How to use the VoipNow built-in firewall

Applies to VoipNow 3.5!

Starting with VoipNow 3.5, a built-in firewall is delivered at installation time. It provides a quick and easy way to restrict access to your server using the iptables tool.

Step-by-step guide

Once VoipNow is installed, a firewall script is delivered. It will automatically detect the roles running on your node and apply only the corresponding access rules. The script also contains a built-in safety feature to ensure you don't lose access to your server.

Firewall installation

1. (optional) Edit /etc/voipnow/local.conf and uncomment the TRUSTED_NET variable, replacing its value with your local network IP and netmask: iptabl

```
# Access from these networks is always allowed (eg: TRUSTED_NET 10.10.34.12/32 10.10.33.1/24)
# TRUSTED_NET NETWORK/MASK
```

2. It should be changed into something similar to:

```
# Access from these networks is always allowed (eg: TRUSTED_NET 10.10.34.12/32 10.10.33.1/24)
TRUSTED_NET 172.16.100.1/24
```

3. Log in to your server and execute the following script: /usr/local/voipnow/admin/sbin/voipnow_firewall

Output sample

```
[root@centos6 ~]# /usr/local/voipnow/admin/sbin/voipnow_firewall

Starting VoipNow firewall configuration...

Your existing firewall has been saved in /tmp/iptables.20650

Firewall has been generated and will be cleared in 10 minutes to avoid being locked out in case something went
wrong.

The new rules have been saved into /etc/sysconfig/iptables and will be applied at system boot.

If everything is correct, please remove the cron job by running:

/root/core/shell/voipnow_firewall ok
```

Outcome

The script will:

- save your existing firewall rules to a temporary file (`/tmp/iptables.20650` in the above example);
- inspect the MySQL database for roles assigned to this role;
- attempt to detect ports used by each role and apply the corresponding firewall rules;
- install a "safety net" consisting of a cron job which does a firewall flush after 10 minutes.

```
*/10    *       *       *       *       /sbin/iptables -P INPUT ACCEPT; /sbin/iptables -P FORWARD ACCEPT;/sbin
/iptables -P OUTPUT ACCEPT;/sbin/iptables -F;/sbin/iptables -X
```

If everything is okay, you need to run again the firewall script with the ok parameter. This will remove the cron job and leave your newly generated firewall rules in place):

```
[root@centos6 ~]# /usr/local/voipnow/admin/sbin/voipnow_firewall ok

Script called with ok option - removing safety net
```

To ensure that the cron job was removed, use crontab -l as root.

A standard VoipNow node having all roles installed will generate a firewall as below:

```
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
   69  7615 bad_tcp    all  --  *      *       0.0.0.0/0            0.0.0.0/0
   69  7615 voipnow_in  all  --  *      *       0.0.0.0/0            0.0.0.0/0
   49  4885 misc_in    all  --  *      *       0.0.0.0/0            0.0.0.0/0
   45  4337 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0           ctstate RELATED,
ESTABLISHED
    0     0 ACCEPT     all  --  *      *       127.0.0.0/8          127.0.0.0/8
    0     0 ACCEPT     all  --  lo     *       0.0.0.0/0            0.0.0.0/0
    0     0 DROP       all  --  *      *       0.0.0.0/0            0.0.0.0/0
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
Chain OUTPUT (policy ACCEPT 23 packets, 10088 bytes)
 pkts bytes target     prot opt in     out     source               destination
   12  1087 ACCEPT     all  --  *      *       127.0.0.0/8          127.0.0.0/8
   24  4052 ACCEPT     all  --  *      lo      0.0.0.0/0            0.0.0.0/0
Chain bad_tcp (1 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       all  --  *      *       0.0.0.0/0            0.0.0.0/0           ctstate INVALID
    0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:!0x17/0x02
ctstate NEW
    0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x3F/0x3F
    0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x3F/0x00
    0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x16/0x00
    0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x29/0x29
    0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x03/0x03
    0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x06/0x06
    0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x05/0x05
    0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x11/0x01
    0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x18/0x08
    0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x30/0x20
    0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x3F/0x00
    0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x06/0x06
    0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x3F/0x29
    0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x3F/0x37
    0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x3F/0x3F
    0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x3F/0x29
    0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x3F/0x00
Chain misc_in (1 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            0.0.0.0/0           icmp type 8
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            0.0.0.0/0           icmp type 0
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            0.0.0.0/0           icmp type 3
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            0.0.0.0/0           icmp type 11
    0     0 DROP       icmp --  *      *       0.0.0.0/0            0.0.0.0/0           icmp type 17
    0     0 DROP       icmp --  *      *       0.0.0.0/0            0.0.0.0/0           icmp type 13
    4   548 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spt:53 dpts:1024:
65535 ctstate RELATED,ESTABLISHED
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:53 dpts:1024:
65535 ctstate RELATED,ESTABLISHED
Chain misc_out (0 references)
 pkts bytes target     prot opt in     out     source               destination
Chain voipnow_in (1 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22 ctstate NEW
    8   716 ACCEPT     tcp  --  lo     *       0.0.0.0/0            0.0.0.0/0           tcp dpt:11211
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:80 ctstate NEW
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:443 ctstate NEW
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:443 ctstate NEW
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:80 ctstate NEW
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:5222 ctstate NEW
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:5269 ctstate NEW
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:5280 ctstate NEW
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:25 ctstate NEW
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:5050 ctstate NEW
    0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpts:10000:20000
ctstate NEW
   12  2014 ACCEPT     tcp  --  lo     *       0.0.0.0/0            0.0.0.0/0           tcp dpt:5672
```

```
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:5060 ctstate NEW
    0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:5060 ctstate NEW
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:5061 ctstate NEW
    0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:5061 ctstate NEW
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:3306 ctstate NEW
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:9200 ctstate NEW
    0     0 ACCEPT     tcp  --  lo     *       0.0.0.0/0            0.0.0.0/0           tcp dpt:10000
Chain voipnow_out (0 references)
 pkts bytes target     prot opt in     out     source               destination
```

If you have trouble running the script, you can pass it the debug argument which will show the script actions in detail and will not apply any firewall rules (they'll only be printed).

Debug output sample

```
[root@centos6 ~]# /usr/local/voipnow/admin/sbin/voipnow_firewall debug
Detected Asterisk SIP port: 5050
Detected Asterisk RTP ports: 10000 20000
Detected Asterisk UDPTL ports: 4000 5999
Detected Jabber ports: 5222 5269 5280
Detected Kamailio ports: 5060 5061
Detected Elasticsearch ports: 9200
Detected HTTP port: 80
Detected Hubring port: 11211
Detected RabbitMQ port: 5672
Detected SMTP port: 25
SSH port not detected, defaulting to 22
Detected SSL port: 443
Detected worker port: 10000
Starting VoipNow firewall configuration...
Your existing firewall has been saved in /tmp/iptables.29129
Calling chain_create()
Calling create_chains()
Calling allow_trusted()
Calling reset_policy()
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
Not calling safety_net() as we're in debug mode
Calling add_chains()
iptables -A INPUT -j bad_tcp
iptables -A INPUT -j voipnow_in
iptables -A INPUT -j misc_in
Calling set_global()
iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -s 127.0.0.0/8 -d 127.0.0.0/8 -j ACCEPT
iptables -A OUTPUT -s 127.0.0.0/8 -d 127.0.0.0/8 -j ACCEPT
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT
Calling enable_icmp
iptables -A misc_in -p icmp -m icmp --icmp-type echo-request -j ACCEPT
iptables -A misc_in -p icmp -m icmp --icmp-type echo-reply -j ACCEPT
iptables -A misc_in -p icmp -m icmp --icmp-type destination-unreachable -j ACCEPT
iptables -A misc_in -p icmp -m icmp --icmp-type time-exceeded -j ACCEPT
iptables -A misc_in -p icmp -m icmp --icmp-type address-mask-request -j DROP
iptables -A misc_in -p icmp -m icmp --icmp-type timestamp-request -j DROP
Calling enable_dns
iptables -A misc_in -p udp --sport 53 --dport 1024:65535 -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
iptables -A misc_in -p tcp --sport 53 --dport 1024:65535 -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
Calling enable_ssh
iptables -A voipnow_in -p tcp --dport 22 -m conntrack --ctstate NEW -j ACCEPT
Calling enable_bad_tcp
iptables -A bad_tcp -m conntrack --ctstate INVALID -j DROP
iptables -A bad_tcp -p tcp ! --syn -m conntrack --ctstate NEW -j DROP
iptables -A bad_tcp -p tcp --tcp-flags ALL ALL -j DROP
iptables -A bad_tcp -p tcp --tcp-flags ALL NONE -j DROP
iptables -A bad_tcp -p tcp -m tcp --tcp-flags SYN,RST,ACK NONE -j DROP
iptables -A bad_tcp -p tcp -m tcp --tcp-flags FIN,PSH,URG FIN,PSH,URG -j DROP
iptables -A bad_tcp -p tcp -m tcp --tcp-flags FIN,SYN FIN,SYN -j DROP
```

```
iptables -A bad_tcp -p tcp -m tcp --tcp-flags SYN,RST SYN,RST -j DROP
iptables -A bad_tcp -p tcp -m tcp --tcp-flags FIN,RST FIN,RST -j DROP
iptables -A bad_tcp -p tcp -m tcp --tcp-flags FIN,ACK FIN -j DROP
iptables -A bad_tcp -p tcp -m tcp --tcp-flags PSH,ACK PSH -j DROP
iptables -A bad_tcp -p tcp -m tcp --tcp-flags ACK,URG URG -j DROP
iptables -A bad_tcp -p tcp -m tcp --tcp-flags FIN,SYN,RST,PSH,ACK,URG NONE -j DROP
iptables -A bad_tcp -p tcp -m tcp --tcp-flags SYN,RST SYN,RST -j DROP
iptables -A bad_tcp -p tcp -m tcp --tcp-flags FIN,SYN,RST,PSH,ACK,URG FIN,PSH,URG -j DROP
iptables -A bad_tcp -p tcp -m tcp --tcp-flags FIN,SYN,RST,PSH,ACK,URG FIN,SYN,RST,ACK,URG -j DROP
iptables -A bad_tcp -p tcp -m tcp --tcp-flags FIN,SYN,RST,PSH,ACK,URG FIN,SYN,RST,PSH,ACK,URG -j DROP
iptables -A bad_tcp -p tcp -m tcp --tcp-flags FIN,SYN,RST,PSH,ACK,URG FIN,PSH,URG -j DROP
iptables -A bad_tcp -p tcp -m tcp --tcp-flags FIN,SYN,RST,PSH,ACK,URG NONE -j DROP
Calling enable_dd
iptables -A voipnow_in -i lo -p tcp -m tcp --dport 11211 -j ACCEPT
Calling enable_http
iptables -A voipnow_in -p tcp --dport 80 -m conntrack --ctstate NEW -j ACCEPT
iptables -A voipnow_in -p tcp --dport 443 -m conntrack --ctstate NEW -j ACCEPT
Calling enable_ic
iptables -A voipnow_in -p tcp --dport 443 -m conntrack --ctstate NEW -j ACCEPT
iptables -A voipnow_in -p tcp --dport 80 -m conntrack --ctstate NEW -j ACCEPT
Calling enable_jabber
iptables -A voipnow_in -p tcp --dport 5222 -m conntrack --ctstate NEW -j ACCEPT
iptables -A voipnow_in -p tcp --dport 5269 -m conntrack --ctstate NEW -j ACCEPT
iptables -A voipnow_in -p tcp --dport 5280 -m conntrack --ctstate NEW -j ACCEPT
Calling enable_mail
iptables -A voipnow_in -p tcp --dport 25 -m conntrack --ctstate NEW -j ACCEPT
Calling enable_pbx
iptables -A voipnow_in -p tcp --dport 5050 -m conntrack --ctstate NEW -j ACCEPT
iptables -A voipnow_in -p udp --dport 10000:20000 -m conntrack --ctstate NEW -j ACCEPT
iptables -A voipnow_in -p udp --dport 20000:4000 -m conntrack --ctstate NEW -j ACCEPT
Calling enable_que
iptables -A voipnow_in -i lo -p tcp -m tcp --dport 5672 -j ACCEPT
Calling enable_sip
iptables -A voipnow_in -p tcp --dport 5060 -m conntrack --ctstate NEW -j ACCEPT
iptables -A voipnow_in -p udp --dport 5060 -m conntrack --ctstate NEW -j ACCEPT
iptables -A voipnow_in -p tcp --dport 5061 -m conntrack --ctstate NEW -j ACCEPT
iptables -A voipnow_in -p udp --dport 5061 -m conntrack --ctstate NEW -j ACCEPT
Calling enable_sql
iptables -A voipnow_in -p tcp --dport 3306 -m conntrack --ctstate NEW -j ACCEPT
Calling enable_es
iptables -A voipnow_in -p tcp --dport 9200 -m conntrack --ctstate NEW -j ACCEPT
Calling enable_wk
iptables -A voipnow_in -i lo -p tcp -m tcp --dport 10000 -j ACCEPT
Calling run_custom()
Calling block_all()
iptables -A INPUT -j DROP
Calling set_kernel()
Done
Saving rules
Firewall has been generated and will be cleared in 10 minutes to avoid being locked out in case something went
wrong.
The new rules have been saved into /etc/sysconfig/iptables and will be applied at system boot.
If everything is correct, please remove the cron job by running:
/usr/local/voipnow/admin/sbin/voipnow_firewall ok
```

Related articles

- How to use the VoipNow 5 built-in firewall
- How to use VoipNow 3 behind a firewall
- How to use the VoipNow built-in firewall