

OLD DOMINION UNIVERSITY

CYSE 301: Cybersecurity Technique and  
Operations

**Assignment 3: Sword vs. Shield**

Alan Schneider

Aschn014

I used the command `nmap -sV -T4 192.168.10.0/24` to scan the network determining open ports, services and software version.

- Run Wireshark in Ubuntu VM while External Kali is scanning the network. Discuss the traffic pattern you observed. What do you find? **Please write a 200-word essay to discuss your findings.**

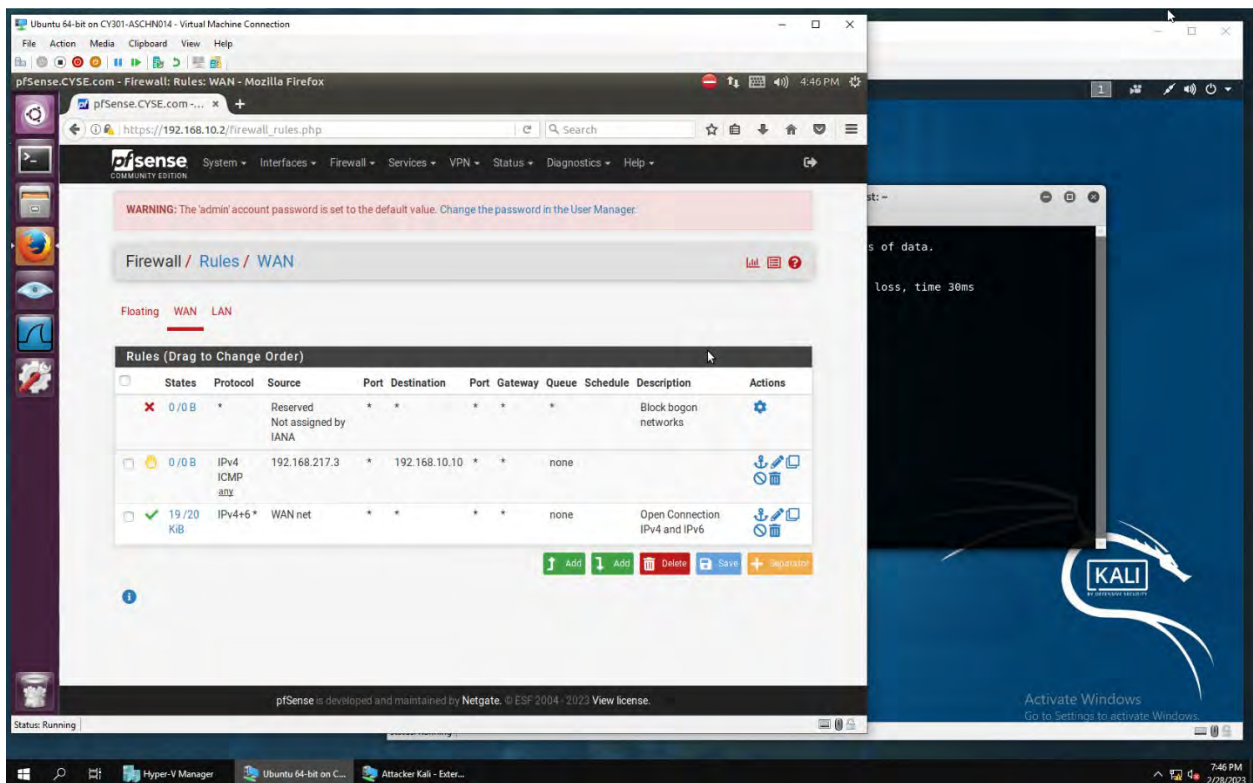
I ran a wireshark filter: `ip.addr==192.168.217.3 && ip.addr==192.168.10.11` to isolate the captured traffic between external kali and ubuntu during the scan. I observed external kali scanning for open ports through 3-way handshake connection between the source: 192.168.217.3 and destination: 192.168.10.11 port. When it found an open port then the source made a request with a SYN packet, a response destination sent SYN, ACK packet and then source sent ACK packets, at last source again sent RST, ACK packets. Open ports discovered were: 21, 80 135, 145 3389 and 49154. For the closed ports a 3-way handshake connection was not possible between source and destination. For example The source sent a Syn packet, to see if port 554 was open, it was not so a three way handshake was not possible. The destination send a response via RST, ACK.

### Task B: Shield – Protect your network with firewall (10 + 10+ 20 + 20 = 60 points)

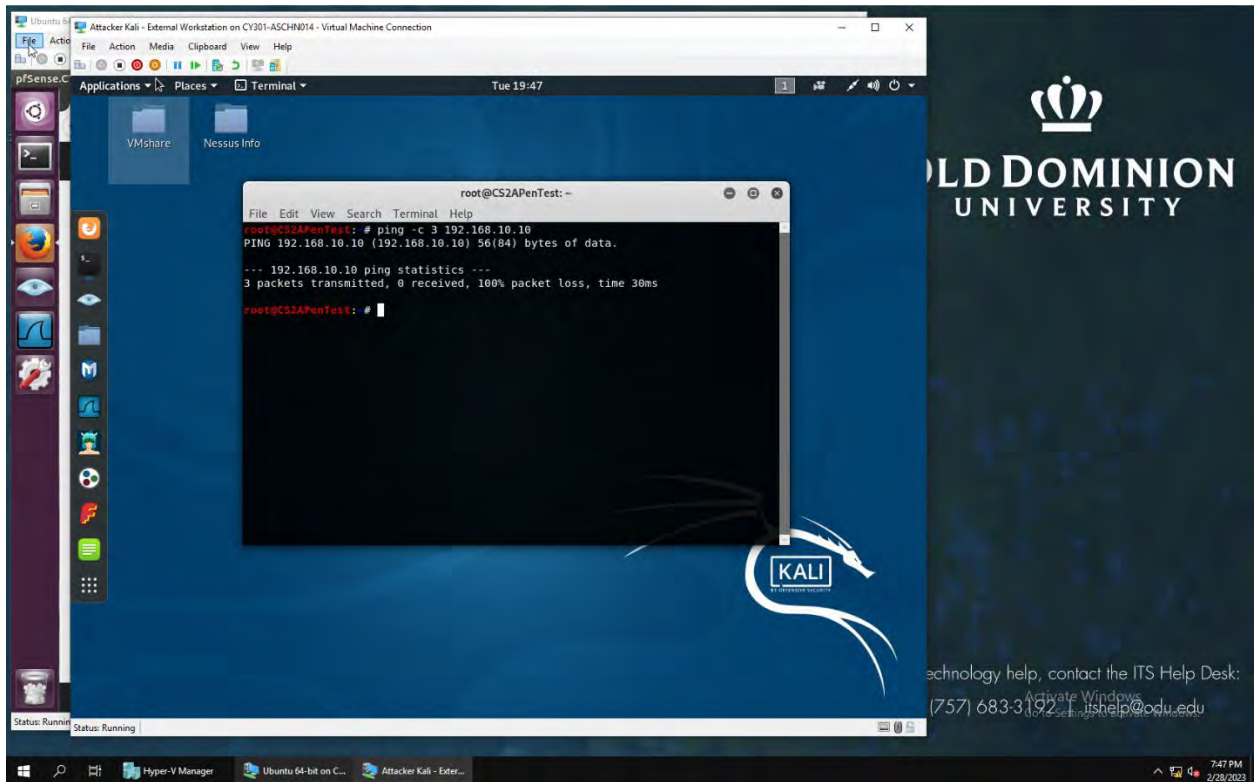
**In order to receive full credits, you need to fill the table (add more rows if needed), implement the firewall rule(s), show me the screenshot of your firewall table, and verify the results.**

- Configure the pfSense firewall rule to block the ICMP traffic from External Kali to Ubuntu VM.

Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if applicable)
01	WAN	reject	192.168.217.3	192.168.10.10	ICMP



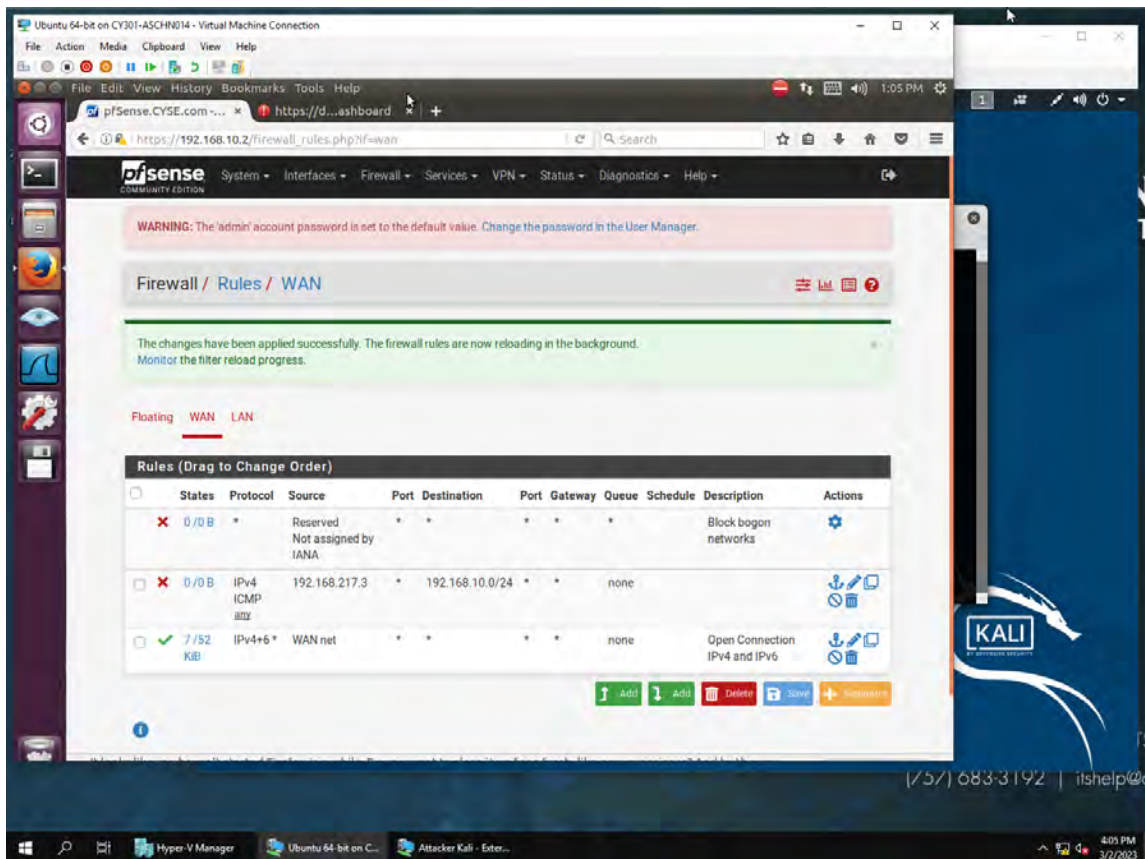
Below are the experiments I used to test the rule.



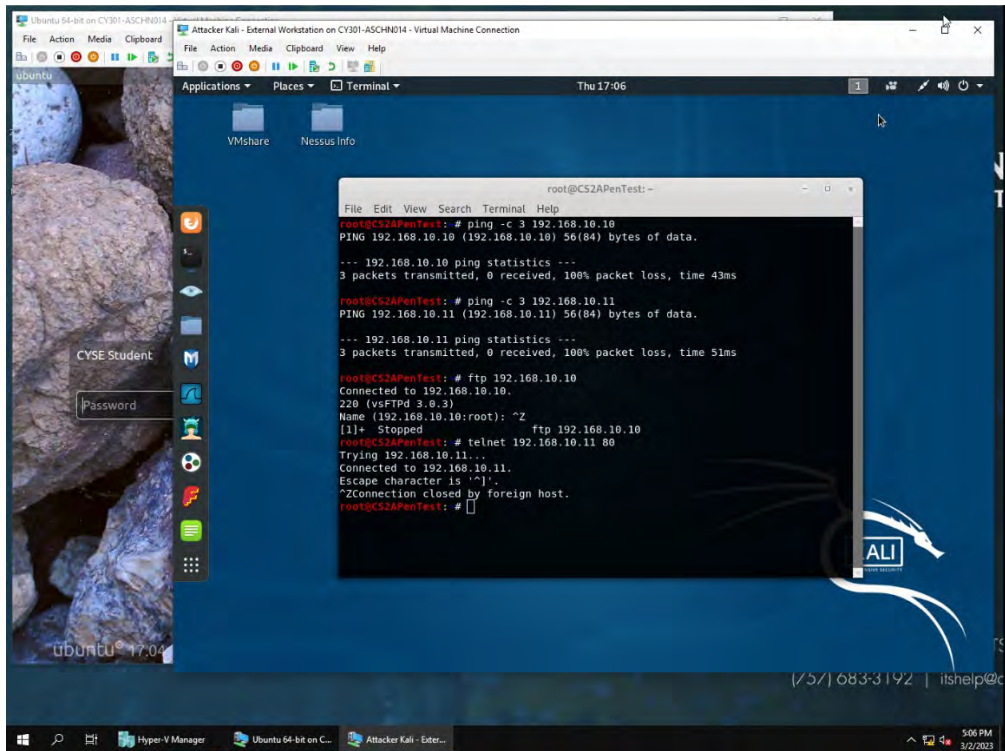
- A. I used Ping -c 3 192.168.10.10 from 192.168.217.3. The result: 3 packets transmitted, 0 received 100% packet loss, time 36ms.

- Clear the previous firewall policies and configure the pfSense firewall to block all ICMP traffic from External Kali to the LAN side.

Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if applicable)
02	WAN	reject	192.168.217.3	192.168.10.0/24	ICMP



Below are the experiments I used to test the rule.



The screenshot shows a Kali Linux virtual machine environment. A terminal window is open, displaying the following commands and output:

```
root@CS2APenTest:~# ping -c 3 192.168.10.10
PING 192.168.10.10 (192.168.10.10) 56(84) bytes of data.
--- 192.168.10.10 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 43ms

root@CS2APenTest:~# ping -c 3 192.168.10.11
PING 192.168.10.11 (192.168.10.11) 56(84) bytes of data.
--- 192.168.10.11 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 51ms

root@CS2APenTest:~# ftp 192.168.10.10
Connected to 192.168.10.10.
220 (vsFTPD 3.0.3)
Name (192.168.10.10:root): ^Z
[!]+ Stopped
root@CS2APenTest:~# telnet 192.168.10.11 80
Trying 192.168.10.11...
Connected to 192.168.10.11.
Escape character is '^['.
^ZConnection closed by foreign host.
root@CS2APenTest:~#
```

- A. I used Ping -c 3 192.168.10.10 command and then ping -c 3 192.168.10.11 from 192.168.217.3. The result for both: 3 packets transmitted, 0 received 100% packet loss, time 36ms and 56ms.ftp
- B. I was able to connect to ubuntu 192.168.10.10 via ftp from 192.168.217.3
- C. I was able to connect to window 8 server 192.168.10.11 via over port 80 http from 192.168.217.3

- Clear the previous firewall policies and configure the pfSense firewall to block ALL traffic from External Kali to the LAN side, except for the FTP protocol towards Windows Server 2008.

Rule #	Interface	Action	Source IP	Destination IP	Protocol (port # if applicable)
01	WAN	Block	192.168.217.3	192.168.10.0/24	All
02	WAN	Pass	192.168.217.3	192.168.10.11	FTP

Ubuntu 64-bit on CY301-ASCHN014 - Virtual Machine Connection

File Action Media Clipboard View Help

pfSense.CYSE.com - Firewall: Rules: WAN - Mozilla Firefox

https://d...ashboard x +

https://192.168.10.2/firewall\_rules.php

Search

pfSense COMMUNITY EDITION

System Interfaces Firewall Services VPN Status Diagnostics Help

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Firewall / Rules / WAN

Floating WAN LAN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✗ 0/0 B	*	Reserved Not assigned by IANA	*	*	*	*	*	*	Block bogon networks	
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	192.168.217.3	*	192.168.10.11	21 (FTP)	*	none		Open Connection IPv4 and IPv6	
<input type="checkbox"/>	✗ 0/0 B	IPv4 *	192.168.217.3	*	192.168.10.0/24	*	*	none		Open Connection IPv4 and IPv6	
<input type="checkbox"/>	✓ 1/393 KIB	IPv4+6	WAN net	*	*	*	*	none		Open Connection IPv4 and IPv6	

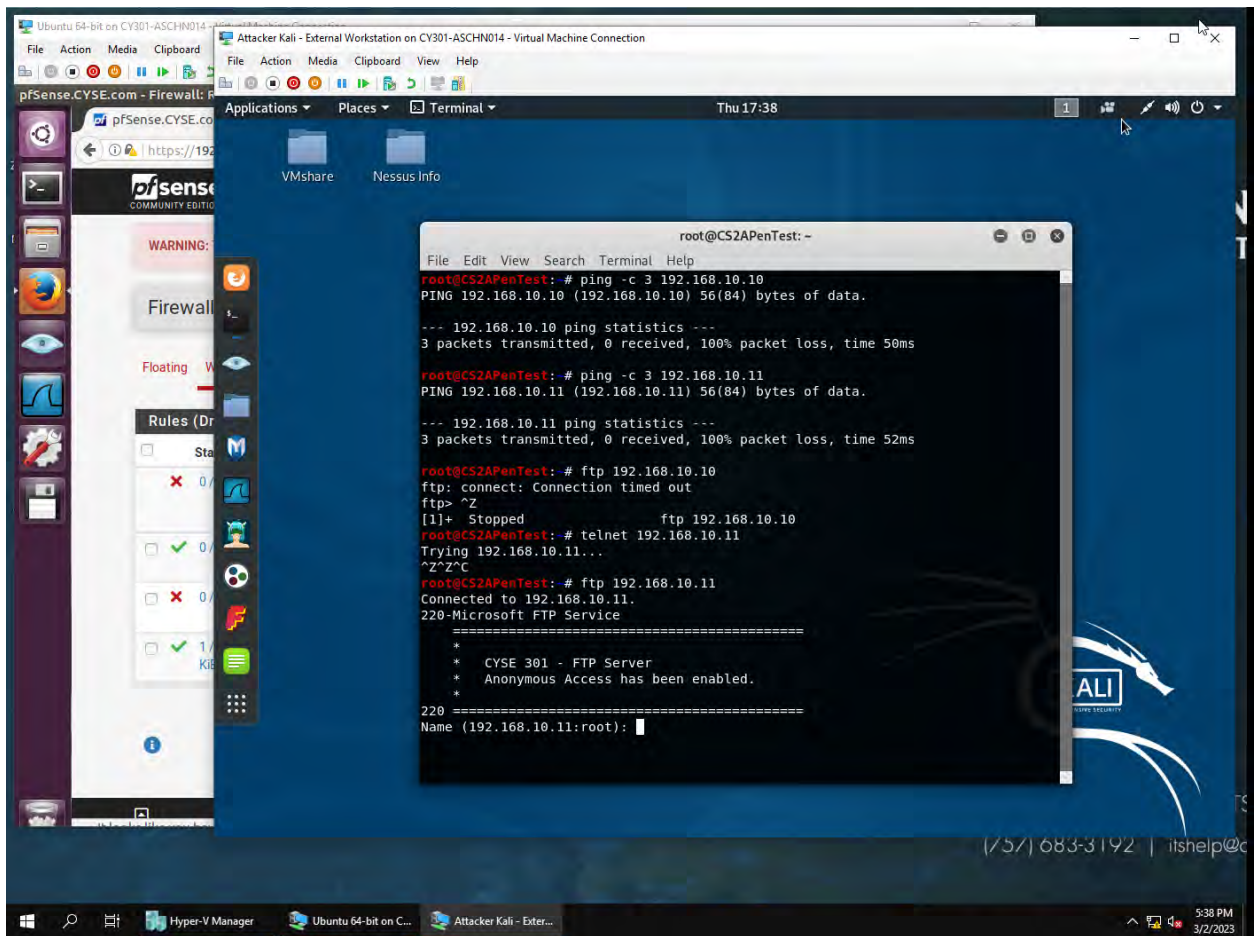
Add Add Delete Save Export

pfSense is developed and maintained by Netgate. © PFSense 2014 - 2022. View license

Hyper-V Manager Ubuntu 64-bit on C... Attacker Kali - Exter...

5:28 PM 3/2/2023

Below are the experiments I used to test the rule



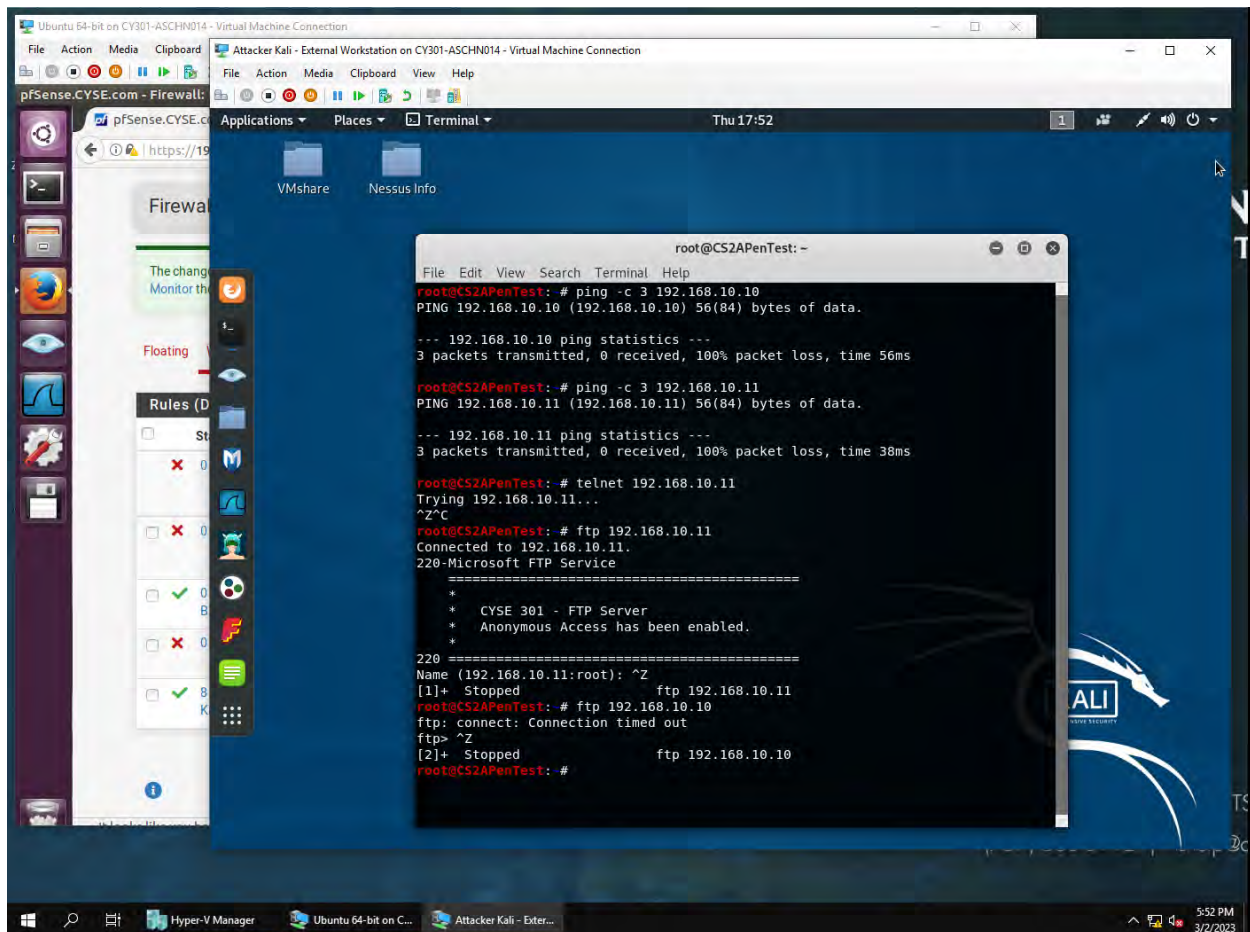
- A. I used Ping -c 3 192.168.10.10 command and then ping -c 3 192.168.10.11 from 192.168.217.3. As I used a block action. The result for both: 3 packets transmitted, 0 received 100% packet loss, time 36ms and 56ms
- B. I was unable to connect to ubuntu 192.168.10.10 via ftp from 192.168.217.3
- C. I was unable to connect to window 8 server 192.168.10.11 via over port 80 http from 192.168.217.3
- D. I was able to connect to Windows 8 server 192.168.10.11 via ftp port 21 from 192.168.217.3

4. Keep the firewall policies you created in Task B.3 and repeat Task A.1. What's the difference?

The screenshot shows the pfSense web interface for configuring Firewall Rules on the WAN interface. A green notification bar at the top states: "The changes have been applied successfully. The firewall rules are now reloading in the background. Monitor the filter reload progress." Below this, the "Rules (Drag to Change Order)" table is displayed. The table has columns for States, Protocol, Source, Port, Destination, Port, Gateway, Queue, Schedule, Description, and Actions. The rules are as follows:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/> 0/0 B	*	Reserved Not assigned by IANA	*	*	*	*	*	*	Block bogon networks	
<input checked="" type="checkbox"/> 0/0 B	IPv4 ICMP	192.168.217.3	*	192.168.10.10	*	*	none			
<input checked="" type="checkbox"/> 0/639 B	IPv4 TCP	192.168.217.3	*	192.168.10.11	21 (FTP)	*	none			
<input checked="" type="checkbox"/> 0/1 KiB	IPv4*	192.168.217.3	*	192.168.10.0/24	*	*	none			
<input checked="" type="checkbox"/> 8/444 KiB	IPv4+6*	WAN net	*	*	*	*	none		Open Connection IPv4 and IPv6	

At the bottom of the table, there are buttons for "Add", "Add", "Delete", "Save", and "Separator". The interface is running on a Kali Linux virtual machine, as indicated by the desktop background and taskbar.



Although the new firewall rule specifically blocks icmp traffic from external kali 192.168.217.3 to ubuntu 192.168.10.10. The previous firewall rule is applied first and already blocks any traffic to include ICMP from external kali 192.168.217.3 to the 192.168.10.0/24 network. Then the firewall rule to pass ftp port 21 from 192.168.217.3 to 192.168.10.11 only.

**Extra credit (15 points):** Use NESSUS to enumerate the security vulnerabilities of Microsoft Windows Server 2008 VM in the CCIA network.