**PUNE INSTITUTE OF COMPUTER TECHNOLOGY,**

**DHANKAWADI PUNE-43.**

# *A*

# *Seminar Report*

# *On*

## SECURITY IN SOFTWARE DEFINED NETWORKS USING FIREWALL


SUBMITTED BY

**NAME:** Jagruti Rajendra Waghulde

**ROLL NO:** 3323

**CLASS:** TE III

GUIDED BY

**PROF. Sumit Shinde**


ISO 9001 : 2008 Certified

## COMPUTER ENGINEERING DEPARTMENT

## Academic Year:2016-17


**PUNE INSTITUTE OF COMPUTER TECHNOLOGY,**

**DHANKAWADI PUNE-43.**

# *CERTIFICATE*

ISO 9001 : 2008 Certified

*This is to certify that Miss. Jagruti Rajendra Waghulde*

*RollNo. 3323 a student of T.E. (Computer Engineering Department) Batch 2016-2017, has satisfactorily completed a seminar report on*

*"Security in Software Defined Networks using Firewall"*

*under the guidance of prof. Sumit Shinde towards the partial fulfillment of the third year Computer Engineering Semester II of Pune University.*

_____ _____

Prof. Sumit Shinde
**Internal Guide**

Dr. R.B. Ingle
**Head of Department,**
**Computer Engineering**

**Date:-**

**Place:- PICT, Pune.**

# SECURITY IN SOFTWARE DEFINED NETWORKS USING FIREWALL.


## ABSTRACT:

*Software Defined Network architecture decouples the network control and forwarding functions enabling the network control to become directly programmable and the underlying infrastructure to be abstracted for applications and network services.*

*Following includes the demonstration of a layer 2 firewall using a tree topology with POX Controller, a switch and three hosts. Implementation includes POX controller at control plane of the architecture using Mininet. The implemented code successfully controls flow of packets between hosts according to firewall rules.*

*Implementation also includes a zone-based firewall designed and Simulated in GNS3 using three routers, switches and underlaying hosts.*



## KEYWORDS:

*Software Defined Networking, SDN Security, SDN based firewall, POX, Mininet, Zone based Firewall.*


## INTRODUCTION:

SDN separates the control plane of networking device (switch/ router) from its data plane, making it possible to control, monitor, and manage a network from a centralized controller.

Network Security is an important issue of today‘s Networking. Recently, Software Defined Networking is an evolving technology that decouples the control from forwarding network devices like switches, routers, hubs etc. SDN splits data plane and control plane . It controls the flow of data through high level program. Since in SDN network control is done programmatically network security is more vital task .

Firewalls are essential components in a network that act as a first level of access control. It protects the local network from other hosts in Internet, which are not trustworthy. Packet filtering can be done at the different levels of the network layer.

A centralized SDN firewall, which centrally defines and enforces the firewall policy on top of a controller, can immediately enforce updated rules in the firewall policy to check security violations.

For increasing the security of SDN firewalls zone based firewalls can be used. Zone based Firewalls are used for stateful inspection of the traffic. Ordinary firewall rule sets are applied on a per-interface basis to act as a packet filter for the interface. In a zone-based firewall, interfaces are grouped into security “zones,” where each interface in a zone has the same security level.

## 1) MOTIVATIONAL SURVEY:

The programmability and centralized control of the network topology in SDN allow enterprises to incorporate various applications easily to improve efficiency, reduce complexity, streamline processes, and provide superior user experience.
The need of securing the network from malicious attacks as well as from viruses and worms lead to the introduction of firewalls in software defined networks

## 2) LITERATURE REVIEW:

One of the fundamental challenges of SDN is to build robust firewalls for protecting OpenFlow-based networks where network states and traffic are frequently changed.

An example of SDN firewall application has been introduced in pox controller where each packet-in behavior triggered by the first packet of a traffic flow which is matched against a set of existing firewall rules that allow or deny a flow at its ingress switch. This preliminary implementation of OpenFlow-based firewall application can examine flow packet violations when new flows come in the network but it cannot check flow policy violations with respect to dynamic network policy updates.

To build robust firewall, Alaauddin Shieha introduce FLOWGUARD , is a comprehensive framework, to facilitate accurate detection as well as effective resolution of firewall policy violations in dynamic OpenFlow-based networks.when network states are updated, FLOWGUARD checks network flow path spaces to detect firewall policy violations. In addition, with the help of several innovative resolution strategies designed ,it conducts automatic and real-time violation resolutions for diverse network update situations. ALAAUDDIN SHIEHA also implement his framework and demonstrate the efficiency of the proposed detection and resolution approaches in FLOWGUARD through experiments with the help of a real-world network topology.

Extract from an IEEE paper:

Building Firewall over the Software-Defined Network Controller : Written by Michelle Suh, Sae Hyong Park, Byungjoon Lee, Sunhee Yang**.**

There were two approaches considered in implementing the firewall: a) pre-installing the rules onto the switch's flow table and b) handling the packets directly as they come in. We chose to handle the incoming packets directly because of the flexibility in management.

The logic of the firewall is as follows:

Each packet headers are checked against the firewall rule from highest to lowest priority, and performs specified action once matching fields are found in the rule. Any unmatched packets are dropped. Installing firewall rules are possible from an external entity through a text-based user interface.

## 3) APPLICATIONS:

- In networks where internal traffic needs to be filtered or inspected
- In networks where centralized control is very important.
- Packets are monitored and filtered at a central location thus useful in organizations where security plays a very important role.

## 4) CHALLENGES IN DOMAIN:

- Complex Configurations.
- Less number of user friendly interfaces available.
- Tough to maintain persistence.
- Needs to learn multiple tools.

**MATHEMATICAL MODEL:**

Let S be the System where,

S={s, c, sw, ho, h1, h2, e}

Where,

s = start state

c = POX controller

c = {f, I , h, l}

where, f = Fetch or load MAC addresses to be blocked by the firewall from .csv file.

f $\in$ {input file with id, source MAC address, destination MAC address}

I = Initiate Openflow protocol with the topology.

h = Handle up connections.

Where, h = {m, fmod ,actions,log}

m = Match function

where, m = {source , destination }

where, source = {Source MAC Address}

destination = {Destination MAC Address}

fmod = construct flow modify message

actions = Perform appropriate actions according to the rules.

log = logs written

l = launch function.

Where , l = {Register and launch the firewall}

sw = Switch

sw $\in$ {Tree Topology}

h0 = host 1

h0 $\in$ {Tree Topology}

h1 = host 2

h1 $\in$ {Tree Topology}

h2 = host 3

h2 $\in$ {Tree Topology}

e = end state.

**DESIGN AND ANALYSIS OF THE SYSTEM:**

- **SDN Firewall:**

  Since a software defined network decouples the data forwarding and control plane. Security must be enforced so as to make our system resistant of malicious attacks. Implementing a Firewall on the software Defined Network which can inspect, monitor, filter the traffic passing through it. Internal traffic is not seen and cannot be filtered by a traditional firewall. An SDN based firewall works both as a packet filter and a policy checker. The first packet goes through the controller and is filtered by the SDN firewall. The subsequent packets of the flow directly match the flow policy defined in the controller. The firewall policy is centrally defined and enforced at the controller.

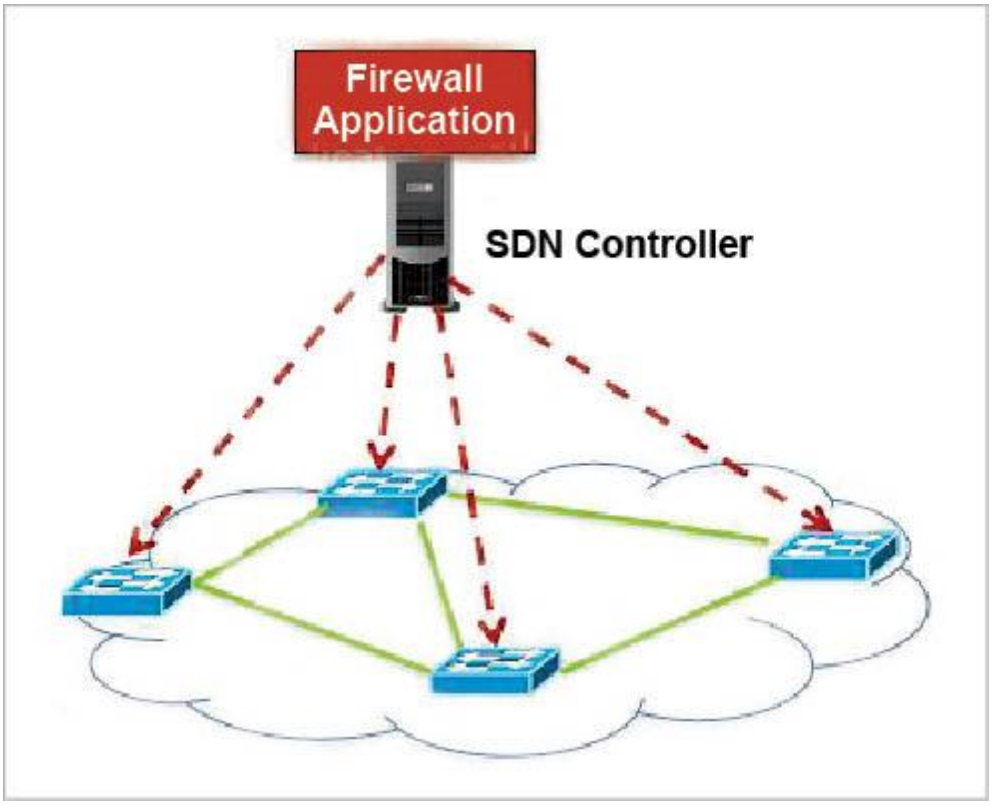



**Fig: Software Defined Network Firewall**

**A Comparison between Traditional and SDN Firewall:**

| Parameters | Traditional Network Firewall | SDN Firewall |
|---|---|---|
| 1. Stateful inspection | Track the state of traffic present on layers 2 to 4. | Track the state of layer 2 to 7. |
| 2. Integrated IPS and IDS | The IPS or IDS deployment is done with the help of a separate appliance or an appliance that is logically separated with the single appliance. | Intrusion Detection System (IDS) and Intrusion Protection System (IPS) is fully integrated. |
| 3. Identity Awareness | Not supported. | Keeps the track of the identity of local traffic device and user. |

**IMPLEMENTING A SDN BASED FIREWALL:**

The system analyses data packets for parameters like L2/L3 headers (i.e., MAC and IP address) or performs deep packet inspection (DPI) for higher layer parameters (like application type and services etc) to filter network traffic.

I have implemented a layer 2 firewall that runs alongside the MAC learning module on the POX OpenFlow controller. The firewall application is provided with a list of MAC address pairs i.e., access control list (ACLs). When a connection establishes between the controller and the switch, the application installs flow rule entries in the OpenFlow table to disable all communication between each MAC pair.

**It consists of two files:**

**firewall.py**: Contains logic for installing firewall rules. It consists of a firewall class that has a _handle_ConnectionUp function. It also has a global variable, policyFile, that holds the path of the firewall-policies.csv file. Whenever a connection is established between the POX controller and the OpenFlow switch the _handle_ConnectionUp functions gets executed.

**firewall-policies.csv:** A list of MAC pairs (i.e., policies) read as input by the firewall application.

id,mac_0,mac_1
1,00:00:00:00:00:01,00:00:00:00:00:02
firewall.csv file contains rules as above

Program reads the policy file and update the _handle_ConnectionUp function. The function should install rules in the OpenFlow switch that drop packets whenever a matching src/dst MAC address (for any of the listed MAC pairs) enters the switch. This will cause the firewall application to install a flow rule entry to disable all communication between host (h1) and host (h2).

**ZONE BASED FIREWALL:**

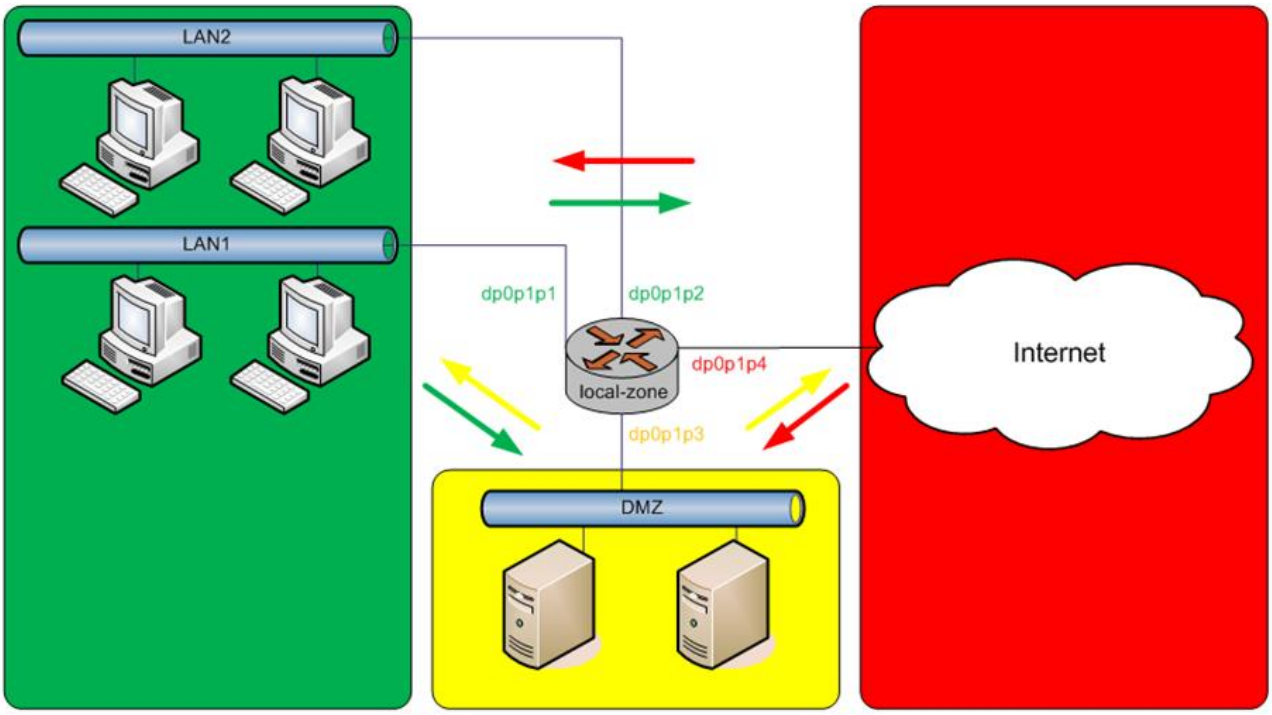



**Fig: A Zone Based Firewall**

Ordinary firewall rules sets are applied on a per-interface basis to act as a packet filter for the interface. In a zone-based firewall, interfaces are grouped into security "zones," where each interface in a zone has the same security level.
Packet-filtering policies are applied to traffic flowing between zones. Traffic flowing between interfaces that lie in the same zone is not filtered and flows freely because the interfaces share the same security level.

**STEPS IN SETTING UP A ZONE BASED FIREWALL:**

**Step 1 - Define the Zone Names and create zones**

Zone security R1

**Step 2 – Put the correct interface in zone**

Zone-member security R1

**Step 3- Define the Zone Pairs (direction of traffic flow)**

Zone-pair security LAN2INTERNET source R1 destination R3

**Step 3 - Create a Policy Maps and class for Zone Pairs**

Class class-default

**Step 4- Assign the Policy Map to a Zone Pair**

Policy-map type inspect LAN2INTERNET

**Step 5-Specify the matching protocols.**

Match protocol ICMP

**Step 6 – Verification ( ping)**

**Rules of Zone-Based Firewall:**

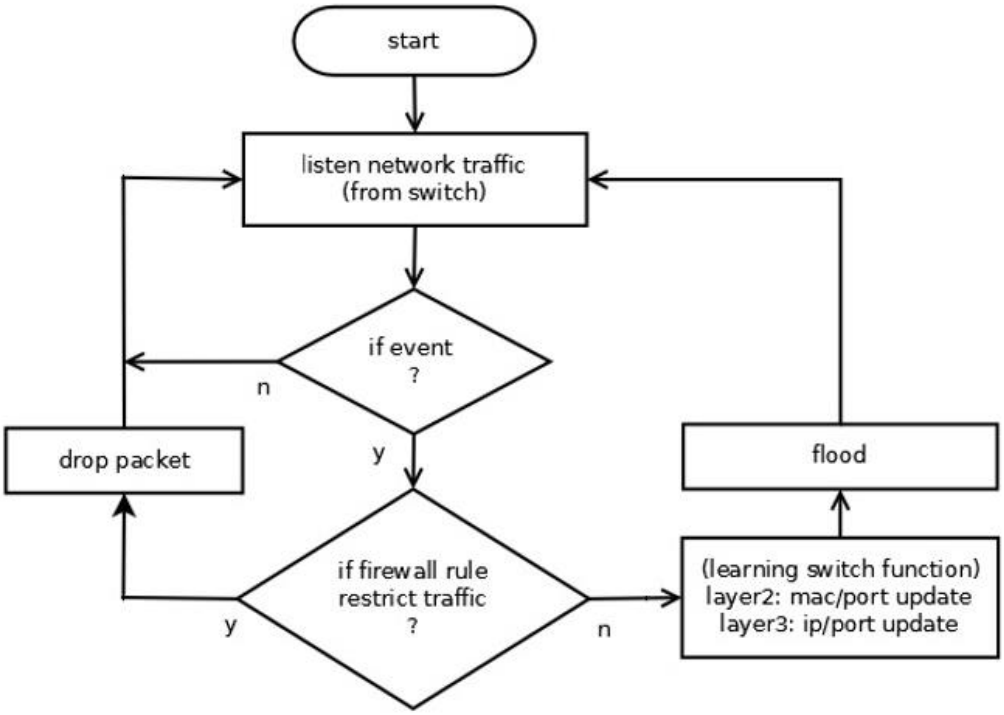
A zone must be configured before interfaces can be assigned to the zone.

An interface can be assigned to only one security zone.All traffic to and from a given interface is implicitly blocked when the interface is assigned to a zone, except traffic to and from other interfaces in the same zone, and traffic to any interface on the router.

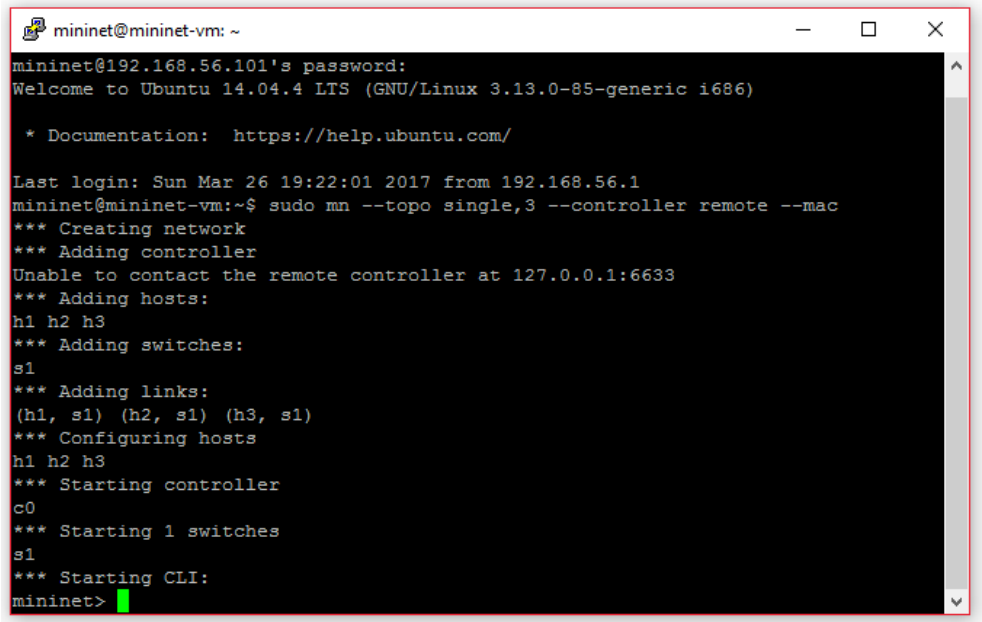
Traffic is implicitly allowed to flow by default among interfaces that are members of the same zone. In order to permit traffic to and from a zone member interface, a policy allowing or inspecting traffic must be configured between that zone and any other zone.

## DISCUSSION OF IMPLEMENTATION OF RESULTS:

- **Flow chart for firewall implementation:**

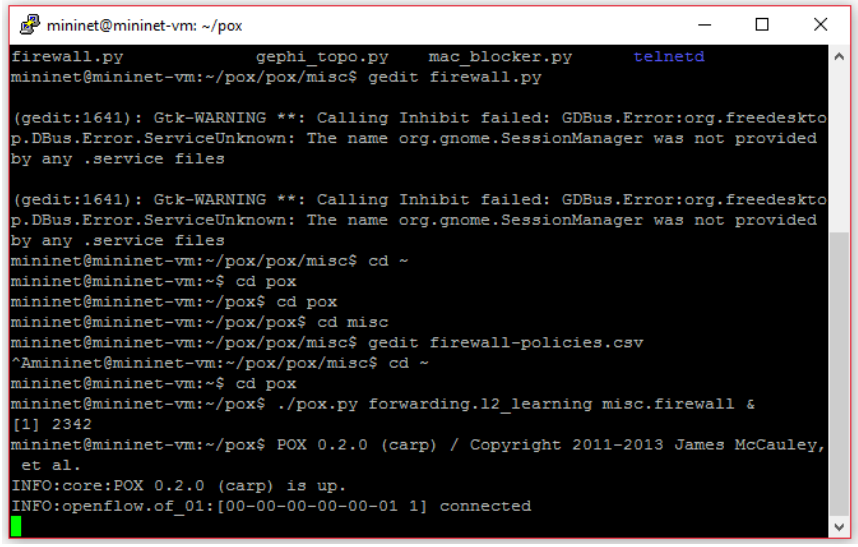



## SNAPSHOTS FROM THE SDN FIREWALL IMPLEMENTATION:

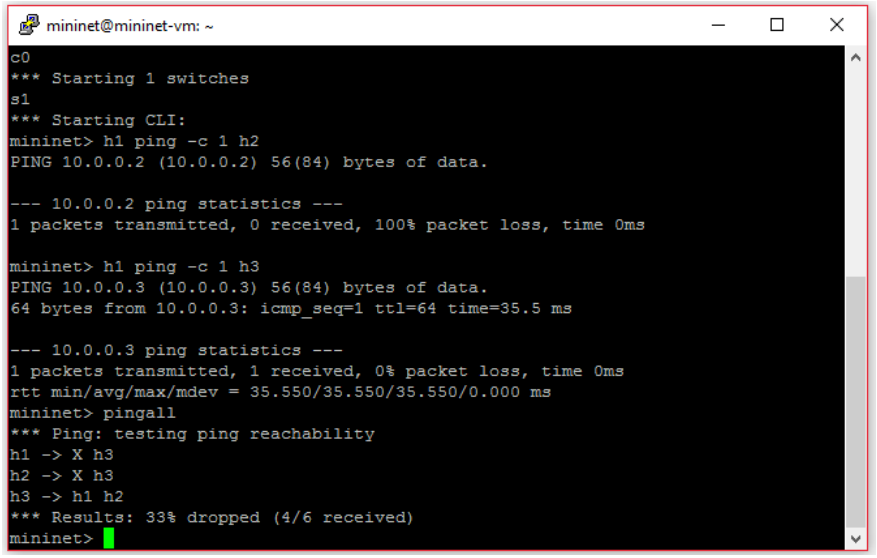



Starting the mininet topology.

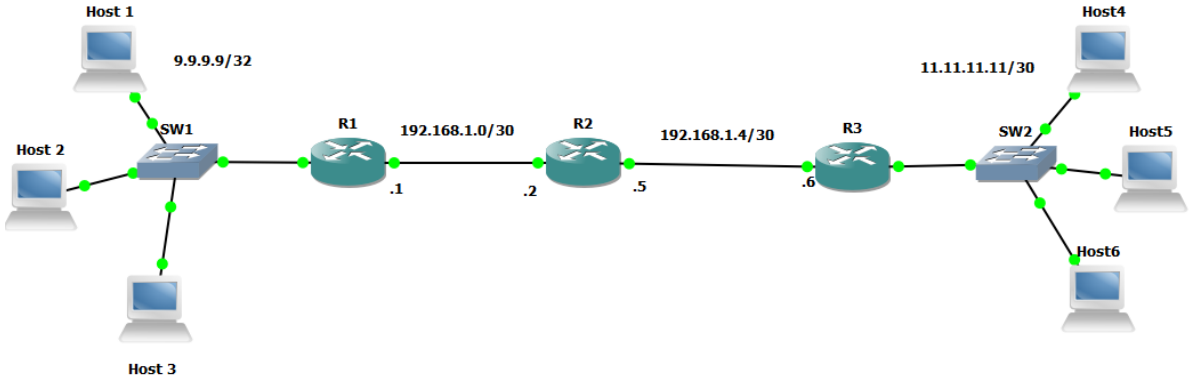
Starting the POX Controller:




Testing Rechability:



## SNAPSHOTS FROM ZONE BASED FIREWALL IMPLEMENTATION:




## Scenario 1:

PING from LAN to INTERNET (reachable)

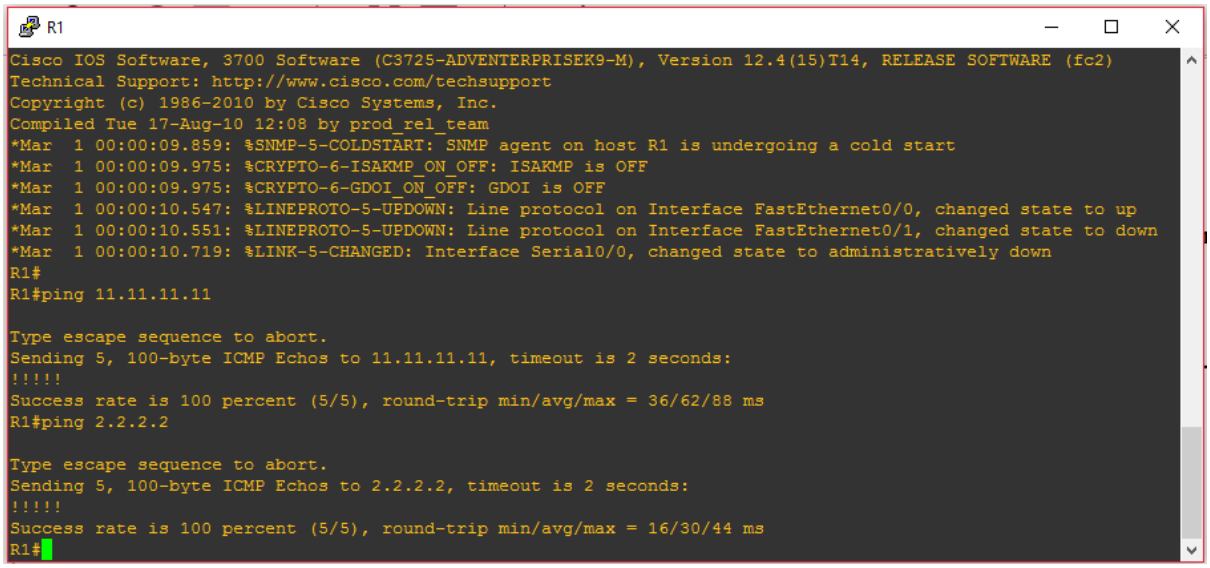
```
R1
Cisco IOS Software, 3700 Software (C3725-ADVENTERPRISEK9-M), Version 12.4(15)T14, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Tue 17-Aug-10 12:08 by prod_rel_team
*Mar  1 00:00:09.859: %SNMP-5-COLDSTART: SNMP agent on host R1 is undergoing a cold start
*Mar  1 00:00:09.975: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
*Mar  1 00:00:09.975: %CRYPTO-6-GDOI_ON_OFF: GDOI is OFF
*Mar  1 00:00:10.547: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
*Mar  1 00:00:10.551: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
*Mar  1 00:00:10.719: %LINK-5-CHANGED: Interface Serial0/0, changed state to administratively down
R1#
R1#ping 11.11.11.11

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 11.11.11.11, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/62/88 ms
R1#ping 2.2.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/30/44 ms
R1#
```

PING from INTERNET to LAN (not reachable)

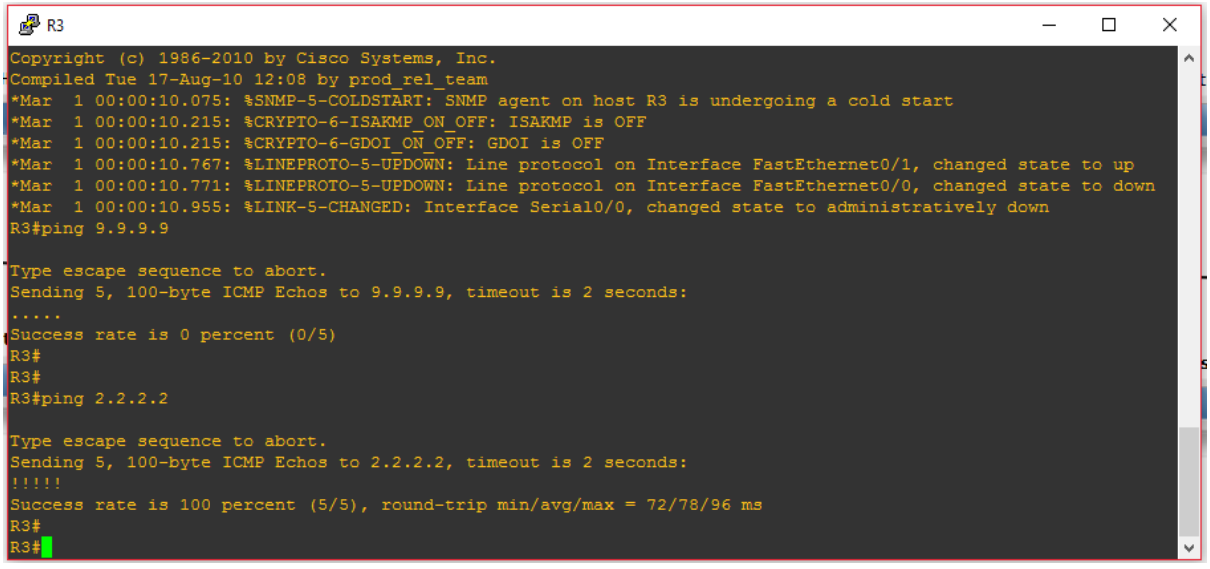
```
R3
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Tue 17-Aug-10 12:08 by prod_rel_team
*Mar  1 00:00:10.075: %SNMP-5-COLDSTART: SNMP agent on host R3 is undergoing a cold start
*Mar  1 00:00:10.215: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
*Mar  1 00:00:10.215: %CRYPTO-6-GDOI_ON_OFF: GDOI is OFF
*Mar  1 00:00:10.767: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
*Mar  1 00:00:10.771: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to down
*Mar  1 00:00:10.955: %LINK-5-CHANGED: Interface Serial0/0, changed state to administratively down
R3#ping 9.9.9.9

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 9.9.9.9, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
R3#
R3#
R3#ping 2.2.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 72/78/96 ms
R3#
R3#
```

## Scenario 2

### PING from LAN to INTERNET and FIREWALL (allowed)




### PING from INTERNET to Firewall is allowed, TELNET not allowed



## CONCLUSION AND FUTURE ENHANCEMENT:

- SDN firewalls are more secure as compared to the traditional and they are more flexible & programmable.Software defined network firewalls results in securing the network by filtering the ingress as well as egress traffic using ACL(access control list).Clubbing Zone based firewalls and SDN Firewalls will make SDN firewalls even more secure ,Since the network will be grouped into zones increasing security thereby making it easy to enforce rules/policies on firewalls .
- When software controls network functions, you can manage and change network functions quickly and easily. The software makes it easy to set up and manage. This will help simplify on-site network infrastructure upgrades and deployments and streamline operations, meaning that you can deploy network functions such as a new router or firewall without waiting and without installing additional on-site hardware.
- **Space and cost savings:** With a network based on software rather than physical equipment, customers invest less in hardware and need less space in the server room.
- **Enhanced security:** SDN enhances security because it is easier for the network service provider to respond to and deploy updates when there is an attack. It is also possible to isolate and contain problems more easily. In the case of a Distributed Denial of Service (DDoS) attack, we can scale the network in near real time to avoid major disruption to customer networks.
- SDN openflow plays a major role in centralizing control while helps SDN firewalls to be deployed at controller useful in avoiding worms and viruses in internal network. Hence it is highly adopted by organizations.
- Demilitarized zone can be used with the sdn firewall to increase security.
- Security enhancement can be done by implementing the firewalls at different layers of network dealing with layer respective protocols such as:
  i) TCP/UDP :- Layer 4
  ii) IP :- Layer 3
  iii) MAC addresses :- Layer 2
- The future of SDN is nothing short of bright. In fact, we expect SDN to become broadly pervasive over the next five years, as standards progress, the benefits become quantified, and end-user organizations proceed down the experience curve.
- One of the very interesting possibilities now appearing is the merging of SDN with that other leading-edge trend in networking, *network function virtualization (NFV).* NFV, like all virtualization technologies, substitutes software-based constructs for what would otherwise require dedicated hardware.

**REFERENCES:**


1) "A Layer2 Firewall for Software Defined Network", 2014 Conference on Information Assurance and Cyber Security (CIACS), Tariq Javid, Tehseen Riaz, Asad Rasheed ,©2015 IEEE.
2) "Building Firewall over the Software-Defined Network Controller" Michelle Suh, Sae Hyong Park, Byungjoon Lee, Sunhee Yang SDN Research Section,Korea, February 16~19, 2014 ICACT2014.
3) "Firewalls Policies Based on Software Defined Networking: A survey" Sailen Dutta Kalita1, Rupam Kumar Sharma2,Assam,India,AJET 2016.
4) "Software Defined Networking based Routing Firewall" Karamjeet Kaur,Sukhveer Kaur,Viping Gupta,Moga,India. ©2016 IEEE.
5) "Development of a Distributed Firewall Using Software Defined Networking Technology" ,Justin Gregory V. Pena and William Emmanuel Yu, Quezon City, Philippines, ©2015 IEEE.
6) "Programmable Firewall Using Software Defined Networking" Karamjeet Kaur, Japinder Singh, Ferozepur, India. 2015 2nd InternationalConference on Computing for SustainableGlobal Development(INDIACom).