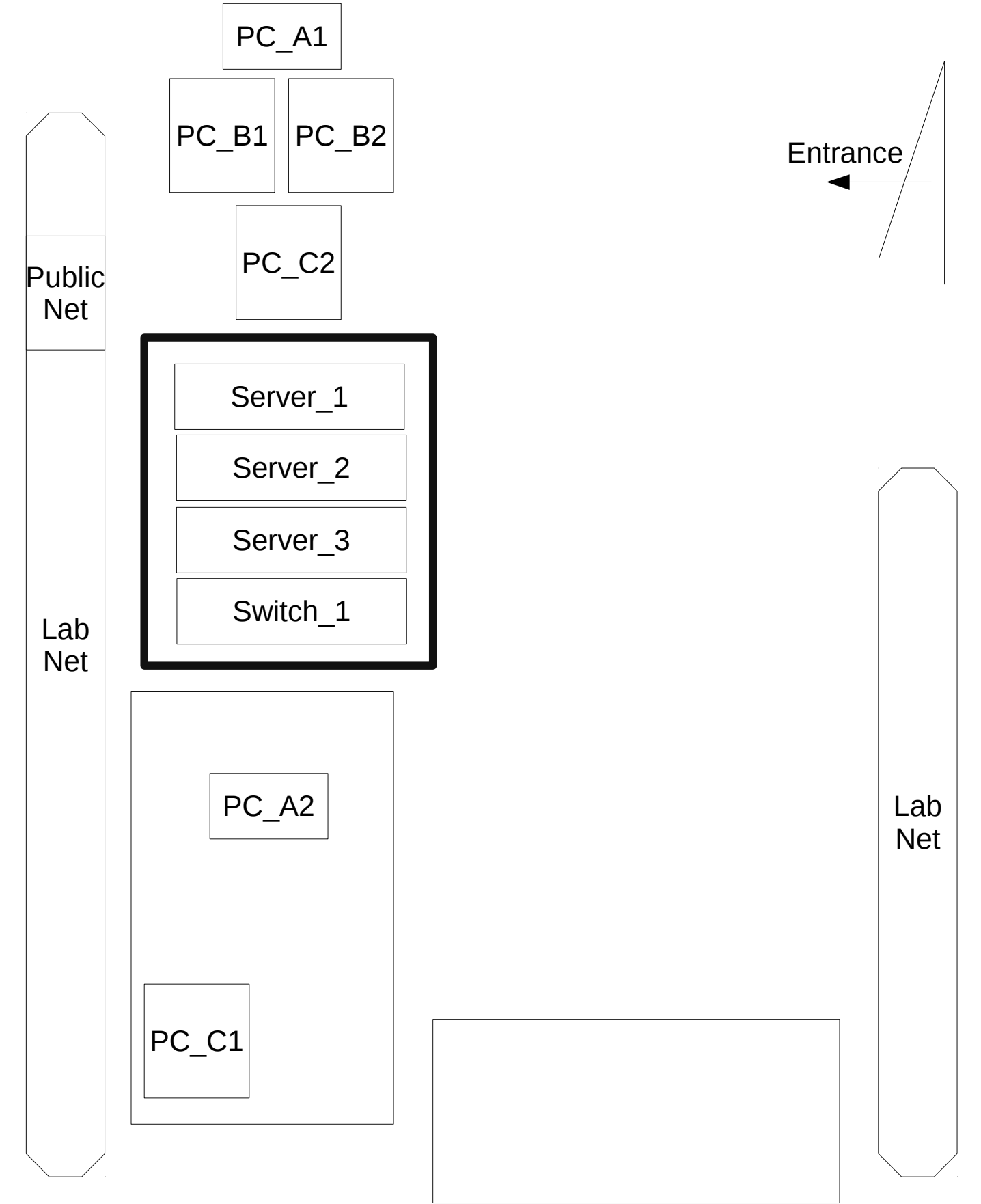


SEIP Lab Setup Description

Lab layout



Machine descriptions

Machine responsibilities:

OpenStack nodes: Server_1, Server_2, Server_3, PC_B1, PC_B2

Fuel manager: PC_A1

Lab terminal: PC_C1

Public access firewall: PC_C2

OpenStack infrastructure switch: Switch_1

Miscellaneous: PC_A2

Set machine network addresses:

Switch_1: 10.30.0.2

PC_A1: 10.20.0.2, 10.30.0.3

PC_C1: 10.20.0.6, 10.30.0.4

PC_C2: 10.30.0.1

Fuel and OpenStack access

All laboratory access is conducted from PC_C1 terminal

Access fuel over ssh through terminal with command:

```
ssh root@10.20.0.2
```

Access fuel web GUI over browser through address: 10.20.0.2

Fuel ssh password is r00tme

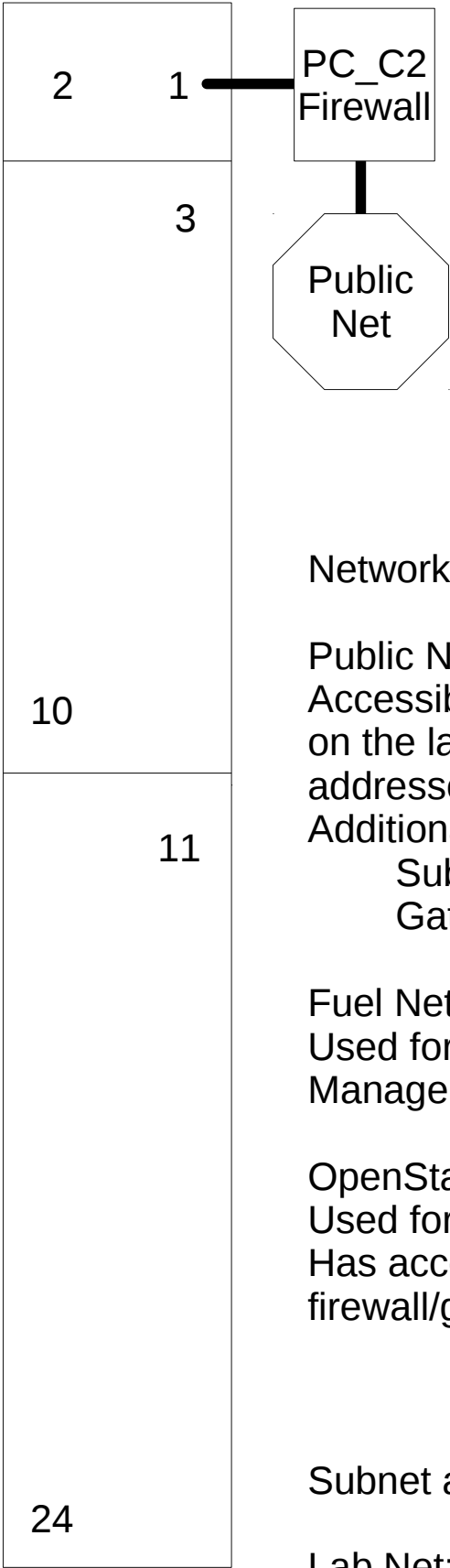
Fuel web credentials are: username: admin password: AkX3UrB9!

OpenStack Horizon access over browser using controller IP address, can be found in fuel web GUI. The standard public IP address is 161.53.40.188

SSH access to OpenStack nodes over fuel manager. SSH to fuel then from there ssh to wanted OpenStack node

Network descriptions

Switch_1
end port start port



Networks / ports :

OpenStack Net / 1-2 11-24
Fuel Net / 3-10

Reserved ports:

1 – Connects to Firewall

Network descriptions:

Public Net:
Accessible trough the 15205-x1 ethernet socket
on the laboratory wall. The available public IP
addresses are 161.53.40.188 and 161.53.40.189
Additional information:
 Subnet mask: 255.255.255.0
 Gateway: 161.53.40.8

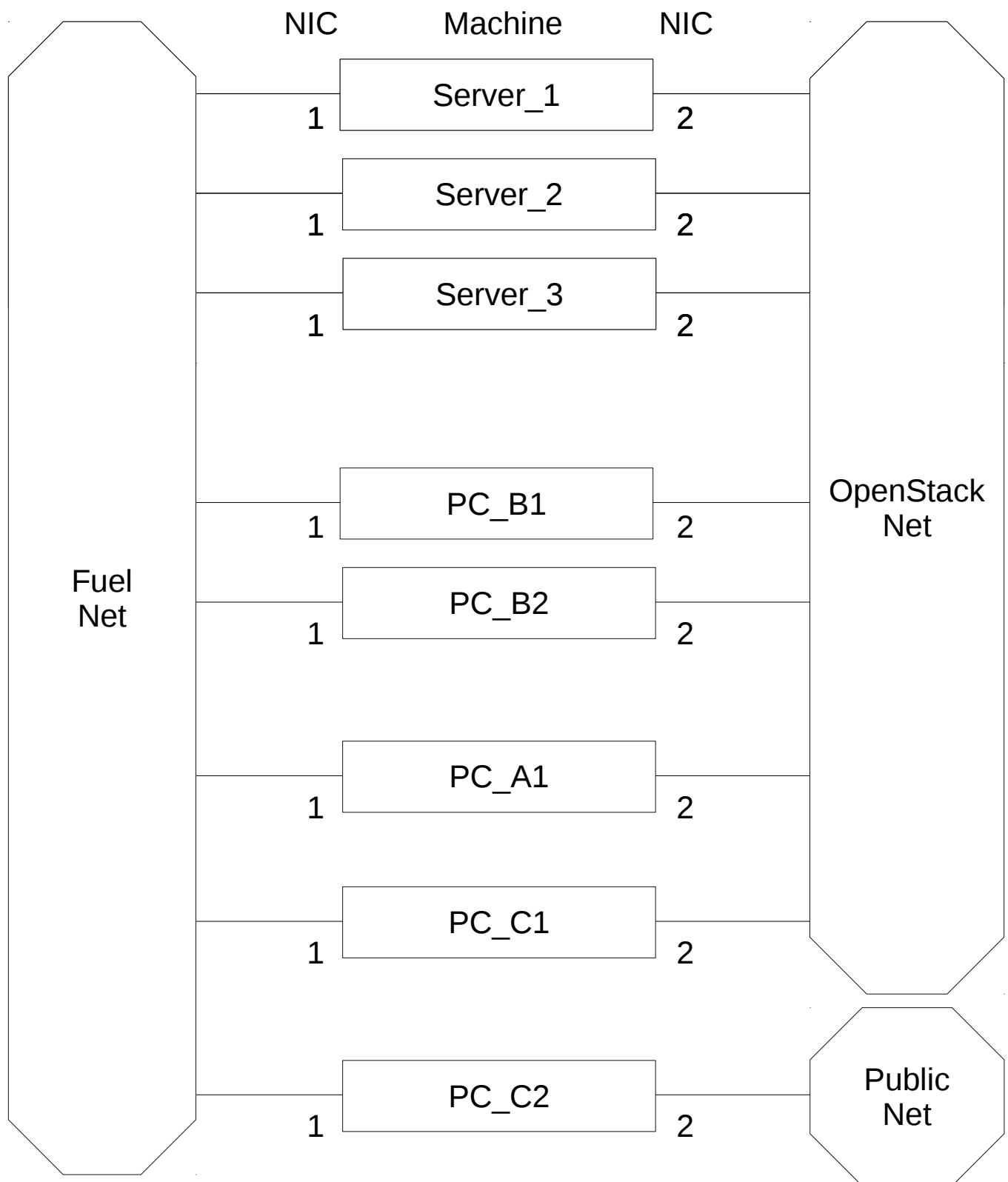
Fuel Net:
Used for Mirantis OpenStack Deployment and
Management

OpenStack Net:
Used for OpenStack infrastructure (multiple VLANs)
Has access to the public network over the
firewall/gateway computer PC_C2

Subnet addresses:

Lab Net: 10.30.0.0/16
Fuel Net: 10.20.0.0/24

Machine network connections



How to know NIC (network interface controller) number on hardware:

Server NIC labeled on the servers itself

PC NIC 1 – PCI express NIC

PC NIC 2 – Motherboard NIC

Proper Fuel settings

Dashboard

Nodes

Networks

Settings

Logs

Health Check

Success

Deployment is done. No changes.
Provision of environment 'OpSt1' is done.

Horizon

The OpenStack dashboard Horizon is now available. For documentation and tutorial videos to help Operators and Developers get up and running faster, see the [Get Started page](#)

Summary

Name

OpSt1

Status

Operational

OpenStack Release

Mitaka on Ubuntu 14.04

Compute

QEMU

Network

Neutron with tunneling segmentation

Storage Backends

Cinder Block device driver
Cinder LVM over ISCSI for volumes

To view the OpenStack health check status go to [Healthcheck tab](#)

Delete Environment

Reset Environment

Capacity

CPU (Cores)	5 (18)	RAM	36.0 GB	HDD	4.5 TB
-------------	--------	-----	---------	-----	--------

Node Statistics

Total Nodes

5

Ready

5

Controller

1

Compute

3

Cinder

1

Cinder Block Device

1

Telemetry - MongoDB

1

+ Add Nodes

Proper Fuel settings

Home / Environments / OpSt1 / Networks

OpSt1 (5 nodes)

Dashboard

Nodes

Networks

Settings

Logs

Health Check

Network Settings (Neutron with tunneling segmentation)

+ Add New Node Network Group

Node Network Groups

default

Settings

Neutron L2

Neutron L3

Other

Network Verification

Connectivity Check

default

This node network group uses a shared admin network and cannot be deleted

Public

The Public network allows inbound connections to VMs (Controllers and Tenant VMs) from external networks (e.g., the Internet) as well as outbound connections from VMs to the external networks.

CIDR

10.30.0.0/16

☐ Use the whole CIDR

Start

End

IP Range

10.30.1.1

10.30.1.255

+

Gateway

10.30.0.1

Use VLAN tagging

☐

Storage

The Storage network is used to provide storage services such as replication traffic from Ceph. The Management network is used for Ceph Public traffic.

CIDR

192.168.1.0/24

☒ Use the whole CIDR

Start

End

IP Range

192.168.1.1

192.168.1.254

+

Use VLAN tagging

☒

21

Management

The Management network is primarily used for OpenStack Cloud Management. It is used to access OpenStack services (nova-api, OpenStack dashboard, etc).

CIDR

192.168.0.0/24

☒ Use the whole CIDR

Start

End

IP Range

192.168.0.1

192.168.0.254

+

Use VLAN tagging

☒

22

Private

The private network facilitates communication between each tenant's VMs. Private network address spaces are not a part of the public network address space; fixed IPs of virtual instances cannot be accessed directly from the rest of the public network.

CIDR

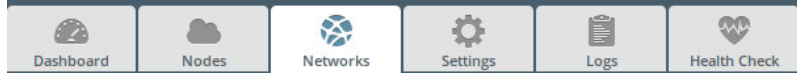
192.168.0.0/24

☒ Use the whole CIDR

Proper Fuel settings

Home / Environments / OpSt1 / Networks

OpSt1 (5 nodes)



Network Settings (Neutron with tunneling segmentation)

+ Add New Node Network Group

Node Network Groups

default

Settings

Neutron L2

Neutron L3

Other

Network Verification

Connectivity
Check

Floating Network Parameters ?

This network is used to assign Floating IPs to tenant VMs.

	Start	End
Floating IP range	<input type="text" value="10.30.2.1"/>	<input type="text" value="10.30.250.255"/>
Floating network name	<input type="text" value="admin_floating_net"/>	

Admin Tenant Network Parameters ?

This Admin Tenant network provides internal network access for Instances. It can be used only by the Admin tenant.

Admin Tenant network CIDR	<input type="text" value="192.168.111.0/24"/>
Admin Tenant network gateway	<input type="text" value="192.168.111.1"/>
Admin Tenant network name	<input type="text" value="admin_internal_net"/>

Proper Fuel settings

Dashboard

Nodes

Networks

Settings

Logs

Health Check

Configure Disks

Configure Interfaces

+ Add Nodes

Sort By

Roles

Select All

Controller (1)

Select All

Fujitsu1

CONTROLLER

READY

CPU: 1 (2) RAM: 8.0 GB HDD: 465.8 GB

Compute (2)

Select All

HP1

COMPUTE

READY

CPU: 1 (6) RAM: 8.0 GB HDD: 931.5 GB

HP2

COMPUTE

READY

CPU: 1 (4) RAM: 8.0 GB HDD: 931.5 GB

Compute, Cinder Block Device (1)

Select All

HP3

COMPUTE - CINDER-BLOCK-DEVICE

READY

CPU: 1 (4) RAM: 8.0 GB HDD: 1.8 TB

Cinder, Telemetry - MongoDB (1)

Select All

Fujitsu2

CINDER - MONGO

READY

CPU: 1 (2) RAM: 4.0 GB HDD: 465.8 GB

Connecting a public IP to a local IP



Logout Help

System Status Network Services **Firewall** Proxy VPN Logs and Reports

Port forwarding / NAT

Outgoing traffic
Inter-Zone traffic
VPN traffic
System access
Firewall Diagrams

Port forwarding / Destination NAT

>> Port forwarding / Destination NAT Source NAT Incoming routed traffic

>> Current rules

[Add a new Port forwarding / Destination NAT rule](#)

#	Incoming IP	Service	Policy	Translate to	Remark	Actions
1	161.53.40.188 (Uplink main)	TCP/80		10.30.1.2 : 80		
	ALLOW with IPS from:		<ANY>			
2	161.53.40.188 (Uplink main)	TCP/443		10.30.1.2 : 443		
	ALLOW with IPS from:		<ANY>			

Legend: ☒ Enabled (click to disable) ☐ Disabled (click to enable) Edit Remove

Show system rules >>

Status: Connected: main (12d 5h 45m 18s) Uptime: 15:34:30 up 12 days, 5:45, 0 users, load average: 0.00, 0.02, 0.05

Endian Firewall Community release 3.2.0beta1 (c) Endian

The firewall/gateway can be configured to forward traffic over specific ports To specific ip/port destinations that are within the OpenStack Net range.

A new forwarding rule is added with the “Add a new Port forwarding /Destination NAT rule” link

The available public IP addresses are 161.53.40.188 and 161.53.40.189

The picture above contains two rules that forward HTTP and HTTPS traffic from the 161.53.49.188 public ip to the 10.30.1.2 local ip that is the Horizon web GUI. Those rules grant as access to the web GUI from any device connected to the internet.

Adding firewall rules



Logout Help

System Status Network Services **Firewall** Proxy VPN Logs and Reports

Port forwarding / NAT

Outgoing traffic

Inter-Zone traffic

VPN traffic

System access

Firewall Diagrams

Outgoing firewall configuration

>> Current rules

[Add a new firewall rule](#)

#	Source	Destination	Service	Policy	Remark	Actions
1	GREEN BLUE	RED	TCP/80		allow HTTP	
2	GREEN BLUE	RED	TCP/443		allow HTTPS	
3	GREEN	RED	TCP/21		allow FTP	
4	GREEN	RED	TCP/25		allow SMTP	
5	GREEN	RED	TCP/110		allow POP	
6	GREEN	RED	TCP/143		allow IMAP	
7	GREEN	RED	TCP/995		allow POP3s	
8	GREEN	RED	TCP/993		allow IMAPs	
9	GREEN ORANGE BLUE	RED	TCP+UDP/53		allow DNS	
10	GREEN ORANGE BLUE	RED	ICMP/8 ICMP/30		allow PING	
11	GREEN	RED	UDP/123		allow ntp	
12	GREEN	RED	TCP/873		allow rsync protocol	
13	GREEN	RED	TCP/22		allow SSH	

Legend Enabled (click to disable) ☐ Disabled (click to enable) Edit Remove

Show system rules >>

>> Outgoing Firewall Settings

Enable Outgoing firewall

To allow new types of traffic between the Public net and the OpenStack Net One must add a new firewall rule to the Firewall over the interface shown above. This is needed if an application is using ports not currently allowed.

Note that if one wishes to forward a port as described on the previous page, that port needs to be allowed by a firewall rule.