# Part 4 Design and implement a countermeasure to the attack from Part3

I. Abstract:

In an ideal world, there would be filters on all BGP sessions that only allow prefixes that are actually supposed to come in over that BGP session. In Part3 practice, ISPs tend to get new IP address blocks to prevent the false origin prefix attack. This means that once an ISP accepts a prefix advertised by a customer, that prefix will be widely propagated.

II. Modified files:

bgpd-R1.conf

bgpd-R2.conf

bgpd-R3.conf

bgpd-R4.conf

bgpd-R5.conf

III. Description of changes:

Added AS prefix filter to prevent the malicious/unknown IP connections. Prelist all the AS ip permits and filter out unknown ones, sample code is like below:

R5

ip prefix-list customer-a seq 5 permit 9.0.5.5/24 le 32

ip prefix-list customer-a seq 10 permit 9.0.8.5/24 le 32

ip prefix-list customer-a seq 15 permit 9.0.6.4/24 le 32

neighbor 9.0.7.6 prefix-list customer-a in (for any new AS added to the system)

R4

ip prefix-list customer-a seq 5 permit 9.0.2.2/24 le 32

ip prefix-list customer-a seq 10 permit 9.0.3.4/24 le 32

ip prefix-list customer-a seq 15 permit 9.0.6.5/24 le 32

R3

ip prefix-list customer-a seq 5 permit 9.0.4.1/24 le 32

ip prefix-list customer-a seq 10 permit 9.0.1.1/24 le 32

ip prefix-list customer-a seq 15 permit 9.0.3.3/24 le 32

ip prefix-list customer-a seq 20 permit 9.0.8.6/24 le 32

R2

ip prefix-list customer-a seq 5 permit 9.0.0.1/24 le 32

ip prefix-list customer-a seq 10 permit 9.0.1.2/24 le 32

ip prefix-list customer-a seq 15 permit 9.0.2.1/24 le 32

ip prefix-list customer-a seq 20 permit 9.0.5.6/24 le 32

R1

ip prefix-list customer-a seq 5 permit 9.0.0.2/24 le 32

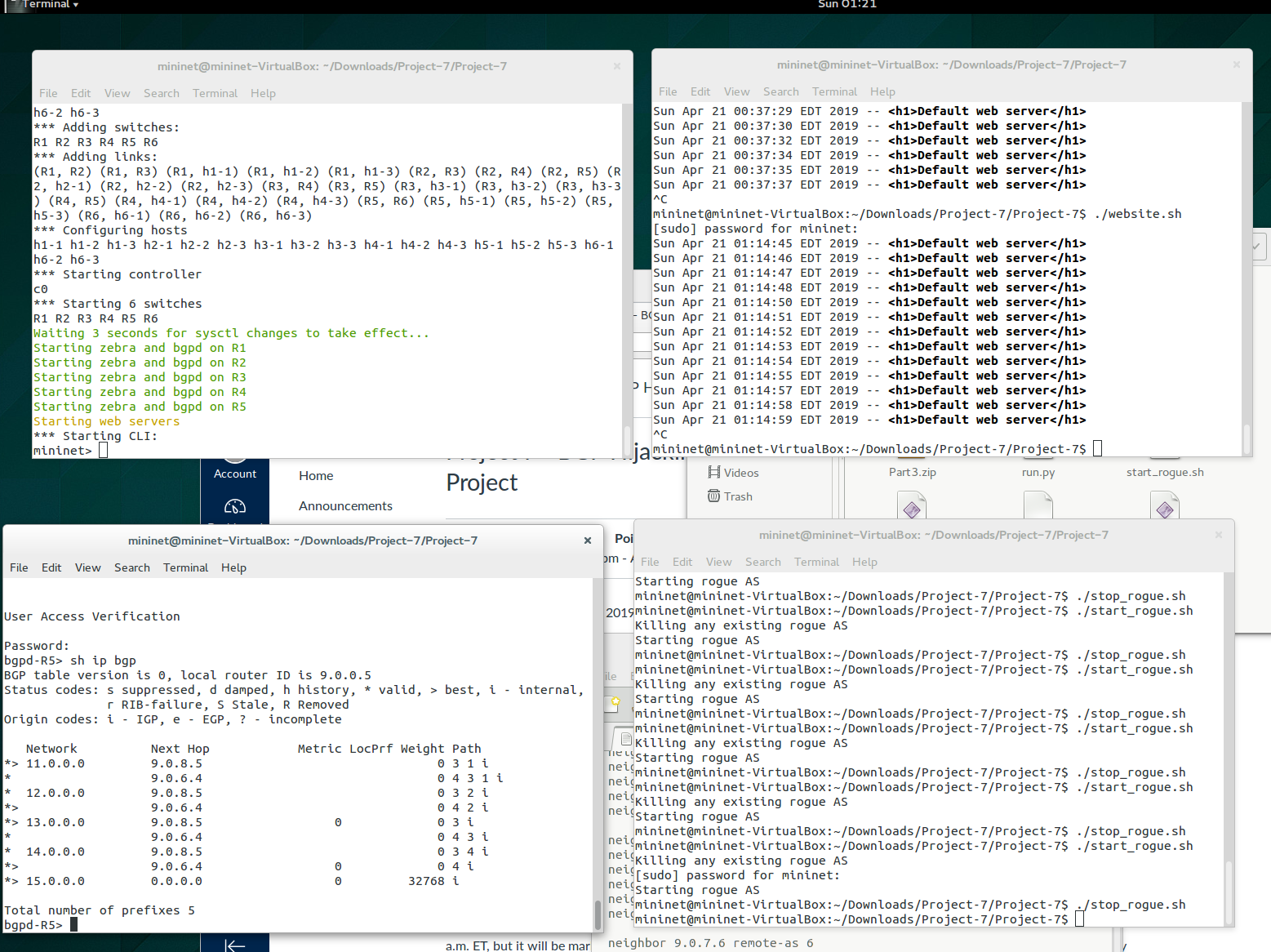
ip prefix-list customer-a seq 10 permit 9.0.4.2/24 le 32

IV. Instructions for demonstration

Similar to Part 2

1. Run sudo python bgp.py
2. Run ./connect.sh in another terminal
3. Run ./website.sh in the third terminal
4. Run ./start\_rogue.sh and ./stop\_rogue.sh in the fourth terminal
5. Run sh ip bgp or sh ip bgp summary in terminal 2 to ensure the hijack prefix attack falls.

Below figure shows how the victim AS routing table maintain its original state:



V. Summary

This approach will block any attack as well as any unknown new AS, in case any AS need to be added to the mininet system, a new filter will be implemented to include them. In real world, ISPs carefully filter prefixes they receive from their customers.

This is a simple prefix list approach that allows the prefixes held by the customer (and the customer’s customers) will do the trick for countermeasure from Part 3. See figure below:

