|  |  |
| --- | --- |
| 产品名称Product name | 密级Confidentiality level |
|  | 秘密 |
| 产品版本Product version | Total pages 共 页 |
|  |

SDN安全策略冲突检测项目测试报告

|  |  |  |  |
| --- | --- | --- | --- |
| Prepared by  拟制 |  | Date  日期 |  |
| Reviewed by  评审人 |  | Date  日期 |  |
| Approved by  批准 |  | Date  日期 |  |
| Authorized by  签发 |  | Date  日期 |  |



Huawei Technologies Co., Ltd.

华为技术有限公司

All rights reserved

版权所有 侵权必究

目录

[1. 项目概述 4](#_Toc395797720)

[1.1 项目目标 4](#_Toc395797721)

[1.1.1 防火墙规则管理 4](#_Toc395797722)

[1.1.2 流表管理 4](#_Toc395797723)

[1.1.3 有效DENY规则 4](#_Toc395797724)

[1.1.4 寻找FlowPath 4](#_Toc395797725)

[1.1.5 冲突检测 4](#_Toc395797726)

[1.1.6 冲突解决 5](#_Toc395797727)

[1.2 实现原理 5](#_Toc395797728)

[1.2.1 防火墙规则管理的实现 5](#_Toc395797729)

[1.2.2 流表管理的实现 5](#_Toc395797730)

[1.2.3 有效DENY规则的实现 5](#_Toc395797731)

[1.2.4 FlowPath动态获取的实现 5](#_Toc395797732)

[1.2.5 冲突检测的实现 6](#_Toc395797733)

[1.2.6 冲突解决的实现 6](#_Toc395797734)

[2. 测试时间地点及人员 6](#_Toc395797735)

[3. 环境描述 7](#_Toc395797736)

[4. 测试关注重点 7](#_Toc395797737)

[4.1 防火墙规则管理 7](#_Toc395797738)

[4.1.1 防火墙规则显示 7](#_Toc395797739)

[4.1.2 防火墙规则添加 7](#_Toc395797740)

[4.1.3 防火墙规则删除 7](#_Toc395797741)

[4.1.4 防火墙规则更新 7](#_Toc395797742)

[4.1.5 防火墙的打开/关闭 7](#_Toc395797743)

[4.2 流表管理 8](#_Toc395797744)

[4.2.1 交换机流表的显示 8](#_Toc395797745)

[4.2.2 添加流表 8](#_Toc395797746)

[4.2.3 删除流表 8](#_Toc395797747)

[4.2.4 更新流表 8](#_Toc395797748)

[4.3 有效DENY规则 8](#_Toc395797749)

[4.4 寻找FlowPath 8](#_Toc395797750)

[4.5 冲突检测 9](#_Toc395797751)

[4.6 冲突解决 9](#_Toc395797752)

[4.7 全局流路径 9](#_Toc395797753)

[5. 测试用例 9](#_Toc395797754)

[5.1 防火墙规则管理 10](#_Toc395797755)

[5.1.1 显示防火墙规则 10](#_Toc395797756)

[5.1.2 添加防火墙规则 11](#_Toc395797757)

[5.1.3 删除防火墙规则 11](#_Toc395797758)

[5.1.4 更新防火墙规则 12](#_Toc395797759)

[5.1.5 防火墙打开关闭 12](#_Toc395797760)

[5.2 流表管理 13](#_Toc395797761)

[5.2.1 显示流表 13](#_Toc395797762)

[5.2.2 添加流表 13](#_Toc395797763)

[5.2.3 删除流表 14](#_Toc395797764)

[5.2.4 更新流表 14](#_Toc395797765)

[5.3 寻找有效DENY规则 15](#_Toc395797766)

[5.4 寻找FlowPath 15](#_Toc395797767)

[5.5 冲突检测 16](#_Toc395797768)

[5.6 冲突解决 17](#_Toc395797769)

[5.7 全局流路径 18](#_Toc395797770)

[6. 测试结果 19](#_Toc395797771)

[6.1 防火墙规则管理 19](#_Toc395797772)

[6.1.1 显示防火墙规则 19](#_Toc395797773)

[6.1.2 添加防火墙规则 19](#_Toc395797774)

[6.1.3 删除防火墙规则 20](#_Toc395797775)

[6.1.4 修改防火墙规则 22](#_Toc395797776)

[6.1.5 防火墙打开和关闭 22](#_Toc395797777)

[6.2 流表管理 23](#_Toc395797778)

[6.2.1 显示流表 23](#_Toc395797779)

[6.2.2 添加流表 24](#_Toc395797780)

[6.2.3 删除流表 24](#_Toc395797781)

[6.2.4 更新流表 26](#_Toc395797782)

[6.3 有效DENY规则 26](#_Toc395797783)

[6.4 寻找FlowPath 27](#_Toc395797784)

[6.5 冲突检测 30](#_Toc395797785)

[6.6 冲突解决 32](#_Toc395797786)

[6.6.1 在浏览器中查看冲突路径。 32](#_Toc395797787)

[6.6.2 基于单个IP的冲突解决。 33](#_Toc395797788)

[6.6.3 基于网段的冲突解决。 34](#_Toc395797789)

[6.7 全局流路径 39](#_Toc395797790)

[6.7.1 在浏览器中查看全局流路径 39](#_Toc395797791)

[6.7.2 生成系统初始全局流路径 40](#_Toc395797792)

[6.8 性能测试 41](#_Toc395797793)

[7. 测试总结 42](#_Toc395797794)

[7.1 防火墙规则管理 42](#_Toc395797795)

[7.2 流表管理 42](#_Toc395797796)

[7.3 有效DENY规则 42](#_Toc395797797)

[7.4 寻找FlowPath 42](#_Toc395797798)

[7.5 冲突检测 42](#_Toc395797799)

[7.6 冲突解决 43](#_Toc395797800)

[7.7 全局流路径 43](#_Toc395797801)

[7.8 性能测试 43](#_Toc395797802)

图目

[图5- 1初始化拓扑结构 6](#_Toc395800704)

[图6- 1初始化的防火墙规则信息 16](#_Toc395800708)

[图6- 2防火墙规则删除成功 16](#_Toc395800709)

[图6- 3添加防火墙规则 17](#_Toc395800710)

[图6- 4查看新添加的防火墙规则 17](#_Toc395800711)

[图6- 5删除防火墙规则 18](#_Toc395800712)

[图6- 6提示删除所有防火墙规则 18](#_Toc395800713)

[图6- 7删除所有防火墙规则成功 18](#_Toc395800714)

[图6- 8修改防火墙规则 19](#_Toc395800715)

[图6- 9 h1和h4无法通信 19](#_Toc395800716)

[图6- 10 h1和h4可以通信 19](#_Toc395800717)

[图6- 11初始流表 20](#_Toc395800718)

[图6- 12删除流表 20](#_Toc395800719)

[图6- 13添加流表 21](#_Toc395800720)

[图6- 14删除流表 21](#_Toc395800721)

[图6- 15提示删除所有流表 22](#_Toc395800722)

[图6- 16删除所有流表成功 22](#_Toc395800723)

[图6- 17更新流表 23](#_Toc395800724)

[图6- 18初始有效DENY规则 23](#_Toc395800725)

[图6- 19删除防火墙规则后的有效DENY规则 23](#_Toc395800726)

[图6- 20初始shifted-flowpaths 24](#_Toc395800727)

[图6- 21测试h1和h4通信 24](#_Toc395800728)

[图6- 22抓取数据包1 25](#_Toc395800729)

[图6- 23抓取数据包2 25](#_Toc395800730)

[图6- 24删除流表 26](#_Toc395800731)

[图6- 25动态生成shifted-flowpath 26](#_Toc395800732)

[图6- 26初始冲突路径 26](#_Toc395800733)

[图6- 27 h1和h4通信测试 27](#_Toc395800734)

[图6- 28生成新冲突路径 27](#_Toc395800735)

[图6- 29测试h7和h13通信1 28](#_Toc395800736)

[图6- 30测试h7和h13通信2 28](#_Toc395800737)

[图6- 31在浏览器中查看冲突路径 29](#_Toc395800738)

[图6- 32基于单个IP的冲突解决 29](#_Toc395800739)

[图6- 33测试冲突解决是否成功 30](#_Toc395800740)

[图6- 34 DENY规则源地址大于冲突路径源地址 31](#_Toc395800741)

[图6- 35 DENY规则源地址等于冲突路径源地址 31](#_Toc395800742)

[图6- 36 DENY规则源地址小于冲突路径源地址 32](#_Toc395800743)

[图6- 37验证是否存在冲突 34](#_Toc395800744)

[图6- 38在浏览器中查看冲突路径 34](#_Toc395800745)

[图6- 39插入的阻断流表 35](#_Toc395800746)

[图6- 40验证冲突是否解决 35](#_Toc395800747)

[图6- 41在浏览器中查看全局流路径 36](#_Toc395800748)

[图6- 42生成系统初始全局流路径 36](#_Toc395800749)

[图6- 43性能测试的拓扑结 37](#_Toc395800750)

表目

[表格5- 1初始防火墙规则 6](#_Toc395800751)

[表格5- 2显示初始防火墙规则 7](#_Toc395800752)

[表格5- 3动态显示防火墙规则变化 7](#_Toc395800753)

[表格5- 4添加防火墙规则 8](#_Toc395800754)

[表格5- 5删除防火墙规则 8](#_Toc395800755)

[表格5- 6删除所有防火墙规则 8](#_Toc395800756)

[表格5- 7更新防火墙规则 9](#_Toc395800757)

[表格5- 8打开关闭防火墙 9](#_Toc395800758)

[表格5- 9显示初始流表 10](#_Toc395800759)

[表格5- 10动态显示流表变化 10](#_Toc395800760)

[表格5- 11添加流表 10](#_Toc395800761)

[表格5- 12删除流表 11](#_Toc395800762)

[表格5- 13删除所有流表 11](#_Toc395800763)

[表格5- 14更新流表 11](#_Toc395800764)

[表格5- 15初始有效DENY规则 12](#_Toc395800765)

[表格5- 16动态生成有效DENY规则 12](#_Toc395800766)

[表格5- 17生成系统初始化的FlowPath 12](#_Toc395800767)

[表格5- 18动态生成FlowPath 13](#_Toc395800768)

[表格5- 19生成系统初始化的冲突路径 13](#_Toc395800769)

[表格5- 20动态生成冲突路径1 13](#_Toc395800770)

[表格5- 21动态生成冲突路径2 14](#_Toc395800771)

[表格5- 22在浏览器中查看冲突路径 14](#_Toc395800772)

[表格5- 23基于IP的冲突解决 14](#_Toc395800773)

[表格5- 24基于网段的冲突解决 15](#_Toc395800774)

[表格5- 25系统初始全局流路径 15](#_Toc395800775)

[表格5- 26在浏览器中查看全局流路径 15](#_Toc395800776)

[表格6- 1性能测试结果 37](#_Toc395800777)

1. 项目概述
2. 项目目标
3. **防火墙规则管理**

防火墙子模块主要实现防火墙规则的图形界面管理，包括增加、删除、更新防火墙规则，以及防火墙功能的打开与关闭。

1. 流表管理

流表管理子模块实现查看SDN网络中的每一个交换机的所有流表，并且可以对交换机中的流表进性插入、删除、修改等操作功能。

1. 有效DENY规则

因为防火墙规则存在优先级的缘故，所以寻找有效的Deny规则是非常有必要的。从若干作用于同一主机防火墙规则中，找出优先级最高的防火墙规则。找到的防火墙规则是最终冲突检测时用于比对FlowPath是否是冲突路径。

1. 寻找FlowPath

当网络拓扑确定后，该系统可以找到网络中一个主机发送的信息到另一个主机所经过的路径。根据在路径中的交换机匹配的流表项是否有包头重写的操作，决定改路径是否是FlowPath。若流表项重写了数据报的包头，那么改路径便是FlowPath。该模块的功能是获得SDN网络中的所用的FlowPath。

1. 冲突检测

该模块对两种不同的情况，采取不同的策略检测是否有冲突出现。

一是添加防火墙规则。由于防火墙规则之间存在依赖，添加防火墙规则时可能引起防火墙有效Deny规则的变化。系统要先寻找有效Deny规则，然后查找是否出现冲突。

另一种情况是修改流表（包括添加、删除和更新）。修改流表后，系统要更新FlowPath，然后再去比对是否有冲突出现。

1. 冲突解决

在获取FlowPath和冲突检测的基础上，系统要解决存在冲突的FlowPath，阻止与防火墙规则相违反的主机之间的通信，同时也要确保尽量减少对主机之间正常通信的影响。

1. 实现原理
2. 防火墙规则管理的实现

Floodlight中实现了开放接口REST API，通过该接口可以以URL的形式向Floodlight传递参数，获得我们所需要的功能。在防火墙规则管理的实现中，该系统主要是通过调用REST ＡＰＩ实现对防火墙的关闭和打开以及防火墙规则的添加、删除和更新等功能。例如：

curl http://localhost:8080/wm/firewall/module/enable/json // 打开防火墙

curl http://localhost:8080/wm/firewall/module/disable/json // 关闭防火墙

1. 流表管理的实现

在Floodlight中同时实现了流表管理的接口REST API。与防火墙规则管理的原理类似，系统通过调用API实现对交换机中的流表添加、删除和更新等功能。简单来说，Floodlight将自己的API通过Rest API的形式向外暴露，关于Rest API，简单来讲，就是讲程序的API封装成为通用的http GET/PUT的形式，这样的话无需关注程序实现细节，通过发送http请求即可完成API操作。

所以，我们可以通过Floodlight的Restful API来向Floodlight请求各种信息，包括交换机状态，能力，拓扑等等，而static flow pusher这套机制则是通过Restful API来进行流表的操作，包括添加，删除流表等等。

1. 有效DENY规则的实现

首先将防火墙的deny规则和allow规则分别装入两个数组，然后判断防火墙规则的优先级，优先级分为allow规则和deny规则之间的比较，以及deny规则和deny规则间的比较，判断allow规则和deny规则时，如果allow规则的优先级大于deny规则的优先级，把两条规则作交运算；如果存在交集，执行deny规则时就要减掉交集部分；如果都是deny规则，存在交集时，优先级别低的源地址范围在执行时要减去交集部分的源地址，最后得到有效的deny规则集合。

1. FlowPath动态获取的实现

该模块探测网络中的主机是否连通，并返回所有的连通的路径，以供冲突检测只用。系统对网络中的每一台主机检测与该主机链接的交换机，用源主机的IP地址匹配交换机中的流表项的源地址，若相同根据流表中的Action跳到下一个交换机中，重复此过程直至到达网络中的某一台主机。若交换机中不存在匹配的流表项或找不到主机，说明此路不通，继续探测下一条路径。当对网络中的每一台主机都进行了该过程以后，获得所有的FlowPath。

1. 冲突检测的实现

添加防火墙规则时，首先要计算有效的deny规则。针对需要检测的DENY规则，首先得到deny规则的源地址和目的地址，然后使用FlowPath探测算法获得满足该规则的Shifted-flowpath。将shifted- flowpath的源地址、目的地址与含有“deny”的防火墙规则的源地址和目的地址进行匹配，匹配成功则说明出现冲突。

否

当添加流表项时，可能引起shifted flowpath的变化，如果shifted flowpath发生变化，把改变后的shifted flowpath的源地址和目的地址与防火墙规则的源地址和目的地址进行匹配，匹配成功则存在冲突，否则不存在冲突。匹配成功的路径成为冲突路径，它们是冲突解决的对象。

1. 冲突解决的实现

对于不同的冲突对象，冲突解决的方式也不同。根据防火墙规则的源地址和冲突路径的源地址的范围大小，具体分为以下两种：

一是基于单个IP的冲突路径或防火墙规则源地址大于等于冲突路径源地址。解决的办法是删除形成冲突路径的转发流表，网络中不存在该FlowPath也就不会有冲突路径。

二是防火墙规则的源地址小于冲突路径的源地址。解决的办法是在冲突路径的首尾交换机插入阻断流表，分别阻断从源主机发出的违反防火墙规则的通信数据包，和将要进入目的主机的违反防火墙规则的通信数据包。

1. 测试时间地点及人员

|  |  |  |  |
| --- | --- | --- | --- |
| 测试时间 | | 测试人员 | 测试地点 |
| 起始时间 | 结束时间 |
|  |  |  |  |
|  |  |  |  |

1. 环境描述

Floodlight控制器运行环境：Ubuntu 12.04 LTS 32bit，Intel CORE i5，4GB ddr3 memory

Floodlight 版本：Version 0.90

VirtualBox版本：Version 4.1.12\_Ubuntu

Mininet版本：Version 2.0.0，基于Ubuntu 12.10 64bit

开发工具：Eclipse

1. 测试关注重点
2. 防火墙规则管理
3. 防火墙规则显示

系统初始化时添加的防火墙规则是否会在防火墙管理界面显示，当向控制器（Floodlight）中添加、删除、更新防火墙规则时，系统能否动态的显示防火墙规则的变化。以及显示的防火墙规则的详细信息是否正确。

1. 防火墙规则添加

测试在通过防火墙管理界面新建的防火墙规则，能否成功添加到控制器中。并且在新添加的规则不违反防火墙规则的语法的前提下，该防火墙规则能否起作用，阻止违反该规则的主机通信。

1. 防火墙规则删除

测试选中某条防火墙规则后，点击删除防火墙规则按钮后，该防火墙规则能否成功的从控制器中删除。点击删除所有规则按钮后，是否所有的防火墙规则都成功的从控制器中删除。

1. 防火墙规则更新

点击选中某条防火墙规则后，显示该防火墙规则的详细信息。修改该规则的若干值，保存修改。刷新显示后，查看修改的防火墙规则是否起到作用。

1. 防火墙的打开/关闭

测试防火墙的打开/关闭功能是否能正常工作。在控制器中已添加若干防火墙规则的前提下，点击关闭防火墙。测试违反已添加的防火墙规则的主机是否能够通信。点击打开防火墙按钮，测试违反已添加防火墙规则的主机之间的通信是否能被防火墙阻止。

1. 流表管理
2. 交换机流表的显示

测试系统初始化建立的网络拓扑中的交换机能否正确的显示在流表管理界面。当网络拓扑发生变化时，刷新流表管理界面，能否动态的显示网络拓扑的变化情况。测试系统初始化时添加的流表能否正确显示在流表的管理界面。在系统运行的过程中，动态的向交换机中添加、删除或修改流表，系统能够动态的作出相应的显示。

1. 添加流表

点击新流，填写正确的流表项值，点击写入按钮。测试通过流表管理界面能否正确的向交换机中添加流表。并通过测试与该流表项相关的主机能否相互通信，判断在添加的流表项内容正确的前提下，该流表项是否其作用。

1. 删除流表

选择交换机，并选择交换机下的某一个流表项，点击删除流按钮，刷新界面。测试能否通过流表管理界面删除交换机中指定的流表项。选择交换机，不选择流表项，点击删除所有流按钮，刷新界面。测试通过流表管理界面能否删除交换机下所有的流表项。

1. 更新流表

选择交换机，并选择交换机下的某一个流表项，在显示流表项内容的界面中修改流表项的值，点击写入按钮，刷新界面，重新选择修改的流表项。测试流表项的内容是否经过修改，并通过测试主机之间的通信，测试修改的流表项是否其作用了。

1. 有效DENY规则

测试在若干条相互依赖的防火墙规则中，能否正确的找出有效的防火墙规则。当添加新的防火墙规则时，调用获取有效DENY规则的方法，测试能否动态的产生正确的有效DENY规则。

1. FlowPath探测

测试在系统初始化时，能否根据系统初始的网络拓扑快速准确的找到FlowPath。当网络拓扑发生变化时，测试系统能否动态的响应网络拓扑的变化，并动态的更新FlowPath。当网络中交换机的流表内容发生变化时，测试系统能否正确的找出新的FlowPath。

1. 冲突检测

测试在系统初始化时，能否根据系统初始的网络拓扑找出的FlowPath和有效的DENY规则中找出冲突路径。在控制器中防火墙规则发生变化，或交换机的流表发生变化时，系统能否找到正确的FlowPath和有效的DENY规则。最后找出正确的冲突路径并显示出来。

1. 冲突解决

测试系统能否解决冲突路径。对于基于单个IP和基于网段的冲突路径，能否正确的解决。在冲突路径中的网段大于、小于或等于防火墙规则中的网段的范围时，能否正确的解决冲突.。

1. 全局流路径

测试系统能否正确的生成全局的流路径，以及生成的全局流路径能否在浏览器中正确的显示。

1. 测试用例

以下测试用例中所说的系统初始化是指，mininet在指定的拓扑结构（见图5-1）下启动，以及向floodlight中添加防火墙规则（见表格5-1）和流表规则（见附件3sw16h\_flows.py）。

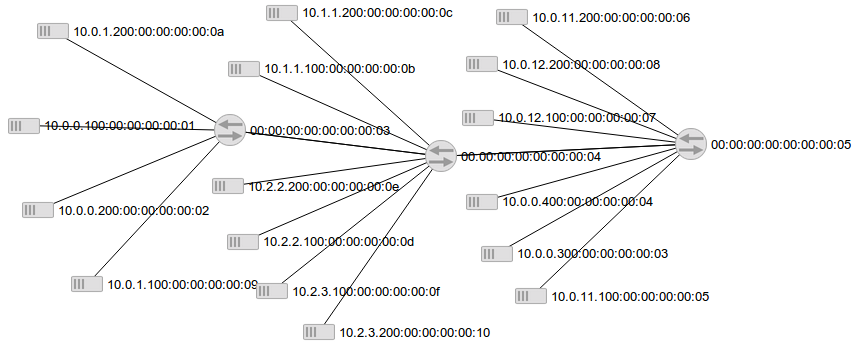


图5- 初始化拓扑结构

表格5- 初始防火墙规则

|  |  |  |  |
| --- | --- | --- | --- |
| 源地址 | 目的地址 | 动作 | 优先级 |
| 10.0.0.1/32 | 10.0.0.4/32 | DENY | 1 |
| 10.0.11.0/24 | 10.0.1.0/24 | DENY | 1 |
| 10.1.0.0/16 | 10.0.12.0/24 | DENY | 1 |
| 10.2.2.0/24 | 10.0.12.0/24 | DENY | 1 |
| 10.0.0.1/32 | 10.0.0.5/32 | DENY | 1 |
| 10.0.0.1/32 | 10.0.0.6/32 | DENY | 1 |
| 10.0.0.1/32 | 10.0.0.7/32 | DENY | 1 |
| 10.3.0.0/16 | 10.0.0.0/24 | DENY | 1 |

在添加防火墙规则之前需要在运行控制器的主机上输入以下指令：

curl http://localhost:8080/wm/firewall/module/enable/json

curl -X POST -d '{"switchid": "00:00:00:00:00:00:00:03","priority":"1"}' http://localhost:8080/wm/firewall/rules/json

curl -X POST -d '{"switchid": "00:00:00:00:00:00:00:04","priority":"1"}' http://localhost:8080/wm/firewall/rules/json

curl -X POST -d '{"switchid": "00:00:00:00:00:00:00:05","priority":"1"}' http://localhost:8080/wm/firewall/rules/json

1. 防火墙规则管理
2. 显示防火墙规则

表格5- 显示初始防火墙规则

|  |  |
| --- | --- |
| 序号 | 1 |
| 名称 | 显示初始防火墙规则 |
| 预置条件 | 系统初始化添加防火墙规则 |
| 测试步骤 | 1. 启动控制器和SDNGuard  2. 登录SDNGuard  3. 单击防火墙，显示防火墙规则  4. 选中规则，显示规则详细信息 |
| 预期结果 | 能准确显示防火墙规则及其详细信息 |

表格5- 动态显示防火墙规则变化

|  |  |
| --- | --- |
| 序号 | 2 |
| 名称 | 动态显示防火墙规则变化 |
| 预置条件 | 系统初始化添加防火墙规则 |
| 测试步骤 | 1. 启动防火墙管理界面。步骤同上，以下略述。  2. 修改防火墙规则（添加或删除）  3. 刷新显示，看是否有规则添加或删除 |
| 预期结果 | 能准确显示防火墙规则及其详细信息 |

1. 添加防火墙规则

表格5- 添加防火墙规则

|  |  |
| --- | --- |
| 序号 | 3 |
| 名称 | 添加防火墙规则 |
| 预置条件 | 系统初始化添加防火墙规则 |
| 测试步骤 | 1. 启动防火墙规则管理。  2. 选择新建规则。  3. 填写防火墙规则参数值。  4. 单击保存规则，防火墙规则写入控制器。 |
| 预期结果 | 防火墙规则成功写入，刷新显示可看到新添加的规则。 |

1. 删除防火墙规则

表格5- 删除防火墙规则

|  |  |
| --- | --- |
| 序号 | 4 |
| 名称 | 删除防火墙规则 |
| 预置条件 | 系统初始化添加防火墙规则 |
| 测试步骤 | 1. 启动防火墙规则管理。  2. 选择某一条防火墙规则。  3. 选择删除防火墙规则。  4. 刷新显示，当前所有的防火墙规则。 |
| 预期结果 | 被选中的规则删除成功 |

表格5- 删除所有防火墙规则

|  |  |
| --- | --- |
| 序号 | 5 |
| 名称 | 删除所有防火墙规则 |
| 预置条件 | 系统初始化添加防火墙规则 |
| 测试步骤 | 1. 启动防火墙规则管理  2. 选择删除所有规则  3. 刷新显示，当前所有的防火墙规则 |
| 预期结果 | 当前所有的防火墙规则都被删除 |

1. 更新防火墙规则

表格5- 更新防火墙规则

|  |  |
| --- | --- |
| 序号 | 6 |
| 名称 | 更新防火墙规则 |
| 预置条件 | 系统初始化添加防火墙规则 |
| 测试步骤 | 1. 启动防火墙规则管理  2. 选择某条防火墙规则  3. 修改防火墙规则的参数值  4. 单击保存，保存防火墙规则  5. 刷新显示 |
| 预期结果 | 防火墙规则修改成功 |

1. 防火墙打开关闭

表格5- 打开关闭防火墙

|  |  |
| --- | --- |
| 序号 | 7 |
| 名称 | 打开关闭防火墙 |
| 预置条件 | 系统初始化添加防火墙规则 |
| 测试步骤 | 1.启动防火墙规则管理  2. 在mininet中对防火墙规则禁止通信的主机进行联通测试  3. 选择防火墙已打开  4. 重复步骤2 |
| 预期结果 | 防火墙已打开的情况下，无法通信。防火墙已关闭的情况下，可以通信。 |

1. 流表管理
2. 显示流表

表格5- 显示初始流表

|  |  |
| --- | --- |
| 序号 | 8 |
| 名称 | 显示初始流表 |
| 预置条件 | 系统初始化添加流表规则 |
| 测试步骤 | 1. 启动控制器和SDNGuard  2. 登录SDNGuard  3. 单击流表管理，显示流表规则  4. 选中交换机，选择流表，显示规则详细信息 |
| 预期结果 | 能准确显示流表规则及其详细信息 |

表格5- 动态显示流表变化

|  |  |
| --- | --- |
| 序号 | 9 |
| 名称 | 动态显示流表变化 |
| 预置条件 | 系统初始化添加流表规则 |
| 测试步骤 | 1. 启动流表管理。步骤同上，以下略述  2. 选择交换机中的流表并删除  3. 单击更新，查看交换机下是否有删除的流表  4. 选中交换机，选择流表，显示规则详细信息 |
| 预期结果 | 交换机下不存在以删除的流表。能准确的显示流表的变化。 |

1. 添加流表

表格5- 添加流表

|  |  |
| --- | --- |
| 序号 | 10 |
| 名称 | 添加流表 |
| 预置条件 | 系统初始化添加流表规则 |
| 测试步骤 | 1. 启动流表管理  2. 选择交换机，单击新流  3. 填写流表参数值  4. 选择新操作，填写操作的参数值，保存  5. 单击写入 |
| 预期结果 | 流表可以被成功的添加到交换机中。 |

1. 删除流表

表格5- 删除流表

|  |  |
| --- | --- |
| 序号 | 11 |
| 名称 | 删除流表 |
| 预置条件 | 系统初始化添加流表规则 |
| 测试步骤 | 1. 启动流表管理  2. 选择交换机中的流表，并选择删除流。  3. 单击更新，查看交换机下是否有删除的流表 |
| 预期结果 | 交换机下不存在以删除的流表。 |

表格5- 删除所有流表

|  |  |
| --- | --- |
| 序号 | 12 |
| 名称 | 删除所有流表 |
| 预置条件 | 系统初始化添加流表规则 |
| 测试步骤 | 1. 启动流表管理  2. 选择交换机，并选择删除所有流。  3. 单击更新，查看交换机下是否有流表 |
| 预期结果 | 交换机下不存在任何的流表 |

1. 更新流表

表格5- 更新流表

|  |  |
| --- | --- |
| 序号 | 13 |
| 名称 | 更新流表 |
| 预置条件 | 系统初始化添加流表规则 |
| 测试步骤 | 1. 启动流表管理  2. 选择交换机中的流表  3. 修改流表的参数值  4. 更新，重新选择修改的流表 |
| 预期结果 | 流表的内容被成功的修改 |

1. 寻找有效DENY规则

表格5- 初始有效DENY规则

|  |  |
| --- | --- |
| 序号 | 14 |
| 名称 | 初始有效DENY规则 |
| 预置条件 | 系统初始化添加的防火墙规则 |
| 测试步骤 | 1. 依次选择冲突检测，防火墙DENY规则  2. 查看显示的防火墙规则是否是有效的DENY规则 |
| 预期结果 | 可以找到正确的DENY规则 |

表格5- 动态生成有效DENY规则

|  |  |
| --- | --- |
| 序号 | 15 |
| 名称 | 动态生成有效DENY规则 |
| 预置条件 | 系统初始化添加的防火墙规则 |
| 测试步骤 | 1. 依次选择冲突检测，防火墙DENY规则  2. 记录当前的防火墙有效DENY规则  3. 添加如下防火墙规则  3. 单击防火墙DENY规则 |
| 预期结果 | 生成正确的防火墙DENY规则 |

1. 寻找FlowPath

表格5- 生成系统初始化的FlowPath

|  |  |
| --- | --- |
| 序号 | 16 |
| 名称 | 生成系统初始化的FlowPath |
| 预置条件 | 系统初始化添加的拓扑结构和流表规则 |
| 测试步骤 | 1. 依次选择冲突检测，shiftd-flowpaths  2. 查看生成的shifted-flowpaths |
| 预期结果 | 生成正确的shifted-flowpaths |

表格5- 动态生成FlowPath

|  |  |
| --- | --- |
| 序号 | 17 |
| 名称 | 动态生成FlowPath |
| 预置条件 | 系统初始化添加的拓扑结构和流表规则 |
| 测试步骤 | 1. 依次选择冲突检测，shiftd-flowpaths  2. 记录当前的shifted-flowpaths  3. 删除交换机中的流表  4. 查看生成的shifted-flowpaths |
| 预期结果 | 动态的生成正确的shifted-flowpaths |

1. 冲突检测

表格5- 生成系统初始化的冲突路径

|  |  |
| --- | --- |
| 序号 | 18 |
| 名称 | 生成系统初始化的冲突路径 |
| 预置条件 | 系统初始化添加的拓扑结构、流表规则和防火墙规则 |
| 测试步骤 | 1. 依次选择冲突检测，冲突路径列表  2. 查看生成的冲突路径 |
| 预期结果 | 生成正确的冲突路径 |

表格5- 动态生成冲突路径1

|  |  |
| --- | --- |
| 序号 | 19 |
| 名称 | 动态生成冲突路径 |
| 预置条件 | 系统初始化添加的拓扑结构、流表规则和防火墙规则 |
| 测试步骤 | 1. 依次选择冲突检测，冲突路径列表  2. 记录当前的冲突路径  3. 添加新的防火墙规则  4. 查看生成的冲突路径 |
| 预期结果 | 生成正确的冲突路径 |

表格5- 动态生成冲突路径2

|  |  |
| --- | --- |
| 序号 | 20 |
| 名称 | 动态生成冲突路径 |
| 预置条件 | 系统初始化添加的拓扑结构、流表规则和防火墙规则 |
| 测试步骤 | 1. 依次选择冲突检测，冲突路径列表  2. 记录当前的冲突路径  3. 删除交换机中的流表  4. 查看生成的冲突路径 |
| 预期结果 | 生成正确的冲突路径 |

1. 冲突解决

表格5- 在浏览器中查看冲突路径

|  |  |
| --- | --- |
| 序号 | 21 |
| 名称 | 在浏览器中查看冲突路径 |
| 预置条件 | 系统初始化添加的拓扑结构、流表规则和防火墙规则 |
| 测试步骤 | 1. 依次选择冲突检测，防火墙DENY规则  2. 选择有冲突的DENY规则  3. 单击在浏览器中查看此路径 |
| 预期结果 | 正确显示冲突路径 |

表格5- 基于IP的冲突解决

|  |  |
| --- | --- |
| 序号 | 22 |
| 名称 | 基于IP的冲突解决 |
| 预置条件 | 系统初始化添加的拓扑结构、流表规则和防火墙规则 |
| 测试步骤 | 1. 依次选择冲突检测，防火墙DENY规则  2. 选择原地址为单个IP的冲突路径  3. 单击解决冲突 |
| 预期结果 | 正确解决冲突路径 |

表格5- 基于网段的冲突解决

|  |  |
| --- | --- |
| 序号 | 23 |
| 名称 | 基于网段的冲突解决 |
| 预置条件 | 系统初始化添加的拓扑结构、流表规则和防火墙规则 |
| 测试步骤 | 1. 依次选择冲突检测，防火墙DENY规则  2. 选择原地址为网段的冲突路径  3. 单击解决冲突 |
| 预期结果 | 正确解决冲突路径 |

1. 全局流路径

表格5- 系统初始全局流路径

|  |  |
| --- | --- |
| 序号 | 24 |
| 名称 | 系统初始全局流路径 |
| 预置条件 | 系统初始化添加的拓扑结构、流表规则 |
| 测试步骤 | 1. 启动SDNGuard，正确添加流表规则  2. 点击全局流路径 |
| 预期结果 | 正确生成系统全局流路径 |

表格5- 在浏览器中查看全局流路径

|  |  |
| --- | --- |
| 序号 | 25 |
| 名称 | 在浏览器中查看全局流路径 |
| 预置条件 | 系统初始化添加的拓扑结构、流表规则 |
| 测试步骤 | 1. 启动SDNGuard，正确添加流表规则  2. 点击全局流路径  3. 点击在浏览器中查看全局流路径 |
| 预期结果 | 正确显示统全局流路径 |

1. 测试结果

以下测试结果均在正常启动floodlight、SDNGuard和mininet，正确的添加了防火墙规则和流表的前提下进行测试得到的结果。

1. 防火墙规则管理
2. 显示防火墙规则

系统初始化的防火墙规则信息。



图6- 初始化的防火墙规则信息

选择ruleid为1824767927的防火墙规则，单击删除选中规则，删除该防火墙规则。系统提示防火墙规则删除成功。

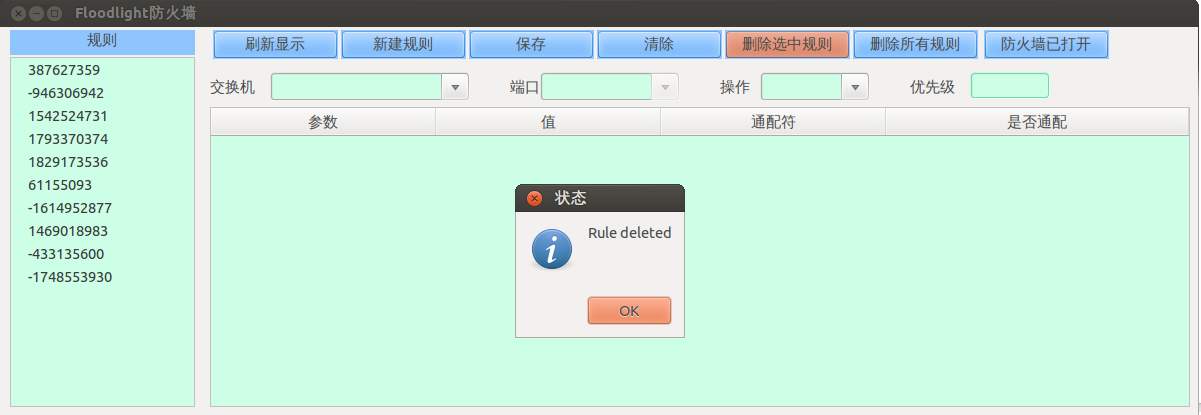


图6- 防火墙规则删除成功

1. 添加防火墙规则

选择新建规则，填写src-ip、dst-ip、操作和优先级，单击保存。系统提示防火墙规则已添加。



图6- 3添加防火墙规则

查看添加的防火墙规则，选择rulrid为421762373的防火墙规则。

图6- 4查看新添加的防火墙规则

1. 删除防火墙规则

选择ruleid为421762373的防火墙规则，单击删除选中规则。系统提示规则已删除。



图6- 删除防火墙规则

单击删除所有规则，点击yes，删除系统所有的防火墙规则。



图6- 提示删除所有防火墙规则

删除所有防火墙规则。



图6- 删除所有防火墙规则成功

1. 修改防火墙规则

选择ruleid为1297349818的防火墙规则，将其操作改为DENY，单击保存。系统生成ruleid为1612153955的防火墙规则。删除ruleid为1297349818的防火墙规则即可。

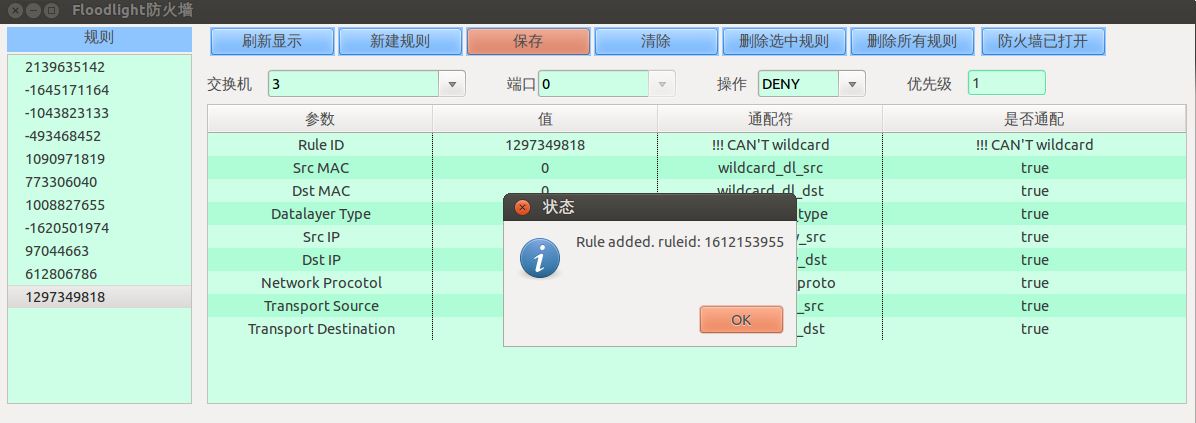


图6- 8修改防火墙规则

1. 防火墙打开和关闭

在防火墙已打开的情况下，由于防火墙规则禁止h1和h4通信，因此h1和h4无法通信。注：为确保防火墙起作用，要删除交换机中的所有流表。

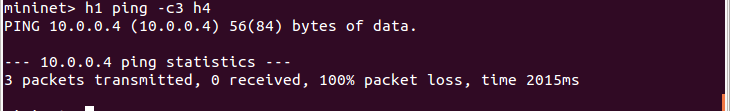


图6- h1和h4无法通信

关闭防火墙，测试h1和h4可以通信。

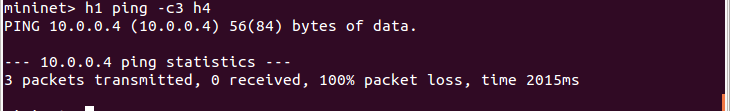


图6- h1和h4可以通信

1. 流表管理
2. 显示流表

系统初始化的流表。下图显示的是交换机00：00：00：00：00：00：00：03中的流表flow-mod-101中的内容。

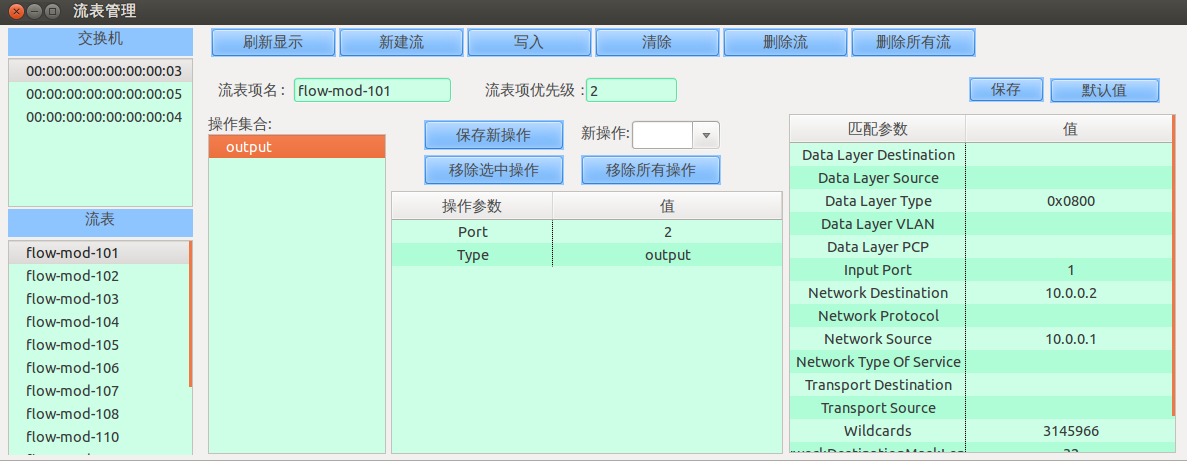


图6- 初始流表

删除流flow-mod-101后的流表，被删除的流表不再显示。



图6- 删除流表

1. 添加流表

单击新建流，填写流表参数，选择动作并保存新动作，最后单击写入。系统提示flow-mod-1020 成功写入交换机。



图6- 添加流表

1. 删除流表

选择交换机00：00：00：00：00：00：00：03中的流表flow-mod-102，单击删除流，删除该流表。

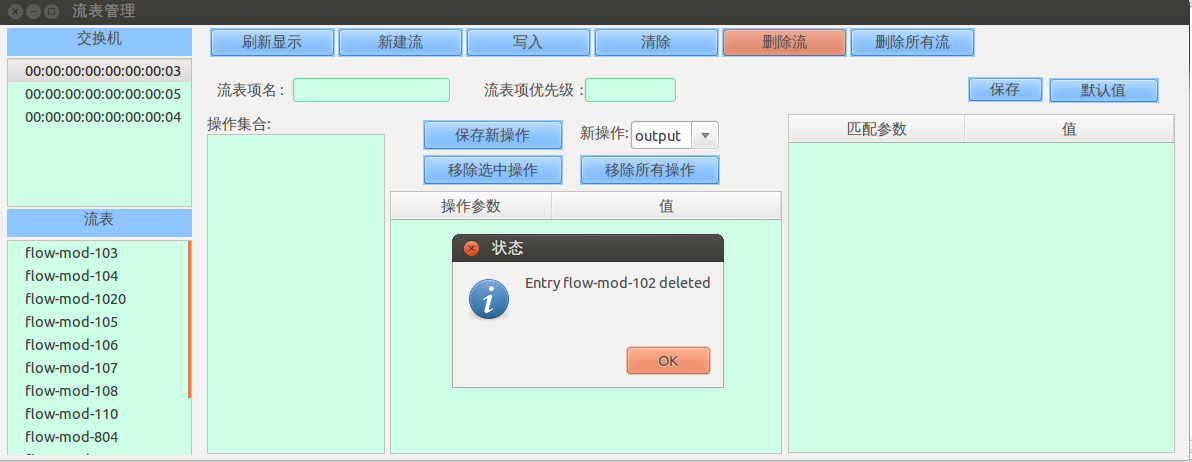


图6- 删除流表

选择交换机00：00：00：00：00：00：00：03中的流表flow-mod-102，单击删除所有流，删除该交换机下所有的流表。



图6- 提示删除所有流表

选择Yes，00：00：00：00：00：00：00：03交换机流表为空。



图6- 删除所有流表成功

1. 更新流表

选择交换机00：00：00：00：00：00：00：04中的流表flow-mod-204，将其操作集合中的port改为1，单击保存新操作，单击写入更改流表flow-mod-204的port值。

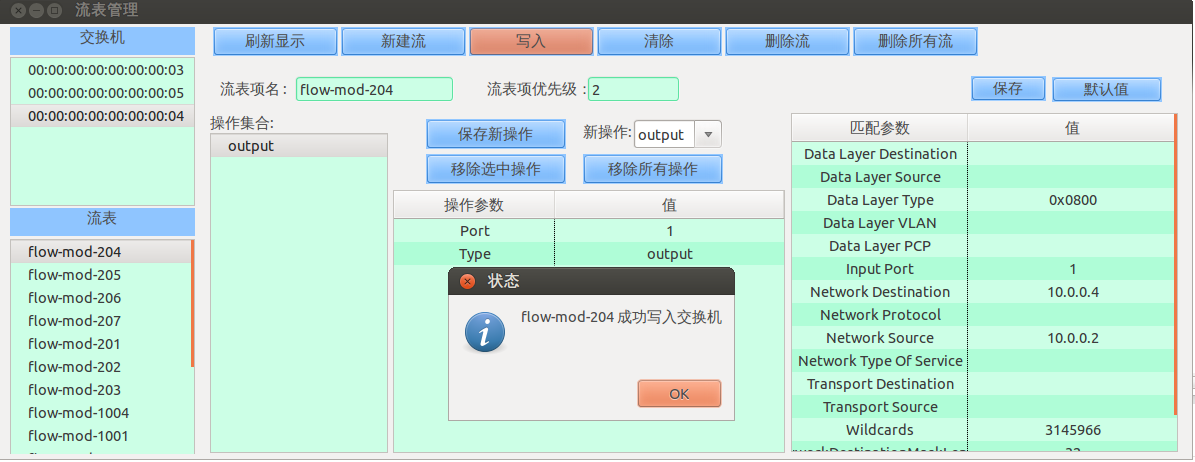


图6- 更新流表

1. 有效DENY规则

系统初始化的有效DENY规则。



图6- 18初始有效DENY规则

ruleid为-2023575572的防火墙规则，刷新得到新的有效DENY规则。



图6- 删除防火墙规则后的有效DENY规则

1. 寻找FlowPath

系统初始化shiifted-flowpath。

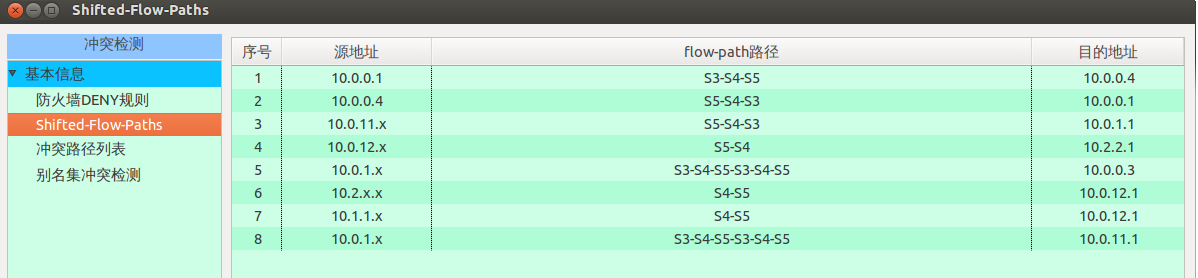


图6- 初始shifted-flowpaths

shifted-flowpaths是否是正确的，下面让我们通过试验来验证。

从图6-20中我们可以看到存在h1-s3-s4-s5-h4这样一条shifted-flowpaths。让主机h1直接ping主机h4，发现无法通信。如图6-21。

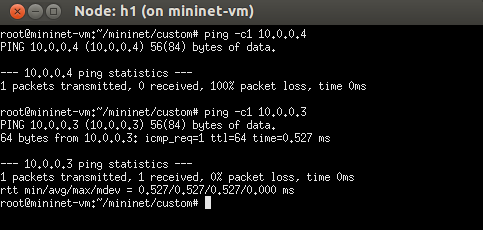


图6- 测试h1和h4通信

这是因为防火墙规则禁止主机h1和h4之间的通信，当h1向h4发送数据包时，由于没有匹配的流表，该数据包被送往控制器，控制器通过决策发现通信违反防火墙规则，因此向交换机下发drop命令，让交换机直接将该数据包丢弃。如图6-22。其中1718数据包是h1向h4发送的ICMP数据包，该数据报被交换机以packet-in的形式发送到控制器。控制器通过决策下发packet-out消息——1720数据包，数据包中没有指定output动作，默认是丢弃数据包。交换机收到1720数据包，根据数据包的信息添加了drop流表，丢弃所有的从h1发往h4的数据包。因此h1和h4便无法通信了。

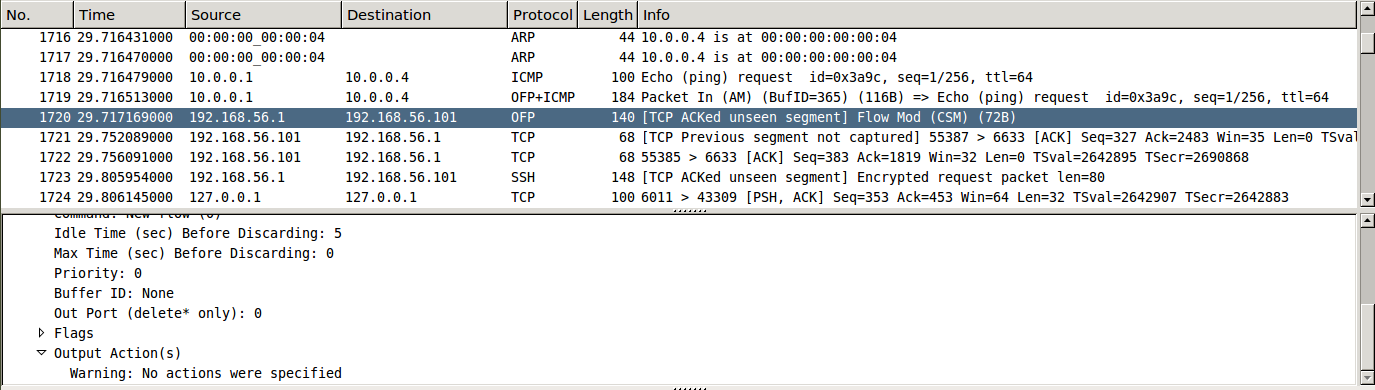


图6- 抓取数据包1

在图6-21中的第二条ping命令是ping –c3 10.0.0.3，发现可以ping通。但是h1究竟是和h3（IP=10.0.0.3）通信还是和其他的主机通信，抓取数据包来验证。

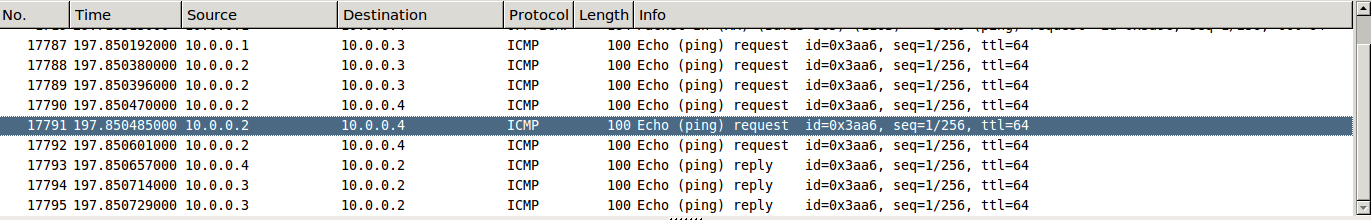


图6- 抓取数据包2

观察图6-23发现ICMP数据包的源地址不是固定的10.0.0.1，目的地址也不是固定的10.0.0.3。但是，ICMP数据包最终到达了主机h4，并且h4 发送了响应的ICMP数据包。说明该PING命令测试的实际是主机h1和主机h4之间的通信。为什么h1向h3发送ICMP请求数据包最终到达了主机h4呢？其实这就是shifted-flowpaths。主机h1向主机h3发送的ICMP数据包在交换机s3中，源地址被修改为10.0.0.2。数据包到达交换机s4时目的地址被修改为10.0.0.4。到达交换机s5是ICMP数据包的源地址是10.0.0.2目的地址是10.0.0.4，于是该数据报被交换机s5转发到主机h4。h4收到请求数据包后，向主机h2发送响应数据包。响应数据包经过和请求数据包相反的修改过程最终到达了主机h1，从而完成了通信。但是，这样的通信并不是直接的通信，而是修改数据包的IP地址间接地通信。这样的通过信路径便是shifted-flowpaths。其他的路径的通信过程和该路径相似。

选择删除交换机s3中的流表flow-mod-6动态生成shifted-flowpath。

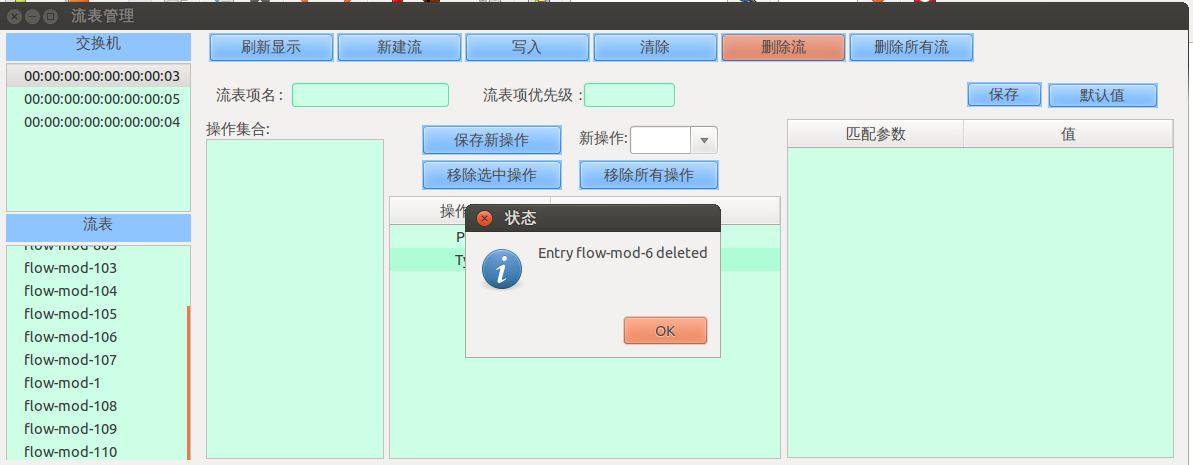


图6- 删除流表

被删除的流表项是构成改路径的众多流表中的一条，删除该流表后，路径便不复存在了。在新的shifted-flowpaths中没有10.0.0.4-s5-s4-s3-10.0.0.1。

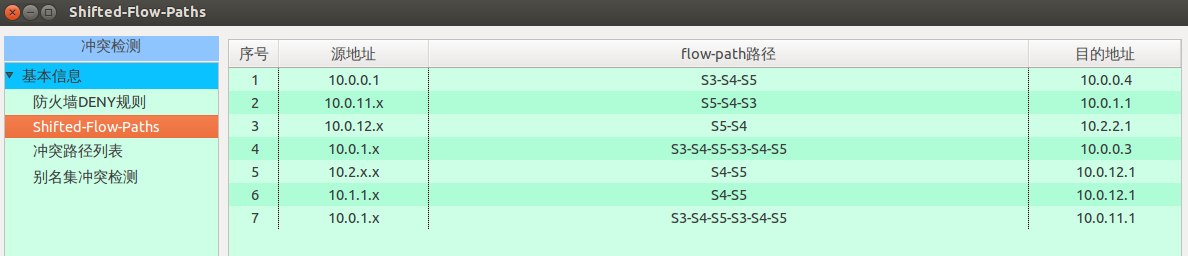


图6- 动态生成shifted-flowpath

1. 冲突检测

系统初始化冲突路径列表。

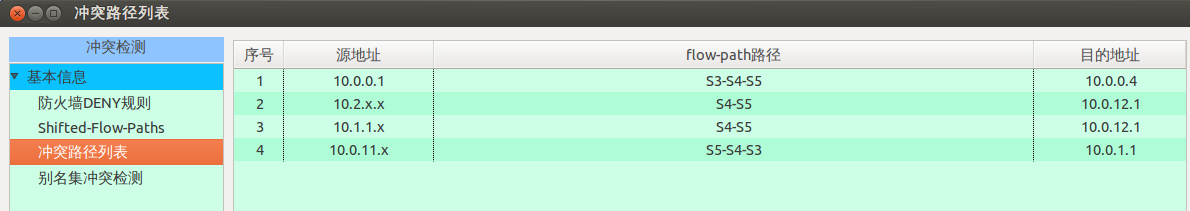


图6- 26初始冲突路径

接下来我们验证10.0.0.1-s3-s4-s5-10.0.0.4是否是冲突路径，即h1和h4可以通信但是违反了防火墙规则。

在图6-27中，主机h4监听来自端口6666的连接信息，主机h1向主机h4发出连接请求。连接失败，“Connection timed out”。正如在6.4中分析的那样，由于防火墙规则禁止主机h1和主机h4之间的通信，主机h1发送的请求数据包被交换机s3丢起了，因此连接失败。如果我们让主机h1向主机h3发出连接请求，发现主机h1最终链接的是主机h4，因为从终端h1中输入的文字都可以在h4的终端上显示，说明h1和h4是可以通信的。通信过程在6.4中进行了解释。综合以上分析可知shifted-flowpaths（h1-s3-s4-s5-h4）是违反防火墙规则的，该路径是冲突路径。列表中其他冲突路径的验证过程与之类似。

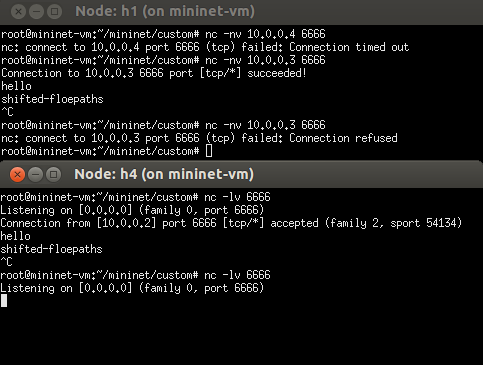


图6- 27 h1和h4通信测试

添加新的防火墙规则 src-ip=10.0.12.0/24，dst-ip=10.2.2.1/32，action=DENY，priority=1。可以看到产生了新的冲突路径10.0.12.x-s5-s4-10.2.2.1 。

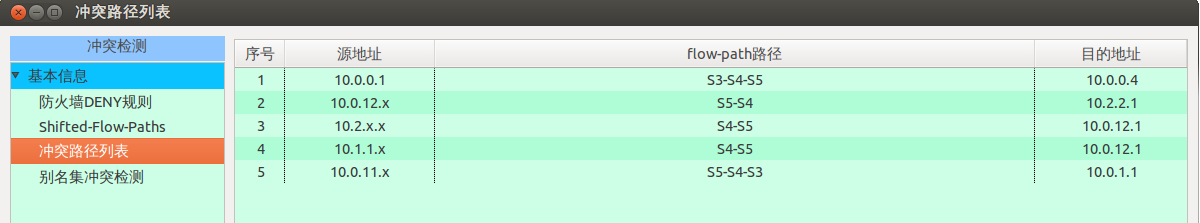


图6- 生成新冲突路径

新产生的冲突路径究竟是否是正确的，类似上述验证方法让我们对其进行验证。见图6-29。主机h13（IP=10.2.2.1）监听端口6666的信息，主机h7（IP=10.0.0.12.1）向IP为10.1.1.1的主机发出监听请求。主机h7和IP为10.1.1.1的主机连接成功，主机h13和IP为10.0.0.3的主机连接成功。但是主机h7发出的信息都可以在主机 h13上显示，说明主机h7实际上是和主机h13连接的，该连接违反了防火墙规则，因此该路径是冲突路径。

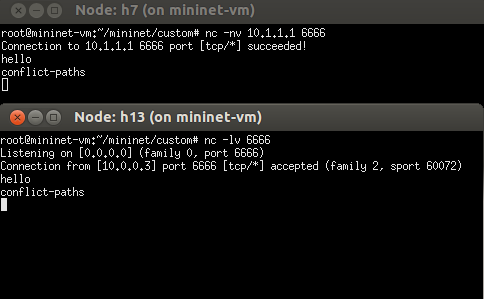


图6- 测试h7和h13通信1

主机h7向主机10.1.1.1发出的连接请求在交换机s5中源地址被修改为10.0.0.3，修改后的数据包到达交换机s5后目的地址被修改为10.2.2.1。数据包当前的目的地址恰好是主机h13的IP地址。因此主机h1发送的数据包最终到达了主机h13。删除交换机s5中的流表flow-mod-1003后，连接无法建立，因为主机h1发送的请求这时真正的到达了主机10.1.1.1，而目的主机没有打开端口6666，因此连接被拒绝。见图6-30。

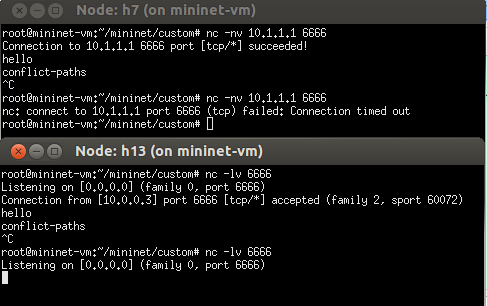


图6- 测试h7和h13通信2

1. 冲突解决
2. 在浏览器中查看冲突路径。

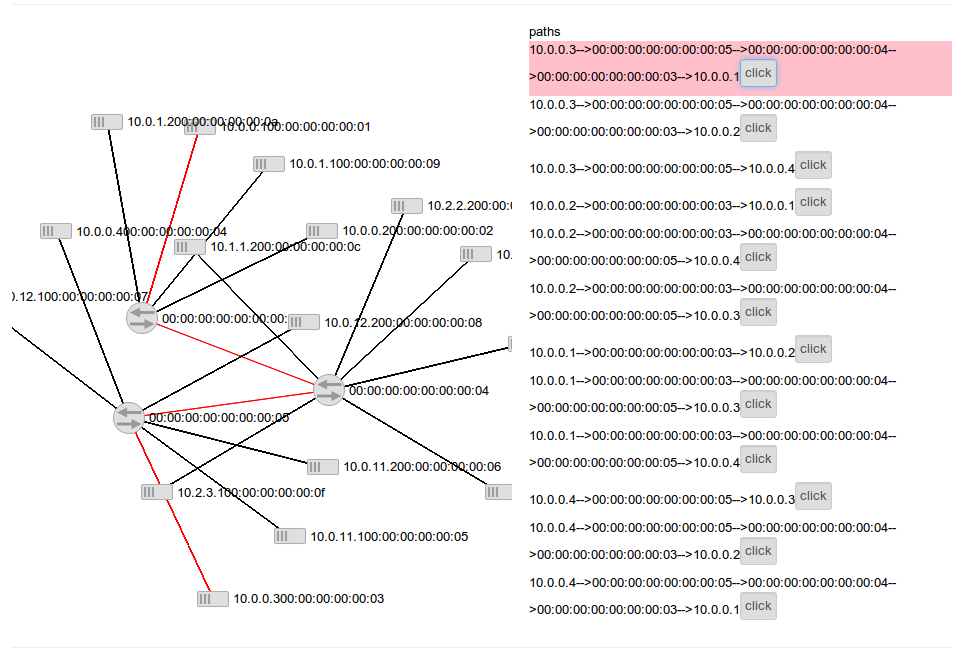


图6- 在浏览器中查看冲突路径

1. 基于单个IP的冲突解决。

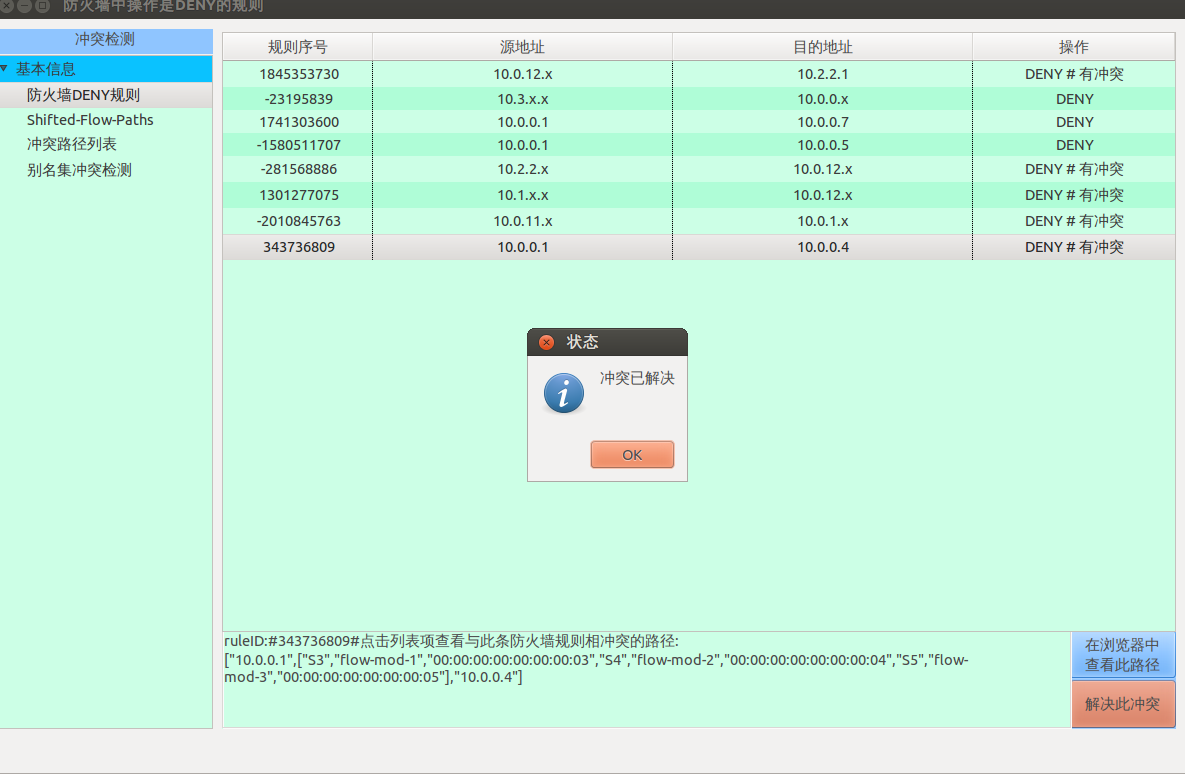


图6- 基于单个IP的冲突解决

在前面我们已经证明了主机h1和主机h4之间是可以通信的，并且通信是违反防火墙规则的。选择ruleid为343736809的DENY规则，点击解决此冲突。冲突成功解决。此时再次测试发现主机h1和h4无法通过冲突路径进行通信，因为构成该冲突路径的所有流表项都被冲突解决删除了。查看交换机s3发现赵不到流表flow-mod-1，同样交换机s4和s5中也找不到流表flow-mod-2和flow-mod-3。图6-33是h1和h4之间通信的测试，冲突未解决之前可以通信，冲突解决之后发现无法通信，说明冲突解决成功。

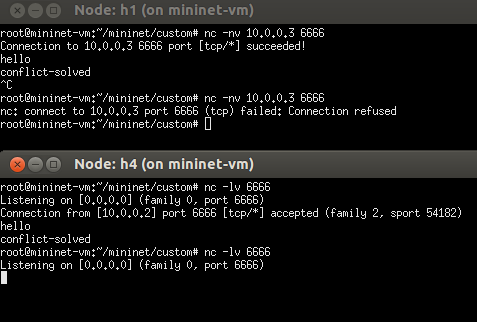


图6- 测试冲突解决是否成功

1. 基于网段的冲突解决。

根据DENY规则的源地址和冲突路径的源地址的范围大小的不同，基于网段的冲突解决分为两种不同的情况。DENY规则的源地址大于等于防火墙规则的源地址时，冲突解决的策略和基于IP的情况相同，都是删除构成冲突路径的所有流表。查看交换机发现流表都被删除。测试结果的验证情况和基于IP的相同因此不再赘述。

DENY规则源地址大于冲突路径源地址。可以成功解决冲突。

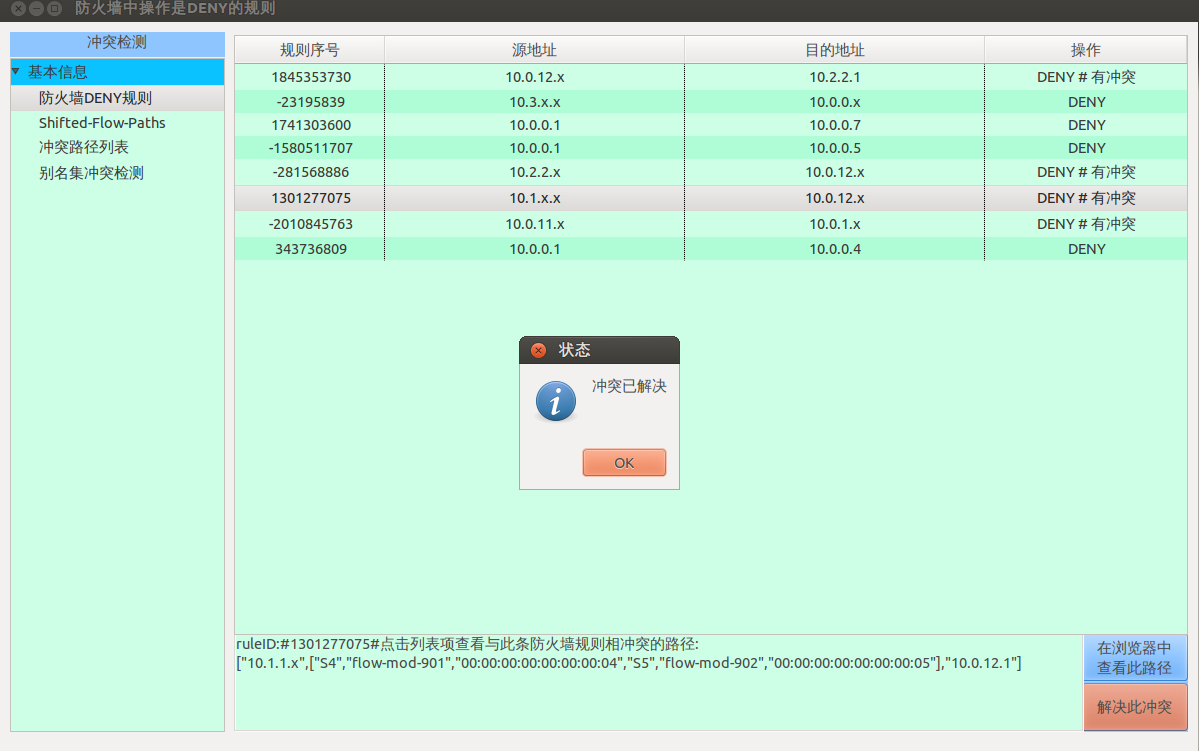


图6- DENY规则源地址大于冲突路径源地址

DENY规则源地址等于冲突路径源地址，可以解决冲突路径。

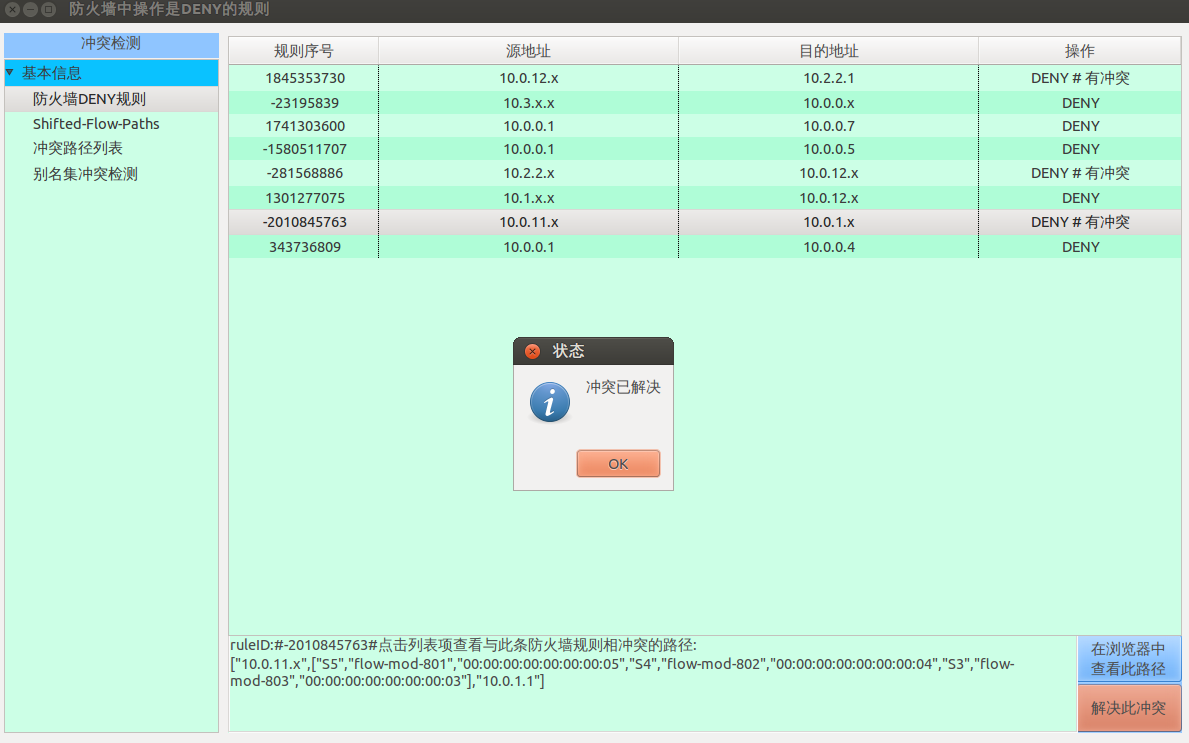


图6- DENY规则源地址等于冲突路径源地址

DENY规则源地址小于冲突路径源地址，以防火墙规则“10.2.2.x --DENY-- 10.0.12.x”为例。点击此防火墙规则，可以在界面下方看到构成该冲突路径的流和经过的交换机，如图6-36



图6- DENY规则源地址小于冲突路径源地址

在流表管理中可以查看上述的流是怎样绕过防火墙的。

在Mininet中用dump命令查看主机信息：  
mininet> dump

<RemoteController c0: 192.168.56.1:6633 pid=12919>

<OVSSwitch s3: lo:127.0.0.1,s3-eth1:None,s3-eth2:None,s3-eth3:None,s3-eth4:None,s3-eth5:None pid=12944>

<OVSSwitch s4: lo:127.0.0.1,s4-eth1:None,s4-eth2:None,s4-eth3:None,s4-eth4:None,s4-eth5:None,s4-eth6:None,s4-eth7:None,s4-eth8:None pid=12949>

<OVSSwitch s5: lo:127.0.0.1,s5-eth1:None,s5-eth2:None,s5-eth3:None,s5-eth4:None,s5-eth5:None,s5-eth6:None,s5-eth7:None pid=12954>

<Host h1: h1-eth0:10.0.0.1 pid=12926>

<Host h2: h2-eth0:10.0.0.2 pid=12927>

<Host h3: h3-eth0:10.0.0.3 pid=12928>

<Host h4: h4-eth0:10.0.0.4 pid=12929>

<Host h5: h5-eth0:10.0.11.1 pid=12930>

<Host h6: h6-eth0:10.0.11.2 pid=12931>

<Host h7: h7-eth0:10.0.12.1 pid=12932>

<Host h8: h8-eth0:10.0.12.2 pid=12933>

<Host h9: h9-eth0:10.0.1.1 pid=12934>

<Host h10: h10-eth0:10.0.1.2 pid=12935>

<Host h11: h11-eth0:10.1.1.1 pid=12936>

<Host h12: h12-eth0:10.1.1.2 pid=12937>

<Host h13: h13-eth0:10.2.2.1 pid=12938>

<Host h14: h14-eth0:10.2.2.2 pid=12939>

<Host h15: h15-eth0:10.2.3.1 pid=12940>

<Host h16: h16-eth0:10.2.3.2 pid=12941>

可见h13的IP地址为10.2.2.1，h7的IP地址为10.0.12.1，满足防火墙规则（10.2.2.x --DENY-- 10.0.12.x）禁止的路径。用xterm命令打开h13 和 h7主机，以nc命令验证h13与h7之间是否可以通信，具体过程如下：

1. 在h7上打开4444端口监听；
2. 在h13上请求访问h3（10.0.0.3）的4444端口（这里解释一下为什么访问10.0.0.3主机，而不是h7主机的IP 10.0.12.1。如前文所说，绕过此防火墙规则的shifted-flow-path为["10.2.x.x",["S4","flow-mod-1001","00:00:00:00:00:00:00:04","S5","flow-mod-1002",

"00:00:00:00:00:00:00:05"],"10.0.12.1"]，构成这条路径的第一条流为flow-mod-1001，在流表管理中可见该流的操作是匹配源IP为10.2.x.x、目的IP为10.0.0.x的数据包，然后将其源IP改为10.1.1.1，从交换机2号端口转发出去。因此，h13假装访问10.0.0.3，最终数据包能够绕过防火墙到达10.0.12.1）；

1. 查看h7能否收到h13发来的信息。

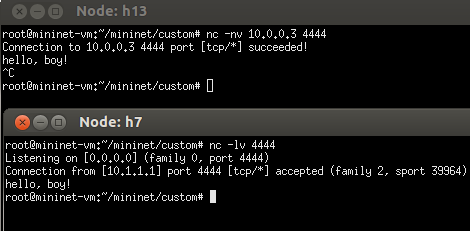


图6- 验证是否存在冲突

可见h7收到h13发来的信息，防火墙规则被绕过，检测出来的冲突路径确实存在。点击下方的“在浏览器中查看冲突路径”，可以在浏览器中看到如下图所示的冲突路径：

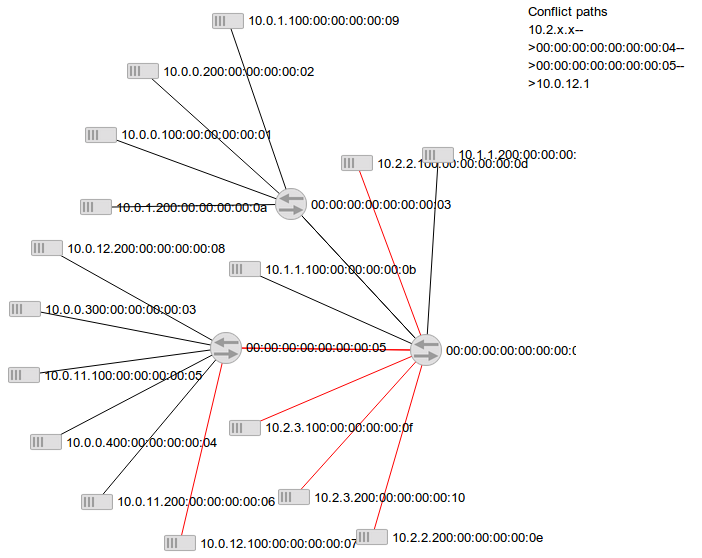


图6- 在浏览器中查看冲突路径

点击“解决此冲突”按钮，可以解决该冲突路径。下图是冲突解决算法生成的阻断流表，通过将该流表写入相应的交换机，阻断存在的冲突路径。

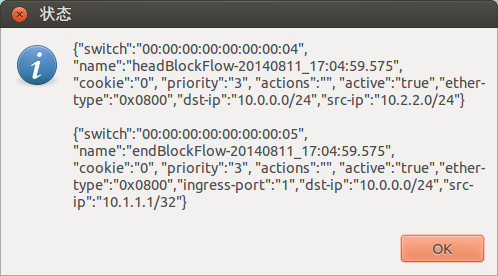


图6- 插入的阻断流表

头阻断流和尾阻断流成功写入交换机，冲突解决。在界面中可见上述冲突已经解决。在Mininet中验证冲突是否解决。

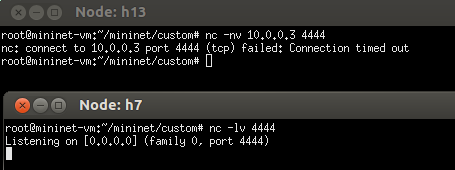


图6- 验证冲突是否解决

从图中可见，h13与h7已经不能通信（连接超时），冲突解决。

1. 全局流路径
2. 在浏览器中查看全局流路径

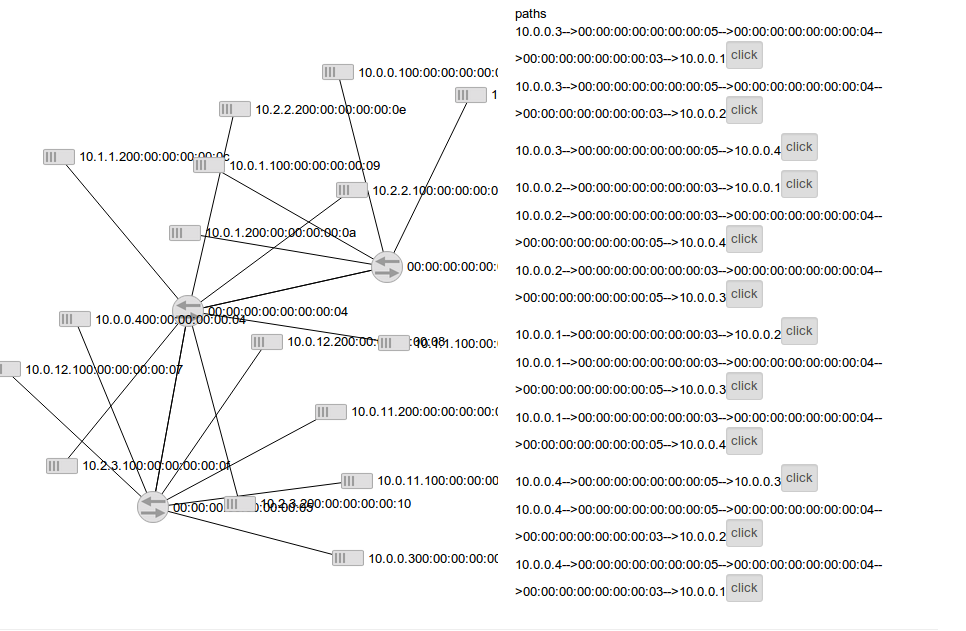


图6- 在浏览器中查看全局流路径

1. 生成系统初始全局流路径

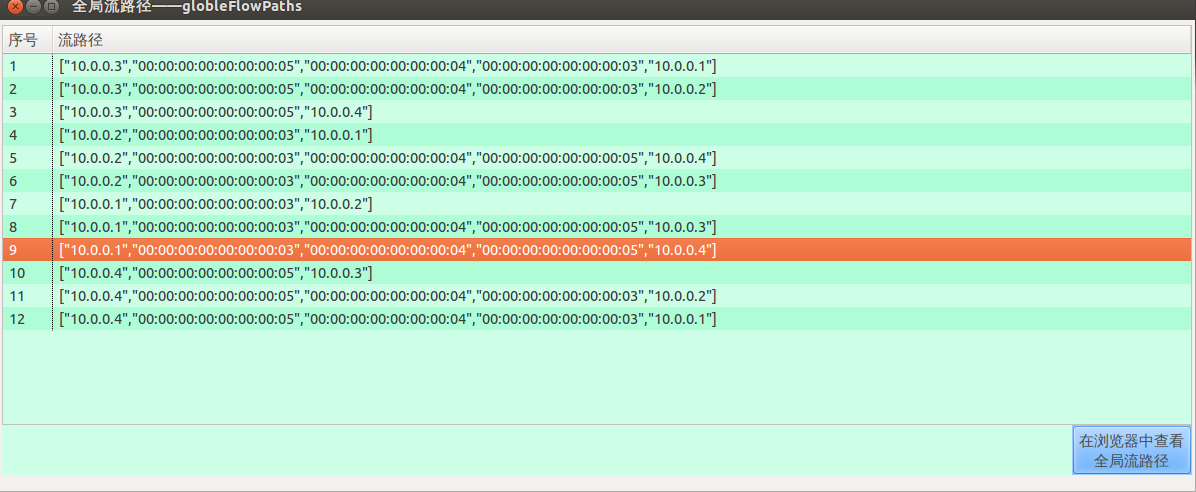


图6- 42生成系统初始全局流路径

1. 性能测试

测试拓扑结构为10个交换机40个主机，拓扑结构如下图所示。防火墙规则见表格5-1。流表规则见附件yoza.py。表格6-1是全局路径建立、冲突检测和冲突解决所需的时间，测试数据分为5组，每一组结果求平均值。其中“DENY>冲突路径”表示DENY规则源地址范围小于冲突路径规则源地址范围，“DENY=冲突路径”和“DENY<冲突路径”表示的内容与之类似。

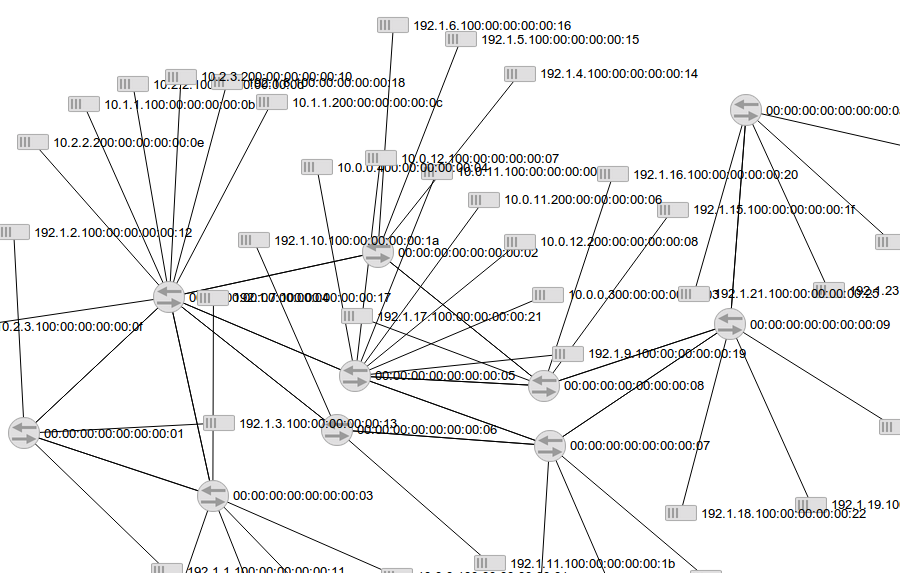


图6- 43性能测试的拓扑结

表格6- 性能测试结果

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | 全局路径建立时间 | 冲突检测时间 | 冲突解决 | | | |
| 基于单个IP | DENY>冲突路径 | DENY=冲突路径 | DENY<冲突路径 |
| 第一组 | 187ms | 57ms | 244ms | 170ms | 210ms | 152ms |
| 第二组 | 90ms, | 34ms | 247ms | 174ms | 225ms | 153ms |
| 第三组 | 275ms | 90ms | 238ms | 155ms | 210ms | 135ms |
| 第四组 | 229ms | 76ms | 215ms | 145ms | 186ms | 131ms |
| 第五组 | 90ms | 98ms | 217ms | 142ms | 192ms | 136ms |
| 平均值 | 174.2ms | 71ms | 232.2ms | 157.2ms | 204.6ms | 141.4ms |
| 性能要求 | <=60s | <=30s |  |  |  |  |

1. 测试总结
2. 防火墙规则管理

防火墙规则管理的测试重点是防火墙规则的显示、添加、删除、更新和防火墙的打开和关闭。内容是防火墙规则显示是否准确，是否可以动态的显示防火墙规则的变化。添加、删除或更新防火墙规则能否生效。防火墙的打开功能是否可用。在测试用例的设计中，分别针对以上各个测试重点进行了测试，测试的结果也都达到了预期。说明系统的防火墙规则管理的功能达到了预期的设计。

1. 流表管理

流表在SDN网络数据包的转发中扮演着重要的作用，对于网络的正常工作是必不可少的。因此方便的流表管理工具对于网络的管理是不可或缺的帮手。流表管理主要的内容是流表的显示，添加、删除或更新流表等。对于这些内容，我们设计了相应的测试用例用于测试流表管理是否正常的工作。测试的结果也和我们的预期相符合，说明流表管理是按照我们的预想工作的。

1. 有效DENY规则

控制器中存在许多的防火墙规则，由于优先级的关系其中一些优先级较低防火墙规则无法起作用。找到有效的DENY规则，可以提高冲突检测的效率。测试生成系统初始化的防火墙规则，和动态修改防火墙规则时系统能否生成正确的有效DENY规则。测试结果均与预期的结果相符。

1. FlowPath探测
2. 冲突检测

冲突检测是找出和防火墙规则相违背的FlowPath，目的是为冲突解决提供帮助。系统初始化的冲突检测和动态修改系统的防火墙规则或流表时的冲突检测功能均得到了我们预期的结果，

1. 冲突解决

对于找到的冲突路径，冲图解绝的目的是避免路径和防火墙规则相违背，对此我们可以修改路径。主要有两种方式解决冲突，一是删除所有与冲突路径相关的流表，另一种是在冲突路径的头尾交换机中插入阻断流表。前一种是基于IP的冲突路径和冲突路径源地址小于等于防火墙规则源地址范围的解决办法，后一种是基于网段的冲突路径源地址大于防火墙规则源地址范围的冲突的解决办法。在测试用例的设计中分别对以上几种情况进行了测试，测试结果也与预期的结果相符合。说明冲突解决功能到达了预想的功能要求。

1. 全局流路径

全局流路径是SDN网络中所有静态添加的交换机流表构成的数据包转发路径，找出全局流路径有助于冲突检测和冲突解决。测试结果显示无论是对系统初始化的全局流路径，还是动态修改后产生新的全局流路径，均得到了预期的正确的结果。说明全局流路径的设计达到了预期的设计目标。

1. 性能测试

通过对系统性能预期要求和实际系统性能对比发现：在给定的足够大的数据量的情况下，系统均能在预期要求的时间内完成功能（详见6.8性能测试）。测试结果说明系统的性能符合系统设计的预期要求。