ΤΕΧΝΟΛΟΓΙΕΣ ΚΑΙ ΥΠΗΡΕΣΙΕΣ ΔΙΑΔΙΚΤΥΟΥ

ΕΡΓΑΣΙΑ ΜΕ ΧΡΗΣΗ ΤΟΥ MININET NETWORK EMULATOR

Υπεύθυνη Εργασίας: Άννα Κεφάλα
Ακαδημαϊκό έτος: 2024-2025
Όνομα Φοιτήτριας: Χρύσα Ριζεάκου
ΑΜ: p3312416

Υλοποίηση Firewall με Mininet και POX Controller

Περιγραφή του Συστήματος

Η εργασία αφορά την υλοποίηση ενός απλού firewall χρησιμοποιώντας τα εργαλεία Mininet και POX Controller, με στόχο την κατανόηση των αρχών του Software-Defined Networking (SDN).

Αρχιτεκτονική του Συστήματος και Ρόλοι Στοιχείων

Το σύστημα αποτελείται από τα ακόλουθα στοιχεία:

1. Mininet Network Emulator

Το Mininet είναι υπεύθυνο για τη δημιουργία εικονικής δικτυακής τοπολογίας που περιλαμβάνει ένα switch (S1) και πέντε hosts (H1-H5). Η κύρια λειτουργία του είναι η εξομοίωση του φυσικού δικτύου σε εικονικό περιβάλλον, επιτρέποντας τη δοκιμή και την ανάπτυξη δικτυακών εφαρμογών χωρίς την ανάγκη φυσικού εξοπλισμού.

2. POX Controller

Ο POX Controller λειτουργεί ως κεντρικός ελεγκτής του δικτύου (SDN Controller) και χρησιμοποιεί το πρωτόκολλο OpenFlow 1.0 για επικοινωνία με το switch. Είναι υπεύθυνος για τη διαχείριση των κανόνων δρομολόγησης (flow rules) στο switch, καθορίζοντας τον τρόπο με τον οποίο τα πακέτα θα επεξεργάζονται και θα προωθούνται στο δίκτυο.

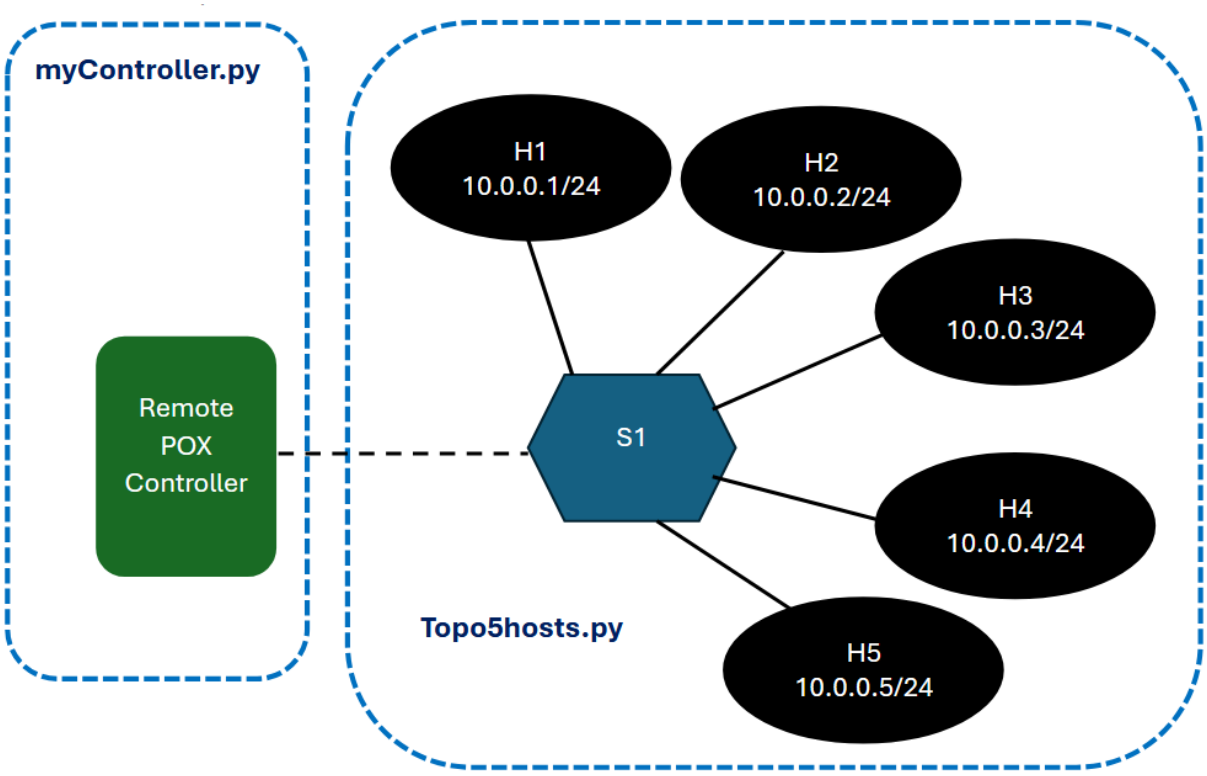
3. OpenFlow Switch (S1)

Το OpenFlow switch S1 είναι υπεύθυνο για την προώθηση πακέτων βάσει των κανόνων που λαμβάνει από τον controller. Πρόκειται για ένα software-defined switch που επικοινωνεί άμεσα με τον POX controller μέσω του πρωτοκόλλου OpenFlow, εκτελώντας τις εντολές που λαμβάνει για τη διαχείριση της δικτυακής κίνησης.

4. Hosts (H1-H5)

Τα πέντε hosts έχουν διευθύνσεις IP από 10.0.0.1/24 έως 10.0.0.5/24 και είναι όλα συνδεδεμένα στο switch S1. Αυτά αντιπροσωπεύουν τους τελικούς χρήστες ή συσκευές του δικτύου που παράγουν και καταναλώνουν δικτυακή κίνηση.

Τοπολογία Δικτύου



<u>Κανόνες Firewall</u>

Το firewall υλοποιεί τους ακόλουθους κανόνες με σειρά προτεραιότητας:

Προτεραιότητα	Src IP	Dst IP	Πρωτόκολλο	Ενέργεια
3 (υψηλότερη)	any	any	ARP	Accept (Flooding)
2	any IPv4	any IPv4	UDP	Accept (Forward to destination)
1 (χαμηλότερη)	any IPv4	any IPv4	-	Drop

Λεπτομερής Ανάλυση Κανόνων:

Κανόνας ARP (Προτεραιότητα 3):
Ο κανόνας με την υψηλότερη προτεραιότητα επιτρέπει την ελεύθερη διέλευση των ARP

πακέτων και χρησιμοποιεί flooding για την εύρεση MAC διευθύνσεων. Αυτός ο κανόνας είναι απαραίτητος για την επικοινωνία στο επίπεδο 2, καθώς τα ARP πακέτα χρειάζονται για τη μετατροπή των IP διευθύνσεων σε MAC διευθύνσεις.

Κανόνας UDP (Προτεραιότητα 2):
Αυτός ο κανόνας επιτρέπει UDP κίνηση με έλεγχο προορισμού, όπου τα πακέτα στέλνονται στον controller για επεξεργασία και στη συνέχεια προωθούνται στη σωστή θύρα βάσει της IP διεύθυνσης προορισμού. Αυτό επιτρέπει την ελεγχόμενη διέλευση UDP κίνησης μέσω του δικτύου.

Κανόνας Drop (Προτεραιότητα 1):
Ο κανόνας με τη χαμηλότερη προτεραιότητα απορρίπτει όλη την υπόλοιπη IP κίνηση, συμπεριλαμβανομένων των TCP και ICMP πακέτων. Λειτουργεί ως default rule και εξασφαλίζει ότι μόνο η επιτρεπόμενη κίνηση (ARP και UDP) μπορεί να διέλθει από το firewall.

Αποτελέσματα και Ανάλυση

Αρχεία:

1. **Topo5hosts.py:** Ορισμός της τοπολογίας δικτύου
2. **myController.py:** Υλοποίηση του firewall στον POX controller

Πριν εφαρμοστούν οι κανόνες του firewall πραγματοιποιήθηκε έλεγχος για να βεβαιωθούμε ότι η τοπολογία λειτουργεί καλά.

```
csuser@csuser-virtualbox:/mnt/mininetProj$ sudo mn --custom Topo5hosts.py --topo topo5hosts --controller default
*** Creating network
*** Adding controller
*** Adding hosts:
h1 h2 h3 h4 h5
*** Adding switches:
s1
*** Adding links:
(h1, s1) (h2, s1) (h3, s1) (h4, s1) (h5, s1)
*** Configuring hosts
h1 h2 h3 h4 h5
*** Starting controller
c0
*** Starting 1 switches
s1 ...
*** Starting CLI:
mininet> pingall
*** Ping: testing ping reachability
h1 -> h2 h3 h4 h5
h2 -> h1 h3 h4 h5
h3 -> h1 h2 h4 h5
h4 -> h1 h2 h3 h5
h5 -> h1 h2 h3 h4
*** Results: 0% dropped (20/20 received)
```

Εκτέλεση του Συστήματος:

1. **Εκκίνηση POX Controller:**

```
csuser@csuser-virtualbox:~/pox$ python3 pox.py openflow.of_01 --port=6653 misc.myController
POX 0.7.0 (gar) / Copyright 2011-2020 James McCauley, et al.
WARNING:version:POX requires one of the following versions of Python: 3.6 3.7 3.8 3.9
WARNING:version:You're running Python 3.12.
WARNING:version:If you run into problems, try using a supported version.
INFO:core:POX 0.7.0 (gar) is up.
INFO:openflow.of_01:[00-00-00-00-00-01 2] connected
INFO:misc.myController:Rule added: Allow ARP (Flood)
INFO:misc.myController:Rule added: Allow UDP (Forward)
INFO:misc.myController:Rule added: Drop all other IP traffic
```

2. **Εκκίνηση Mininet:**

```
csuser@csuser-virtualbox:/mnt/mininetProj$ sudo python3 Topo5hosts.py
[sudo] password for csuser:
mininet>
```

Αποτελέσματα εντολών

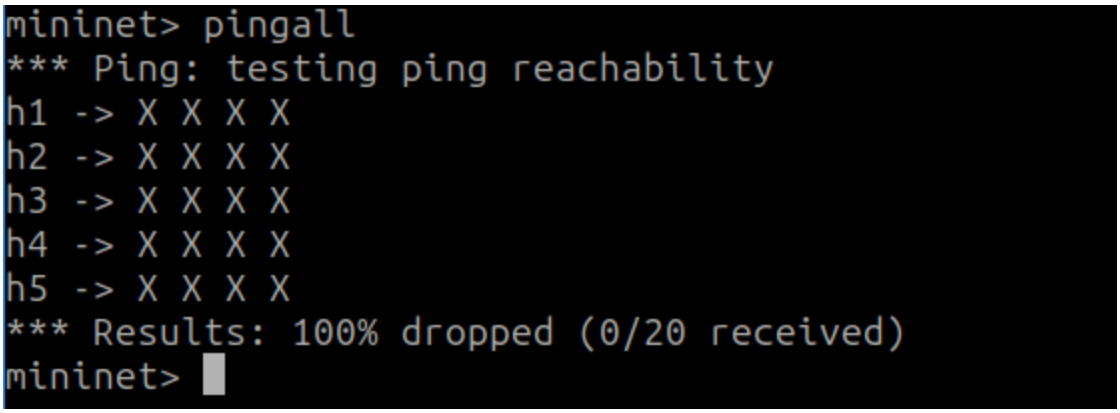
Εντολή dump: Η εντολή mininet> dump έχει ως σκοπό την εμφάνιση λεπτομερειών των κόμβων του δικτύου. Κατά την εκτέλεσή της εμφανίζονται οι IP διευθύνσεις, τα PIDs και τα interfaces όλων των hosts και του switch, επιβεβαιώνοντας τη σωστή δημιουργία της τοπολογίας.

```
mininet> dump
<Host h1: h1-eth0:10.0.0.1 pid=1711>
<Host h2: h2-eth0:10.0.0.2 pid=1713>
<Host h3: h3-eth0:10.0.0.3 pid=1715>
<Host h4: h4-eth0:10.0.0.4 pid=1717>
<Host h5: h5-eth0:10.0.0.5 pid=1719>
<OVSSwitch s1: lo:127.0.0.1,s1-eth1:None,s1-eth2:None,s1-eth3:None,s1-eth4:None,s1-eth5:None pid=1724>
<RemoteController c0: 127.0.0.1:6653 pid=1705>
```

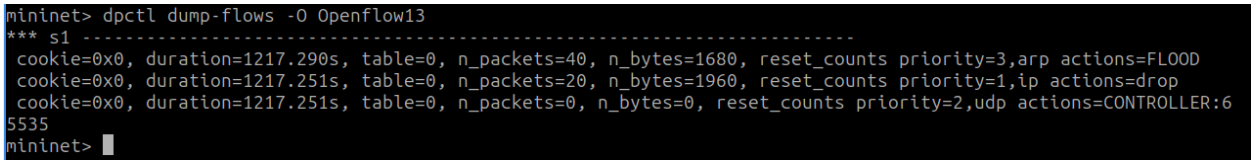
Εντολή net: Η εντολή mininet> net χρησιμοποιείται για την εμφάνιση των δικτυακών συνδέσεων μεταξύ των κόμβων. Τα αποτελέσματά της επιβεβαιώνουν τη σωστή σύνδεση όλων των hosts με το switch S1 και την ορθή διαμόρφωση των virtual ethernet interfaces.

```
mininet> net
h1 h1-eth0:s1-eth1
h2 h2-eth0:s1-eth2
h3 h3-eth0:s1-eth3
h4 h4-eth0:s1-eth4
h5 h5-eth0:s1-eth5
s1 lo:  s1-eth1:h1-eth0 s1-eth2:h2-eth0 s1-eth3:h3-eth0 s1-eth4:h4-eth0 s1-eth5:h5-eth0
c0
```

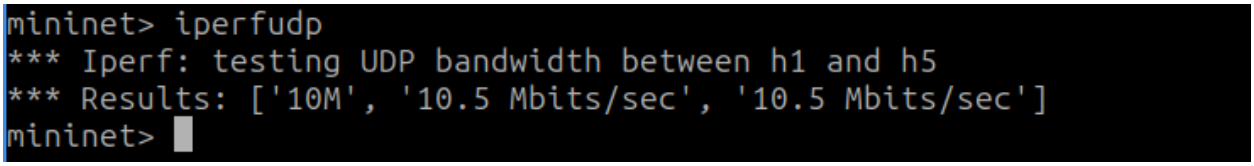
Εντολή pingall: Η εντολή mininet> pingall εκτελεί έλεγχο ICMP κίνησης μεταξύ όλων των hosts του δικτύου. Σύμφωνα με τη λειτουργία του firewall, αναμένεται να αποτύχουν όλα τα pings καθώς το firewall απορρίπτει την ICMP κίνηση, επιτρέποντας μόνο ARP και UDP πακέτα.



Εντολή dpctl dump-flows: Η εντολή mininet> dpctl dump-flows -O Openflow13 s1 εμφανίζει τους εγκατεστημένους flow rules στο switch. Τα αποτελέσματα δείχνουν τους τρεις κανόνες του firewall που έχουν εγκατασταθεί στο switch με τις αντίστοιχες προτεραιότητές τους, επιβεβαιώνοντας τη σωστή λειτουργία του controller.



Εντολή iperfudp: Η εντολή mininet> iperfudp πραγματοποιεί έλεγχο UDP κίνησης μεταξύ των hosts του δικτύου. Αναμένεται επιτυχής μετάδοση UDP πακέτων καθώς το firewall επιτρέπει αυτόν τον τύπο κίνησης, με τα πακέτα να προωθούνται στη σωστή θύρα βάσει της IP διεύθυνσης προορισμού.



Πράγματι:

```
INFO:misc.myController:Handling UDP packet for destination: 10.0.0.5
INFO:misc.myController:Forwarding UDP packet to port 5
INFO:misc.myController:Handling UDP packet for destination: 10.0.0.5
INFO:misc.myController:Forwarding UDP packet to port 5
INFO:misc.myController:Handling UDP packet for destination: 10.0.0.1
INFO:misc.myController:Forwarding UDP packet to port 1
INFO:misc.myController:Handling UDP packet for destination: 10.0.0.1
INFO:misc.myController:Forwarding UDP packet to port 1
```

Συμπεράσματα

Η εργασία υλοποιήθηκε επιτυχώς και το firewall λειτουργεί σύμφωνα με τις προδιαγραφές:

- Επιτρέπει ARP κίνηση (flooding)
- Επιτρέπει UDP κίνηση (προώθηση στον σωστό προορισμό)
- Απορρίπτει όλη την υπόλοιπη IP κίνηση (TCP, ICMP)
