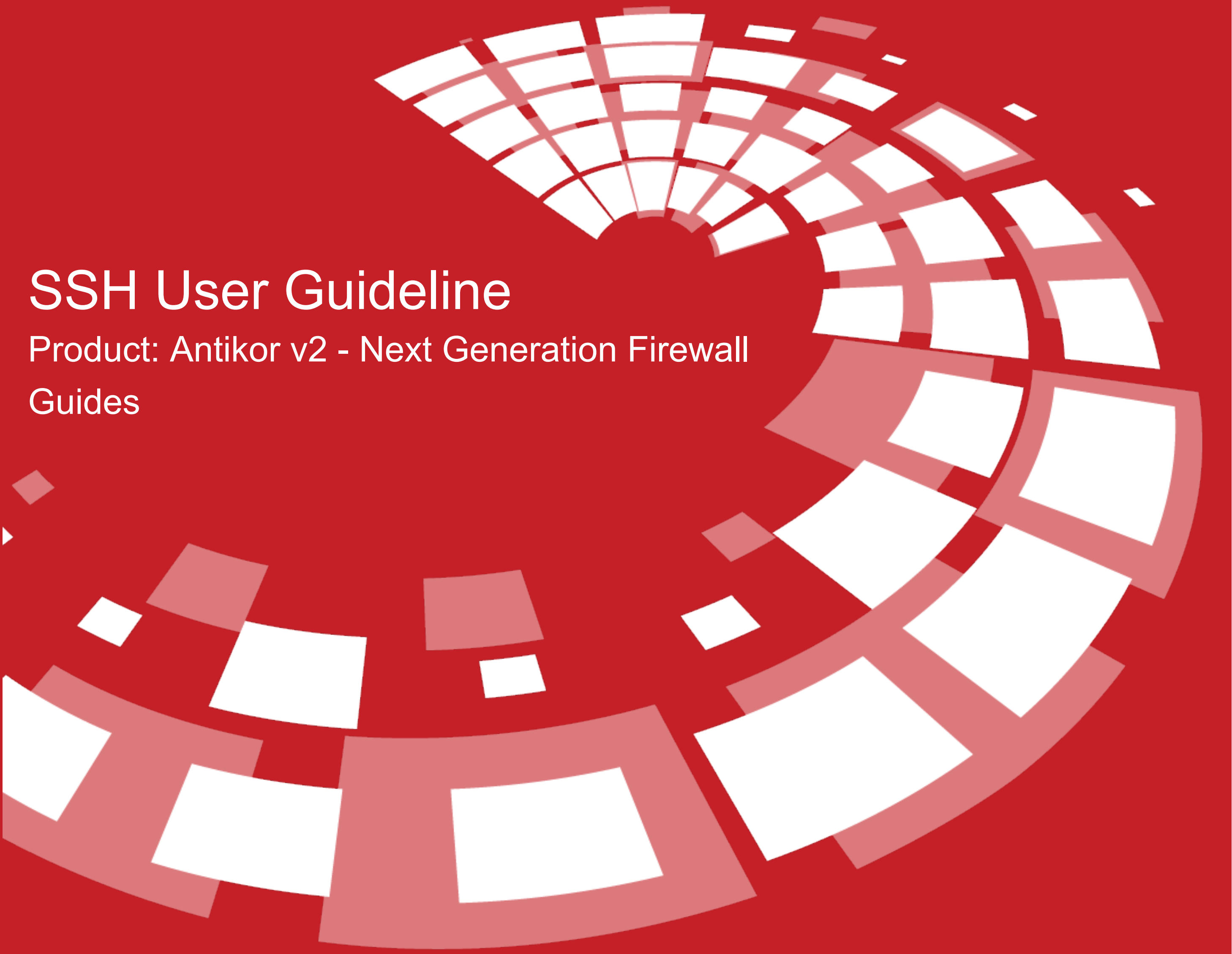
epati



SSH User Guideline

Product: Antikor v2 - Next Generation Firewall

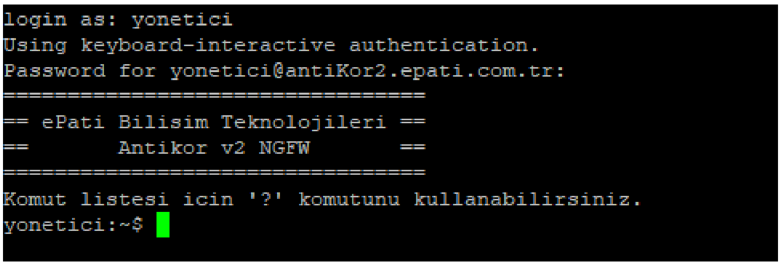
Guides

www.epati.com.tr

SSH User Guideline

In order to log into Antikor as Administrator Putty program is used. We use Antikor's internal IP in the event we access from inside the organization. Otherwise we use Antikor's external IP if we access from outside the organization. Port number is 22022. The username is "admin" (Do not try port "22" from a remote site, as you will be blocked since it is added into Honeypot service. There will be no blocking if you add your IP address into ignored list.)

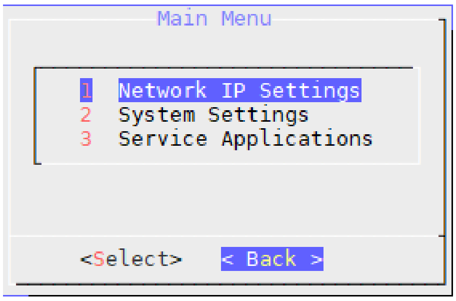
To open SSH control panel in AntiKor, a password is given by the company personnel or through "Console Panel". Subsequent password operations can be performed with the administrator "ssh-password-change" command.



```
login as: yonetici
Using keyboard-interactive authentication.
Password for yonetici@antiKor2.epati.com.tr:
=================================
== ePati Bilisim Teknolojileri ==
==       Antikor v2 NGFW       ==
=================================
Komut listesi icin '?' komutunu kullanabilirsiniz.
yonetici:~$
```

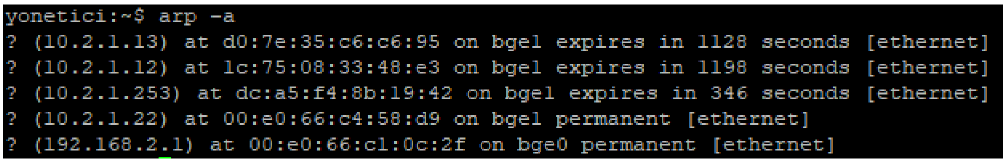
- **adminConsole** command

> It is now possible to run the console to which we already have access via keyboard and monitor over SSH. When you execute "Logoff" command SSH console will be prompted again.



- **arp** command

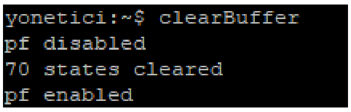
> IP is a protocol that allows us to learn the physical addresses of known devices. The command arp 172.29.148.5 gives us the MAC address of the device. The usage can be expanded by listing the parameters.



```
yonetici:~$ arp -a
? (10.2.1.13) at d0:7e:35:c6:c6:95 on bge1 expires in 1128 seconds [ethernet]
? (10.2.1.12) at 1c:75:08:33:48:e3 on bge1 expires in 1198 seconds [ethernet]
? (10.2.1.253) at dc:a5:f4:8b:19:42 on bge1 expires in 346 seconds [ethernet]
? (10.2.1.22) at 00:e0:66:c4:58:d9 on bge1 permanent [ethernet]
? (192.168.2.1) at 00:e0:66:c1:0c:2f on bge0 permanent [ethernet]
```

- **clearBuffer** command

> clearBuffer command is the command to clear security rules connections. The below figure shows clearing of 38627 security rule connections.



```
yonetici:~$ clearBuffer
pf disabled
70 states cleared
pf enabled
```

- **cd** command

> This command enables to navigate between directories. In order to go one path backwards use “cd.” command.

- **clear** command

> It is the command of UNIX / Linux operating system. This clears the SSH screen that you are on.

- **cluster-penalty-score** command

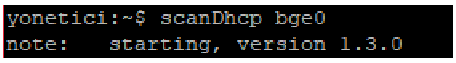
> Shows cluster penalty points.

- **cluster-status** command

> Gives information about cluster status.

- **scanDhcp** command

> This command scans the network environment for DHCP server.

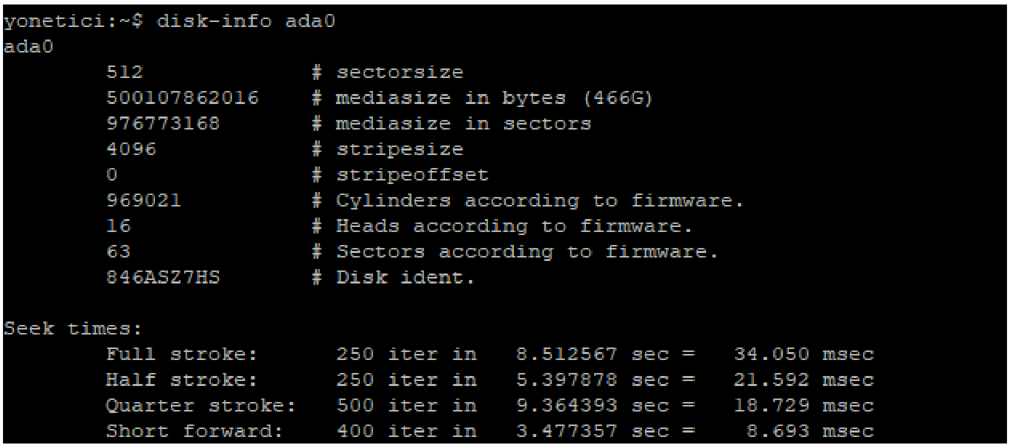


```
yonetici:~$ scanDhcp bge0
note:   starting, version 1.3.0
```

The above image does not return any results because the DHCP server does not exist in the environment. Otherwise if the DHCP server existed, it would have notified us with a few output. Output results can be expanded by using other parameters.

- **disk-info** command

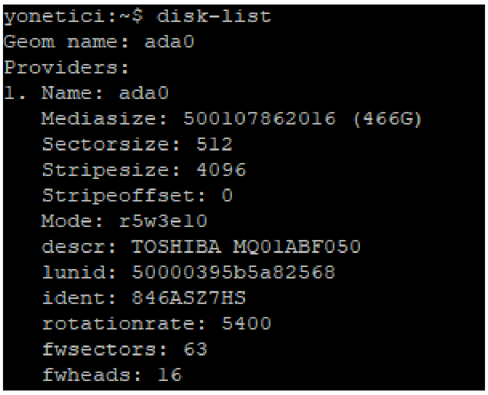
> This gives us disk performance information based on disk selection. The performance results of disk ada0 are as followes:



```
yonetici:~$ disk-info ada0
ada0
        512             # sectorsize
        500107862016    # mediasize in bytes (466G)
        976773168       # mediasize in sectors
        4096            # stripesize
        0               # stripeoffset
        969021          # Cylinders according to firmware.
        16              # Heads according to firmware.
        63              # Sectors according to firmware.
        846ASZ7HS       # Disk ident.

Seek times:
        Full stroke:      250 iter in   8.512567 sec =   34.050 msec
        Half stroke:      250 iter in   5.397878 sec =   21.592 msec
        Quarter stroke:   500 iter in   9.364393 sec =   18.729 msec
        Short forward:    400 iter in   3.477357 sec =    8.693 msec
```

- **disk-list** command

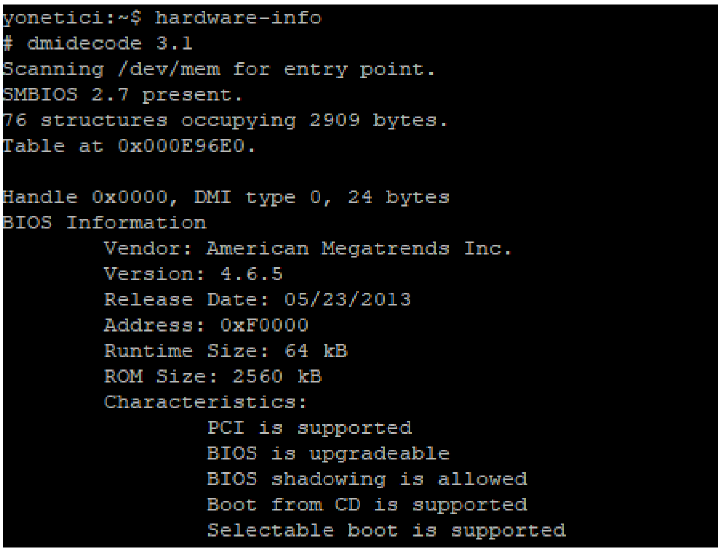
> This command shos information on existing disks. The following shows description, size and etc. details of disk ada0:



```
yonetici:~$ disk-list
Geom name: ada0
Providers:
1. Name: ada0
   Mediasize: 500107862016 (466G)
   Sectorsize: 512
   Stripesize: 4096
   Stripeoffset: 0
   Mode: r5w3e10
   descr: TOSHIBA MQ01ABF050
   lunid: 50000395b5a82568
   ident: 846ASZ7HS
   rotationrate: 5400
   fwsectors: 63
   fwheads: 16
```

- **hardware-info** command

> This command shows hardware details (e.g. RAM, CPU, etc.). You may see rest of the output by pressing Enter key.



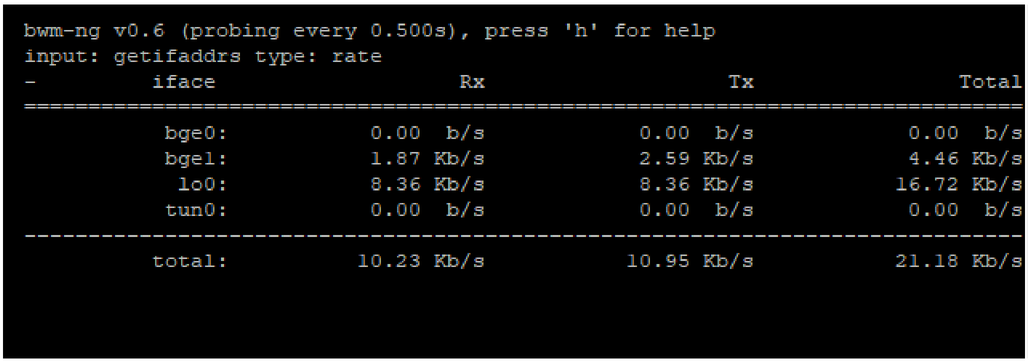
```
yonetici:~$ hardware-info
# dmidecode 3.1
Scanning /dev/mem for entry point.
SMBIOS 2.7 present.
76 structures occupying 2909 bytes.
Table at 0x000E96E0.

Handle 0x0000, DMI type 0, 24 bytes
BIOS Information
        Vendor: American Megatrends Inc.
        Version: 4.6.5
        Release Date: 05/23/2013
        Address: 0xF0000
        Runtime Size: 64 kB
        ROM Size: 2560 kB
        Characteristics:
                PCI is supported
                BIOS is upgradeable
                BIOS shadowing is allowed
                Boot from CD is supported
                Selectable boot is supported
```

- **interface** command

> When we type Ethernet and hit Enter real-tine send/receive traffic over all Ethernets and VLAN Ethernets will be showed. In this screen Rx Download, and Tx Upload. Press h to retrieve values and time information from the help menu. For example:

- d automatically converts values into Byte/KB/MB/GB.
- u shows values in bytes, bits, packets, errors. Every time we press u, it proceeds to the next one. In this screen packets number of packages per second, and errors number of errors per second.
- t current rate, max, sum since start, average for last 30s.
- a This shows unused ethernets.
- ”+” Default value is 0.500 s. Every time we press + time increases by 100 ms.
- ”-“ Default value 0.500 s. Every time we press - time decreases by 100 ms.
- n This changes input value.
- q This enables us to quit program.

The Ethernet program looks like the following:



```
bwm-ng v0.6 (probing every 0.500s), press 'h' for help
input: getifaddrs type: rate
-         iface                   Rx                   Tx                Total
==============================================================================
           bge0:           0.00  b/s           0.00  b/s           0.00  b/s
           bge1:           1.87 Kb/s           2.59 Kb/s           4.46 Kb/s
            lo0:           8.36 Kb/s           8.36 Kb/s          16.72 Kb/s
           tun0:           0.00  b/s           0.00  b/s           0.00  b/s
------------------------------------------------------------------------------
          total:          10.23 Kb/s          10.95 Kb/s          21.18 Kb/s
```

- **exit** command

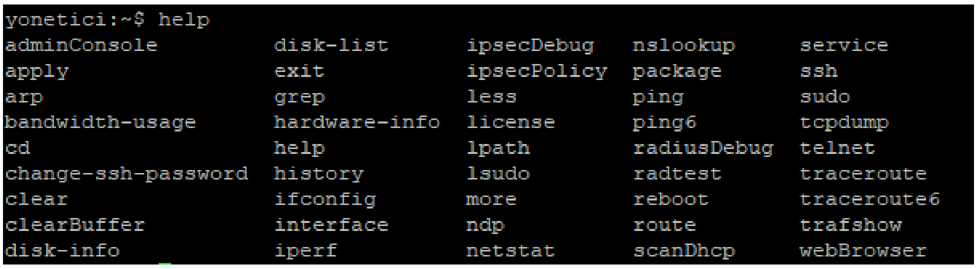
> This is a command in UNIX/Linux operating system. This disconnects our SSH connection.

- **grep** command

> This allows that the input files are used to perform a line-by-line search.

- **help** command

> This opens help menu and has the same function as “?”.



```
yonetici:~$ help
adminConsole         disk-list      ipsecDebug   nslookup     service
apply                exit           ipsecPolicy  package      ssh
arp                  grep           less         ping         sudo
bandwidth-usage      hardware-info  license      ping6        tcpdump
cd                   help           lpath        radiusDebug  telnet
change-ssh-password  history        lsudo        radtest      traceroute
clear                ifconfig       more         reboot       traceroute6
clearBuffer          interface      ndp          route        trafshow
disk-info            iperf          netstat      scanDhcp     webBrowser
```

- **history** command

> This shows outputs of last commands used in SSH.

- **http-logs** command

> This command shows instant http and http access requests.

- **ifconfig** command
  It is the command of UNIX / Linux operating system. The basic purpose is to assign IP to the vlan ethernet we have created with real ethernet, or to see the IP information by typing “ifconfig”. For example in order to assign an IP you may type the following: `sudo ifconfig bge0 10.2.2.1/24 up`

- **iperf** command

> This is used to test network speed between two clients. IPerf -s parameter makes one client to act like a server. IPerf -c host parameter makes one client to act like a client.

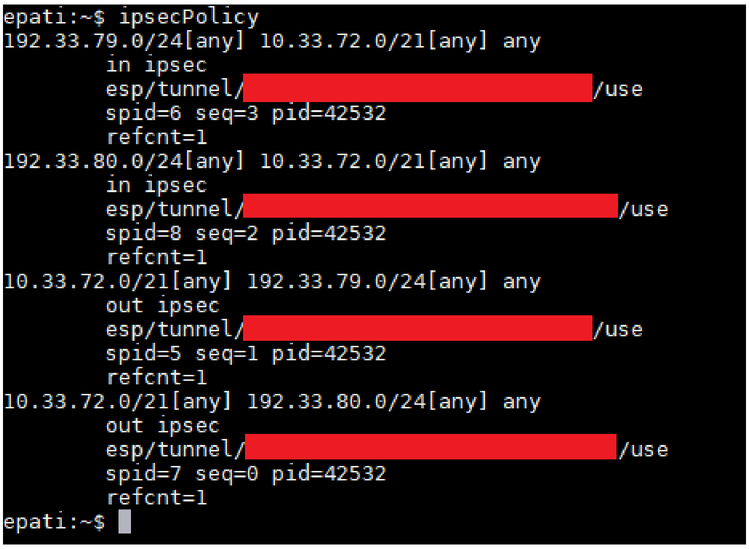
- **ipsecDebug** command

> This is used to show positive/negative outputs related to Ipsec VPN.

- **ipsecPolicy** command

> This shows IPSEC VPN policies. IpsecPolicy output contains information on tunnels created.

(Note: Fields had to be highlighted with red, as external IP addresses were entered therein.)



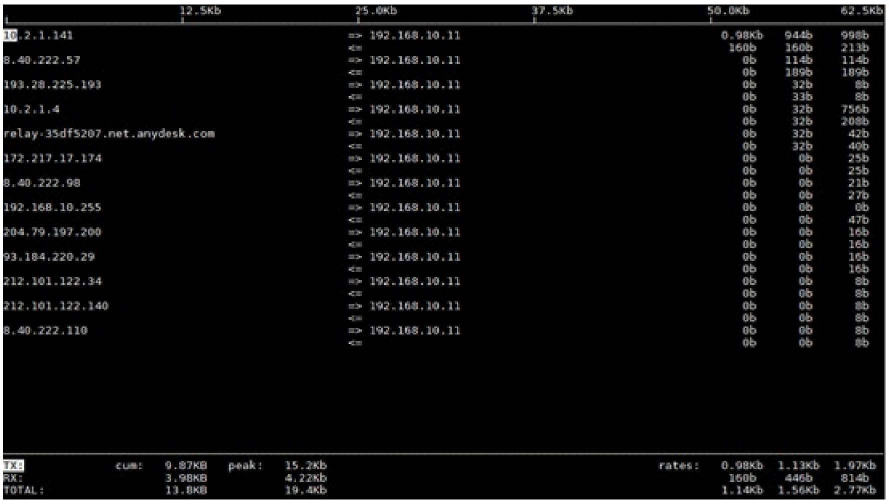
```
epati:~$ ipsecPolicy
192.33.79.0/24[any] 10.33.72.0/21[any] any
        in ipsec
        esp/tunnel/[redacted]/use
        spid=6 seq=3 pid=42532
        refcnt=1
192.33.80.0/24[any] 10.33.72.0/21[any] any
        in ipsec
        esp/tunnel/[redacted]/use
        spid=8 seq=2 pid=42532
        refcnt=1
10.33.72.0/21[any] 192.33.79.0/24[any] any
        out ipsec
        esp/tunnel/[redacted]/use
        spid=5 seq=1 pid=42532
        refcnt=1
10.33.72.0/21[any] 192.33.80.0/24[any] any
        out ipsec
        esp/tunnel/[redacted]/use
        spid=7 seq=0 pid=42532
        refcnt=1
epati:~$
```

- **bandwidth-usage** command

> When we type user and hit Enter, this shows users of the firts Ethernet.

- kullanici –i bge0, This shows IPs on our Local Network and IP addresses on the Internet.
- kullanici –i bge1, It shows the actual IPs on the external side and the IP addresses on the internet.
- kullanici –i bge2, It shows IPs on server area and the IP addresses on the internet.

You can also see the 65536 port here while Instant Web Access shows only web requests in AntiKor’s web interface. So the torrent users reveal themselves. The below figure shows how an IP (10.2.1.22) downloads.



```
                    12.5Kb              25.0Kb              37.5Kb              50.0Kb          62.5Kb
10.2.1.141                           => 192.168.10.11                            0.98Kb   944b    998b
                                     <=                                            160b   160b    213b
8.40.222.57                          => 192.168.10.11                               0b    114b    114b
                                     <=                                             0b    189b    189b
193.28.225.193                       => 192.168.10.11                               0b     32b      8b
                                     <=                                             0b     33b      8b
10.2.1.4                             => 192.168.10.11                               0b     32b    756b
                                     <=                                             0b     32b    208b
relay-35df5207.net.anydesk.com       => 192.168.10.11                               0b     32b     42b
                                     <=                                             0b     32b     40b
172.217.17.174                       => 192.168.10.11                               0b      0b     25b
                                     <=                                             0b      0b     25b
8.40.222.98                          => 192.168.10.11                               0b      0b     21b
                                     <=                                             0b      0b     27b
192.168.10.255                       => 192.168.10.11                               0b      0b      0b
                                     <=                                             0b      0b     47b
204.79.197.200                       => 192.168.10.11                               0b      0b     16b
                                     <=                                             0b      0b     16b
93.184.220.29                        => 192.168.10.11                               0b      0b     16b
                                     <=                                             0b      0b     16b
212.101.122.34                       => 192.168.10.11                               0b      0b      8b
                                     <=                                             0b      0b      8b
212.101.122.140                      => 192.168.10.11                               0b      0b      8b
                                     <=                                             0b      0b      8b
8.40.222.110                         => 192.168.10.11                               0b      0b      8b
                                     <=                                             0b      0b      8b

TX:           cum:   9.87KB   peak:   15.2Kb                      rates:   0.98Kb  1.13Kb  1.97Kb
RX:                  3.98KB            4.22Kb                                160b    446b    814b
TOTAL:              13.8KB            19.4Kb                              1.14Kb  1.56Kb  2.77Kb
```

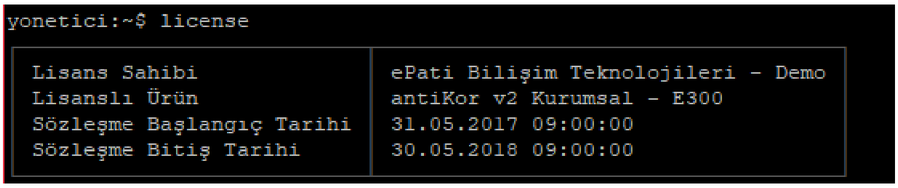
For example, if we are going to look up users only in one VLAN we need to type –i bge0.166.

- **less** command

> We can see entire output, which is longer than the length of the screen by typing less command to fit it to size of the screen.

- **license** command

> This shows license details of Antikor.



```
yonetici:~$ license
 ┌────────────────────────────┬──────────────────────────────────┐
 │ Lisans Sahibi              │ ePati Bilişim Teknolojileri - Demo │
 │ Lisanslı Ürün              │ antiKor v2 Kurumsal - E300         │
 │ Sözleşme Başlangıç Tarihi  │ 31.05.2017 09:00:00                │
 │ Sözleşme Bitiş Tarihi      │ 30.05.2018 09:00:00                │
 └────────────────────────────┴──────────────────────────────────┘
```

- **lpath** command

> This lists authorized folders. In the image below, the authorized folders are listed.

- **lsudo** command

> This lists the commands with sudo authorization. In the image below, the commands that can be used with sudo command are listed. We can use the following commands with sudo.

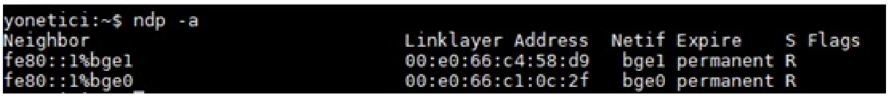
- **more** command

> This is the command to be used to retrieve more details from a command. When I call for help menu for “less” command and add “more” command to it this will allow us to receive more detail on “less” command.

- **ndp** command

> This has replaced such function as ARP, ICMP, etc. used in IPv4 protocol.

- ndp – a, Shows all relevant ndp entries.
- ndp –d, Parameter –d enables a super user to delete any entery for a hostname
- ndp –i, Coupled with paramater –s a ndp entry specified directory of interface to be used.
- ndp –I, This command deletes default Ethernet discovery interface.
- ndp –s → This creates a ndp entry for hardware address and hostname. The entry would be permanent unless command includes the term temp.

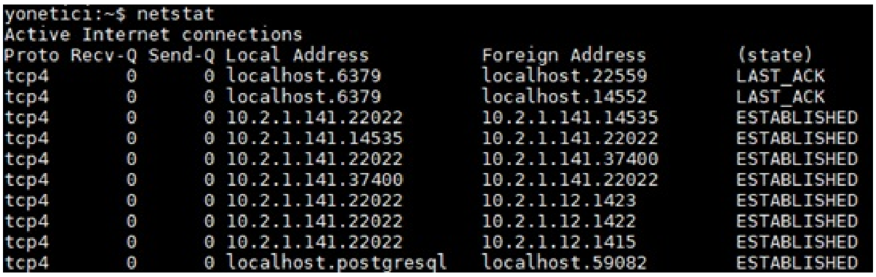


```
yonetici:~$ ndp -a
Neighbor                            Linklayer Address  Netif Expire    S Flags
fe80::1%bge1                        00:e0:66:c4:58:d9   bge1 permanent R
fe80::1%bge0                        00:e0:66:c1:0c:2f   bge0 permanent R
```

- **netstat** command

> This is a command of UNIX/Linux operating system. This shows details of network connections (e.g. TCP, UDP, Port Number, Status, etc..) It has many parameters.

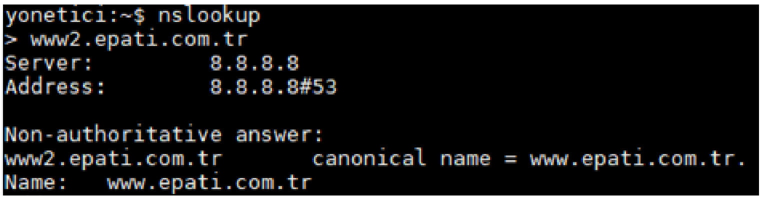
- For example: netstat –m, It gives us information on Network status.
- netstat –n, Shows list of connections made on the server.



```
yonetici:~$ netstat
Active Internet connections
Proto Recv-Q Send-Q Local Address          Foreign Address        (state)
tcp4       0      0 localhost.6379         localhost.22559        LAST_ACK
tcp4       0      0 localhost.6379         localhost.14552        LAST_ACK
tcp4       0      0 10.2.1.141.22022       10.2.1.141.14535       ESTABLISHED
tcp4       0      0 10.2.1.141.14535       10.2.1.141.22022       ESTABLISHED
tcp4       0      0 10.2.1.141.22022       10.2.1.141.37400       ESTABLISHED
tcp4       0      0 10.2.1.141.37400       10.2.1.141.22022       ESTABLISHED
tcp4       0      0 10.2.1.141.22022       10.2.1.12.1423         ESTABLISHED
tcp4       0      0 10.2.1.141.22022       10.2.1.12.1422         ESTABLISHED
tcp4       0      0 10.2.1.141.22022       10.2.1.12.1415         ESTABLISHED
tcp4       0      0 localhost.postgresql   localhost.59082        ESTABLISHED
```

- **nslookup** command

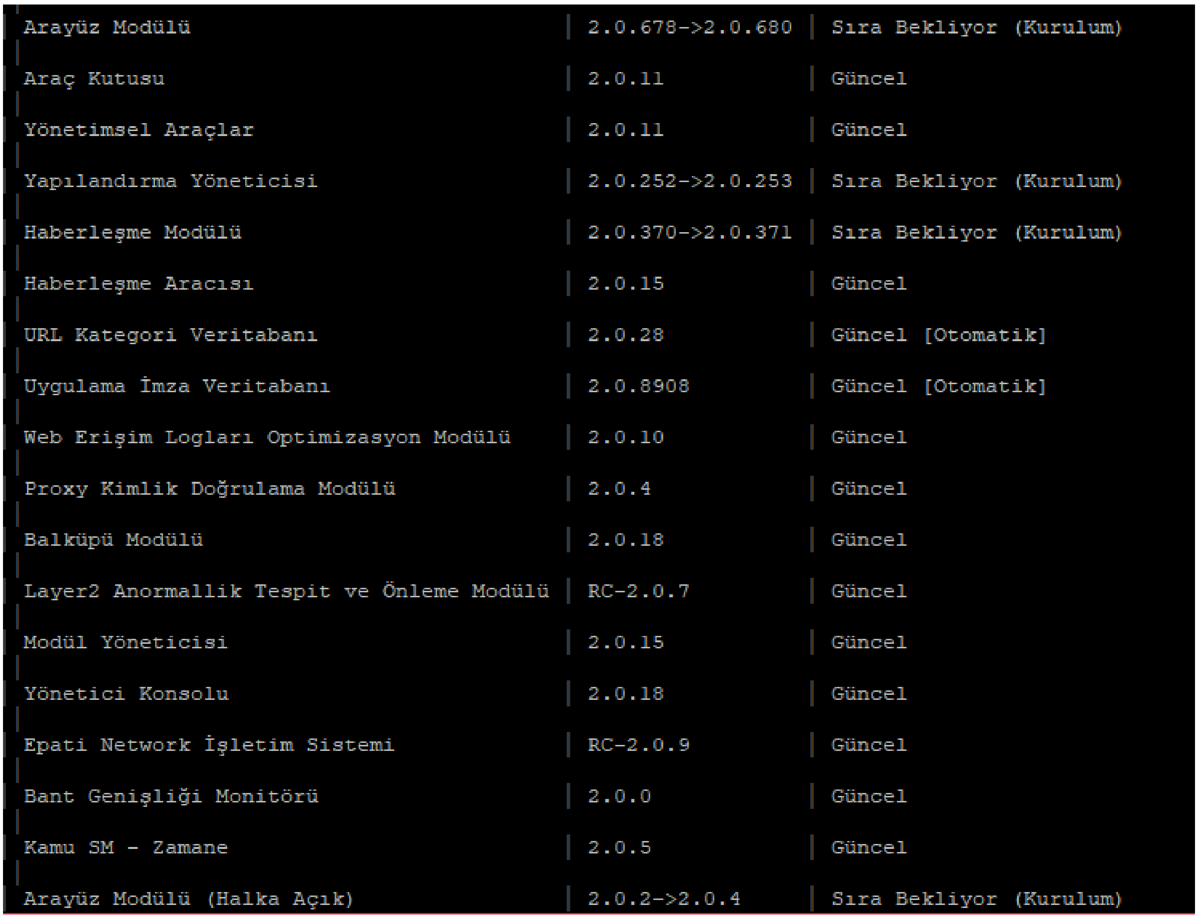
> This is used to check whether or not DNS server runs smoothly. The below figure shows result of inqury about Epati.



```
yonetici:~$ nslookup
> www2.epati.com.tr
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
www2.epati.com.tr       canonical name = www.epati.com.tr.
Name:   www.epati.com.tr
```

- **package** command

> This provides details on version and status of Antikor packages.



```
| Arayüz Modülü                             | 2.0.678->2.0.680 | Sıra Bekliyor (Kurulum)
|
| Araç Kutusu                               | 2.0.11           | Güncel
|
| Yönetimsel Araçlar                        | 2.0.11           | Güncel
|
| Yapılandırma Yöneticisi                   | 2.0.252->2.0.253 | Sıra Bekliyor (Kurulum)
|
| Haberleşme Modülü                         | 2.0.370->2.0.371 | Sıra Bekliyor (Kurulum)
|
| Haberleşme Aracısı                        | 2.0.15           | Güncel
|
| URL Kategori Veritabanı                   | 2.0.28           | Güncel [Otomatik]
|
| Uygulama İmza Veritabanı                  | 2.0.8908         | Güncel [Otomatik]
|
| Web Erişim Logları Optimizasyon Modülü    | 2.0.10           | Güncel
|
| Proxy Kimlik Doğrulama Modülü             | 2.0.4            | Güncel
|
| Balküpü Modülü                            | 2.0.18           | Güncel
|
| Layer2 Anormallik Tespit ve Önleme Modülü | RC-2.0.7         | Güncel
|
| Modül Yöneticisi                          | 2.0.15           | Güncel
|
| Yönetici Konsolu                          | 2.0.18           | Güncel
|
| Epati Network İşletim Sistemi             | RC-2.0.9         | Güncel
|
| Bant Genişliği Monitörü                   | 2.0.0            | Güncel
|
| Kamu SM - Zamane                          | 2.0.5            | Güncel
|
| Arayüz Modülü (Halka Açık)                | 2.0.2->2.0.4     | Sıra Bekliyor (Kurulum)
```

- **ping** command

> This is used to determine such functions of a target computer, server, and etc as operating status, distance, and etc. The following image shows ping perform on IP address 10.2.1.141 and successful response.

- Icmp_seq, Package header information will increase the header order in each ping packet.
- TTL (time to live), Time to live of package.

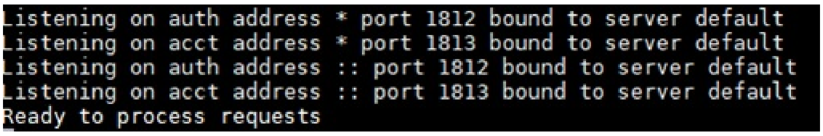
- Time, Information about how long the Ping communication takes place..

- **ping6** command

> Ping6 is a model of Ping developed for IPv6 için geliştirilmiş modelidir. This is for those who use IPv6 protocol.

- **radiusDebug** command

> This shows positive/nagative outputs in Radius server.



```
Listening on auth address * port 1812 bound to server default
Listening on acct address * port 1813 bound to server default
Listening on auth address :: port 1812 bound to server default
Listening on acct address :: port 1813 bound to server default
Ready to process requests
```

- **radtest** command

> This has been developed to test Radius server.

- radtest –d This is a command to set up a Radius directory.
- radtest –t This is a command to specify IT check method.
- radtest –p This is a commond that enables us to select a protocol.
- radtest –x This is a command to parse error outputs.

- radtest -4 This is a command used to assign an IPv4 address for NAS.

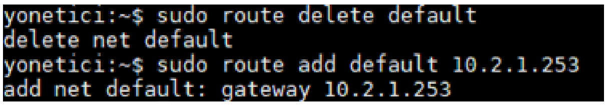
- radtest -6 This is a command used to assign an IPv6 address for NAS.

- **route** command

> This is a command for UNIX/Linux operating system. It is use to clear or define a new route for the operating system.

- sudo route delete default → deletes the route then existed.
- sudo route add default 10.2.1.253

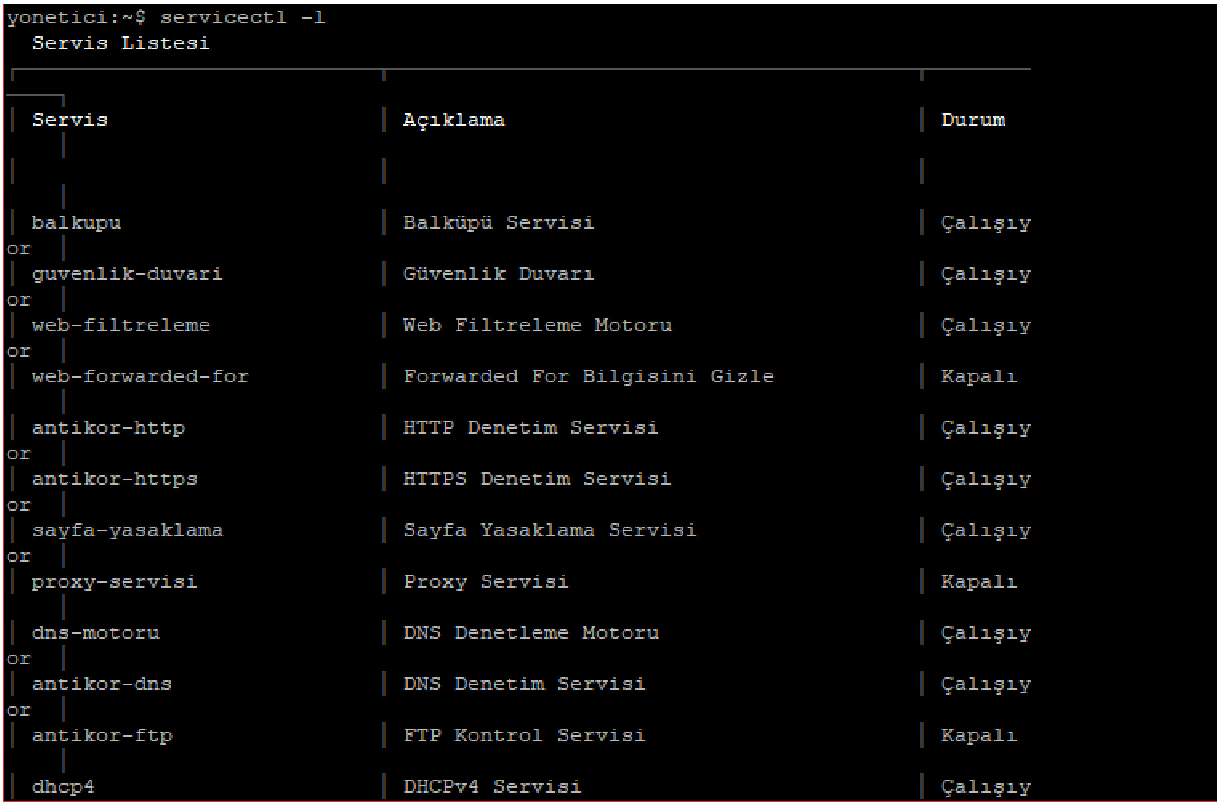
In the following image first of all the route was deleted and then it was re-added.



```
yonetici:~$ sudo route delete default
delete net default
yonetici:~$ sudo route add default 10.2.1.253
add net default: gateway 10.2.1.253
```

- **servicectl** command

> It gives information about the status of the antiKor services. As shown in the following image, the services appear as “Running, Off, Bypass, or Not Configured”.



```
yonetici:~$ servicectl -l
  Servis Listesi
┌────────────────────────────┬────────────────────────────────────────────┬────────
───┐
│  Servis                     │ Açıklama                                   │ Durum
   │
│                             │                                            │
   │
│  balkupu                    │ Balküpü Servisi                            │ Çalışıy
or │
│  guvenlik-duvari            │ Güvenlik Duvarı                            │ Çalışıy
or │
│  web-filtreleme             │ Web Filtreleme Motoru                      │ Çalışıy
or │
│  web-forwarded-for          │ Forwarded For Bilgisini Gizle              │ Kapalı
   │
│  antikor-http               │ HTTP Denetim Servisi                       │ Çalışıy
or │
│  antikor-https              │ HTTPS Denetim Servisi                      │ Çalışıy
or │
│  sayfa-yasaklama            │ Sayfa Yasaklama Servisi                    │ Çalışıy
or │
│  proxy-servisi              │ Proxy Servisi                              │ Kapalı
   │
│  dns-motoru                 │ DNS Denetleme Motoru                       │ Çalışıy
or │
│  antikor-dns                │ DNS Denetim Servisi                        │ Çalışıy
or │
│  antikor-ftp                │ FTP Kontrol Servisi                        │ Kapalı
   │
│  dhcp4                      │ DHCPv4 Servisi                             │ Çalışıy
```

- **ssh** command

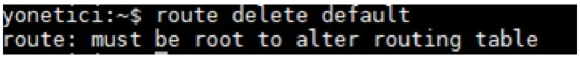
> This is a protocol used for a remote conenction.

- **change-ssh-password** command

> This is the command used to change SSH password (Note: Password characters are hidden and they are not visible when creating a password)

- **sudo** command

> This enables commands, which are permitted to run with Sudo, to run with root permission. For example, when performing Route command or in the event we wish to delete a Route, which is already added, an error message will be displayed to us, as there is not any Sudo authorization.

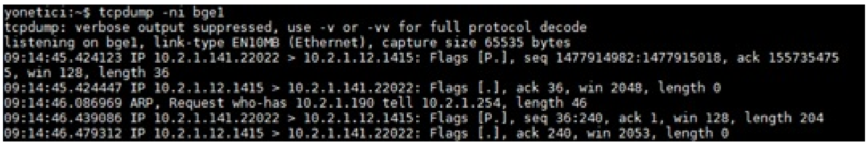


```
yonetici:~$ route delete default
route: must be root to alter routing table
```

- **tcpdump** command

> This is a command of UNIX/Linux operating system. It has many parameters. Examples of its usage are as follows:

tcpdump –D, This lists all interfaces which can be monitored over the network.
tcpdump –i bge0, This enables to monitor bge0 interface.
tcpdump -n src net 10.2.1.141, This command lists packages received from specified network address.
tcpdump –ni bge0, This command monitors local network traffic. It shows VLANs connected to this Ethernet over the VLAN.
tcpdump –ni bge0.166 host 10.2.2.2, This command shows traffic of only this IP on VLAN.
tcpdump ether host 11:22:33:44:55:66, This command shows traffic of computer with this MAC address.
tcpdump -i bge0.166 host 10.2.2.2 or 10.2.2.10, This command shows traffic of this 2 IPs.
tcpdump udp and (src port 161 or 162 or 514), This command shows UDP and those with source ports 161, 162, and 514. It is possible to give more example.



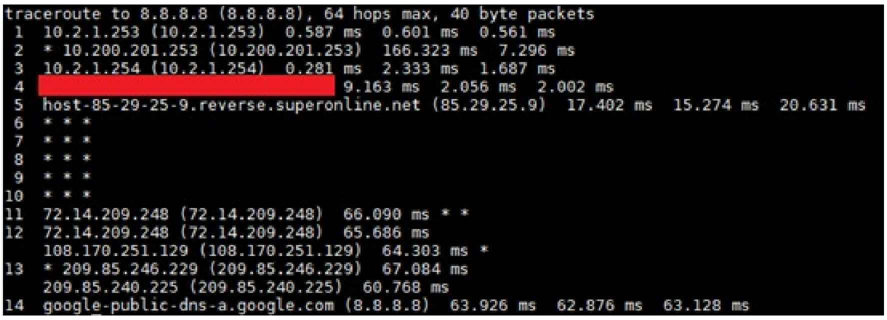
```
yonetici:~$ tcpdump -ni bge1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on bge1, link-type EN10MB (Ethernet), capture size 65535 bytes
09:14:45.424123 IP 10.2.1.141.22022 > 10.2.1.12.1415: Flags [P.], seq 1477914982:1477915018, ack 155735475
5, win 128, length 36
09:14:45.424447 IP 10.2.1.12.1415 > 10.2.1.141.22022: Flags [.], ack 36, win 2048, length 0
09:14:46.086969 ARP, Request who-has 10.2.1.190 tell 10.2.1.254, length 46
09:14:46.439086 IP 10.2.1.141.22022 > 10.2.1.12.1415: Flags [P.], seq 36:240, ack 1, win 128, length 204
09:14:46.479312 IP 10.2.1.12.1415 > 10.2.1.141.22022: Flags [.], ack 240, win 2053, length 0
```

- **telnet** command

> This is command used to connect to a remote computer or server. It is less secure than SSH. You can make a connection like the one in the following image, if the settings for telnet are configured, the connection session will be established.

- **traceroute** command

> This command shows what routers the IP package passes through on the way to its target. traceroute command was run for Google's DNS server. (Note: Fields had to be highlighted with red, as external IP addresses were entered therein.)



```
traceroute to 8.8.8.8 (8.8.8.8), 64 hops max, 40 byte packets
 1  10.2.1.253 (10.2.1.253)  0.587 ms  0.601 ms  0.561 ms
 2  * 10.200.201.253 (10.200.201.253)  166.323 ms  7.296 ms
 3  10.2.1.254 (10.2.1.254)  0.281 ms  2.333 ms  1.687 ms
 4  [redacted] 9.163 ms  2.056 ms  2.002 ms
 5  host-85-29-25-9.reverse.superonline.net (85.29.25.9)  17.402 ms  15.274 ms  20.631 ms
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  72.14.209.248 (72.14.209.248)  66.090 ms * *
12  72.14.209.248 (72.14.209.248)  65.686 ms
    108.170.251.129 (108.170.251.129)  64.303 ms *
13  * 209.85.246.229 (209.85.246.229)  67.084 ms
    209.85.240.225 (209.85.240.225)  60.768 ms
14  google-public-dns-a.google.com (8.8.8.8)  63.926 ms  62.876 ms  63.128 ms
```

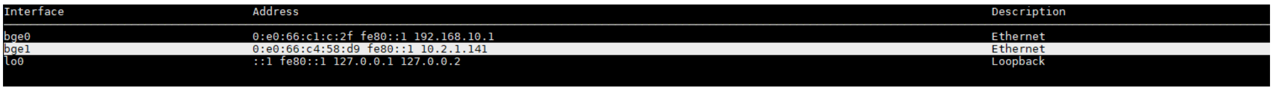
- **traceroute6** command

> This is the version of traceroute command developed for IPv6.

- **trafshow** command

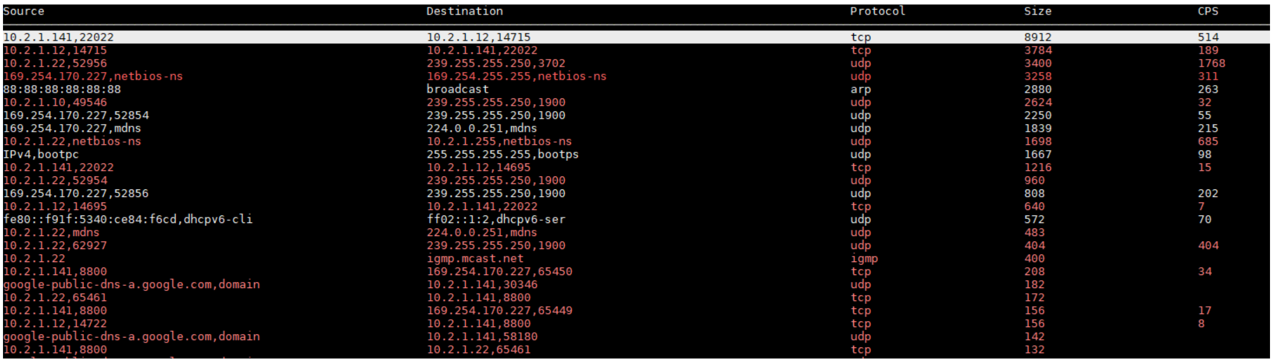
> This enables to monitor traffic by selecting Ethernet legs.

We first select the Ethernet leg to monitor:



```
Interface               Address                                       Description

bge0                    0:e0:66:c1:c:2f fe80::1 192.168.10.1          Ethernet
bge1                    0:e0:66:c4:58:d9 fe80::1 10.2.1.141           Ethernet
lo0                     ::1 fe80::1 127.0.0.1 127.0.0.2               Loopback
```

We select Bge1 leg and proceed:



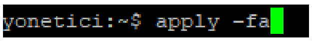
```
Source                                        Destination                                   Protocol          Size              CPS
==========================================================================================================================================
10.2.1.141,22022                              10.2.1.12,14715                               tcp               8912              514
10.2.1.12,14715                               10.2.1.141,22022                              tcp               3784              189
10.2.1.22,52956                               239.255.255.250,3702                          udp               3400              1768
169.254.170.227,netbios-ns                    169.254.255.255,netbios-ns                    udp               3258              311
88:88:88:88:88:88                             broadcast                                     arp               2880              263
10.2.1.10,49546                               239.255.255.250,1900                          udp               2624              32
169.254.170.227,52854                         239.255.255.250,1900                          udp               2250              55
169.254.170.227,mdns                          224.0.0.251,mdns                              udp               1839              215
10.2.1.22,netbios-ns                          10.2.1.255,netbios-ns                         udp               1698              685
IPv4,bootpc                                   255.255.255.255,bootps                        udp               1667              98
10.2.1.141,22022                              10.2.1.12,14695                               tcp               1216              15
10.2.1.22,52954                               239.255.255.250,1900                          udp               960
169.254.170.227,52856                         239.255.255.250,1900                          udp               808               202
10.2.1.12,14695                               10.2.1.141,22022                              tcp               640               7
fe80::f91f:5340:ce84:f6cd,dhcpv6-cli          ff02::1:2,dhcpv6-ser                          udp               572               70
10.2.1.22,mdns                                224.0.0.251,mdns                              udp               483
10.2.1.22,62927                               239.255.255.250,1900                          udp               404               404
10.2.1.22                                     igmp.mcast.net                                igmp              400
10.2.1.141,8800                               169.254.170.227,65450                         tcp               208               34
google-public-dns-a.google.com,domain         10.2.1.141,30346                              udp               182
10.2.1.22,65461                               10.2.1.141,8800                               tcp               172
10.2.1.141,8800                               169.254.170.227,65449                         tcp               156               17
10.2.1.12,14722                               10.2.1.141,8800                               tcp               156               8
google-public-dns-a.google.com,domain         10.2.1.141,58180                              udp               142
10.2.1.141,8800                               10.2.1.22,65461                               tcp               132
```

- **apply** command

> This has the same function as the “Apply Changes” button in interface.

- apply –a, this command implements definitions pending to be implemented
- apply –cf, this command enables desired rule to be implemented.
- apply -fa, this command applies all definitions again.

For example, the following figure shows that we have re-implemented DNS settings.



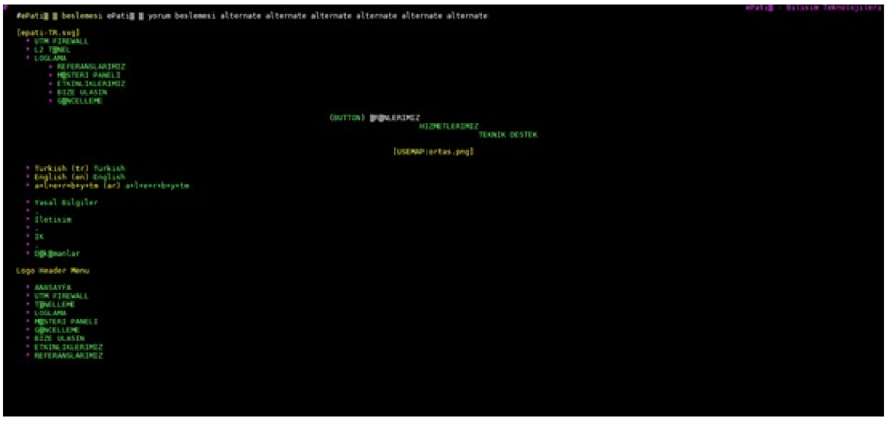
```
yonetici:~$ apply -fa
```

- uygula –fa, This command re-implements all commands in Antikor.

- uygula –la, This command provides information on status of services.

- **webBrowser** command

> This is the command to open all web services over the console. Epati Information Technologies’s web site at www2.epati.com.tr has been accessed over the console.



```
#ePati█ █ beslemesi ePati█ █ yorum beslemesi alternate alternate alternate alternate alternate alternate          ePati█ - Bilisim Teknolojileri

[epati-TR.svg]
  * UTM FIREWALL
  * L2 T█NEL
  * LOGLAMA
       + REFERANSLARIMIZ
       + M█STERI PANELI
       + ETKINLIKLERIMIZ
       + BIZE ULASIN
       + G█NCELLEME

                                               (BUTTON) █R█NLERIMIZ
                                                            HIZMETLERIMIZ
                                                                   TEKNIK DESTEK

                                                          [USEMAP:ortas.png]

  * Turkish (tr) Turkish
  * English (en) English
  * [illegible] (ar) [illegible]

  * Yasal Bilgiler
  * .
  * Iletisim
  * .
  * IK
  * .
  * D█k█manlar

Logo Header Menu

  * ANASAYFA
  * UTM FIREWALL
  * T█NELLEME
  * LOGLAMA
  * M█STERI PANELI
  * G█NCELLEME
  * BIZE ULASIN
  * ETKINLIKLERIMIZ
  * REFERANSLARIMIZ
```

- **reboot** command

> This command is used to restart Antikor from a remote site.

- **?** command

> This command prompts help menu and it has the same function as the “help”.