Typology:

A blue circle with green and black dots and a white arrow

Description automatically generated with medium confidence

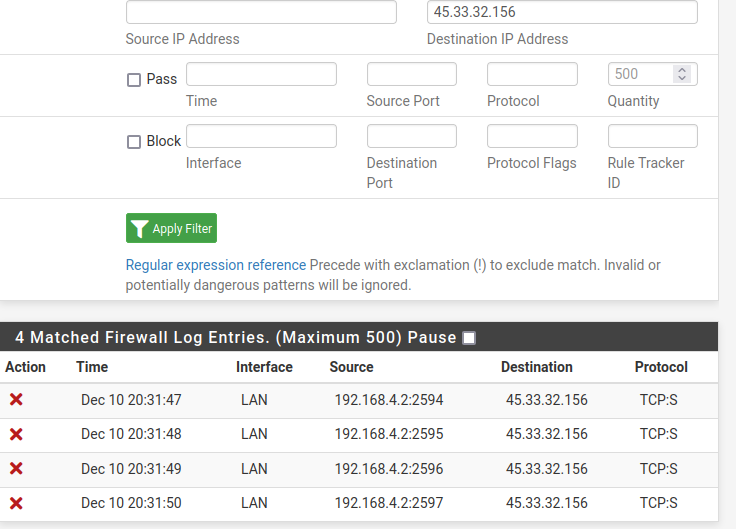
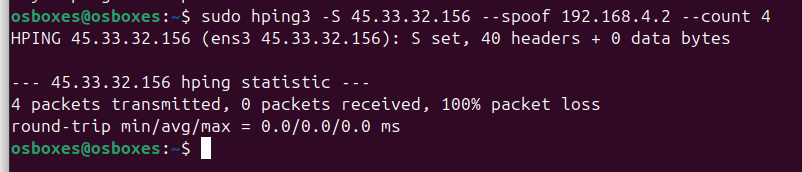
1. The IP address that the firewall's DHCP server assigns to the Lubuntu VM on the internal network.

**192.168.1.100**

A screenshot of a computer

Description automatically generated

2. Use hping3 to ping the IP 45.33.32.156 while spoofing the IP address to be 192.168.4.2.



The firewall logs clearly show evidence of pfSense's anti-spoofing policy working as intended. Multiple RCP:S packets with a spoofed source IP of 192.168.4.2 (outside the LAN's 192.168.1.0/24 subnet) were blocked, as indicated by the red "X" icons. The destination IP 45.33.32.156 matches the target of the hping3 test, but since the source address was invalid for the LAN interface, pfSense intercepted and blocked the packets. It is important to note that the "S" in the logs indicates the first step of a stateful TCP connection (SYN flag), which is essential to establishing a valid connection. The firewall correctly identified and blocked these spoofed SYN packets, confirming that the anti-spoofing mechanism effectively prevents spoofed traffic from leaving the network.

3. Using hping, but this time spoof a source IP address that is part of the internal network served by this firewall.

A screenshot of a computer

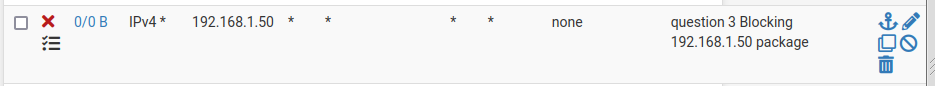
Description automatically generated

A screenshot of a computer

Description automatically generated

**No**, the packet was not blocked. The screenshot shows that the spoofed packet with a source IP of **192.168.1.50** (within the internal network's subnet) was allowed by the firewall, indicated by the green checkmark. Since the IP is part of the LAN subnet, pfSense treated it as valid for the interface and did not block it, demonstrating that anti-spoofing policies do not inherently block spoofed traffic within the same subnet.

4. Next, configurering a pfSense firewall rule that specifically blocks all outgoing packets with the source IP in the previous question



A screenshot of a computer program

Description automatically generated

A screenshot of a number

Description automatically generated

**Yes**, the IP is blocked now. The new rule explicitly blocks all traffic originating from **192.168.1.50**, as shown in the rules configuration screenshot. The block rule is applied to the LAN interface, and its placement ensures it takes precedence over the default "allow" rules. This configuration effectively prevents any outgoing packets from the specified source IP, confirming the packet is now blocked.

3. Next, configure the LAN-to-WAN rule that blocks all outgoing ICMP packets.

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

Blocking outgoing ICMP packets from the LAN to the WAN adds an extra layer of security by preventing devices in the internal network from sending ICMP-based requests, such as pings, to external destinations. This measure can help mitigate risks associated with network reconnaissance, where attackers might use ICMP to map the network or identify active devices. Additionally, it prevents ICMP-based denial-of-service (DoS) attacks originating from compromised internal devices. While ICMP has legitimate uses, such as diagnostics and troubleshooting, these functions are rarely needed for regular users on the LAN. By blocking ICMP while allowing other traffic, the network maintains its functionality while reducing its exposure to potential threats.

4. Add rules to ban traffic to at least 5 address blocks from network addresses hosted in Russia and China. Test your rule. Please provide screenshot evidence and explanations.

**Website 1: Russian website kremlin.ru**

A screenshot of a web page

Description automatically generated

**Implementing a firewall rule to block the website**

A screenshot of a computer

Description automatically generated

A computer screen with white text

Description automatically generated

This image shows all the ping being blocked after the firewall rule implementation.

A screenshot of a computer

Description automatically generated

This image shows TCP package is also being blocked at the end of the photo, which shows that I can’t reach the website in the browser as well.

A screenshot of a computer

Description automatically generated

**Website 2: Second Russian website, www.mid.ru**

**Proof of accessing the website before firewall configuration.**

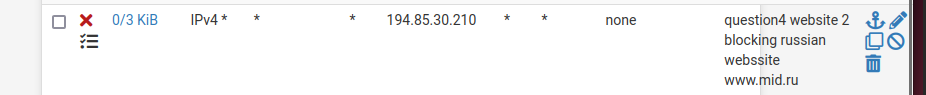
A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Firewall rule implementation for website 2



Now you can see I can’t access the same website

A screenshot of a browser

Description automatically generated

Log file which shows it’s block

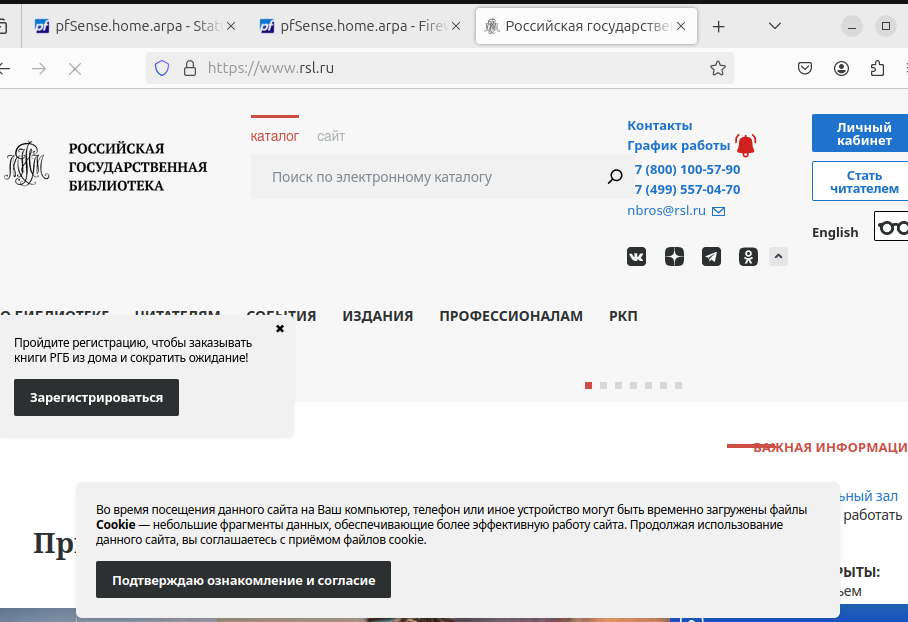
A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

**Website 3: Russian website : rsl.ru**

Proof that I can access it before firewall configuration:



A screenshot of a computer program

Description automatically generated

A screenshot of a computer

Description automatically generated

Rule to block the www.rsl.ru

A white background with black numbers

Description automatically generated

Proof that now it’s being blocked:

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a browser

Description automatically generated

**Website 4: Chinese website fmprc.gov.cn**

Proof that I can access it before firewall implementation. TCP/ICMP pings

A screenshot of a computer

Description automatically generated

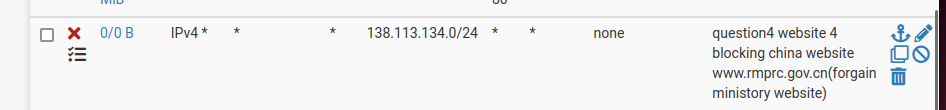
A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Firewall Implementation: as you can see, the IP range is going to be blocked for this website



Proof after implementation it is being blocked:

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**Website 5: mofcom.gov.con Chinese website**

Proof that I can assess the website before implementation of rules

A screenshot of a computer

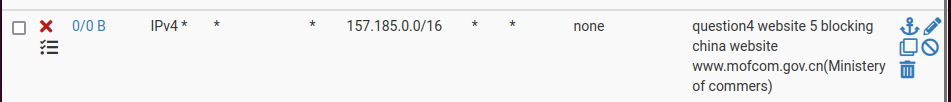
Description automatically generated

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

Firewall rule implementation:



Proof of after implementation now I can’t access the website:

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a browser

Description automatically generated

**End of question 4**

**5. Only allows https sessions with the server hosting Fullerton.edu domain.**

Proof of Pinging Fullerton and Google before implementation:

A screenshot of a computer

Description automatically generatedA screenshot of a computer program

Description automatically generated

Firewall implementation:

A screenshot of a computer

Description automatically generated

After firewall implementation, you can see google is being blocked but it’s allowing Fullerton.edu

A screenshot of a browser

Description automatically generatedA screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

This is an additional image for the firewall rule, including all regulations, for your clarification.

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated