Assignment Information				
Name:	Mario Morales		Assignment:	Project 1
Date Submitted:			Course Section:	
Course:	COSN 215			

The purpose of this project is to set up a working DMZ network within VirtualBox. This network will be used throughout the course and you will continue to expand it.

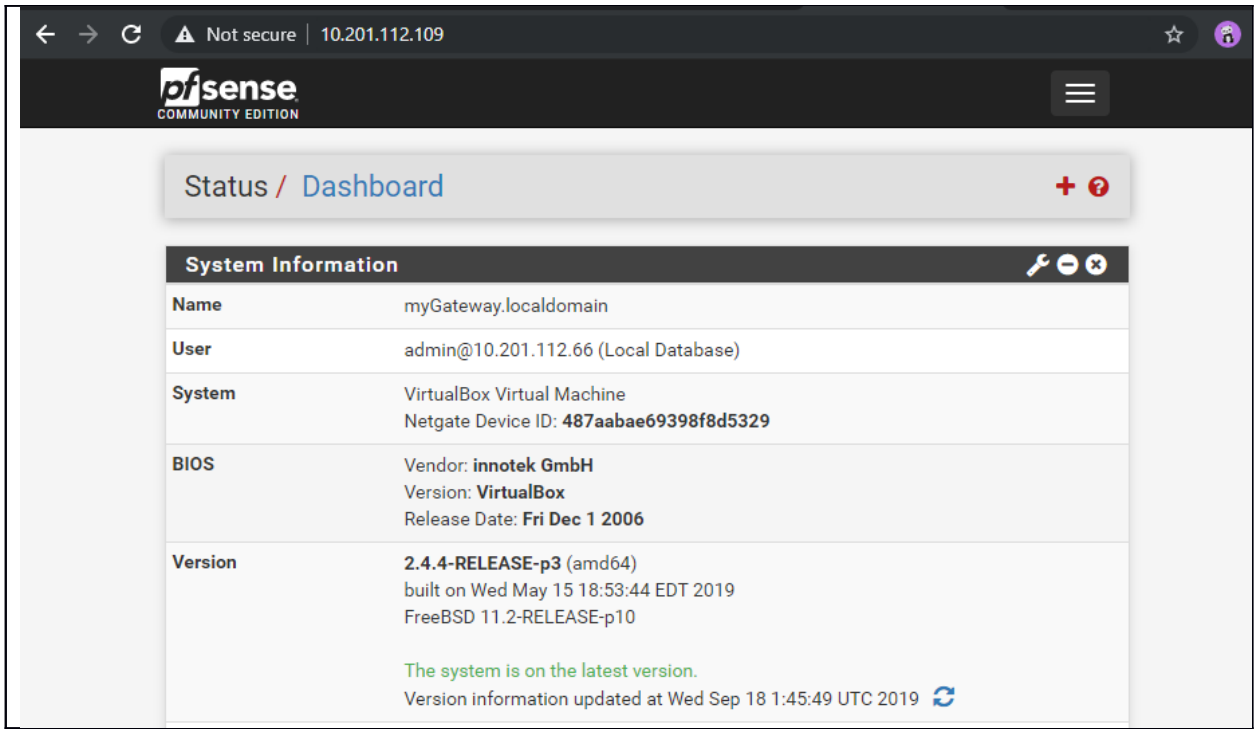
Phase 0

Enable ssh within **myGateway**. Then turn it off, and restart it in headless mode. Then ssh into **myGateway** as root from **myClient** and paste a screenshot below:

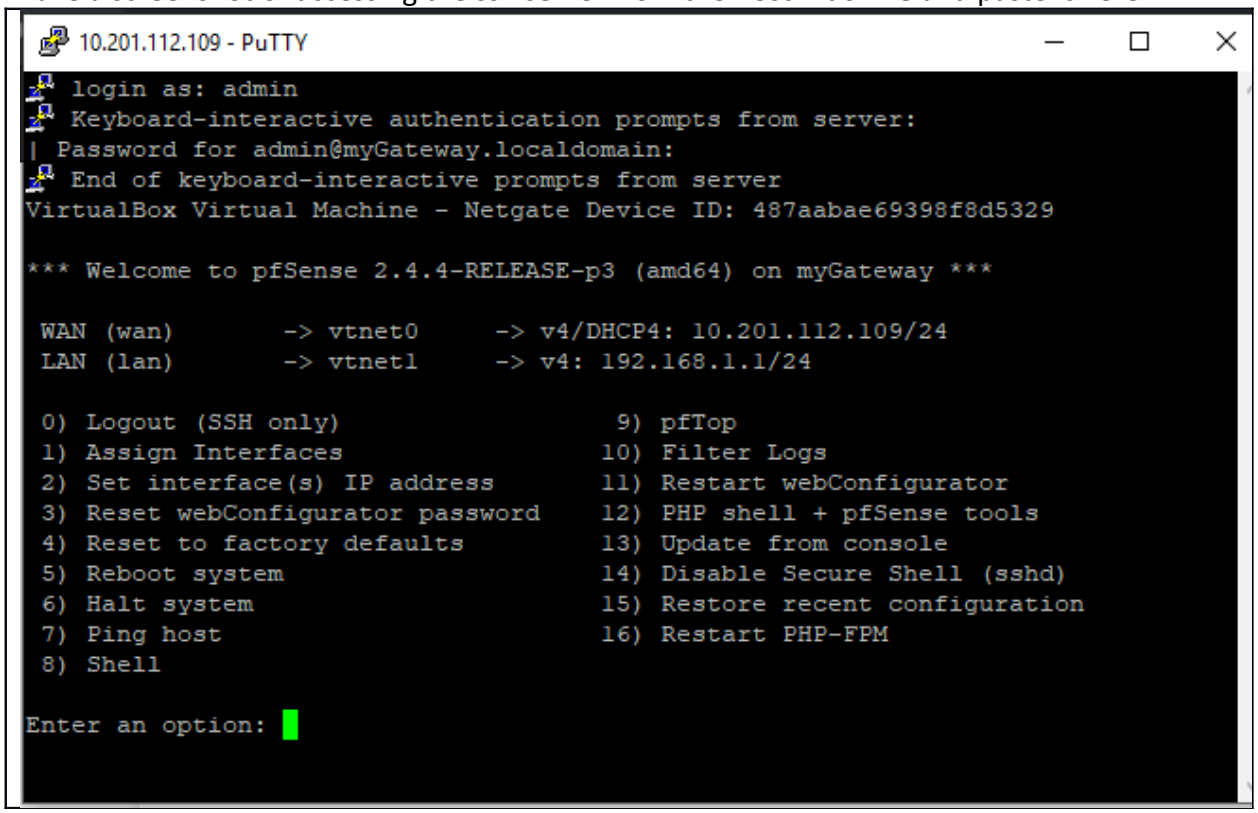
```
student@student-VirtualBox:~$ ssh -l admin 192.168.1.1
Password for admin@myGateway.localdomain:
VirtualBox Virtual Machine - Netgate Device ID: 487aabae69398f8d5329

*** Welcome to pfSense 2.4.4-RELEASE-p3 (amd64) on myGateway ***

 WAN (wan)       -> vtnet0     -> v4/DHCP4: 10.201.112.109/24
 LAN (lan)       -> vtnet1     -> v4: 192.168.1.1/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Disable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option:
```

You will no longer need to access **myGateway** directly.

It would be nice if you didn't need to use **myClient** to control **myGateway** too. Configure **myGateway**'s firewall to allow https and ssh traffic from the WAN in to itself. Take a screenshot of accessing the web interface from the **host machine** and paste it here:

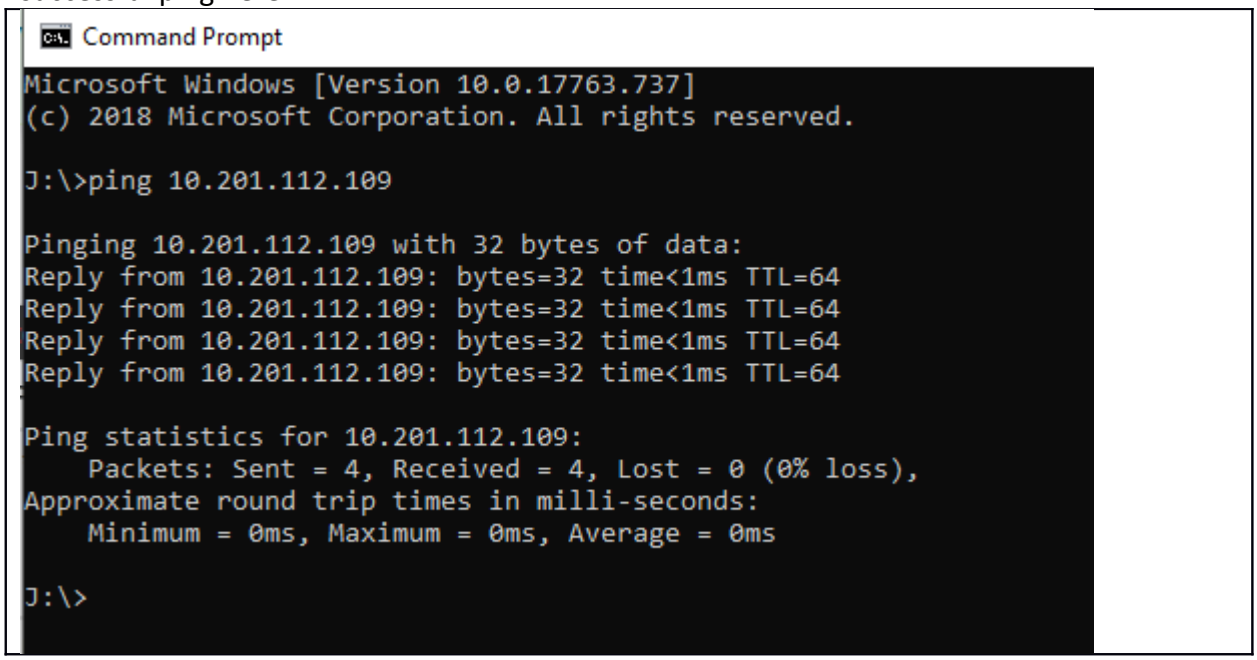


Take a screenshot of accessing the ssh server from the **host machine** and paste it here:



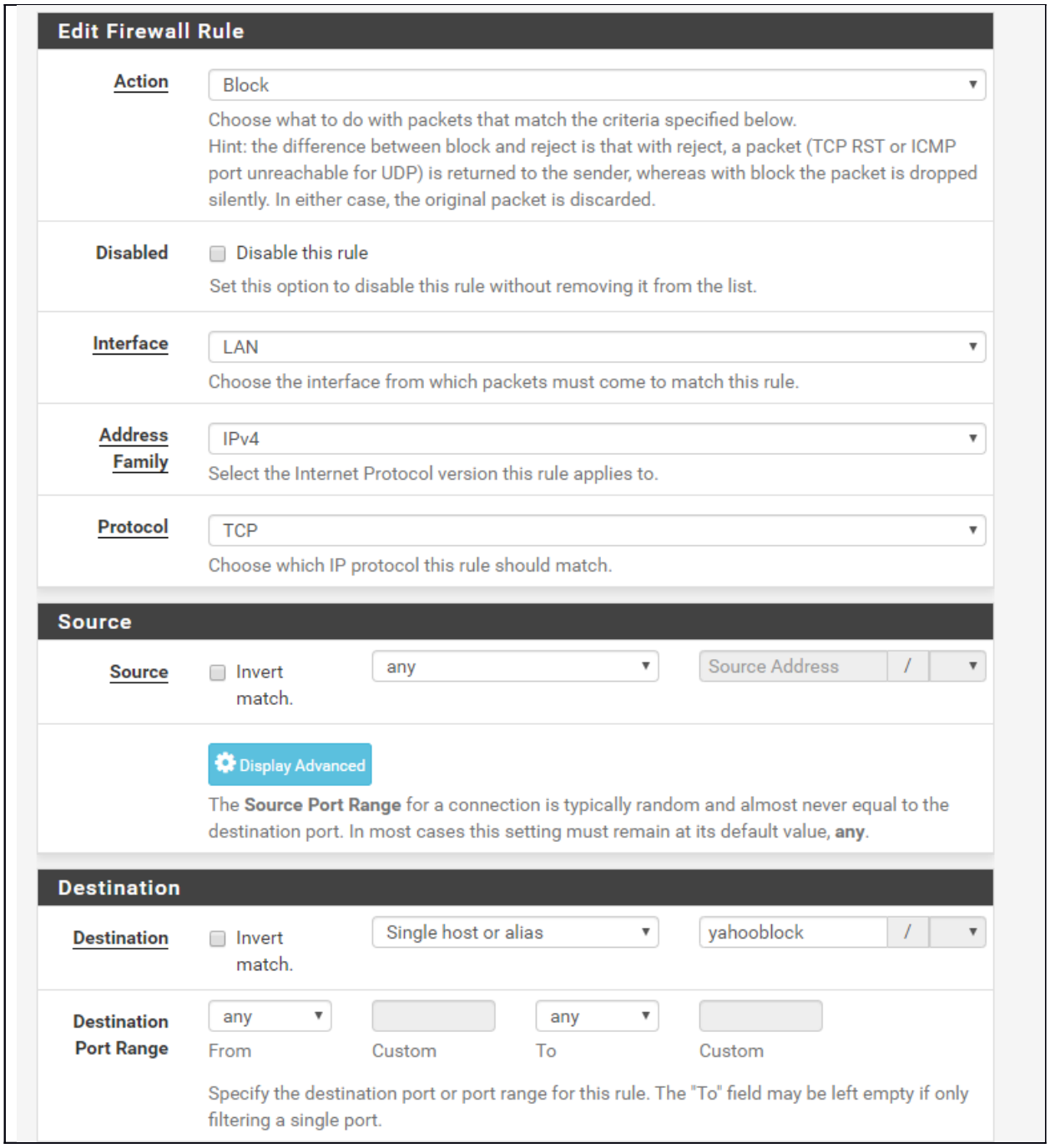
You will no longer need to access **myGateway** through **myClient**, you can do it entirely from the **host machine**.

If we are trouble shooting **myGateway** it is helpful if we can ping it from the **host machine**. Change the firewall rules so that **myGateway** only is pingable from the WAN and paste a successful ping here:



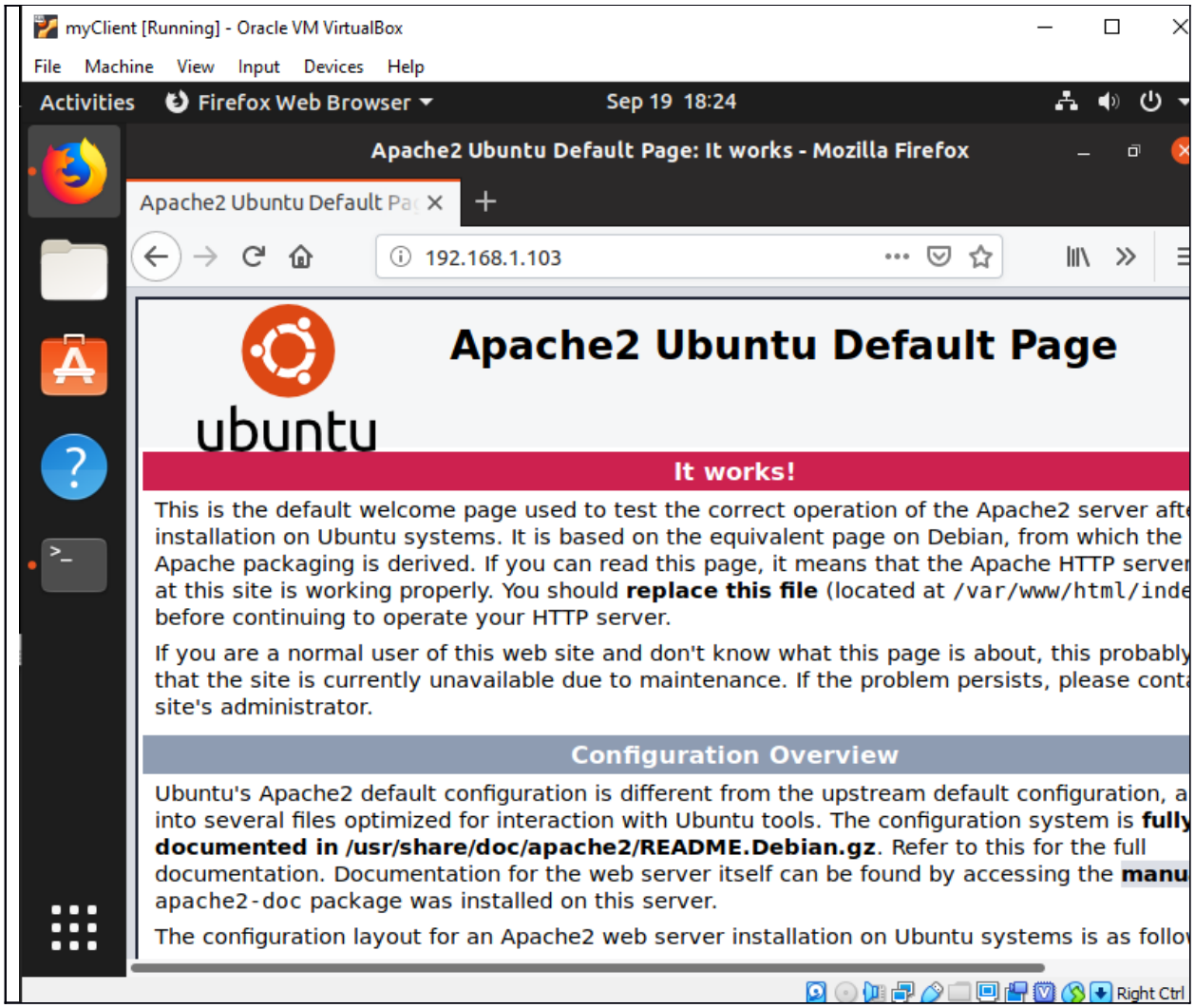
Phase 0.5

You have noticed that Phil, the lazy guy who works on **myClient,** farting around on www.yahoo.com all day. Block it and show the rule implementation here:



Phase 1

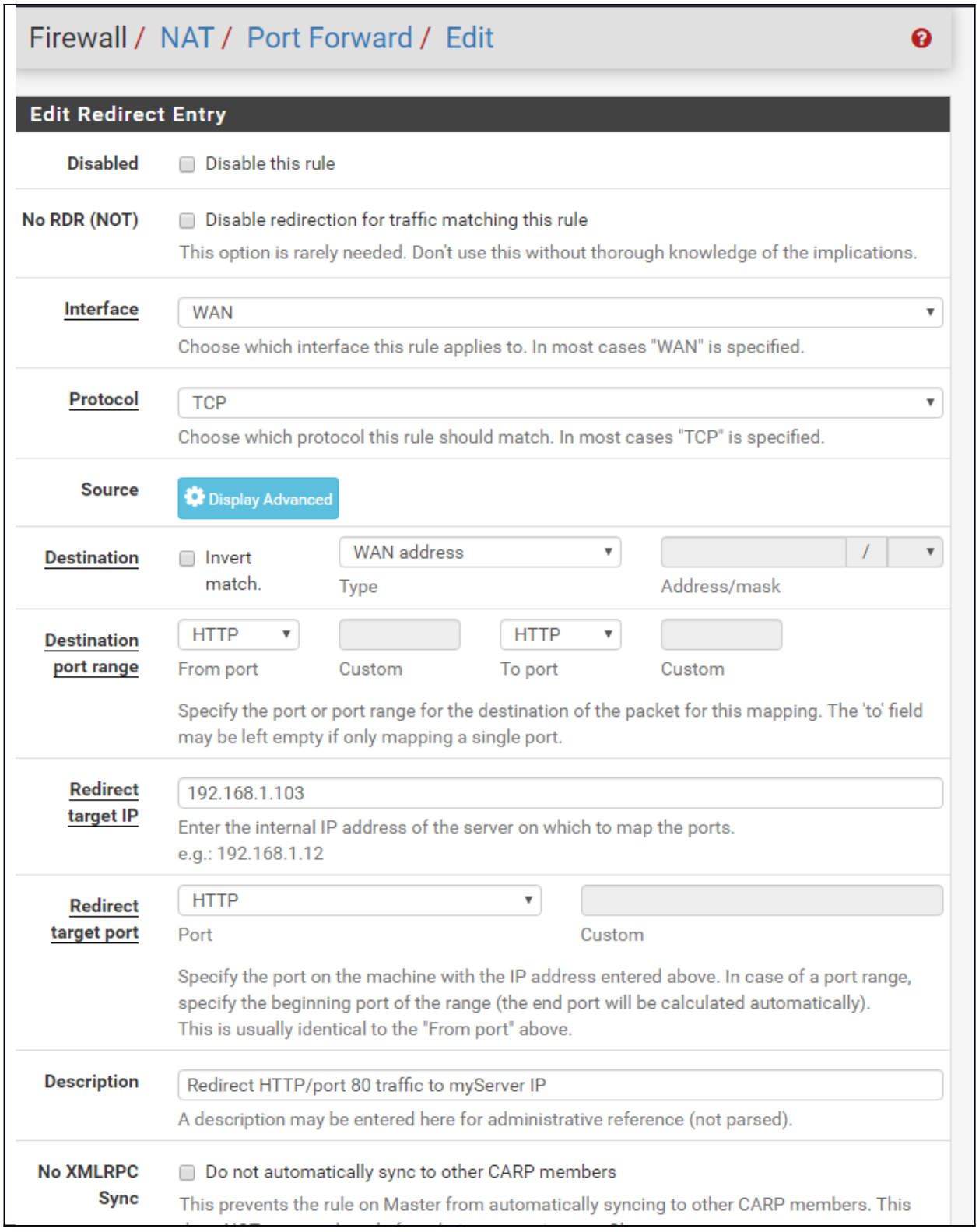
On **myServer**, install Apache Web Server and verify it is working correctly by connecting from **myClient** using the web browser. Paste a screenshot here:

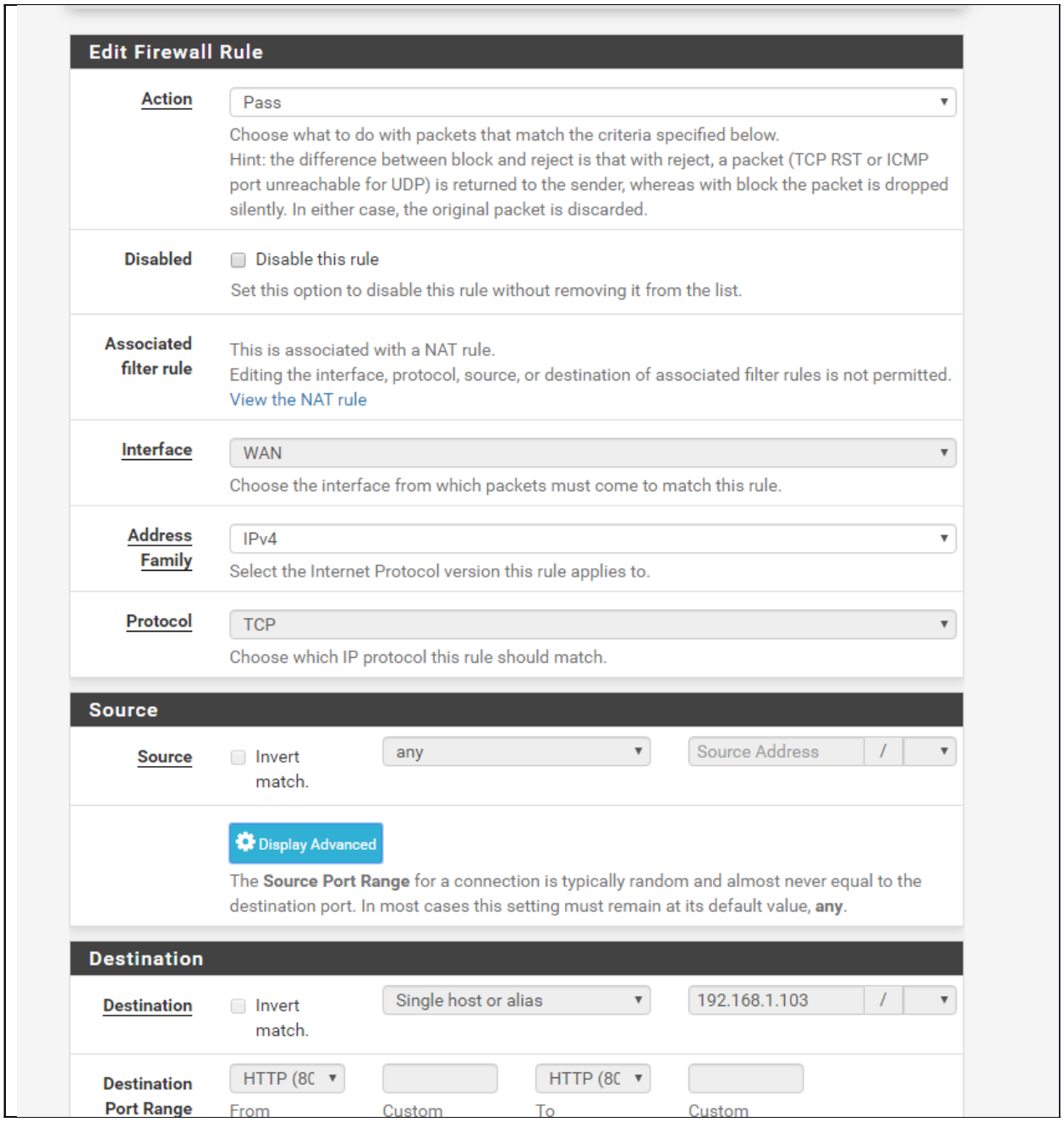


Change the Apache homepage to say anything you like (that is not vulgar) and access it from **myClient** again. Paste a screenshot here:

Now lets set up **myGateway** to forward port 80 traffic to **myServer** from the WAN so that we don't need to access **myClient** in order to view the web page. Then we'll be that much closer getting rid of that lazy SOB Phil!

Paste a screenshot of the NAT and associated firewall rule here:

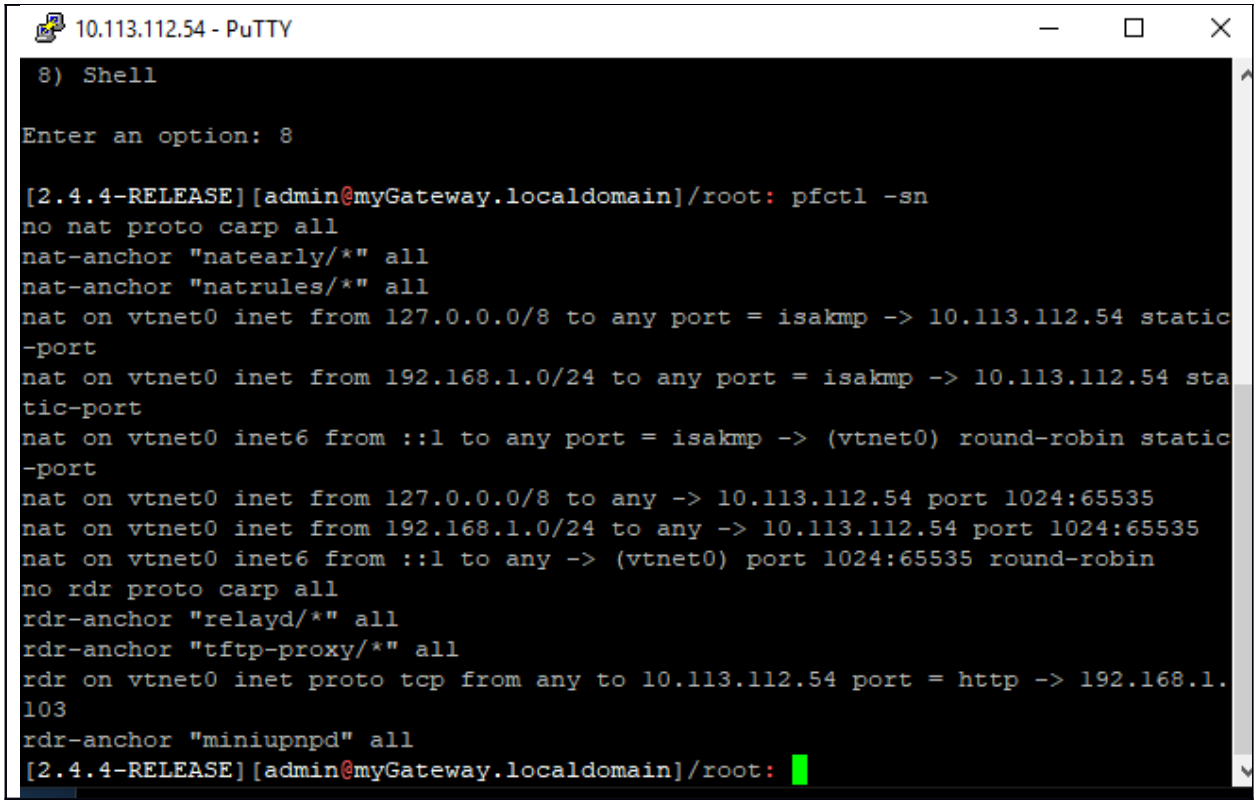

Firewall / NAT / Port Forward / Edit
Edit Redirect Entry
Disabled
Disable this rule
No RDR (NOT)
Disable redirection for traffic matching this rule
This option is rarely needed. Don't use this without thorough knowledge of the implications.
Interface
WAN
Choose which interface this rule applies to. In most cases "WAN" is specified.
Protocol
TCP
Choose which protocol this rule should match. In most cases "TCP" is specified.
Source
Display Advanced
Destination
Invert match.
WAN address
Type
Address/mask
Destination port range
HTTP
From port
Custom
HTTP
To port
Custom
Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.
Redirect target IP
192.168.1.103
Enter the internal IP address of the server on which to map the ports.
e.g.: 192.168.1.12
Redirect target port
HTTP
Port
Custom
Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically).
This is usually identical to the "From port" above.
Description
Redirect HTTP/port 80 traffic to myServer IP
A description may be entered here for administrative reference (not parsed).
No XMLRPC Sync
Do not automatically sync to other CARP members
This prevents the rule on Master from automatically syncing to other CARP members. This



Paste a screenshot of successfully accessing the web page from the **host machine** here:

Phase 2

Use ssh to connect to **myGateway** from the **host machine**. Get a shell, and then show the NAT rules and paste them here:



Which rule will forward web traffic from the WAN to **myServer**?

```
rdr on vtnet0 inet proto tcp from any to 10.113.112.54 port = http -> 192.168.1.
103
```

What would the command be, using **pfctl**, to add that rule manually?

Pfctl –T add [address]

-T *command* [*address* ...]
Specify the *command* (may be abbreviated) to apply to the table. Commands include:

-T kill Kill a table.
-T flush Flush all addresses of a table.
-T add Add one or more addresses in a table. Automatically create a persistent table if it does not exist.
-T delete Delete one or more addresses from a table.
-T expire *number*
Delete addresses which had their statistics cleared more than *number* seconds ago. For entries which have never had their statistics cleared, *number* refers to the time they were added to the table.
-T replace Replace the addresses of the table. Automatically create a persistent table if it does not exist
-T show Show the content (addresses) of a table.
-T test Test if the given addresses match a table.
-T zero Clear all the statistics of a table.

For the **add**, **delete**, **replace**, and **test** commands, the list of addresses can be specified either directly or the command line and/or in an unformatted text file, using the **-f** flag. Comments starting with a '#' are allowed in the text file. With these commands, the **-v** flag can also be used once or twice, in which case **pfctl** will print the detailed result of the operation for each individual address, prefixed by one of the following letters:

A The address/network has been added.
C The address/network has been changed (negated).
D The address/network has been deleted.
M The address matches (**test** operation only).
X The address/network is duplicated and therefore ignored.
Y The address/network cannot be added/deleted due to conflicting '!' attributes.
Z The address/network has been cleared (statistics).

Each table can maintain a set of counters that can be retrieved using the **-v** flag of **pfctl**. For example, the following commands define a wide open firewall which will keep track of packets going to or coming from the OpenBSD FTP server. The following commands configure the firewall and send 10 pings to the FTP server:

```
# printf "table <test> counters { ftp.openbsd.org }\n \
    pass out to <test>\n" | pfctl -f-
# ping -qc10 ftp.openbsd.org
```