

epati

SSH User Guideline

Product: Antikor v2 - Layer2 Tunnel
Guides

SSH User Guideline

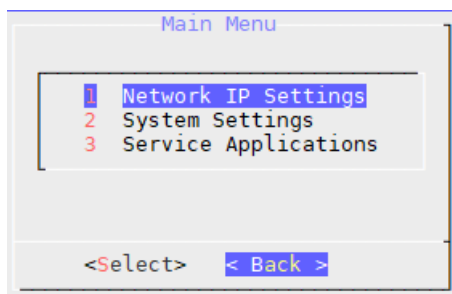
In order to log into Antikor as Administrator Putty program is used. We use Antikor’s internal IP in the event we access from inside the organization. Otherwise we use Antikor’s external IP if we access from outside the organization. Port number is 22022. The username is “admin” (Do not try port “22” 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:
Last login: Fri May 11 14:16:59 2018 from 10.2.4.16
=====
== ePati Information Technologies ==
==   Antikor v2 UTM Firewall   ==
=====
To list commands, type '?'.
yonetici:~$ ?
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
```

- **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:~$ bufferTemizle
pf disabled
485 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 follows:

```
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.
846AS27HS   # 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 shows 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
   Stripsize: 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.

- **eth-logs**

This command shows outputs of ethernet status logs.

- **interface** command

When we type Ethernet and hit Enter real-time 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
|-----|-----|-----|-----|
|   ix0:                  0.00 b/s                0.00 b/s                0.00 b/s
|   ix1:                 106.03 Mb/s              6.07 Mb/s              112.10 Mb/s
|   igb0:                 335.57 Kb/s              0.00 b/s               335.57 Kb/s
|   lo0:                 401.98 Kb/s             401.98 Kb/s            803.95 Kb/s
|   igb0.1003:            10.43 Kb/s              0.00 b/s               10.43 Kb/s
|   igb0.1004:             9.05 Kb/s              0.00 b/s               9.05 Kb/s
|   igb0.1006:             0.00 b/s                0.00 b/s                0.00 b/s
|   igb0.1008:           902.26 b/s                0.00 b/s              902.26 b/s
|   igb0.1009:           11.45 Kb/s              0.00 b/s              11.45 Kb/s
|   igb0.1010:             0.00 b/s                0.00 b/s                0.00 b/s
|   igb0.1011:           59.09 Kb/s              0.00 b/s              59.09 Kb/s
|   igb0.1013:           902.26 b/s                0.00 b/s              902.26 b/s
|   igb0.1015:             0.00 b/s                0.00 b/s                0.00 b/s
|   igb0.1018:             0.00 b/s                0.00 b/s                0.00 b/s
|   igb0.1019:           1.76 Kb/s                0.00 b/s               1.76 Kb/s
|   igb0.1007:           60.34 Kb/s              0.00 b/s              60.34 Kb/s
|   igb0.1020:             0.00 b/s                0.00 b/s                0.00 b/s
|   igb0.1012:           56.38 Kb/s              0.00 b/s              56.38 Kb/s
|   igb0.1017:             0.00 b/s                0.00 b/s                0.00 b/s
|   igb0.1014:             0.00 b/s                0.00 b/s                0.00 b/s
|   igb0.1005:          125.31 Kb/s              0.00 b/s             125.31 Kb/s
|   igb0.1021:             0.00 b/s                0.00 b/s                0.00 b/s
|-----|-----|-----|-----|
|   total:               107.07 Mb/s              6.47 Mb/s             113.54 Mb/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.

- **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:~$ █
```

- **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.

- **mac-table** command,

For show the mac address table.

- **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.

```
yoneticici:~$ 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 inquiry about Epati.

```
yoneticici:~$ 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.

Paket Sürüm Listesi		
Paket	Sürüm	Durum
Arayüz Modülü	2.0.40	Güncel
Araç Kutusu	2.0.15	Güncel
Yönetimsel Araçlar	2.0.11	Güncel
Yapılandırma Yöneticisi	2.0.28	Güncel
Haberleşme Modülü	2.0.58	Güncel
Haberleşme Aracısı	2.0.15	Güncel
Modül Yöneticisi	2.0.15	Güncel
Yönetici Konsolu	2.0.25	Güncel
Epati Network İşletim Sistemi	RC-2.0.9	Güncel

- **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.

- **port-stats** komutu,

For list the status of the ports.

```
PORT                RX-PKT      RX-BYTE      TX-PKS      TX-BYTE
tunel5:             74700706   6722525656   7126352021  1747852198131
tunel3:             37003446   4187978025   19304333082 3025363782890
tunel6:             110177399  11648916490  7737212759  3608448061572
tunel2:             42809873   5470227763   7876080710  3127184625991
ens1f0:             37641748760 27742468378103 872271344 97744504793
tunel7:             616228748 57183021841 10036985854 6406654788286
tunel4:             125400739 17175017582 10002768352 6973935411495
tunel1:             1062949334 85281777212 13142597236 8768754174723
```

- **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 command 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
tunel-omurga	Tünel Omurga Motoru	Çalışıyor
routing	Layer3 Yönlendirme	Kapalı
snmp-servisi	SNMP Servisi	Kapalı

- **ssh** command

This is a protocol used for a remote connection.

- **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
```

- **switch-list** command,

Shows the list of switches.

- **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
09:14:46.479912 IP 10.2.1.12.1415 > 10.2.1.141.22022: Flags [.], ack 240, win 2052, 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 10.2.1.12.1415 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.

- **apply** command

This has the same function as the "Apply Changes" button in interface.

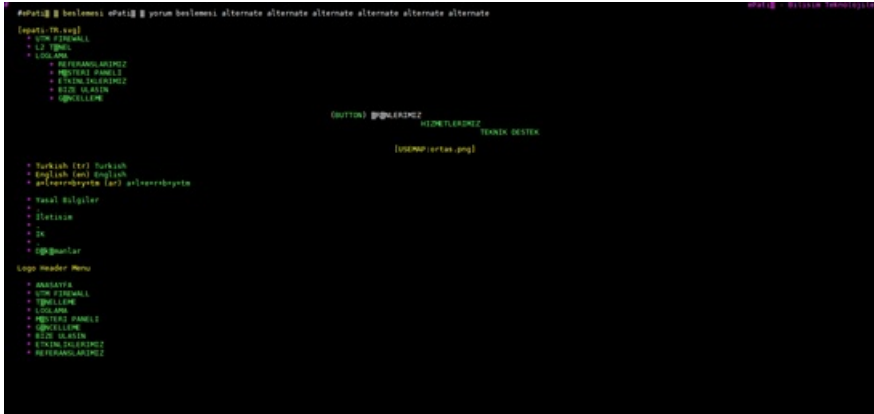
- apply -a, This command implements definitions pending to be implemented
- apply -cf, This command enables desired rule to be implemented.

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.



- **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".

ePati Cyber Security Technologies Inc.
 Mersin Universitesi Ciftlikkoy Kampusu
 Teknopark Idari Binasi Kat: 4 No: 411
 Zip Code: 33343 Yenisehir / MERSIN / TURKIYE

 www.epati.com.tr
 info@epati.com.tr
 +90 324 361 02 33
 +90 324 361 02 39

