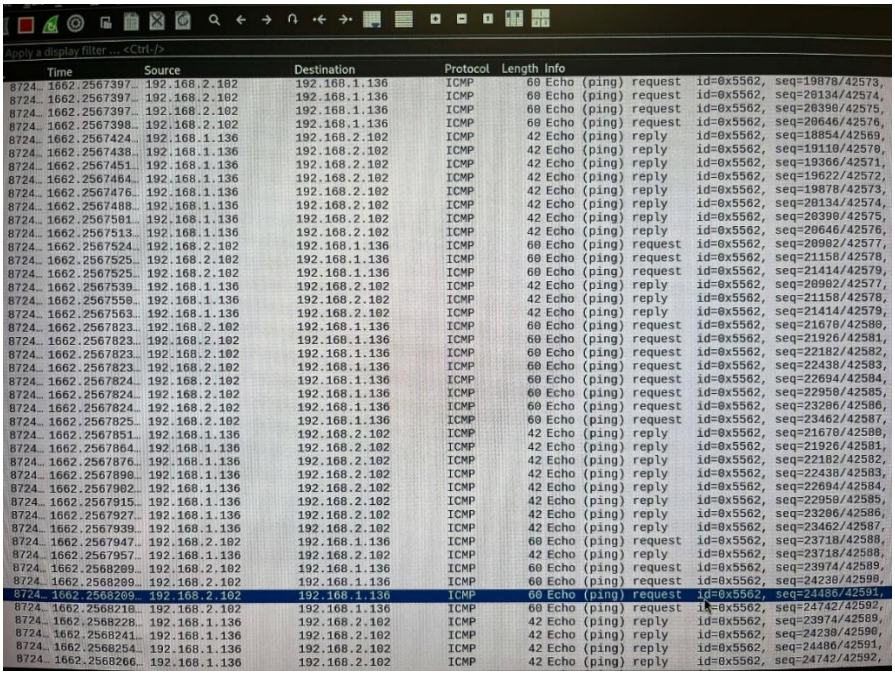
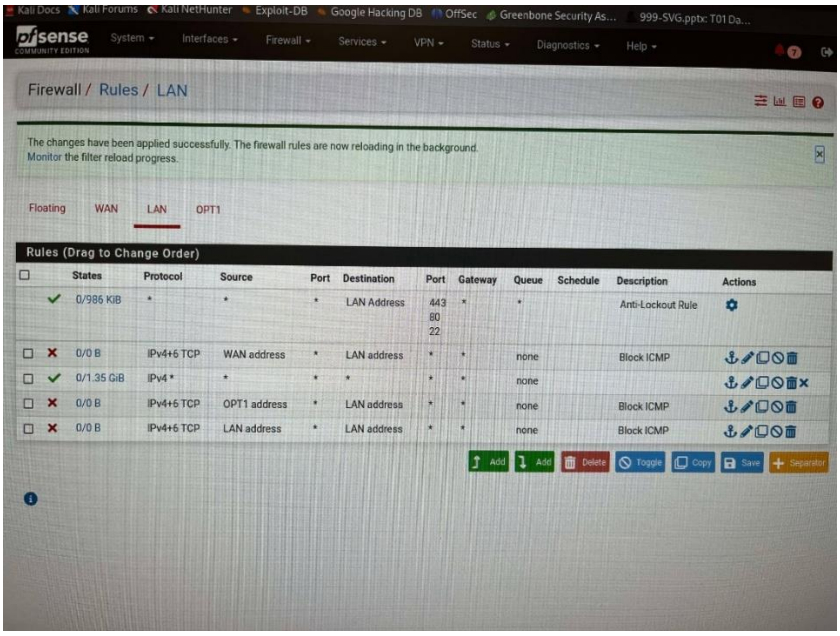
Lab Project: DDOS attacks defend

I used Wireshark to see the network traffic and identify that the systems were being attacked by DDoS. If thousands of ICMP packets are sent to the system or a computer from a spoofed source, this means this is a DDoS attack using ICMP.

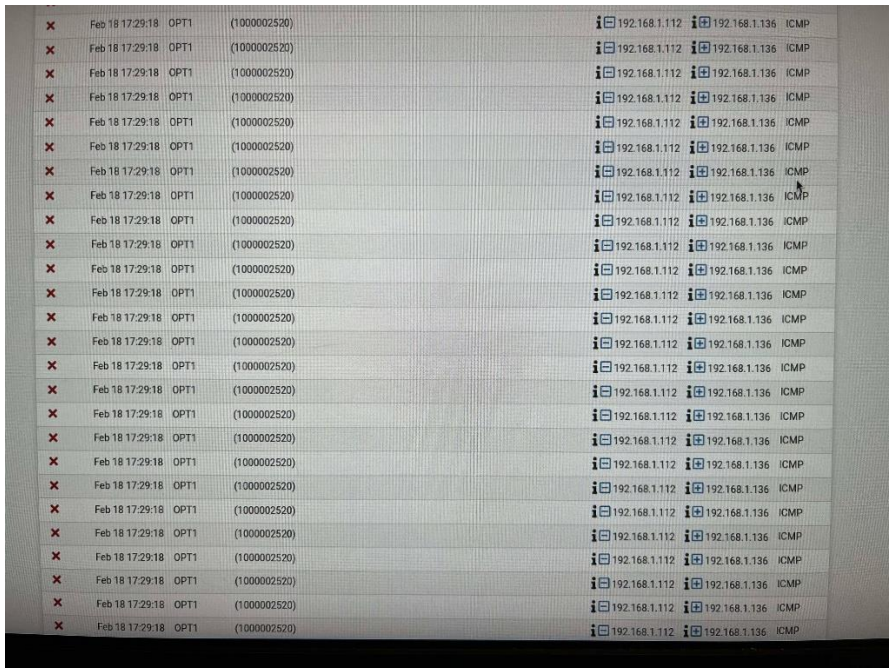


Time	Source	Destination	Protocol	Length	Info
8724… 1662.2567397…	192.168.2.102	192.168.1.136	ICMP	60	Echo (ping) request id=0x5562, seq=19878/42573,
8724… 1662.2567397…	192.168.2.102	192.168.1.136	ICMP	60	Echo (ping) request id=0x5562, seq=20134/42574,
8724… 1662.2567397…	192.168.2.102	192.168.1.136	ICMP	60	Echo (ping) request id=0x5562, seq=20390/42575,
8724… 1662.2567398…	192.168.2.102	192.168.1.136	ICMP	60	Echo (ping) request id=0x5562, seq=20646/42576,
8724… 1662.2567424…	192.168.1.136	192.168.2.102	ICMP	42	Echo (ping) reply id=0x5562, seq=18854/42569,
8724… 1662.2567438…	192.168.1.136	192.168.2.102	ICMP	42	Echo (ping) reply id=0x5562, seq=19110/42570,
8724… 1662.2567451…	192.168.1.136	192.168.2.102	ICMP	42	Echo (ping) reply id=0x5562, seq=19366/42571,
8724… 1662.2567464…	192.168.1.136	192.168.2.102	ICMP	42	Echo (ping) reply id=0x5562, seq=19622/42572,
8724… 1662.2567476…	192.168.1.136	192.168.2.102	ICMP	42	Echo (ping) reply id=0x5562, seq=19878/42573,
8724… 1662.2567488…	192.168.1.136	192.168.2.102	ICMP	42	Echo (ping) reply id=0x5562, seq=20134/42574,
8724… 1662.2567501…	192.168.1.136	192.168.2.102	ICMP	42	Echo (ping) reply id=0x5562, seq=20390/42575,
8724… 1662.2567513…	192.168.1.136	192.168.2.102	ICMP	42	Echo (ping) reply id=0x5562, seq=20646/42576,
8724… 1662.2567524…	192.168.2.102	192.168.1.136	ICMP	60	Echo (ping) request id=0x5562, seq=20902/42577,
8724… 1662.2567525…	192.168.2.102	192.168.1.136	ICMP	60	Echo (ping) request id=0x5562, seq=21158/42578,
8724… 1662.2567525…	192.168.2.102	192.168.1.136	ICMP	60	Echo (ping) request id=0x5562, seq=21414/42579,
8724… 1662.2567539…	192.168.1.136	192.168.2.102	ICMP	42	Echo (ping) reply id=0x5562, seq=20902/42577,
8724… 1662.2567558…	192.168.1.136	192.168.2.102	ICMP	42	Echo (ping) reply id=0x5562, seq=21158/42578,
8724… 1662.2567553…	192.168.1.136	192.168.2.102	ICMP	42	Echo (ping) reply id=0x5562, seq=21414/42579,
8724… 1662.2567823…	192.168.2.102	192.168.1.136	ICMP	60	Echo (ping) request id=0x5562, seq=21670/42580,
8724… 1662.2567823…	192.168.2.102	192.168.1.136	ICMP	60	Echo (ping) request id=0x5562, seq=21926/42581,
8724… 1662.2567823…	192.168.2.102	192.168.1.136	ICMP	60	Echo (ping) request id=0x5562, seq=22182/42582,
8724… 1662.2567823…	192.168.2.102	192.168.1.136	ICMP	60	Echo (ping) request id=0x5562, seq=22438/42583,
8724… 1662.2567824…	192.168.2.102	192.168.1.136	ICMP	60	Echo (ping) request id=0x5562, seq=22694/42584,
8724… 1662.2567824…	192.168.2.102	192.168.1.136	ICMP	60	Echo (ping) request id=0x5562, seq=22950/42585,
8724… 1662.2567824…	192.168.2.102	192.168.1.136	ICMP	60	Echo (ping) request id=0x5562, seq=23206/42586,
8724… 1662.2567825…	192.168.2.102	192.168.1.136	ICMP	60	Echo (ping) request id=0x5562, seq=23462/42587,
8724… 1662.2567851…	192.168.1.136	192.168.2.102	ICMP	42	Echo (ping) reply id=0x5562, seq=21670/42580,
8724… 1662.2567864…	192.168.1.136	192.168.2.102	ICMP	42	Echo (ping) reply id=0x5562, seq=21926/42581,
8724… 1662.2567876…	192.168.1.136	192.168.2.102	ICMP	42	Echo (ping) reply id=0x5562, seq=22182/42582,
8724… 1662.2567890…	192.168.1.136	192.168.2.102	ICMP	42	Echo (ping) reply id=0x5562, seq=22438/42583,
8724… 1662.2567902…	192.168.1.136	192.168.2.102	ICMP	42	Echo (ping) reply id=0x5562, seq=22694/42584,
8724… 1662.2567915…	192.168.1.136	192.168.2.102	ICMP	42	Echo (ping) reply id=0x5562, seq=22950/42585,
8724… 1662.2567927…	192.168.1.136	192.168.2.102	ICMP	42	Echo (ping) reply id=0x5562, seq=23206/42586,
8724… 1662.2567939…	192.168.1.136	192.168.2.102	ICMP	42	Echo (ping) reply id=0x5562, seq=23462/42587,
8724… 1662.2567947…	192.168.2.102	192.168.1.136	ICMP	60	Echo (ping) request id=0x5562, seq=23718/42588,
8724… 1662.2567957…	192.168.1.136	192.168.2.102	ICMP	42	Echo (ping) reply id=0x5562, seq=23718/42588,
8724… 1662.2568209…	192.168.2.102	192.168.1.136	ICMP	60	Echo (ping) request id=0x5562, seq=23974/42589,
8724… 1662.2568209…	192.168.2.102	192.168.1.136	ICMP	60	Echo (ping) request id=0x5562, seq=24230/42590,
8724… 1662.2568209…	192.168.2.102	192.168.1.136	ICMP	60	Echo (ping) request id=0x5562, seq=24486/42591,
8724… 1662.2568218…	192.168.2.102	192.168.1.136	ICMP	60	Echo (ping) request id=0x5562, seq=24742/42592,
8724… 1662.2568228…	192.168.1.136	192.168.2.102	ICMP	42	Echo (ping) reply id=0x5562, seq=23974/42589,
8724… 1662.2568241…	192.168.1.136	192.168.2.102	ICMP	42	Echo (ping) reply id=0x5562, seq=24230/42590,
8724… 1662.2568254…	192.168.1.136	192.168.2.102	ICMP	42	Echo (ping) reply id=0x5562, seq=24486/42591,
8724… 1662.2568266…	192.168.1.136	192.168.2.102	ICMP	42	Echo (ping) reply id=0x5562, seq=24742/42592,

To prevent this, I set up the pfSense firewall rules as below to block all ICMP packets that are coming:

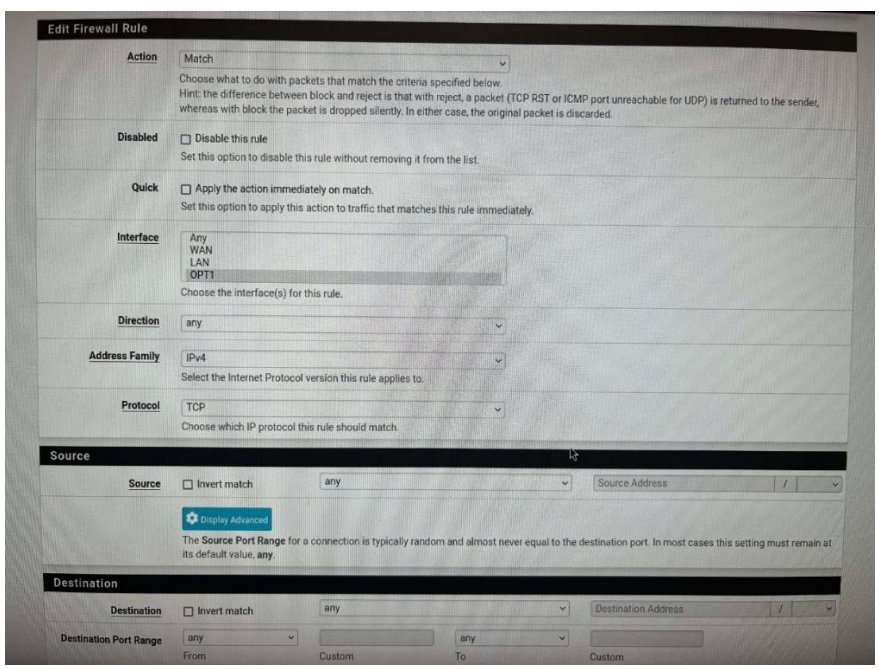


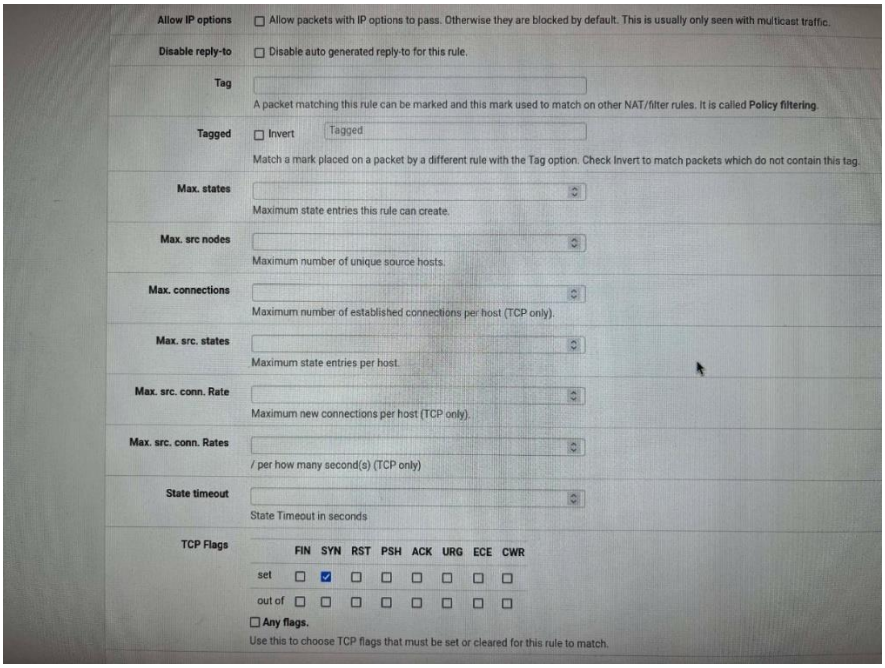
It seems that the firewall rules are working well:

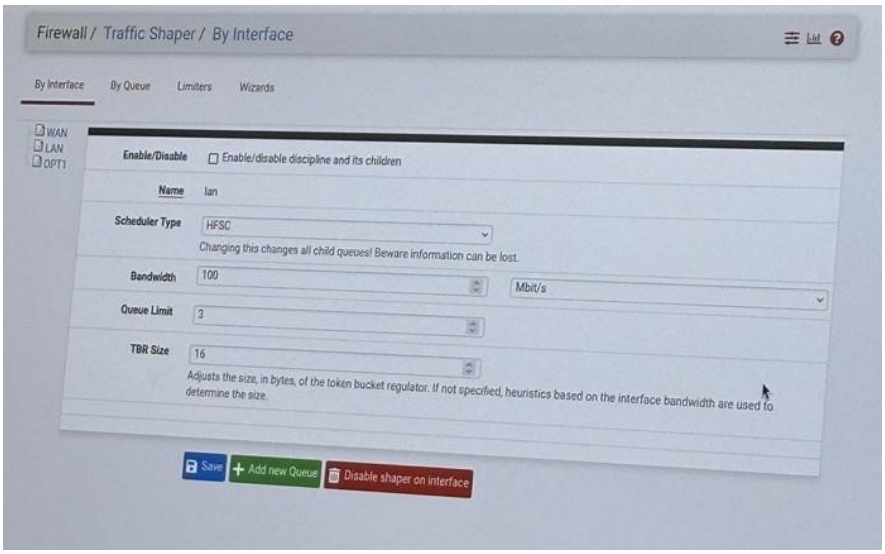


Feb 18 17:29:18	OPT1	(1000002520)	192.168.1.112	192.168.1.136	ICMP
Feb 18 17:29:18	OPT1	(1000002520)	192.168.1.112	192.168.1.136	ICMP
Feb 18 17:29:18	OPT1	(1000002520)	192.168.1.112	192.168.1.136	ICMP
Feb 18 17:29:18	OPT1	(1000002520)	192.168.1.112	192.168.1.136	ICMP
Feb 18 17:29:18	OPT1	(1000002520)	192.168.1.112	192.168.1.136	ICMP
Feb 18 17:29:18	OPT1	(1000002520)	192.168.1.112	192.168.1.136	ICMP
Feb 18 17:29:18	OPT1	(1000002520)	192.168.1.112	192.168.1.136	ICMP
Feb 18 17:29:18	OPT1	(1000002520)	192.168.1.112	192.168.1.136	ICMP
Feb 18 17:29:18	OPT1	(1000002520)	192.168.1.112	192.168.1.136	ICMP
Feb 18 17:29:18	OPT1	(1000002520)	192.168.1.112	192.168.1.136	ICMP
Feb 18 17:29:18	OPT1	(1000002520)	192.168.1.112	192.168.1.136	ICMP
Feb 18 17:29:18	OPT1	(1000002520)	192.168.1.112	192.168.1.136	ICMP
Feb 18 17:29:18	OPT1	(1000002520)	192.168.1.112	192.168.1.136	ICMP
Feb 18 17:29:18	OPT1	(1000002520)	192.168.1.112	192.168.1.136	ICMP
Feb 18 17:29:18	OPT1	(1000002520)	192.168.1.112	192.168.1.136	ICMP
Feb 18 17:29:18	OPT1	(1000002520)	192.168.1.112	192.168.1.136	ICMP
Feb 18 17:29:18	OPT1	(1000002520)	192.168.1.112	192.168.1.136	ICMP
Feb 18 17:29:18	OPT1	(1000002520)	192.168.1.112	192.168.1.136	ICMP
Feb 18 17:29:18	OPT1	(1000002520)	192.168.1.112	192.168.1.136	ICMP
Feb 18 17:29:18	OPT1	(1000002520)	192.168.1.112	192.168.1.136	ICMP
Feb 18 17:29:18	OPT1	(1000002520)	192.168.1.112	192.168.1.136	ICMP
Feb 18 17:29:18	OPT1	(1000002520)	192.168.1.112	192.168.1.136	ICMP
Feb 18 17:29:18	OPT1	(1000002520)	192.168.1.112	192.168.1.136	ICMP
Feb 18 17:29:18	OPT1	(1000002520)	192.168.1.112	192.168.1.136	ICMP

To defend against a SYN flood attack, I changed the firewall rule to limit the SYN rate passing through the network:







In this lab, I learned how basic DDoS works and performs with ICMP and SYN floods. I also know how to perform these kinds of attacks, how to detect them using Wireshark, and how to prevent them with a firewall. Now, I know how to configure a firewall to prevent not only DDOS attack potential but also unknown traffic or traffic from suspected sources.