

安全配置

目 录

第 1 章 AAA配置.....	1
1.1 AAA概述.....	1
1.1.1 AAA安全服务.....	1
1.1.2 使用AAA的优点.....	2
1.1.3 AAA基本原理.....	2
1.1.4 AAA认证方法列表.....	2
1.2 AAA配置过程.....	4
1.2.1 AAA配置过程概览.....	4
1.2.2 配置任务相关文档.....	4
1.3 AAA认证配置任务列表.....	4
1.4 AAA认证配置任务.....	5
1.4.1 使用AAA配置登录认证.....	5
1.4.2 使用AAA进行PPP认证.....	7
1.4.3 在进入特权级别时开启口令保护.....	8
1.4.4 改变提示输入口令时的字符串.....	9
1.4.5 建立本地认证数据库.....	9
1.4.6 建立本地用户组数据库.....	10
第 2 章 IPsec配置.....	11
2.1 IPsec概述.....	11
2.1.1 支持的标准.....	11
2.1.2 术语.....	12
2.1.3 限制.....	12
2.1.4 IPsec工作过程概述.....	12
2.1.5 IPsec嵌套.....	13
2.2 IPsec配置任务列表.....	14
2.3 IPsec配置任务.....	14
2.3.1 确保访问列表和IPsec相兼容.....	14
2.3.2 创建加密访问列表.....	14
2.3.3 加密访问列表技巧.....	15
2.3.4 在加密访问列表中使用any关键字.....	15
2.3.5 定义变换集合.....	16
2.3.6 创建加密映射表.....	16
2.3.7 应该建立多少个加密映射表.....	17
2.3.8 创建手工方式的加密映射表.....	18
2.3.9 创建使用IKE的加密映射表.....	19
2.3.10 将加密映射表集合应用于接口.....	19
2.4 IPsec配置示例.....	19

第 3 章 配置Internet密钥交换安全协议	21
3.1 概述.....	21
3.1.1 IKE概要.....	21
3.1.2 支持的标准	21
3.1.3 术语	22
3.2 IKE配置任务列表	22
3.3 IKE配置任务	22
3.3.1 确保访问列表与IKE兼容.....	22
3.3.2 创建IKE策略.....	22
3.3.3 配置预共享密钥	25
3.3.4 清除IKE连接（可选）	25
3.3.5 IKE诊断（可选）	25
3.4 IKE配置示例	26

第1章 AAA配置

1.1 AAA概述

访问控制是用来控制接入路由器或网络访问服务器（NAS）的用户，并限制他们可使用的服务种类。提供认证、授权和记录（Authentication, Authorization, Accounting）功能，以提高网络安全性能。

1.1.1 AAA安全服务

AAA 是使用相同方式配置三种独立的安全功能的一种体系结构。它提供了完成下列服务的模块化方法：

- 认证（Authentication）——提供一种识别用户的方法，包括用户名和口令的询问，以及根据所选择的安全协议进行加密。

认证是接受用户访问请求和提供网络服务之前识别他们身份的方法。通过定义一张命名的认证方法列表来对 AAA 认证进行配置，然后应用该列表于各种接口。方法列表定义了所执行的认证的类型和它们执行的次序；任何定义的认证方法执行之前都必须应用在具体的接口上。唯一的例外是缺省方法列表（其名称为 **default**）。如果没有定义其它方法列表，缺省方法列表自动应用于所有接口。定义任何方法列表将覆盖缺省方法列表。有关所有认证的配置方法的详细资料，请参见“认证配置”。

- 授权（Authorization）——提供一种远程访问控制的方法，用于限制用户的服务权限。

AAA 授权通过相对于该用户的一组属性来发挥作用，这些属性描述了用户被授予哪些权限。将这些属性与包括在数据库中某个特定用户的信息相比较，结果返回给 AAA，以确定该用户的实际权限。这个数据库可以位于所访问的本地服务器或路由器，或者位于远程 RADIUS 或 TACACS+ 安全服务器。像 RADIUS 和 TACACS+ 这样的远程安全服务器，通过与用户相联系的属性值（AV）对（Attribute-Value Pairs）来完成对用户的授权，属性值（AV）对定义了允许授予的权限。所有的授权方法必须通过 AAA 定义。与认证一样，首先要定义一个授权方法列表，然后在各种接口中应用该列表。有关使用 AAA 进行授权配置的详细情况，请参见“授权配置”。

- 记录（Accounting）——提供一种收集用户服务信息，并发送给安全服务器的方法，这些信息可用于开列帐单、审计和形成报表，如用户标识、开始时间和停止时间、执行的命令、数据包的数量以及字节数。

记录功能不仅可以跟踪用户访问的服务，同时还可以跟踪他们消耗的网络资源数量。当激活 AAA 记录功能时，网络访问服务器以记录的形式向 TACACS+ 或 RADIUS 安全服务器报告用户的活动。每条记录包括记录属性值（AV）对，存储在安全服务器上。这些数据可用于网络管理、客户帐单或审计分析。与认证和授权一样，要先定义一个记录方法列表，然后在不同的接口中使用这张表。有关使用 AAA 进行记录配置的详细材料，请参见“记录配置”。

1.1.2 使用AAA的优点

AAA 提供了如下优点：

- 灵活性和易于控制
- 方便升级
- 标准化的认证方法，如 RADIUS、TACACS+
- 多重备用系统

1.1.3 AAA基本原理

AAA 用来动态配置基于每条线路（每个用户）或者每项服务（例如，IP、IPX 或 VPDN）的认证和授权类型。通过创建方法列表定义认证和授权的类型，然后把这些方法列表应用到具体服务或接口上。

1.1.4 AAA认证方法列表

要对认证进行配置，首先定义一个命名的认证方法列表，然后在不同的端口上应用这张列表。该方法列表定义了所要执行的认证类型，以及他们将被执行的次序；所定义的任何认证方法列表在被执行之前，必须应用于某一个具体的端口。唯一例外的是缺省方法列表（default）。缺省方法列表自动的应用于所有的接口。除非该端口明确引用了其他方法列表，这时此方法列表将替代缺省方法列表。

方法列表是认证用户时需要顺序查询的认证方法的表格。在方法列表中可以指派一个或多个安全协议。因此确保了万一最初的方法失败后有一个备用的认证系统。本公司路由器软件使用方法列表中的第一个认证方法鉴别用户；如果该方法没有反应，则会选择方法列表中的下一个认证方法。这一个过程一直进行下去，直至所列的某个方法成功的进行认证，或者所有的方法用完为止。

注意到这一点是很重要的，即本公司路由器软件仅仅在前面的方法没有反应时，才尝试使用列在后面的认证方法进行认证。如果认证在这个过程中的任何一点上失败了，即安全服务器或是本地用户数据库的反应是拒绝用户访问，则认证过程停止，并且不再尝试其他的认证方法。

下图显示了一个很有代表性的 AAA 网络配置，包含四个安全服务器，R1 和 R2 是 RADIUS 服务器，T1 和 T2 是 TACACS+ 服务器。

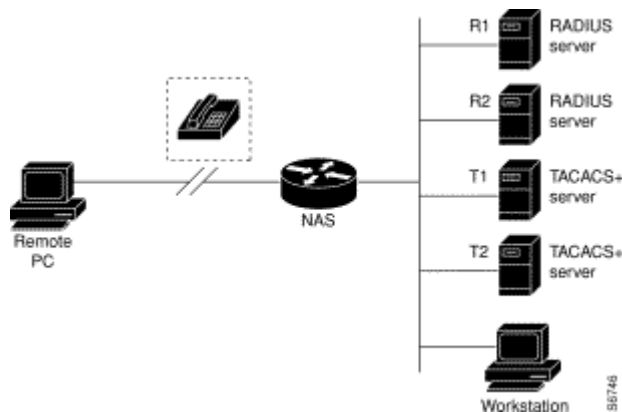


图 错误！未找到引用源。-1 AAA 网络配置示意图

假设系统管理员决定，在其安全方案中所有的接口使用同样的认证方法来认证基于 PPP 协议的连接：首先接通了 R1 来了解有关认证信息，如果 R1 没有反应，接通 R2，如果 R2 仍没有反应，接通 T1，如果 T1 也没有反应，接通 T2，如果所有指派的服务器都没有反应，认证工作就落在访问服务器本身的本地用户名数据库上。要实现这一点，系统管理员应该输入下面的命令,创建一张缺省的方法列表：`aaa authentication ppp default radius local`。

本例中，**default** 是方法列表的名称，包括在方法列表中的协议以及他们将被查询的次序列在方法列表名称后面。缺省列表自动的应用于所有的接口。

当远程用户试图通过拨号进入网络时，网络访问服务器首先在 R1 上查询有关的认证信息，如果鉴别该用户合法，他就发一条 **PASS** 应答给网络访问服务器，从而允许用户访问服务器。如果 R1 返回一条 **FAIL** 应答，则该用户被拒绝访问，本次对话结束。如果 R1 没有反应，网络访问服务器将其当成一次错误，并且在 R2 上查阅有关的认证信息。这种模式在剩下的方法中一直进行下去，直到该用户被接受或者被拒绝、或者本次对话结束为止。

记住这一条是很重要的，即 **FAIL** 应答与 **ERROR** 应答是截然不同的两个东西，**FAIL** 意味着用户没有满足包含在认证数据库中要认证成功所需的标准。认证以 **FAIL** 应答结束。**ERROR** 意味着该安全服务器对认证查询没有应答。仅仅当 AAA 检测到 **ERROR** 应答时，他才选择定义在认证方法链表中的下一个认证方法。

假设系统管理员想将方法列表仅仅应用于某个或某种特定的端口。在这种情况下，系统管理员应当创建一个非缺省的方法列表，然后把这个命名的列表应用到适当的端口上。下面的实例演示了系统管理员如何实现某个认证方法只应用异步端口的过程：

```
aaa authentication ppp default radius local
aaa authentication ppp async0 radius tacacs+ local none
interface async 0/0
ppp authentication chap async0
```

在这个例子中，**async0** 是方法列表的名称，包括在这个方法列表中的认证协议依次列在他的后面，他们将有可能被依次使用。创建好方法列表后，将列表应用到合适的端口上。注意，`aaa authentication` 命令中的方法名称必须与 `ppp authentication` 命令中的方法列表名称相匹配。

1.2 AAA配置过程

首先，必须决定想要实现何种类型的安全方案。用户需要评估自己网络中的安全风险，并且确定合适的方法来阻止未经授权的登录和攻击。

1.2.1 AAA配置过程概览

在明白了配置所涉及的基本过程后，配置 AAA 就相对简单了。在本公司路由器或访问服务器上使用 AAA 进行安全配置，遵循如下步骤：

- 如果决定使用安全服务器，则先配置安全协议参数，如 RADIUS，TACACS+。
- 使用命令 `aaa authentication` 定义用于认证的方法列表。
- 如果需要的话，把该方法列表应用到某个具体的接口或线路上。
- 使用命令 `aaa authorization` 进行授权配置（可选）。
- 使用命令 `aaa accounting` 进行记录配置（可选）。

1.2.2 配置任务相关文档

下表说明了 AAA 配置任务以及在何处查找更多的资料。

表 错误！未找到引用源。-1 任务与文档

进一步配置任务	参考资料
配置本地登录认证。	认证配置。
使用安全服务器控制登录认证。	认证配置。
定义用于认证的方法列表。	认证配置。
把方法列表应用到具体接口或线路上。	认证配置。
配置RADIUS协议参数。	配置RADIUS。
配置TACACS+协议参数。	配置TACACS+。

1.3 AAA认证配置任务列表

- 使用 AAA 配置登录认证
- 使用 AAA 进行 PPP 认证
- 在进入特权级别时开启口令保护
- 改变提示输入口令时的字符串
- 建立本地用户名认证数据库

1.4 AAA认证配置任务

AAA 认证的一般配置过程

要配置 AAA 认证，需要完成下列配置过程：

- (1) 如果使用的是安全服务器，配置安全协议参数，如 RADIUS、TACACS+。具体配置方法参见相应章节。
- (2) 使用 `aaa authentication` 命令定义认证方法列表。
- (3) 如果需要的话，把方法列表应用到特定的端口或是线路上。

1.4.1 使用AAA配置登录认证

AAA 安全服务使得使用各种认证方法变得更容易了，不论决定使用哪种登录方法，都使用 `aaa authentication` 命令开启 AAA 认证。在 `aaa authentication login` 命令中，创建一张或是多张认证方法的列表，这些列表在登录时使用。使用线路配置命令 `login authentication` 来应用这些列表。配置时，从全局配置模式开始，使用如下命令：

命令	目的
<code>aaa authentication login {default list-name} method1 [method2...]</code>	创建全局认证列表。
<code>line [aux console tty vty] line-number [ending-line-number]</code>	进入某个线路的配置状态。
<code>login authentication {default list-name}</code>	应用该认证列表于某条或是某几个线路上。

关键字 `list-name` 是用来命名所创建的列表的任何字符串。关键字 `method` 指定认证过程所采用的实际方法。仅当前面所用的方法返回认证错误时，才会使用其他的认证方法，如果前面的方法指明认证失败了，则不再使用其他的认证方法。如果要指定即使所有的方法都返回认证错误仍能成功登录，只要在命令行中指定 `none` 作为最后一个认证方法。例如：即使 TACACS+ 服务返回错误仍能认证成功，可用下面的命令行：

```
aaa authentication login default tacacs+ none
```

使用 `default` 参数可建立一个缺省的列表，缺省列表自动的应用于所有的接口。例如：指定 RADIUS 作为用户登录时的缺省认证方式，使用下面的命令：

```
aaa authentication login default radius
```

注意：

由于关键字 `none` 使得登录的任何用户都可成功的通过认证，所以应当将该关键字作为备用的认证方法。

下表列出了目前支持的登录认证方式：

关键字	说明
<code>enable</code>	使用 <code>enable</code> 口令进行认证。
<code>group</code>	使用服务器组进行认证。

group-restrict	使用服务器组进行认证，但当用户指定使用某台服务器后，此服务器组失效。
line	使用线路密码进行认证。
local	使用本地数据库进行认证。
localgroup	使用本地用户组数据库进行认证
local-case	使用本地用户名数据库进行认证(用户名区分大小写)。
none	认证无条件通过。
radius	使用 RADIUS 认证。
tacacs+	使用TACACS+ 认证

(1) 使用 enable 口令进行登录认证

在 `aaa authentication login` 命令中使用 `enable` 方法关键字指定 `enable` 口令作为登录认证方法，例如：在没有定义其他方法时，指定 `enable` 口令作为登录时用户认证的方法，使用下面的命令：

```
aaa authentication login default enable
```

(2) 使用线路口令进行登录认证

在使用 `aaa authentication login` 命令时，用 `line` 方法关键字指定线路口令作为登录时的认证方法。例如，在用户登录时指定线路口令为用户认证方法，并且不定义任何其他方法，可以输入下面的命令行：

```
aaa authentication login default line
```

在能够使用线路口令进行注册认证之前，需要定义一条线路口令。

(3) 使用本地口令进行登录认证

在使用 `aaa authentication login` 命令时，用 `local` 方法关键字指定使用本地用户名数据库作为登录认证方法。例如，在用户注册时指定本地用户名数据库为用户认证方法，并且不定义任何其他方法，可以输入下面的命令行：

```
aaa authentication login default local
```

有关增加用户到本地用户名数据库中的详细资料，参见“建立本地认证数据库”。

(4) 使用 RADIUS 进行登录认证

在使用 `aaa authentication login` 命令时，用 `radius` 方法关键字指定 `RADIUS` 作为登录认证方法。例如在用户登录时指定 `RADIUS` 为用户认证方法，并且不定义任何其他方法，可以输入下面的命令：

```
aaa authentication login default radius
```

在能使用 `RADIUS` 作为注册认证方法之前，需要首先配置 `RADIUS` 服务，有关的更多信息参见“配置 `RADIUS`”。

(5) 使用 TACACS+ 进行登录认证

在使用 `aaa authentication login` 命令时，使用 `TACACS+` 方法关键字指定 `TACACS+` 作为认证方法。例如，在用户登录时指定 `TACACS+` 认证方法，并且不定义任何其他方法，可以输入下面的命令：

```
aaa authentication login default tacacs+
```

在能够使用 `TACACS+` 进行认证方法之前，需要首先配置 `TACACS+` 服务，有关详细信息，参见“配置 `TACACS+`”。

1.4.2 使用AAA进行PPP认证

许多用户通过异步或是 ISDN 拨号访问网络中心服务器。AAA 安全服务使得在串口上大量运行 PPP 时的认证方法变得容易了。不管决定使用所支持的何种 PPP 认证方法，均可以使用 `aaa authentication ppp` 开启 AAA 认证。配置时，在全局配置模式下使用下面的命令：

命令	目的
<code>aaa authentication ppp {default list-name} method1 [method2...]</code>	创建本地认证列表。
<code>interface interface-type number</code>	进入端口配置模式，认证列表将应用于该端口上。
<code>ppp authentication {chap pap chap pap pap chap} {default list-name}</code>	将认证列表应用于某条或是某几条线路上。

使用 `aaa authentication` 命令，可以创建一张或是几张认证方法列表，在用户开始运行 PPP 时使用这些列表。使用 `ppp authentication` 配置命令来应用这些列表。要创建一张缺省列表，使用 `default` 参数，在其后紧跟缺省情况下想要使用的方法。例如，指定本地用户名数据库作为认证的缺省方法，输入下面的命令行：

```
aaa authentication ppp default local
```

关键字 `list-name` 是用来命名所建立的列表的任何字符串。关键字 `method` 指定认证过程所采用的实际方法。仅当前面的方法返回认证错误时，才会使用其他的认证方法。如果前面使用的方法返回认证失败，则不再使用其他的认证方法。如果指定即使所有的方法都返回错误仍能成功认证，只需在命令行中指定 `none` 作为最后一个认证方法。例如，下面例子中即使 TACACS+ 服务器返回错误，仍要保证认证成功，可以输入下面的命令行：

```
aaa authentication ppp default tacacs+ none
```

注意：

由于关键字 `none` 使得登录的任何用户都能成功的被认证，所以应当将该关键字作为备用的认证方法。

下表列出了 PPP 可使用的认证方式：

关键字	说明
<code>group</code>	使用服务器组进行认证。
<code>group-restrict</code>	使用服务器组进行认证，但当用户指定使用某台服务器后，此服务器组失效。
<code>local</code>	使用本地用户名数据库认证。
<code>localgroup</code>	使用本地用户组数据库进行认证
<code>local-case</code>	使用本地用户名数据库进行认证(用户名区分大小写)。
<code>none</code>	认证无条件通过。
<code>radius</code>	使用RADIUS 认证。
<code>tacacs+</code>	使用TACACS+ 认证。

(1) 使用本地口令进行 PPP 认证

在 **aaa authentication ppp** 命令中,用 **local** 关键字指定使用本地用户名数据库进行认证。例如,在运行 **PPP** 的线路上要指定本地用户名数据库为认证方法,并且不需要其他任何方法,可以输入下面的命令行:

```
aaa authentication ppp default local
```

有关更多的增加用户到本地用户名数据库的更多信息,参见“建立本地认证数据库”。

(2) 使用 RADIUS 进行 PPP 认证

在 **aaa authentication ppp** 命令中,用 **RADIUS** 关键字指定 **RADIUS** 作为运行 **PPP** 时的认证方法。例如,要指定 **RADIUS** 为用户认证的方法,并且不需要定义其他方法,可以输入下面的命令行:

```
aaa authentication ppp default radius
```

在使用 **RADIUS** 作为注册认证方法时,需要配置 **RADIUS** 服务,有关详细信息参见“配置 **RADIUS**”。

(3) 使用 TACACS+进行 PPP 认证

在 **aaa authentication ppp** 命令中,用 **TACACS+**关键字指定 **TACACS+**作为运行 **PPP** 的端口的认证方法。例如,要指定 **TACACS+**为用户认证的方法,并且不需要定义其他方法,可以输入下面的命令行:

```
aaa authentication ppp default tacacs+
```

在能够使用**TACACS+**作为**PPP**认证方法之前,需要首先配置**TACACS+**服务,有关详细信息参见“配置**TACACS+**”。

1.4.3 在进入特权级别时开启口令保护

使用 **aaa authentication enable default** 命令创建一个认证方法列表,这些方法决定了某个用户是否可以执行特权级别的 **EXEC** 命令。可以至多指定四种认证方法。仅当前面所用的方法返回认证错误时,才会使用其他的认证方法。如果前面使用的方法返回认证失败,则不再使用其他的认证方法,如果指定即使所有的方法都返回错误仍能成功认证,只需在命令中指定 **none** 作为最后一个认证方法。配置时,在全局配置模式下使用下面的命令:

命令	目的
aaa authentication enable default method1 [method2...]	在用户进入特权级别时开启口令认证。

关键字 **method** 指定认证过程使用的实际方法,在认证时依输入的次序使用。

下表列出了所支持的口令保护认证方法:

关键字	说明
enable	使用 enable 口令认证。
group	使用服务器组进行认证。
group-restrict	使用服务器组进行认证,但当用户指定使用某台服务器后,此服务器组失效。
line	使用线路口令认证。
none	认证无条件通过。

radius	使用RADIUS进行认证。
tacacs+	使用TACACS+ 认证。

当配置了 **enable** 认证方法为远端认证时（即配置了 **group**、**group-restrict**、**radius** 或 **tacacs+**关键字时），使用 **RADIUS** 进行认证和使用 **TACACS+**认证的用户名不同，下面分别介绍：

(1) 使用 **RADIUS** 进行 **enable** 认证：

认证的用户名为\$ENABLElevel\$, 其中 **level** 是指用户要进入的特权级别，即 **enable** 命令后的特权级别的数字，举例来说，如果某用户要进入级别为 7 的特权级别，需要输入命令 **enable 7**，如果此时配置了使用 **RADIUS** 进行认证，则提交给 **Radius Server** 的用户名为\$ENABLE7\$, 缺省条件下 **enable** 进入的特权级别均为 15，即在使用 **RADIUS** 进行认证时，提交给 **Radius Server** 的用户名为\$ENABLE15\$。这就需要预先在 **Radius Server** 上配置相应的用户名和密码，特别要指出的是：在 **Radius Server** 的用户数据库中，要指明用于特权认证的用户的服务类型（**Service-Type**）为 6，即 **Admin-User**。

(2) 使用 **TACACS+**进行 **enable** 认证：

进行 **enable** 认证时使用的用户名为该用户登录路由器时使用的用户名，举例来说，如果某用户登录进路由器时输入的用户名为 **chen**，则进行 **enable** 认证时使用的用户名也是 **chen**，如果用户登录路由器时没有被要求认证或者认证时没有被要求输入用户名，则登录成功后该用户的用户名为 **DEFAULT**，需要在 **TACACS+ Server** 的用户数据库中进行相应设置。

1.4.4 改变提示输入口令时的字符串

使用 **aaa authentication password-prompt** 命令可以改变提示用户输入口令时所显示的缺省文本。这条命令不仅改变 **enable** 口令的口令提示，也同时改变远端登录时的口令提示。该命令的 **no** 形式恢复口令提示为如下形式的缺省值：

Password:

命令 **aaa authentication password-prompt** 不改变远程 **TACACS+**或是 **RADIUS** 服务器所提供的任何提示信息。配置时，在全局模式下使用下面的命令：

命令	目的
aaa authentication password-prompt <i>text-string</i>	在提示用户输入口令时改变缺省的显示文本。

1.4.5 建立本地认证数据库

可以创建基于用户名的本地认证系统，用于下列情况：

- 为不支持 **TACACS+**的网络提供像 **TACACS+**一样的用户名或是加密的口令认证系统
- 提供灵活的登录环境；例如，访问列表验证、登录时自动执行（**autocommand**）等情况。

要建立本地用户名认证，可以在全局配置模式下，使用下面命令进行配置：

命令	目的
username <i>name</i> password { <i>password</i> [encryption-type] <i>encrypted-password</i> }	建立用户名及对应的密码。

1.4.6 建立本地用户组数据库

在需要认证的用户较少的情况下，可选择使用本地用户认证（即 **local** 方式），但是如果想在本地图用户中再细化区分不同用户（比如想实现一部分本地用户可以通过某些认证，另一部分不能通过等），这时就需要使用本地用户组认证（即 **localgroup** 方式）

要建立本地用户名组认证，需要在全局配置模式下，先进入本地用户组配置模式，使用下面命令进入：

命令	目的
Localgroup {1到4}	进入本地用户组。

然后在本地用户组模式下配置本地用户名，使用下面命令：

命令	目的
username <i>name</i> password { <i>password</i> [encryption-type] <i>encrypted-password</i> }	建立用户名及对应的密码。

至此，在一个本地用户组中就建立好了一个本地用户。

注意：不同本地用户组中可以出现相同的用户名，删除其中的一个，不影响其他的本地用户组。也就是说不同本地用户组互不相干。

第2章 IPSec配置

本章阐述了如何配置 IPSec。IPSec 是由 IETF 开发的开放标准框架。IPSec 为无保护网络（例如 Internet）上传输敏感数据提供了安全性。IPSec 在网络层起作用，对参与 IPSec 的设备（例如本公司路由器）之间传输的 IP 包进行保护和验证。

IPSec 提供了下列网络安全性服务。这些服务是可选的。通常，本地安全策略将规定使用下列这些服务的一种或多种：

- 数据机密性——IPSec 发送方在通过网络传输报文前对报文进行加密。
- 数据完整性——IPSec 接收方对发送方发送来的报文进行验证，以确保数据在传输过程中没有被篡改。
- 数据来源验证——IPSec 接收方对 IPSec 报文的源地址进行验证。这项服务基于数据完整性服务。
- 抗重播——IPSec 接收方可以检测和拒绝被重播的报文。

有了 IPSec，数据在通过公共网络传输时，就不用担心被监视、篡改和伪造。

要得到本章所用到的 IPSec 命令的完整阐述，请参阅“IPSec 配置命令”。

2.1 IPSec概述

IPSec 提供的安全性解决方案非常健壮、并且是基于标准的。作为对数据机密性的补充，IPSec 还提供了数据验证和抗重播服务。

2.1.1 支持的标准

本公司路由器 IPSec 实现了如下标准：

- IPSec——IP 安全性协议。IPSec 是在参与通信的两端之间提供数据机密性、数据完整性、数据验证的一种开放标准框架。IPSec 在 IP 层提供这些安全性服务；它使用 IKE 来协商基于本地策略的协议和算法，并产生加密和验证密钥供 IPSec 使用。IPSec 可为一对主机、一对安全网关或一台主机和一台安全网关之间的一条或多条数据流提供保护。
- Internet 密钥交换 (IKE)——一种在 ISAKMP 网络中实现 Oakley 和 SKEME 密钥交换的混合协议。尽管 IKE 可以和其他协议一起使用，它最初是和 IPSec 协议一起使用的。IKE 提供对 IPSec 对端的验证，协商 IPSec 安全联盟，生成 IPSec 密钥。要进一步了解 IKE，请参阅“配置 Internet 密钥交换安全性协议”。

2.1.2 术语

- **DES**——数据加密标准（DES）用于对包数据进行加密，属于对称加密算法，本公司路由器使用 IV 为 56 位 DES-CBC。CBC 需要一个初始化向量（IV）来进行加密。
- **3DES**——3DES 用于对包数据进行加密，属于对称加密算法。本公司路由器使用 IV 为 168 位 DES-CBC。3DES 比 DES 更为安全。
- **MD5（HMAC 变量）**——MD5 是一种散列算法。HMAC 是一个用于对数据进行验证的加密散列变量。
- **SHA（HMAC 变量）**——SHA 是一种散列算法。HMAC 是一个用于对数据进行验证的加密散列变量。

本公司路由器软件的 IPSec 还支持下列这些标准：

- **AH**——是一种安全协议，用于为 IP 提供数据完整性、数据原始身份验证和一些可选的抗重播服务。AH 可用来保护一个上层协议（传输模式）或一个完整的 IP 数据包（隧道模式）。AH 可单独使用，也可与 ESP 一起使用。定义在 RFC2402 中。
- **ESP**——是一种安全协议，用于为 IP 提供机密性、数据源验证、抗重播以及数据完整性等安全服务。ESP 可用来保护一个上层协议（传输模式）或一个完整的 IP 数据包（隧道模式）。定义在 RFC2406 中。

2.1.3 限制

现阶段，IPSec 只能用于单点传送 IP 数据报。因为 IPSec 工作组还没有从事组密钥分布的工作，IPSec 目前不支持多点传送或广播 IP 数据报。如果使用网络地址翻译技术（NAT），那么应该配置静态 NAT 翻译来使 IPSec 正常工作。总而言之，NAT 翻译必须在路由器进行 IPSec 封装之前进行；换句话说，IPSec 应该使用全局地址。

2.1.4 IPSec工作过程概述

IPSec 可以为两个路由器之间提供安全隧道。自己定义哪些报文由这些安全隧道传送。并且，通过指定这些隧道的参数来定义用于保护这些敏感报文的参数。然后，当 IPSec 得到这样的一个报文时，它将建立起相应的安全隧道，通过这条隧道将数据报文传送给对端。

更精确的说，隧道是 IPSec 两端建立的安全联盟的集合。这些安全联盟定义了哪些协议和算法将被应用于敏感报文，同时指定了 IPSec 两端将使用到的密钥。安全联盟是单向的，每个安全性协议（AH 或 ESP）都分别建立。

在 IPSec 中，通过配置访问列表，将访问列表配置在加密映射表中，再将加密映射表应用到接口上，可以使特定通信将受到保护。因此，可以基于源和目标地址、任意的第四层协议或端口对通信进行过滤（用于 IPSec 的访问列表只用于定义哪些通信将受到 IPSec 的保护，而不是定义哪些通信允许通过或禁止通过某个接口。一个加密映射表集合可包含多个加密映射表，每个都对应一个不同的访问列表。

当报文匹配某个特定访问列表中的第一条 **permit** 规则时，并且相应的加密映射表类型为 **ipsec-isakmp**，将由 IPsec 来处理。如果没有保护报文的安全联盟存在，IPsec 使用 IKE 来和对端协商建立安全联盟。

如果加密映射表类型为 **ipsec-manual**，将由 IPsec 来处理。如果没有保护报文的安全联盟存在，报文将被丢弃。在这种情况下，安全联盟通过手工配置，而无需 IKE。如果安全联盟不存在，那么一定没有配置所有必须的参数。

安全联盟集合一旦被建立，就被应用于处理报文，以及随后的适用报文。适用报文是指那些满足相同访问列表条件的报文。

如果使用 IKE 来建立安全联盟，那么这些安全联盟将具有生命周期，它们将阶段性地超时，需要重新协商（这提供了一层附加的安全性）。

IPsec 两端可以存在多条 IPsec 隧道来对不同数据流进行加密，每条隧道对应一个独立的安全联盟集合。例如，一些数据流可能只需要被验证，同时另一些数据流既需要被加密又需要被验证。IPsec 加密映射表所设置的访问列表指定了需要对哪些通信进行 IPsec 保护。进入报文依据加密映射表进行处理——如果一个未加密报文匹配了一个 IPsec 加密映射表设置的特定访问列表中的 **permit**，这个报文将被丢弃，因为它不是作为一个受 IPsec 保护的报文被传送的。加密映射表同时包括了变换集合。一个变换集合是安全性协议、算法以及将用于受 IPsec 保护的通信的其它设置的组合。在 IPsec 安全联盟协商期间，一致使用一个特定的变换集合来保护一个数据报文。

2.1.5 IPsec嵌套

你可以在一系列的 IPsec 路由器上进行 IPsec 通信的嵌套。例如，为了使通信横穿多个防火墙（这些防火墙都有相应的策略，不允许自己不能验证的通信通过），路由器需要按次序和每个防火墙建立 IPsec 隧道。

在下图所示的例子中，路由器 A 使用 IPsec 对去往路由器 C 的通信进行封装（路由器 C 是 IPsec 对端）。但是，在路由器 A 能够传送通信之前，它必须使用 IPsec 对这个通信进行预封装，其目的是为了将报文传送给路由器 B。



图 错误！未找到引用源。-1 IPsec 路由器嵌套示例图

外部 IPsec 两端之间可能拥有同一种保护（例如数据验证），内部 IPsec 两端之间也可能拥有不同的保护（例如既有数据验证，又有加密）。

2.2 IPSec配置任务列表

在完成 IKE 配置以后，进行 IPSec 配置。要配置 IPSec，就要在每台参与通信的 IPSec 路由器上完成下列各节的操作。

- 确保访问列表和 IPSec 相兼容
- 创建加密访问列表
- 加密访问列表技巧
- 在加密访问列表中使用 any 关键字
- 定义变换集合
- 创建加密映射表
- 应该建立多少个加密映射表
- 创建手工方式的加密映射表
- 创建使用 IKE 的加密映射表
- 将加密映射表集合应用于接口

2.3 IPSec配置任务

2.3.1 确保访问列表和IPSec相兼容

IKE 使用 UDP 端口 500。IPSec ESP 和 AH 协议使用 IP 协议号 50、51。确信在配置访问列表时，IPSec 使用的接口上协议 50、51 以及 UDP 端口 500 的通信没有被禁止。

2.3.2 创建加密访问列表

加密访问列表用于定义哪些 IP 通信要被加密保护，哪些不要被加密保护（这些访问列表和一般的访问列表不同，一般的访问列表用于决定一个接口上的哪些通信可以通过，哪些要被禁止）。

IPSec 加密映射表指定的加密访问列表有四个主要功能：

- 判断由 IPSec 进行保护的出报文（permit 为保护）。
- 当开始协商 IPSec 安全联盟时，指示数据流将由新安全联盟进行保护（由一条单独的 permit 指出）。
- 处理入报文，其目的是过滤和丢弃那些本应受到 IPSec 保护而没有受到保护的通信。

- 在处理 IPSec 对端发起的 IKE 协商时，决定是否接受其 IPSec 安全联盟申请。
- 如果想让某种报文使用一种 IPSec 保护的组合（例如，只是验证），另一种报文使用另一种不同的 IPSec 保护的组合（例如，既要验证又要加密），那么就需要创建两个不同的加密访问列表来定义这两种不同类型的通信。这两个不同的访问列表用在不同的加密映射表中，这些加密映射表设定了不同的 IPSec 策略。

以后应用加密映射表集合到接口的时候，就把这些加密访问列表和这些接口联系起来了。在全局配置态下使用下列命令来创建加密访问列表：

命令	目的
ip access-list extended name	进入的IP访问扩展列表配置模式。
permit	允许命令设置访问规则。
deny permit	禁止命令设置访问规则。
protocol source source-mask destination destination-mask	定义哪些IP通信要被加密保护。

注意：

加密访问列表名称必须以“VPN_”开头，在 telnet 配置时也必须以“VPN_”开头，否则 Web 方式则不显示该配置名称。

2.3.3 加密访问列表技巧

使用 **permit** 关键字将使得满足条件的所有 IP 通信都受到相应加密映射表中所描述策略的加密保护。使用 **deny** 关键字可以防止通信受到特定加密映射表的加密保护（换句话说，它不允许此加密映射表中指定的策略被应用到这个通信上）。如果某通信被接口上的所有加密映射表拒绝，那么该通信将不被加密保护。

在定义了相应的加密映射表，并且将加密映射表集合应用到接口上以后，所指定的加密访问列表将被应用到这个接口上。入和出报文将被相同的 IPSec 访问列表进行判定。因此，访问列表既对出报文正向使用，又对入报文反向使用。所以只需在访问列表中定义一条规则，IPSec 在使用这个规则时会匹配具有正好相反的源和目标地址的数据报文。

如果为一个给定的加密访问列表配置了多条规则，那么起作用的只是第一条规则。

2.3.4 在加密访问列表中使用any关键字

在创建加密访问列表的时候，使用 **any** 关键字可能会带来问题。所以不提倡用 **any** 关键字来指定源或目标地址。

当需要通过 IPSec 接口传输多点传送的通信时，不提倡在 **permit** 语句中使用 **any** 关键字；**any** 关键字将导致多点传送失败。**permit any any** 语句尤其不宜使用，因为这将导致所有的出报文受到保护（并且所有的受保护报文都被发送到在相应的加密映射表中指定的对端），并且将要求所有的入报文都要受到保护。

2.3.5 定义变换集合

变换集合是特定安全协议和算法的组合。在 IPsec 安全联盟协商期间，两端协商使用一个特定的变换集合来保护特定的数据流。

可以定义多个变换集合，然后在一个加密映射表中设置这些变换集合中的一个或多个。

在 IKE 协商安全联盟时，两端会查找双方一致的变换集合，当找到这样的变换集合后，安全联盟使用这变换集合保护保护特定的数据流。

对于手工建立的安全联盟，两端之间不存在协商过程，所以双方必须指定相同的变换集合。

如果对变换集合的定义进行改变，那么改变将只被应用于设置了这个变换集合的加密映射表中。改变将不被应用于现存的安全联盟，但它将被应用于随后建立新安全联盟的协商中。如果让这些新的设置马上生效，可以通过使用 `clear crypto sa` 命令将安全联盟数据库部分或全部清除。

在全局配置态下使用下列命令来定义一个变换集合：

命令	目的
crypto ipsec transform-set <i>transform-set-name</i>	定义一个变换集合执行此命令将进入加密变换配置态。
transform-type <i>transform1</i> [<i>transform2</i> [<i>transform3</i>]]	设置变换类型。
mode [tunnel transport]	（可选）改变变换集合的模式。模式设置只对那些源和目标地址都是IPsec两端地址的通信有用；对于所有其他通信无效（所有其他通信都只在隧道模式下进行）。
exit	退出加密变换配置态。

下表为可行的变换组合：

为变换集合选择变换：可行的变换组合					
AH 变换中选择一种		ESP 加密变换中选择一种		ESP 验证变换中选择一种	
变换	描述	变换	描述	变换	描述
ah-md5-hmac	带 MD5（HMAC变量）的AH验证算法	esp-des	采用 DES 的 ESP加密算法	esp-md5-hmac	带 MD5（HMAC变量）的ESP验证算法
ah-sha-hmac	带 SHA（HMAC变量）的AH验证算法	esp-3des	采用 3DES 的 ESP加密算法	esp-sha-hmac	带 SHA（HMAC变量）的ESP验证算法

2.3.6 创建加密映射表

关于加密映射表

为 IPsec 创建的加密映射表包括以下部分：

- 哪些通信应该受到 IPsec 保护（加密访问列表）
- 将受到一个安全联盟集合保护的数据流间隔
- 用于 IPsec 通信的对端地址
- 用于 IPsec 通信的本端地址
- 对这些通信应用哪些 IPsec 安全策略（从一个或多个变换集中选择）
- 安全联盟是手工建立还是通过 IKE 建立
- 其他可能用于定义 IPsec 安全联盟的参数

具有相同加密映射表名（但映射序列号不同）的加密映射表组成一个加密映射表集合。然后将加密映射表集合应用到接口上；这样，所有通过这接口的 IP 报文都将被应用在接口上的加密映射表集合进行判断。如果一个加密映射表匹配到应该受到保护的出报文，并且加密映射表指定了使用 IKE，将根据该加密映射表中所包含的参数与对端进行安全联盟协商。如果加密映射表使用手工建立的安全联盟，那么安全联盟在进行配置时就必须已经被建立好了。如果是本地发起协商，那么将使用加密映射表中指定的策略来创建发送给 IPsec 对端。如果是 IPsec 对端发起协商，那么本地路由器将在加密映射表检查对端所提供的策略，再决定是接受还是拒绝对端的申请。

为了使 IPsec 两端之间的 IPsec 通信能够顺利进行，两端的加密映射表必须包含相兼容的配置语句。

当两端尝试建立安全联盟时，双方都必须至少有一条加密映射表和对端的一条加密映射表相兼容。两条加密映射表相兼容必须至少满足以下条件：

- 加密映射表必须包含兼容的加密访问列表。
- 双方的加密映射表都必须确定对端地址。
- 加密映射表必须至少有一个相同的变换集合。

2.3.7 应该建立多少个加密映射表

对于单个接口可以只应用一个加密映射表集合。加密映射表集合中包含了 IPsec/ipsec-isakmp，或 IPsec/ipsec-manual 的组合。如果想要将相同的策略应用到多个接口上，也可以让多个接口共享同一加密映射表集合。

如果为给定的接口创建多个加密映射表，那么就要使用映射的 seq-num 参数将这些映射排序；seq-num 值越小，优先级越高。在配有这个加密映射表集合的接口上，首先用高优先级的映射对通信进行判断。如果存在下面几种情况中的一种，就必须为一个接口创建多个加密映射表：

- 如果不同的数据报文将由不同的 IPsec 对端进行处理。

- 如果想要对不同类型的数据报文应用不同的 IPsec 安全策略；例如，想让一组子网间的通信使用验证，而另一组子网间的通信既使用验证又使用加密。在这种情况下，不同类型的通信应该在两个不同的访问列表中被定义，并且必须为每个加密访问列表创建一个单独的加密映射表。
- 如果使用手工方式建立安全联盟，并且想要指定多个访问列表，那么必须创建不同的访问列表（每一个包含一条 **permit**），并且为每一个访问列表指定一个单独的加密映射表集合。

2.3.8 创建手工方式的加密映射表

手工安全联盟的使用是本地路由器和 IPsec 对端管理员之间预先安排的结果。双方可能想在开始的时候使用手工安全联盟，然后再使用基于 IKE 的安全联盟上来，或者远端系统可能不支持 IKE。如果不用 IKE 来建立安全联盟，那么就不存在安全联盟的协商过程，所以为了 IPsec 顺利处理报文，两端的配置必须完全一样。

路由器可以同时支持手工建立安全联盟，又支持 IKE 建立安全联盟。

要创建手工方式的加密映射表，在全局配置态下使用下列命令：

命令	目的
crypto map <i>map-name</i> <i>seq-num</i> ipsec-manual	创建或修改的加密映射表，执行此命令将进入加密映射表配置态。
match address <i>access-list-name</i>	设置IPsec访问列表。这个访问列表决定哪些报文受到IPsec的保护，哪些报文不受到此加密映射表中定义的IPsec安全性的保护。
set peer <i>ip-address</i>	设置IPsec对端地址。受到IPsec保护的报文将被发往这个地址。
set transform-set <i>transform-set-name</i>	设置变换集合（对于ipsec-manual加密映射表，只能指定一个变换集合。对于ipsec-isakmp，可以指定不多于六个加密映射表集合）。
set security-association inbound ah <i>spi</i> <i>hex-key-data</i> 和 set security-association outbound ah <i>spi</i> <i>hex-key-data</i>	如果指定的变换集合包括了AH协议，则要使用这条命令来为出和入的报文设置AH安全参数索引（SPIs）和密钥。这条命令手工指定了AH安全联盟将用于保护报文。
set security-association inbound esp <i>spi</i> [<i>cipher</i> <i>hex-key-data</i>] [<i>authenticator</i> <i>hex-key-data</i>] 和 set security-association outbound esp <i>spi</i> [<i>cipher</i> <i>hex-key-data</i>] [<i>authenticator</i> <i>hex-key-data</i>]	如果指定的变换集合包括了ESP协议，那么就要使用这条命令来为出和入报文设置ESP安全参数索引和密钥。如果变换集合包括了ESP加密算法，必须给出加密密钥。如果变换集合包括了ESP验证算法，必须给出验证密钥。这条命令手工指定了ESP安全联盟将用于保护通信。
exit	退出加密映射表配置态，并返回全局配置态。

重复这些步骤来建立其他加密映射表。

2.3.9 创建使用IKE的加密映射表

要创建使用 IKE 来建立安全联盟的加密映射表，在全局配置态下使用下列命令：

命令	目的
crypto map <i>map-name</i> <i>seq-num</i> ipsec-isakmp	创建或修改的加密映射表，执行此命令将进入加密映射表配置态。
match address <i>access-list-name</i>	设置IPSec访问列表。这个访问列表决定哪些报文受到IPSec的保护，哪些报文不受到此加密映射表中定义的IPSec安全性的保护。
set peer <i>ip-address</i>	设置IPSec对端地址。受到IPSec保护的报文将被发往这个地址。
set transform-set <i>transform-set-name1</i> [<i>transform-set-name2</i> ... <i>transform-set-name6</i>]	设置变换集合，可以指定不多于六个加密映射表集合（第一个具有最高优先级）。
set security-association lifetime seconds <i>seconds</i> 或 set security-association lifetime kilobytes <i>kilobytes</i>	（可选）设置加密映射表进行协商的安全联盟的生命周期。
set pfs [<i>group1</i> <i>group2</i>]	（可选）指定IPSec使用此加密映射表申请新安全联盟时，同时申请理想转发安全机制，还要求从IPSec对端发回的申请中必须有PFS要求。
exit	退出加密映射表配置态，并且返回全局配置态。

重复这些步骤来建立其他加密映射表。

2.3.10 将加密映射表集合应用于接口

要使配置的加密映射表开始工作，要将加密映射表集合应用于接口。路由器使用该加密映射表集合来判断通过此接口的所有报文，并在安全联盟协商过程中，对不同的受保护的报文使用特定的策略。

要将加密映射表集合应用于接口，在接口配置态下使用下面的命令。

命令	目的
crypto map <i>map-name</i>	将加密映射表集合应用于接口。

可以将同一加密映射表集合应用于多个接口。

2.4 IPSec配置示例

下面是使用 IKE 协商安全联盟的 IPSec 配置的例子。

关于 IKE，请参考“配置 IKE”文档。

1. 定义加密访问列表

```
ip access-list extended VPN_aaa
permit ip 130.130.0.0 255.255.0.0 131.131.0.0 255.255.0.0
```

2. 定义变换集合

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

3. 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 VPN_aaa
set transform-set one
set peer 192.2.2.1
```

4. 将加密映射表作用于接口

```
interface Serial1/1
ip address 192.2.2.2
crypto map toShanghai
```

第3章 配置Internet密钥交换安全协议

3.1 概述

本章讨论如何配置 Internet 密钥交换(IKE)协议。IKE 是一种密钥管理协议标准，与 IPSec 标准一起使用。IPSec 可以不使用 IKE，但 IKE 通过提供额外功能、灵活性及使 IPSec 更易于配置，增强了 IPSec 的功能。IKE 是一种混合协议，该协议在因特网安全联盟及密钥管理协议 (ISAKMP) 框架内实现了 Oakley 密钥交换和 Skeme 密钥交换 (ISAKMP、Oakley 和 Skeme 是 IKE 实现的安全协议)。

3.1.1 IKE概要

IKE 自动地处理 IPSec 安全联盟 (SA)，无需预先手工配置而进行 IPSec 安全通信。IKE 提供了下列好处：

- IKE 避免了在通信两端的加密映射表中用手工设置所有的 IPSec 安全参数。
- IKE 允许指定 IPSec 安全联盟的生命周期。
- IKE 允许在 IPSec 会话期间更换加密密钥。
- IKE 允许 IPSec 提供抗重播服务。
- IKE 允许在端与端之间动态验证。

3.1.2 支持的标准

路由器实现了下列标准：

IPSec——IPSec 是一种开放标准体制，在端与端之间提供数据加密、数据完整性以及数据验证服务。IPSec 在 IP 层提供这些安全服务，使用 IKE 来协商协议及算法，并生成 IPSec 所用的加密和验证密钥。IPSec 可以用来保护一对主机之间、一对安全网关之间或者一个安全网关与一台主机之间的一个或多个数据流。

IKE——该混合协议在 ISAKMP 框架内实现了 Oakley 和 Skeme 密钥交换协议，可以与其它协议一起使用，而其最初实现的目的是与 IPSec 协议一起使用。IKE 提供了 IPSec 两端的验证，协商 IPSec 密钥以及协商 IPSec 安全联盟。

ISAKMP——该协议框架定义了有效负荷的格式，实现密钥交换协议的机制以及安全协会的协商。

Oakley——一种密钥交换协议，定义如何得到验证的密钥材料。

Skeme——一种密钥交换协议，定义如何得到验证的密钥材料，并可进行快速密钥更新。

3.1.3 术语

DES——数据加密标准（DES）。

3DES——3DES 用于对包数据进行加密。

Diffie-Hellman——一种公钥加密协议，允许两个组在非保密的通信信道上建立共享的秘密。Diffie-Hellman 与 IKE 一起使用建立会话密钥。支持 768 比特和 1024 比特 Diffie-Hellman 组。

MD5（HMAC 变量）——MD5 是一种散列算法。HMAC 是一个用于对数据进行验证的加密散列变量。

SHA（HMAC 变量）——SHA 是一种散列算法。HMAC 是一个用于对数据进行验证的加密散列变量。

3.2 IKE配置任务列表

要配置 IKE，执行下面各节的任务。开头三节的任务是必需的；其余的是可选的，这取决于所配置的参数。

- 确保访问列表与 IKE 兼容
- 创建 IKE 策略
- 配置预共享密钥
- 清除 IKE 连接（可选）
- IKE 诊断（可选）

3.3 IKE配置任务

3.3.1 确保访问列表与IKE兼容

IKE 协商使用端口 500 的 UDP。确保 UDP 端口 500 的通信在 IKE 和 IPSec 使用的接口上不被禁止。在有些情况下需要在访问列表中增加一条规则来明确地允许 UDP 端口 500 的报文。

3.3.2 创建IKE策略

必须在 IPSec 两端创建 IKE 策略。IKE 策略定义了 IKE 协商期间使用的安全参数组合。

要创建 IKE 策略，注意以下问题：

- 创建策略的原因

- 策略中定义的参数
- IKE 如何达成匹配的策略
- 确定策略参数值
- 创建策略
- IKE 策略所需要的额外配置

1. 创建策略的原因

IKE 协商必须被保护起来，因此每个 IKE 协商从达成公共的 IKE 策略开始。这个策略描述了使用哪些安全参数来保护后续的 IKE 协商。

在两端达成公共的一个 IKE 策略后，该策略的安全参数由每端建立的 ISAKMP 安全联盟标识，在协商期间这些安全联盟将应用于所有的后续 IKE 通信。

必须在每端创建多个具有不同优先级的策略，以确保至少有一个策略能够匹配远端的策略。

2. 策略中定义的参数

在每个 IKE 策略中定义五个参数：

参数	接受的值	关键字	缺省值
加密算法	56位 DES-CBC 168位3DES-CBC	des 3des	56位 DES-CBC
哈希算法	SHA-1 MD5	sha md5	SHA-1
验证方法	预共享密钥 RSA签名 RSA 实时加密	pre-share rsa-sig rsa-encr	预共享密钥
Diffie-Hellman 组标识	768比特 Diffie-Hellman 1024比特Diffie-Hellman	1 2	768比特Diffie-Hellman
安全联盟的生命周期	可以指定60到86400秒之间任意数目的秒数	—	86400 秒 (一天)

3. IKE如何达成匹配的策略

当 IKE 协商开始时，IKE 寻找一个在两端都一样 IKE 策略。发起协商端将其所有的策略发给远端，而远端会试着寻找一个匹配的策略。远端通过将其最高优先级的策略与所接收到的策略相比较来寻找匹配项。远端按优先级的次序（最高优先级优先）检查其每一种策略直到发现一个匹配的策略。

当来自两端的策略均包括相同的加密、哈希、验证及 Diffie-Hellman 参数值，并且当远端的策略所指定的生命周期小于或等于所比较的策略生命周期时作出匹配选择。

如果没有发现可接受的匹配策略，IKE 拒绝协商，从而不会建立 IPSec。

如果找到一种匹配的策略，IKE 将完成协商，并且创建 IPSec 安全联盟。

注意：

根据策略中指定的验证方法的不同，需要对参数进行额外的配置。

4. 确定策略参数值

加密算法有两个选择：56 位 DES-CBC 和 168 位 3DES-CBC。3DES-CBC 更安全。

哈希算法有两个选项：SHA-1 和 MD5。MD5 的摘要信息较少，要比 SHA-1 快一些。针对 MD5 的攻击有一种被证明是成功的（但极其困难）；然而，由 IKE 使用的 HMAC 变体能阻止这种攻击。

验证方法有三种选择：目前只支持预共享密钥。

Diffie-Hellman 组有两种选择：768 比特或 1024 比特 Diffie-Hellman。1024 比特 Diffie-Hellman 较难于攻克，但要求更多的 CPU 时间来执行。

安全联盟的生命周期可以设置为 60 到 86400 秒之间任意值。生命周期越短，IKE 协商将越安全。对于较长的生命期，后面 IPSec 安全联盟可以更快地建立起来。关于该参数的更多信息以及如何使用该参数，参见 `lifetime`（IKE 策略）命令的命令描述。

5. 创建策略

可以创建多重 IKE 策略，每条策略对应不同的参数值组合。对所创建的每一条策略，须分配唯一的优先权（1 到 10000，1 是最高优先级）。

可以在每台终端上配置多重策略——然而至少这些策略中的某条策略必须包含与远程终端上某个策略完全一样的加密、哈希、验证及 Diffie-Hellman 参数值。

如果不配置任何策略，则路由器使用缺省的策略，该策略总是设为最低优先级，并包含每个参数的缺省值。

要配置一条策略，在全局配置模式下使用下面的命令：

命令	目的
<code>crypto isakmp policy priority</code>	创建IKE策略（每条策略唯一地由优先级标识） （该命令使你进入ISAKMP策略配置态）。
<code>encryption {des 3des}</code>	指定加密算法。
<code>hash {sha md5}</code>	指定哈希算法。
<code>authentication { pre-share rsa-sig rsa-encr}</code>	指定验证方法。
<code>group {1 2}</code>	指定Diffie-Hellman组。

lifetime seconds	指定IKE安全联盟的生命周期。
exit	退出ISAKMP策略配置态。
show crypto isakmp policy	(可选) 显示所有存在的IKE策略 (在管理态使用该命令)。

如果不给参数指定数值，则使用缺省值。

注意：

在发出 show running 命令时，缺省策略和所配置的策略的缺省值并不在配置中显示出来。

要查看缺省策略和所配置的策略内的缺省值，使用 show crypto isakmp policy 命令。

6. IKE策略所需要的额外配置

预共享密钥验证方法：如果在策略中指定预共享密钥作为验证方法，则必须配置预共享密钥。

3.3.3 配置预共享密钥

在 IPsec 两端指定共享密钥。注意所给的预共享密钥是在两端共享的。在两端上应当指定相同的密钥。

要在配置预共享密钥，在全局配置态下使用下面的命令：

命令	目的
crypto isakmp key keystring peer-address	在本端：指定与远端一起使用的共享密钥。
crypto isakmp key keystring peer-address	在远端：指定与本端一起使用的共享密钥。

3.3.4 清除IKE连接（可选）

如果需要，可以清除已经存在的 IKE 连接。要清除 IKE 连接，在管理态使用下面的命令：

命令	目的
show crypto isakmp sa	显示存在的isakmp SA 。
clear crypto isakmp [map map-name peer ip-address]	清除isakmp连接。

3.3.5 IKE诊断（可选）

要在 IKE 诊断中获取帮助，在管理态使用下面的命令：

命令	目的
show crypto isakmp policy	浏览IKE策略的参数。
show crypto isakmp sa	浏览所有当前IKE安全联盟。

debug crypto isakmp	显示关于IKE事件的debug消息。
----------------------------	--------------------

在完成 IKE 配置后，可以配置 IPsec。参见“配置 IPSEC”

3.4 IKE配置示例

本例创建了两个 IKE 策略，其中策略 10 为最高优先级，策略 20 为下一个优先级，已知的缺省优先级为最低的优先级。该策略同时创建一条预共享密钥，与 IP 地址为 192.168.1.3 的远端策略一起使用。

```
crypto isakmp policy 10
encryption des
hash md5
authentication pre-share
group 2
lifetime 5000
crypto isakmp policy 20
authentication pre-share
lifetime 10000
crypto isakmp key 1234567890 192.168.1.3
```

在上面示例中，策略 10 的 encryption des 在书面配置中将不会出现，因为这是加密算法参数的缺省值。

如果用这个配置发出 show crypto isakmp policy 命令，则输出可为下面的形式：

```
Protection suite of priority 10
  encryption algorithm:  DES - Data Encryption Standard (56 bit keys).
  hash algorithm:       Message Digest 5
  authentication method: Pre-Shared Key
  Diffie-Hellman group: #1 (768 bit)
  lifetime:             5000 seconds
Protection suite of priority 20
  encryption algorithm:  DES - Data Encryption Standard (56 bit keys).
  hash algorithm:       Secure Hash Standard
  authentication method: Pre-Shared Key
  Diffie-Hellman group: #1 (768 bit)
  lifetime:             10000 seconds
Default protection suite
  encryption algorithm:  DES - Data Encryption Standard (56 bit keys).
  hash algorithm:       Secure Hash Standard
  authentication method: Pre-Shared Key
  Diffie-Hellman group: #1 (768 bit)
  lifetime:             86400 seconds。
```