目 录

1 ACL 配置

说明

- 本文将用于 IPv4 和 IPv6 的 ACL 分别简称为 IPv4 ACL 和 IPv6 ACL。若非特别指明，本文所指的 ACL 均包括 IPv4 ACL 和 IPv6 ACL。
- WEB 界面上所有灰化的选项均不支持配置，本文中不再对此类选项进行解释。

1.1 概述

ACL（Access Control List，访问控制列表）是用来实现流识别功能的。网络设备为了过滤报文，需要配置一系列的匹配条件对报文进行分类，这些条件可以是报文的源地址、目的地址、端口号等。

当设备的端口接收到报文后，即根据当前端口上应用的 ACL 规则对报文的字段进行分析，在识别出特定的报文之后，根据预先设定的策略允许或禁止该报文通过。

由 ACL 定义的报文匹配规则可以应用在诸多领域，如安全、QoS 等，有关 ACL 在这些领域的具体应用，请参见相关的配置手册。

1.1.1 ACL 的分类

根据功能以及规则制定依据的不同，可以将 ACL 分为三种类型，如下表所示。

表1-1 ACL 的分类

ACL 类型	编号范围	适用的 IP 版本	区分报文的依据
基本ACL	2000～2999	IPv4	只根据报文的源IP地址信息制定匹配规则
		IPv6	只根据报文的源IPv6地址信息制定匹配规则
高级ACL	3000～3999	IPv4	根据报文的源IP地址信息、目的IP地址信息、IP承载的协议类型、协议的特性等三、四层信息制定匹配规则
		IPv6	根据报文的源IPv6地址信息、目的IPv6地址信息、IPv6承载的协议类型、协议的特性等三、四层信息制定匹配规则
链路层ACL	4000～4999	IPv4&IPv6	根据报文的源MAC地址、目的MAC地址、802.1p优先级、链路层协议类型等二层信息制定匹配规则

1.1.2 ACL 的匹配顺序

一个 ACL 由一条或多条描述报文匹配选项的判断语句组成，这样的判断语句就称为“规则”。由于每条规则中的报文匹配选项不同，从而使这些规则之间可能存在重复甚至矛盾的地方，因此在将一个报文与 ACL 的各条规则进行匹配时，就需要有明确的匹配顺序来确定规则执行的优先级。ACL 的规则匹配顺序有以下两种：

- 配置顺序：按照用户配置规则的先后顺序进行匹配，但由于本质上系统是按照规则编号由小到大进行匹配，因此后插入的规则如果编号较小也有可能先被匹配。
- 自动排序：按照“深度优先”原则由深到浅进行匹配，不同类型 ACL 的“深度优先”排序法则如下表所示。


说明

当报文与各条规则进行匹配时，一旦匹配上某条规则，就不会再继续匹配下去，系统将依据该规则对该报文执行相应的操作。

表1-2 各类型 ACL 的“深度优先”排序法则

ACL 类型	“深度优先”排序法则
IPv4基本ACL	(1) 先比较规则中的源 IPv4 地址范围，较小者优先 (2) 如果源 IPv4 地址范围相同，再比较配置顺序，配置在前者优先
IPv4高级ACL	(1) 先比较规则中的协议范围，指定有 IPv4 承载的协议类型者优先 (2) 如果协议范围相同，再比较源 IPv4 地址范围，较小者优先 (3) 如果源 IPv4 地址范围也相同，再比较目的 IPv4 地址范围，较小者优先 (4) 如果目的 IPv4 地址范围也相同，再比较四层端口（即 TCP/UDP 端口）号范围，较小者优先 (5) 如果四层端口号范围也相同，再比较配置顺序，配置在前者优先
IPv6基本ACL	(1) 先比较规则中的源 IPv6 地址范围，较小者优先 (2) 如果源 IPv6 地址范围相同，再比较配置顺序，配置在前者优先
IPv6高级ACL	(1) 先比较规则中的协议范围，指定有 IPv6 承载的协议类型者优先 (2) 如果协议范围相同，再比较源 IPv6 地址范围，较小者优先 (3) 如果源 IPv6 地址范围也相同，再比较目的 IPv6 地址范围，较小者优先 (4) 如果目的 IPv6 地址范围也相同，再比较四层端口（即 TCP/UDP 端口）号范围，较小者优先 (5) 如果四层端口号范围也相同，再比较配置顺序，配置在前者优先
链路层ACL	(1) 先比较规则中的源 MAC 地址范围，较小者优先 (2) 如果源 MAC 地址范围相同，再比较目的 MAC 地址范围，较小者优先 (3) 如果目的 MAC 地址范围也相同，再比较配置顺序，配置在前者优先


说明

- 比较 IPv4 地址范围的大小，就是比较 IPv4 地址通配符掩码中“0”位的多少：“0”位越多，范围越小。通配符掩码（又称反向掩码）以点分十进制表示，并以二进制的“0”表示“匹配”，“1”表示“不关心”，这与子网掩码恰好相反，譬如子网掩码 255.255.255.0 对应的通配符掩码就是 0.0.0.255。此外，通配符掩码中的“0”或“1”都可以是不连续的，这样可以更加灵活地进行匹配，譬如 0.255.0.255 就是一个合法的通配符掩码。
- 比较 IPv6 地址范围的大小，就是比较 IPv6 地址前缀的长短：前缀越长，范围越小。
- 比较 MAC 地址范围的大小，就是比较 MAC 地址掩码中“1”位的多少：“1”位越多，范围越小。

1.1.3 ACL 的步长

ACL 内的每条规则都有自己的编号，每个规则的编号在一个 ACL 中都是唯一的。在创建规则时，可以人为地为其指定一个编号，也可以由系统为其自动分配一个编号。

在自动分配编号时，为了方便后续在已有规则之前插入新的规则，系统通常会在相邻编号之间留下一定的空间，这个空间的大小（即相邻编号之间的差值）就称为 ACL 的步长。譬如，当步长为 5 时，系统会将编号 0、5、10、15……依次分配给新创建的规则。

系统为规则自动分配编号的方式如下：系统按照步长从 0 开始，自动分配一个大于现有最大编号的最小编号。譬如原有编号为 0、5、9、10 和 12 的五条规则，步长为 5，此时如果创建一条规则且不指定编号，那么系统将自动为其分配编号 15。

说明

如果改变步长，ACL 内原有全部规则的编号都将自动从 0 开始按新步长重新排列。譬如，某 ACL 内原有编号为 0、5、9、10 和 15 的五条规则；当修改步长为 2 之后，这些规则的编号将依次变为 0、2、4、6 和 8。

1.1.4 ACL 的生效时间段

时间段用于描述一个特定的时间范围。用户可能有这样的需求：一些 ACL 规则只需在某个或某些特定的时间段内生效（即进行报文过滤），这也称为基于时间段的 ACL 过滤。为此，用户可以先配置一个或多个时间段，然后在 ACL 规则下引用这些时间段，那么该规则将只在指定的时间段内生效。

1.1.5 ACL 对 IPv4 分片报文的处理

传统的报文过滤并不处理所有的 IPv4 报文分片，而只对首片分片报文进行匹配处理，而对后续分片一律放行。这样，网络攻击者可能构造后续的分片报文进行流量攻击，就带来了安全隐患。

为提高网络安全性，ACL 规则缺省会匹配所有报文（包括非分片报文和分片报文的每个分片）。同时，为了提高匹配效率，用户也可以对此匹配策略进行修改，譬如可指定规则仅对分片报文的非首个分片有效等。

1.2 配置ACL

1.2.1 配置概述

1. 配置 IPv4 ACL

IPv4 ACL 配置的推荐步骤如下表所示。

表1-3 IPv4 ACL 配置步骤

步骤	配置任务	说明
1	1.2.2 配置时间段	可选 新建时间段，ACL中的每条规则都可选择一个时间段，这条规则只在该指定的时间段内生效

步骤	配置任务	说明
2	1.2.3 配置基本IPv4 ACL	三者必选其一 新建ACL，定义ACL中的匹配规则 须根据不同类型的ACL，配置不同类型的规则
	1.2.4 配置高级IPv4 ACL	
	1.2.7 配置二层ACL组	

2. 配置 IPv6 ACL

IPv6 ACL 配置的推荐步骤如下表所示。

表1-4 IPv6 ACL 配置步骤

步骤	配置任务	说明
1	1.2.2 配置时间段	可选 新建时间段，ACL中的每条规则都可选择一个时间段，这条规则只在该指定的时间段内生效
2	1.2.5 配置基本IPv6 ACL	二者必选其一 新建IPv6 ACL，定义ACL中的匹配规则 须根据不同类型的IPv6 ACL，配置不同类型的规则
	1.2.6 配置高级IPv6 ACL	

1.2.2 配置时间段

(1) 在导航栏中选择“资源 > 时间段”。

(2) 单击，进入时间段的配置页面，如下图所示。

图1-1 添加时间段

(3) 配置时间段，详细配置如下表所示。

(4) 单击<确定>按钮完成操作。

表1-5 时间段的详细配置

配置项		说明	
名称		设置时间段的名称	
周期时间段	开始时间	设置一个周期时间范围的开始时间	在一个时间段中，如果同时设置了周期时间段和绝对时间段，则生效时间范围为二者的交集
	结束时间	设置一个周期时间范围的结束时间，必须大于开始时间	
	周日～周六	设置要配置的时间范围在每星期几有效。可选择周日～周六前的复选框	
绝对时间段	开始时间	设置一个绝对时间范围从某年某月某日的某一时间开始	
	开始日期		
	结束时间	设置一个绝对时间范围到某年某月某日的某一时间结束，必须大于有效时间范围的开始时间	
	结束日期		

1.2.3 配置基本 IPv4 ACL

(1) 在导航栏中选择“资源 > IPv4”。

(2) 单击  ，进入 IPv4 ACL 的新建页面，如下图所示。

图1-2 IPv4 ACL 新建

(3) 进行基本 IPv4 ACL 的配置，详细配置如下表所示。

(4) 单击<确定>按钮完成操作。进入基本 IPv4 ACL 规则的配置页面，如下图所示。

表1-6 新建 IPv4 ACL 的详细配置

配置项	说明
类型	设置IPv4 ACL的类型，包括基本ACL和高级ACL 此处选择“基本ACL”
编号	设置IPv4 ACL的编号，如下： • 当类型设置为基本 ACL 时，编号的范围是 2000-2999 • 当类型设置为高级 ACL 时，编号的范围是 3000-3999
名称	设置IPv4 ACL的名称
规则匹配顺序	设置IPv4 ACL中各规则的匹配顺序 • 按照配置顺序：按用户的配置顺序进行规则匹配 • 自动排序：系统自动排序，即按深度优先的原则进行规则匹配
规则编号步长	设置IPv4 ACL的规则编号步长
描述	设置IPv4 ACL的描述信息

图1-3 基本 IPv4 ACL 配置

(5) 配置基本 IPv4 ACL 规则，详细配置如下表所示。

(6) 单击<确定>按钮完成操作。

表1-7 基本 IPv4 ACL 规则的详细配置

配置项	说明
ACL编号	显示IPv4 ACL的编号
规则编号	设置所配置规则的编号 如果不指定，系统将为该规则自动指定一个规则ID 提示 如果指定的规则 ID 已经存在，则将该规则修改为新指定的配置
描述	设置IPv4基本ACL的规则
动作	设置对匹配该规则的IPv4报文所进行的操作 • 允许：表示允许匹配该规则的 IPv4 报文通过 • 禁止：表示禁止匹配该规则的 IPv4 报文通过

配置项		说明
匹配条件		设置是否匹配源IP地址/通配符掩码
规则生效时间段		设置规则生效的时间段
分片报文		设置该规则仅对非首片分片报文有效，对首片分片报文和非分片报文无效 如不设置，则规则对非分片报文和分片报文均有效
记录日志		设置对匹配该规则的IPv4报文记录日志 日志内容包括：ACL规则的序号、报文通过或被丢弃、IP承载的上层协议类型、源/目的地址、源/目的端口号、报文的数目 此功能暂不支持
匹配统计	开启本规则的匹配统计功能	设置是否开启本规则的匹配功能
	继续添加下一条规则	设置是否继续添加下一条规则

1.2.4 配置高级 IPv4 ACL

(1) 在导航栏中选择“资源 > IPv4”。

(2) 单击  ，进入 IPv4 ACL 的新建页面，如下图所示。

图1-4 IPv4 ACL 新建

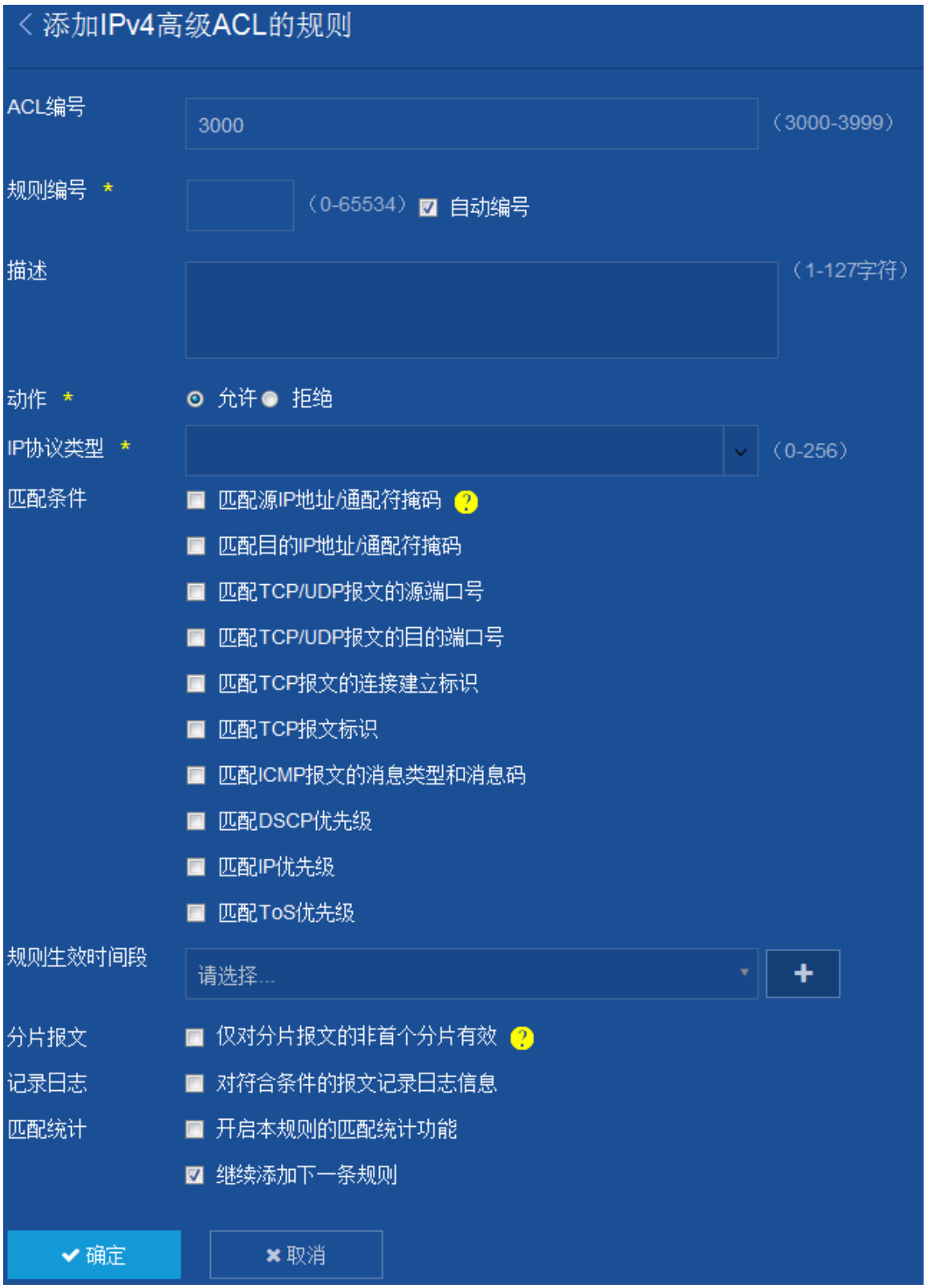
(3) 进行新建高级 IPv4 ACL 的配置，详细配置如下表所示。

(4) 单击<确定>按钮完成操作。进入高级 IPv4 ACL 规则的配置页面，如下图所示。

表1-8 新建 IPv4 ACL 的详细配置

配置项	说明
类型	设置IPv4 ACL的类型，包括基本ACL和高级ACL 此处选择“高级ACL”
编号	设置IPv4 ACL的编号，如下： • 当类型设置为基本 ACL 时，编号的范围是 2000-2999 • 当类型设置为高级 ACL 时，编号的范围是 3000-3999
名称	设置IPv4 ACL的名称
规则匹配顺序	设置IPv4 ACL中各规则的匹配顺序 • 按照配置顺序：按用户的配置顺序进行规则匹配 • 自动排序：系统自动排序，即按深度优先的原则进行规则匹配
规则编号步长	设置IPv4 ACL的规则编号步长
描述	设置IPv4 ACL的描述信息

图1-5 添加 IPv4 高级 ACL 的规则



(5) 配置高级 IPv4 ACL 规则，详细配置如下表所示。

(6) 单击<确定>按钮完成操作。

表1-9 高级 IPv4 ACL 规则的详细配置

配置项		说明
ACL编号		显示ACL编号
规则编号		设置所配置规则的ID 如果不指定，系统将为该规则自动指定一个规则ID 提示 如果指定的规则 ID 已经存在，则将该规则修改为新指定的配置
动作		设置对匹配该规则的报文所进行的操作 • 允许：表示允许匹配该规则的报文通过 • 禁止：表示禁止匹配该规则的报文通过
协议		设置IP承载的协议类型 例如，选择“6 TCP”或“17 UDP”协议后，可配置TCP/UDP端口
匹配条件		设置匹配条件
规则生效时间段		设置规则生效的时间段
分片报文		设置该规则仅对非首片分片报文有效，对首片分片报文和非分片报文无效 如不设置，则规则对非分片报文和分片报文均有效
记录日志		设置对匹配该规则的报文记录日志 日志内容包括：ACL规则的序号、报文通过或被丢弃、IP承载的上层协议类型、源/目的地址、源/目的端口号、报文的数目 此功能暂不支持
匹配统计	开启本规则的匹配统计功能	设置是否开启本规则的匹配功能
	继续添加下一条规则	设置是否继续添加下一条规则

1.2.5 配置基本 IPv6 ACL

(1) 在导航栏中选择“资源 > IPv6”。

(2) 单击  ，进入 IPv6 ACL 的新建页面，如下图所示。

图1-6 IPv6 ACL 新建

(3) 进行基本 IPv6 ACL 的配置，详细配置如下表所示。

(4) 单击<确定>按钮完成操作。进入基本 IPv6 ACL 规则的配置页面，如下图所示。

表1-10 新建 IPv6 ACL 的详细配置

配置项	说明
类型	设置IPv6 ACL的类型，包括基本ACL和高级ACL 此处选择“基本ACL”
编号	设置IPv6 ACL的编号，如下： • 当类型设置为基本 ACL 时，编号的范围是 2000-2999 • 当类型设置为高级 ACL 时，编号的范围是 3000-3999
名称	设置IPv6 ACL的名称
规则匹配顺序	设置IPv6 ACL中各规则的匹配顺序 • 按照配置顺序：按用户的配置顺序进行规则匹配 • 自动排序：系统自动排序，即按深度优先的原则进行规则匹配
规则编号步长	设置IPv6 ACL的规则编号步长
描述信息	设置IPv6 ACL的描述信息

图1-7 基本 IPv6 ACL 配置

(5) 配置基本 IPv6 ACL 规则，详细配置如下表所示。

(6) 单击<确定>按钮完成操作。

表1-11 基本 IPv6 ACL 规则的详细配置

配置项	说明
ACL编号	显示IPv6 ACL的编号
规则编号	设置所配置规则的编号 如果不指定，系统将为该规则自动指定一个规则ID 提示 如果指定的规则 ID 已经存在，则将该规则修改为新指定的配置
描述	设置IPv6基本ACL的规则

配置项		说明
动作		设置对匹配该规则的IPv6报文所进行的操作 • 允许：表示允许匹配该规则的 IPv6 报文通过 • 禁止：表示禁止匹配该规则的 IPv6 报文通过
匹配条件	匹配源IPv6地址/前缀长度	设置是否匹配源IPv6地址/前缀长度
	匹配路由头类型	设置是否匹配路由头类型
规则生效时间段		设置规则生效的时间段
分片报文		设置该规则仅对非首片分片报文有效，对首片分片报文和非分片报文无效 如不设置，则规则对非分片报文和分片报文均有效
记录日志		设置对匹配该规则的IPv6报文记录日志 日志内容包括：ACL规则的序号、报文通过或被丢弃、IP承载的上层协议类型、源/目的地址、源/目的端口号、报文的数目 此功能暂不支持
匹配统计	开启本规则的匹配统计功能	设置是否开启本规则的匹配功能
	继续添加下一条规则	设置是否继续添加下一条规则

1.2.6 配置高级 IPv6 ACL

(1) 在导航栏中选择“资源 > IPv6”。

(2) 单击  ，进入 IPv6 ACL 的新建页面，如下图所示。

图1-8 IPv6 ACL 新建

(3) 进行新建高级 IPv6 ACL 的配置，详细配置如下表所示。

(4) 单击<确定>按钮完成操作。进入高级 IPv6 ACL 规则的配置页面，如下图所示。

表1-12 新建 IPv6 ACL 的详细配置

配置项	说明
类型	设置IPv6 ACL的类型，包括基本ACL和高级ACL 此处选择“高级ACL”
编号	设置IPv6 ACL的编号，如下： • 当类型设置为基本 ACL 时，编号的范围是 2000-2999 • 当类型设置为高级 ACL 时，编号的范围是 3000-3999
名称	设置IPv6 ACL的名称
规则匹配顺序	设置IPv6 ACL中各规则的匹配顺序 • 按照配置顺序：按用户的配置顺序进行规则匹配 • 自动排序：系统自动排序，即按深度优先的原则进行规则匹配
规则编号步长	设置IPv6 ACL的规则编号步长
描述信息	设置IPv6 ACL的描述信息

图1-9 添加 IPv6 高级 ACL 的规则

(5) 配置高级 IPv6 ACL 规则，详细配置如下表所示。

(6) 单击<确定>按钮完成操作。

表1-13 高级 IPv6 ACL 规则的详细配置

配置项		说明
ACL编号		显示ACL编号
规则编号		设置所配置规则的ID 如果不指定，系统将为该规则自动指定一个规则ID 提示 如果指定的规则 ID 已经存在，则将该规则修改为新指定的配置
动作		设置对匹配该规则的报文所进行的操作 • 允许：表示允许匹配该规则的报文通过 • 禁止：表示禁止匹配该规则的报文通过
协议		设置IP承载的协议类型 例如，选择“6 TCP”或“17 UDP”协议后，可配置TCP/UDP端口
匹配条件		设置匹配条件
规则生效时间段		设置规则生效的时间段
分片报文		设置该规则仅对非首片分片报文有效，对首片分片报文和非分片报文无效 如不设置，则规则对非分片报文和分片报文均有效
记录日志		设置对匹配该规则的报文记录日志 日志内容包括：ACL规则的序号、报文通过或被丢弃、IP承载的上层协议类型、源/目的地址、源/目的端口号、报文的数目 此功能暂不支持
匹配统计	开启本规则的匹配统计功能	设置是否开启本规则的匹配功能
	继续添加下一条规则	设置是否继续添加下一条规则

1.2.7 配置二层 ACL 组

(1) 在导航栏中选择“资源 > 二层”。

(2) 单击  ，进入添加二层 ACL 的页面，如下图所示。

图1-10 添加二层 ACL

(3) 进行二层 ACL 的配置，详细配置如下表所示。

(4) 单击<确定>按钮完成操作。进入二层 ACL 规则的配置页面，如下图所示。

表1-14 新建二层 ACL 的详细配置

配置项	说明
编号	设置二层ACL的编号，编号的范围是4000-4999
名称	设置二层ACL的名称
规则匹配顺序	设置二层ACL中各规则的匹配顺序 • 按照配置顺序：按用户的配置顺序进行规则匹配 • 自动排序：系统自动排序，即按深度优先的原则进行规则匹配
规则编号步长	设置二层ACL的规则编号步长
描述	设置二层ACL的描述信息

图1-11 二层 ACL 配置

(5) 配置二层 ACL 规则，详细配置如下表所示。

(6) 单击<确定>按钮完成操作。

表1-15 二层 ACL 规则的详细配置

配置项	说明
ACL编号	显示二层ACL的编号
规则编号	设置所配置规则的编号 如果不指定，系统将为该规则自动指定一个规则ID 提示 如果指定的规则 ID 已经存在，则将该规则修改为新指定的配置
描述	设置二层ACL的规则

配置项		说明
动作		设置对匹配该规则的二层报文所进行的操作 • 允许：表示允许匹配该规则的二层报文通过 • 禁止：表示禁止匹配该规则的二层报文通过
匹配条件		设置是否匹配源IP地址/通配符掩码
规则生效时间段		设置规则生效的时间段
匹配统计	开启本规则的匹配统计功能	设置是否开启本规则的匹配功能
	继续添加下一条规则	设置是否继续添加下一条规则

1.3 注意事项

对 ACL 进行配置时，需要注意如下事项：

(1) 新创建或修改后的规则不能和已经存在的规则相同，否则会导致新建或修改不成功，系统会提示这条规则已经存在。

(2) 当 ACL 的匹配顺序为“用户配置”时，用户可以修改该 ACL 中的任何一条已经存在的规则，在修改 ACL 中的某条规则时，该规则中没有修改到的部分仍旧保持原来的状态；当 ACL 的匹配顺序为“自动”时，用户不能修改该 ACL 中的任何一条已经存在的规则，否则系统会提示错误信息。

2 SSL

说明

设备运行于 FIPS 模式时，本特性部分配置相对于非 FIPS 模式有所变化，具体差异请见本文相关描述。

2.1 SSL简介

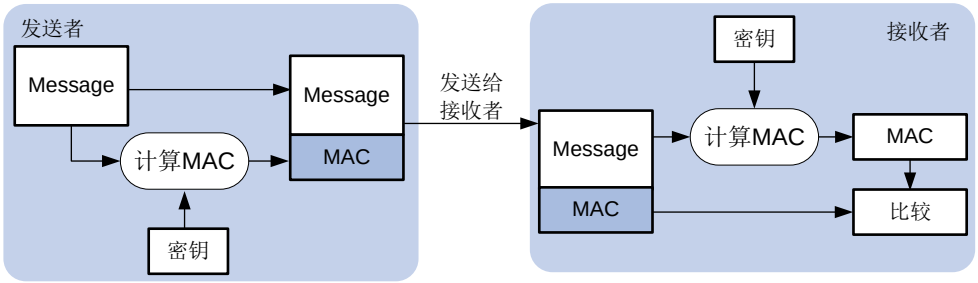
SSL（Secure Sockets Layer，安全套接字层）是一个安全协议，为基于 TCP 的应用层协议（如 HTTP）提供安全连接。SSL 协议广泛应用于电子商务、网上银行等领域，为应用层数据的传输提供安全性保证。

2.1.1 SSL 安全机制

SSL 提供的安全连接可以实现如下功能：

- 保证数据传输的机密性：利用对称密钥算法对传输的数据进行加密，并利用密钥交换算法，如 RSA（Rivest Shamir and Adleman），加密传输对称密钥算法中使用的密钥。对称密钥算法、非对称密钥算法 RSA 的详细介绍请参见“安全配置指导”中的“公钥管理”。
- 验证数据源的身份：基于数字证书利用数字签名方法对 SSL 服务器和 SSL 客户端进行身份验证。SSL 服务器和 SSL 客户端通过 PKI（Public Key Infrastructure，公钥基础设施）提供的机制获取数字证书。PKI 及数字证书的详细介绍请参见“安全配置指导”中的“PKI”。
- 保证数据的完整性：消息传输过程中使用 MAC（Message Authentication Code，消息验证码）来检验消息的完整性。MAC 算法在密钥的参与下，将任意长度的原始数据转换为固定长度的数据，原始数据的任何变化都会导致计算出的固定长度数据发生变化。如图 2-1 所示，利用 MAC 算法验证消息完整性的过程为：
  a. 发送者在密钥的参与下，利用 MAC 算法计算出消息的 MAC 值，并将其加在消息之后发送给接收者。
  b. 接收者利用同样的密钥和 MAC 算法计算出消息的 MAC 值，并与接收到的 MAC 值比较。
  c. 如果二者相同，则接收者认为报文没有被篡改；否则，认为报文在传输过程中被篡改，接收者将丢弃该报文。

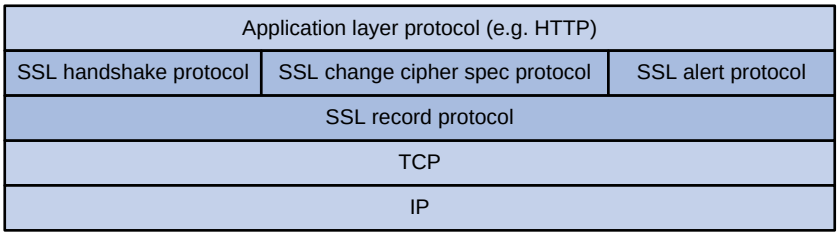
图2-1 MAC 算法示意图



2.1.2 SSL 协议结构

如图 2-2 所示，SSL 协议可以分为两层：下层为 SSL 记录协议（SSL Record Protocol）；上层为 SSL 握手协议（SSL Handshake Protocol）、SSL 密码变化协议（SSL Change Cipher Spec Protocol）和 SSL 告警协议（SSL Alert Protocol）。

图2-2 SSL 协议栈



- SSL 记录协议：主要负责对上层的数据进行分块、计算并添加 MAC、加密，最后把加密后的记录块传输给对方。
- SSL 握手协议：用来协商通信过程中使用的加密套件（数据加密算法、密钥交换算法和 MAC 算法等），实现服务器和客户端的身份验证，并在服务器和客户端之间安全地交换密钥。客户端和服务器通过握手协议建立会话。一个会话包含一组参数，主要有会话 ID、对方的数字证书、加密套件及主密钥。
- SSL 密码变化协议：客户端和服务器端通过密码变化协议通知对端，随后的报文都将使用新协商的加密套件和密钥进行保护和传输。
- SSL 告警协议：用来向对端报告告警信息，以便对端进行相应的处理。告警消息中包含告警的严重级别和描述。

2.2 配置SSL服务器端策略

(1) 在导航栏中选择“资源 > SSL”，默认进入“服务器端”页签的页面。

图2-3 SSL

(2) 单击，进入 SSL 服务器端策略的配置页面，如下图所示。

图2-4 添加 SSL 服务器端策略

(3) 配置 SSL 服务器端策略，详细配置如下表所示。

(4) 单击<确定>按钮完成操作。

表2-1 SSL 服务器端策略的详细配置

配置项	说明
策略名称	设置SSL服务器端策略的名称
PKI域	选择PKI域。若没有PKI域，则需要新建一个 单击可新增一个PKI域
加密套件	选择加密套件
最大缓存会话数目	设置最大缓存会话数目

配置项	说明
客户端验证	设置是否需要客户端验证

(5)　添加 PKI 域。

如图 2-4 所示，单击“PKI 域”后的，进入如下图所示页面。

图2-5 添加 PKI 域

(6)　配置 PKI 域的信息，详细配置如下表所示。

(7)　单击<确定>按钮完成操作。

表2-2 PKI 域的详细配置

配置项	说明
域名称	设置域名称
PKI实体	选择PKI实体。若没有PKI实体，则需要新建一个 单击可新增一个PKI实体
申请证书使用的密钥对	选择算法，如下： • RSA，设置密钥对名称和密钥长度，设置是否为加密和签名使用不同的公钥 • DSA，设置密钥对名称和密钥长度 • ECDSA，设置密钥对名称和密钥长度
CRL检查	设置是否检查证书已经被CA吊销

配置项	说明
证书的扩展用途	设置证书的扩展用途，包括IKE、SSL服务器、SSL客户端

(8) 添加 PKI 实体。

如图 2-5 所示，单击“PKI 域”后的  ，进入如下图所示页面。

图2-6 添加 PKI 域

(9) 配置 PKI 实体的信息，详细配置如下表所示。

(10) 单击<确定>按钮完成操作。

表2-3 PKI 实体的详细配置

配置项	说明
实体名称	设置PKI实体的名称
通用名	设置通用名
国家代码	设置国家代码
州或省的名称	设置州或省的名称
地理区域名称	设置地理区域名称
组织名称	设置组织名称
组织部门名称	设置组织部门名称
完全合格域名	设置完全合格域名
IP地址	设置IP地址

2.3 配置SSL客户端策略

(1) 在导航栏中选择“资源 > SSL”，默认进入“服务器端”页签的页面。

(2) 单击“客户端”页签。

(3) 单击  ，进入 SSL 客户端策略的配置页面，如下图所示。

图2-7 添加 SSL 客户端策略

(4) 配置 SSL 客户端策略，详细配置如下表所示。

(5) 单击<确定>按钮完成操作。

表2-4 SSL 服务器端策略的详细配置

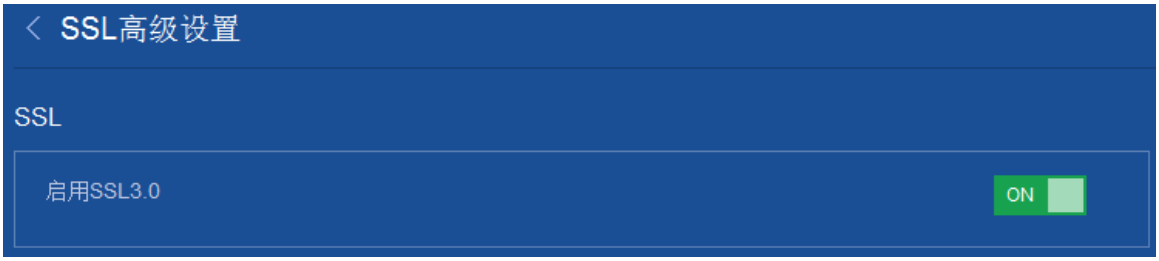
配置项	说明
策略名称	设置SSL客户端策略的名称
SSL协议版本	设置SSL协议的版本，包括： • TLS 1.0 • TLS 3.0
PKI域	选择PKI域。若没有PKI域，则需要新建一个 单击可新增一个PKI域 详细请参见“2.2 配置SSL服务器端策略”的添加PKI域
加密套件	选择加密套件
最大缓存会话数目	设置最大缓存会话数目
客户端验证	设置是否需要客户端验证

2.4 显示SSL高级信息

(1) 在导航栏中选择“资源 > SSL”，默认进入“服务器”页签的页面。

(2) 单击，进入 SSL 高级设置页面，如下图所示。此处显示了 SSL3.0 启用状态。

图2-8 SSL 高级设置



3 公钥

3.1 生成本地非对称密钥对

(1) 在导航栏中选择“资源 > 公钥”，默认进入“本地密钥”页签的页面。

图3-1

(2) 单击，进入“生成本地非对称密钥对”页面，如下图所示。

图3-2 生成本地非对称密钥对

(3) 配置本地非对称密钥对的信息，详细配置如下表所示。

(4) 单击<确定>按钮完成操作。

表3-1 本地非对称密钥对的详细配置

配置项	说明
算法	选择算法，包括RSA、DSA和ECDSA
密钥对名称	设置密钥对名称
密钥长度（比特）	设置密钥长度，当算法选择为“ECDSA”时，密钥长度无法设置，默认为192

3.2 导入远端主机公钥

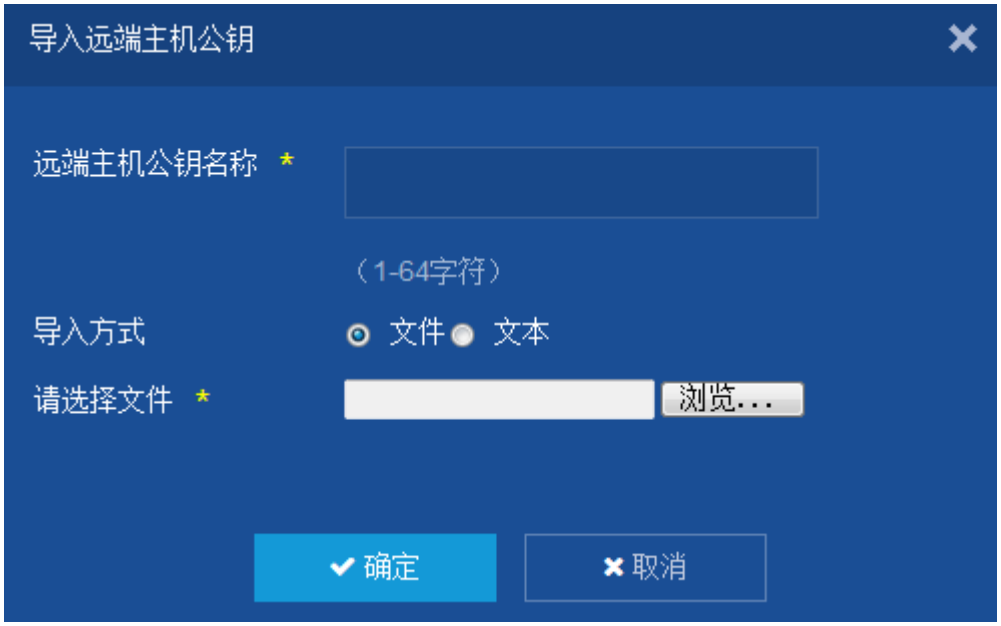
(1) 在导航栏中选择“资源 > 公钥”，默认进入“本地密钥”页签的页面。

(2) 单击“对端公钥”页签，如下图所示。

图3-3 对端公钥

(3) 单击  ，进入下图所示界面。

图3-4 导入远端主机公钥



(4) 配置导入远端主机公钥的信息，详细配置如下表所示。

(5) 单击<确定>按钮完成操作。

表3-2 导入远端主机公钥的详细配置

配置项	说明
远端主机公钥名称	设置远端主机公钥的名称
导入方式	选择导入方式，包括文件和文本
请选择文件	单击“浏览”导入需要的文件

4 PKI

4.1 概述

PKI（Public Key Infrastructure，公钥基础设施）是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的一种体系。

PKI 的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，为用户获取证书、访问证书和宣告证书作废提供了方便的途径。同时利用数字证书及相关的各种服务（证书发布、黑名单发布等）实现通信过程中各实体的身份认证，保证了通信数据的机密性、完整性和不可否认性。

4.1.1 相关术语

1. 数字证书

数字证书是一个经证书授权中心数字签名的、包含公开密钥及相关的用户身份信息的文件。最简单的数字证书包含一个公开密钥、名称及证书授权中心的数字签名。一般情况下数字证书中还包括密钥的有效时间、发证机关（证书授权中心）的名称和该证书的序列号等信息，证书的格式遵循 ITU-T X.509 国际标准。本手册中涉及两类证书：本地（local）证书和 CA（Certificate Authority）证书。本地证书为 CA 签发给实体的数字证书；CA 证书也称为根证书，为 CA“自签”的数字证书。

2. 证书废除列表（CRL，Certificate Revocation List）

由于用户姓名的改变、私钥泄漏或业务中止等原因，需要存在一种方法将现行的证书撤消，即撤消公开密钥及相关的用户身份信息的绑定关系。在 PKI 中，所使用的这种方法为证书废除列表。任何一个证书被废除以后，CA 就要发布 CRL 来声明该证书是无效的，并列出所有被废除的证书的序列号。CRL 提供了一种检验证书有效性的方式。

当一个 CRL 的撤消信息过多时会导致 CRL 的发布规模变得非常庞大，且随着 CRL 大小的增加，网络资源的使用性能也会随之下降。为了避免这种情况，允许一个 CA 的撤消信息通过多个 CRL 发布出来。CRL 片断也称为 CRL 发布点。

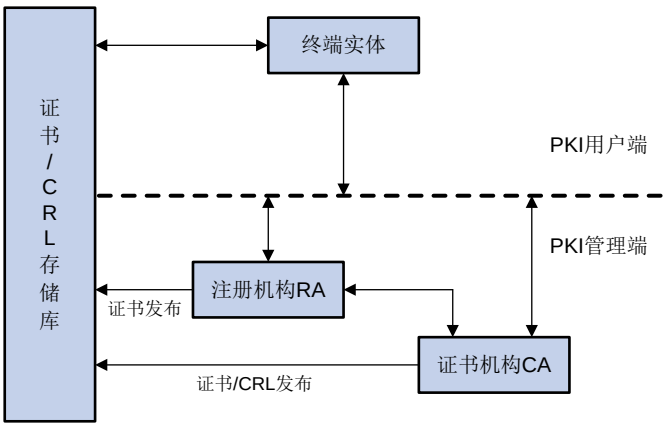
3. CA 策略

CA 在受理证书请求、颁发证书、吊销证书和发布 CRL 时所采用的一套标准被称为 CA 策略。通常，CA 以一种叫做证书惯例声明（CPS，Certification Practice Statement）的文档发布其策略，CA 策略可以通过带外（如电话、磁盘、电子邮件等）或其他方式获取。由于不同的 CA 使用不同的方法验证公开密钥与实体之间的绑定，所以在选择信任的 CA 进行证书申请之前，必须理解 CA 策略，从而指导对实体进行相应的配置。

4.1.2 体系结构

一个 PKI 体系由终端实体、证书机构、注册机构和 PKI 存储库四类实体共同组成，如下图所示。

图4-1 PKI 体系结构图



2. 终端实体

终端实体是 PKI 产品或服务的最终使用者，可以是个人、组织、设备（如路由器、交换机）或计算机中运行的进程。

3. 证书机构（CA，Certificate Authority）

CA 是 PKI 的信任基础，是一个用于签发并管理数字证书的可信实体。其作用包括：发放证书、规定证书的有效期和通过发布 CRL 确保必要时可以废除证书。

4. 注册机构（RA，Registration Authority）

证书申请的受理一般由一个独立的注册机构（即 RA）来承担。RA 功能包括：审查用户的申请资格，并决定是否同意 CA 给其签发数字证书；管理 CRL；产生和备份密钥对等。注册机构并不给用户签发证书，而只是对用户进行资格审查。有时 PKI 把注册管理的职能交给 CA 来完成，而不设立独立运行的 RA，但这并不是取消了 PKI 的注册功能，而只是将其作为 CA 的一项功能而已。PKI 国际标准推荐由一个独立的 RA 来完成注册管理的任务，这样可以增强应用系统的安全性。

5. PKI 存储库

PKI 存储库包括 LDAP（Lightweight Directory Access Protocol，轻量级目录访问协议）服务器和普通数据库，用于对用户申请、证书、密钥、CRL 和日志等信息进行存储和管理，并提供一定的查询功能。

LDAP 提供了一种访问 PKI 存储库的方式，通过该协议来访问并管理 PKI 信息。LDAP 服务器负责将 RA 服务器传输过来的用户信息以及数字证书进行存储，并提供目录浏览服务。用户通过访问 LDAP 服务器获取自己和其他用户的数字证书。

4.1.3 主要应用

PKI 技术的广泛应用能满足人们对网络交易安全保障的需求。作为一种基础设施，PKI 的应用范围非常广泛，并且在不断发展之中，下面给出几个应用实例。

1. 虚拟专用网络（VPN，Virtual Private Network）

VPN 是一种构建在公用通信基础设施上的专用数据通信网络，利用网络层安全协议（如 IPSec）和建立在 PKI 上的加密与数字签名技术来获得机密性保护。

2. 安全电子邮件

电子邮件的安全也要求机密、完整、认证和不可否认，而这些都可以利用 PKI 技术来实现。目前发展很快的安全电子邮件协议 S/MIME(Secure/Multipurpose Internet Mail Extensions，安全/多用途 Internet 邮件扩充协议)，是一个允许发送加密和有签名邮件的协议。该协议的实现需要依赖于 PKI 技术。

3. Web 安全

为了透明地解决 Web 的安全问题，在两个实体进行通信之前，先要建立 SSL（Secure Sockets Layer，安全套接字层）连接，以此实现对应用层透明的安全通信。利用 PKI 技术，SSL 协议允许在浏览器和服务器之间进行加密通信。此外，服务器端和浏览器端通信时双方可以通过数字证书确认对方的身份。

4.1.4 PKI 的工作过程

针对一个使用 PKI 的网络，配置 PKI 的目的就是为指定的实体向 CA 申请一个本地证书，并由设备对证书的有效性进行验证。下面是 PKI 的工作过程：

(1) 实体向 CA 提出证书申请；

(2) RA 审核实体身份，将实体身份信息和公开密钥以数字签名的方式发送给 CA；

(3) CA 验证数字签名，同意实体的申请，颁发证书；

(4) RA 接收 CA 返回的证书，发送到 LDAP 服务器以提供目录浏览服务，并通知实体证书发行成功；

(5) 实体获取证书，利用该证书可以与其它实体使用加密、数字签名进行安全通信；

(6) 实体希望撤消自己的证书时，向 CA 提交申请。CA 批准实体撤消证书，并更新 CRL，发布到 LDAP 服务器。

4.2 配置PKI

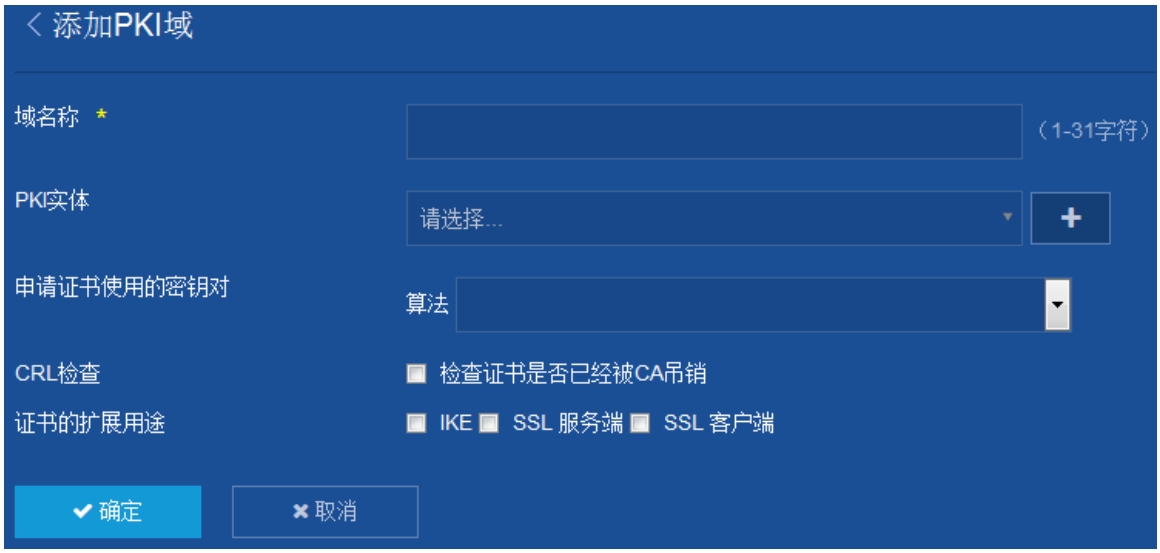
4.2.1 添加 PKI 域

(1) 在导航栏中选择“资源 > PKI”，默认进入“证书”页签的页面，如下图所示。

图4-2 PKI

(2) 单击  ，进入添加 PKI 域的配置页面，如下图所示。

图4-3 添加 PKI 域



(3) 配置 PKI 域的信息，详细配置如下表所示。

(4) 单击<确定>按钮完成操作。

表4-1 PKI 域的详细配置

配置项	说明
域名称	设置域名称
PKI实体	选择PKI实体。若没有PKI实体，则需要新建一个 单击可新增一个PKI实体
申请证书使用的密钥对	选择算法，如下： • RSA，设置密钥对名称和密钥长度，设置是否为加密和签名使用不同的公钥 • DSA，设置密钥对名称和密钥长度 • ECDSA，设置密钥对名称和密钥长度
CRL检查	设置是否检查证书已经被CA吊销
证书的扩展用途	设置证书的扩展用途，包括IKE、SSL服务器、SSL客户端

4.2.2 添加实体

(1) 在导航栏中选择“资源 > PKI”，默认进入“证书”页签的页面。

(2) 单击“实体”页签，如下图所示。

图4-4 实体

(3) 单击  ，进入添加 PKI 实体的配置页面，如下图所示。

图4-5 添加 PKI 实体

(4) 配置 PKI 实体的信息，详细配置如下表所示。

(5) 单击<确定>按钮完成操作。

表4-2 PKI 实体的详细配置

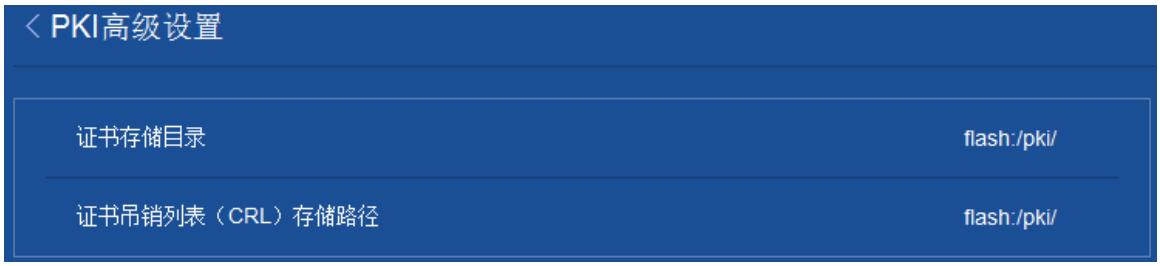
配置项	说明
实体名称	设置PKI实体的名称
通用名	设置通用名
国家代码	设置国家代码
州或省的名称	设置州或省的名称
地理区域名称	设置地理区域名称
组织名称	设置组织名称
组织部门名称	设置组织部门名称
完全合格域名	设置完全合格域名
IP地址	设置IP地址

4.2.3 PKI 高级设置

(1) 在导航栏中选择“资源 > PKI”，默认进入“服务器”页签的页面。

(2) 单击  ，进入 PKI 高级设置页面，如下图所示。

图4-6 PKI 高级设置



(3) 设置证书存储目录和证书吊销列表（CRL）存储路径。

(4) 单击<应用>按钮完成操作。

5 证书访问控制

5.1 配置属性组

(1) 在导航栏中选择“资源 > 证书访问控制”，默认进入“策略”页签的页面，如下图所示。

图5-1 证书访问控制

(2) 单击“属性组”页签，如下图所示。

图5-2 属性组

(3) 单击  ，进入如下图所示界面。

图5-3 添加属性组

(4) 配置属性组的信息，详细配置如下表所示。

(5) 配置完后，单击。

(6) 单击<确定>按钮完成操作。

表5-1 属性组的详细配置

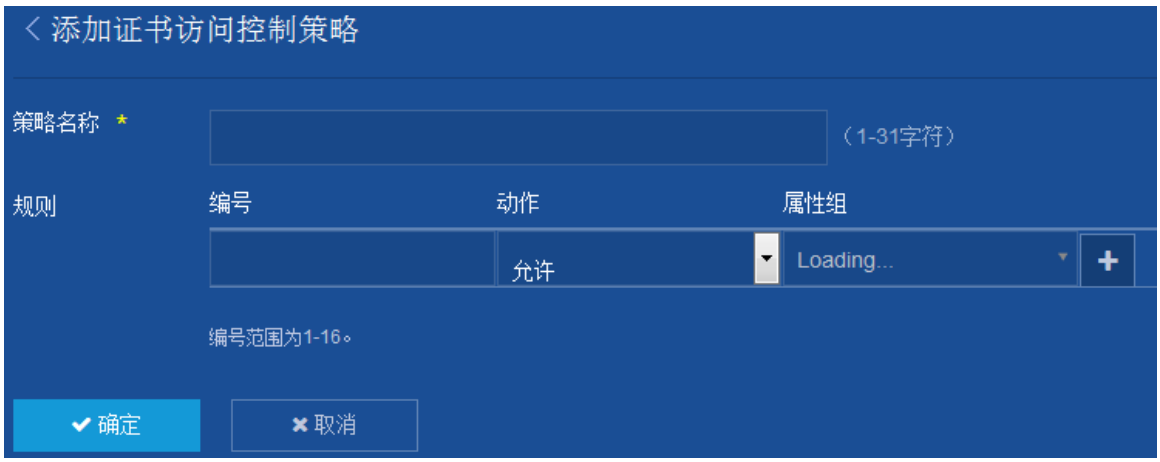
配置项		说明
属性组名称		设置属性组的名称
规则	编号	设置规则编号
	属性	设置规则属性，包括证书备注主题名、证书颁发者名、证书主题名
	操作符	设置操作符，包括包含、相等、不包含、不等于
	属性域	设置属性域，包括DN、FQDN、IP
	值	设置规则的值

5.2 配置证书访问控制策略

(1) 在导航栏中选择“资源 > 证书访问控制”，默认进入“策略”页签的页面，如图 5-1 所示。

(2) 单击，进入如下图所示页面。

图5-4 添加证书访问控制策略



(3) 配置证书访问控制策略的信息，详细配置如下表所示。

(4) 配置完后，单击。

(5) 单击<确定>按钮完成操作。

表5-2 证书访问控制策略的详细配置

配置项		说明
策略名称		设置策略的名称
规则	编号	设置规则的编号
	动作	设置规则的动作，包括允许和拒绝
	属性组	选择属性组