[FortiGate] Summary of various status confirmation commands in CLI

FortiGate Basics:

Introduction:

FortiGate NGFWs enable security-driven networking and consolidate industry-leading security capabilities such as intrusion prevention system (IPS), web filtering, secure sockets layer (SSL) inspection, and automated threat protection.

Fortinet NGFWs meet the performance needs of highly scalable, hybrid IT architectures, enabling organizations to reduce complexity and manage security risks.

Some of Fortinet UTM Features:
- Security Profiles
- Traffic inspection
- IPS & IDS
- VPN
- Suspicious traffic attributes
- Application control
- AntiVirus
- FortiGuard Web Filtering
- Email filter
- Advance Threat Protection
- Web filtering
- Email filtering
- SD-WAN
-Vulnerability Assessment
-Switch & Wifi Controller

Model used

- FortiGate 60E
  - version 6.2.x

System related

get system status

- Display various system information

```
# get system status
Version: FortiGate-60E v6.2.4,build1112,200511 (GA)
Virus-DB: 1.00000(2018-04-09 18:07)
Extended DB: 1.00000(2018-04-09 18:07)
IPS-DB: 6.00741(2015-12-01 02:30)
IPS-ETDB: 0.00000(2001-01-01 00:00)
APP-DB: 15.00897(2020-07-29 03:26)
INDUSTRIAL-DB: 6.00741(2015-12-01 02:30)
Serial-Number: FGT60ETKxxxxxxxx
IPS Malicious URL Database: 2.00729(2020-08-07 07:31)
Botnet DB: 1.00000(2012-05-28 22:51)
BIOS version: 05000012
System Part-Number: P18816-03
Log hard disk: Not available
Hostname: FW01
Operation Mode: NAT
Current virtual domain: root
Max number of virtual domains: 10
Virtual domains status: 1 in NAT mode, 0 in TP mode
Virtual domain configuration: disable
FIPS-CC mode: disable
Current HA mode: a-p, master
Cluster uptime: 1 days, 3 hours, 44 minutes, 43 seconds
Cluster state change time: 2020-08-07 18:49:10
Branch point: 1112
Release Version Information: GA
System time: Sat Aug  8 15:37:10 2020
Copy
```

get system performance status

- View performance information such as resource usage

```
# get system performance status
CPU states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU0 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU1 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU2 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU3 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 1911268k total, 578572k used (30.3%), 1272712k free (66.6%), 59984k
freeable (3.1%)
Average network usage: 40 / 49 kbps in 1 minute, 890 / 885 kbps in 10 minutes, 414
/ 409 kbps in 30 minutes
Average sessions: 116 sessions in 1 minute, 123 sessions in 10 minutes, 103
sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per
second in last 10 minutes, 0 sessions per second in last 30 minutes
```

```
Average NPU sessions: 50 sessions in last 1 minute, 60 sessions in last 10
minutes, 48 sessions in last 30 minutes
Average nTurbo sessions: 0 sessions in last 1 minute, 0 sessions in last 10
minutes, 0 sessions in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 0 days,  23 hours,  42 minutes
Copy
```

Hardware related

get hardware status

- Display various hardware information

```
# get hardware status
Model name: FortiGate-60E
ASIC version: SOC3
ASIC SRAM: 64M
CPU: ARMv7
Number of CPUs: 4
RAM: 1866 MB
EMMC: 3662 MB(MLC) /dev/mmcblk0
Hard disk: not available
USB Flash: not available
Network Card chipset: FortiASIC NP6LITE Adapter (rev.)
Copy
```

Time related

execute time

- Show current time
- Shows last NTP sync time

```
# execute time
current time is: 15:02:56
```

```
last ntp sync:Sat Aug  8 14:49:25 2020
Copy
```

get system ntp

- Show NTP settings

```
# get system ntp
ntpsync             : enable
type                : fortiguard
syncinterval        : 60
source-ip           : 0.0.0.0
source-ip6          : ::
server-mode         : enable
authentication      : disable
interface           : "VLAN30" "VLAN50" "VLAN60" "VLAN40" "VLAN10"
Copy
```

diagnose sys ntp status

- Show NTP server status

```
# diagnose sys ntp status
HA master: yes, HA master ip: 169.254.0.1, management_vfid: 0 ha_direct=1,
ha_mgmt_vfid=1
synchronized: yes, ntpsync: enabled, server-mode: enabled

ipv4 server(ntp1.fortiguard.com) 208.91.113.70 -- reachable(0xff) S:1 T:54
        server-version=4, stratum=2
        reference time is e2d8bb75.8480a029 -- UTC Sat Aug  8 05:49:41 2020
        clock offset is 0.025183 sec, root delay is 0.000092 sec
        root dispersion is 0.011795 sec, peer dispersion is 216 msec

ipv4 server(ntp2.fortiguard.com) 208.91.114.23 -- reachable(0xfb) S:1 T:104
        server-version=4, stratum=2
        reference time is e2d8bb80.63241def -- UTC Sat Aug  8 05:49:52 2020
        clock offset is 0.021793 sec, root delay is 0.000107 sec
        root dispersion is 0.012390 sec, peer dispersion is 1399 msec

ipv4 server(ntp2.fortiguard.com) 208.91.113.71 -- reachable(0xff) S:1 T:18
selected
        server-version=4, stratum=2
        reference time is e2d8bb44.5be013 -- UTC Sat Aug  8 05:48:52 2020
        clock offset is 0.025585 sec, root delay is 0.000092 sec
        root dispersion is 0.012115 sec, peer dispersion is 415 msec

ipv4 server(ntp1.fortiguard.com) 208.91.114.98 -- reachable(0xff) S:1 T:15
        server-version=4, stratum=2
        reference time is e2d8bb8a.bd7757f0 -- UTC Sat Aug  8 05:50:02 2020
        clock offset is 0.023176 sec, root delay is 0.000137 sec
        root dispersion is 0.011032 sec, peer dispersion is 320 msec
Copy
```

Interface related

get system interface physical

- Display the status of each interface such as up / down, speed, duplex, etc.

```
# get system interface physical
== [onboard]
        ==[dmz]
                mode: static
                ip: 0.0.0.0 0.0.0.0
                ipv6: ::/0
                status: down
                speed: n/a
        ==[internal1]
                mode: static
                ip: 0.0.0.0 0.0.0.0
                ipv6: ::/0
                status: up
                speed: 100Mbps (Duplex: full)
        ==[internal2]
                mode: static
                ip: 0.0.0.0 0.0.0.0
                ipv6: ::/0
                status: down
                speed: n/a
        ==[internal3]
                mode: static
                ip: 0.0.0.0 0.0.0.0
                ipv6: ::/0
                status: down
                speed: n/a
        ==[internal4]
                mode: static
                ip: 0.0.0.0 0.0.0.0
                ipv6: ::/0
                status: down
                speed: n/a
        ==[internal5]
                mode: static
                ip: 10.1.10.254 255.255.255.0
                ipv6: ::/0
                status: up
                speed: 100Mbps (Duplex: full)
#略
Copy
```

get hardware nic <port>

- Shows the state and statistics of the specified interface

```
# get hardware nic internal1
Description     :FortiASIC NP6LITE Adapter
```

```
Driver Name     :FortiASIC NP6LITE Driver
Board           :60E
lif id          :3
lif oid         :67
netdev oid      :67
tx group        :0
Current_HWaddr   00:09:0f:09:00:03
Permanent_HWaddr e8:1c:ba:ec:5e:e1
========== Link Status ==========
Admin           :up
netdev status   :up
autonego_setting:1
link_setting    :0
speed_setting   :10
duplex_setting  :0
Speed           :100
Duplex          :Full
link_status     :Up
============ Counters ===========
Rx Pkts         :36499273
Rx Bytes        :6739209314
Tx Pkts         :55609593
Tx Bytes        :62790039477
Host Rx Pkts    :9950463
Host Rx Bytes   :1763170780
Host Tx Pkts    :1554815
Host Tx Bytes   :268492979
Host Tx dropped :0
FragTxCreate    :0
FragTxOk        :0
FragTxDrop      :0
Copy
```

diagnose hardware deviceinfo nic <port>

- Shows the state and statistics of the specified interface
- Exactly the same output as `get hardware nic <port>`

```
# diagnose hardware deviceinfo nic internal1
Description     :FortiASIC NP6LITE Adapter
Driver Name     :FortiASIC NP6LITE Driver
Board           :60E
lif id          :3
lif oid         :67
netdev oid      :67
tx group        :0
Current_HWaddr   00:09:0f:09:00:03
Permanent_HWaddr e8:1c:ba:ec:5e:e1
========== Link Status ==========
Admin           :up
```

```
netdev status   :up
autonego_setting:1
link_setting    :0
speed_setting   :10
duplex_setting  :0
Speed           :100
Duplex          :Full
link_status     :Up
============ Counters ===========
Rx Pkts         :1444261
Rx Bytes        :219738338
Tx Pkts         :2841449
Tx Bytes        :3330430470
Host Rx Pkts    :489552
Host Rx Bytes   :34587523
Host Tx Pkts    :87910
Host Tx Bytes   :7659907
Host Tx dropped :0
FragTxCreate    :0
FragTxOk        :0
FragTxDrop      :0
Copy
```

arp information

get system arp

- Show arp table

```
FW01 # get system arp
Address           Age(min)   Hardware Addr      Interface
192.168.179.1     0          6c:e4:da:e7:07:5c wan1
10.1.10.3         0          84:af:ec:74:b8:6f VLAN10
10.1.10.2         4          ac:17:c8:5b:4d:65 VLAN10
Copy
```

diagnose ip arp list

- Show arp table

```
FW01 # diagnose ip arp list
index=20 ifname=VLAN10 10.1.10.254 e8:1c:ba:ec:5e:e5 state=00000004 use=19100
confirm=22129 update=18615 ref=0
index=5 ifname=wan1 192.168.179.1 6c:e4:da:e7:07:5c state=00000004 use=758
confirm=2350 update=171 ref=80
index=20 ifname=VLAN10 10.1.10.4 state=00000020 use=804285 confirm=827248
update=803985 ref=1
index=20 ifname=VLAN10 10.1.10.3 84:af:ec:74:b8:6f state=00000002 use=100
confirm=95 update=6022 ref=69
index=20 ifname=VLAN10 10.1.10.2 ac:17:c8:5b:4d:65 state=00000004 use=5144
confirm=9361 update=928 ref=3
```

```
Copy
```

HA relationship

get system ha

- Display HA setting status

```
FW01 # get system ha
group-id              : 0
group-name            : HA-Group
mode                  : a-p
sync-packet-balance   : disable
password              : *
hbdev                 : "internal6" 200 "internal7" 100
session-sync-dev      :
route-ttl             : 10
route-wait            : 0
route-hold            : 10
multicast-ttl         : 600
sync-config           : enable
encryption            : disable
authentication        : enable
hb-interval           : 2
hb-lost-threshold     : 6
hello-holddown        : 20
gratuitous-arps       : enable
arps                  : 5
arps-interval         : 8
session-pickup        : enable
session-pickup-connectionless: disable
session-pickup-expectation: disable
session-pickup-delay: disable
link-failed-signal    : disable
uninterruptible-upgrade: enable
ha-mgmt-status        : enable
ha-mgmt-interfaces:
    == [ 1 ]
    id:     1
ha-eth-type           : 8890
hc-eth-type           : 8891
l2ep-eth-type         : 8893
ha-uptime-diff-margin: 300
vcluster2             : disable
vcluster-id           : 1
override              : enable
priority              : 200
override-wait-time    : 0
monitor               : "internal1" "wan1"
pingserver-monitor-interface:
vdom                  : "root"
ha-direct             : enable
ssd-failover          : disable
memory-compatible-mode: disable
```

```
inter-cluster-session-sync: disable
logical-sn          : disable
Copy
```

get system ha status

- Show HA status

```
FW01 # get system ha status
HA Health Status: OK
Model: FortiGate-60E
Mode: HA A-P
Group: 0
Debug: 0
Cluster Uptime: 0 days 2:41:55
Cluster state change time: 2020-08-07 12:13:40
Master selected using:
    <2020/08/07 12:13:40> FGT60ETKxxxxxxxx is selected as the master because it
has the largest value of override priority.
    <2020/08/07 11:52:10> FGT60ETKxxxxxxxx is selected as the master because it's
the only member in the cluster.
ses_pickup: enable, ses_pickup_delay=disable
override: enable
Configuration Status:
    FGT60ETKxxxxxxxx(updated 2 seconds ago): in-sync
    FGT60ETKyyyyyyyy(updated 2 seconds ago): in-sync
System Usage stats:
    FGT60ETKxxxxxxxx(updated 2 seconds ago):
        sessions=71, average-cpu-user/nice/system/idle=0%/0%/0%/99%, memory=31%
    FGT60ETKyyyyyyyy(updated 2 seconds ago):
        sessions=27, average-cpu-user/nice/system/idle=0%/0%/0%/100%, memory=32%
HBDEV stats:
    FGT60ETKxxxxxxxx(updated 2 seconds ago):
        internal6: physical/1000auto, up, rx-
bytes/packets/dropped/errors=22031628/66675/0/0, tx=39667019/70366/0/0
        internal7: physical/1000auto, up, rx-
bytes/packets/dropped/errors=18560694/46359/0/0, tx=18712447/45415/0/0
    FGT60ETKyyyyyyyy(updated 2 seconds ago):
        internal6: physical/1000auto, up, rx-
bytes/packets/dropped/errors=38350647/67170/0/0, tx=20728120/62466/0/0
        internal7: physical/1000auto, up, rx-
bytes/packets/dropped/errors=17396561/42221/0/0, tx=17262772/42219/0/0
MONDEV stats:
    FGT60ETKxxxxxxxx(updated 2 seconds ago):
        internal1: physical/100auto, up, rx-
bytes/packets/dropped/errors=27134716/142668/0/0, tx=88164022/134514/0/0
        wan1: physical/100auto, up, rx-
bytes/packets/dropped/errors=68478268/101399/0/0, tx=12222874/69742/0/0
    FGT60ETKyyyyyyyy(updated 2 seconds ago):
        internal1: physical/100auto, up, rx-
bytes/packets/dropped/errors=3528048/35145/0/0, tx=0/0/0/0
        wan1: physical/100auto, up, rx-
bytes/packets/dropped/errors=1264451/3661/0/0, tx=88132/487/0/0
Master: FW01            , FGT60ETKxxxxxxxx, HA cluster index = 1
Slave : FW02            , FGT60ETKyyyyyyyy, HA cluster index = 0
number of vcluster: 1
vcluster 1: work 169.254.0.2
```

```
Master: FGT60ETKxxxxxxxx, HA operating index = 0
Slave : FGT60ETKyyyyyyyyy, HA operating index = 1
Copy
```

Link monitor related

diagnose sys link-monitor status all

- Display the status of the monitor target

```
# diagnose sys link-monitor status all

Link Monitor: 1, Status: alive, Server num(1), Create time: Sat Dec 28 08:52:08
2019
Source interface: VLAN50 (23)
Interval: 1
  Peer: 192.168.179.1(192.168.179.1)
        Source IP(10.1.50.1)
        Route: 10.1.50.1->192.168.179.1/32, gwy(10.1.50.254)
        protocol: ping, state: alive
                Latency(Min/Max/Avg): 1.971/28.514/3.938 ms
                Jitter(Min/Max/Avg): 0.002/23.504/2.436
                Packet lost: 0.000%
                Number of out-of-sequence packets: 2081298
                Fail Times(0/1)
                Packet sent: 3265569, received: 2146619, Sequence(sent/rcvd/exp):
54306/54306/65536
Copy
```

Routing relationship

get router info routing-table all

- View all of the routing table

```
# get router info routing-table all

Routing table for VRF=0
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

S*      0.0.0.0/0 [10/0] via 192.168.179.1, wan1
C       10.1.10.0/24 is directly connected, VLAN10
                     is directly connected, VLAN10
C       10.1.20.0/24 is directly connected, VLAN20
```

```
C       10.1.30.0/24 is directly connected, VLAN30
C       192.168.179.0/24 is directly connected, wan1
Copy
```

- `get router info routing-table <option>`
  - The routing table for each protocol can be displayed by changing the `option` part.

```
# get router info routing-table
details      show routing table details information
all          show all routing table entries
rip          show rip routing table
ospf         show ospf routing table
bgp          show bgp routing table
isis         show isis routing table
static       show static routing table
connected    show connected routing table
database     show routing information base
Copy
```

OSFP related

get router info ospf neighbor

- Show neighbor information

```
# get router info ospf neighbor

OSPF process 0, VRF 0:
Neighbor ID     Pri   State           Dead Time   Address         Interface
10.200.30.2       1   Full/DR         00:00:35    10.10.2.2       wan1
Copy
```

get router info ospf route

- Show OSPF routes

```
# get router info ospf route

OSPF process 0:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

C  10.10.2.0/30 [1] is directly connected, wan1, Area 0.0.0.0
E2 10.10.3.0/24 [1/20] via 10.10.2.2, wan1
E2 10.200.30.2/32 [1/20] via 10.10.2.2, wan1
Copy
```

Other commands

```
# get router info ospf
database          show ospf database information
interface         show ospf interfaces
route             show ospf routing table
neighbor          show ospf neighbors
border-routers    show ospf border routers
status            show ospf status
virtual-links     show ospf virtual links
Copy
```

BGP relationship

get router info bgp summary

- View BGP summary

```
# get router info bgp summary
BGP router identifier 10.10.2.1, local AS number 1
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down
State/PfxRcd
10.10.2.2       4          1      34      35        1    0    0 00:28:41        1

Total number of neighbors 1
Copy
```

get router info bgp network

- View BGP table

```
# get router info bgp network
BGP table version is 2, local router ID is 10.10.2.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight RouteTag Path
*> 10.10.1.0/24     0.0.0.0                  100  32768        0 i
*>i10.10.3.0/24     10.10.2.2                0    100      0        0 i
```

```
Total number of prefixes 2
Copy
```

Other commands

```
# get router info bgp
attribute-info              list all bgp attribute information
cidr-only                   display routes with non-natural netmasks
community                   display routes matching the communities
community-info              list all bgp community information
community-list              display routes matching the community-list
dampening                   display router dampening infomation
filter-list                 display routes conforming to the filter-list
inconsistent-as             display routes with inconsistent AS Paths
neighbors                   show BGP neighbors
network                     show BGP info for network
network-longer-prefixes     show BGP info for route and more specific routes
paths                       path information
prefix-list                 display routes conforming to the prefix-list
regexp                      display routes matching the AS path regular expression
quote-regexp                display routes matching the AS path "regular
expression"
route-map                   display routes conforming to the route-map
scan                        display BGP scan status
summary                     summary of BGP neighbor status
memory                      BGP memory table
Copy
```

NAT relationship

get system session list

- View NAT table

```
# get system session list
PROTO   EXPIRE SOURCE           SOURCE-NAT       DESTINATION      DESTINATION-NAT
icmp    58     10.10.1.10:1     10.10.3.250:60417 10.10.3.10:8     -
igmp    345    10.10.10.1:0     -                 224.0.0.22:0     -
tcp     3599   10.10.1.10:52627 -                 10.10.1.254:22   -
Copy
```

VPN related

get vpn ipsec tunnel summary

- View IPsec tunnel status summary

```
# get vpn ipsec tunnel summary
'hogeVPN' 200.1.1.2:0  selectors(total,up): 1/1  rx(pkt,err): 1/0  tx(pkt,err):
6/3
Copy
```

get vpn ipsec tunnel details

- View IPsec tunnel status details

```
# get vpn ipsec tunnel details

gateway
  name: 'hogeVPN'
  type: route-based
  local-gateway: 200.1.1.1:0 (static)
  remote-gateway: 200.1.1.2:0 (static)
  mode: ike-v1
  interface: 'wan2' (6)
  rx  packets: 1  bytes: 112  errors: 0
  tx  packets: 6  bytes: 360  errors: 3
  dpd: on-demand/negotiated  idle: 20000ms  retry: 3  count: 0
  selectors
    name: 'hogeVPN'
    auto-negotiate: disable
    mode: tunnel
    src: 0:10.10.1.0/255.255.255.0:0
    dst: 0:10.10.3.0/255.255.255.0:0
    SA
      lifetime/rekey: 3600/939
      mtu: 1446
      tx-esp-seq: 7
      replay: enabled
      inbound
        spi: b6d3bcf0
        enc:    3des  a4593314d86840877574ce505f3cb5a1da5dad776bcdcabd
        auth:   sha1  a17f6c017664fa6a9f04306451f1012af1290eb6
      outbound
        spi: 930527e7
        enc:    3des  2b0e04adf13362a39983efde93b753e2e7c2419e2ba45451
        auth:   sha1  0cbc298567e94e4e711582a2a1728c22dbb9f6cf
      NPU acceleration: encryption(outbound) decryption(inbound)
Copy
```

Log related

View local log

1. `execute log filter device <number>`
    - Specify the save location of the log to be displayed

        - 0: disk
        - 1: memory
        - 2: faz
        - 4: fds
2. `execute log filter view-lines <5-1000>`
    - Specify the number of log lines to display
3. `execute log filter category <number>`
    - Specify the log category to display
        - 16: netscan
        - 10: application control
        - 9: dlp
        - 6: content
        - 5: spam
        - 4: ids
        - 3: webfilter
        - 2: virus
        - 1: event
        - 0: traffic
4. `execute log display`
    - View log
5. `execute log filter reset`
    - Reset the settings in steps 1 to 3 above

Happy Learning…

Follow for more updates: https://www.linkedin.com/in/rakesh-sa-b2b664167

Thanks

Rakesh