Firefox

https://192.168.50.1/firewall_rules_edit.php?id=0

Kali Linux 🐉 Kali Tools 📖 Kali Docs 🐉 Kali Forums 🐉 Kali NetHunter 🔴 Exploit-DB 🔴 Google Hacking DB 🔴 OffSec 🐍 Online Python Compil... ⚡ Online Python Compil...

Firewall / Rules / Edit

Edit Firewall Rule

Action

Pass

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

Address or Alias

192.168.60.101   /

⚙ 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

Address or Alias

192.168.50.101   /

Destination Port Range

any

any

Firewall / Rules / Edit

Edit Firewall Rule

Action
Pass

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
LAN2

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   Address or Alias   192.168.50.101   /

⚙ 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   Address or Alias   192.168.60.100   /

Destination Port Range
any | Custom | any | Custom
From   To

```
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default 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 noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN group default qlen 1000
    link/ether 08:00:27:d2:ce:6d brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:c5:2c:e7 brd ff:ff:ff:ff:ff:ff
    inet 192.168.60.100/24 brd 192.168.60.255 scope global noprefixroute eth1
       valid_lft forever preferred_lft forever
    inet6 fe80::824f:55da:c2da:4a80/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
4: eth2: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN group default qlen 1000
    link/ether 08:00:27:ac:e9:2a brd ff:ff:ff:ff:ff:ff

┌──(kali㉿kali)-[~]
└─$ ping 192.168.50.101
PING 192.168.50.101 (192.168.50.101) 56(84) bytes of data.
64 bytes from 192.168.50.101: icmp_seq=1 ttl=63 time=2.52 ms
64 bytes from 192.168.50.101: icmp_seq=2 ttl=63 time=1.72 ms
64 bytes from 192.168.50.101: icmp_seq=3 ttl=63 time=1.69 ms
64 bytes from 192.168.50.101: icmp_seq=4 ttl=63 time=1.95 ms
^C
── 192.168.50.101 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
rtt min/avg/max/mdev = 1.691/1.969/2.517/0.331 ms
```

File   Macchina   Visualizza   Inserimento   Dispositivi   Aiuto

Pfsense.home.arpa - Fire...

https://192.168.50.1/firewall_rules_edit.php?id=4

Kali Linux   Kali Tools   Kali Docs   Kali Forums   Kali NetHunter   Exploit-DB   Google Hacking DB   OffSec   Online Python Compil...   Online Python Compil...

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
LAN2

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   Address or Alias   192.168.50.101   /

⚙ 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   Address or Alias   192.168.60.100   /

Destination Port Range   any   any

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
Address or Alias
192.168.60.101 /

⚙ 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**.

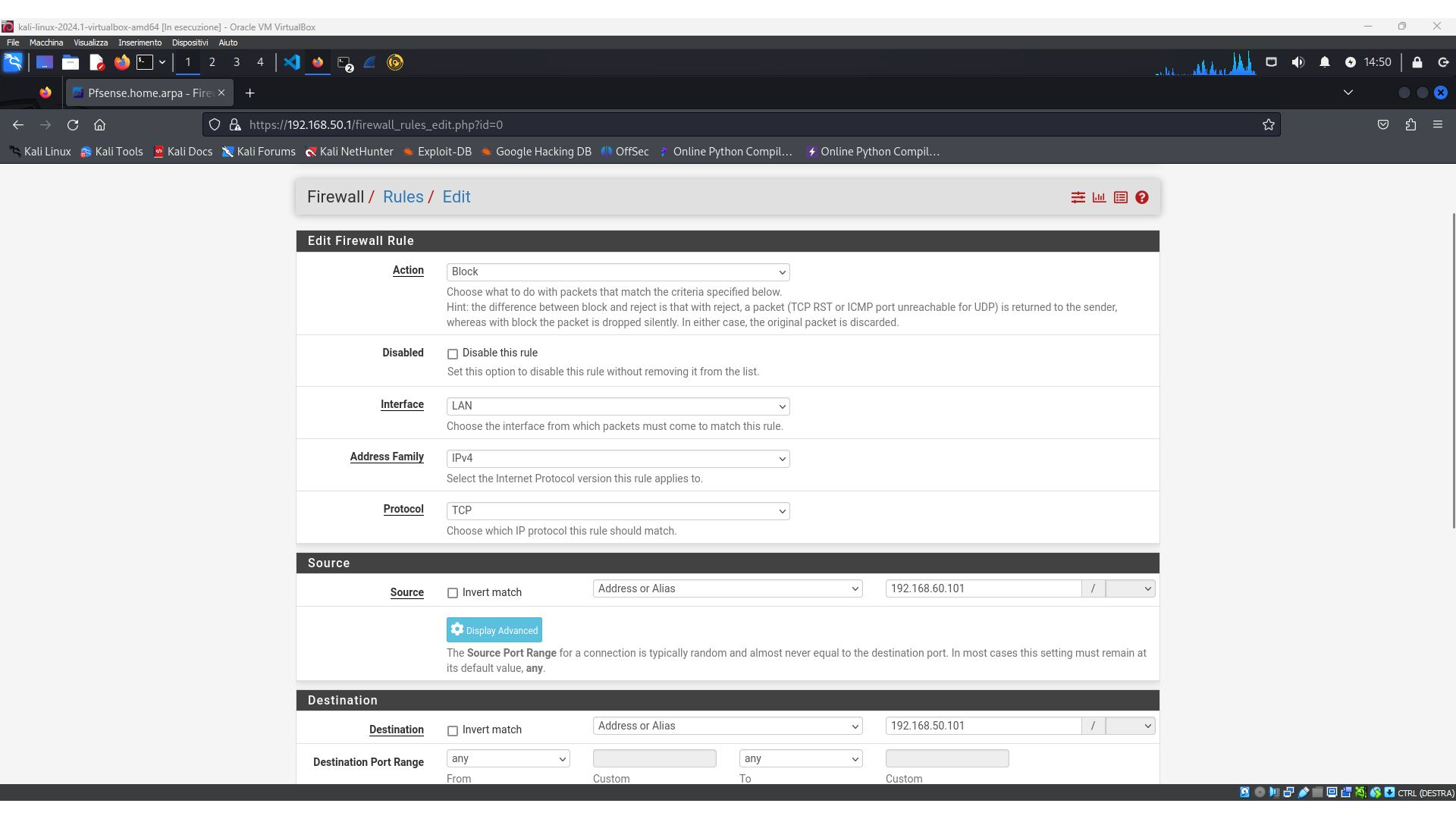## Destination

Destination
☐ Invert match
Address or Alias
192.168.50.101 /

Destination Port Range
any   any
From   Custom   To   Custom

```
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default 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 noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN group default qlen 1000
    link/ether 08:00:27:d2:ce:6d brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:c5:2c:e7 brd ff:ff:ff:ff:ff:ff
    inet 192.168.60.100/24 brd 192.168.60.255 scope global noprefixroute eth1
        valid_lft forever preferred_lft forever
    inet6 fe80::824f:55da:c2da:4a80/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
4: eth2: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN group default qlen 1000
    link/ether 08:00:27:ac:e9:2a brd ff:ff:ff:ff:ff:ff

┌──(kali㉿kali)-[~]
└─$ ping 192.168.50.101
PING 192.168.50.101 (192.168.50.101) 56(84) bytes of data.
^C
── 192.168.50.101 ping statistics ──
206 packets transmitted, 0 received, 100% packet loss, time 209788ms
```