

This project explores how to capture and analyze network traffic on a pfSense firewall using Wireshark and tcpdump. The goal is to gain insight into the traffic passing through the firewall and identify any potential security issues or suspicious activity.

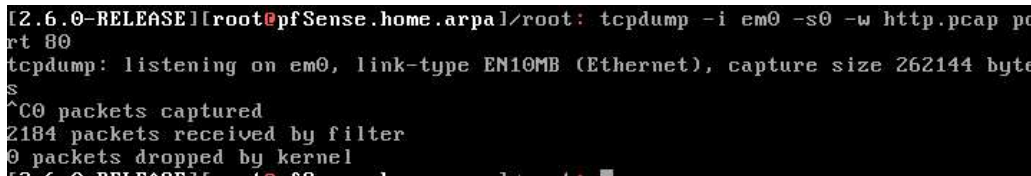
To start with go to Wireshark

After it has been running for a few minutes go to the website of your choice

On the pfSense firewall, access the shell by selecting option 8

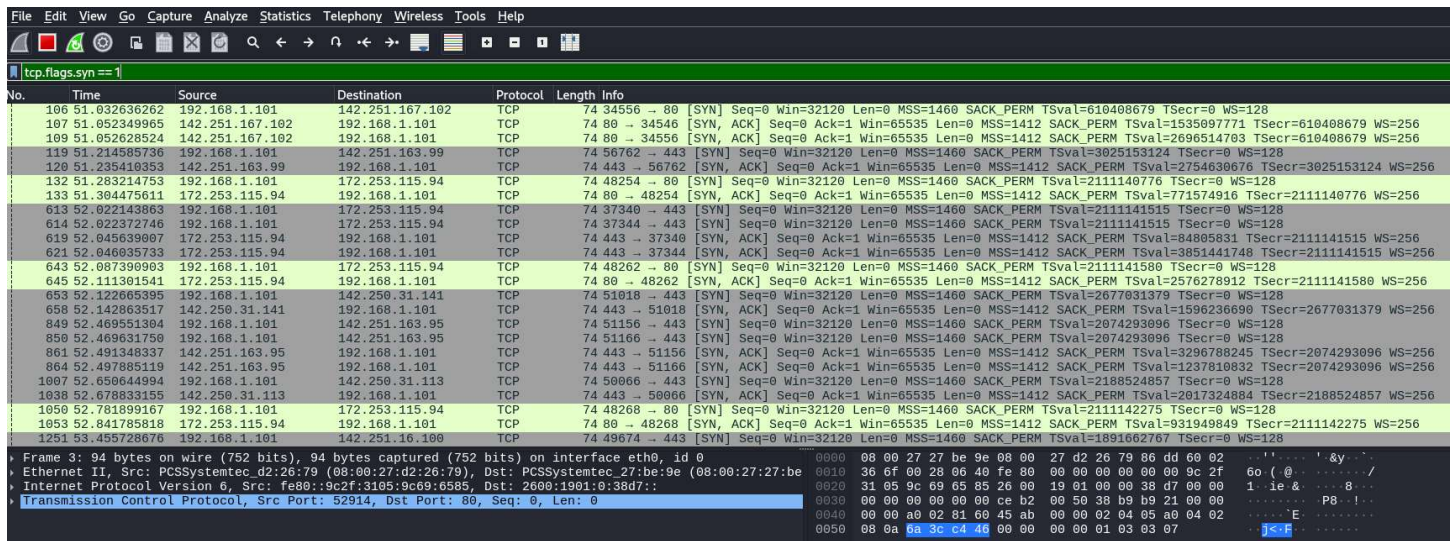


In the shell, run the following tcpdump command to capture all HTTP traffic on the em0 interface and save it to a file named http.pcap: “tcpdump -i em0 -s0 -w http.pcap port 80”

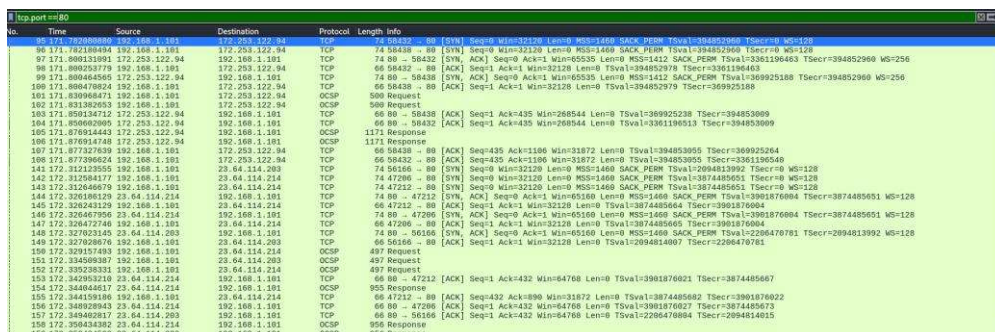


In Wireshark, you can apply the following filters to view specific traffic:

ip.dst == 192.168.1.101 to see traffic to a specific IP address



tcp.port == 80 to see only HTTP traffic



http to see HTTP protocol-specific information

No.	Time	Source	Destination	Protocol	Length	Info
101	171.830968471	192.168.1.101	172.253.122.94	OCSP	500	Request
102	171.831382653	192.168.1.101	172.253.122.94	OCSP	500	Request
105	171.876914443	172.253.122.94	192.168.1.101	OCSP	1171	Response
106	171.876914748	172.253.122.94	192.168.1.101	OCSP	1171	Response
150	172.329157493	192.168.1.101	23.64.114.214	OCSP	497	Request
151	172.334509387	192.168.1.101	23.64.114.203	OCSP	497	Request
152	172.335238331	192.168.1.101	23.64.114.214	OCSP	497	Request
154	172.344044617	23.64.114.214	192.168.1.101	OCSP	955	Response
158	172.350434382	23.64.114.214	192.168.1.101	OCSP	956	Response
159	172.350434599	23.64.114.203	192.168.1.101	OCSP	956	Response
235	172.650303918	192.168.1.101	172.253.122.94	OCSP	494	Request
238	172.697680318	172.253.122.94	192.168.1.101	OCSP	768	Response
542	173.019746383	192.168.1.101	23.64.114.203	OCSP	497	Request
622	173.040324754	23.64.114.203	192.168.1.101	OCSP	955	Response
855	173.105338394	192.168.1.101	23.64.114.203	OCSP	497	Request
1046	173.149406252	23.64.114.203	192.168.1.101	OCSP	955	Response
4133	174.413907781	192.168.1.101	23.64.114.203	OCSP	497	Request
4142	174.429627267	23.64.114.203	192.168.1.101	OCSP	956	Response
4145	174.430342716	192.168.1.101	23.64.114.203	OCSP	497	Request
4150	174.440222397	192.168.1.101	34.107.221.82	HTTP	376	GET /success.txt?ipv4 HTTP/1.1
4153	174.447700520	23.64.114.203	192.168.1.101	OCSP	956	Response
4168	174.461837304	34.107.221.82	192.168.1.101	HTTP	282	HTTP/1.1 200 OK (text/plain)

Following the TCP stream by right-clicking on a packet and select "Follow" > "TCP Stream"

```
Wireshark · Follow TCP Stream (tcp.stream eq 18) · eth0

GET /success.txt?ipv4 HTTP/1.1
Host: detectportal.firefox.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Priority: u=4
Pragma: no-cache
Cache-Control: no-cache

HTTP/1.1 200 OK
Server: nginx
Content-Length: 8
Via: 1.1 google
Date: Tue, 03 Dec 2024 04:05:11 GMT
Age: 50490
Content-Type: text/plain
Cache-Control: public,must-revalidate,max-age=0,s-maxage=3600

success
```

In this project, you can see how to capture and analyze network traffic on a pfSense firewall using Wireshark and tcpdump. By applying various filters and techniques, you can identify suspicious activity and investigate potential security issues within your network. This knowledge can be valuable for maintaining the security and integrity of your network infrastructure.