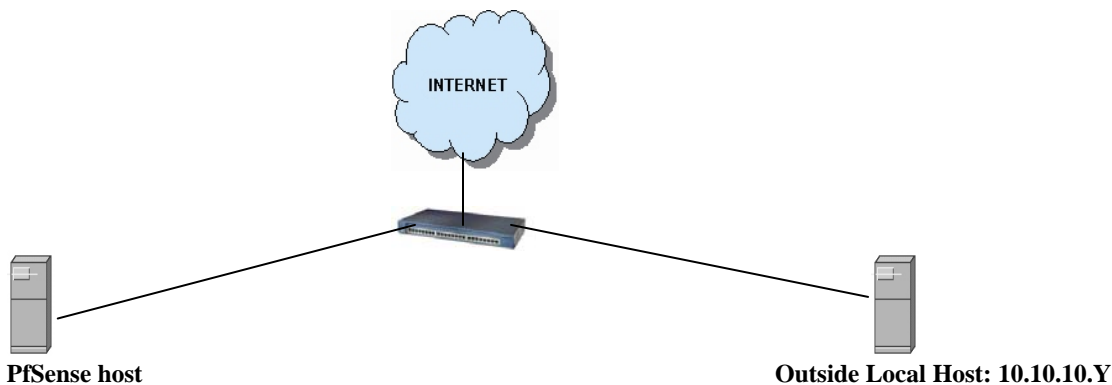


**Defend host with PfSense using loopback interface. This is optional assignment. Skip to page 5.**



**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: Ubuntu 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**

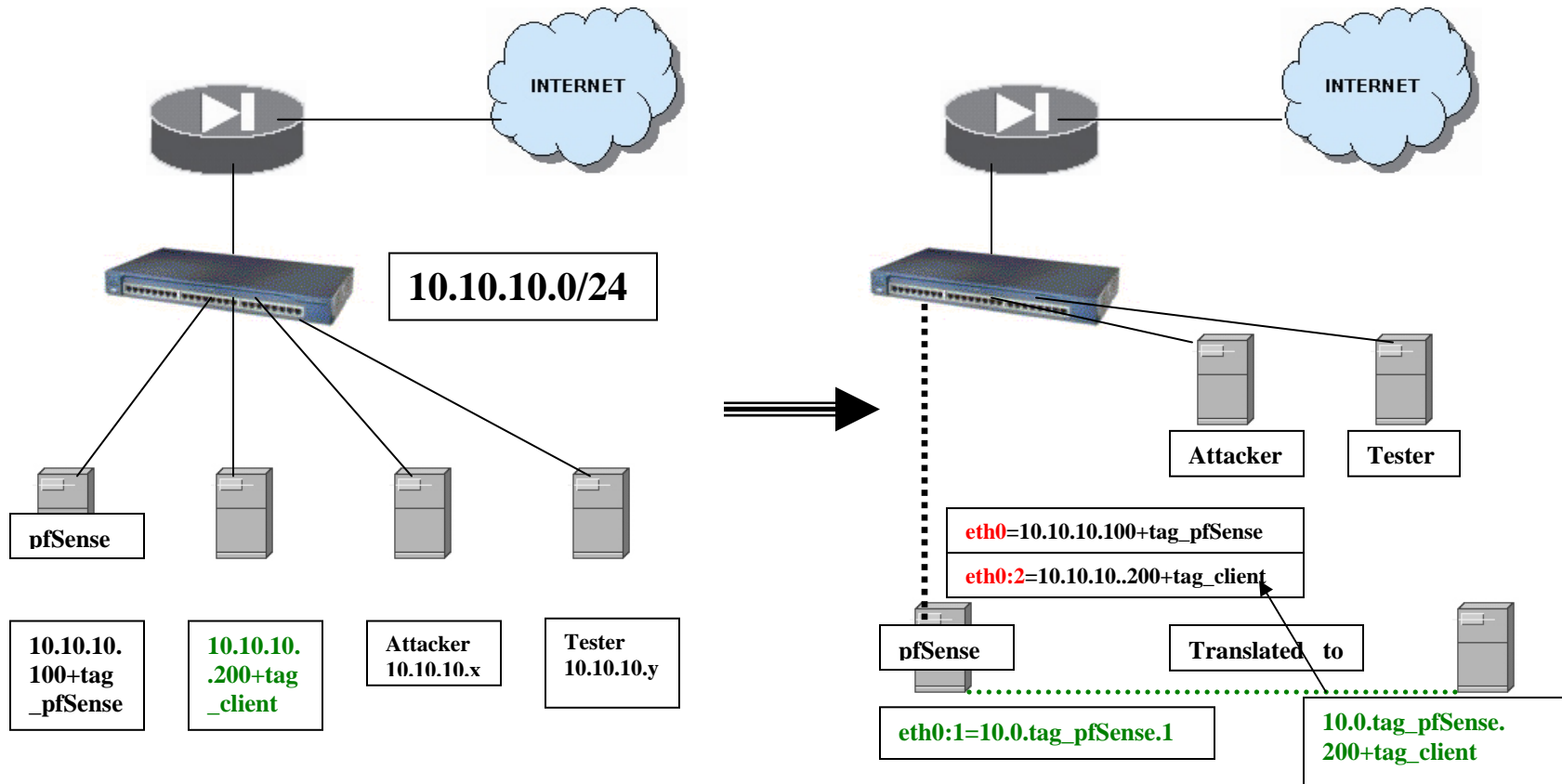
```
[user@admin ~]$ su
Password: (Type in your root password here)
[root@admin /]# yum install tunctl
[root@admin /]# modprobe tun
[root@admin /]# cd /usr/sbin

[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 interface**

```
[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 exercise 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.

The screenshot shows the pfSense web interface. At the top, there is a navigation bar with the following items: System, Interfaces, Firewall, Services (expanded), VPN, Status, Diagnostics, and Help. The 'Services' menu is open, listing various services: Captive Portal, DHCP Relay, DHCP Server, DNS Forwarder, Dynamic DNS, IGMP proxy, Load Balancer, OLSR, OpenNTPD, PPPoE Server, RIP, SNMP, Snort (highlighted), UPnP & NAT-PMP, and Wake on LAN. Below the navigation bar, the main content area is titled 'System: Package Manager'. It has two tabs: 'Available Packages' and 'Installed Packages'. A table lists available packages:

Package Name	Category	Package Info	Description
snort	Security	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.

Additional icons for package management (pkg, xml) are visible in the bottom right of the table area.

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

The screenshot shows the PfSense web interface with the following elements:

- Navigation Bar:** System > Interfaces > Firewall > Services > VPN > Status > Diagnostics > Help. The user is logged in as pfsense.localdomain.
- Page Title:** Services: Snort: Global Settings
- Sub-headers:** Snort Interfaces, Global Settings (selected), Updates, Alerts, Blocked, Whitelists, Suppress, Help.
- Section: Please Choose The Type Of Rules You Wish To Download**
  - Install Snort.org rules:** Includes radio buttons for "Do NOT Install" and "Install Basic Rules or Premium rules" (selected). Below is a text input field for "Oinkmaster code" with a hint: "Obtain a snort.org Oinkmaster code and paste here."
  - Install Emergingthreats rules:** Includes a checkbox and a description: "Emerging Threats is an open source community that produces fastest moving and diverse Snort Rules."
  - Update rules automatically:** A dropdown menu is set to "NEVER". Hint: "Please select the update times for rules. Hint: in most cases, every 12 hours is a good choice."
- Section: General Settings**
  - Log Directory Size Limit:** Radio buttons for "Enable directory size limit (Default)" and "Disable directory size limit". A warning states: "Warning: Nanobsd should use no more than 10MB of space." Below is a "Size in MB" input field with a hint: "Default is 20% of available space." A note indicates "Available space is 88440MB".
  - Remove blocked hosts every:** A dropdown menu is set to "1 HOUR". Hint: "Please select the amount of time you would like hosts to be blocked for. Hint: in most cases, 1 hour is a good choice."
  - Alerts file description type:** A dropdown menu is set to "FULL". Hint: "Please choose the type of Alert logging you will like see in your alert file. Hint: Best practice is to chose full logging. WARNING: On change, alert file will be cleared."
  - Keep snort settings after deinstall:** A checkbox is checked. Hint: "Settings will not be removed during deinstall."
- Buttons:** "Reset" (with a warning: "This will reset all global and interface settings.") and "Save".
- Final Note:** "Note: Changing any settings on this page will affect all interfaces. Please, double check if your oink code is correct and the type of snort.org account you hold."



For this exercise, do not update the rules:

The screenshot shows the pfSense web interface. At the top, there is a navigation bar with the following items: System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The current page is titled "Services: Snort: Updates". Below the title, there are several tabs: Snort Interfaces, Global Settings, Updates (selected), Alerts, Blocked, Whitelists, Suppress, and Help. The main content area is divided into three sections:

- INSTALLED SIGNATURE RULESET**: This section shows the status of three rule sources:
  - SNORT.ORG >>> N/A
  - EMERGINGTHREATS.NET >>> N/A
  - PFSENSE.ORG >>> N/A
- UPDATE YOUR RULES**: This section contains a button labeled "Update Rules". Below the button, there is a warning message:

**WARNING:** No rule types have been selected for download. "Global Settings Tab"  
**WARNING:** The main rules directory is empty. /usr/local/etc/snort/rules
- VIEW UPDATE LOG**: This section contains a button labeled "Update Log".

At the bottom of the page, there is a note with a warning icon: **NOTE:** Snort.org and Emergingthreats.net will go down from time to time. Please be patient.

### Make sure Snort interfaces are added.

The screenshot shows the pfSense web interface for editing a Snort interface rule. The breadcrumb navigation at the top reads: System > Interfaces > Firewall > Services > VPN > Status > Diagnostics > Help. The current page title is "Snort: Interface Edit: 0 27555 em0".

Navigation tabs include: Snort Interfaces, If Settings, Categories, Rules, Servers, Preprocessors, and Barnyard2. The "If Settings" tab is active.

**General Settings**

- Enable:**  Enable or Disable
- Interface:** WAN (dropdown menu)  
Choose which interface this rule applies to.  
Hint: in most cases, you'll want to use WAN here.
- Description:** Outside (text input field)  
You may enter a description here for your reference (not parsed).
- Memory Performance:** AC-STD (dropdown menu)  
Lowmem and ac-bnfa are recommended for low end systems, Ac: high memory, best performance, ac-std: moderate memory, high performance, acs: small memory, moderate performance, ac-banded: small memory, moderate performance, ac-sparsebands: small memory, high performance.

**Choose the networks snort should inspect and whitelist.**

- Home net:** default (dropdown menu)  
Choose the home net you will like this rule to use.  
Note: Default home net adds only local networks.  
Hint: Most users add a list of friendly ips that the firewall cant see.
- External net:** default (dropdown menu)  
Choose the external net you will like this rule to use.  
Note: Default external net, networks that are not home net.  
Hint: Most users should leave this setting at default.
- Block offenders:**   
Checking this option will automatically block hosts that generate a Snort alert.
- Kill states:**   
Should firewall states be killed for the blocked ip
- Which ip to block:** src (dropdown menu)  
Which ip extracted from the packet you want to block
- Whitelist:** default (dropdown menu)
- Suppression and filtering:** default (dropdown menu)  
Choose the suppression or filtering file you will like this rule to use.  
Note: Default option disables suppression and filtering.

**Choose the types of logs snort should create.**

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

**Services: Snort 2.9.1 pkg v. 2.1.1**

Snort Interfaces Global Settings Updates Alerts Blocked Whitelists Suppress Help

If	Snort	Performance	Block	Barnyard2	Description
WAN	ENABLED	AC-STD	ENABLED	DISABLED	Outside
LAN	ENABLED	AC-STD	ENABLED	DISABLED	Inside

click to toggle start/stop snort

**Note:**  
This is the **Snort Menu** where you can see an over view of all your interface settings. Please edit the **Global Settings** tab before adding an interface.

**Warning:**  
New settings will not take effect until interface restart.

Click on the icon to add a interface.  
Click on the icon to edit a interface and settings.  
Click on the icon to delete a interface and settings.

Click on the icon to **start** snort and barnyard2.  
Click on the icon to **stop** snort and barnyard2.

Edit the WAN interface > go to Categories, enable snort\_icmp\_info.rules, and save.

### Snort: Interface 0 45029 em0 Categories



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

Enabled	Ruleset: Rules that end with "so.rules" are shared object rules.
<input type="checkbox"/>	pfsense-voip.rules
<input type="checkbox"/>	snort_attack-responses.rules
<input type="checkbox"/>	snort_backdoor.rules
<input type="checkbox"/>	snort_bad-traffic.rules
<input type="checkbox"/>	snort_bad-traffic.so.rules
<input type="checkbox"/>	snort_blacklist.rules
<input type="checkbox"/>	snort_botnet-cnc.rules
<input type="checkbox"/>	snort_chat.rules
<input type="checkbox"/>	snort_chat.so.rules
<input type="checkbox"/>	snort_content-replace.rules
<input type="checkbox"/>	snort_ddos.rules
<input type="checkbox"/>	snort_deleted.rules
<input type="checkbox"/>	snort_dns.rules
<input type="checkbox"/>	snort_dos.rules
<input type="checkbox"/>	snort_dos.so.rules
<input type="checkbox"/>	snort_experimental.rules
<input type="checkbox"/>	snort_exploit.rules
<input type="checkbox"/>	snort_exploit.so.rules
<input type="checkbox"/>	snort_file-identify.rules
<input type="checkbox"/>	snort_finger.rules
<input type="checkbox"/>	snort_ftp.rules
<input checked="" type="checkbox"/>	snort_icmp-info.rules
<input type="checkbox"/>	snort_icmp.rules
<input type="checkbox"/>	snort_icmp.so.rules

**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:

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

Click Status > Services to show:

**Status: Services**

Service	Description	Status
dnsmasq	DNS Forwarder	Running
ntpd	NTP clock sync	Running
snort	Snort is the most widely deployed IDS/IPS technology worldwide.	Running

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 stopped. 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.**  
**Services: Snort Blocked Hosts**



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

---

**Last 500 Blocked.** This page lists hosts that have been blocked by Snort. Hosts are removed every hour.

Save or Remove Hosts Download All blocked hosts will be saved. Clear **Warning:** all hosts will be removed.

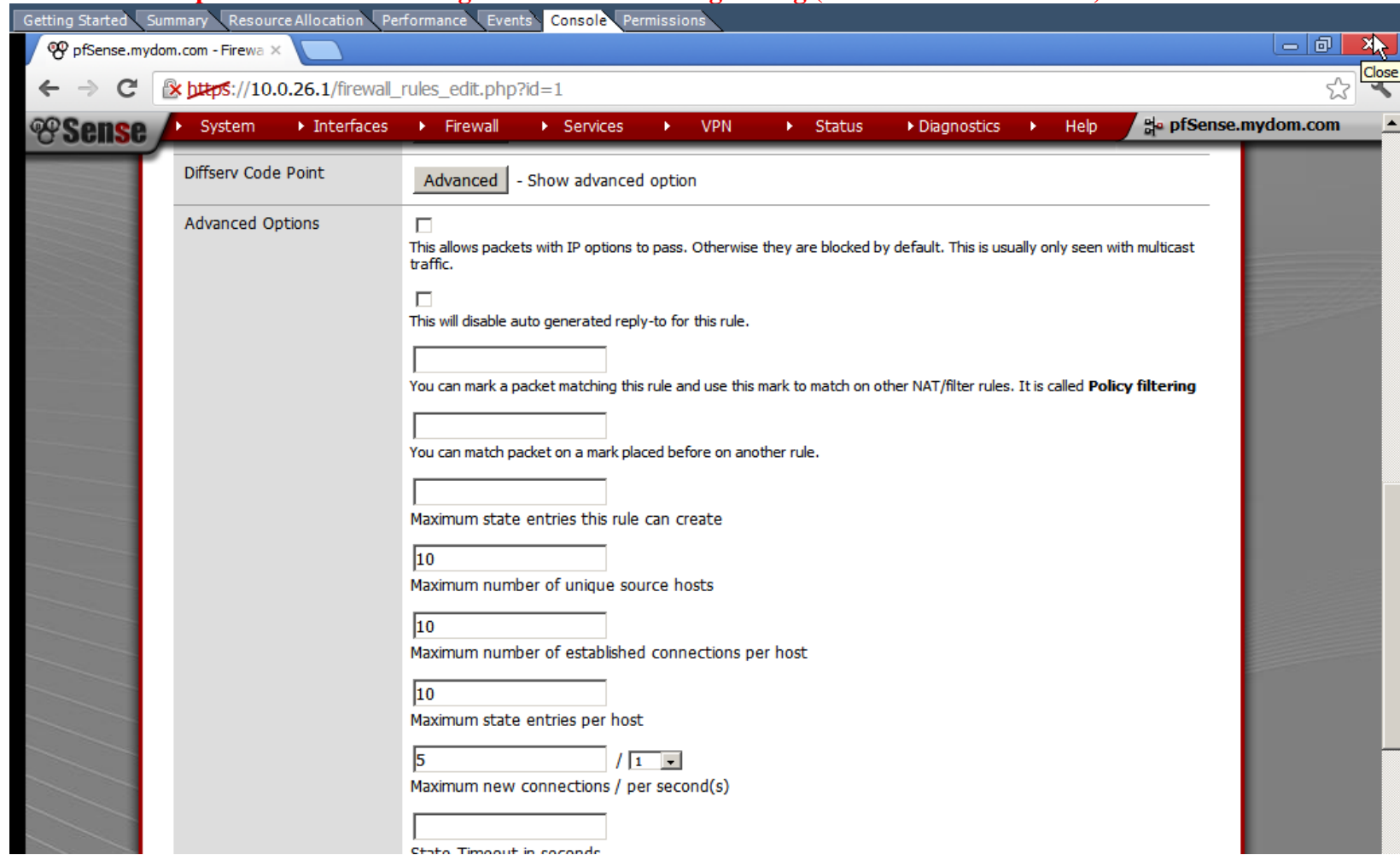
Auto Refresh and Log View Save Refresh  **Default is ON.**  Enter the number of blocked entries to view. **Default is 500.**

---

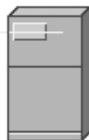
Remove	#	IP	Alert Description
	1	10.10.10.64	ICMP-INFO PING Windows 1 items listed.

**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)**



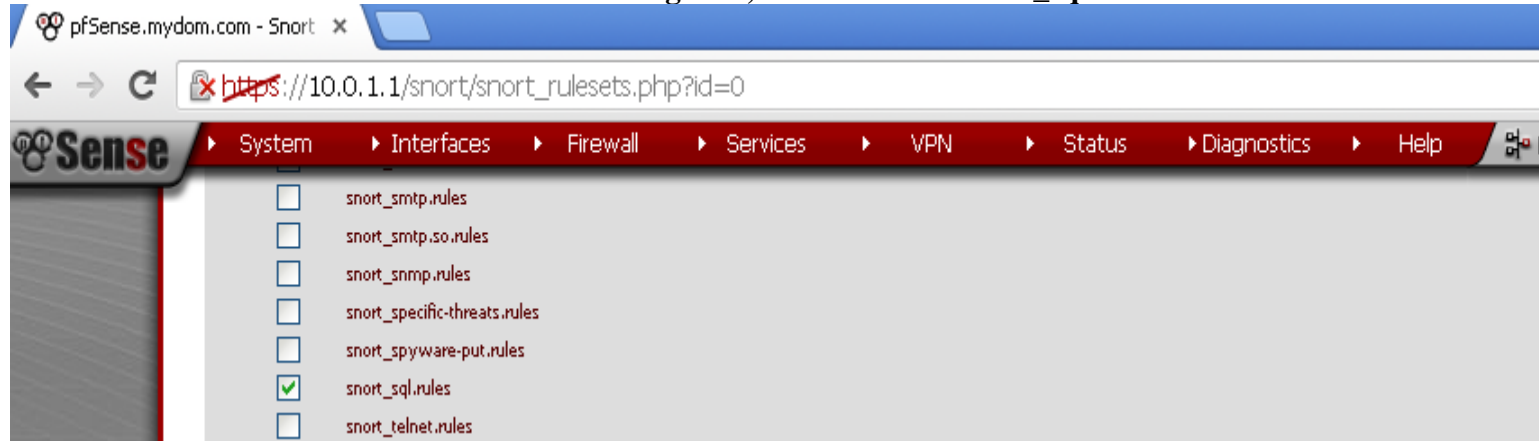
### Exercise Slammer with pfSense:



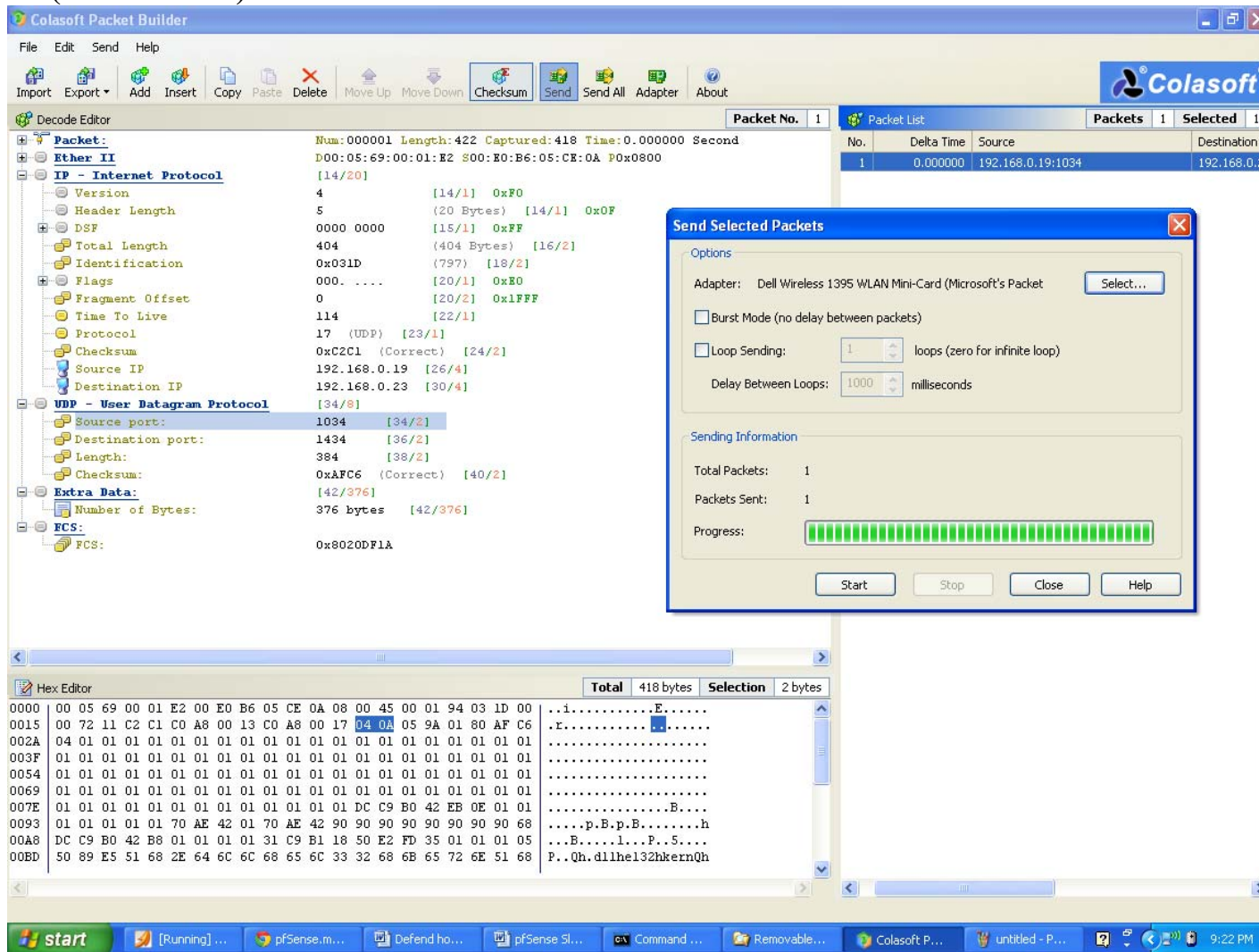
Virtual Box: pfSense inside: 10.0.1.1; outside 192.168.0.23
Host: 192.168.0.19 as attacker
Host: 10.0.1.4 as SQL server translated to 192.168.0.4

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.

The screenshot shows the pfSense web interface at the URL `https://10.0.1.1/snort/snort_blocked.php`. The page title is "Services: Snort Blocked Hosts". The navigation menu includes System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main content area has tabs for Snort Interfaces, Global Settings, Updates, Alerts, Blocked, Whitelists, Suppress, and Help. A red banner at the top of the main content area reads "Last 500 Blocked. This page lists hosts that have been blocked by Snort. Hosts are removed every hour." Below this banner are controls for "Save or Remove Hosts" (Download, Clear) and "Auto Refresh and Log View" (Save, Refresh, Default is ON, 500). A table lists the blocked hosts:

Remove	#	IP	Alert Description
	1	192.168.0.19	Slammer Worm Jim
	2	192.168.0.19	ICMP-INFO PING
	3	192.168.0.19	ICMP-INFO PING Windows

3 items listed.

### 6. View the System logs with filter:

The screenshot shows the pfSense web interface. The browser address bar displays `https://10.0.1.1/diag_logs.php`. The navigation menu includes System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main content area is titled "Status: System logs: System" and features a sub-menu with options: System, Firewall, DHCP, Portal Auth, IPsec, PPP, VPN, Load Balancer, OpenVPN, OpenNTPD, Wireless, and Settings. The "System" tab is selected, showing "Last 50 system log entries". The log entries are as follows:

Time	Message
Nov 18 04:56:28	snort[42122]: [1:1000009:9] Slammer Worm Jim {UDP} 192.168.0.19:1034 -> 192.168.0.23:1434
Nov 18 04:56:28	snort[42122]: [1:1000009:9] Slammer Worm Jim {UDP} 192.168.0.19:1034 -> 192.168.0.23:1434
Nov 18 04:56:30	snort[42122]: [1:1000009:9] Slammer Worm Jim {UDP} 192.168.0.19:1034 -> 192.168.0.23:1434
Nov 18 04:56:30	snort[42122]: [1:1000009:9] Slammer Worm Jim {UDP} 192.168.0.19:1034 -> 192.168.0.23:1434

At the bottom of the log view, there is a "Clear log" button, a text input field containing "Slammer", and a "Filter" button.

### 7. View Snort log at:

The screenshot shows the pfSense web interface. The browser address bar displays `https://10.0.1.1/snort/snort_alerts.php`. The navigation menu includes System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main heading is "Services: Snort: Snort Alerts". Below this, there are tabs for Snort Interfaces, Global Settings, Updates, Alerts, Blocked, Whitelists, Suppress, and Help. The "Alerts" tab is active.

Under the "Alerts" tab, there are two sections:

- Last 250 Alert Entries.** Latest Alert Entries Are Listed First. This section contains a "Download" button (with the note "All log files will be saved.") and a "Clear" button (with the note "Warning: all log files will be deleted.>").
- Auto Refresh and Log View.** This section contains a "Save" button, a "Refresh" checkbox (which is unchecked), a "Default is ON." checkbox (which is checked), a text input field with the value "250", and the text "Enter the number of log entries to view. Default is 250."

Below these sections is a filter area with a dropdown menu set to "PRIORITY", a text input field, and "Submit" and "Clear" buttons.

The main content is a table of alert entries:

#	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.**