Traffic debugging on Gibraltar Firewall

Overview:

There are certain ways to debug traffic that is passing a Gibraltar Firewall. In this How-To we will give a quick overview of the most common tools tcpdump and iptraf.

Tcpdump:

Tcpdump prints out the headers of packets on a network interface that match the boolean expression. It can also be run with the -w flag, which causes it to save the packet data to a file for later analysis, and/or with the -r flag, which causes it to read from a saved packet file rather than to read packets from a network interface. In all cases, only packets that match expression will be processed by tcpdump.

Usage:

tcpdump [OPTIONS] [EXPRESSION]

Useful Options:

`-I <INTERFACE>`	*specifies the interface to listen on*
`-A`	*Print each packet (minuts its link level header) in ASCII. Handy for capturing web pages.*
`-c`	*Exit after receiving count packets*
`-D`	*Print the list of the network interfaces available on the system and on wich tcpdump can capture packets.*

Useful Expressions:

`src host`	*True if the IPv4/v6 source field of the packet is host, which may be either an address or a name.*
`dst host`	*True if the IPv4/v6 source destination of the packet is host.*
`host`	*True if either the IPv4/v6 source or destination of the packet is host.*
`src net`	*True if the IPv4/v6 source address of the packet has a network number of net.*
`dst net`	*True if the IPv4/v6 destination address of the packet has a network number of net.*
`net`	*True if either the IPv4/v6 source or destination address of the packet has a network number of net.*
`src port`	*True if the packet is ip/tcp, ip/udp, ip6/tcp or ip6/udp and has a source port value of port.*
`dst port`	*True if the packet has a destination port value of port.*
`port`	*True if either the source or destination port of the packet is port.*
`ether broadcast`	*True if the packet is an ethernet broadcast packet.*
`ip broadcast`	*True if the packet is an IPv4 broadcast packet.*
`ether multicast`	*True if the packet is an ethernet multicast packet.*
`ip multicast`	*True if the packet is an ip multicast packet.*

This expressions can all be combined by using operators like:

'**!**' *or* '**not**' *for Negation*

'**&&**' *or* '**and**' *for Concatenation*

'**||**' *or* '**or**' *for Alternation*

Examples:

 # To print all traffic that stands in any relation with the host 10.0.0.5

```
tcpdump -i INT host 10.0.0.5
```

 # To print all traffic that stands in any relation with the host 10.0.0.5 except traffic from and to 1.1.1.1

```
tcpdump -i INT host 10.0.0.5 and not host 1.1.1.1
```

 # To print ip multicast traffic on our interface 'INT'

```
tcpdump -i INT ip multicast
```

 # To print all packets on our interface 'INT' that comes from 10.0.0.5 and is dedicated to 1.1.1.1 or 1.1.1.2 using port 80

```
tcpdump -i INT src host 10.0.0.5 and dst host 1.1.1.1 or 1.1.1.2 and dst port 80
```

 # To print the HTTP traffic between our client 10.0.0.15 and a webserver on 200.0.0.1 in ASCII format

```
tcpdump -A -i INT src host 200.0.0.1 && dst host 10.0.0.15 && port http
```

Iptraf:

iptraf is an ncurses-based IP LAN monitor that generates various network statistics including TCP info, UDP counts, ICMP and OSPF information, Ethernet load info, node stats, IP checksum errors, and others.

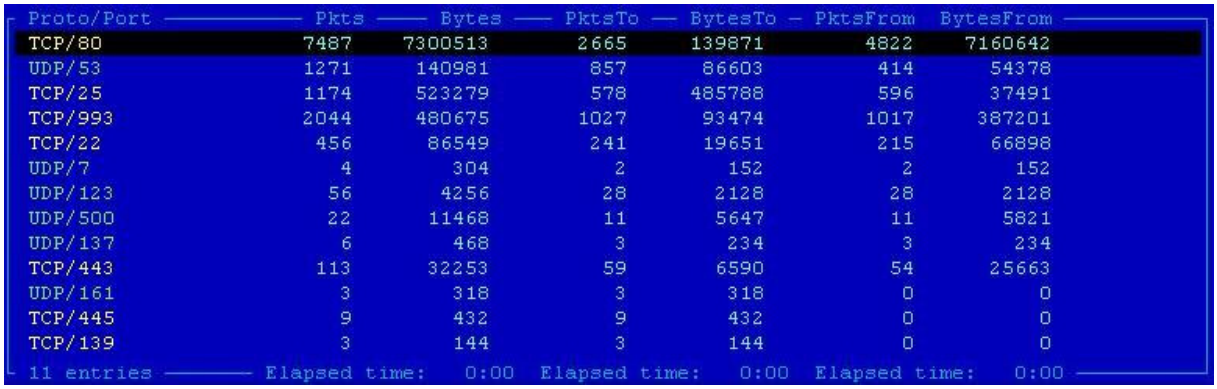
- IP Traffic Monitor
  Shows all running connections with the associated traffic, you can sort this output by pressing SHIFT+S and b(byte count) or p(packet count)
- General interface statistics
  Shows packet count and current kbits/sec for each interface
- Detailed Interface statistics
  Gives a overview of what is currently going on in your network, displaying incoming and outgoing traffic rates as well as total packet and byte counts

Useful Options:

`-u`	This option is needed because Gibraltar forces you to change the names of your network interfaces and iptraf does not recognize interfaces with changed names by default
`-i interface`	Immediately starts the IP Traffic Monitor on the specified `interface`
`-g`	Immediately starts the General Interface Statistics
`-d interface`	Immediately starts the Detailed Interface Statistics on the specified `interface`
`-s interface`	*allows you to immediately monitor TCP and UDP traffic on the specified* `interface`

Example:

```
gibraltar:~# iptraf -u -s wan
```



Proto/Port	Pkts	Bytes	PktsTo	BytesTo	PktsFrom	BytesFrom
TCP/80	7487	7300513	2665	139871	4822	7160642
UDP/53	1271	140981	857	86603	414	54378
TCP/25	1174	523279	578	485788	596	37491
TCP/993	2044	480675	1027	93474	1017	387201
TCP/22	456	86549	241	19651	215	66898
UDP/7	4	304	2	152	2	152
UDP/123	56	4256	28	2128	28	2128
UDP/500	22	11468	11	5647	11	5821
UDP/137	6	468	3	234	3	234
TCP/443	113	32253	59	6590	54	25663
UDP/161	3	318	3	318	0	0
TCP/445	9	432	9	432	0	0
TCP/139	3	144	3	144	0	0
11 entries	Elapsed time:	0:00	Elapsed time:	0:00	Elapsed time:	0:00

Resources and useful links:

http://en.wikipedia.org/wiki/Tcpdump
http://www.tcpdump.org/tcpdump_man.html
http://www.msamir.net/the-art-of-network-debugging-with-tcpdump/
http://pwet.fr/man/linux/administration_systeme/iptraf
http://iptraf.seul.org/2.7/manual.html
http://de.wikipedia.org/wiki/IPTraf