Network Administration/System Administration (NTU CSIE, Spring 2024) Homework #6 - OPNSense

B12902110 呂承諺

March 31, 2024

Short Answers

1. "Block" drops traffic silently, while "Reject" notifies the client with a TCP RST packet or a UDP ICMP UNREACHABLE packet. "Block" is more suitable on WAN interfaces, so that to external attackers it appears as if there is nothing. "Reject" is more suitable on LAN interfaces, so that clients don't have to wait for timeouts.

   References

   - Rules —OPNsense documentation
   - Transmission Control Protocol - Wikipedia
   - Reject | block What's the difference ? | Netgate Forum

2. The "interface net" refers to the entire subnet of that interface; "interface address" refers to the address of this firewall on that interface. For example, if the LAN address of this firewall is `192.168.1.1/24`, then "LAN net" is `192.168.1.0` to `192.168.1.255`, while "LAN address" is `192.168.1.1`.

   References

   - What is the difference between the interface net and address items in the source/destination dropdowns? : r/PFSENSE

3. A stateful firewall keeps tracks of the state of a connection, such as LISTEN, ESTABLISHED, or CLOSING, which can boost performance and enhance security. On the other hand, a stateless firewall only checks the headers and doesn't track the connection. OPNsense is a stateful firewall.

   References

   - Rules —OPNsense documentation
   - Stateful firewall - Wikipedia

4.

pfSense	OPNsense
Less frequent updates	More frequent updates
More plugins	Less plugins
Apache License 2.0 (Community Edition)	Simplified BSD / FreeBSD License

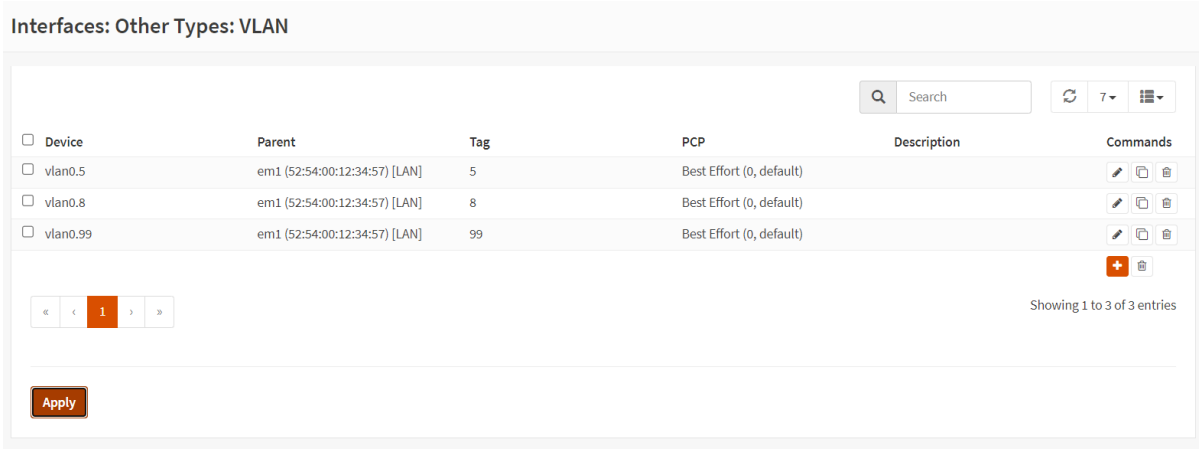
References

- pfSense - Wikipedia
- OPNsense - Wikipedia
- OpnSense vs pfSense: Unveiling the Best Firewall Solution

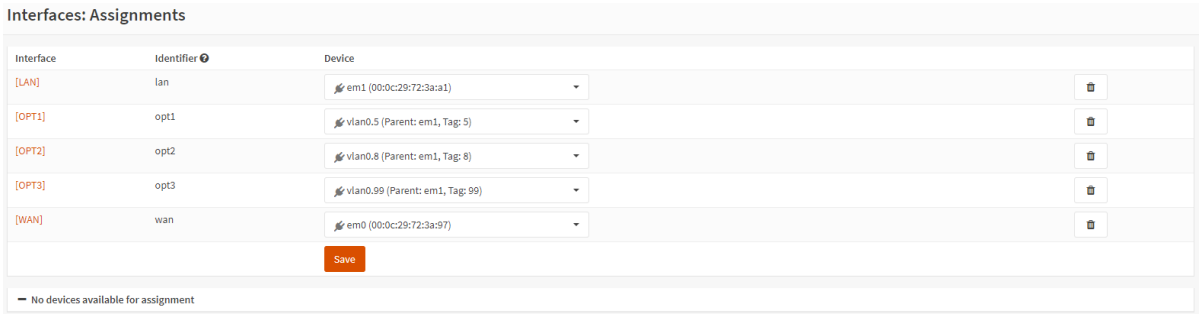
OPNSense

5. **Steps**

   (a) Go to **Interfaces: Other Types: VLAN** and create VLANs 5, 8, and 99.



   (b) Go to **Interfaces: Assignments** and assign VLAN devices to OPT1, OPT2, and and OPT3.



   (c) Go to **Interfaces: [OPT1]**.

      i. Select **Enable Interface**.

      ii. In the **IPv4 Configuration Type** list, select **Static IPv4**.

      iii. In the **IPv4 address** box, `enter 10.5.0.1/24`.

   (d) Repeat step (c) for interfaces OPT2 and OPT3, but use IPv4 addresses `10.8.0.1/24` and `10.99.0.1/24` respectively.

   (e) **Steps**
   Go to **Services: ISC DHCPv4: [OPT1]**.

      i. Select **Enable DHCP server on the OPT1 interface**.

      ii. In the **Range** boxs, enter `10.5.0.2` in the **from** box and `10.5.0.254` in the **to** box.

      iii. in the **DNS servers** boxes, enter `8.8.8.8` and `8.8.4.4`.

   (f) Repeate step (e) for interfaces OPT2 and OPT3, but use ranges `10.8.0.2-10.8.0.254` and `10.99.0.2-10.99.0.254` respectively.

Result

eth0.5

```
localhost:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:BD:21:20
          inet6 addr: fe80::20c:29ff:febd:2120/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:701 errors:0 dropped:0 overruns:0 frame:0
          TX packets:368 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:984155 (961.0 KiB)  TX bytes:24923 (24.3 KiB)

eth0.5    Link encap:Ethernet  HWaddr 00:0C:29:BD:21:20
          inet addr:10.5.0.2  Bcast:0.0.0.0  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:febd:2120/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3 errors:0 dropped:0 overruns:0 frame:0
          TX packets:12 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:698 (698.0 B)  TX bytes:1480 (1.4 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

eth0.8

```
localhost:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:4A:9A:98
          inet6 addr: fe80::20c:29ff:fe4a:9a98/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:696 errors:0 dropped:0 overruns:0 frame:0
          TX packets:356 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:983187 (960.1 KiB)  TX bytes:24117 (23.5 KiB)

eth0.8    Link encap:Ethernet  HWaddr 00:0C:29:4A:9A:98
          inet addr:10.8.0.2  Bcast:0.0.0.0  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe4a:9a98/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:704 (704.0 B)  TX bytes:1200 (1.1 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

eth0.99

```
localhost:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:1D:EA:D5
          inet6 addr: fe80::20c:29ff:fe1d:ead5/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:823 errors:0 dropped:0 overruns:0 frame:0
          TX packets:433 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1001114 (977.6 KiB)  TX bytes:34998 (34.1 KiB)

eth0.99   Link encap:Ethernet  HWaddr 00:0C:29:1D:EA:D5
          inet addr:10.99.0.2  Bcast:0.0.0.0  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe1d:ead5/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:118 errors:0 dropped:0 overruns:0 frame:0
          TX packets:96 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:15023 (14.6 KiB)  TX bytes:12653 (12.3 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:4 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:336 (336.0 B)  TX bytes:336 (336.0 B)
```

cat /etc/resolv.conf:

```
localhost:~# cat /etc/resolv.conf
search b12902110
nameserver 8.8.8.8
nameserver 8.8.4.4
localhost:~# _
```

References

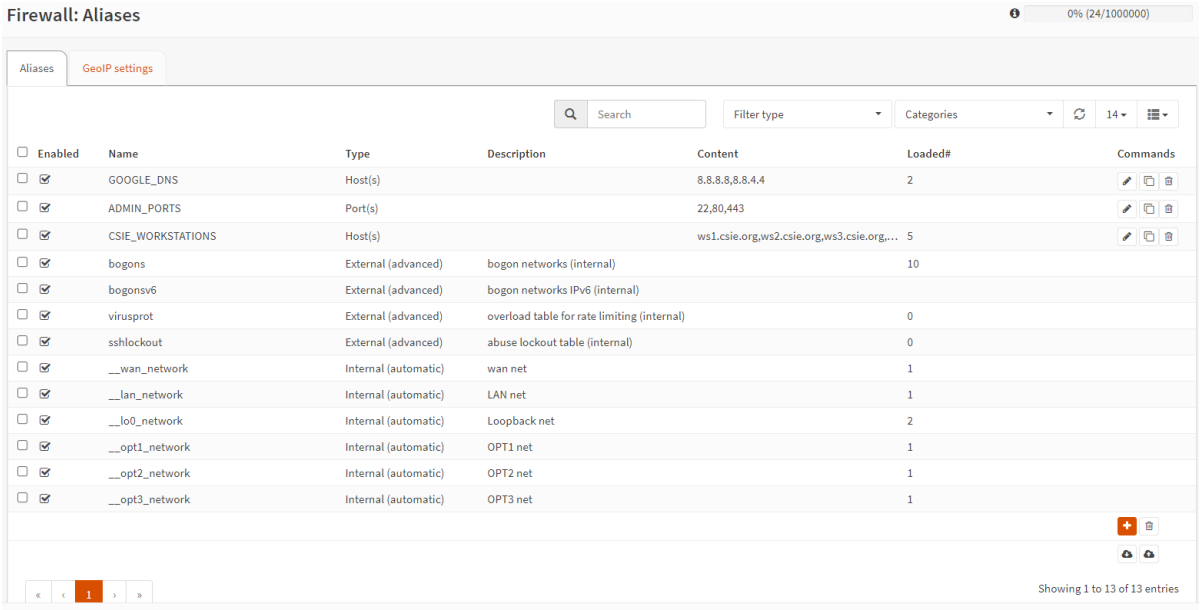
- NASA 2024 OPNsense lab - HackMD

6. **Steps**

   Go to **Firewall: Aliases** and add the aliases.

   - – **Name**: `GOOGLE_DNS`
     – **Type**: Host(s)
     – **Content**: `8.8.8.8`, `8.8.4.4`
   - – **Name**: `ADMIN_PORTS`
     – **Type**: Port(s)
     – **Content**: `22`, `80`, `443`
   - – **Name**: `CSIE_WORKSTATIONS`
     – **Type**: Host(s)
     – **Content**: `ws1.csie.org`, `ws2.csie.org`, `ws3.csie.org`, `ws4.csie.org`, `ws5.csie.org`

   Result



References

- Aliases —OPNsense documentation

7. **Steps**

   Go to **System: Settings: Administration**.

   (a) Select **Enable Secure Shell**.

   (b) Select **Permit root user login**.

   (c) Select **Permit password login**.

   (d) In the **Listen Interfaces** list, select **WAN** and **OPT3**.

   Result

```
localhost:~# ssh 10.5.0.1
ssh: connect to host 10.5.0.1 port 22: Operation timed out
localhost:~# _
```

```
localhost:~# ssh 10.8.0.1
ssh: connect to host 10.8.0.1 port 22: Operation timed out
localhost:~# _
```

8. **Steps**

   Go to **Firewall: Rules: OPT3** and add the following rules. (Note: Traffic from OPT1 and OPT2 are blocked by default.)

   - – **Action**: Pass
     – **Interface**: OPT3
     – **Direction**: in
     – **TCP/IP Version**: IPv4
     – **Protocol**: any
     – **Source**: any
     – **Destination**: GOOGLE_DNS
   - – **Action**: Pass
     – **Interface**: OPT3
     – **Direction**: in
     – **TCP/IP Version**: IPv4
     – **Protocol**: any
     – **Source**: any
     – **Destination**: CSIE_WORKSTATIONS
   - – **Action**: Pass
     – **Interface**: OPT3
     – **Direction**: in
     – **TCP/IP Version**: IPv4
     – **Protocol**: TCP
     – **Source**: any
     – **Destination**: This Firewall
     – **Destination port range**: from: ADMIN_PORTS, to: ADMIN_ports

Result

```
localhost:~# ping 8.8.8.8 -c 2
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: seq=0 ttl=113 time=39.676 ms
64 bytes from 8.8.8.8: seq=1 ttl=113 time=52.271 ms

--- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 39.676/45.973/52.271 ms
localhost:~# traceroute ws1.csie.org
traceroute to ws1.csie.org (140.112.30.186), 30 hops max, 46 byte packets
 1  10.99.0.1 (10.99.0.1)  0.636 ms  0.838 ms  0.436 ms
 2  192.168.84.223 (192.168.84.223)  3.577 ms  5.689 ms  4.498 ms
 3  *  *  *
 4  10.54.148.210 (10.54.148.210)  51.334 ms  52.046 ms  42.760 ms
 5  10.254.66.123 (10.254.66.123)  39.141 ms  51.625 ms  60.038 ms
 6  *  *  *
 7  60-199-4-169.static.tfn.net.tw (60.199.4.169)  40.778 ms  58.316 ms  60-199-4-165.static.tfn.net.tw (60.199.4.165)  45.034 ms
 8  60-199-3-194.static.tfn.net.tw (60.199.3.194)  60.106 ms  36.549 ms  41.916 ms
 9  60-199-14-49.static.tfn.net.tw (60.199.14.49)  36.500 ms  60-199-14-97.static.tfn.net.tw (60.199.14.97)  34.588 ms  60-199-14-49.static.tfn.net.tw (60.199.1
4.49)  49.070 ms
10  211-78-221-26.static.tfn.net.tw (211.78.221.26)  63.513 ms  40.817 ms  51.936 ms
11  wan0069.cc.ntu.edu.tw (140.112.0.69)  33.981 ms  42.006 ms  37.624 ms
12  core_wan_0201.cc.ntu.edu.tw (140.112.0.201)  47.871 ms  39.277 ms  44.808 ms
13  140.112.0.237 (140.112.0.237)  57.417 ms  140.112.0.217 (140.112.0.217)  46.496 ms  140.112.0.237 (140.112.0.237)  126.920 ms
14  140.112.149.122 (140.112.149.122)  79.734 ms  39.397 ms  41.164 ms
15  ws1.csie.ntu.edu.tw (140.112.30.186)  40.035 ms  52.323 ms  47.091 ms
localhost:~# _
```

```
localhost:~# ssh 10.99.0.1
The authenticity of host '10.99.0.1 (10.99.0.1)' can't be established.
ED25519 key fingerprint is SHA256:ptBEIpRCnKlg0BHk5YcQN5IIKH9JEzmHVBDKW1TzIUY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.99.0.1' (ED25519) to the list of known hosts.
(root@10.99.0.1) Password:
Last login: Sun Mar 31 17:21:34 2024
-------------------------------------------------
|      Hello, this is OPNsense 24.1             |         @@@@@@@@@@@@@@@@
|                                               |       @@@@         @@@@
| Website:      https://opnsense.org/           |         @@@\\\   ///@@@
| Handbook:     https://docs.opnsense.org/      |       )))))))   (((((((
| Forums:       https://forum.opnsense.org/     |         @@@///   \\\@@@
| Code:         https://github.com/opnsense     |       @@@@         @@@@
| Twitter:      https://twitter.com/opnsense    |         @@@@@@@@@@@@@@@@
-------------------------------------------------

*** OPNsense.b12902110: OPNsense 24.1 ***

 LAN (em1)       -> v4: 192.168.1.1/24
 OPT1 (vlan0.5)  -> v4: 10.5.0.1/24
 OPT2 (vlan0.8)  -> v4: 10.8.0.1/24
 OPT3 (vlan0.99) -> v4: 10.99.0.1/24
 WAN (em0)       -> v4/DHCP4: 192.168.84.120/24
                    v6/DHCP6: 2402:7500:586:55b5:20c:29ff:fe72:3a97/64

 HTTPS: SHA256 FB 64 B2 6C 53 0C 67 56 21 C9 EF 65 F7 3B 8C 69
               81 57 C9 82 EA 85 F9 5E 68 25 FA 54 AC 66 DA CF
 SSH:   SHA256 kt202w5ePb3Ch8tUhLq9oYlSm4vPFpvsLRGRZGwLeJ8 (ECDSA)
 SSH:   SHA256 ptBEIpRCnKlg0BHk5YcQN5IIKH9JEzmHVBDKW1TzIUY (ED25519)
 SSH:   SHA256 LZqLPGo0HtDk3hU4Ph8c63+PEE+j/yPLYt+KySfchks (RSA)

  0) Logout                              7) Ping host
  1) Assign interfaces                   8) Shell
  2) Set interface IP address            9) pfTop
  3) Reset the root password            10) Firewall log
  4) Reset to factory defaults          11) Reload all services
  5) Power off system                   12) Update from console
  6) Reboot system                      13) Restore a backup

Enter an option:
```

References

- B12902040 黃昱翔

9. **Steps**

   (a) Go to **Firewall: Rules: OPT1** and add the following rule.

   - **Action**: Pass
   - **Interface**: OPT1
   - **Direction**: in
   - **TCP/IP Version**: IPv4
   - **Protocol**: ICMP
   - **ICMP type**: any
   - **Source**: OPT1 net
   - **Destination**: OPT2 net

   (b) Go to **Firewall: Rules: OPT2** and add the following rules.

   - – **Action**: Pass
     – **Interface**: OPT2
     – **Direction**: in
     – **TCP/IP Version**: IPv4
     – **Protocol**: ICMP
     – **ICMP type**: Echo Reply
     – **Source**: OPT2 net
     – **Destination**: OPT1 net
   - – **Action**: Block
     – **Interface**: OPT2
     – **Direction**: in
     – **TCP/IP Version**: IPv4
     – **Protocol**: ICMP
     – **ICMP type**: Echo Request
     – **Source**: OPT2 net
     – **Destination**: OPT1 net

Result

On `10.5.0.2`, ping `10.8.0.2`:

```
localhost:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 00:0c:29:bd:21:20 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::20c:29ff:febd:2120/64 scope link
       valid_lft forever preferred_lft forever
3: eth0.5@eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP qlen 1000
    link/ether 00:0c:29:bd:21:20 brd ff:ff:ff:ff:ff:ff
    inet 10.5.0.2/24 scope global eth0.5
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:febd:2120/64 scope link
       valid_lft forever preferred_lft forever
localhost:~# ping 10.8.0.2 -c 4
PING 10.8.0.2 (10.8.0.2): 56 data bytes
64 bytes from 10.8.0.2: seq=0 ttl=63 time=1.341 ms
64 bytes from 10.8.0.2: seq=1 ttl=63 time=1.098 ms
64 bytes from 10.8.0.2: seq=2 ttl=63 time=1.299 ms
64 bytes from 10.8.0.2: seq=3 ttl=63 time=1.523 ms

--- 10.8.0.2 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 1.098/1.315/1.523 ms
localhost:~# _
```

On `10.8.0.2`, ping `10.5.0.2`:

```
localhost:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 00:0c:29:4a:9a:98 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::20c:29ff:fe4a:9a98/64 scope link
       valid_lft forever preferred_lft forever
3: eth0.8@eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP qlen 1000
    link/ether 00:0c:29:4a:9a:98 brd ff:ff:ff:ff:ff:ff
    inet 10.8.0.2/24 scope global eth0.8
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe4a:9a98/64 scope link
       valid_lft forever preferred_lft forever
localhost:~# ping 10.5.0.2 -c 4
PING 10.5.0.2 (10.5.0.2): 56 data bytes

--- 10.5.0.2 ping statistics ---
4 packets transmitted, 0 packets received, 100% packet loss
localhost:~# _
```

10. **Steps**

    - Go to **Firewall: Settings: Schedules** and add the folowing schedule.
      - **Name**: 2024-03-14
      - **Month**: March_24
      - **Day**: 14
      - **Time**: Start time: 0:00, Stop time: 23:59
    - Go to **Firewall: Rules: OPT1** and add the following rule as the first rule.
      - **Action**: Block
      - **Interface**: OPT1
      - **Direction**: in
      - **TCP/IP Version**: IPv4+IPv6
      - **Protocol**: any
      - **Source**: any
      - **Destination**: any
      - **Schedule**: 2024-03-14

11. **Observations**

- The graph's y-axis scales automatically according to the maximum value during the time span.
- The graph samples data at regular intervals, and the data seems to be the average over a few seconds.
- Each interface is represented with a different color.

Steps

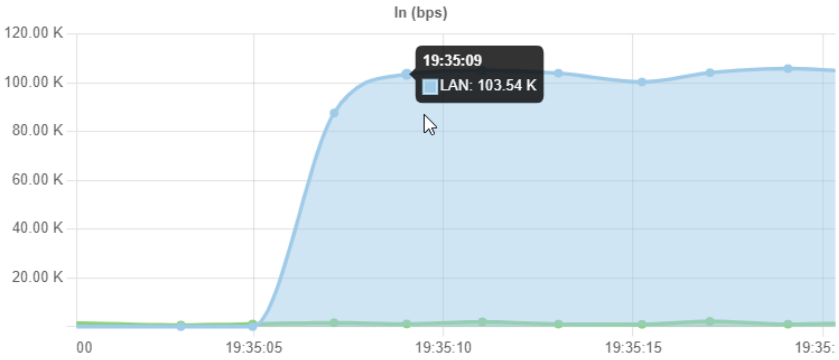
- Install:

```
apk add hping3 --update-cache --repository \
  http://dl-cdn.alpinelinux.org/alpine/edge/testing
```

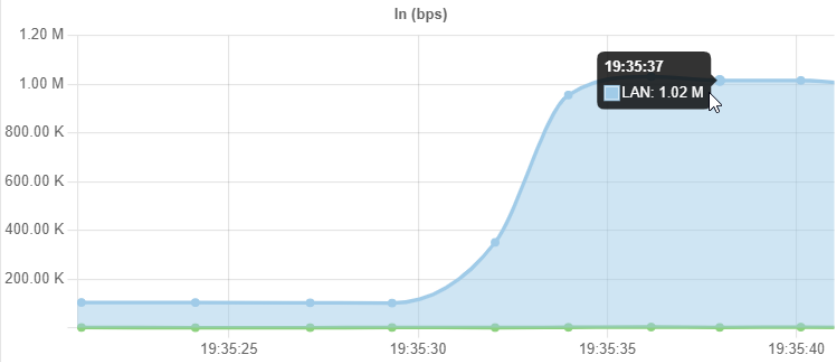
- 100kbps: `hping3 -d 1250 -i u100000 192.168.1.1`
- 1Mbps: `hping3 -d 12500 -i u100000 192.168.1.1`
- 10Mbps: `hping3 -d 15000 -i u10000 192.168.1.1`
- 50Mbps: `hping3 -d 50000 -i u5000 192.168.1.1`

Result

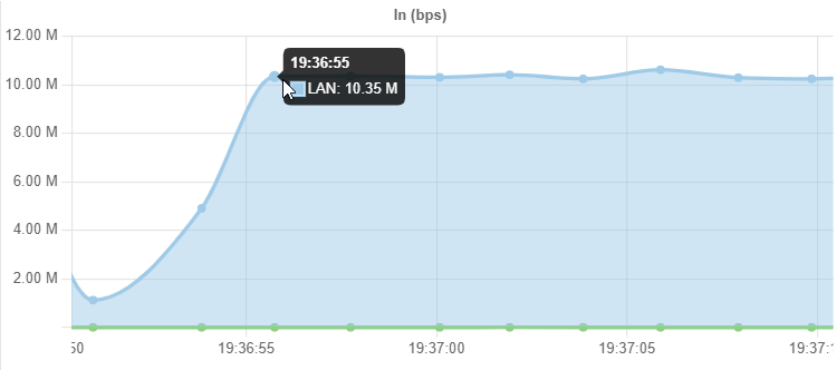
100kbps:



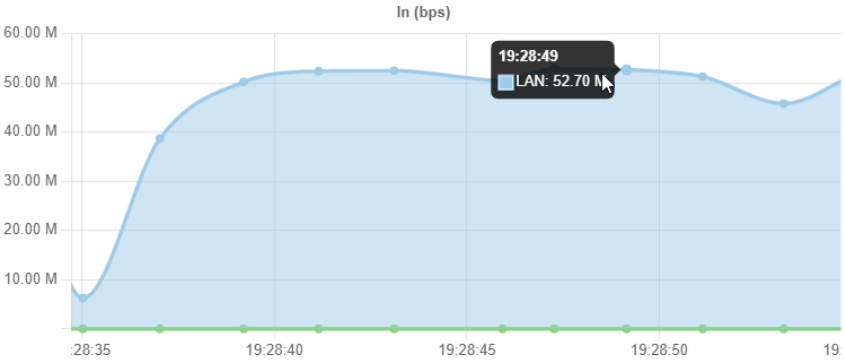
1Mbps:



10Mbps:



50Mbps:



References

- Alpine Linux packages - hping3
- software installation - Alpine Linux unable to install hping; ERROR: unsatisfiable constraints - Unix & Linux Stack Exchange
- hping3(8) - Linux man page
- Reporting: Traffic —OPNsense documentation
- Know about hping3 linux tool. hping3 is a network tool that can be⋯| by Jyothi | Medium