
# ISP Packet filters

Olof Hagsand
Pehr Söderman
KTH/CSC

| | |
|---|---|
| Group Nr | |
| Name 1 | |
| Name 2 | |
| Name 3 | |
| Name 4 | |
| Date | |
| Instructor's Signature | |

# Table of Contents

1 Goals....3
2 Introduction....3
3 Preparations....3
4 Lab setup....4
4.1 Equipment....4
4.2 Dumping traffic....4
4.3 Internal network....4
4.4 External peering....5
4.5 Peering with other ISPs....5
4.6 Verify connectivity....6
5 Support ticket 1....7
5.1 Identify the attack....7
5.2 Develop a counter-measure....7
5.3 Verify the success....7
6 Support ticket 2....8
6.1 Identify the valid source addresses....8
6.2 Choose where to deploy your solution....8
6.3 Deploy the solution....8
6.4 Verify the solution....8
7 Support ticket 3....9
7.1 Develop a solution....9
7.2 Implement the solution....9
7.3 Verify the solution....9
8 Support ticket 4....10
8.1 List invalid prefixes....10
8.2 Implement a route filter....10
8.3 Verify your route filter....10
9 Support ticket 5....11
9.1 Implement Communities....11
9.2 Create a black hole....11
9.3 Verify that you no longer recieve DDoS....11
10 Cleanup....11
11 References....11

# 1 Goals

The goal with this lab is to introduce you to the concepts of filtering and management of a small ISP enviroment. In particular, the lab covers packet filtering, handling of DDoS attacks, common filtering paradigms and route filters in BGP.

Read through the lab instructions before the lab, some questions can be answered in advance which will save you time and make it easier to carry out the lab.

If you have not made labs with the Juniper routers before, you should make the CLI tutorial in [1] before starting this lab.

# 2 Introduction

The laboratory system consists of routers and hosts. The routers are Juniper J routers, see [1] for an introduction to the Junipers and the lab equipment. The policy framework manual in the online Juniper documentation [2] contains a complete reference to firewall filters.

You have one management host available on your network. You can use this host to test connectivity. You also have a number of customer computers on your network. You do not have access to these computers, other than a simple web server giving you some connectivity information.

The lab is carried out in groups, where each group has four routers and one host. All lab networks are interconnected, therefore changes you do in your network will have effects on the other networks.

The routers are placed in the CSC routerlab which you do not have physical access to.

# 3 Preparations

You need to master the Juniper routers in order to start this lab in time. If you do not, you should make an introductory Juniper lab before this lab. Reference [1] contains a tutorial.

You will receive the login password for virtual hosts and routers at the lab.

The IP address for your network is listed in the network topology map (see Appendix A).

# 4 Lab setup

To begin with you should familiarize yourself with the setup of your lab network before you begin the actual laboration. The setup is similar to the routing introduction[1].

## 4.1 Equipment

The equipment of the lab are Juniper routers and virtual hosts. The physical network and basic routing is set-up in advance.

The virtual hosts a1.xen.netlab.csc.kth.se, a2.xen.netlab.csc.kth.se, etc are divided into customers and management hosts. You can access the management hosts a2, b2, c2, and d2, but you may not access the customer hosts (That would violate the customers privacy,...).

All virtual hosts run SUSE linux and are accessed using ssh. The username is `laban`. To perform commands with super-user privileges, issue the `sudo` command.

To connect to the routers, you use telnet to a console server. In this way, you access the routers serial port. The following table shows which address and telnet port to use to connect:

| Group | Routers | Terminal server | telnet port |
|---|---|---|---|
| A | RTA1-RTA4 | terminal1.netlab.csc.kth.se | 2001-2004 |
| B | RTB1-RTB4 | terminal1.netlab.csc.kth.se | 2005-2008 |
| C | RTC1-RTC4 | terminal2.netlab.csc.kth.se | 2001-2004 |
| D | RTD1-RTD4 | terminal2.netlab.csc.kth.se | 2005-2008 |
| E | RTE1-RTE4 | terminal2.netlab.csc.kth.se | 2009-2012 |

## 4.2 Dumping traffic

The lab assistants will be able to sniff any link by using port mirroring. When you need to look at the traffic on a link, contact the assistants and they will provide a dump of the traffic on a specific link for you. Before you contact the assistants about this, however, prepare thoroughly which link you wish to monitor and if you wish to filter traffic in any way.

## 4.3 Internal network

The lab is made in four groups with 4-5 people in each group. The router groups have been set up in advance for groups X=A, B, C, D (Alternatively 1, 2, 3, 4).

Our group number is:_____

Regard the network map in Appendix A.

OSPF is enabled on all routers RTX1-RTX4 so that you have full connectivity internally (within AS 650X1). The customer networks (and DMZs) are announced declaring OSPF as passive over those interfaces. The internal network contains a core network (192.168.X.0/24) and a set of customer networks (10.X.0.0/16). The core network contains a management subnet (192.168.X.40/30) where servers, etc for the ISP are placed. There are only two customers, and one connected address in each. You should imagine you have many more.

You should now be able to ping all internal hosts and routers within your network AS 650X1. Verify this before you proceed.

## 4.4 External peering

External BGP peering is enabled to the “Internet” from the border router RTX1. Your customer and core networks including the router ID:s are announced using aggregation. Which prefixes are announced to the internet?

_____
_____
_____
_____
_____

Check which prefixes you receive from the internet?

_____
_____
_____
_____
_____

## 4.5 Peering with other ISPs

In addition to a global transit connection, peering is also setup to the two neighbour ISPs from RTX1. Your core and customer network are announced on these as well.
How do you expect the traffic to go into and out from your network given these three BGP connections?

_____
_____
_____
_____

## 4.6 Verify connectivity

Verify that your customer networks have connectivity to all the other customer networks and the internet. You can do this by

checking the HTTP servers on the customer computers. If you still lack connectivity to any network work together with that group to ensure your customer networks get full connectivity.

**Milestone 1: Setup.**
Signature: _____

# 5 Support ticket 1

One of your customers, Media Solutions LDT, is using your network for a local office. These are located in x4. They have recently been experiencing network slowdowns and problems connecting over SSH. From time to time their downlink have been full. They suspect they might be under a DDoS attack and asks you to try to migrate the attack.

## 5.1 Identify the attack

Using the monitor functions in the routers and the traffic dumping you should try to identify the attack. What are the characteristics of the attack?

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

## 5.2 Develop a counter-measure

As the customer do not have enough bandwidth to handle the attack on their own they ask you to stop the attack for them. Develop a packet filter that stops the attack without disrupting the customer network connectivity.

Where in your network will you deploy the packet filter? Why?

_____
_____
_____
_____
_____

## 5.3 Verify the success

Verify that the attack have been stopped and the customer no longer receives any data matching the attack profile.

**Milestone 2: Incoming DDoS**
Signature: _____

# 6 Support ticket 2

You have recently been contacted by the transit provider you are connected to (e.g the operator that provides the link and peering to RTE4). There have been complaints about a large amount of packets with invalid source addresses originating in your network. You are asked to solve this problem.

## 6.1 Identify the valid source addresses

For each router in your network you should write down the source addresses you expect to see and in which direction the packets should be going.

## 6.2 Choose where to deploy your solution

Choose which routers that should filter the traffic. All traffic leaving your network should have valid source addresses.

## 6.3 Deploy the solution

Using the previously gathered information, create packet filters implementing the solution. Deploy the packet filters on the routers you choose.

## 6.4 Verify the solution

Verify that no traffic with invalid source addresses still leaves your network.

**Milestone 3: Invalid source addresses.**
Signature: _____

# 7 Support ticket 3

There have recently been several attacks on our routers. These have been both in the form of distributed DoS attacks and aimed attacks at various protocols on the routers, such as TCP reset attacks. To prevent new attacks we need to protect the routers. You have been given the task of designing and implementing a filter for the router engines (located on the loopback interface of a Juniper Router).

## 7.1 Develop a solution

For each router identify the protocols the router have to communicate over and who have to be able to connect to the router. Some protocols (such as SSH) you might have to allow for a large range of addresses to simplify management. Make sure you rate-limit the traffic using policers to avoid DoS attacks.

Reference [3] might be helpful.

## 7.2 Implement the solution

Implement the solution and deploy it on all routers in your network.

## 7.3 Verify the solution

Verify that the solution works as intended. How do you verify that it works? What kind of issues will this cause?

_____
_____
_____
_____
_____

**Milestone 4: Protect the core network**
Signature: _____

# 8 Support ticket 4

After a recent routing failure at a neighbouring ISP where several routers lost connections due to the inclusion of an invalid 127.0.0.1 route you have been asked to protect your network from similar issues in the future.

## 8.1 List invalid prefixes

Make a list of the martian prefixes you do not wish to route. Note that you will need to allow RFC 1918 prefixes.

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

## 8.2 Implement a route filter

Create a filter that removes all these routes before they are included in the routing tables of your routers.

## 8.3 Verify your route filter

Make sure that the martians are no longer in the routing tables in your network.

**Milestone 5: No martian routes**
Signature: _____

# 9 Support ticket 5

The host located in x4 (Media Solutions LDT) is still drawing significant DDoS traffic. This is placing a lot of load on our border routers and lowers the service quality to such a degree that we are having problems fullfilling some of our SLA (Service Level Agreements). To lower the load on our network we have decided to blackhole this host using the BGP community that has been designated for this purpose.

## 9.1 Implement Communities

RFC1997 covers communities. The community we use to black hole traffic is 1:6666. We have to implement this community and drop all traffic destined to routes belonging to this community, for example by marking all routes related to this community as next hop discard.

## 9.2 Create a black hole

Remove a (minimal) part of our IP space by marking the addresses under DDoS attack with the blackhole community and announce the new route to the neighbouring AS

## 9.3 Verify that you no longer recieve DDoS

Check the border router so no DDoS traffic can be seen there.

**Milestone 6: Black Hole**
Signature: _____

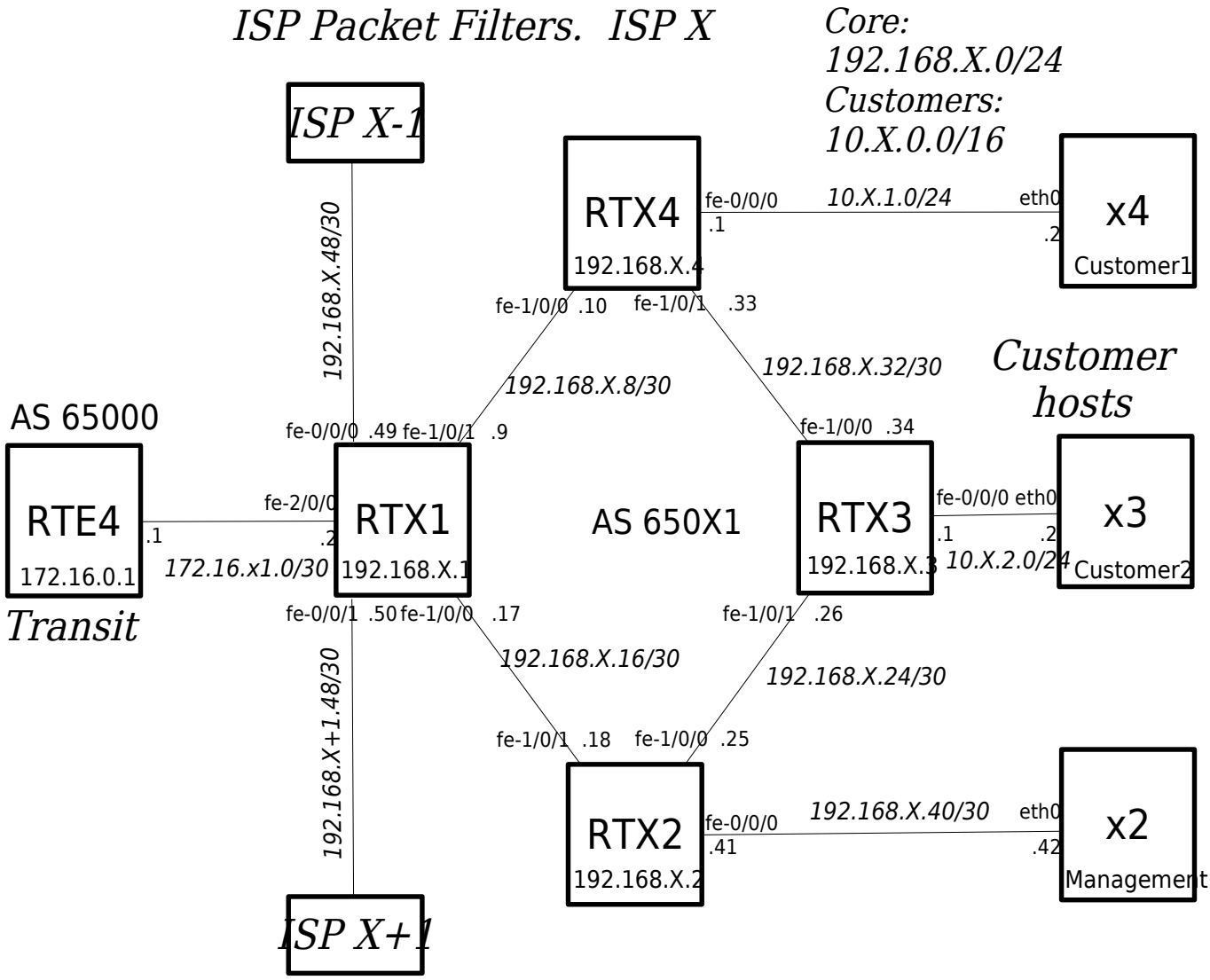
# 10 Cleanup

Remove router configuration rules from the routers.

# 11 References

[1] KTHNOC Introduction to routing
[2] JunOS reference manuals – http://www.juniper.net/techpubs/software/junos/junos90/
[3] Peymani, Kolon, “Juniper Application Note 350013 : Best common practices for hardening the infrastructure”, Juniper Networks, 2002

# Appendix A


ISP Packet Filters. ISP X
Core:
192.168.X.0/24
Customers:
10.X.0.0/16
ISP X-1
192.168.X.48/30
RTX4
192.168.X.4
fe-0/0/0
.1
10.X.1.0/24
eth0
.2
x4
Customer1
fe-1/0/0 .10
fe-1/0/1 .33
192.168.X.8/30
192.168.X.32/30
Customer
hosts
AS 65000
fe-0/0/0 .49
fe-1/0/1 .9
fe-1/0/0 .34
RTE4
172.16.0.1
fe-2/0/0
.1
.2
RTX1
192.168.X.1
AS 650X1
RTX3
192.168.X.3
fe-0/0/0 eth0
.1
.2
x3
Customer2
172.16.x1.0/30
10.X.2.0/24
Transit
fe-0/0/1 .50
fe-1/0/0 .17
fe-1/0/1 .26
192.168.X.16/30
192.168.X.24/30
192.168.X+1.48/30
fe-1/0/1 .18
fe-1/0/0 .25
RTX2
192.168.X.2
fe-0/0/0
.41
192.168.X.40/30
eth0
.42
x2
Management
ISP X+1