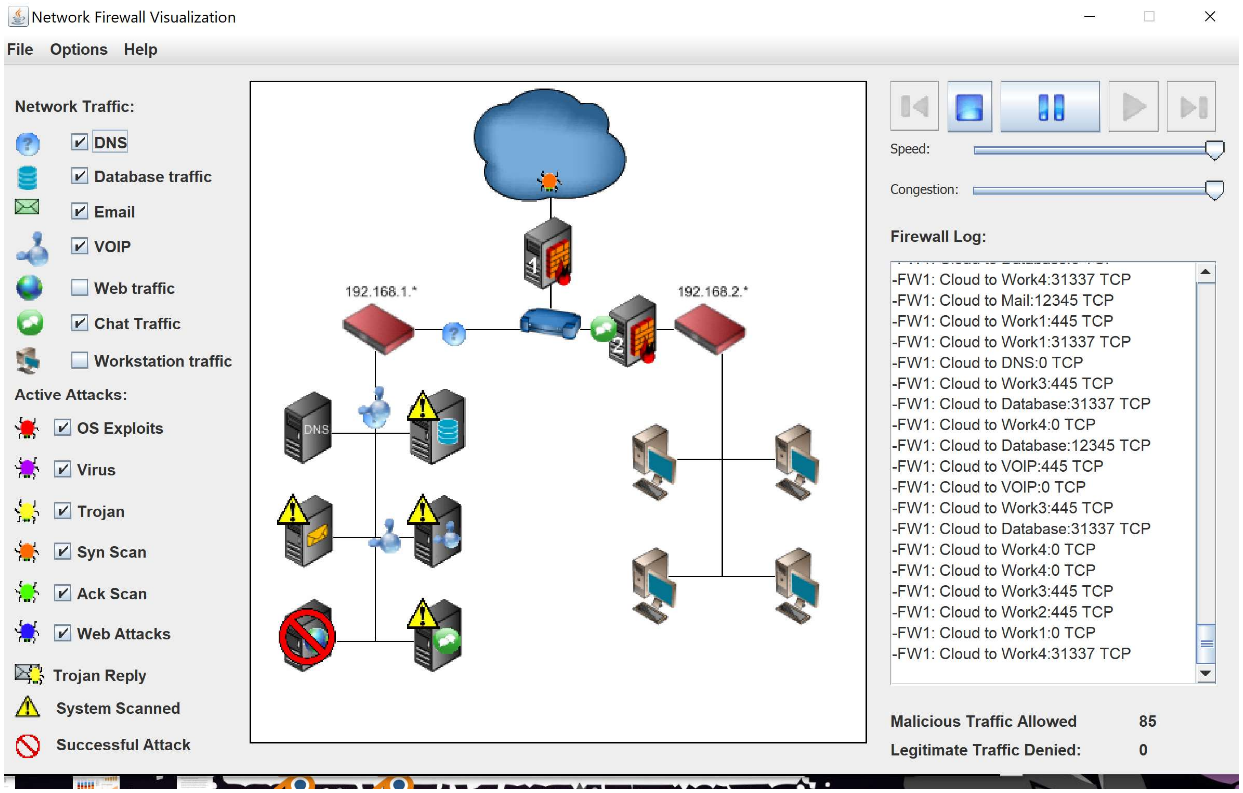
Alex Smetana

12/05/2021

This simulation overall turned out okay. The approach that I went for was to make sure that all legitimate traffic went through, while limiting as much malicious traffic in the process. For the simulation, I made 2 rules for each of the network traffic options. One rule to limit the incoming traffic and another rule to limit the outgoing traffic. I made the rules for each option possible to ensure the best security. For most of my rules I focused on using TCP. Although slower than UDP, I tried to make it as secure as possible. I was not able to measure the speed so I can assume that it would have been slower in comparison to UDP.

The simulation worked very well on DNS, database, email, and chat traffic, barely allowing any malicious software. However, the simulation allowed more malicious traffic was allowed than I would have preferred. Unfortunately, I had to compromise on the web traffic. About 80% of the malicious traffic that was allowed was through web traffic. I was not sure how to tackle the web traffic option without blocking all web traffic all together. Although it let malicious software through, it didn't block any legitimate traffic. Overall, the simulation was very limited, but I made the best that I could.

This is the program after running it after a couple of minutes. It allowed a lot of malicious traffic through the web traffic. Otherwise, the rest of the programs turned out alright, however, eventually would allow malware.



Network Traffic:

☑ DNS
☑ Database traffic
☑ Email
☑ VOIP
☐ Web traffic
☑ Chat Traffic
☐ Workstation traffic

Active Attacks:

☑ OS Exploits
☑ Virus
☑ Trojan
☑ Syn Scan
☑ Ack Scan
☑ Web Attacks

Trojan Reply
System Scanned
Successful Attack

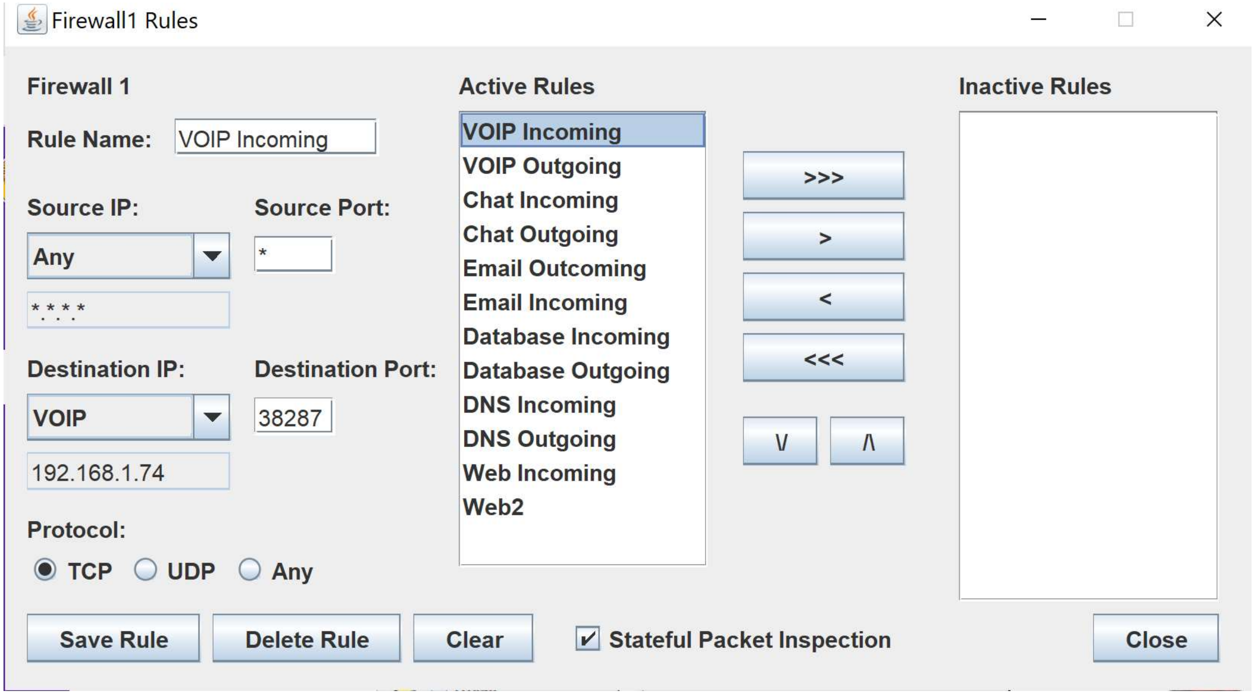
Firewall Log:

```
-FW1: Cloud to Work4:31337 TCP
-FW1: Cloud to Mail:12345 TCP
-FW1: Cloud to Work1:445 TCP
-FW1: Cloud to Work1:31337 TCP
-FW1: Cloud to DNS:0 TCP
-FW1: Cloud to Work3:445 TCP
-FW1: Cloud to Database:31337 TCP
-FW1: Cloud to Work4:0 TCP
-FW1: Cloud to Database:12345 TCP
-FW1: Cloud to VOIP:445 TCP
-FW1: Cloud to VOIP:0 TCP
-FW1: Cloud to Work3:445 TCP
-FW1: Cloud to Database:31337 TCP
-FW1: Cloud to Work4:0 TCP
-FW1: Cloud to Work4:0 TCP
-FW1: Cloud to Work3:445 TCP
-FW1: Cloud to Work2:445 TCP
-FW1: Cloud to Work1:0 TCP
-FW1: Cloud to Work4:31337 TCP
```

Malicious Traffic Allowed 85

Legitimate Traffic Denied: 0

An example of an incoming ruleset. Same format for the rest of the incoming ruleset.



Firewall1 Rules

Firewall 1

Rule Name: VOIP Incoming

Source IP: Any

..*.*

Source Port: *

Destination IP: VOIP

192.168.1.74

Destination Port: 38287

Protocol: ● TCP ○ UDP ○ Any

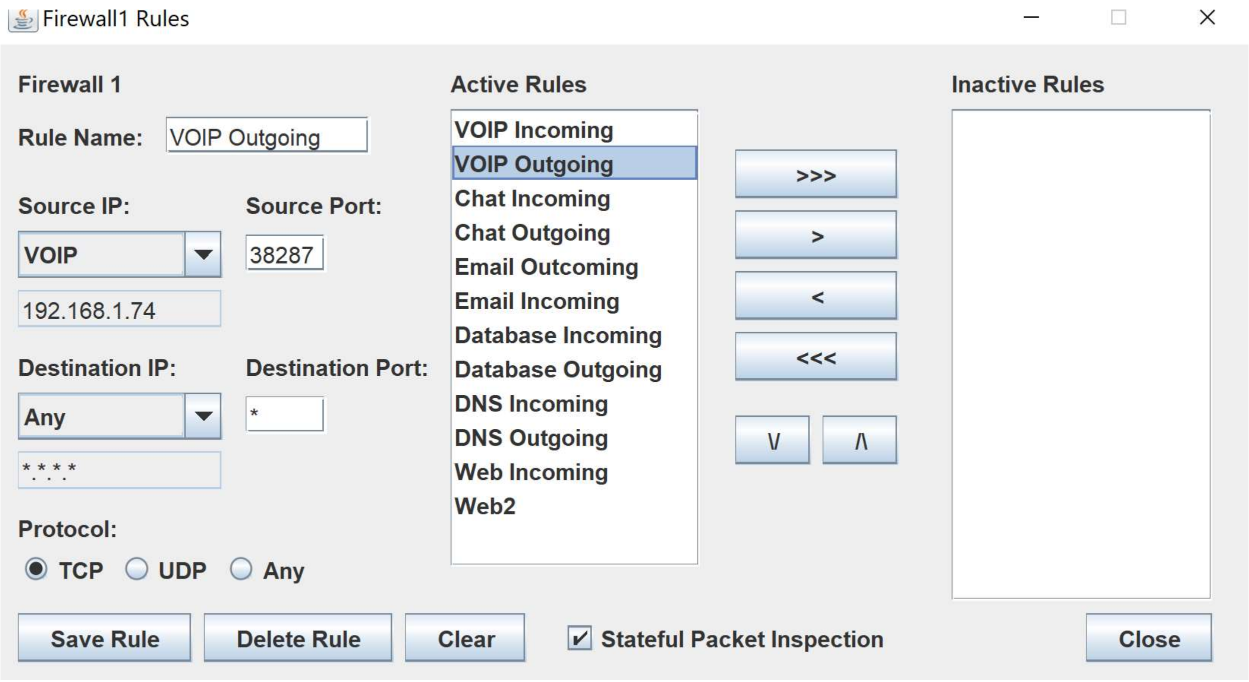
Active Rules

- VOIP Incoming
- VOIP Outgoing
- Chat Incoming
- Chat Outgoing
- Email Outcoming
- Email Incoming
- Database Incoming
- Database Outgoing
- DNS Incoming
- DNS Outgoing
- Web Incoming
- Web2

Inactive Rules

☑ Stateful Packet Inspection

An example of an outgoing ruleset. Same format for the rest of the outgoing rulesets.



Firewall1 Rules

Firewall 1

Rule Name: VOIP Outgoing

Source IP: VOIP

192.168.1.74

Source Port: 38287

Destination IP: Any

..*.*

Destination Port: *

Protocol: ● TCP ○ UDP ○ Any

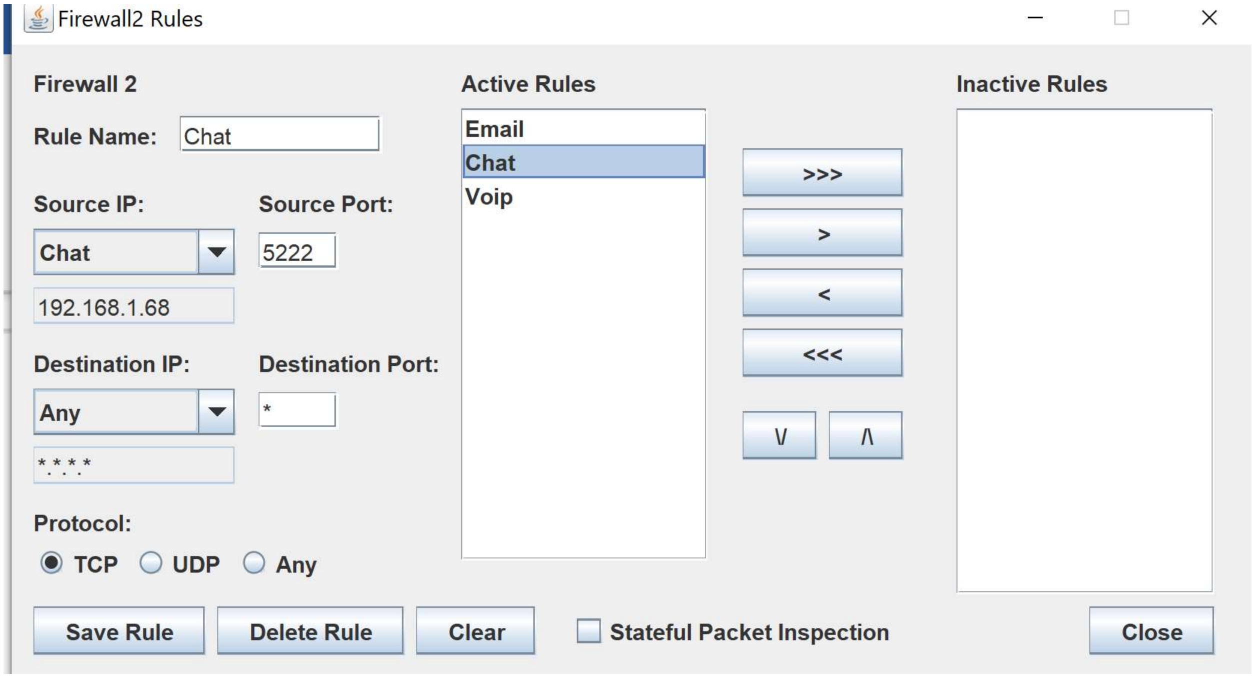
Active Rules

- VOIP Incoming
- VOIP Outgoing
- Chat Incoming
- Chat Outgoing
- Email Outcoming
- Email Incoming
- Database Incoming
- Database Outgoing
- DNS Incoming
- DNS Outgoing
- Web Incoming
- Web2

Inactive Rules

☑ Stateful Packet Inspection

This is Firewall 2s rules. The rest of the rules have the same format. Allows traffic to flow.



Firewall2 Rules

Firewall 2

Rule Name: Chat

Source IP: Chat

192.168.1.68

Source Port: 5222

Destination IP: Any

..*.*

Destination Port: *

Protocol:

● TCP ○ UDP ○ Any

Active Rules

- Email
- Chat
- Voip

Inactive Rules

☐ Stateful Packet Inspection