The basic commands for the firewall:

1. Command firewalllog -- To check the firewall logs and to find out source, destination, ports, request is passing or blocking and matching firewall rule no. etc…

```
superuser@securegate > firewalllog
2015:02:16-09:47:54 kernel: [671650.802321] GSHIELD=pass*rule-51 IN=eth0 OUT=
MAC=00:90:fb:4a:ab:8a:20:68:9d:d0:30:5f:08:00 SRC=192.168.2.214 DST=115.112.0.7 LEN=52
TOS=0x00 PREC=0x00 TTL=128 ID=19191 DF PROTO=TCP SPT=59821 DPT=80
WINDOW=8192 RES=0x00 SYN URGP=0 MARK=0x20000
```

----

2. Command firewalllog -f 192.168.2.28
-f command is useful when we have to search particular phrase in the file. In this e.g. we are viewing firewall logs and we have to see the particular request from the ip 192.168.2.28 and for that we have used “-f” command. **(More about -f command in point no. 18)**

```
superuser@securegate > firewalllog -f 192.168.2.28
2015:02:16-09:55:02 kernel: [672078.559146] GSHIELD=pass*rule-51 IN=eth0 OUT=
MAC=00:90:fb:4a:ab:8a:20:68:9d:d0:30:5f:08:00 SRC=192.168.2.214 DST=115.112.0.7 LEN=52
TOS=0x00 PREC=0x00 TTL=128 ID=21920 DF PROTO=TCP SPT=55078 DPT=80
WINDOW=8192 RES=0x00 SYN URGP=0 MARK=0x20000
2015:02:16-09:55:02 kernel: [672078.576350] GSHIELD=pass*rule-51 IN=eth0 OUT=
MAC=00:90:fb:4a:ab:8a:00:16:3e:7e:3e:e6:08:00 SRC=192.168.2.95 DST=84.39.152.31 LEN=44
TOS=0x00 PREC=0x00 TTL=64 ID=30179 DF PROTO=TCP SPT=49746 DPT=80 WINDOW=5840
RES=0x00 SYN URGP=0 MARK=0x20000
```

----

3 . Command tcpdump –n –i eth0 – To sniff the request on interface eth0 on the firewall. Here you can use any interface (i.e. eth0, eth1….) which is configure on the firewall.

```
superuser@securegate > tcpdump -n -i eth0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
13:03:38.232840 IP 192.168.2.28.43983 > 192.168.2.199.80: Flags [S], seq 3347908027, win 5840,
options [mss 1460,sackOK,TS val 14256998 ecr 0,nop,wscale 7], length 0
13:03:38.232928 IP 192.168.2.199.80 > 192.168.2.28.43983: Flags [S.], seq 1154539632, ack
3347908028, win 14600, options [mss 1460], length 0
13:03:38.233039 IP 192.168.2.28.43983 > 192.168.2.199.80: Flags [.], ack 1, win 5840, length 0
13:03:38.233448 IP 192.168.2.28.43983 > 192.168.2.199.80: Flags [P.], seq 1:344, ack 1, win 5840,
length 343
```

In above output first ip which is showing is source ip with source port and after ‘>’ sign ip showing is destination ip with destination port.

4. Here if you use –e option that it will show you MAC address of source and destination ip addresses:

```
superuser@securegate > tcpdump -n -e -i eth0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
13:11:06.862741 00:16:17:4b:47:6c > 00:90:fb:4a:ab:8a, ethertype IPv4 (0x0800), length 781:
192.168.2.28.38029 > 74.125.236.162.80: Flags [P.], seq 1299923395:1299924122, ack 2666660037,
win 65535, length 727
13:11:06.862810 00:90:fb:4a:ab:8a > 00:16:17:4b:47:6c, ethertype IPv4 (0x0800), length 54:
74.125.236.162.80 > 192.168.2.28.38029: Flags [.], ack 727, win 65535, length 0
13:11:07.108850 00:90:fb:4a:ab:8a > 00:16:17:4b:47:6c, ethertype IPv4 (0x0800), length 539:
```

----

5. After mentioning interface name you can search the logs for particular ip address or particular ports or both in tcpdump command:

```
superuser@securegate > tcpdump -n -e -i eth0 host 192.168.2.28
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
13:11:06.862741 00:16:17:4b:47:6c > 00:90:fb:4a:ab:8a, ethertype IPv4 (0x0800), length 781:
192.168.2.28.38029 > 74.125.236.162.80: Flags [P.], seq 1299923395:1299924122, ack 2666660037,
win 65535, length 727
13:11:06.862810 00:90:fb:4a:ab:8a > 00:16:17:4b:47:6c, ethertype IPv4 (0x0800), length 54:
74.125.236.162.80 > 192.168.2.28.38029: Flags [.], ack 727, win 65535, length 0
13:11:07.108850 00:90:fb:4a:ab:8a > 00:16:17:4b:47:6c, ethertype IPv4 (0x0800), length 539:
74.125.236.162.80 > 192.168.2.28.38029: Flags [P.], seq 1:486, ack 727, win 65535, length 485
13:11:07.108901 00:90:fb:4a:ab:8a > 00:16:17:4b:47:6c, ethertype IPv4 (0x0800), length 89:
74.125.236.162.80 > 192.168.2.28.38029: Flags [P.], seq 486:521, ack 727, win 65535, length 35
```

----

6. To use host as well as port you have to use ‘and’ as a separator:

```
 superuser@securegate > tcpdump -n -i eth0 host 192.168.2.28 and port 80
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
20:02:23.982726 IP 203.199.74.17.80 > 192.168.2.21.4323: P
2315864785:2315865953(1168) ack 77231547 win 6432
20:02:23.985342 IP 203.199.74.17.80 > 192.168.2.21.4323: F 1168:1168(0) ack 1 win
6432
20:02:23.985592 IP 192.168.2.21.4323 > 203.199.74.17.80: . ack 1169 win 16352
```

----

7. Command – To check the current users browsing

```
superuser@securegate > browsinglog
1424072863 192.168.2.121 anita http://radarfeed.moneycontrol.com/mcradar/processing.php?
q_a=d&ep131222&callback=LTD 1290 200 text/html Finance Desktop#Windows_7#Microsoft
Internet Explorer_11.0
1424072864 192.168.2.219 anil http://img5a.flixcart.com/www/prod/images/social-sprite-
b3c0ada7.png 17839 200 image/png Entertainment Desktop#Windows_8.1#Chrome_40.0.2214.111
1424072864 192.168.2.26 vikram https://6-edge-chat.facebook.com/pull?
channel=p_1066906342&seq=123&partition=-2&clientid=607899c1&cb=gklr&idle=23&cap=8&uid=
1066906342&viewer_uid=1066906342&sticky_token=371&sticky_pool=frc1c06_chat-
```

```
proxy&traceid=ZEftv&state=active 1392 200 application/json Social_Networking
Desktop#Linux#Firefox_35.0
```

----

8. Command ipseclog – To check the IPSec VPN logs

superuser@securegate > ipseclog

```
2007:06:06-19:47:51 gsfw pluto[4653]: packet from  59.123.1.2:500: ignoring Vendor
ID payload [26244d38eddb61b3172a36e3d0cfb
819]
2007:06:06-19:47:51 gsfw pluto[4653]: \"arun_0\"[3]  59.123.1.2 #5: responding to
Main Mode from unknown peer 59.183.47.23
1
2007:06:06-19:47:51 gsfw pluto[4653]: \"arun_0\"[3]  59.123.1.2 #5: transition from
state (null) to state STATE_MAIN_R1
2007:06:06-19:47:52 gsfw pluto[4653]: \"arun_0\"[3]  59.123.1.2 #5: NAT-
Traversal: Result using draft-ietf-ipsec-nat-t-ike
-02/03: no NAT detected
2007:06:06-19:47:52 gsfw pluto[4653]: \"arun_0\"[3]  59.123.1.2 #5: transition from
state STATE_MAIN_R1 to state STATE_MAI
N_R2
2007:06:06-19:47:52 gsfw pluto[4653]: \"arun_0\"[3]  59.123.1.2 #5: Main mode
peer ID is ID_IPV4_ADDR: \' 59.123.1.2\'
2007:06:06-19:47:52 gsfw pluto[4653]: \"arun_0\"[3]  59.123.1.2 #5: transition from
state STATE_MAIN_R2 to state STATE_MAI
N_R3
2007:06:06-19:47:52 gsfw pluto[4653]: \"arun_0\"[3]  59.123.1.2 #5: sent MR3,
ISAKMP SA established
2007:06:06-19:47:52 gsfw pluto[4653]: \"arun_0\"[3]  59.123.1.2 #6: responding to
Quick Mode
2007:06:06-19:47:52 gsfw pluto[4653]: \"arun_0\"[3]  59.123.1.2 #6: transition from
state (null) to state STATE_QUICK_R1
2007:06:06-19:47:53 gsfw pluto[4653]: \"arun_0\"[3]  59.123.1.2 #6: transition from
state STATE_QUICK_R1 to state STATE_QU
ICK_R2
2007:06:06-19:47:53 gsfw pluto[4653]: \"arun_0\"[3]  59.123.1.2 #6: IPsec SA
established
```

----

9. Command : siteblocklog : Shows site block logs

superuser@securegate > siteblocklog

```
2015:02:18-09:37:37| gsfw redirect: |rajesh|192.168.2.28|http://www.youtube.com/favicon.ico|Blocked|
123|Entertainment category blocked|Desktop#Linux#Firefox_15.0
```

----

10. Command : mimeblocklog : Shows mime block logs

superuser@securegate > mimeblocklog

```
2015:02:18-09:41:18| gsfw mimeblock: |hariom|192.168.2.12|
https://ssl.gstatic.com/chat/sounds/incoming_video_long_f40743cff9a983482913249d4ff66102.ogg|
audio/ogg|Blocked|Mime type audio/ogg blocked|Desktop#Windows_7#Firefox_16.0
2015:02:18-09:41:21| gsfw mimeblock: |testid|10.10.16.5|
https://www.gstatic.com/chat/sounds/chat_message_52df20dbc4522c398abba5d0b6377131.mp3|
audio/mpeg|Blocked|Mime type audio/mpeg blocked|Desktop#Windows_7#Firefox_35.0
```

---

10. Command : usersenselog - Shows user-sense logs

```
superuser@securegate > usersenselog
2015:02:18-11:01:47syslog: Log In|ajay|192.168.2.26|Wed Feb 18 11:01:47 2015|1424237507|LDAP|
Desktop#Linux#Firefox_35.0
2015:02:18-11:10:08syslog: Log In|vikram|192.168.2.156|Wed Feb 18 11:10:08 2015|1424238008|
LDAP|Desktop#Ubuntu_Linux#Firefox_29.0
2015:02:18-11:25:55syslog: Log In|anju|192.168.2.236|Wed Feb 18 11:25:55 2015|1424238955|LDAP|
Desktop#Windows_8.1#Firefox_35.0
```

---

11. Command : ipconf - Configured interface IP address details

```
superuser@securegate > ipconf
```

---

12. Command :livebwusage - Show live bandwidth usage

```
superuser@securegate >livebwusage
```

When you run "livebwusage" you will find At the very top of the screen is a scale that goes along with the bar graph livebwusage might display with each connection. The next rows of output correspond to each network connection between a pair of hosts. In between the two hosts are arrows that let you know the direction the traffic is flowing. The final three columns provide average bandwidth for each connection during the last 2, 10 and 40 seconds, respectively. Underneath all the transmit and receive columns at the bottom of the screen are a series of statistics for overall transmitted and received traffic (TX and RX, respectively) including 2-, 10- and 40-second averages for both those and, finally, the totals for the interface.

Other Useful Command

13. traceroute	Print the route packets take to network host
14. downloadlog	Shows download logs
15. ipslog	Shows IPS logs
16. spamlog	Shows SPAM logs
17. uploadlog	Shows upload logs

---

18. Command : -f : to filter the traffic

For Ex. From command browsinglog you want to filter 192.168.2.28

```
superuser@securegate > browsinglog -f 192.168.2.28
```

then it will show you browsing log only for the system 192.168.2.28, -f command is useful when we

have to search particular phrase in the file
Same filter can to applied for other commands log related command

19 firewallstart --- Install all firewall rules
20 firewallstop --- Remove all firewall rules, makes the system open
21 fwdate --- View/Change firewall date-time
22 ping --- Send ICMP ECHO_REQUEST to network hosts
23 restartnetwork --- Restart the network
24 route -- Show or manipulate the IP routing table

25 usersenselog Show user-sense logs

```
superuser@securegate > usersenselog

2015:05:07-10:21:54syslog: Log In|guest|192.168.2.74|Thu May  7 10:21:54 2015|1430974314|Local|
Desktop#Windows_8.1#Chrome_42.0.2311.135
```