.20.20.20 eq 1701 ! ! line con 0 exec-timeout 0 0 password ww login line 1 16 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 DEMO2#
```

次のコマンド出力例は、ホーム ゲートウェイからのものです。

```
CD#write terminal Building configuration... Current configuration: ! version 11.2 no service pad
no service password-encryption service udp-small-servers service tcp-small-servers ! hostname CD
! enable password ww ! username NAS1 password 0 SECRET username HomeGateway password 0 SECRET
username user@cisco.com password 0 cisco no ip domain-lookup vpdn enable vpdn incoming NAS1
HomeGateway virtual-template 1 ! crypto public-key wan2511 01496536 C8EA7C21 DF3E48F5 C6C069DB
3A5E1B08 8B830AD4 4F1DABCE D62F5F46 ED08C81D 5646DC78 DDC77EFC 823F302A F112AF97 668E39A1
E2FCDC05 545E0529 9B3C9553 quit ! crypto key-timeout 1440 ! crypto map vpdn 10 set peer wan2511
match address 144 ! ! hub ether 0 1 link-test auto-polarity ! interface Loopback0 ip address
70.70.70.1 255.255.255.0 ! interface Ethernet0 ip address 30.30.30.30 255.255.255.0 ! interface
Virtual-Template1 ip unnumbered Loopback0 no ip mroute-cache peer default ip address pool
default ppp authentication chap ! interface Serial0 ip address 20.20.20.20 255.255.255.0
encapsulation ppp clockrate 2000000 crypto map vpdn ! interface Serial1 no ip address shutdown !
interface BRI0 no ip address shutdown ! ip local pool default 70.70.70.2 70.70.70.77 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 udp
host 20.20.20.20 eq 1701 host 20.20.20.21 eq 1701 ! 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
```

トラブルシューティング

一般に、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は、次の show コマンドを使用して情報を収集することです。 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	
show crypto cisco algorithms	show crypto cisco key-timeout
show crypto cisco pregen-dh-pairs	* show crypto engine connections active
show crypto engine connections dropped-packet	show crypto engine configuration
show crypto key mypubkey dss	* show crypto key pubkey-chain dss
show crypto map interface serial 1	* show crypto map
debug crypto engine	* debug crypto sess
debug cry key	clear crypto connection
crypto zeroize	no crypto public-key

- **show crypto cisco algorithms**- 暗号化を行う他のピア ルータと通信するために使用するすべての Data Encryption Standard (DES; データ暗号規格) アルゴリズムを有効にする必要があります。 DES アルゴリズムを有効にしていないと、後で crypto map にそのアルゴリズムを割り当てようとしても、このアルゴリズムは使用できません。あるルータがピア ルータとの暗号化通信セッションをセットアップしようとした場合、両端で 2 つのルータが同じ DES ア

ルゴリズムを有効にしていないと、暗号化セッションは失敗します。 1 つでも共通の DES アルゴリズムが両端で有効になっている場合は、暗号化セッションを続行できます。**注** : Cisco IOS ソフトウェア リリース 11.3 では、新しいキーワード cisco が追加されました。このキーワードは、Cisco IOS ソフトウェア リリース 11.2 で使用されているシスコ固有の暗号化と IPSec とを区別するために必要です。`Loser#`**`show crypto cisco algorithms`** `des cfb-64 des cfb-8 40-bit-des cfb-64 40-bit-des cfb-8`

- show crypto cisco key-timeout - 確立された暗号化通信セッションは、特定の時間だけ有効になっています。 この時間が経過すると、セッションはタイムアウトします。 暗号化された通信を続けるには、新しいセッションをネゴシエートし、新しい DES（セッション）キーを生成する必要があります。 暗号化通信セッションが期限切れ（タイムアウト）になるまでの経過時間を変更するには、このコマンドを使用します。`Loser#`**`show crypto cisco key-timeout`** `Session keys will be re-negotiated every 30 minutes` DES キーが再ネゴシエートされるまでの時間の長さを決定するには、次のコマンドを使用します。`StHelen#`**`show crypto conn`** `Connection Table PE UPE Conn_id New_id Algorithm Time 0.0.0.1 0.0.0.1 4 0 DES_56_CFB64 Mar 01 1993 03:16:09 flags:TIME_KEYS StHelen#`**`show crypto key`** `Session keys will be re-negotiated every 30 minutes StHelen#`**`show clock`** `*03:21:23.031 UTC Mon Mar 1 1993`
- show crypto cisco pregen-dh-pairs - 各暗号化セッションは、DH 番号の固有のペアを使用します。 新しいセッションが確立されるたびに、新しい DH 番号ペアを生成する必要があります。 セッションが完了すると、これらの番号は破棄されます。 新しい DH 番号ペアの生成は CPU に負荷のかかる作業であり、セッションのセットアップが遅くなる可能性があります。特に、ローエンドのルータには影響があります。セッションのセットアップを加速するためには、指定した数の DH 番号ペアをあらかじめ生成し、予備として保持しておくことができます。 その後、暗号化通信セッションがセットアップされるときには、この予備から DH 番号ペアが提供されます。 DH 番号ペアが使用されると、予備には新しい DH 番号ペアが自動的に補充されるので、常に使用可能な DH 番号ペアが存在することになります。ルータが複数の暗号化セッションを頻繁にセットアップするためにあらかじめ生成されている予備の DH 番号ペアの数が 1 個や 2 個では短時間で使用されてしまうのでない限り、通常は、あらかじめ生成しておく DH 番号ペアの数は 1 個または 2 個で十分です。`Loser#`**`show crypto cisco pregen-dh-pairs`** `Number of pregenerated DH pairs: 10`
- **show crypto cisco connections active**次に示すのは、このコマンドの出力例です。`Loser#`**`show crypto engine connections active`** `ID Interface IP-Address State Algorithm Encrypt Decrypt 16 Serial1 19.19.19.19 set DES_56_CFB64 376 884`
- **show crypto cisco engine connections dropped-packet**次に示すのは、このコマンドの出力例です。`Loser#`**`show crypto engine connections dropped-packet`** `Interface IP-Address Drop Count Serial1 19.19.19.19 39`
- show crypto engine configuration（Cisco IOS ソフトウェア リリース 11.2 では show crypto engine brief でした）次に示すのは、このコマンドの出力例です。`Loser#`**`show crypto engine configuration`** `slot: 0 engine name: fred engine type: software serial number: 02802219 platform: rp crypto engine crypto lib version: 10.0.0 Encryption Process Info: input queue top: 465 input queue bot: 465 input queue count: 0`
- **show crypto key mypubkey dss**次に示すのは、このコマンドの出力例です。`Loser#`**`show crypto key mypubkey dss`** `crypto public-key fred 02802219 79CED212 AF191D29 702A9301 B3E06602 D4FB26B3 316E58C8 05D4930C CE891810 C0064492 5F6684CD 3FC326E5 679BCA46 BB155402 D443F68D 93487F7E 5ABE182E quit`
- **show crypto key pubkey-chain dss**次に示すのは、このコマンドの出力例です。`Loser#`**`show crypto key pubkey-chain dss`** `crypto public-key barney 05694352 B407A360 204CBFA3 F9A0C0B0 15D6185D 91FD7D3A 3232EBA2 F2D31D21 53AE24ED 732EA43D 484DEB22 6E91515C 234B4019 38E51D64 04CB9F59 EE357477 91810341 quit`
- **show crypto map interface serial 1**次に示すのは、このコマンドの出力例です。`Loser#`**`show crypto map interface serial 1`** `Crypto Map "oldstyle" 10 cisco Connection Id = 16 (8 established, 0 failed) Peer = barney PE = 40.40.40.0 UPE = 30.30.30.0 Extended IP access list 133 access-list 133 permit ip source: addr = 40.40.40.0/0.0.0.255 dest: addr = 30.30.30.0/0.0.0.255` ping コマンドを使用したときの時間の違いに注意してください。`wan-`

5200b#**ping 30.30.30.30** Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 30.30.30.30, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 52/54/56 ms wan-5200b# ---------- wan-5200b#**ping 30.30.30.31** Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 30.30.30.31, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 52/53/56 ms ---------- wan-5200b#**ping 19.19.19.20** Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 19.19.19.20, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 20/21/24 ms ----------

- **show crypto map interface serial 1**次に示すのは、このコマンドの出力例です。Loser#**show crypto map** Crypto Map "oldstyle" 10 cisco Connection Id = 16 (8 established, 0 failed) Peer = barney PE = 40.40.40.0 UPE = 30.30.30.0 Extended IP access list 133 access-list 133 permit ip source: addr = 40.40.40.0/0.0.0.255 dest: addr = 30.30.30.0/0.0.0.255
- **debug crypto engine**次に示すのは、このコマンドの出力例です。Loser#**debug crypto engine** Mar 17 11:49:07.902: Crypto engine 0: generate alg param Mar 17 11:49:07.906: CRYPTO_ENGINE: Dh phase 1 status: 0 Mar 17 11:49:07.910: Crypto engine 0: sign message using crypto engine Mar 17 11:49:09.894: CRYPTO_ENGINE: packets dropped: State = 0 Mar 17 11:49:11.758: Crypto engine 0: generate alg param Mar 17 11:49:12.246: CRYPTO_ENGINE: packets dropped: State = 0 Mar 17 11:49:13.342: CRYPTO ENGINE 0: get syndrome for conn id 25 Mar 17 11:49:13.346: Crypto engine 0: verify signature Mar 17 11:49:14.054: CRYPTO_ENGINE: packets dropped: State = 0 Mar 17 11:49:14.402: Crypto engine 0: sign message using crypto engine Mar 17 11:49:14.934: Crypto engine 0: create session for conn id 25 Mar 17 11:49:14.942: CRYPTO ENGINE 0: clear dh number for conn id 25 Mar 17 11:49:24.946: Crypto engine 0: generate alg param
- **debug crypto sessmgmt**次に示すのは、このコマンドの出力例です。StHelen#**debug crypto sessmgmt** Mar 17 11:49:08.918: IP: s=40.40.40.40 (Serial1), d=30.30.30.30, len 328, Found an ICMP connection message. Mar 17 11:49:08.922: CRYPTO: Dequeued a message: CIM Mar 17 11:49:08.926: CRYPTO-SDU: Key Timeout, Re-exchange Crypto Keys Mar 17 11:49:09.978: CRYPTO: Verify done. Status=OK Mar 17 11:49:09.994: CRYPTO: DH gen phase 1 status for conn_id 22 slot 0:OK Mar 17 11:49:11.594: CRYPTO: DH gen phase 2 status for conn_id 22 slot 0:OK Mar 17 11:49:11.598: CRYPTO: Syndrome gen status for conn_id 22 slot 0:OK Mar 17 11:49:12.134: CRYPTO: Sign done. Status=OK Mar 17 11:49:12.142: CRYPTO: ICMP message sent: s=19.19.19.20, d=19.19.19.19 Mar 17 11:49:12.146: CRYPTO-SDU: act_on_nnc_req: NNC Echo Reply sent Mar 17 11:49:12.154: CRYPTO: Create encryption key for conn_id 22 slot 0:OK Mar 17 11:49:15.366: CRYPTO: Dequeued a message: CCM Mar 17 11:49:15.370: CRYPTO: Syndrome gen status for conn_id 22 slot 0:OK Mar 17 11:49:16.430: CRYPTO: Verify done. Status=OK Mar 17 11:49:16.434: CRYPTO: Replacing -23 in crypto maps with 22 (slot 0) Mar 17 11:49:26.438: CRYPTO: Need to pregenerate 1 pairs for slot 0. Mar 17 11:49:26.438: CRYPTO: Pregenerating DH for conn_id 32 slot 0 Mar 17 11:49:28.050: CRYPTO: DH phase 1 status for conn_id 32 slot 0:OK ~~ <---------- This is good ----------> ~~ crypto map で正しくないピアが設定されている場合は、次のエラー メッセージを受け取ります。Mar 2 12:19:12.639: CRYPTO-SDU:Far end authentication error:

Connection message verify failed暗号アルゴリズムが一致しない場合は、次のエラー メッセージを受け取ります。Mar 2 12:26:51.091: CRYPTO-SDU: Connection failed due to incompatible policyDSS キーがない場合、または無効な場合は、次のエラー メッセージを受け取ります。Mar 16 13:33:15.703: CRYPTO-SDU:Far end authentication error:

Connection message verify failed

- **debug crypto key**次に示すのは、このコマンドの出力例です。StHelen#**debug crypto key** Mar 16 12:16:45.795: CRYPTO-KE: Sent 4 bytes. Mar 16 12:16:45.795: CRYPTO-KE: Sent 2 bytes. Mar 16 12:16:45.799: CRYPTO-KE: Sent 6 bytes. Mar 16 12:16:45.799: CRYPTO-KE: Sent 2 bytes. Mar 16 12:16:45.803: CRYPTO-KE: Sent 64 bytes. Mar 16 12:16:56.083: CRYPTO-KE: Received 4 bytes. Mar 16 12:16:56.087: CRYPTO-KE: Received 2 bytes. Mar 16 12:16:56.087: CRYPTO-KE: Received 4 bytes. Mar 16 12:16:56.091: CRYPTO-KE: Received 2 bytes. Mar 16 12:16:56.091: CRYPTO-KE: Received 52 bytes. Mar 16 12:16:56.095: CRYPTO-KE: Received 12 bytes.
- **clear crypto connection**次に示すのは、このコマンドの出力例です。wan-2511#**show crypto engine connections act** ID Interface IP-Address State Algorithm Encrypt Decrypt 9 Serial0 20.20.20.21 set DES_56_CFB64 29 28 wan-2511#**clear crypto connection 9** wan-2511# *Mar 5 04:58:20.690: CRYPTO: Replacing 9 in crypto maps with 0 (slot 0) *Mar 5 04:58:20.694: Crypto engine 0: delete connection 9 *Mar 5 04:58:20.694: CRYPTO: Crypto Engine clear conn_id 9 slot 0: OK wan-2511# wan-2511#**show crypto engine connections act** ID Interface IP-Address State Algorithm Encrypt Decrypt wan-2511#

- **crypto zeroize**次に示すのは、このコマンドの出力例です。wan-2511#**show crypto mypubkey** crypto public-key wan2511 01496536 11F43C02 70C0ADB7 5DD50600 A0219E04 C867A5AF C40A4FE5 CE99CCAB A8ECA840 EB95FBEE D727ED5B F0A6F042 BDB5529B DBB0698D DB0B2756 F6CABE8F 05E4B27F quit wan-2511#**configure terminal** Enter configuration commands, one per line. End with CNTL/Z. wan-2511(config)#crypto zeroize Warning! Zeroize will remove your DSS signature keys. Do you want to continue? [yes/no]: **yes** % Keys to be removed are named wan2511. Do you really want to remove these keys? [yes/no]: **yes** % Zeroize done. wan-2511(config)#**^Z** wan-2511# wan-2511#show crypto mypubkey wan-2511#
- **no crypto public-key**次に示すのは、このコマンドの出力例です。wan-2511#**show crypto pubkey** crypto public-key wan2516 01698232 B1C127B0 78D79CAA 67ECAD80 03D354B1 9012C80E 0C1266BE 25AEDE60 37A192A2 B066D299 77174D48 7FBAB5FC 2B60893A 37E5CB7B 62F6D902 9495733B 98046962 quit wan-2511#**configure terminal** Enter configuration commands, one per line. End with CNTL/Z. wan-2511(config)#**crypto public-key ?** WORD Peer name wan-2511(config)# wan-2511(config)#**no crypto public-key wan2516 01698232** wan-2511(config)#**^Z** wan-2511# wan-2511#**show crypto pubkey** wan-2511#

ESA を使用する Cisco 7200 のトラブルシューティング

Cisco 7200 シリーズ ルータで暗号化を行うために、ESA と呼ばれるハードウェア支援オプションが提供されています。 ESA は、VIP2-40 カード用のポート アダプタ、または Cisco 7200 用のスタンドアロン ポート アダプタの形態になっています。 このアレンジにより、ハードウェア アダプタまたは VIP2 ソフトウェア エンジンのいずれかを使用して、Cisco 7500 VIP2 カードのインターフェイスを通して送受信されるデータの暗号化と復号化を行うことができます。 Cisco 7200 では、Cisco 7200 シャーシの任意のインターフェイスでのトラフィックの暗号化をハードウェアで支援できます。 暗号化支援機能を使用することで、貴重な CPU サイクルを節約して、ルーティングや Cisco IOS の他の機能などのために使用できます。

Cisco 7200 では、スタンドアロン ポート アダプタは、Cisco IOS ソフトウェア暗号化エンジンとまったく同じように設定されます。ただし、ハードウェア用、および暗号化を行うエンジン（ソフトウェアまたはハードウェア）を決定するためにだけ使用される追加コマンドがいくつかあります。

まず次のように、ルータをハードウェア暗号化用に準備します。

```
wan-7206a(config)#
%OIR-6-REMCARD: Card removed from slot 3, interfaces disabled
*Mar  2 08:17:16.739: ...switching to SW crypto engine
```

wan-7206a#**show crypto card 3** Crypto card in slot: 3 Tampered: No Xtracted: Yes Password set: Yes DSS Key set: Yes FW version 0x5049702 wan-7206a# wan-7206a(config)# wan-7206a(config)#**crypto zeroize 3** Warning! Zeroize will remove your DSS signature keys. Do you want to continue? [yes/no]: **yes** % Keys to be removed are named hard. Do you really want to remove these keys? [yes/no]: **yes** [OK]

次に示すようにして、ハードウェア暗号化を有効または無効にします。

wan-7206a(config)#**crypto esa shutdown 3** ...switching to SW crypto engine wan-7206a(config)#**crypto esa enable 3** There are no keys on the ESA in slot 3- ESA not enabled.

次に、ESA を有効にする前に、ESA 用のキーを生成します。

wan-7206a(config)#**crypto gen-signature-keys hard** % Initialize the crypto card password. You will need this password in order to generate new signature keys or clear the crypto card extraction latch. Password: Re-enter password: Generating DSS keys .... [OK] wan-7206a(config)# wan-7206a#**show crypto mypubkey** crypto public-key hard 00000052 EE691A1F BD013874 5BA26DC4 91F17595 C8C06F4E F7F736F1 AD0CACEC 74AB8905 DF426171 29257F8E B26D49B3 A8E11FB0 A3501B13 D3F19623 DCCE7322 3D97B804 quit wan-7206a# wan-7206a(config)#**crypto esa enable 3** ...switching to HW crypto engine wan-7206a#**show crypto engine brie** crypto engine name: hard crypto engine type: ESA serial number: 00000052 crypto engine state: installed crypto firmware version: 5049702 crypto engine in slot: 3 wan-7206a#

ESA を使用する VIP2 のトラブルシューティング

VIP2 カードの ESA ハードウェア ポート アダプタは、VIP2 カードのインターフェイスを通して送受信されるデータを暗号化および復号化するために使用されます。 Cisco 7200 の場合と同様に、暗号化支援機能を使用することで、貴重な CPU サイクルを節約できます。 この場合、ESA が装着されていると、ESA ポート アダプタが VIP2 カードのポートに対する暗号化を行うので、crypto esa enable コマンドはありません。 ESA ポート アダプタを初めて取り付けた場合、または外してから取り付け直した場合は、crypto clear-latch をそのスロットに適用する必要があります。

Router#show crypto card 11 Crypto card in slot: 11 Tampered: No Xtracted: Yes Password set: Yes DSS Key set: Yes FW version 0x5049702 Router#

ESA 暗号モジュールを取り外したので、そのスロットに対して crypto clear-latch コマンドを実行するまでは、次のエラー メッセージが表示されます。

```
----
*Jan 24 02:57:09.583: CRYPTO: Sign done. Status= Extraction latch set. Request not allowed.
-----
```

Router(config)#**crypto clear-latch ?** <0-15> Chassis slot number Router(config)#**crypto clear-latch 11** % Enter the crypto card password. Password: Router(config)#**^Z**

以前に割り当てたパスワードを忘れた場合は、crypto clear-latch コマンドの代わりに crypto zeroize コマンドを使用して、ESA をリセットします。 crypto zeroize コマンドを発行した後は、DSS キーを生成し直して再度交換する必要があります。 DSS キーを再生成するときは、新しいパスワードを作成するように要求されます。 次に例を示します。

Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#**show crypto card 11** Crypto card in slot: 11 Tampered: No Xtracted: No Password set: Yes DSS Key set: Yes FW version 0x5049702 Router# ---------- - Router#**show crypto engine brief** crypto engine name: TERT crypto engine type: software serial number: 0459FC8C crypto engine state: dss key generated crypto lib version: 5.0.0 crypto engine in slot: 6 crypto engine name: WAAA crypto engine type: ESA serial number: 00000078 crypto engine state: dss key generated crypto firmware version: 5049702 crypto engine in slot: 11 Router# ---------- Router(config)#**crypto zeroize** Warning! Zeroize will remove your DSS signature keys. Do you want to continue? [yes/no]: **yes** % Keys to be removed are named TERT. Do you really want to remove these keys? [yes/no]: **yes** % Zeroize done. Router(config)#crypto zeroize 11 Warning! Zeroize will remove your DSS signature keys. Do you want to continue? [yes/no]: **yes** % Keys to be removed are named WAAA. Do you really want to remove these keys? [yes/no]: **yes** [OK] Router(config)#**^Z** Router#**show crypto engine brief** crypto engine name: unknown crypto engine type: software serial number: 0459FC8C crypto engine state: installed crypto lib version: 5.0.0 crypto engine in slot: 6 crypto engine name: unknown crypto engine type: ESA serial number: 00000078 crypto engine state: installed crypto firmware version: 5049702 crypto engine in slot: 11 Router# ---------- Router(config)#**crypto gen-signature-keys VIPESA 11** % Initialize the crypto card password. You will need this password in order to generate new signature keys or clear the crypto card extraction latch. Password: Re-enter password: Generating DSS keys .... [OK] Router(config)# *Jan 24 01:39:52.923: Crypto engine 11: create key pairs. ^Z Router# ------ Router#**show crypto engine brief** crypto engine name: unknown crypto engine type: software serial number: 0459FC8C crypto engine state: installed crypto lib version: 5.0.0 crypto engine in slot: 6 crypto engine name: VIPESA crypto engine type: ESA serial number: 00000078 crypto engine state: dss key generated crypto firmware version: 5049702 crypto engine in slot: 11 Router# ---------- Router#**show crypto engine connections active 11** ID Interface IP-Address State Algorithm Encrypt Decrypt 2 Serial11/0/0 20.20.20.21 set DES_56_CFB64 9996 9996 Router# Router#**clear crypto connection 2 11** Router# *Jan 24 01:41:04.611: CRYPTO: Replacing 2 in crypto maps with 0 (slot 11) *Jan 24 01:41:04.611: Crypto engine 11: delete connection 2 *Jan 24 01:41:04.611: CRYPTO: Crypto Engine clear conn_id 2 slot 11: OK Router#**show crypto engine connections active 11** No connections. Router# *Jan 24 01:41:29.355: CRYPTO ENGINE:Number of connection entries received from VIP 0 ---------- Router#**show crypto mypub** % Key for slot 11: crypto public-key VIPESA 00000078 CF33BA60 56FCEE01 2D4E32A2 5D7ADE70 6AF361EE 2964F3ED A7CE08BD

```
A87BF7FE 90A39F1C DF96143A 9B7B9C78 5F59445C 27860F1E 4CD92B6C FBC4CBCC 32D64508 quit
Router#show crypto pub crypto public-key wan2516 01698232 C5DE8C46 8A69932C 70C92A2C 729449B3
FD10AC4D 1773A997 7F6BA37D 61997AC3 DBEDBEA7 51BF3ADD 2BB35CB5 B9126B4D 13ACF93E 0DF0CD22
CFAAC1A8 9CE82985 quit Router# ---------- interface Serial11/0/0 ip address 20.20.20.21
255.255.255.0 encapsulation ppp ip route-cache distributed no fair-queue no cdp enable crypto
map test ! ---------- Router#show crypto eng conn act 11 ID Interface IP-Address State Algorithm
Encrypt Decrypt 3 Serial11/0/0 20.20.20.21 set DES_56_CFB64 761 760 Router# *Jan 24
01:50:43.555: CRYPTO ENGINE:Number of connection entries received from VIP 1 Router#
```

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： IPSec と ISAKMP - 第 2 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