基于SDN的网络安全策略自动迁移机制

# 摘要

1. **绪论**
   1. **研究背景**

本小节主要介绍

1. 网络安全设备越多，有关安全设备与安全策略的部署和管理就越复杂。
2. 网络管理员在手动配置相关安全策略时，容易出现错配或漏配的现象。
3. 随着虚拟技术的广泛应用，网络拓扑日趋动态变化，使得安全策略的迁移不易实施。
4. 软件定义网络成为解决网络僵化问题的新途径。
   1. **国内外研究现状**

本小节主要介绍

1. 安全点的概念

1. 传统网络中安全策略迁移研究现状
2. 软件定义网络与OpenFlow协议
3. 软件定义网络中安全策略迁移研究现状
   1. **研究内容**

本小节主要介绍

1. 通过实验验证交换机的选择的重要性
2. 基于安全点的交换机选择算法的研究与设计
3. 基于安全策略的流表生成算法的研究与设计
   1. **论文组织结构**

本小节简述论文各章节的主要内容。

* 1. **本章小节**

本小节主要对本章内容进行简要总结。

1. **基于安全点选择交换机的重要性**

**2.1 安全点**

本节主要介绍

1. 安全设备部署的现状
2. 安全点的提出

在文献A Formal Framework for Network Security Design Synthesis[C]中，作者提出一个综合网络安全配置的自动化框架。该框架在综合考虑网络拓扑、安全需求、可用性约束和设备部署成本约束的条件下，采用高效的自动化算法，能够获得网络安全设备的最优放置位置。本文称该位置为“安全点”。

**2.2 实验验证“围绕安全点选择合适交换机的重要性”**

本节主要通过实验，来描述“交换机的选择，会对网络数据流传递产生一定影响”，因此得出结论要选择合适的交换机。

**2.2.1实验平台**

1.软硬件环境

2.实验拓扑及安全点

3.实验安全策略

**2.2.2单播通信实验**

在点对点的通信模式下，主要是针对在流量入口端选择交换机和流量出口端选择交换机两种选择方式下，进行正常请求和非正常请求同时访问的实验。

为了更好的模拟真实主机间的交互，实验对正常请求和非正常请求访问模式分成了5组类型：（1）组1是两种请求的源主机在一个交换机上；（2）组2是两种请求的源主机不在一个交换机上；（3）组3是两种请求的目的主机在一个交换机上；（4）组4是两种请求的目的主机不在一个交换机上；（5）组5是两种请求的源主机和目的主机均不在一个交换机上。

针对5组访问类型，进行网络数据包的丢包率和非正常数据包的拦截率的统计。见表1。

表1

**2.2.3多播通信实验**

针对多播通信模式，选择流量入口端的交换机下发流表项是不可取的。因为如果在入口端把流量拦截，那么正常流量也因此被拦截。因此，在这种通信模式下，主要是针对在流量分叉处选择交换机和在流量出口端选择交换机两种选择方式下，进行正常请求和非正常请求同时访问的实验。

对实验结果进行网络数据包的丢包率和非正常数据包的拦截率的统计。见表2.

表2

**2.2.4实验结果分析**

由上述实验可得出，围绕安全点进行OpenFlow交换机选择时，应最小化数据流的非安全传递路径。

**2.3 本章小节**

本小节主要对本章内容进行简要总结。

1. **基于安全点的交换机选择算法的研究与设计**

**3.1问题定义**

本小节主要介绍

对于真实的网络拓扑，通信流是双向的。因此，我们使用无向图来模拟网络拓扑。在本文中，交换机的选择包括permit规则的交换机选择算法和deny规则的交换机选择算法两部分。Deny规则的交换机选择，是从源节点s到不可访问的目的节点t（t可以为一个集合）之间，找到距离源节点s最近且位于安全点一侧（左或者右）的交换机节点。Permit规则的交换机选择，（有待解决） 。

定义1：令G =（V，E）是无向图。 G中的路径p：v->w（“v->w”表示从v到w的路径）是从v到w前进的节点和边的序列，并且其所有节点是不同的。如果所有节点都是不同的，成为简单路径。从源节点s到目的节点ti（ti∈目的节点集合={t1,t2……tn}）的所有简单路径属于称为asp（s，t）的路径集合。

定义2：如果G是无向图，从源节点s出发广度优先遍历图G，建立以s为根，以目的节点ti（ti∈目的节点集合={t1,t2……tn}）为叶子的一颗生成树switch\_Tree。

定义3：设w是switch\_Tree树中的一个节点，由w以及w的所有后代导出的子树w\_Subtree，称为switch\_Tree的子树，其中w是子树的根。

定义4：令G =（V，E）是无向图。在G中某相邻两个节点w1和w2之间有一个安全点，则称<w1~w2>为在w1和w2之间的安全点。

**3.2 子树的分类与合并**

**3.2.1 子树的分类**

目的主机分为两种，源主机可访问的节点，和源主机不可访问的节点

根据目的主机的不同，可以将根为s的子树类型分为以下三种：

A. 子树的叶子节点是一个或多个不可访问的主机节点。

B. 子树的叶子节点是一个或多个可访问的主机节点。

C. 子树的叶子节点既有不可访问的主机节点，也有可访问的主机节点。

**3.2.2 子树的合并**

根据子树类型的不同，子树向上合并分三种情况：

1. 当子树的叶子节点仅有不可访问的主机节点时，子树合并方式见图a 。其中ChildNodeFlag=1表示后继仅有不可访问的节点。

图a

1. 当子树的叶子节点仅有可访问的主机节点时，子树合并方式见图b。其中ChildNodeFlag=2表示后继仅有可访问的节点。

图b

1. 当子树的叶子节点既有可访问的主机节点，也有不可访问的主机节点时，子树合并方式见图c。其中，ChildNodeFlag=3表示后继既有可访问的节点，也有不可访问节点。



图c

**3.3 交换机选择算法的描述**

本节主要介绍交换机选择算法的具体实现思路，并结合示例进行说明。

**3.4交换机选择算法的实验对比**

本节将算法与其他算法(还在查找)进行对比实验。

**3.5 本章小节**

本小节主要对本章内容进行简要总结。

1. **基于安全策略的流表生成算法**

**4.1 算法描述**

本节主要介绍安全策略的流表生成算法的具体实现思路，并结合示例进行说明。

**4.2 基于安全点的安全策略自动部署实验**

本节主要通过实验验证，围绕安全点选择交换机，并将安全策略映射成流表自动部署到网络交换机的正确性。

**4.2.1实验平台**

1.软硬件环境

2.实验拓扑及安全点

3.实验安全策略

**4.2.2 实验步骤与结果分析**

本小节主要对实验步骤进行说明，并对实验结果作出分析。

**4.3 本章小节**

本小节主要对本章内容进行简要总结。

1. **总结与展望**