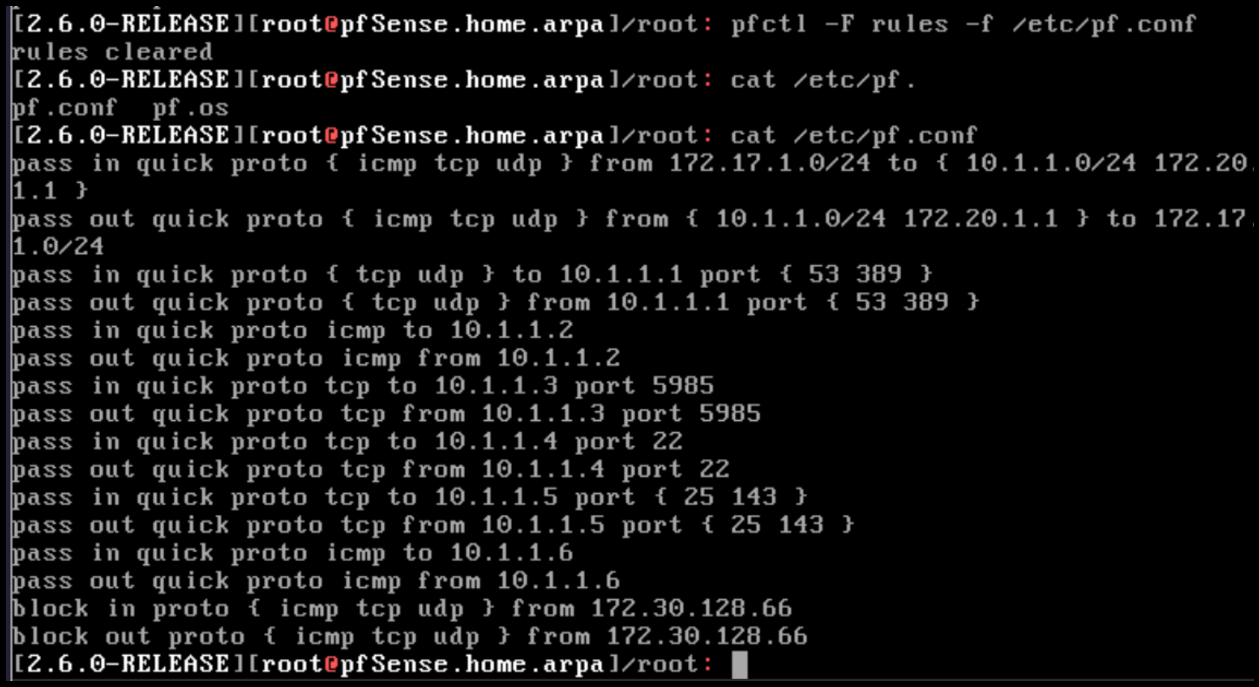
Inject #5: DDOS

MAIL FROM: Team 1 “Club Penguin”
RCPT TO: Circle for the Protection of Antarctica
SUBJECT: DDOS

Hello Circle For The Protection of Antarctica,

Hello we have written a firewall rule to block the incoming DDOS attack. This was written to our PFSense router. The rule can be seen below in the attached screenshot. Our tests suggest that it will work against the attacker’s planned DDOS attack. Thank you for your forewarning of this attack. The warning was valuable for our ability to operate.



```
[2.6.0-RELEASE][root@pfSense.home.arpa]/root: pfctl -F rules -f /etc/pf.conf
rules cleared
[2.6.0-RELEASE][root@pfSense.home.arpa]/root: cat /etc/pf.
pf.conf   pf.os
[2.6.0-RELEASE][root@pfSense.home.arpa]/root: cat /etc/pf.conf
pass in quick proto { icmp tcp udp } from 172.17.1.0/24 to { 10.1.1.0/24 172.20.
1.1 }
pass out quick proto { icmp tcp udp } from { 10.1.1.0/24 172.20.1.1 } to 172.17.
1.0/24
pass in quick proto { tcp udp } to 10.1.1.1 port { 53 389 }
pass out quick proto { tcp udp } from 10.1.1.1 port { 53 389 }
pass in quick proto icmp to 10.1.1.2
pass out quick proto icmp from 10.1.1.2
pass in quick proto tcp to 10.1.1.3 port 5985
pass out quick proto tcp from 10.1.1.3 port 5985
pass in quick proto tcp to 10.1.1.4 port 22
pass out quick proto tcp from 10.1.1.4 port 22
pass in quick proto tcp to 10.1.1.5 port { 25 143 }
pass out quick proto tcp from 10.1.1.5 port { 25 143 }
pass in quick proto icmp to 10.1.1.6
pass out quick proto icmp from 10.1.1.6
block in proto { icmp tcp udp } from 172.30.128.66
block out proto { icmp tcp udp } from 172.30.128.66
[2.6.0-RELEASE][root@pfSense.home.arpa]/root: █
```

Regards,
Team 1 “Club Penguin”