PKI配置

目 录

第 1 章 配置PKI 1
1.1 概述 1
1.1.1 PKI概要 1
1.1.2 支持的标准 1
1.1.3 术语 1
1.2 PKI配置任务列表 1
1.3 PKI配置任务 2
1.3.1 创建RSA密钥对 2
1.3.2 创建PKI信任点 2
1.3.3 配置CA证书 3
1.3.4 配置本地证书 3
1.4 基于证书认证的IKE配置 3
1.4.1 配置本地证书 3
1.4.2 创建IKE策略 4
1.4.3 基于证书认证的IPSec配置示例 4

第1章　配置PKI

1.1　概述

本章讨论如何配置 PKI。PKI 是一个用公开密钥原理和技术来实现并提供安全服务的具有通用性的安全基础设施。通过 PKI，可实现通信实体之间的身份认证以及通信数据的安全性。在路由器上，PKI 可用于实现基于证书认证的 IKE 协议。

1.1.1　PKI概要

PKI 是一组服务和策略，提供了将公钥和用户身份绑定的机制，以及如何实施并维护这个绑定相关信息的框架。通过使用公开密钥技术和数字证书来确保系统信息安全，并负责验证数字证书持有者身份。

PKI 的主要功能是通过签发数字证书来绑定证书持有者的身份和相关的公开密钥；用户可以获取证书、访问证书以及撤销证书；通过利用数字证书及相关的各种服务实现通信过程中各实体的身份认证，保证了通信数据的完整性和不可否认性。

1.1.2　支持的标准

路由器实现了下列标准：

RSA——Ron Rivest, Adi Shamir, Leonard Adleman 非对称加密算法。

PKIX——Public-Key Infrastructure (X.509)。

1.1.3　术语

CA——认证机构。用于签发证书和认证证书。

DN——识别名。采用 X.500 标准，以一系列“属性=值”对构成，各个“属性=值”对之间使用逗号分隔。

1.2　PKI配置任务列表

要配置 PKI，执行下面各节的任务。

(1) 创建 RSA 密钥对

(2) 创建 PKI 信任点

(3) 配置信任点 CA 证书

(4) 配置信任点本地证书

1.3 PKI配置任务

要配置 PKI，需要有参与 PKI 的 RSA 密钥对、用于签发和认证数字证书的 CA 以及与密钥对绑定的本地数字证书。

1.3.1 创建RSA密钥对

要配置一对 RSA 密钥对，在全局配置模式下使用下面的命令：

命令	目的
crypto key generate [rsa] [general-keys | encryption | signature] [exportable] [label *NAME***] [modulus** *NUMBER***]**	创建一对 RSA 密钥对，并制定该密钥对的以下属性：生成密钥长度、密钥对名称以及是否可导出。支持的密钥长度有 512、1024 以及 2048。密钥长度越长，安全性越高，计算开销越大。

如果在命令中不指定参数，则使用缺省值：密钥对名称的缺省值为当前路由器主机名称；密钥对缺省不可导出；密钥缺省长度为 512bit。

1.3.2 创建PKI信任点

要配置一个 PKI 信任点，在全局配置模式下使用下面的命令：

命令	目的
crypto pki trustpoint *NAME*	创建名为 *NAME* 的信任点。
subject-name *NAME*	指定在该信任点下所使用的主题名。主题名是与该信任点所绑定的 RSA 密钥对的身份标识信息，采用 DN 格式。

rsakeypair *NAME*	（可选）指定与该信任点绑定的本地 RSA 密钥对。缺省将使用与当前路由器主机名同名的密钥对。
fqdn *NAME*	（可选）指定该信任点下所使用的替代主题名域名。
Exit	退出信任点配置态。

1.3.3 配置CA证书

要配置某一信任点的 CA 证书，在全局配置态下使用下面的命令：

命令	目的
crypto pki authencate *NAME* **pem {terminal | flash** *FILE* **| http** *URL***}**	为信任点 *NAME* 导入 CA 证书。指定的 CA 证书须为 PEM 格式。

1.3.4 配置本地证书

要配置某一信任点的本地证书，在全局配置态下使用下面的命令：

命令	目的
crypto pki enroll *NAME* **pem {terminal | flash** *FILE* **| http** *URL***}**	为信任点 *NAME* 生成本地证书申请。生成的证书申请为 PEM 格式。
crypto pki import *NAME* **certificate pem {terminal | flash** *FILE* **| http** *URL***}**	为信任点 *NAME* 导入本地证书。指定的本地证书须为 PEM 格式。

1.4 基于证书认证的IKE配置

1.4.1 配置本地证书

通过 PKI 配置任务中为路由器生成 RSA 密钥对以及相应的本地数字证书。

1.4.2 创建IKE策略

为路由器配置验证方法是 RSA 签名的 IKE 策略。关于 IKE 策略的详细配置，请参见 IKE 配置。

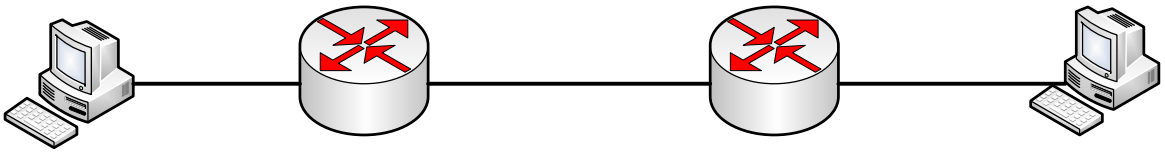
在全局配置模式下使用下面的命令：

命令	目的
crypto isakmp policy *priority*	创建 IKE 策略。
encryption {des | 3des | aes128 | aes192 | aes256}	指定加密算法。
hash {sha | md5}	指定哈希算法。
authentication rsa-sig	指定验证方法为 RSA 签名。
group {1 | 2 | 5}	指定 Diffie-Hellman 组。
lifetime *seconds*	指定 IKE 安全联盟的生命周期。
exit	退出 IKE 策略配置态。

1.4.3 基于证书认证的IPSec配置示例

下面是使用基于证书认证 IKE 协商安全联盟的 IPSec 的配置示例。

关于 IKE 配置以及 IPSec 配置说明，请参见相关文档。



1. **寻找共同的 CA（带外方式）**
2. **创建用于 IKE 验证的 RSA 密钥对**

   crypto key generate rsa general-keys label ike-r1 module 1024

3. 创建 **PKI** 信任点，并绑定密钥对

crypto pki trustpoint r1

rsakeypair ike-r1

subject-name C=CN,O=ORGANIZE,OU=UNIT,CN=R1

4. 配置 **CA** 证书并生成本地证书请求

crypto pki authenticate r1 pem terminal

crypto pki enroll r1 pem terminal

5. 生成本地证书后，配置本地证书

crypto pki import r1 certificate pem terminal

6. 创建 **IKE** 策略

crypto isakmp policy 10

encryption des

hash md5

authentication rsa-sig

group 2

lifetime 5000

7. 定义加密访问列表

ip access-list extended aaa

permit ip 130.130.0.0 255.255.0.0 131.131.0. 0 255.255.0.0

8. 定义变换集合

crypto ipsec transform-set one esp-des esp-sha-hmac

9. 加密映射表设置 **IPSec** 访问列表和变换集合，并指定加密报文发往何处（**IPSec** 对端）

crypto map toShanghai 100 ipsec-isakmp

match address aaa

set transform-set one

set peer 192.2.2.1

10. 将加密映射表作用于接口

interface g0/1

ip address 192.2.2.2

crypto map toShanghai