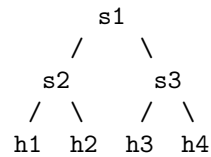


SDN Network ACL Implementation Project

Overview

This project implements Access Control List (ACL) rules in a Software-Defined Network using OpenFlow 1.3. The implementation focuses on controlling specific traffic types between hosts in a tree topology.

Network Topology



Components

- **Switches:** 3 OpenFlow 1.3 switches (s1, s2, s3)
- **Hosts:** 4 hosts (h1, h2, h3, h4)
- **Topology Type:** Tree topology with depth=2 and fanout=2
- **Links:**
 - s1-eth1 <-> s2-eth3
 - s1-eth2 <-> s3-eth3
 - s2-eth1 <-> h1-eth0
 - s2-eth2 <-> h2-eth0
 - s3-eth1 <-> h3-eth0
 - s3-eth2 <-> h4-eth0

Requirements

ACL Rules

Implement the following packet filtering rules: 1. Block ICMP packets from h1 to h4 2. Block TCP packets from h2 to h3 3. Block ICMP packets from h4 to h1 4. Block TCP packets from h3 to h2

Traffic Flow

- All other traffic not specified in ACL rules should flow normally
- ARP packets must be allowed for network discovery

Testing

Prerequisites

```
# Install required packages
sudo apt-get install mininet
```

```
sudo apt-get install openvswitch-switch
```

Test Commands

1. Start Mininet with custom topology:

```
sudo mn --custom topology.py --topo mytopo --controller remote --switch ovs,protocols=OpenFlow13
```

2. Test ICMP Connectivity:

```
mininet> h1 ping h4 # Should fail
mininet> h4 ping h1 # Should fail
mininet> h1 ping h2 # Should succeed
```

3. Test TCP Connectivity:

```
# Start TCP server on h3
mininet> h3 iperf -s &

# Test from h2 (should fail)
mininet> h2 iperf -c 10.0.0.3
```

4. Verify Flow Rules:

```
sudo ovs-ofctl -O OpenFlow13 dump-flows s1
sudo ovs-ofctl -O OpenFlow13 dump-flows s2
sudo ovs-ofctl -O OpenFlow13 dump-flows s3
```

Expected Results

- ICMP (ping) tests:
 - h1 h4: Blocked in both directions
 - All other ping combinations: Successful
- TCP tests:
 - h2 → h3: Connection refused
 - h3 → h2: Connection refused
 - All other TCP connections: Successful

Troubleshooting

- Check OpenFlow version: `sudo ovs-vsctl show`
- Verify switch connections: `mininet> net`
- Inspect flow tables: `sudo ovs-ofctl dump-flows <switch>`
- Check host connectivity: `mininet> pingall`

Additional Notes

- The implementation uses multiple flow tables
- Priority levels are used to ensure proper rule matching
- ARP packets are flooded to enable network discovery

- Default rules are set with lower priority