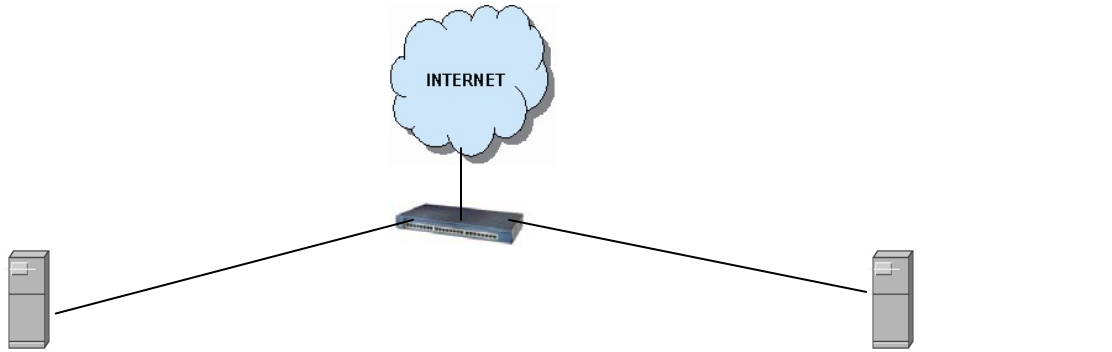
Defend host with PfSense using loopback interface. This is optional assignment. Skip to page 5.



PfSense host
em0: vlan10 IP: 10.10.10.Z
em1: vlan100 IP: 10.0.1.1
em1 dhcp server range: 10.0.1.100-10.0.1.200

Outside Local Host: 10.10.10.Y

Original Physical NIC IP: 10.10.10.Z changed to no IP
Loopback NIC: DHCP (10.0.1.100)

1. Install a loopback interface for Window or Linux box.
2. Record the original IP of the physical NIC and change the IP to 100.100.100.100 or uncheck the IPv4.
3. Set the loopback NIC to DHCP.
4. Virtualbox set NIC1 to physical and NIC2 to loopback.
5. Install PfSense, set VLan em0 to 10, and VLan em1 to 100
6. Set em0 (physical NIC) as WAN and em1 (loopback NIC) as LAN in PfSense.
7. Enable DHCP in em1 with IP DHCP scope from 10.0.1.100 to 10.0.1.200.
8. **Ping** 4.2.2.1 from the PfSense host. If not working check the loopback NIC IP address. Enter ipconfig /renew if needed.
9. In NAT outbound **uncheck** Automatic outbound NAT rule generation (PfSense will not automatically PAT for all inside hosts.)
10. **Ping** 4.2.2.1 from the PfSense host should still work because the outbound NAT rule has been created automatically by PfSense.
11. Edit the second Auto created rule; check the box do not NAT.

12. **Ping** 4.2.2.1 and nslookup/dig from the PfSense host should fail. Ping an outside local host and sniff at the outside local host. You should not see any packet from the translated address for the PfSense host.
13. In **Firewall:NAT 1:1** add an entry to statically translate the loopback IP address (**10.0.1.100**) to the original IP (**10.10.10.Z**) of the physical NIC recorded in step 2.
14. **Ping** 4.2.2.1 from the PfSense host; it should still fail. Ping an outside local host and sniff from the outside local host. The icmp echo request from the statically translated IP address should be captured. **The PfSense outside NIC will not respond to ARP request for the statically translated address until the Virtual IP has been created.** The nslookup and dig should work because the DNS for the loopback NIC is the PSsense LAN. In the nslookup change the DNS server to 4.2.2.1; the name resolution will fail.
15. In **Firewall:Virtual IP** address, add an entry for the IP address (**10.10.10.Z**) that has been translated in Firewall:NAT1:1. This is the original IP address in step 13 and step 2.
16. All outbound should work for the PfSense host now.

For inbound traffic:

1. In Firewall > rules > WAN, add a new rule to allow ICMP echo request to come to the loopback IP address (**10.0.1.100**). This is similar to the Cisco ASA 8.3 and above access-list that uses the inside host ip address in the rules to permit or deny.
2. Ping the translated outside IP address (**10.10.10.Z**) of the PfSense host from outside local host should fail.
3. In Firewall:rules:WAN disable the rule to block the RFC1918 networks.
4. Repeat step 2 test and it should work.

Note: Ubunto VM Host Loopback tap installation

user@admin-desktop:~$ sudo –i
root@ admin-desktop:~#apt-get install uml-utilities
root@ admin-desktop:~#modprobe tun
root@ admin-desktop:~#tunctl This will create loopback interface tap0
root@ admin-desktop:~#ifconfig tap0 10.100.100.100 netmask 255.255.255.0 up
root@ admin-desktop:~#ifconfig verify that tap0 is up and given ip is assigned.

If you want to add one more loopback inferface

root@ admin-desktop:~#tunctl ***This will create loopback interface tap1***
root@ admin-desktop:~#ifconfig tap1 10.100.101.100 netmask 255.255.255.0 up

Loopback tap installation on Centos/Redhat/Fedora

We need **tunctl** which is not available in our local repositories. So we'll have to add RPMForge repository. Steps to add this repo is given here **http://wiki.centos.org/AdditionalResources/Repositories/RPMForge** (Steps are the same for other 2 distros as well)

Lets install **tunctl**

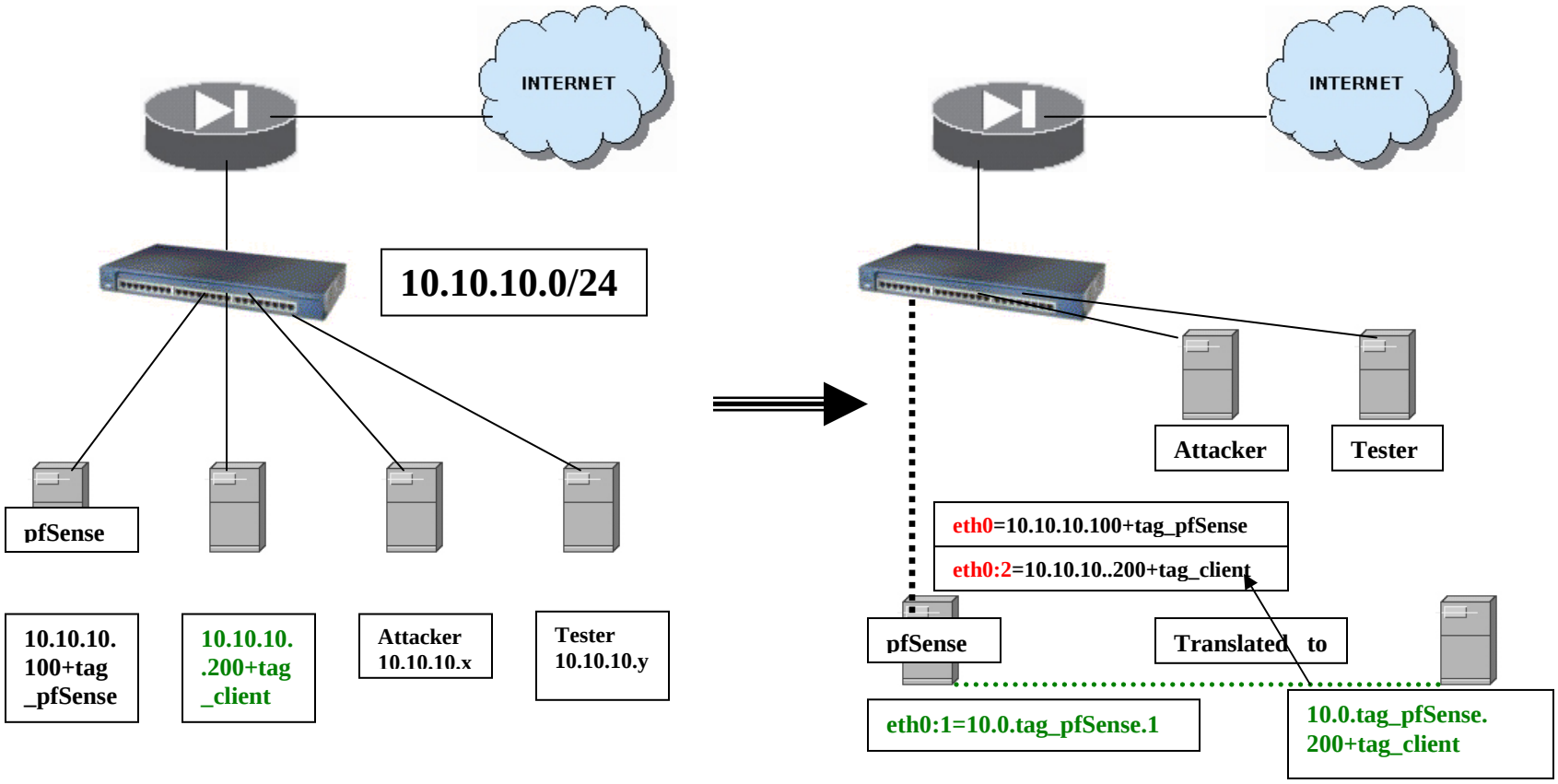
[user@admin ~]$ su
Password: (Type in your root password here)
[root@admin /]# yum install tunctl
[root@admin /]# modprobe tun
[root@admin /]# cd /usr/sbin

[root@admin sbin]#./tunctl ***This will create loopback interface tap0***
[root@admin sbin]# /sbin/ifconfig tap0 10.100.100.100 netmask 255.255.255.0 up
[root@admin sbin]# /sbin/ ifconfig ***verify that tap0 is up and given ip is assigned.***

If you want to add one more loopback inferface

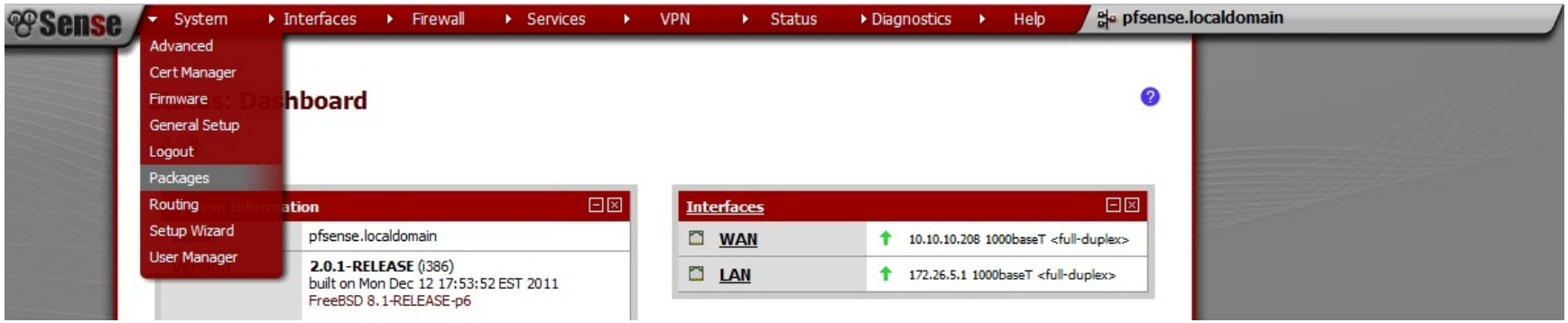
[root@admin sbin]#./tunctl ***This will create loopback interface tap1***
[root@admin sbin]# /sbin/ifconfig tap1 10.100.101.100 netmask 255.255.255.0 up
Change the ip with ifconfig according to your requirement.

Protect hosts with pfSense using two logical interfaces with one physical interface:



- **Configure pfSense with 2 logical NIC (in Virtualbox, choose the same NIC as the second interface in the setting of pfSense)**
- **Continue the esercise to protect the hosts with Snort IPS sensor.**

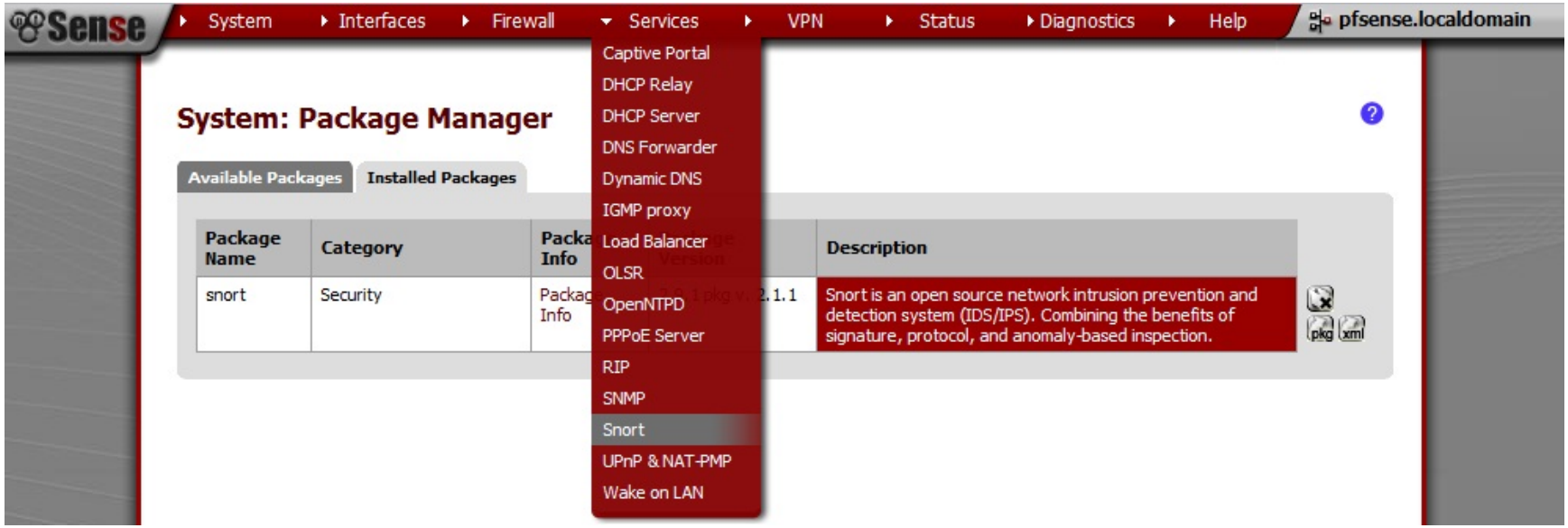
The Snort package has been install in the VM image.



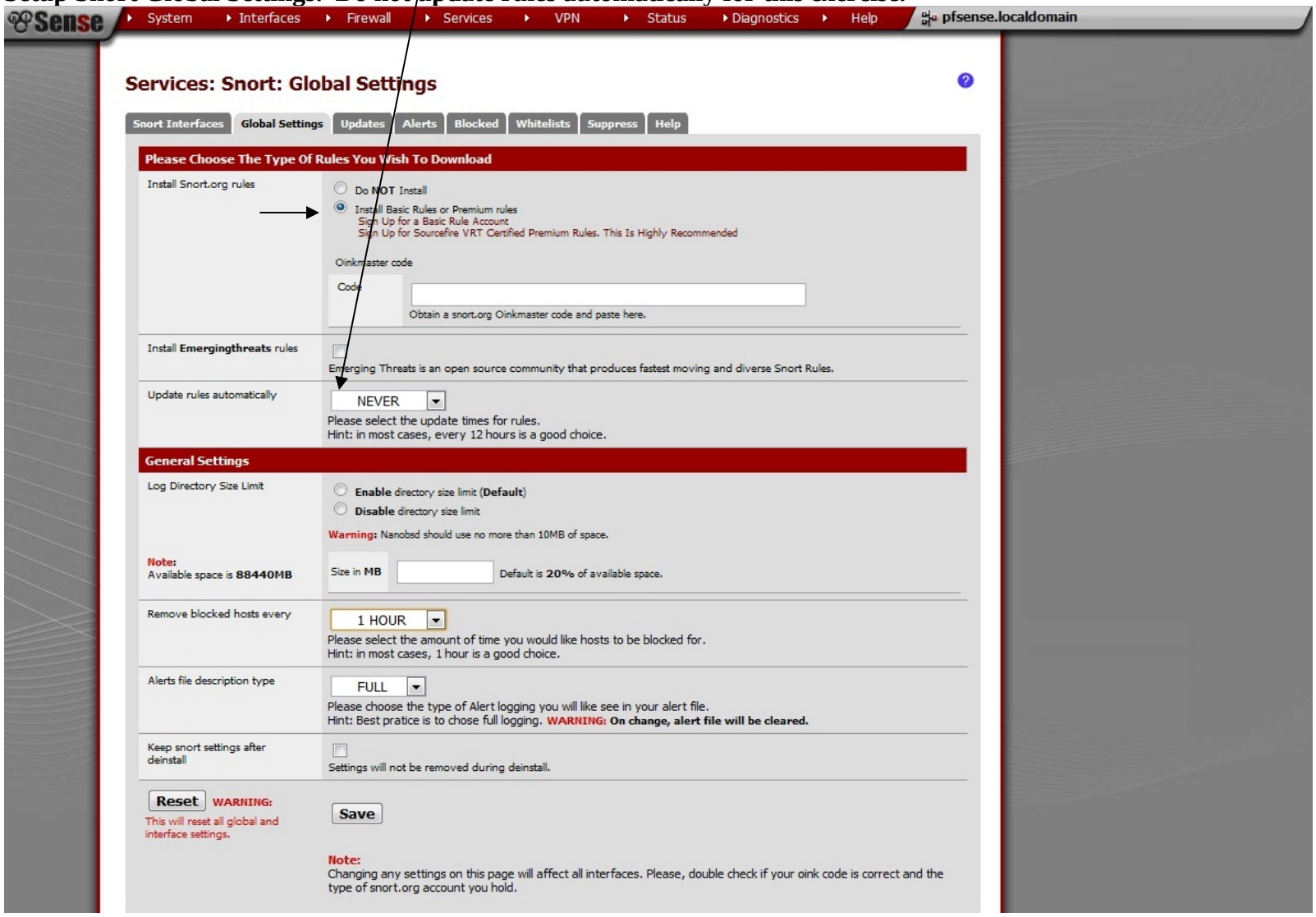
Review the available packages.

Strikeback	Services	BETA 0.1 platform: 2.0	Package Info	Detect port scans with iplog and strikeback
snort	Security	Stable 2.9.1 pkg v. 2.1.1 platform: 2.0	Package Info	Snort is an open source network intrusion prevention and detection system (IDS/IPS). Combining the benefits of signature, protocol, and anomaly-based inspection.
spamd	Services	Beta 4.5.0_4 platform: 1.2.1	No info, check the forum	Tarpits like spamd are fake SMTP servers, which accept connections but don't deliver mail. Instead, they keep the connections open and reply very slowly. If the peer is patient enough to actually complete the SMTP dialogue (which will take ten minutes or more), the tarpit returns a 'temporary error' code (4xx), which indicates that the mail could not be delivered successfully and that the sender should keep the mail in their queue and retry again later.
siproxd	Services	Beta 0.8.0_2 platform: 1.2.1	Package Info	Proxy for handling NAT of multiple SIP devices to a single public IP.

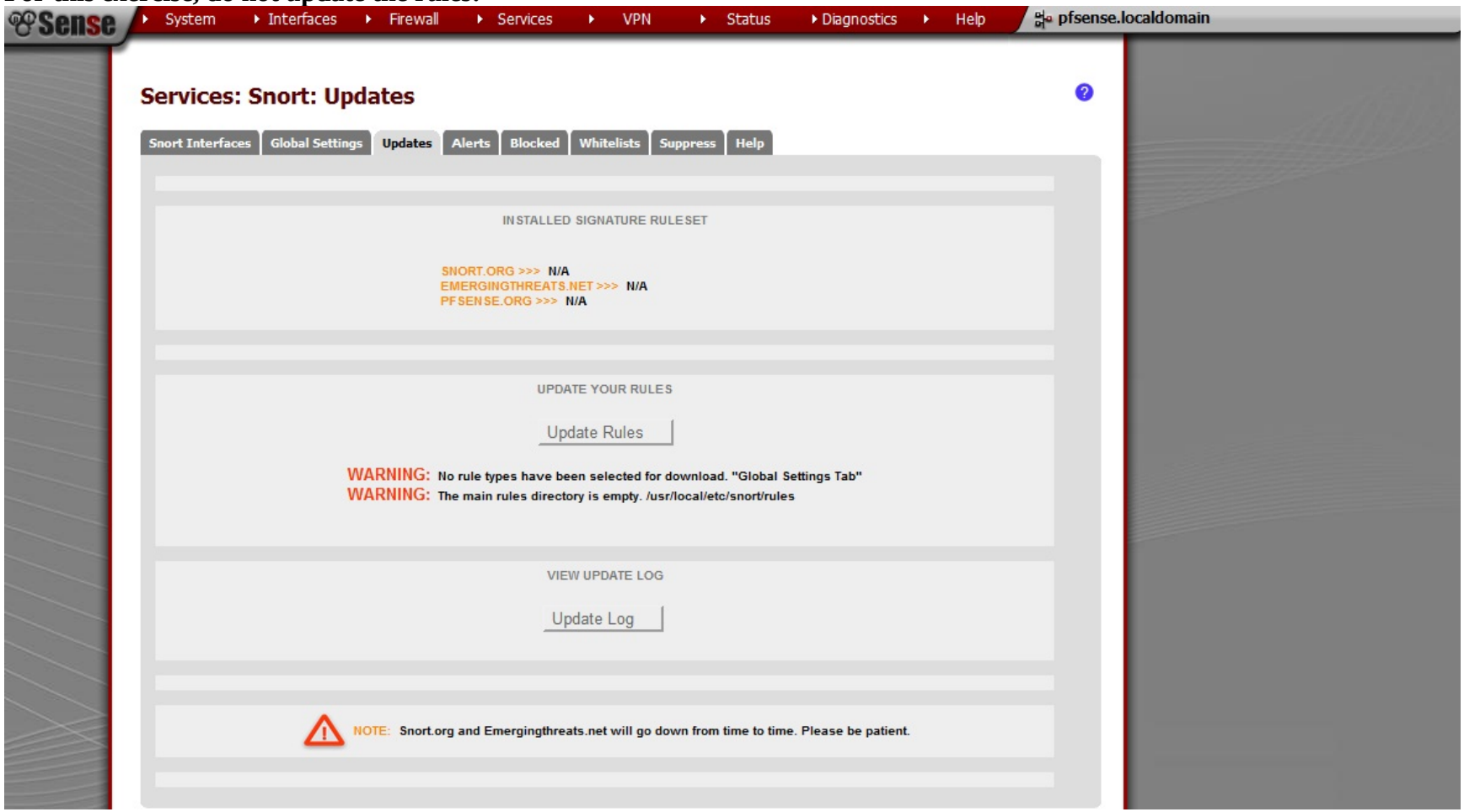
Make sure the Snort package has been installed and click Services > Snort.



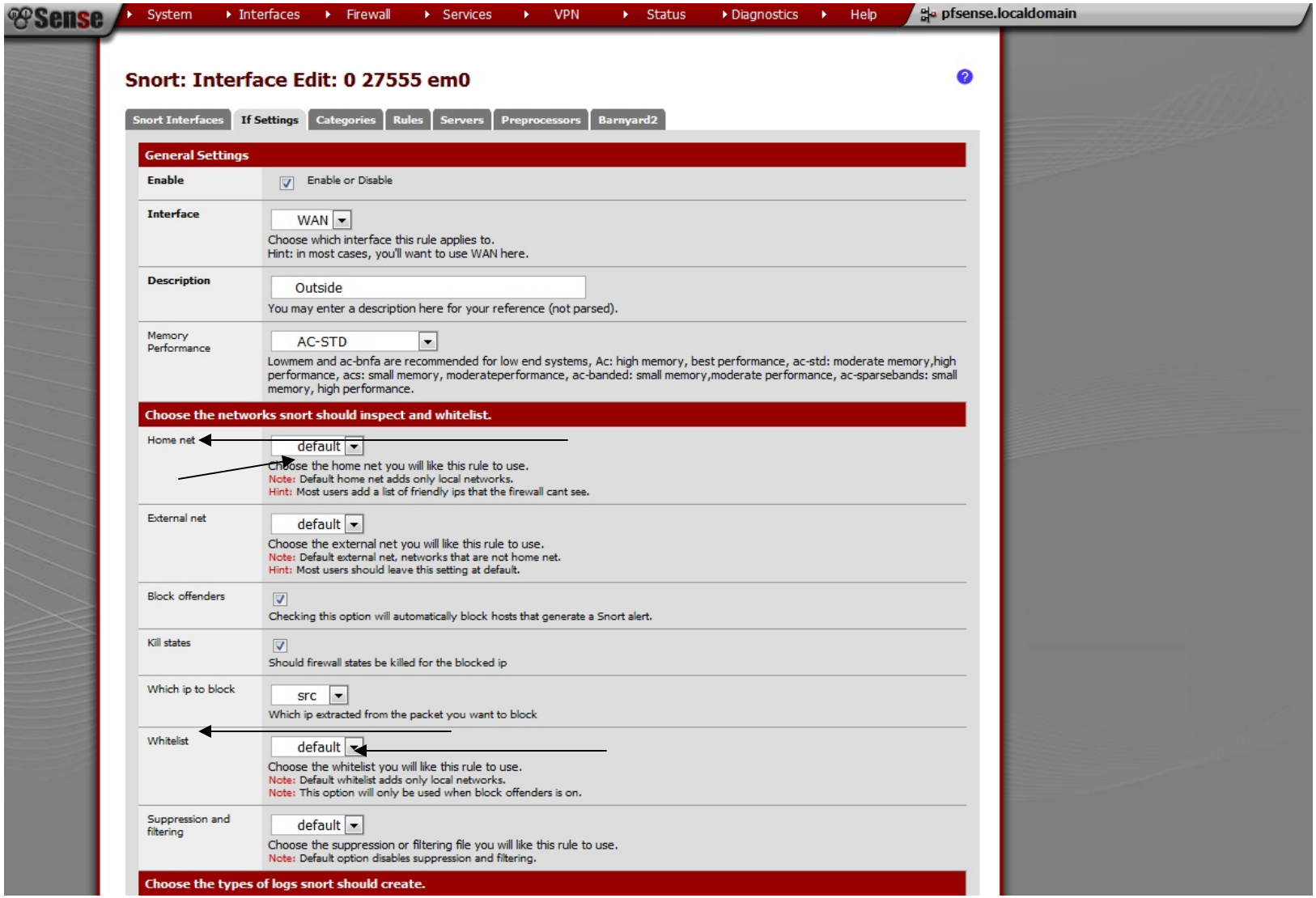
Setup Snort Global Settings. Do not update rules automatically for this exercise.



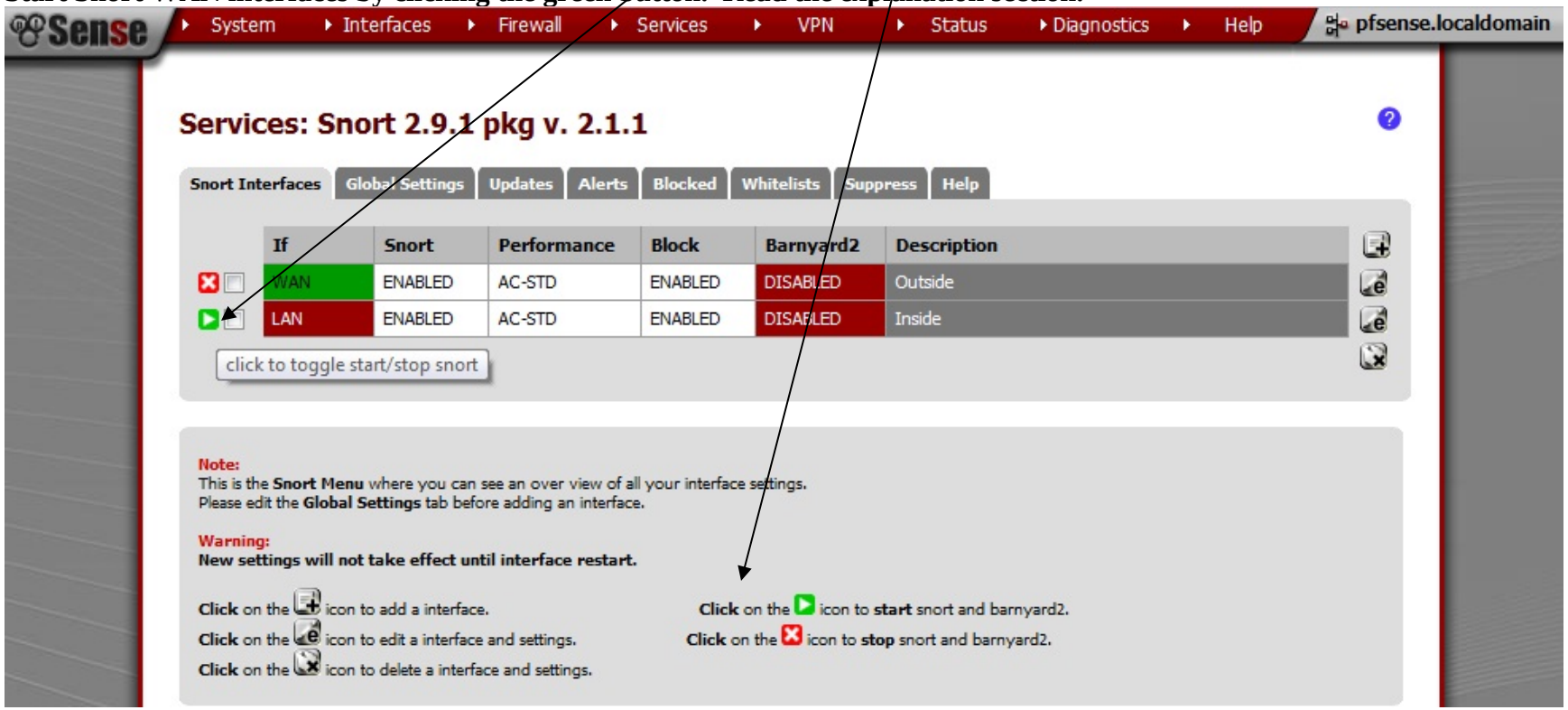
For this exercise, do not update the rules:



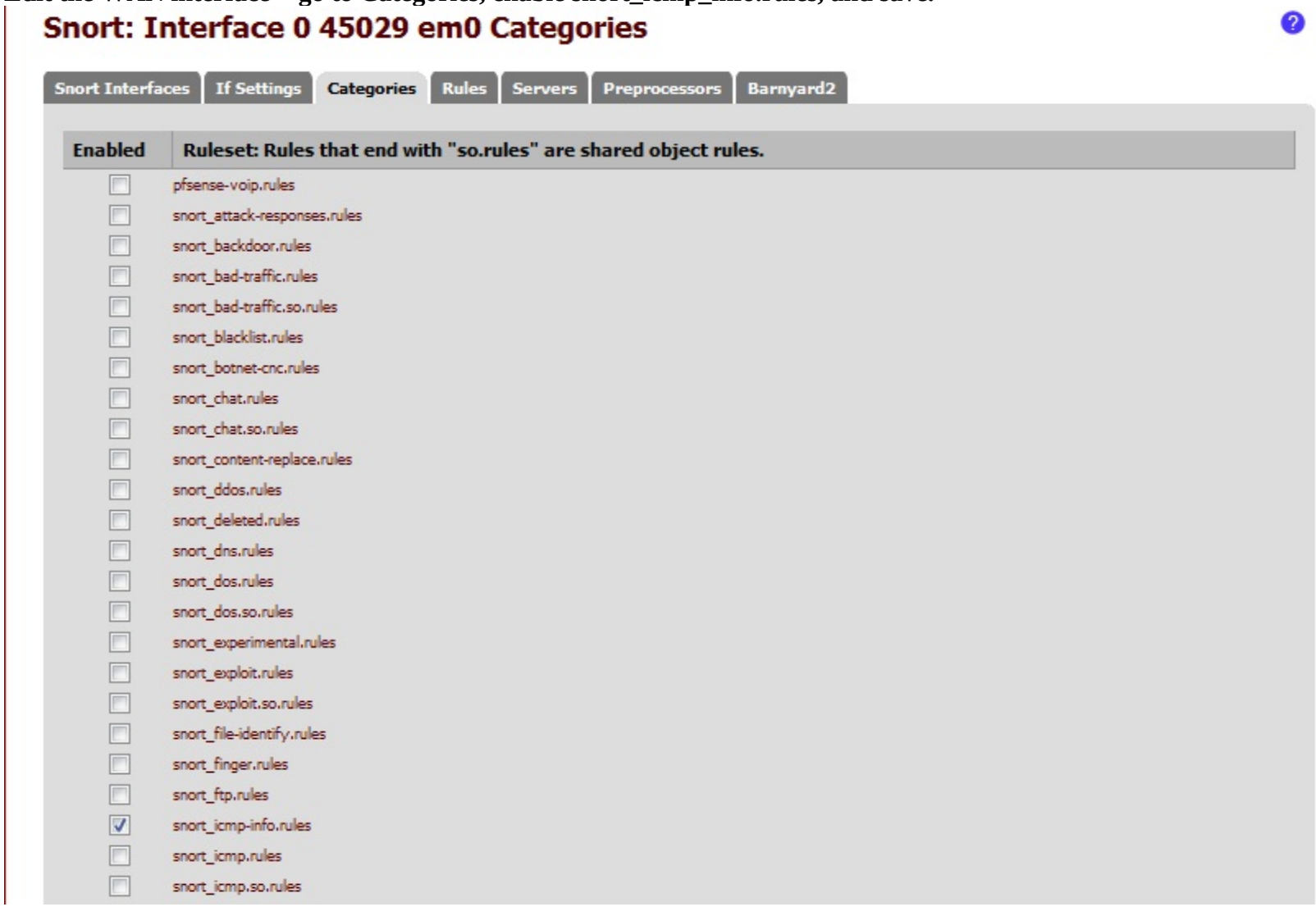
Make sure Snort interfaces are added.



Start Snort WAN interfaces by clicking the green button. Read the explanation section.



Edit the WAN interface > go to Categories, enable snort_icmp_info.rules, and save.



View /usr/local/etc/snort/snort_#####_em0/rules/snort_icmp-info.rules

Click the dimmed snort_icmp_info Rules 375 and 382 to enable both rules.

Snort: 0 57372 em0 Category: snort_icmp-info.rules

Snort Interfaces | If Settings | Categories | Rules | Servers | Preprocessors | Barnyard2

Category: snort_icmp-info.rules

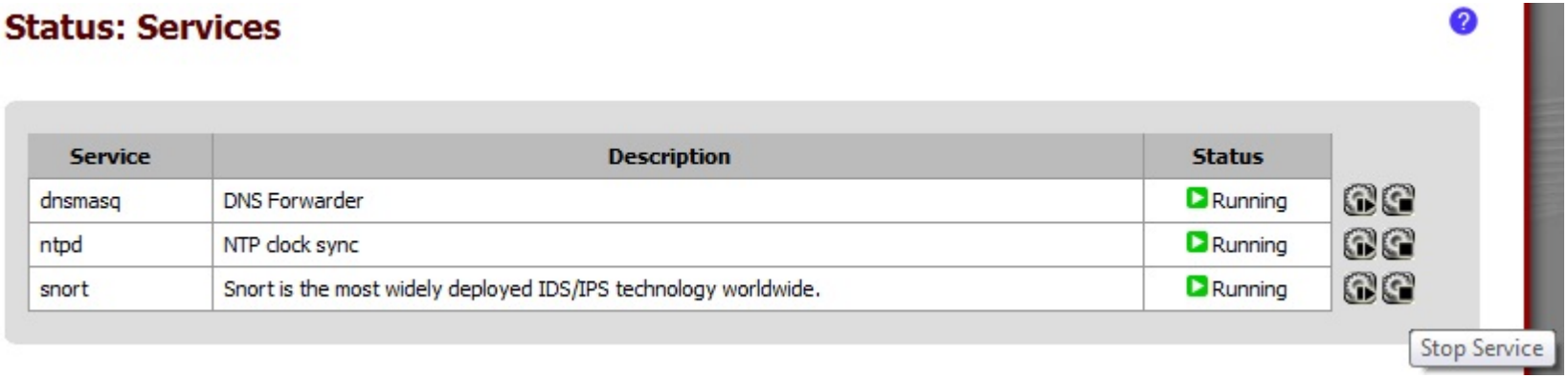
SID	Proto	Source	Port	Destination	Port	Message
363	icmp	$EXTERNAL_NET...	any	$HOME_NET...	any	ICMP-INFO IRDP router advertisement
364	icmp	$EXTERNAL_NET...	any	$HOME_NET...	any	ICMP-INFO IRDP router selection
366	icmp	$EXTERNAL_NET...	any	$HOME_NET...	any	ICMP-INFO PING *NIX
368	icmp	$EXTERNAL_NET...	any	$HOME_NET...	any	ICMP-INFO PING BSDtype
369	icmp	$EXTERNAL_NET...	any	$HOME_NET...	any	ICMP-INFO PING BayRS Router
370	icmp	$EXTERNAL_NET...	any	$HOME_NET...	any	ICMP-INFO PING BeOS4.x
371	icmp	$EXTERNAL_NET...	any	$HOME_NET...	any	ICMP-INFO PING Cisco Type.x
372	icmp	$EXTERNAL_NET...	any	$HOME_NET...	any	ICMP-INFO PING Delphi-Piette Windows
373	icmp	$EXTERNAL_NET...	any	$HOME_NET...	any	ICMP-INFO PING Flowpoint2200 or Network Management Software
374	icmp	$EXTERNAL_NET...	any	$HOME_NET...	any	ICMP-INFO PING IP NetMonitor Macintosh
375	icmp	$EXTERNAL_NET...	any	$HOME_NET...	any	ICMP-INFO PING LINUX/*BSD
376	icmp	$EXTERNAL_NET...	any	$HOME_NET...	any	ICMP-INFO PING Microsoft Windows
377	icmp	$EXTERNAL_NET...	any	$HOME_NET...	any	ICMP-INFO PING Network Toolbox 3 Windows
378	icmp	$EXTERNAL_NET...	any	$HOME_NET...	any	ICMP-INFO PING Ping-O-MeterWindows
379	icmp	$EXTERNAL_NET...	any	$HOME_NET...	any	ICMP-INFO PING Pinger Windows
380	icmp	$EXTERNAL_NET...	any	$HOME_NET...	any	ICMP-INFO PING Seer Windows
381	icmp	$EXTERNAL_NET...	any	$HOME_NET...	any	ICMP-INFO PING Oracle Solaris
382	icmp	$EXTERNAL_NET...	any	$HOME_NET...	any	ICMP-INFO PING Windows
385	icmp	$EXTERNAL_NET...	any	$HOME_NET...	any	ICMP-INFO traceroute
384	icmp	$EXTERNAL_NET...	any	$HOME_NET...	any	ICMP-INFO PING

View /usr/local/etc/snort/snort_#####_em0/rules/snort_icmp-info.rules to verify the # in front of rule 375 and 382 are gone.

A few notes to remember and understand:

1. **In case you lock yourself out form pfSense, issue pfctl –d to disable and pfctl –e to enable pfSense firewall.**
2. **Inside vi editor, use x to delete characters.**
3. **When the Snort service is stopped, the/usr/local/etc/snort/snort_#####_em0 and em1 directories will not be deleted. Stop the Snort service, check the files in the folder, go to the rules subfolder, and verify that the rules 375 and 382 are still enabled. If you stop the interface and restarted the interface, the interface folder will be deleted and everything in the interface subfolder will be recreated from default. If a rule has been changed, the snort service must be restarted for the changed rule to take effect. Stop the interface and restart the interface will wipe out your change and load the default seting.**

Click Status > Services to show:



4. **The /usr/local/etc/snort/snort_#####_em0 and em1 directories are created or deleted when the WAN and LAN interfaces being started or stopped. Therefore, all changed rules are gone once the interface is stoped. Stop the WAN interface and verify that 375 and 382 are dimmed and the /usr/local/etc/snort/snort_#####_em0 is deleted.**
5. **The /usr/local/etc/snort/rules contains the original rules to be copied to WAN and LAN rules under the /usr/local/etc/snort/snort_#####_em0 and em1 directories once the WAN or LAN interfaces restarted.**
6. **Make sure there is a space between the # and the rules that will be commented out.**
7. **Only the rule sets checked under Category will be applied. Refer to page 12 for image. The checked Categories are the include $RUTH_PATH/"the checked Category" in snort.conf file.**
8. **Select whitelist for each interfaces at: /usr/local/etc/snort/whitelist/defaultwlist and other customized whitelist**

9. **Modify /usr/local/pkg/snort/snort.inc to delete the /{sn} for the HOME_NET variable for the snort.conf file for the /usr/local/etc/snort/snort_#####_em0 and em1 directories. Alternatively, change the default setting of Home_Net under interface settings on page 10. Below is the snort.conf sample file.**

```
# snort configuration file
# generated by the pfSense
# package manager system
# see /usr/local/pkg/snort.inc
# for more information
#       snort.conf
#   Snort can be found at http://www.snort.org/

##########################
                         #
# Define Local Network   #
                         #
##########################

var HOME_NET [10.10.10.208/24,172.26.5.1/24,10.10.10.10,127.0.0.1,8.8.8.8,10.10.
10.209,127.0.0.1]
var EXTERNAL_NET !$HOME_NET

####################
                   #
# Define Servers   #
                   #
####################
```

10. **Add whitelist and choose the name of the whitelist under interface settings on page 10.**
11. **Stop and start the Snort service.**
12. **Verify the HOME_NET does not including the 10.0.tag.1 /24 and 10.10.10.100+tag_pfSense /24. Otherwise, the rule will not be applied because the whole class C inside and outside addresses are defined as HOME_NET.**
13. **Ping from the tester or attacker to the pfSense outside interface or the translated address of 10.10.10.200+tag_client.**

```
C:\Users\ciss23>ping 10.10.10.208

Pinging 10.10.10.208 with 32 bytes of data:
Reply from 10.10.10.208: bytes=32 time<1ms TTL=64
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.10.10.208:
    Packets: Sent = 4, Received = 1, Lost = 3 (75% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\ciss23>
```

Notice that the attacker or tester still got one icmp response back! Compare icmp and SQL Slammer.

14. Alert showing the ping detected.

Services: Snort: Snort Alerts

Snort Interfaces | Global Settings | Updates | Alerts | Blocked | Whitelists | Suppress | Help

Last 250 Alert Entries.	Latest Alert Entries Are Listed First.
Save or Remove Logs	Download All log files will be saved. Clear Warning: all log files will be deleted.
Auto Refresh and Log View	Save Refresh Default is ON. 250 Enter the number of log entries to view. Default is 250.

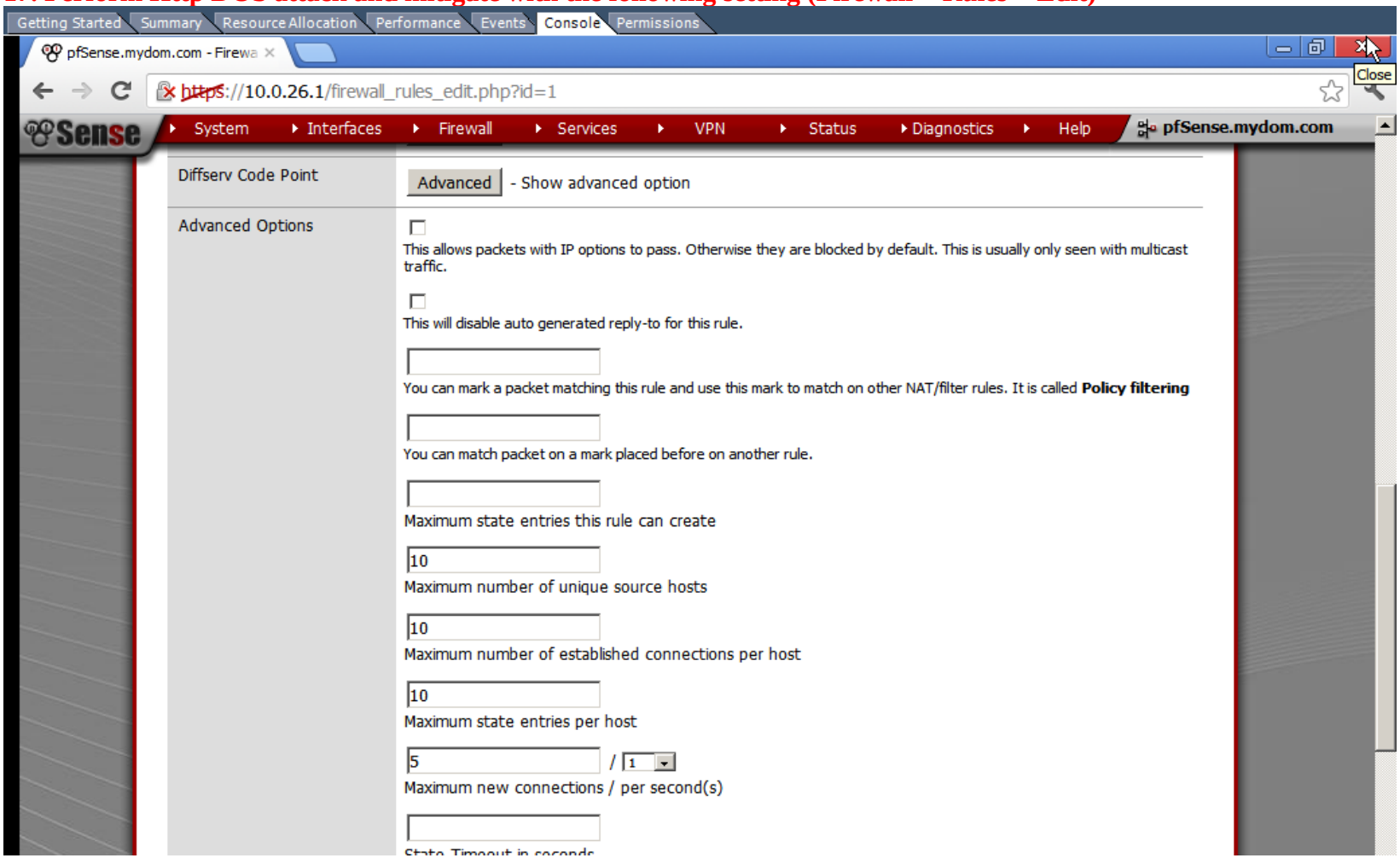
Filter: PRIORITY Submit Clear

#	PRI	PROTO	DESCRIPTION	CLASS	SRC	SPORT	FLOW	DST	DPORT	SID	Date
1	3	ICMP	ICMP-INFO PING Windows	Misc activity	10.10.10.64	empty	->	10.10.10.208	empty	1:382:9	05/12-11:27:51
2	3	ICMP	ICMP-INFO PING Windows	Misc activity	10.10.10.64	empty	->	10.10.10.208	empty	1:382:9	05/12-11:27:46
3	3	ICMP	ICMP-INFO PING Windows	Misc activity	10.10.10.64	empty	->	10.10.10.208	empty	1:382:9	05/12-11:27:41
4	3	ICMP	ICMP-INFO PING Windows	Misc activity	10.10.10.64	empty	->	10.10.10.208	empty	1:382:9	05/12-11:27:40

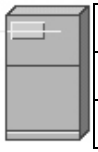
15. Attacker or tester IP address is blocked.

16. route add default 10.10.10.10 to add default gateway by command line.

17. Perform Http DOS attack and mitigate with the following setting (Firewall > Rules > Edit)



Exercise Slammer with pfSense:

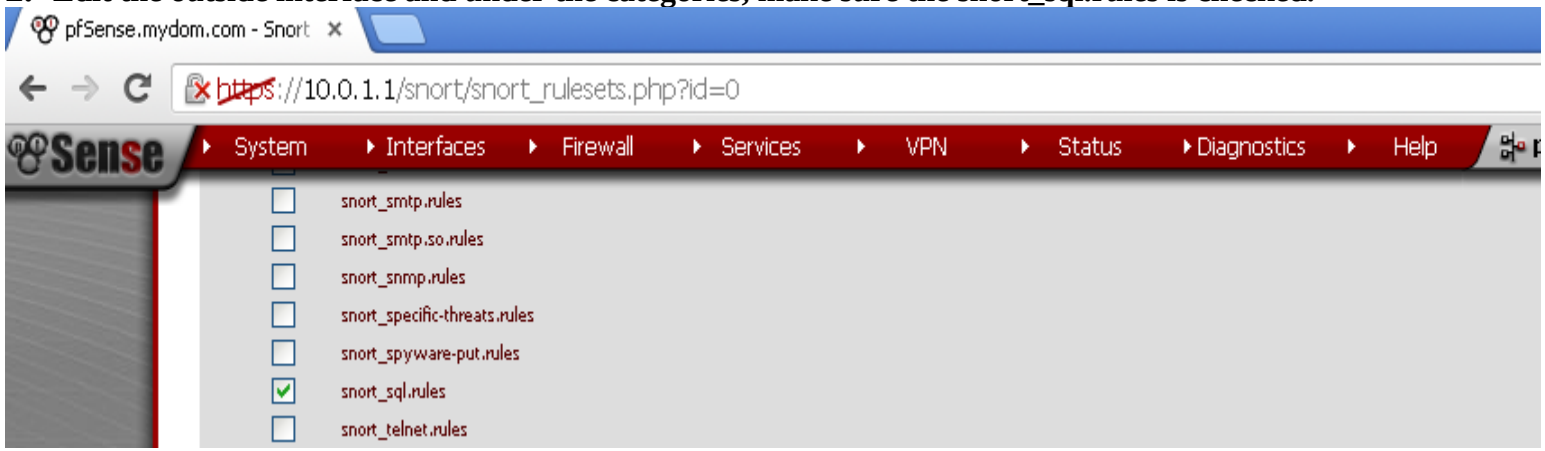


Virtual Box: pfSense inside: 10.0.1.1; outside 192.168.0.23
Host: 192.168.0.19 as attacker
Host: 10.0.1.4 as SQL server translated to 192.168.0.4

1. **Edit pfSense /usr/local/etc/snort/rules/snort_sql.rules (alert udp $EXTERNAL_NET any -> $HOME_NET 1434 (msg:"Slammer Worm"; content:"|c050 ff16 89c6 09db 81f3 3c61 d9ff 8b45|"; sid:1000001; rev:1;)**

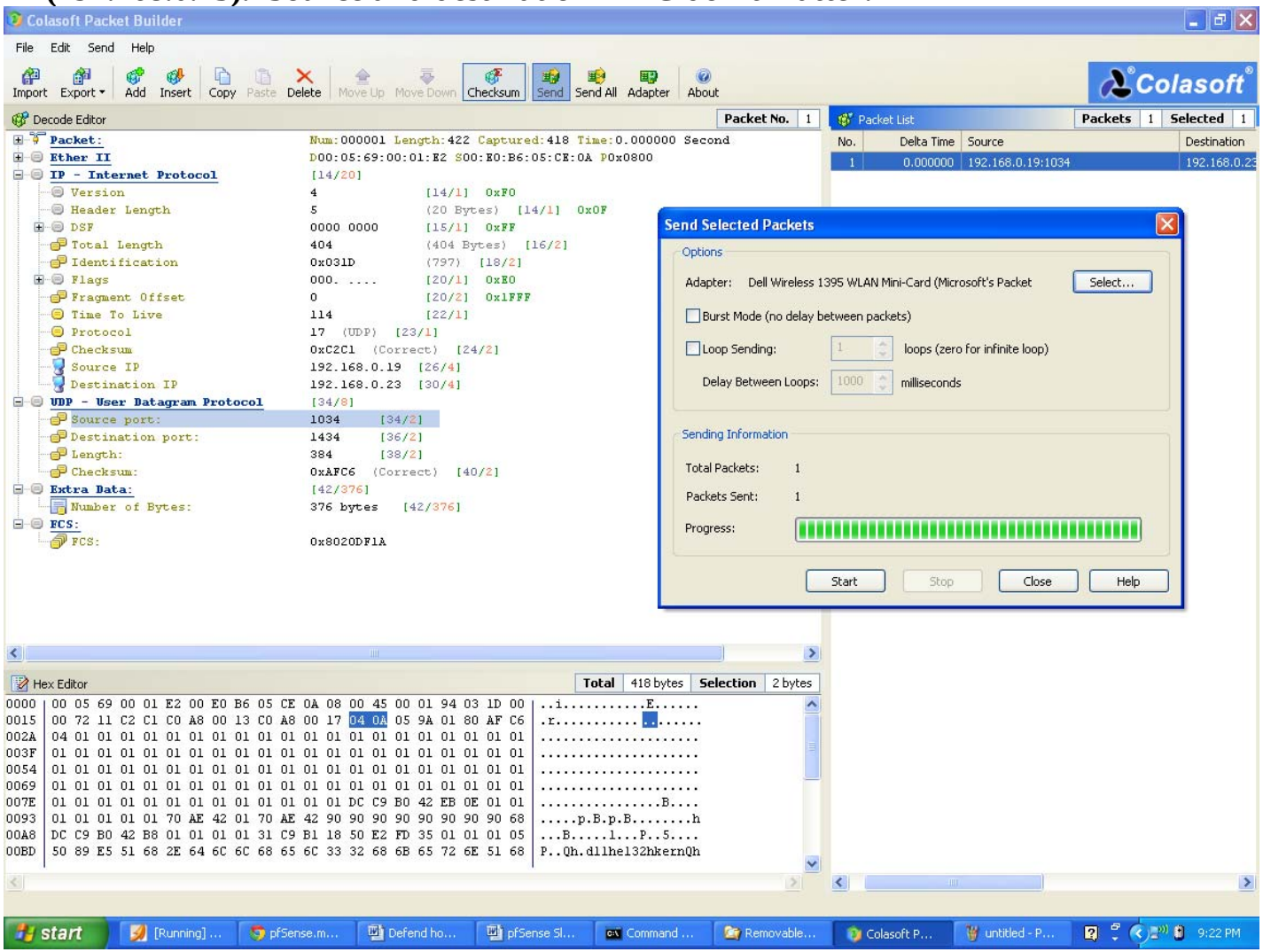
```
# Copyright 2001-2005 Sourcefire, Inc. All Rights Reserved
#
# This file may contain proprietary rules that were created, tested and
# certified by Sourcefire, Inc. (the "VRT Certified Rules") as well as
# rules that were created by Sourcefire and other third parties and
# distributed under the GNU General Public License (the "GPL Rules").  The
# VRT Certified Rules contained in this file are the property of
# Sourcefire, Inc. Copyright 2005 Sourcefire, Inc. All Rights Reserved.
# The GPL Rules created by Sourcefire, Inc. are the property of
# Sourcefire, Inc. Copyright 2002-2005 Sourcefire, Inc. All Rights
# Reserved.  All other GPL Rules are owned and copyrighted by their
# respective owners (please see www.snort.org/contributors for a list of
# owners and their respective copyrights).  In order to determine what
# rules are VRT Certified Rules or GPL Rules, please refer to the VRT
# Certified Rules License Agreement.
#
#
# $Id: sql.rules,v 1.88.2.15 2012-02-09 17:44:18 vrtbuild Exp $
#----------
# SQL RULES
#----------
alert udp $EXTERNAL_NET any -> $HOME_NET 1434 (msg:"Slammer Worm Jim";content:"|
c050 ff16 89c6 09db 81f3 3c61 d9ff 8b45|"; sid:1000009; rev:9;)
# alert tcp $EXTERNAL_NET any -> $SQL_SERVERS 139 (msg:"SQL sp_start_job - progr
```

2. **Edit the outside interface and under the categories, make sure the snort_sql.rules is checked.**

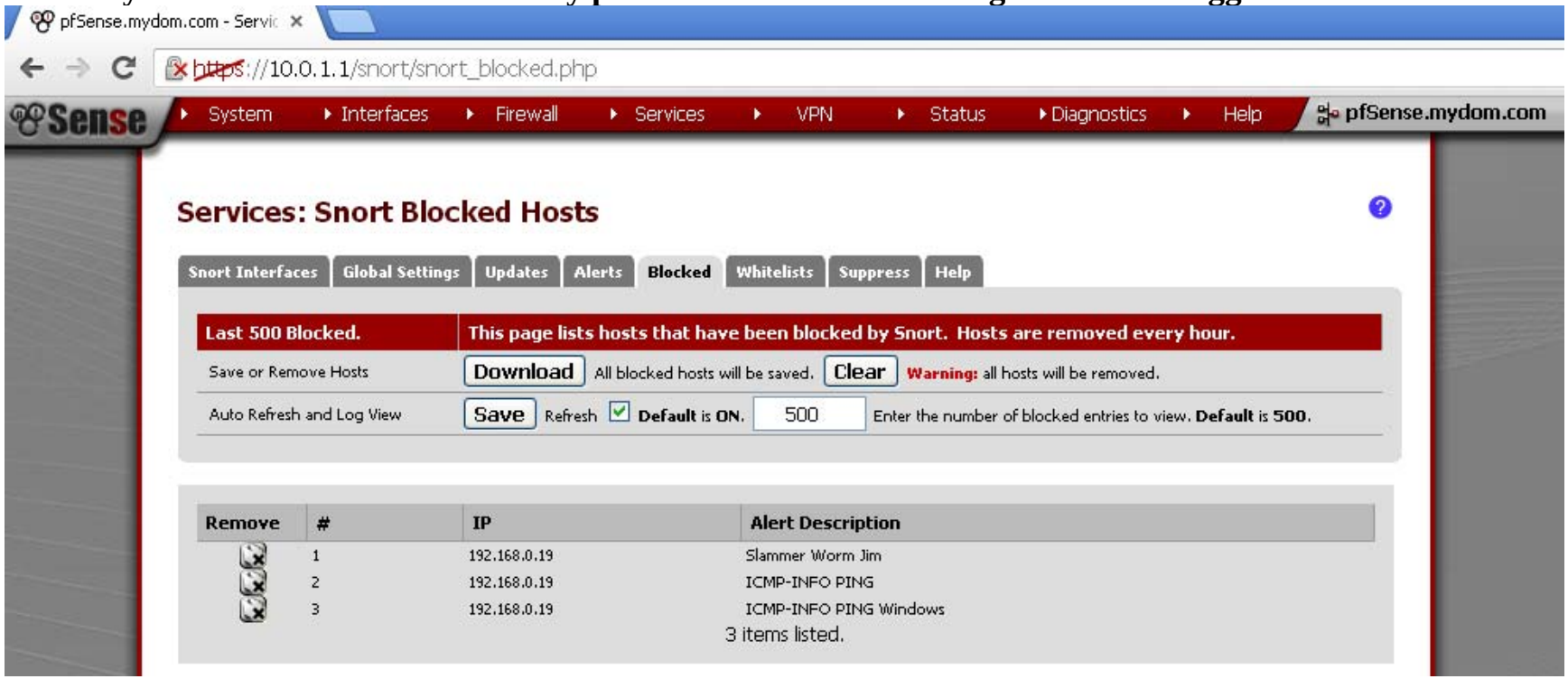


3. **Restart the snort service and start the snort WAN interface.**

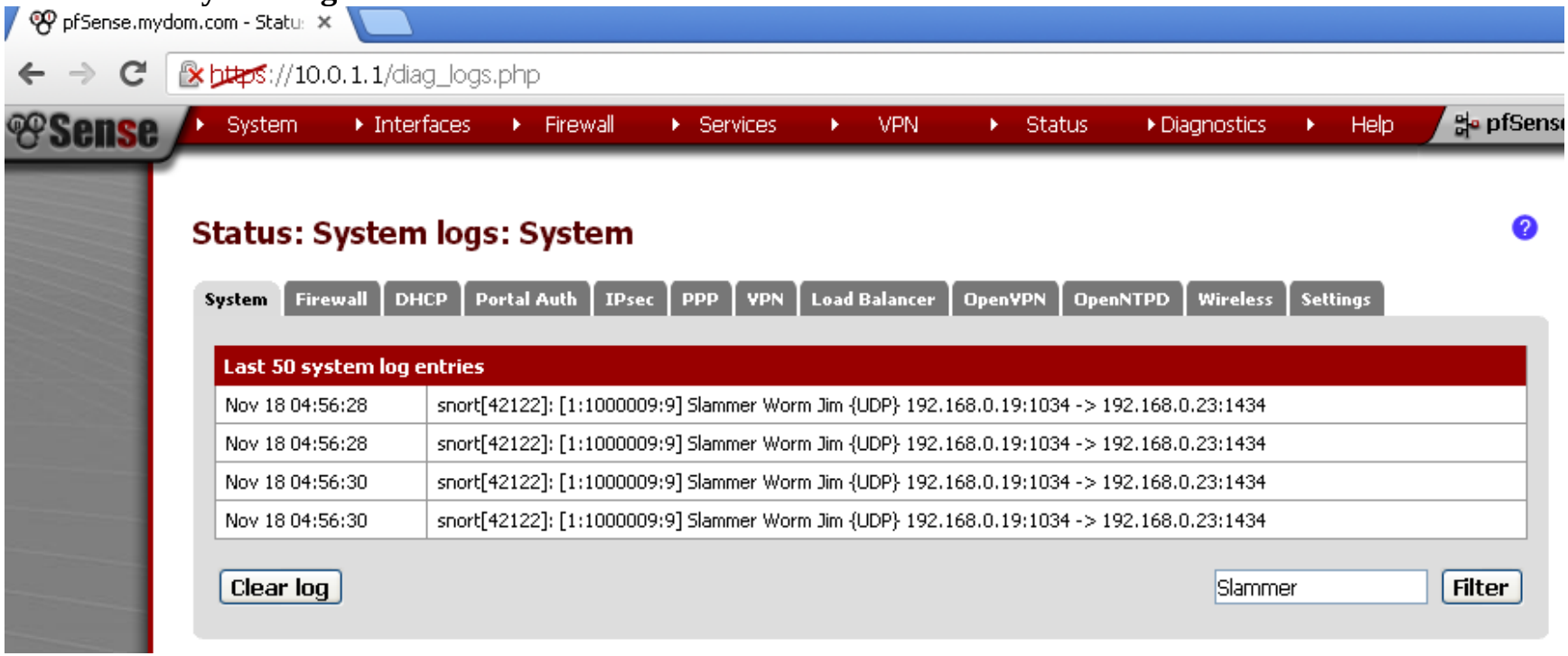
4. For now, use Colasoft Packet Builder to send slammer packet to pfSense outside interface (192.168.0.23). Source and destination MAC don't matter.



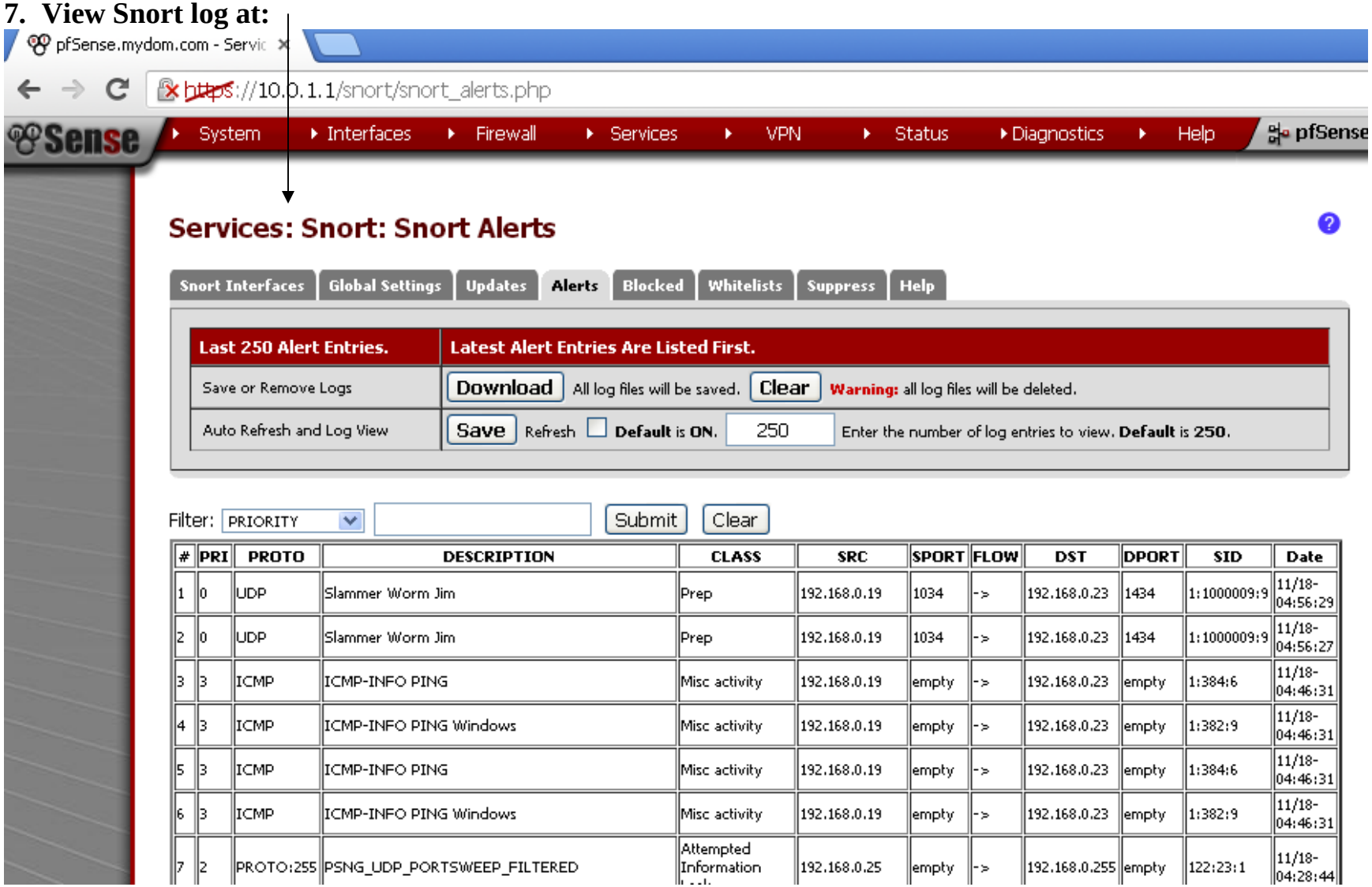
5. Verify that the attacker is blocked by pfSense and the Slammer signature was triggered.



6. View the System logs with filter:



7. View Snort log at:



#	PRI	PROTO	DESCRIPTION	CLASS	SRC	SPORT	FLOW	DST	DPORT	SID	Date
1	0	UDP	Slammer Worm Jim	Prep	192.168.0.19	1034	->	192.168.0.23	1434	1:1000009:9	11/18-04:56:29
2	0	UDP	Slammer Worm Jim	Prep	192.168.0.19	1034	->	192.168.0.23	1434	1:1000009:9	11/18-04:56:27
3	3	ICMP	ICMP-INFO PING	Misc activity	192.168.0.19	empty	->	192.168.0.23	empty	1:384:6	11/18-04:46:31
4	3	ICMP	ICMP-INFO PING Windows	Misc activity	192.168.0.19	empty	->	192.168.0.23	empty	1:382:9	11/18-04:46:31
5	3	ICMP	ICMP-INFO PING	Misc activity	192.168.0.19	empty	->	192.168.0.23	empty	1:384:6	11/18-04:46:31
6	3	ICMP	ICMP-INFO PING Windows	Misc activity	192.168.0.19	empty	->	192.168.0.23	empty	1:382:9	11/18-04:46:31
7	2	PROTO:255	PSNG_UDP_PORTSWEEP_FILTERED	Attempted Information	192.168.0.25	empty	->	192.168.0.255	empty	122:23:1	11/18-04:28:44

8. **The HOME_NET will be created to include the virtual ip address. Complete this exercise by translate an internal SQL server (10.0.1.4) to the outside (192.168.0.4). The Slammer packet will be send to the SQL nat address of 192.168.0.4. The attacker will be blocked only if the HOME_NET includes the host that is under attack. Make sure the translated address of 192.168.0.4 is included in the HOME_NET of snort.conf file. If not, the attacker will not be blocked.**

Enjoy your exercises.

Special thanks to Jimmy Tu who made great contribution to make pfSense exercises successful.