LAB REPORT 2

ECE 455

ODU Honor pledge

"I pledge to support the Honor System of Old Dominion University.

I will refrain from any form of academic dishonesty or deception, such as cheating or plagiarism. I am aware that as a member of the academic community it is my responsibility to turn in all suspected violation of the Honor Code. I will report to a hearing if summoned."

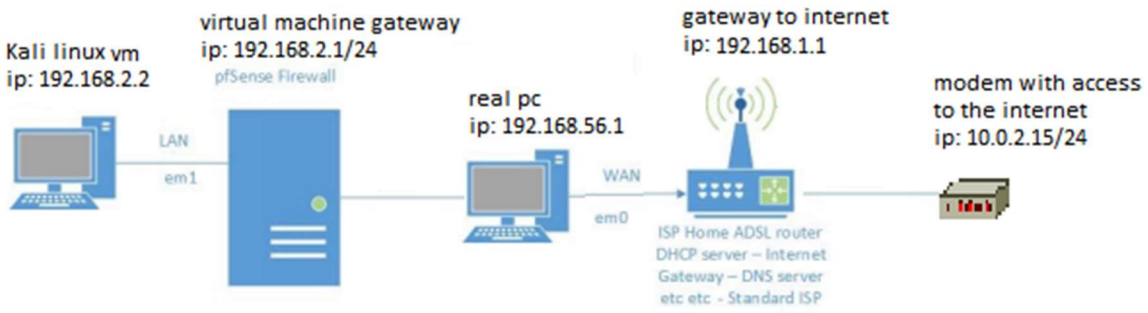
Your name: Bradley McKee

UIN: 00975338

Sign here: BLM (initials represent signature)

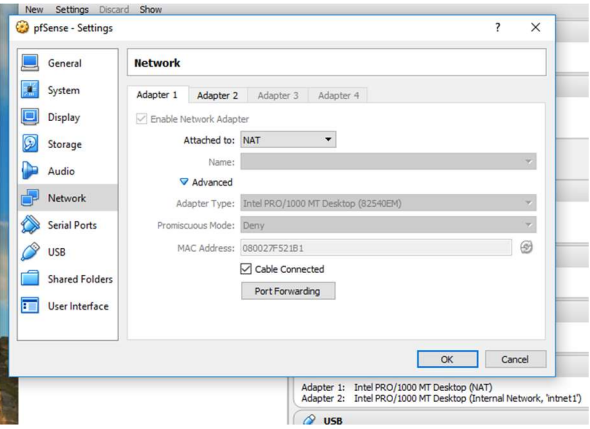
In this lab we were instructed to do the networking lab with a program called pfSense. After reading the lab I decided that it would make it a lot easier on myself if I had a computer than ran Kali Linux. I decided to make a partition on my laptop and install kali linux mainly because it comes with all the software we will be using this semester. Last semester I became familiar with using Wireshark in ECE 355. The main purpose of this lab is to perform and understand basic firewall procedures and we use wireshark to analyze which packets and what type of protocols is being sent /received. Attached will be screenshots taken from my laptop as proof that I went through and completed the lab.

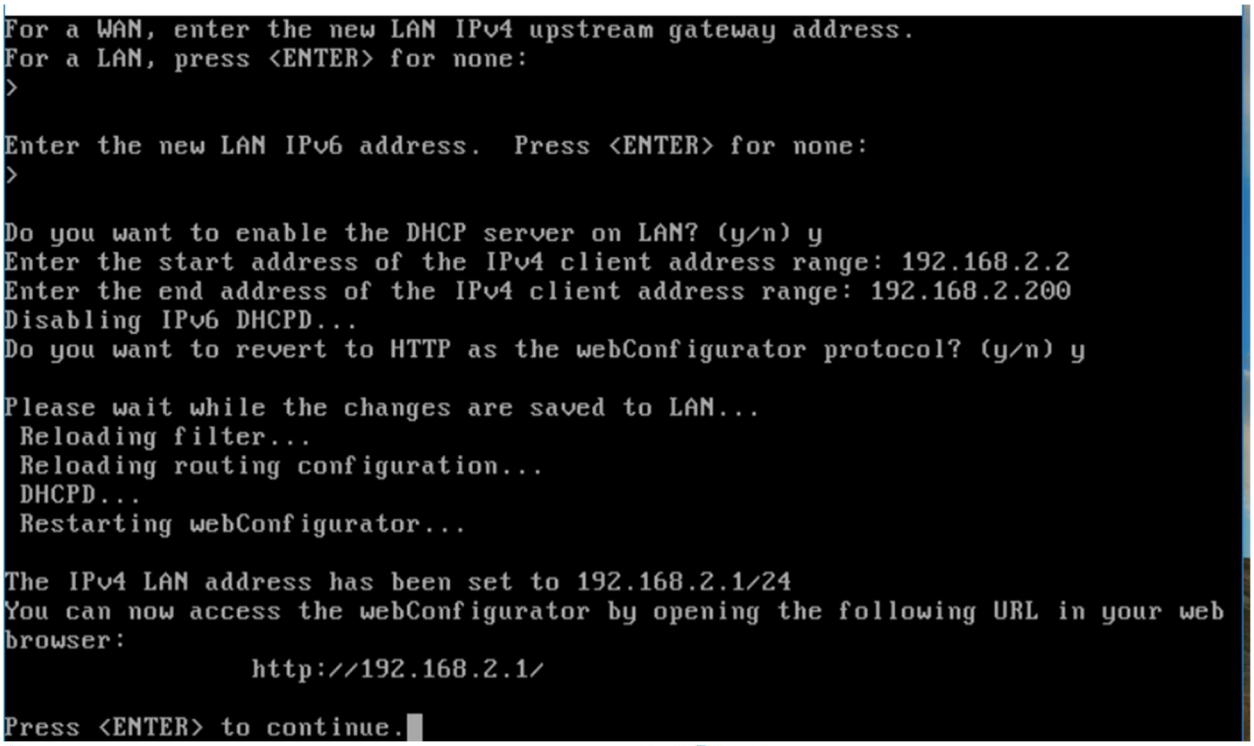
The topology of my network is very simple. The virtual machine that I ran was Kali linux, that had an internal network linked only to pfSense. pfSense acts like a gateway from the internal network to the physical network that has access to the internet. The kali virtual machine (vm) had access to the virtual machine firewall (basically it's only way to access the internet so I called it a gateway) the connection of that passes through the real physical computer to see what the DHCP4 gateway which gives it access to the internet. The firewall is used to pass, reject, and block certain ports and allow certain types of traffic between internal as well as external ip addresses. The physical computer and router just pass this information to the modem which has access to the internet. The router acts like a dns server to the pfSense. The dns server/router has an ip: 10.0.2.15/24 to the virtual machine. The modem has a real ip of 127.0.0.1 but it is indirectly connected to pfSense.

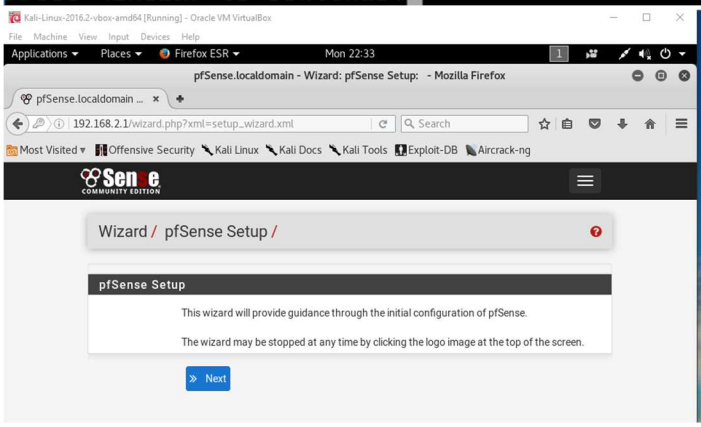


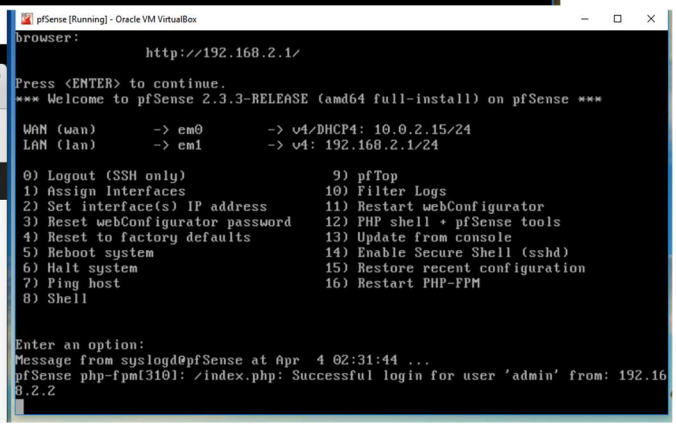
```
Generating RRD graphs...done.
Starting syslog...done.
Starting CRON... done.
pfSense (pfSense) 2.3.3-RELEASE amd64 Thu Feb 16 06:59:53 CST 2017
Bootup complete

FreeBSD/amd64 (pfSense.localdomain) (ttyv0)

*** Welcome to pfSense 2.3.3-RELEASE (amd64 full-install) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 10.0.2.15/24
 LAN (lan)       -> em1        ->

 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) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option:
```

```
 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) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option: 1

Valid interfaces are:

em0    08:00:27:f5:21:b1   (up) Intel(R) PRO/1000 Legacy Network Connection 1.1.
em1    08:00:27:f6:8e:87   (up) Intel(R) PRO/1000 Legacy Network Connection 1.1.

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y|n]?
```

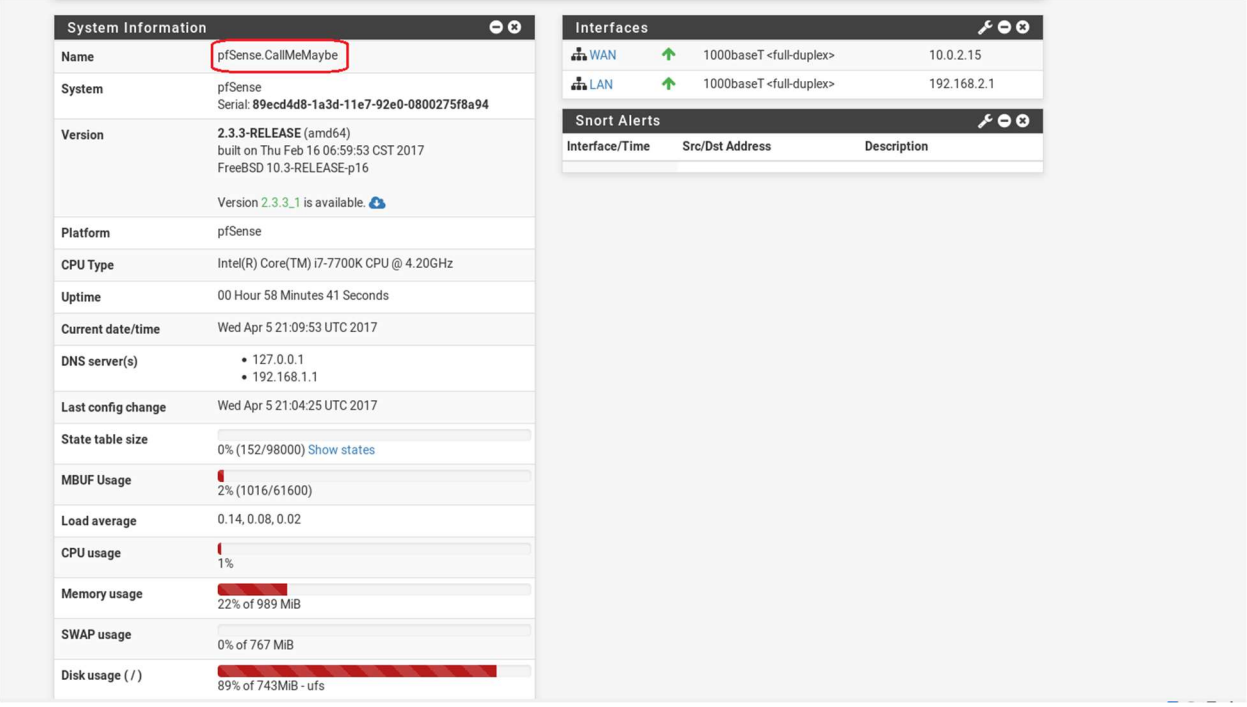



For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>
Enter the new LAN IPv6 address. Press <ENTER> for none:
>
Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 192.168.2.2
Enter the end address of the IPv4 client address range: 192.168.2.200
Disabling IPv6 DHCPD...
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) y
Please wait while the changes are saved to LAN...
Reloading filter...
Reloading routing configuration...
DHCPD...
Restarting webConfigurator...
The IPv4 LAN address has been set to 192.168.2.1/24
You can now access the webConfigurator by opening the following URL in your web browser:
http://192.168.2.1/
Press <ENTER> to continue.

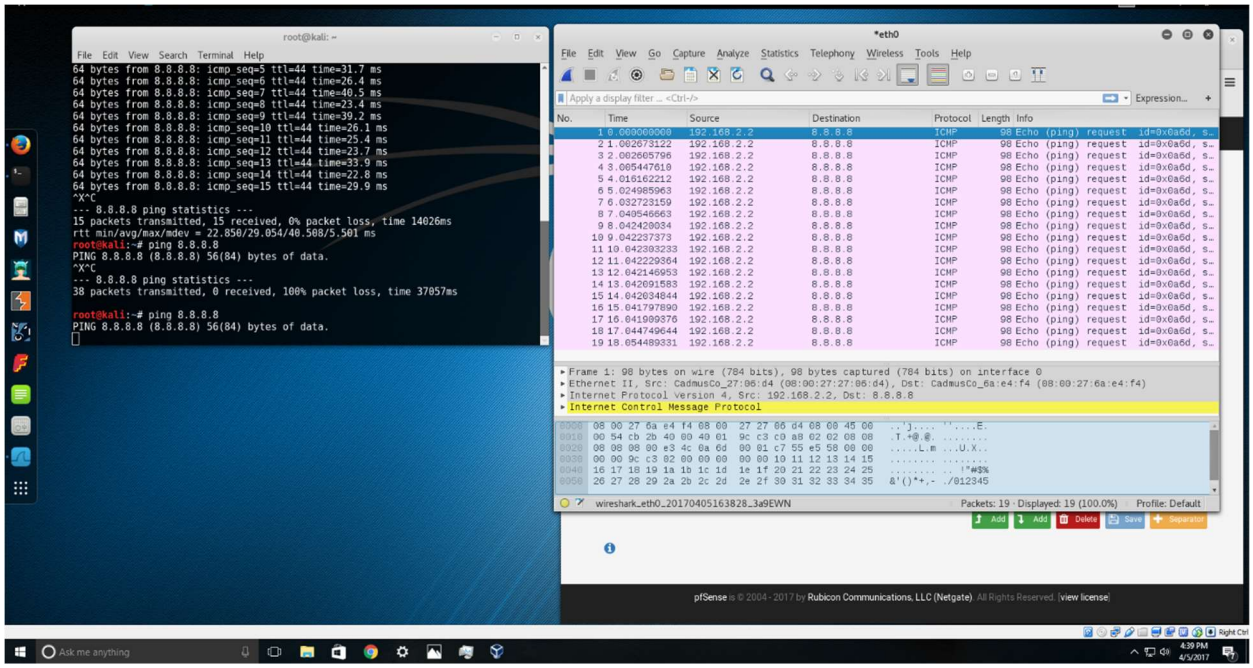

Kali-Linux-2016.2-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Firefox ESR Mon 22:33
pfSense.localdomain - Wizard: pfSense Setup: - Mozilla Firefox
pfSense.localdomain ...
192.168.2.1/wizard.php?xml=setup_wizard.xml
Search
Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng
COMMUNITY EDITION
Wizard / pfSense Setup /
pfSense Setup
This wizard will provide guidance through the initial configuration of pfSense.
The wizard may be stopped at any time by clicking the logo image at the top of the screen.
Next

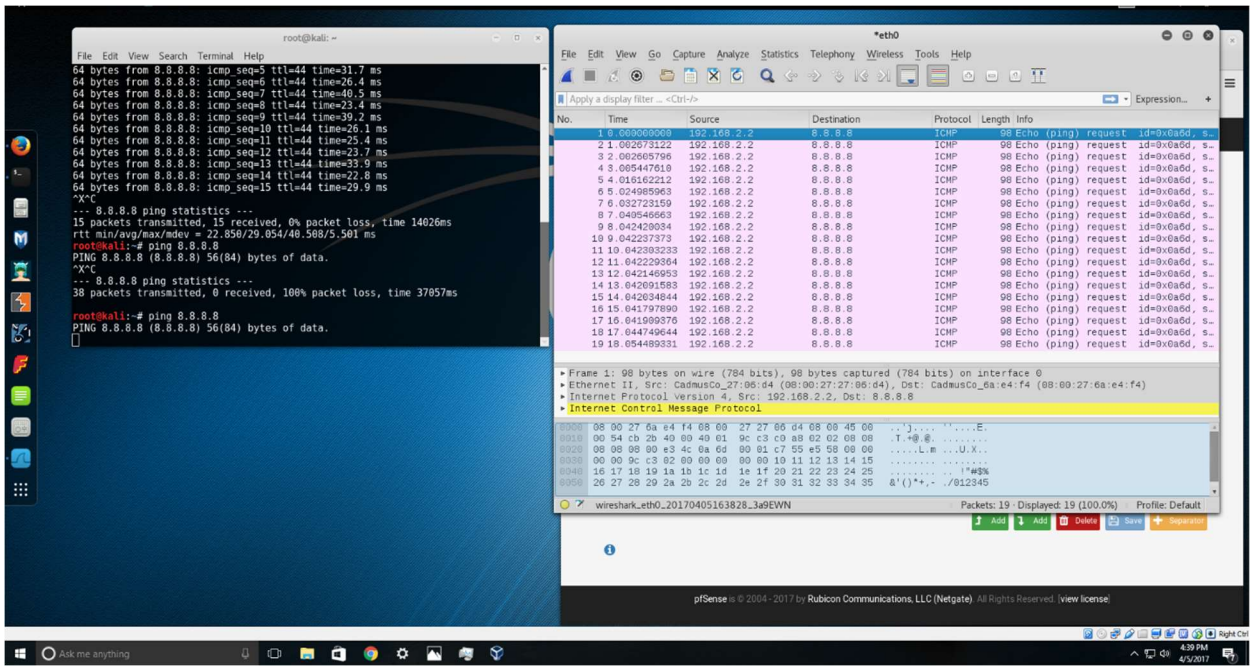

pfSense [Running] - Oracle VM VirtualBox
browser:
http://192.168.2.1/
Press <ENTER> to continue.
*** Welcome to pfSense 2.3.3-RELEASE (amd64 full-install) on pfSense ***
WAN (wan) -> em0 -> v4/DHCP4: 10.0.2.15/24
LAN (lan) -> em1 -> v4: 192.168.2.1/24
0) Logout (SSH only) 9) pfTop
1) Assign Interfaces 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) Enable Secure Shell (sshd)
6) Halt system 15) Restore recent configuration
7) Ping host 16) Restart PHP-FPM
8) Shell
Enter an option:
Message from syslogd@pfSense at Apr 4 02:31:44 ...
pfSense php-fpm[310]: /index.php: Successful login for user 'admin' from: 192.168.2.2

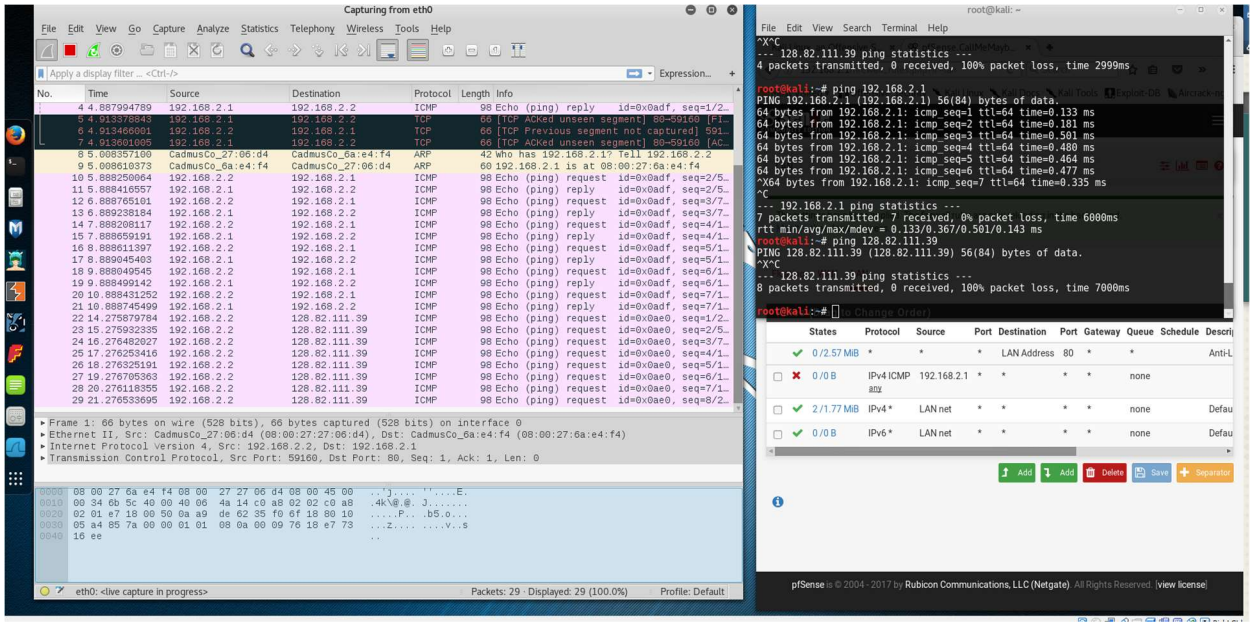
2.

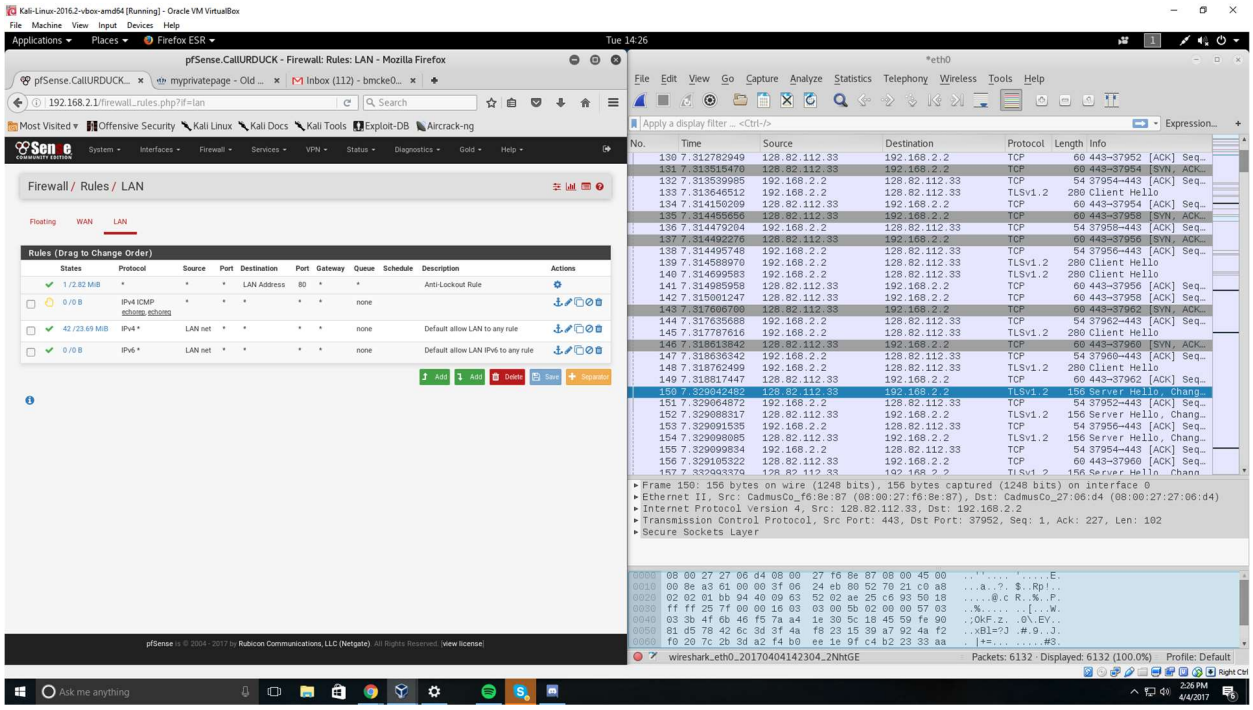

System Information
Name
pfSense.CallMeMaybe
System
pfSense
Serial: 89ecd4d8-1a3d-11e7-92e0-0800275f8a94
Version
2.3.3-RELEASE (amd64)
built on Thu Feb 16 06:59:53 CST 2017
FreeBSD 10.3-RELEASE-p16
Version 2.3.3_1 is available.
Platform
pfSense
CPU Type
Intel(R) Core(TM) i7-7700K CPU @ 4.20GHz
Uptime
00 Hour 58 Minutes 41 Seconds
Current date/time
Wed Apr 5 21:09:53 UTC 2017
DNS server(s)
127.0.0.1
192.168.1.1
Last config change
Wed Apr 5 21:04:25 UTC 2017
State table size
0% (152/98000) Show states
MBUF Usage
2% (1016/61600)
Load average
0.14, 0.08, 0.02
CPU usage
1%
Memory usage
22% of 989 MiB
SWAP usage
0% of 767 MiB
Disk usage (/)
89% of 743MiB - ufs
Interfaces
WAN
1000baseT <full-duplex>
10.0.2.15
LAN
1000baseT <full-duplex>
192.168.2.1
Snort Alerts
Interface/Time
Src/Dst Address
Description

3.

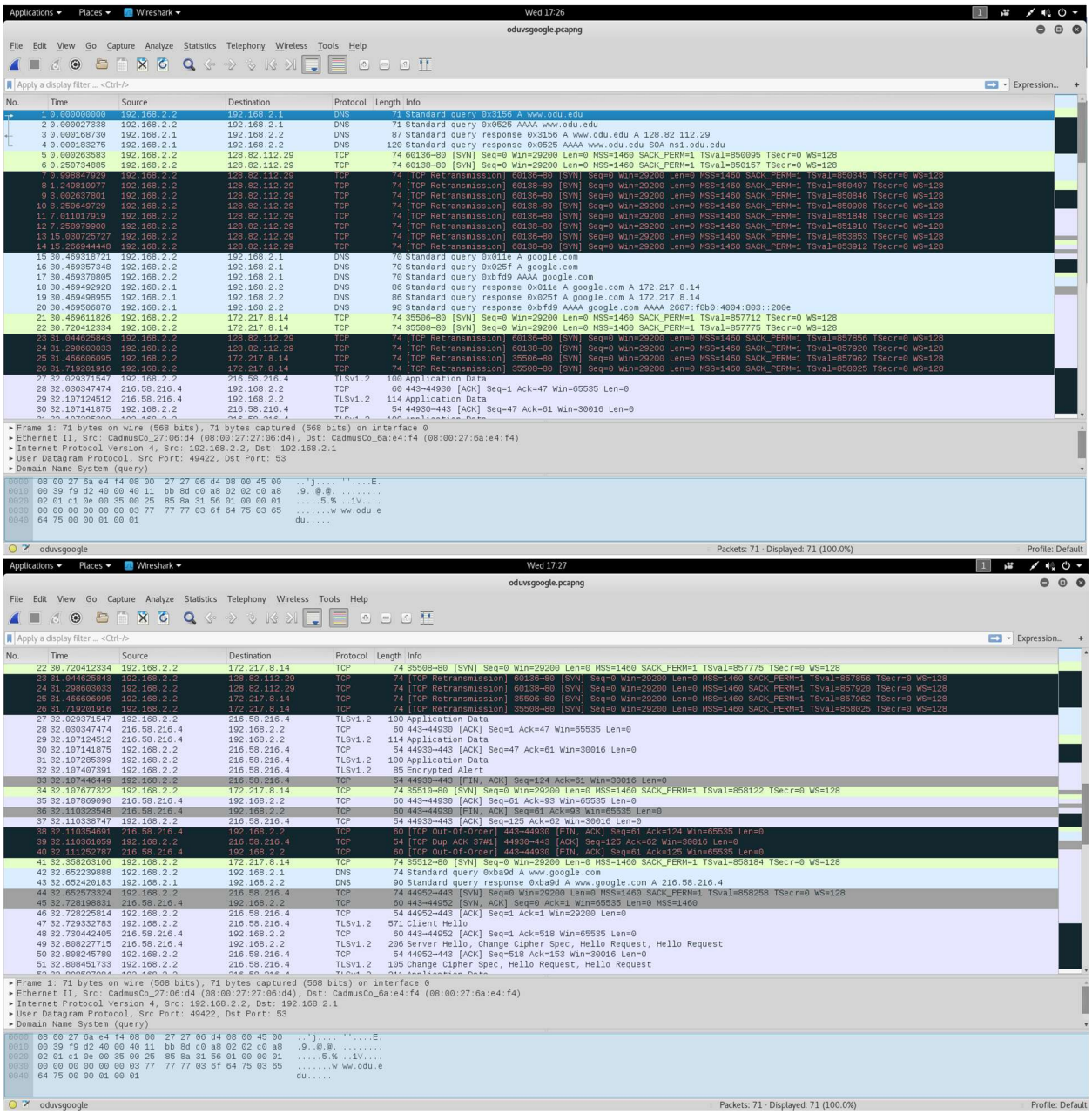

root@kali: ~
File Edit View Search Terminal Help
64 bytes from 8.8.8.8: icmp_seq=5 ttl=44 time=31.7 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=44 time=26.4 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=44 time=40.5 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=44 time=23.4 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=44 time=39.2 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=44 time=26.1 ms
64 bytes from 8.8.8.8: icmp_seq=11 ttl=44 time=25.4 ms
64 bytes from 8.8.8.8: icmp_seq=12 ttl=44 time=23.7 ms
64 bytes from 8.8.8.8: icmp_seq=13 ttl=44 time=33.9 ms
64 bytes from 8.8.8.8: icmp_seq=14 ttl=44 time=22.8 ms
64 bytes from 8.8.8.8: icmp_seq=15 ttl=44 time=29.9 ms
^X^C
--- 8.8.8.8 ping statistics ---
15 packets transmitted, 15 received, 0% packet loss, time 14026ms
rtt min/avg/max/mdev = 22.850/29.054/40.508/5.501 ms
root@kali:~# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
^X^C
--- 8.8.8.8 ping statistics ---
38 packets transmitted, 0 received, 100% packet loss, time 37057ms
root@kali:~# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
1 0.000000000 192.168.2.2 8.8.8.8 ICMP 98 Echo (ping) request id=0x0a6d, s...
2 1.002673122 192.168.2.2 8.8.8.8 ICMP 98 Echo (ping) request id=0x0a6d, s...
3 2.002605796 192.168.2.2 8.8.8.8 ICMP 98 Echo (ping) request id=0x0a6d, s...
4 3.005447610 192.168.2.2 8.8.8.8 ICMP 98 Echo (ping) request id=0x0a6d, s...
5 4.016162212 192.168.2.2 8.8.8.8 ICMP 98 Echo (ping) request id=0x0a6d, s...
6 5.024985963 192.168.2.2 8.8.8.8 ICMP 98 Echo (ping) request id=0x0a6d, s...
7 6.032723159 192.168.2.2 8.8.8.8 ICMP 98 Echo (ping) request id=0x0a6d, s...
8 7.040546663 192.168.2.2 8.8.8.8 ICMP 98 Echo (ping) request id=0x0a6d, s...
9 8.042420034 192.168.2.2 8.8.8.8 ICMP 98 Echo (ping) request id=0x0a6d, s...
10 9.042237373 192.168.2.2 8.8.8.8 ICMP 98 Echo (ping) request id=0x0a6d, s...
11 10.042303233 192.168.2.2 8.8.8.8 ICMP 98 Echo (ping) request id=0x0a6d, s...
12 11.042229364 192.168.2.2 8.8.8.8 ICMP 98 Echo (ping) request id=0x0a6d, s...
13 12.042146953 192.168.2.2 8.8.8.8 ICMP 98 Echo (ping) request id=0x0a6d, s...
14 13.042091583 192.168.2.2 8.8.8.8 ICMP 98 Echo (ping) request id=0x0a6d, s...
15 14.042034844 192.168.2.2 8.8.8.8 ICMP 98 Echo (ping) request id=0x0a6d, s...
16 15.041797890 192.168.2.2 8.8.8.8 ICMP 98 Echo (ping) request id=0x0a6d, s...
17 16.041999376 192.168.2.2 8.8.8.8 ICMP 98 Echo (ping) request id=0x0a6d, s...
18 17.044749644 192.168.2.2 8.8.8.8 ICMP 98 Echo (ping) request id=0x0a6d, s...
19 18.054489331 192.168.2.2 8.8.8.8 ICMP 98 Echo (ping) request id=0x0a6d, s...
Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
Ethernet II, Src: CadmusCo_27:06:d4 (08:00:27:27:06:d4), Dst: CadmusCo_6a:e4:f4 (08:00:27:6a:e4:f4)
Internet Protocol version 4, Src: 192.168.2.2, Dst: 8.8.8.8
Internet Control Message Protocol
0000 08 00 27 6a e4 f4 08 00 27 27 06 d4 08 00 45 00 ..'j.... ''....E.
0010 00 54 cb 2b 40 00 40 01 9c c3 c0 a8 02 02 08 08 .T.+@.@. ....
0020 08 08 08 00 e3 4c 0a 6d 00 01 c7 55 e5 58 00 00 .....L.m ...U.X..
0030 00 00 9c c3 02 00 00 00 00 00 10 11 12 13 14 15 ....
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 .... !"#$%
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 &'()*+,- ./012345
wireshark_eth0_20170405163828_3a9EWN
Packets: 19 · Displayed: 19 (100.0%)
Profile: Default
Add Add Delete Save Separator
pfSense is © 2004 - 2017 by Rubicon Communications, LLC (Netgate). All Rights Reserved. [view license]
Ask me anything
4:39 PM
4/5/2017


root@kali: ~
File Edit View Search Terminal Help
64 bytes from 8.8.8.8: icmp_seq=5 ttl=44 time=31.7 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=44 time=26.4 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=44 time=40.5 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=44 time=23.4 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=44 time=39.2 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=44 time=26.1 ms
64 bytes from 8.8.8.8: icmp_seq=11 ttl=44 time=25.4 ms
64 bytes from 8.8.8.8: icmp_seq=12 ttl=44 time=23.7 ms
64 bytes from 8.8.8.8: icmp_seq=13 ttl=44 time=33.9 ms
64 bytes from 8.8.8.8: icmp_seq=14 ttl=44 time=22.8 ms
64 bytes from 8.8.8.8: icmp_seq=15 ttl=44 time=29.9 ms
^X^C
--- 8.8.8.8 ping statistics ---
15 packets transmitted, 15 received, 0% packet loss, time 14026ms
rtt min/avg/max/mdev = 22.850/29.054/40.508/5.501 ms
root@kali:~# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
^X^C
--- 8.8.8.8 ping statistics ---
38 packets transmitted, 0 received, 100% packet loss, time 37057ms
root@kali:~# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
1 0.000000000 192.168.2.2 8.8.8.8 ICMP 98 Echo (ping) request id=0x0a6d, s...
2 1.002673122 192.168.2.2 8.8.8.8 ICMP 98 Echo (ping) request id=0x0a6d, s...
3 2.002605796 192.168.2.2 8.8.8.8 ICMP 98 Echo (ping) request id=0x0a6d, s...
4 3.005447610 192.168.2.2 8.8.8.8 ICMP 98 Echo (ping) request id=0x0a6d, s...
5 4.016162212 192.168.2.2 8.8.8.8 ICMP 98 Echo (ping) request id=0x0a6d, s...
6 5.024985963 192.168.2.2 8.8.8.8 ICMP 98 Echo (ping) request id=0x0a6d, s...
7 6.032723159 192.168.2.2 8.8.8.8 ICMP 98 Echo (ping) request id=0x0a6d, s...
8 7.040546663 192.168.2.2 8.8.8.8 ICMP 98 Echo (ping) request id=0x0a6d, s...
9 8.042420034 192.168.2.2 8.8.8.8 ICMP 98 Echo (ping) request id=0x0a6d, s...
10 9.042237373 192.168.2.2 8.8.8.8 ICMP 98 Echo (ping) request id=0x0a6d, s...
11 10.042303233 192.168.2.2 8.8.8.8 ICMP 98 Echo (ping) request id=0x0a6d, s...
12 11.042229364 192.168.2.2 8.8.8.8 ICMP 98 Echo (ping) request id=0x0a6d, s...
13 12.042146953 192.168.2.2 8.8.8.8 ICMP 98 Echo (ping) request id=0x0a6d, s...
14 13.042091583 192.168.2.2 8.8.8.8 ICMP 98 Echo (ping) request id=0x0a6d, s...
15 14.042034844 192.168.2.2 8.8.8.8 ICMP 98 Echo (ping) request id=0x0a6d, s...
16 15.041797890 192.168.2.2 8.8.8.8 ICMP 98 Echo (ping) request id=0x0a6d, s...
17 16.041999376 192.168.2.2 8.8.8.8 ICMP 98 Echo (ping) request id=0x0a6d, s...
18 17.044749644 192.168.2.2 8.8.8.8 ICMP 98 Echo (ping) request id=0x0a6d, s...
19 18.054489331 192.168.2.2 8.8.8.8 ICMP 98 Echo (ping) request id=0x0a6d, s...
Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
Ethernet II, Src: CadmusCo_27:06:d4 (08:00:27:27:06:d4), Dst: CadmusCo_6a:e4:f4 (08:00:27:6a:e4:f4)
Internet Protocol version 4, Src: 192.168.2.2, Dst: 8.8.8.8
Internet Control Message Protocol
0000 08 00 27 6a e4 f4 08 00 27 27 06 d4 08 00 45 00 ..'j.... ''....E.
0010 00 54 cb 2b 40 00 40 01 9c c3 c0 a8 02 02 08 08 .T.+@.@. ....
0020 08 08 08 00 e3 4c 0a 6d 00 01 c7 55 e5 58 00 00 .....L.m ...U.X..
0030 00 00 9c c3 02 00 00 00 00 00 10 11 12 13 14 15 ....
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 .... !"#$%
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 &'()*+,- ./012345
wireshark_eth0_20170405163828_3a9EWN
Packets: 19 · Displayed: 19 (100.0%)
Profile: Default
Add Add Delete Save Separator
pfSense is © 2004 - 2017 by Rubicon Communications, LLC (Netgate). All Rights Reserved. [view license]
Ask me anything
4:39 PM
4/5/2017


Capturing from eth0
root@kali: ~
pfSense is © 2004 - 2017 by Rubicon Communications, LLC (Netgate). All Rights Reserved. [view license]

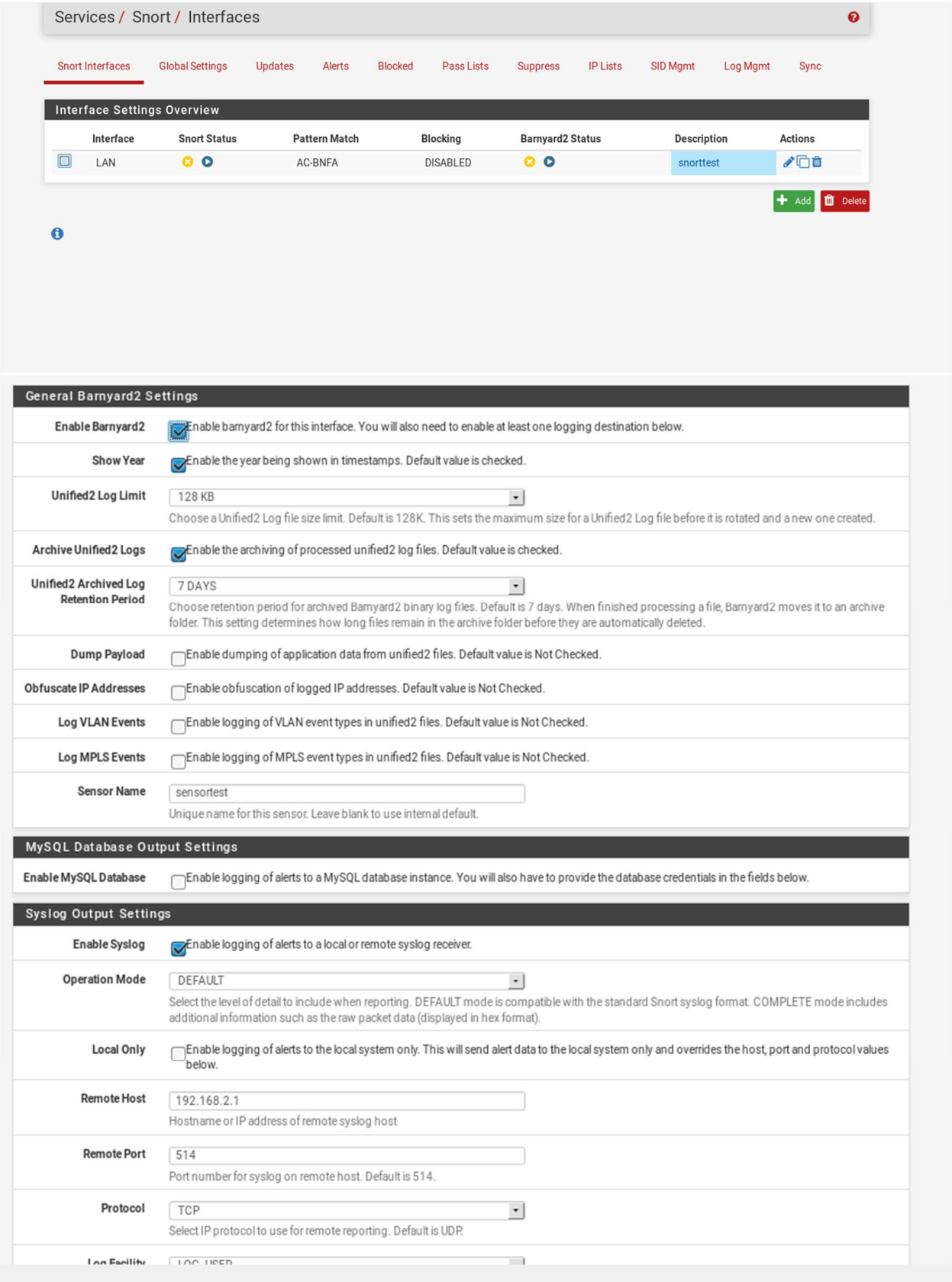

Kali-Linux-2016.2-vbox-amd64 [Running] - Oracle VM VirtualBox
pfSense.CallURDUCK - Firewall: Rules: LAN - Mozilla Firefox
Firewall / Rules / LAN
Rules (Drag to Change Order)
*eth0
pfSense is © 2004 - 2017 by Rubicon Communications, LLC (Netgate). All Rights Reserved. [view license]

4.



When I blocked HTTP port 80 on my system I wasn't able to visit www.odu.edu . I was able to try and see different protocol transfers such a TCP and DNS but the TCP didn't allow transmission from my virtual machine to the website. I think the results would have been a little bit different if I was on the same network as the destination (ip for odu's website: 128.82.112.29) obviously these ports weren't the ones that were blocked. When I tried to search something on google I got a whole bunch of new protocols I haven't see before which is very interesting. It takes should the alternative way it was able to make a hello and create a handshake between the two ip's using TLS v1.2. The reason for the two different results is because the server types that are being accessed have different methods of communication between the two systems.

5.


Services / Snort / Interfaces
Snort Interfaces
Global Settings
Updates
Alerts
Blocked
Pass Lists
Suppress
IP Lists
SID Mgmt
Log Mgmt
Sync
Interface Settings Overview
Interface
Snort Status
Pattern Match
Blocking
Barnyard2 Status
Description
Actions
LAN
AC-BNFA
DISABLED
snorttest
Add
Delete
General Barnyard2 Settings
Enable Barnyard2
Enable barnyard2 for this interface. You will also need to enable at least one logging destination below.
Show Year
Enable the year being shown in timestamps. Default value is checked.
Unified2 Log Limit
128 KB
Choose a Unified2 Log file size limit. Default is 128K. This sets the maximum size for a Unified2 Log file before it is rotated and a new one created.
Archive Unified2 Logs
Enable the archiving of processed unified2 log files. Default value is checked.
Unified2 Archived Log Retention Period
7 DAYS
Choose retention period for archived Barnyard2 binary log files. Default is 7 days. When finished processing a file, Barnyard2 moves it to an archive folder. This setting determines how long files remain in the archive folder before they are automatically deleted.
Dump Payload
Enable dumping of application data from unified2 files. Default value is Not Checked.
Obfuscate IP Addresses
Enable obfuscation of logged IP addresses. Default value is Not Checked.
Log VLAN Events
Enable logging of VLAN event types in unified2 files. Default value is Not Checked.
Log MPLS Events
Enable logging of MPLS event types in unified2 files. Default value is Not Checked.
Sensor Name
sensortest
Unique name for this sensor. Leave blank to use internal default.
MySQL Database Output Settings
Enable MySQL Database
Enable logging of alerts to a MySQL database instance. You will also have to provide the database credentials in the fields below.
Syslog Output Settings
Enable Syslog
Enable logging of alerts to a local or remote syslog receiver.
Operation Mode
DEFAULT
Select the level of detail to include when reporting. DEFAULT mode is compatible with the standard Snort syslog format. COMPLETE mode includes additional information such as the raw packet data (displayed in hex format).
Local Only
Enable logging of alerts to the local system only. This will send alert data to the local system only and overrides the host, port and protocol values below.
Remote Host
192.168.2.1
Hostname or IP address of remote syslog host
Remote Port
514
Port number for syslog on remote host. Default is 514.
Protocol
TCP
Select IP protocol to use for remote reporting. Default is UDP.

General | Remote Cache | Local Cache | Antivirus | ACLs | Traffic Mgmt | Authentication | Users | Real Time | Sync

Squid General Settings

Enable Squid Proxy
☐ Check to enable the Squid proxy.
Important: If unchecked, ALL Squid services will be disabled and stopped.

Keep Settings/Data
☑ If enabled, the settings, logs, cache, AV defs and other data will be preserved across package reinstalls.
Important: If disabled, all settings and data will be wiped on package uninstall/reinstall/upgrade.

Proxy Interface(s)
LAN
WAN
loopback
The interface(s) the proxy server will bind to. Use CTRL + click to select multiple interfaces.

Proxy Port
3128
This is the port the proxy server will listen on. Default: 3128

ICP Port
This is the port the proxy server will send and receive ICP queries to and from neighbor caches.
Leave this blank if you don't want the proxy server to communicate with neighbor caches through ICP.

Allow Users on Interface
☑ If checked, the users connected to the interface(s) selected in the 'Proxy interface(s)' field will be allowed to use the proxy.
There will be no need to add the interface's subnet to the list of allowed subnets.

Patch Captive Portal
This feature was removed - see Bug #5594 for details!

Resolve DNS IPv4 First
☐ Enable this to force DNS IPv4 lookup first.
This option is very useful if you have problems accessing HTTPS sites.

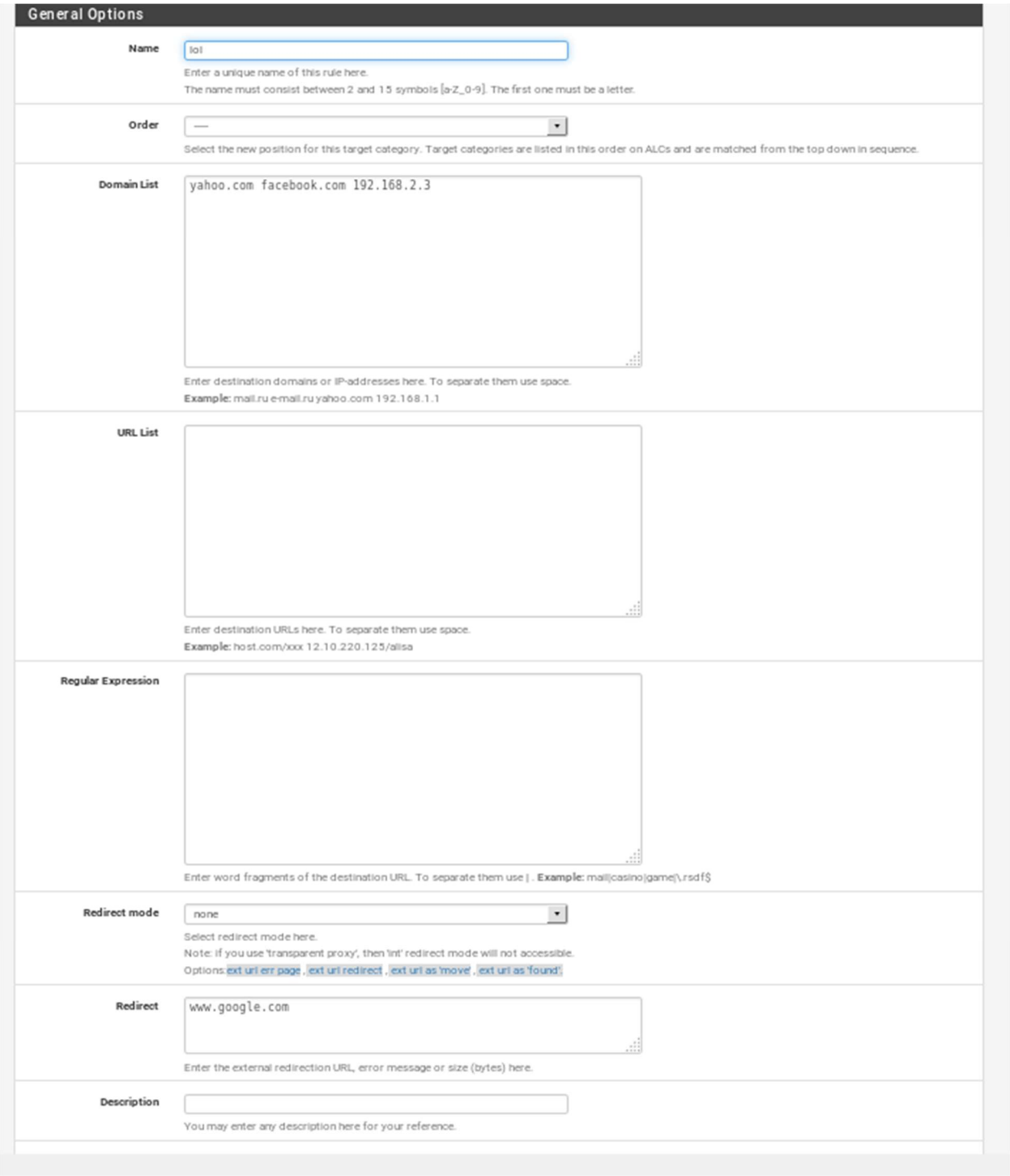
Disable ICMP
☐ Check this to disable Squid ICMP pinger helper.

Use Alternate DNS Servers for the Proxy Server
To use DNS servers other than those configured in System > General Setup, enter the IP(s) here. Separate entries by semi-colons (;)

Transparent Proxy Settings

Transparent HTTP Proxy
☐ Enable transparent mode to forward all requests for destination port 80 to the proxy server.
Transparent proxy mode works without any additional configuration being necessary on clients.
Important: Transparent mode will filter SSL (port 443) if you enable 'HTTPS/SSL Interception' below.
Hint: In order to proxy both HTTP and HTTPS protocols **without intercepting SSL connections**, configure WPAD/PAC options on your DNS/DHCP servers.

Transparent Proxy Interface(s)
LAN
WAN
The interface(s) the proxy server will transparently intercept requests on. Use CTRL + click to select multiple interfaces.



I learned a lot from this lab actually. I find great uses for the squid as well as the squidGuard because it can redirect traffic. Say you have children or something you can create a list of websites that you don't want them to be on and make it redirect their browsers to a local page or even other domains. Also it has features such as man in the middle protocols to where both protocols go through a mid point between the source and destination. I found that this kind of security and implementation is crucial with cryptology because it is a way of trying to keep information secured. I use a man in the middle

method when I'm port forwarding to make sure that I'm not losing any packets in transaction. I wasn't able to find or download darkstat or HAVP- anti virus proxy to work with my virtual machine but I can see how both are important especially darkstat because it tells you who's talking and listening on a network. If too much traffic is going on there are ways to see what is going where and which ports are using more bandwidth than others. Kali linux has a lot of great programs that cover all of these network monitoring methods as well as monitoring them. Last summer I took a shadowed a company that worked with network penetration and some of the stuff that they did with Kali linux was very impressive and this lab helped me understand how systems communicate with one another and how you can modify a path that it takes.