Secure Socket Layer の実装

このモジュールでは、SSL の実装方法について説明します。

Secure Socket Layer（SSL）プロトコルと Transport Layer Security（TLS）は、相互認証、整合性を目的としたハッシュの使用、プライバシーを目的とした暗号化を許可することで、クライアントとサーバとの間のセキュアな通信を提供するアプリケーションレベルのプロトコルです。 SSL および TLS は証明書、公開キー、および秘密キーを使用します。

証明書はデジタル ID カードに似ています。 この証明書は、クライアントに対してサーバの ID を証明します。 VeriSign や Thawte などの認証局（CA）が証明書を発行します。 各証明書には、発行した機関の名前、証明書の発行先エンティティの名前、エンティティの公開キー、および証明書の有効期限を示すタイムスタンプが含まれます。

公開キーおよび秘密キーは、情報の暗号化および復号化に使用される暗号キーです。 公開キーは非常に簡単に共有されますが、秘密キーは公開されることはありません。 公開キーと秘密キーの各キー ペアは連携して動作します。公開キーで暗号化されたデータは秘密キーでのみ復号化できます。

（注） このモジュールで使用されている公開キーインフラストラクチャ（PKI）の詳細については、『*Cisco ASR 9000 Series Aggregation Services Router System Security Command Reference*』の「*Public Key Infrastructure Commands on* Cisco ASR 9000 Series Router」モジュールを参照してください。このモジュールの他のコマンドに関するマニュアルについては、コマンド リファレンス マスター インデックスを使用するか、オンラインで検索します。

Secure Socket Layer の実装の機能履歴

リリース	変更点
リリース 3.7.2	この機能を追加しました。

Secure Socket Layer の実装に関する前提条件

SSL を実装するには、次の前提条件を満たす必要があります。

- 適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 このコマンド リファレンスには、各コマンドに必要なタスク ID が含まれます。 ユーザ グループの割り当てが原因でコマンドを使用できないと考えられる場合、AAA 管理者に連絡してください。
- セキュリティ ソフトウェアのパッケージインストレーション エンベロープ（PIE）をインストールしてアクティブにする必要があります。

  オプションの PIE インストールの詳細については、『*Cisco ASR 9000 Series Aggregation Services Router Getting Started Guide*』を参照してください。
- SSL の使用を開始する前に、Rivest, Shamir, and Adelman（RSA）またはデジタル署名アルゴリズム（DSA）キー ペアを生成し、CA に登録して、ルータ キーの CA 証明書を取得する必要があります。
- SSL サーバは Advanced Encryption Standard（AES）をサポートしています。AES のキー サイズには 128 ビット、192 ビット、および 256 ビットがあります。

  これらの作業の実行に必要なコマンドの詳細については、『*Cisco ASR 9000 Series Aggregation Services Router System Security Command Reference*』の「*Public Key Infrastructure Commands on* Cisco ASR 9000 シリーズ ルータ」モジュールの **crypto key generate rsa** コマンド、**crypto key generate dsa** コマンド、**crypto ca enroll** コマンド、および **crypto ca authenticate** コマンドを参照してください。

Secure Socket Layer の実装について

SSL を実装するには、次の概念を理解しておく必要があります。

認証局の目的

認証局（CA）は、証明書要求を管理し、関係する IPSec ネットワーク デバイスへの証明書を発行します。 これらのサービスは、参加デバイスのキー管理を一元化して行います。

CA は、IPSec ネットワーク デバイスの管理を簡素化します。 CA は、ルータなど、複数の IPSec 対応デバイスを含むネットワークで使用できます。

Public Key Cryptography によりイネーブルにされたデジタル署名は、デバイスおよび個人ユーザをデジタル認証します。 RSA 暗号化システムなどの Public Key Cryptography では、各ユーザは、公開キーと秘密キーの両方を含むキーペアを使用します。 これらのキーは、補足として機能し、一方で暗号化されたものは、もう一方で復号化できます。 つまり、シグニチャは、データがユーザの秘密キーで暗号化されるときに形成されます。 受信側は、送信側の公開キーを使用してメッセージを復号化することで、シグニチャを検証します。 メッセージは、送信側の公開キーを使用して復号化できるため、秘密キーの所有者、つまり送信者がメッセージを作成することになります。 このプロセスは、受信者が送信者の公開キーのコピーを持っていて、これが本当に送信者のものであり、送信者を騙る他人のものではないことを高い確実性を持って知っていることを基盤としています。

デジタル証明書はリンクを提供します。 デジタル証明書には、名前、シリアル番号、企業、部署またはIPアドレスなど、ユーザまたはデバイスを特定する情報を含んでいます。 また、エンティティの公開キーのコピーも含んでいます。 証明書自体は、受信者が身元を証明し、デジタル証明書を作成するうえで確実に信頼できるサード パーティである、CA により署名されます。

CA のシグニチャを検証するには、受信者は、CA の公開キーを認識している必要があります。 通常、このプロセスは、アウトオブバンドで、またはインストールで行われる操作により処理されます。 たとえば、通常の Web ブラウザでは、デフォルトで、複数の CA の公開キーが設定されています。 IPSec の基本コンポーネントであるインターネット キー交換（IKE）は、デジタル シグニチャを使用して、セキュリティ アソシエーション（SA）を設定する前にピア デバイスをスケーラブルに認証できます。

デジタル シグニチャがない場合、ユーザは、IPSec を使用するデバイスの各ペア間で公開キーまたはシークレットを手動で交換して、通信を保護する必要があります。 証明書がない場合、ネットワークに新しいデバイスが追加されるたびに、安全に通信を行う他のすべてのデバイスで設定を変更する必要があります。 デジタル証明書がある場合、各デバイスは、CA に登録されます。 2 台のデバイスが通信する場合、証明書を交換し、データをデジタル署名して、お互いを認証します。 新しいデバイスがネットワークに追加されると、ユーザは、そのデバイスを CA に登録します。他のデバイスでは変更の必要はありません。 新しいデバイスが IPSec 接続を試行すると、証明書が自動的に交換され、デバイスを認証できます。

Secure Socket Layer の実装方法

HTTP サーバやオブジェクト リクエスト ブローカ（ORB）サーバなど、任意のアプリケーションで SSL を使用できるように設定するには、次の項で説明されている作業を実行します。

Secure Socket Layer の設定

ここでは、SSL の設定方法について説明します。

手順の概要

1. **crypto key generate rsa** [**usage-keys** | **general-keys**] [*keypair-label*]
2. configure
3. **domain ipv4 hos t** *host-name v4address1* [*v4address2...v4address8*] [**unicast** | **multicast**]
4. **crypto ca trustpoint** *ca-name*
5. **enrollment url CA-URL**
6. 次のいずれかのコマンドを使用します。
   - **end**
   - **commit**
7. RP/0/RSP0/CPU0:router**crypto ca authenticate** *ca-name*
8. **crypto ca enroll** *ca-name*
9. show crypto ca certificates

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**crypto key generate rsa** [**usage-keys** | **general-keys**] [*keypair-label*]
	
	例：
	`RP/0/RSP0/CPU0:router# crypto key generate rsa general-keys`
	`The name for the keys will be: the_default`
	`% You already have keys defined for the_default`
	`Do you really want to replace them? [yes/no]:`
		RSA キー ペアを生成します。
		• RSA キーペアはインターネット キー交換（IKE）キー管理メッセージの署名および暗号化に使用されます。また、ルータの証明書を取得する際に必要です。
		• **usage-keys** キーワードを使用して、特定目的のキーを指定します。**general-keys** キーワードを使用して、汎用 RSA キーを指定します。
		• *keypair-label* 引数は、RSA キー ペアを指定する RSA キー ペア ラベルです。
		• DSA キーペアを生成するには、EXEC モードで **crypto key generate dsa** コマンドを使用します。

ステップ 2	configure 例： `RP/0/RSP0/CPU0:router# configure`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**domain ipv4 hos t** *host-name v4address1* [*v4address2...v4address8*] [**unicast** | **multicast**] 例： `RP/0/RSP0/CPU0:router(config)# domain ipv4 host ultra5 192.168.7.18`	ホスト名とアドレスのスタティック マッピングを IPv4 を使用してホスト キャッシュに定義します。

	コマンドまたはアクション	目的
ステップ 4	**crypto ca trustpoint** *ca-name* 例： `RP/0/RSP0/CPU0:router(config)# crypto ca trustpoint myca`	ルータがピアに対して発行された証明書を確認できるように、選択した名前で信頼できるポイントを設定します。 • トラストポイント コンフィギュレーション モードを開始します。
ステップ 5	**enrollment url CA-URL** 例： `RP/0/RSP0/CPU0:router(config-trustp)# enrollment url http://ca.domain.com/certsrv/mscep/mscep.dll`	CA の URL を指定します。 • URL には、非標準 cgi-bin スクリプトの場所が含まれている必要があります。

ステップ 6	次のいずれかのコマンドを使用します。
	• **end**
	• **commit**
	
	例：
	`RP/0/RSP0/CPU0:router(config)# end`
	または
	`RP/0/RSP0/CPU0:router(config)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		◦ yes と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		◦ no と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		◦ cancel と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。
		• 実行コンフィギュレーション ファイルに設定変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

ステップ 7	RP/0/RSP0/CPU0:router**crypto ca authenticate** *ca-name* 例： `RP/0/RSP0/CPU0:router# crypto ca authenticate myca`	このコマンドは、CA の公開キーを含む CA 証明書を取得することで、ルータに対して CA を認証します。 • 確認の画面が表示されたら、「**y**」を入力して証明書を承認します。

	コマンドまたはアクション	目的
ステップ 8	**crypto ca enroll** *ca-name* 例： `RP/0/RSP0/CPU0:router# crypto ca enroll myca`	すべての RSA キー ペアの証明書を要求します。 • このコマンドでは、ルータは存在する RSA キー ペアと同数の証明書を要求するため、特定目的の RSA キー ペアがある場合にも、このコマンドは 1 回しか実行する必要はありません。 • このコマンドでは、設定に保存されないチャレンジ パスワードを作成する必要があります。 証明書を失効させる必要が生じた場合、このパスワードが要求されるので、このパスワードを覚えておく必要があります。 • 証明書はすぐに発行できます。または、登録リトライ時間に達し、タイムアウトが発生するまで、ルータが証明書要求を毎分送信します。 タイムアウトが発生した場合、システム管理者に要求承認を依頼して、このコマンドを再入力します。 • **show crypto ca certificates** コマンドを使用して、証明書が許可されていることを確認します。
ステップ 9	show crypto ca certificates 例： `RP/0/RSP0/CPU0:router# show crypto ca certificates`	証明書と CA 証明書に関する情報を表示します。

Secure Socket Layer の実装の設定例

この項では、次の設定例について説明します。

Secure Socket Layer の設定：例

次に、ルータの RSA キーの生成、トラストポイントの設定、CA サーバの認証、キーに対する CA からの証明書の取得、および証明書に関する情報の表示の例を示します。

```
crypto key generate rsa general-keys commit configure domain ipv4 host
           xyz-ultra5 10.0.0.5 crypto ca trustpoint myca enrollment url http://xyz-ultra5
end
           crypto ca authenticate myca crypto ca enroll myca show crypto ca certificates
```

参考資料

ここでは、SSL の実装に関する関連資料について説明します。

関連資料

関連項目	ドキュメント名
PKI コマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト設定、使用上のガイドライン、および例	『*Cisco ASR 9000 Series Aggregation Services Router System Security Command Reference*』の「*Public Key Infrastructure Commands on Cisco ASR 9000* シリーズ ルータ」モジュール
SSL コマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト設定、使用上のガイドライン、および例	『*Cisco ASR 9000 Series Aggregation Services Router System Security Command Reference*』の「*Secure Socket Layer Protocol Commands on* Cisco ASR 9000 シリーズ ルータ」モジュール

標準

標準	タイトル
この機能でサポートが追加または変更された標準はありません。また、この機能で変更された既存の標準のサポートはありません。	—

MIB

MIB	MIB リンク
—	Cisco IOS XR ソフトウェアを使用して MIB を検出およびダウンロードするには、URL（http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml）にある Cisco MIB Locator を使用して、[Cisco Access Products] メニューでプラットフォームを選択します。

RFC

RFC	タイトル
RFC 2246	『The TLS Protocol, Version 1』、T. Dierks, C. Allen. 1999 年 1 月。

シスコのテクニカル サポート

説明	リンク
シスコのテクニカル サポート Web サイトには、数千ページに及ぶ検索可能な技術情報があります。製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクもあります。 Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html