FortiGate

设备常用维护命令手册

v1.2

版本时间	修改内容	版本编号	修改人员
2021-3-4	创建文档。	v1.0	白冰、刘康明
2021-3-4	增加硬件故障处理。	v1.1	白冰
2021-5-14	1、 更正 VLAN 配置显示的命令。 2、 增加 VDOM ID 的查看命令。	v1.2	白冰

目录

一、基本信息

1、 版本/序列号

```
# get system status
Version: FortiGate-3800D v6.0.7,build9227,201208 (GA)
Virus-DB: 1.00000(2018-04-09 18:07)
Extended DB: 1.00000(2018-04-09 18:07)
Extreme DB: 1.00000(2018-04-09 18:07)
IPS-DB: 6.00741(2015-12-01 02:30)
IPS-ETDB: 6.00741(2015-12-01 02:30)
APP-DB: 6.00741(2015-12-01 02:30)
INDUSTRIAL-DB: 6.00741(2015-12-01 02:30)
Serial-Number: FG380DTB19800450
IPS Malicious URL Database: 1.00001(2015-01-01 01:01)
Botnet DB: 1.00000(2012-05-28 22:51)
BIOS version: 05000011
System Part-Number: P19020-10
Log hard disk: Available
Hostname: SXXY-PSC-P9F2-3800D-1
Operation Mode: NAT
Current virtual domain: NAT
Max number of virtual domains: 10
Virtual domains status: 4 in NAT mode, 0 in TP mode
Virtual domain configuration: enable
FIPS-CC mode: disable
Current HA mode: a-p, master
Cluster uptime: 2 hours, 43 minutes, 48 seconds
Cluster state change time: 2021-03-02 11:27:55
Branch point: 0302
Release Version Information: GA
FortiOS x86-64: Yes
System time: Tue Mar  2 14:11:17 2021
```

2、 HA 状态

① 主备状态/优先级

```
# config global
# diagnose sys ha status
HA information
Statistics
        traffic.local = s:0 p:36 b:5039
        traffic.total = s:0 p:44 b:5367
        activity.ha_id_changes = 2
        activity.fdb  = c:0 q:0
Model=80007, Mode=2 Group=77 Debug=0
nvcluster=1, ses_pickup=0, delay=0
[Debug_Zone HA information]
HA group member information: is_manage_primary=1.
FGVM04TM21000013:       Primary, serialno_prio=1, usr_priority=120, hostname=FGT1-MASTER
FGVM04TM21000014:     Secondary, serialno_prio=0, usr_priority=100, hostname=FGT2-SLAVE
[Kernel HA information]
vcluster 1, state=work, primary_ip=169.254.0.2, primary_id=0:
FGVM04TM21000013:       Primary, ha_prio/o_ha_prio=0/0
FGVM04TM21000014:     Secondary, ha_prio/o_ha_prio=1/1
```

② 同步状态

```
# config global
# get sys ha status
HA Health Status: OK
Model: FortiGate-VM64-KVM
Mode: HA A-P
Group: 77
Debug: 0
Cluster Uptime: 0 days 0:4:49
Cluster state change time: 2021-03-02 14:48:16
Primary selected using:
    <2021/03/02 14:48:16> FGVM04TM21000013 is selected as the primary because it has the largest value of override priority.
    <2021/03/02 14:48:13> FGVM04TM21000013 is selected as the primary because it's the only member in the cluster.
ses_pickup: disable
override: disable
```

```
Configuration Status:
    FGVM04TM21000013(updated 3 seconds ago): in-sync
    FGVM04TM21000014(updated 4 seconds ago): in-sync
System Usage stats:
    FGVM04TM21000013(updated 3 seconds ago):
        sessions=5, average-cpu-user/nice/system/idle=0%/0%/3%/92%, memory=46%
    FGVM04TM21000014(updated 4 seconds ago):
        sessions=3, average-cpu-user/nice/system/idle=0%/0%/1%/95%, memory=45%
HBDEV stats:
    FGVM04TM21000013(updated 3 seconds ago):
        port7: physical/10000full, up, rx-bytes/packets/dropped/errors=1255440/5862/0/0, tx=1132417/3296/0/0
        port8: physical/10000full, up, rx-bytes/packets/dropped/errors=560384/1408/0/0, tx=579480/1431/0/0
    FGVM04TM21000014(updated 4 seconds ago):
        port7: physical/10000full, up, rx-bytes/packets/dropped/errors=1129768/3287/0/0, tx=1250336/5842/0/0
        port8: physical/10000full, up, rx-bytes/packets/dropped/errors=577455/1426/0/0, tx=557598/1401/0/0
MONDEV stats:
    FGVM04TM21000013(updated 3 seconds ago):
        port3: physical/10000full, up, rx-bytes/packets/dropped/errors=0/0/0/0, tx=2860/37/0/0
    FGVM04TM21000014(updated 4 seconds ago):
        port3: physical/10000full, up, rx-bytes/packets/dropped/errors=0/0/0/0, tx=0/0/0/0
Primary      : FGT1-MASTER       , FGVM04TM21000013, HA cluster index = 1
Secondary    : FGT2-SLAVE        , FGVM04TM21000014, HA cluster index = 0
number of vcluster: 1
vcluster 1: work 169.254.0.2
Primary: FGVM04TM21000013, HA operating index = 0
Secondary: FGVM04TM21000014, HA operating index = 1
```

③ 不同步恢复方法

a) 首先查看两端 checksum 是否一致。

```
# config global
# diagnose sys ha checksum show
is_manage_primary()=1, is_root_primary()=1
debugzone
global: 09 f1 70 b8 44 df 10 5d 09 21 8a c5 4a 1a 73 64
root: b5 ca 8d 95 7c 6e 2f c0 48 ac 33 35 3b a5 61 3f
WAN: 11 27 3a f5 c9 33 66 b1 c3 51 5f ab b2 38 ab ab
NAT: 09 84 ba cd 85 cc bb 14 20 0c bc c0 1d 42 74 d7
IPv6: 59 5c e2 c8 f3 ff 43 85 0c c8 4d 65 f9 3d e3 1f
all: b8 18 45 56 d7 c6 49 54 95 67 cc 38 d3 e2 7e 2b
checksum
global: 09 f1 70 b8 44 df 10 5d 09 21 8a c5 4a 1a 73 64
root: b5 ca 8d 95 7c 6e 2f c0 48 ac 33 35 3b a5 61 3f
WAN: 91 f7 aa fe b9 34 66 b1 c3 51 3e ab b1 88 eb ab
NAT: 09 84 ba cd 85 cc bb 14 20 0c bc c0 1d 42 74 d7
IPv6: 59 5c e2 c8 f3 ff 43 85 0c c8 4d 65 f9 3d e3 1f
all: c3 18 45 56 d7 c6 49 54 95 67 cc 38 43 22 7e 5f
```

b) 如果不一致，则在当前主设备上执行 dialog sys ha recalculate 进行同步。

```
# diagnose sys ha checksum recalculate
# diagnose sys ha checksum show
is_manage_primary()=1, is_root_primary()=1
debugzone
global: 09 f1 70 b8 44 df 10 5d 09 21 8a c5 4a 1a 73 64
root: b5 ca 8d 95 7c 6e 2f c0 48 ac 33 35 3b a5 61 3f
WAN: 91 f7 aa fe b9 34 66 b1 c3 51 3e ab b1 88 eb ab
NAT: 09 84 ba cd 85 cc bb 14 20 0c bc c0 1d 42 74 d7
IPv6: 59 5c e2 c8 f3 ff 43 85 0c c8 4d 65 f9 3d e3 1f
all: b8 18 45 56 d7 c6 49 54 95 67 cc 38 d3 e2 7e 2b
checksum
global: 09 f1 70 b8 44 df 10 5d 09 21 8a c5 4a 1a 73 64
root: b5 ca 8d 95 7c 6e 2f c0 48 ac 33 35 3b a5 61 3f
WAN: 91 f7 aa fe b9 34 66 b1 c3 51 3e ab b1 88 eb ab
NAT: 09 84 ba cd 85 cc bb 14 20 0c bc c0 1d 42 74 d7
IPv6: 59 5c e2 c8 f3 ff 43 85 0c c8 4d 65 f9 3d e3 1f
all: b8 18 45 56 d7 c6 49 54 95 67 cc 38 d3 e2 7e 2b
```

④ HA 切换命令，在当前主设备上执行：

```
# config global
# diagnose sys ha reset-uptime
```

3、 uptime 显示

```
# config global
# get system performance status
CPU states: 0% user 2% system 0% nice 94% idle 0% iowait 4% irq 0% softirq
CPU0 states: 0% user 2% system 0% nice 94% idle 0% iowait 4% irq 0% softirq
Memory: 2058360k total, 988656k used (48.0%), 821544k free (39.9%), 248160k freeable (12.1%)
Average network usage: 58 / 64 kbps in 1 minute, 63 / 56 kbps in 10 minutes, 58 / 61 kbps in 30 minutes
Average sessions: 35 sessions in 1 minute, 36 sessions in 10 minutes, 30 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
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 0 days,  0 hours,  30 minutes
```

二、硬件相关

1、 电源状态

```
# config global
# diagnose hardware deviceinfo psu
PSU[1]:
  Vendor                : Murata-PS
  Model                 : D1U54P-W-1200-12-HA4PC
  FW Revision           : 0801-1001-0000
  SN                    : DH1910RM005U
PSU[2]:
  Vendor                : Murata-PS
  Model                 : D1U54P-W-1200-12-HA4PC
  FW Revision           : 0000-1001-0000
  SN                    : DH1910RM00CG
```

2、 风扇状态、CPU 温度信息

```
# config global
# exe sensor list
 1 MB CPU0 VTT          alarm=0   value=0.992   threshold_status=0
 2 MB CPU1 VTT          alarm=0   value=0.992   threshold_status=0
 3 MB DDR3 VDQ AB       alarm=0   value=1.344   threshold_status=0
 4 MB DDR3 VDQ CD       alarm=0   value=1.344   threshold_status=0
 5 MB DDR3 VDQ EF       alarm=0   value=1.328   threshold_status=0
 6 MB DDR3 VDQ GH       alarm=0   value=1.344   threshold_status=0
 7 MB CP8 VCCK A        alarm=0   value=0.992   threshold_status=0
 8 MB CP8 VCCK B        alarm=0   value=0.992   threshold_status=0
 9 MB CP8 VCCK C        alarm=0   value=0.992   threshold_status=0
10 MB CP8 VCCK D        alarm=0   value=0.992   threshold_status=0
11 MB NCT7904D 3VDD     alarm=0   value=3.216   threshold_status=0
12 MB NCT7904D 3VSB     alarm=0   value=3.312   threshold_status=0
13 IO +12V              alarm=0   value=12.077   threshold_status=0
14 IO +3.3V             alarm=0   value=3.3024   threshold_status=0
15 IO +2.5V             alarm=0   value=2.5169   threshold_status=0
16 IO +1.2V             alarm=0   value=1.2157   threshold_status=0
17 IO VBAT              alarm=0   value=3.216   threshold_status=0
18 IO BCM56860 DVDD     alarm=0   value=1.0001   threshold_status=0
19 IO BCM56860 AVDD     alarm=0   value=1.0099   threshold_status=0
20 IO NCT7904D 3VDD     alarm=0   value=3.264   threshold_status=0
21 IO NCT7904D 3VSB     alarm=0   value=3.312   threshold_status=0
22 IO VDD CORE          alarm=0   value=0.992   threshold_status=0
23 IO VDD ANLG          alarm=0   value=0.992   threshold_status=0
24 IO P1V2              alarm=0   value=1.2   threshold_status=0
25 DTS CPU0             alarm=0   value=46   threshold_status=0
26 DTS CPU1             alarm=0   value=44   threshold_status=0
27 CPU0 Core 0          alarm=0   value=43   threshold_status=0
28 CPU0 Core 1          alarm=0   value=41   threshold_status=0
29 CPU0 Core 2          alarm=0   value=39   threshold_status=0
30 CPU0 Core 3          alarm=0   value=40   threshold_status=0
31 CPU0 Core 4          alarm=0   value=41   threshold_status=0
32 CPU0 Core 5          alarm=0   value=40   threshold_status=0
33 CPU0 Core 6          alarm=0   value=45   threshold_status=0
34 CPU0 Core 7          alarm=0   value=41   threshold_status=0
35 CPU0 Core 8          alarm=0   value=46   threshold_status=0
36 CPU0 Core 9          alarm=0   value=43   threshold_status=0
37 CPU1 Core 0          alarm=0   value=41   threshold_status=0
38 CPU1 Core 1          alarm=0   value=41   threshold_status=0
39 CPU1 Core 2          alarm=0   value=45   threshold_status=0
40 CPU1 Core 3          alarm=0   value=44   threshold_status=0
41 CPU1 Core 4          alarm=0   value=40   threshold_status=0
42 CPU1 Core 5          alarm=0   value=40   threshold_status=0
43 CPU1 Core 6          alarm=0   value=39   threshold_status=0
44 CPU1 Core 7          alarm=0   value=44   threshold_status=0
45 CPU1 Core 8          alarm=0   value=45   threshold_status=0
46 CPU1 Core 9          alarm=0   value=41   threshold_status=0
47 MB NCT7904D          alarm=0   value=40   threshold_status=0
48 IO NCT7904D          alarm=0   value=35   threshold_status=0
49 TD1                  alarm=0   value=43   threshold_status=0
50 TD2                  alarm=0   value=43   threshold_status=0
51 TD3                  alarm=0   value=32   threshold_status=0
52 TD4                  alarm=0   value=33   threshold_status=0
53 TS1                  alarm=0   value=40   threshold_status=0
```

```
54 TS2                  alarm=0   value=31    threshold_status=0
55 TS3                  alarm=0   value=32    threshold_status=0
56 TIR1                 alarm=0   value=42    threshold_status=0
57 Fan 1                alarm=0   value=3400    threshold_status=0
58 Fan 2                alarm=0   value=3200    threshold_status=0
59 Fan 3                alarm=0   value=3300    threshold_status=0
60 Fan 4                alarm=0   value=2600    threshold_status=0
61 Fan 5                alarm=0   value=2500    threshold_status=0
62 Fan 6                alarm=0   value=2600    threshold_status=0
63 Fan 7                alarm=0   value=2500    threshold_status=0
64 PS1 VIN              alarm=0   value=236    threshold_status=0
65 PS1 VOUT 12V         alarm=0   value=11.969    threshold_status=0
66 PS1 Temp 1           alarm=0   value=32    threshold_status=0
67 PS1 Temp 2           alarm=0   value=43    threshold_status=0
68 PS1 Fan 1            alarm=0   value=11264    threshold_status=0
69 PS1 Status           alarm=0
70 PS2 VIN              alarm=1   value=0    threshold_status=0x7
71 PS2 VOUT 12V         alarm=1   value=1.763    threshold_status=0x7
72 PS2 Temp 1           alarm=0   value=34    threshold_status=0
73 PS2 Temp 2           alarm=0   value=0    threshold_status=0
74 PS2 Fan 1            alarm=1   value=0    threshold_status=0x7
75 PS2 Status           alarm=1
76 DNP6-1-TIR1          alarm=0   value=39    threshold_status=0
77 DNP6-2-TIR1          alarm=0   value=39    threshold_status=0
78 DNP6-3-TIR1          alarm=0   value=39    threshold_status=0
79 DNP6-4-TIR1          alarm=0   value=39    threshold_status=0
80 TP2-TS1              alarm=0   (reading unavailable)
```

3、 CF 卡/硬盘状态、使用情况

```
# config global
# diagnose hardware deviceinfo disk
Disk SYSTEM(boot)                14.9GiB      type: SSD [ATA 16GB SATA Flash] dev: /dev/sda
   partition             247.0MiB, 178.0MiB free    mounted: N    label:    dev: /dev/sda1(boot) start: 1
   partition             247.0MiB, 178.0MiB free    mounted: Y    label:    dev: /dev/sda2(boot) start: 524289
   partition ref:    3   14.2GiB,    14.0GiB free    mounted: Y    label:    dev: /dev/sda3 start: 1048577
Disk HDD1                ref:   16 447.1GiB      type: SSD [ATA INTEL SSDSC2KB48] dev: /dev/sdb
   partition ref:   17 440.1GiB, 439.0GiB free    mounted: Y    label: LOGUSEDXE7671FAC dev: /dev/sdb1 start: 2048
Disk HDD2                ref:   32 447.1GiB      type: SSD [ATA INTEL SSDSC2KB48] dev: /dev/sdc
   partition ref:   33 125.4GiB, 124.9GiB free    mounted: N    label: WANOPTXXBF766E7F dev: /dev/sdc1 start: 2048
   partition ref:   34 127.4GiB, 127.4GiB free    mounted: N    label:    dev: /dev/sdc2 start: 267245568
   partition ref:   35 169.9GiB, 169.9GiB free    mounted: N    label:    dev: /dev/sdc3 start: 534489088
Total available disks: 3
Max SSD disks: 2   Available storage disks: 2
```

三、接口相关

1、 网络接口状态

```
# config global
# get system interface
== [ port1 ]
name: port1    status: up    type: physical    scan-botnet-connections: disable    src-check: enable    aggregate: To_FW
== [ port2 ]
name: port2    status: up    type: physical    scan-botnet-connections: disable    src-check: enable    aggregate: To_FW
== [ port3 ]
name: port3    mode: static    management-ip: 0.0.0.0 0.0.0.0    ip: 0.0.0.0 0.0.0.0    status: up    netbios-forward: disable    type: physical    netflow-sampler: disable    sflow-sampler: disable    scan-botnet-connections: disable    src-check: enable    mtu-override: disable    wccp: disable    drop-overlapped-fragment: disable    drop-fragment: disable
.....
== [ mgmt1 ]
name: mgmt1    management-ip: 0.0.0.0 0.0.0.0    ip: 10.186.6.12 255.255.255.0    status: up    netbios-forward: disable    type: physical    netflow-sampler: disable    sflow-sampler: disable    scan-botnet-connections: disable    src-check: enable    mtu-override: disable    wccp: disable    drop-overlapped-fragment: disable    drop-fragment: disable
.....
== [ To_FW ]
name: To_FW    mode: static    management-ip: 0.0.0.0 0.0.0.0    ip: 0.0.0.0 0.0.0.0    status: up    netbios-forward: disable    type: aggregate    netflow-sampler: disable    sflow-sampler: disable    scan-botnet-connections: disable    src-check: enable    mtu-override: disable    wccp: disable    drop-overlapped-fragment: disable    drop-fragment: disable
== [ ipv4_internal ]
name: ipv4_internal    mode: static    management-ip: 0.0.0.0 0.0.0.0    ip: 10.186.4.46 255.255.255.252    status: up    netbios-forward: disable    type: vlan    netflow-sampler: both    sflow-sampler: disable    scan-botnet-connections: disable    src-check: enable    mtu-override: disable    wccp: disable    drop-overlapped-fragment: disable    drop-fragment: disable
== [ ipv4_external ]
name: ipv4_external    mode: static    management-ip: 0.0.0.0 0.0.0.0    ip: 10.186.4.42 255.255.255.252    status: up    netbios-forward: disable    type: vlan    netflow-sampler: both    sflow-sampler: disable    scan-botnet-connections: disable    src-check: enable    mtu-override: disable    wccp: disable    drop-overlapped-fragment: disable    drop-fragment: disable
```

2、 接口丢包统计

```
# config global
# diagnose hardware deviceinfo nic port1 ( 接口名称 )
=Description        :FortiASIC NP6 Adapter
Driver Name         :FortiASIC Unified NPU Driver
Name                :np6_0
PCI Slot            :0000:05:00.0
irq                 :26
Board               :FGT3800D
SN                  :FG380DTB19800450
Major ID            :14
Minor ID            :0
lif id              :0
lif oid             :160
netdev oid          :160
netdev flags        :1b83
Current_HWaddr      00:09:0f:09:00:00
Permanent_HWaddr 04:d5:90:4b:27:d6
phy name            :port1
bank_id             :255
phy_addr            :0x40
lane                :0
flags               :244002
sw_port             :1
sw_np_port          :8
vid_phy[6]          :[0x02][0x00][0x00][0x00][0x00][0x00]
vid_fwd[6]          :[0x00][0x00][0x00][0x00][0x00][0x00]
oid_fwd[6]          :[0x00][0x00][0x00][0x00][0x00][0x00]
========== Link Status ==========
Admin               :up
netdev status       :down
autonego_setting:0
link_setting        :1
link_speed          :100000
link_duplex         :1
Speed               :0
Duplex              :Half
link_status         :Down
rx_link_status      :0
int_phy_link        :0
```

```
local_fault       :0
local_warning     :0
remote_fault      :0
============ Counters ===========
Rx_Internal_Mac_Errors:0
Rx_CRC_Errors     :0
rx_carrier        :0
Rx_Frame_Too_Longs:0
rx_undersize      :0
tx_collision      :0
Rx Pkts           :0
Rx Bytes          :0
Tx Pkts           :0
Tx Bytes          :0
Host Rx Pkts      :0
Host Rx Bytes     :0
Host Tx Pkts      :0
Host Tx Bytes     :0
Host Tx dropped :0
FragTxCreate      :0
FragTxOk          :0
FragTxDrop        :0
sw_rx_pkts        :0
sw_rx_bytes       :0
sw_tx_pkts        :0
sw_tx_bytes       :0
sw_rx_mc_pkts     :0
sw_rx_bc_pkts     :0
sw_in_drop_pkts :0
sw_out_drop_pkts:0
```

3、 光口收发光情况

```
# config global
# get sys interface transceiver
Interface port9 - SFP/SFP+
   Vendor Name   :                FINISAR CORP.
   Part No.      :                FTLX8574D3BCL
   Serial No.    :                A2MB1UC
Interface port10 - SFP/SFP+
   Vendor Name   :                FINISAR CORP.
   Part No.      :                FTLX8574D3BCL
   Serial No.    :                A2MB1UE
Interface port11 - SFP/SFP+
   Vendor Name   :                FINISAR CORP.
   Part No.      :                FTLX8574D3BCL
   Serial No.    :                A2MB1T5
Interface port12 - SFP/SFP+
   Vendor Name   :                FINISAR CORP.
   Part No.      :                FTLX8574D3BCL
   Serial No.    :                A2MB1UK
                                                 Optical        Optical        Optical
SFP/SFP+       Temperature   Voltage        Tx Bias        Tx Power       Rx Power
Interface      (Celsius)     (Volts)        (mA)           (dBm)          (dBm)
-------------- ------------- -------------- -------------- -------------- --------------
port9          35.8          3.35           8.95           -2.6           -3.3
port10         36.2          3.36           8.98           -2.6           -3.9
port11         35.1          3.37           8.94           -2.7           -3.3
port12         35.8          3.34           8.92           -2.7           -3.1
   ++ : high alarm, + : high warning, - : low warning, -- : low alarm, ? : suspect.
```

4、 聚合口状态

```
# config vdom
# edit root
# diagnose netlink aggregate list
List of 802.3ad link aggregation interfaces:
 1   name To_FW                  status down      algorithm L4   lacp-mode active
```

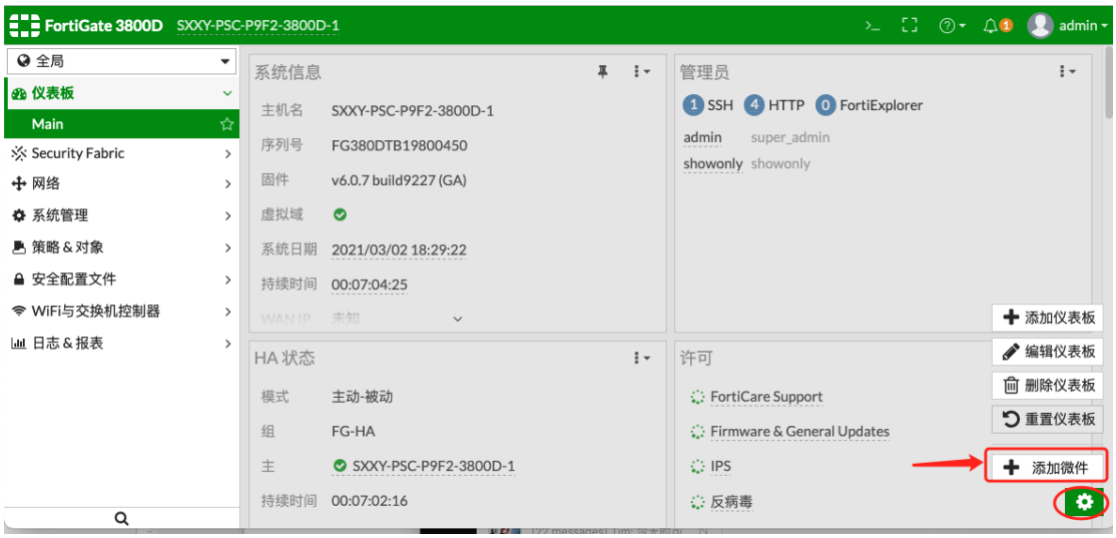
5、 VLAN 配置

```
# config vdom
# edit root
# diagnose sys vlan list
```

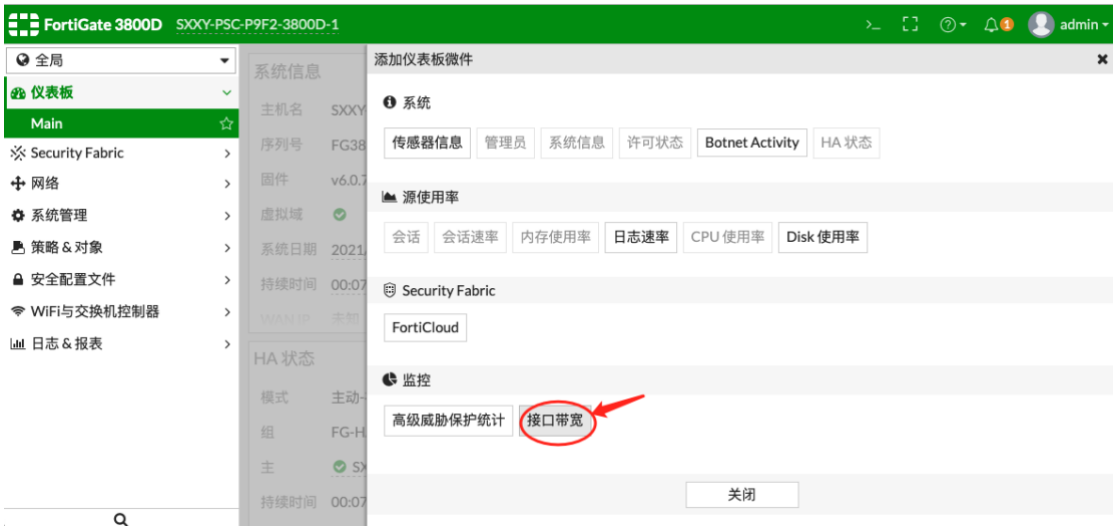
```
total vlan malloc times=0
list vlan info
To_FW ipv6_external vid=006c
To_FW ipv6_internal vid=006e
To_FW ipv4_external vid=006b
To_FW ipv4_internal vid=006d
```

6、 接口带宽利用率

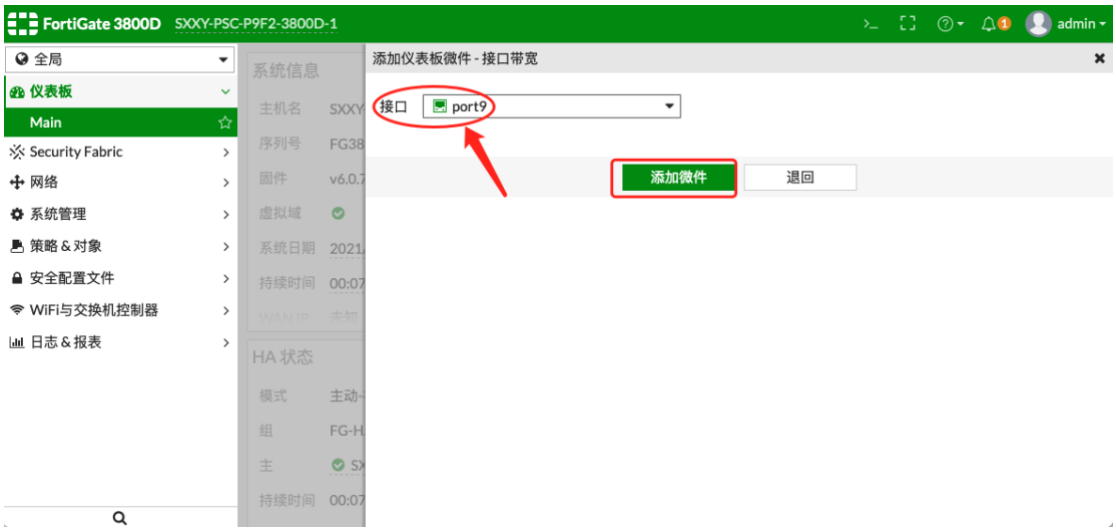
① 添加接口微件，点击仪表盘右下角的齿轮图标，点击添加微件。



② 选择监控→接口带宽。



③ 选择要监控带宽的接口，然后点击添加微件。



④ 在仪表盘上，查看该微件，图形化显示接口带宽，简单直观。

7、 ARP 表

```
# config vdom
# edit root
# get system arp
Address          Age(min)    Hardware Addr        Interface
192.168.15.2     1           aa:bb:cc:80:a0:00 vlan15
192.168.16.2     1           aa:bb:cc:80:10:00 vlan16
169.254.0.1      -           50:00:00:04:00:06 port7
```

8、 手工端口 down/up 操作

```
# config vdom
# edit root
# config system interface
# edit port1（接口名称）
# set status down
# set status up
# end
```

四、性能相关

1、 CPU/内存/吞吐量/会话状态

```
# config global
# 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
CPU4 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU5 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU6 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU7 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU8 states: 7% user 0% system 0% nice 93% idle 0% iowait 0% irq 0% softirq
CPU9 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU10 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU11 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU12 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU13 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU14 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU15 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU16 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU17 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU18 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU19 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU20 states: 9% user 1% system 0% nice 90% idle 0% iowait 0% irq 0% softirq
CPU21 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU22 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU23 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU24 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU25 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU26 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU27 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU28 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU29 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU30 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU31 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU32 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU33 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU34 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU35 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU36 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU37 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU38 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU39 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 132107524k total, 13362652k used (10.1%), 118589048k free (89.8%), 155824k freeable (0.1%)
Average network usage: 36 / 0 kbps in 1 minute, 38 / 6 kbps in 10 minutes, 37 / 7 kbps in 30 minutes
Average sessions: 7 sessions in 1 minute, 8 sessions in 10 minutes, 8 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: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 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,  5 hours,  44 minutes
```

2、 进程 top 状态

```
# config global
# diagnose sys top
Run Time:  0 days, 5 hours and 48 minutes
1U, 0N, 0S, 99I, 0WA, 0HI, 0SI, 0ST; 129011T, 115809F
             garpd       458       R       50.0       0.0     22
         bcm.user        338       S <      7.9       0.0     8
        forticron       433       S        0.4       0.0     2
          reportd       438       S        0.0       0.8     0
          miglogd       423       S        0.0       0.2     39
          miglogd       500       S        0.0       0.2     39
          miglogd       508       S        0.0       0.2     36
          miglogd       507       S        0.0       0.2     31
          miglogd       510       S        0.0       0.2     30
          miglogd       503       S        0.0       0.2     38
```

```
        miglogd     514     S       0.0     0.2     36
        miglogd     501     S       0.0     0.2     37
        miglogd     502     S       0.0     0.2     38
        miglogd     505     S       0.0     0.2     33
        miglogd     515     S       0.0     0.2     36
        miglogd     509     S       0.0     0.2     29
        miglogd     513     S       0.0     0.2     28
        miglogd     504     S       0.0     0.2     34
        miglogd     506     S       0.0     0.2     34
        miglogd     511     S       0.0     0.2     30
```
（键入 shift+P 以 CPU 占用排序，键入 shift+M 以内存占用排序）

五、会话相关

1、 VDOM ID 查看

```
# config global
# diagnose sys vd list | grep index
sname=root/root index=0 enabled fib_ver=25 use=83 rt_num=1 asym_rt=0 sip_helper=0, sip_nat_trace=1, mc_fwd=0, mc_ttl_nc=0, tpmc_sk_pl=0
name=vpn1004/vpn1004 index=1 enabled fib_ver=4 use=43 rt_num=0 asym_rt=0 sip_helper=0, sip_nat_trace=1, mc_fwd=0, mc_ttl_nc=0, tpmc_sk_pl=0
name=FG-traffic/FG-traffic index=2 enabled fib_ver=4 use=43 rt_num=0 asym_rt=0 sip_helper=0, sip_nat_trace=1, mc_fwd=0, mc_ttl_nc=0, tpmc_sk_pl=0
name=vpn1003/vpn1003 index=3 enabled fib_ver=4 use=43 rt_num=0 asym_rt=0 sip_helper=0, sip_nat_trace=1, mc_fwd=0, mc_ttl_nc=0, tpmc_sk_pl=0
name=vpn1001/vpn1001 index=4 enabled fib_ver=4 use=46 rt_num=0 asym_rt=0 sip_helper=0, sip_nat_trace=1, mc_fwd=0, mc_ttl_nc=0, tpmc_sk_pl=0
name=vpn1002/vpn1002 index=5 enabled fib_ver=4 use=43 rt_num=0 asym_rt=0 sip_helper=0, sip_nat_trace=1, mc_fwd=0, mc_ttl_nc=0, tpmc_sk_pl=0
name=vsys_hamgmt/vsys_hamgmt index=6 enabled fib_ver=8 use=47 rt_num=3 asym_rt=0 sip_helper=0, sip_nat_trace=1, mc_fwd=0, mc_ttl_nc=0, tpmc_sk_pl=0
name=vsys_ha/vsys_ha index=7 enabled fib_ver=18 use=53 rt_num=7 asym_rt=0 sip_helper=0, sip_nat_trace=1, mc_fwd=0, mc_ttl_nc=0, tpmc_sk_pl=0
name=vsys_fgfm/vsys_fgfm index=8 enabled fib_ver=4 use=40 rt_num=0 asym_rt=0 sip_helper=0, sip_nat_trace=1, mc_fwd=0, mc_ttl_nc=0, tpmc_sk_pl=0
```

2、 会话统计情况

```
# config global
# diagnose sys session full-stat
session table:                table_size=33554432 max_depth=1 used=14
misc info:          session_count=7 setup_rate=0 exp_count=0 clash=0
            memory_tension_drop=0 ephemeral=0/8454144 removeable=0
            npu_session_count=0
            nturbo_session_count=0
delete=0, flush=0, dev_down=0/0 ses_flush_filters=0
flush_work_num=0
TCP sessions:
             2 in ESTABLISHED state
firewall error stat:
error1=00000000
error2=00000000
error3=00000000
error4=00000000
tt=00000000
cont=00000000
ids_recv=00000000
url_recv=00000000
av_recv=00000000
fqdn_count=00000000
fqdn6_count=00000000
```

3、 单 IP 会话列表

① 配置过滤条件

```
# config global
# diagnose sys session filter src 192.168.15.1（过滤条件-源 IP）
# diagnose sys session filter dst 114.114.114.114（过滤条件-目的 IP）
# diagnose sys session filter sport 5001（过滤条件-源端口）
# diagnose sys session filter dport 443（过滤条件-目的端口）
# diagnose sys session filter dst 114.114.114.114（过滤条件-目的 IP）
# diagnose sys session filter proto 17（过滤条件-协议）
# diagnose sys session filter sintf port1（过滤源接口）
# diagnose sys session filter dintf port2（过滤目的接口）
# diagnose sys session filter vd 2（过滤 VDOM ID）
```

② 查看过滤器

```
# diagnose sys session filter（查看会话过滤器）
session filter:
            vd: 2
            sintf: 3
            dintf: 4
```

```
        proto: 6
        proto-state: any
        source ip: 192.168.15.1-192.168.15.1
        NAT'd source ip: any
        dest ip: 114.114.114.114-114.114.114.114
        source port: 5001-5001
        NAT'd source port: any
        dest port: 443-443
        policy id: any
        expire: any
        duration: any
        state1: any
        state2: any
```

③ 查看会话列表

```
# diagnose sys session list ( 查看会话列表 )
session info: proto=6 proto_state=00 duration=40 expire=23 timeout=0 flags=00000000 sockflag=00000000 sockport=0 av_idx=0
use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty
statistic(bytes/packets/allow_err): org=420/5/1 reply=420/5/1 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=16->6/6->16 gwy=192.168.118.1/192.168.35.2
hook=post dir=org act=snat 192.168.15.1:5001->114.114.114.114:443(192.168.118.17:5001)
hook=pre dir=reply act=dnat 114.114.114.114:443->192.168.118.17:5001(192.168.15.1:5001)
src_mac=aa:bb:cc:80:a0:00
misc=0 policy_id=4 auth_info=0 chk_client_info=0 vd=2
serial=00005f04 tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id = 00000000
dd_type=0 dd_mode=0
total session 1
```

④ 清空会话过滤器

```
# diagnose sys session filter clear
# diagnose sys session filter
session filter:
        vd: any
        sintf: any
        dintf: any
        proto: any
        proto-state: any
        source ip: any
        NAT'd source ip: any
        dest ip: any
        source port: any
        NAT'd source port: any
        dest port: any
        policy id: any
        expire: any
        duration: any
        state1: any
        state2: any
```

六、路由相关

1、 路由表查看

① 当前路由表

```
# config vdom
# edit NAT ( 进入需要查看路由的 VDOM )
# 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 172.16.0.1, npu4_vlink1
                   [10/0] via 172.16.0.5, npu5_vlink1
                   [10/0] via 172.16.0.9, npu6_vlink1
                   [10/0] via 172.16.0.13, npu7_vlink1
                   [10/0] via 172.16.0.17, npu0_vlink1
                   [10/0] via 172.16.0.21, npu1_vlink1
                   [10/0] via 172.16.0.25, npu2_vlink1
                   [10/0] via 172.16.0.29, npu3_vlink1
S        36.133.97.172/32 [10/0] is a summary, Null
S        36.133.98.185/32 [10/0] is a summary, Null
S        36.133.99.2/32 [10/0] is a summary, Null
S        36.133.99.23/32 [10/0] is a summary, Null
S        36.133.99.48/32 [10/0] is a summary, Null
S        36.133.99.234/32 [10/0] is a summary, Null
S        36.133.99.241/32 [10/0] is a summary, Null
S        36.133.100.190/32 [10/0] is a summary, Null
S        36.133.100.231/32 [10/0] is a summary, Null
S        36.133.101.144/32 [10/0] is a summary, Null
S        36.133.101.154/32 [10/0] is a summary, Null
S        36.133.101.157/32 [10/0] is a summary, Null
S        36.133.104.233/32 [10/0] is a summary, Null
S        36.133.104.244/32 [10/0] is a summary, Null
C        172.16.0.0/30 is directly connected, npu4_vlink1
C        172.16.0.4/30 is directly connected, npu5_vlink1
C        172.16.0.8/30 is directly connected, npu6_vlink1
C        172.16.0.12/30 is directly connected, npu7_vlink1
C        172.16.0.16/30 is directly connected, npu0_vlink1
C        172.16.0.20/30 is directly connected, npu1_vlink1
C        172.16.0.24/30 is directly connected, npu2_vlink1
C        172.16.0.28/30 is directly connected, npu3_vlink1
```

② 路由 database 查看

```
# config vdom
# edit NAT ( 进入需要查看路由的 VDOM )
# get router info routing-table database
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
       > - selected route, * - FIB route, p - stale info
Routing table for VRF=0
O E2 *> 0.0.0.0/0 [110/10] via 192.168.15.2, vlan15, 00:36:24
O E2 *> 10.10.1.0/24 [110/20] via 192.168.16.2, vlan16, 01:21:08
S     *> 10.10.4.0/24 [254/0] is a summary, Null
S        10.10.4.0/24 [10/0] is directly connected, FGT1-to-FGT4 inactive
O         192.168.15.0/24 [110/1] is directly connected, vlan15, 01:22:03
C     *> 192.168.15.0/24 is directly connected, vlan15
O         192.168.16.0/24 [110/1] is directly connected, vlan16, 03:10:04
C     *> 192.168.16.0/24 is directly connected, vlan16
O     *> 192.168.35.0/24 [110/2] via 192.168.15.2, vlan15, 01:21:09
Routing table for VRF=2
C     *> 5.5.5.0/24 is directly connected, port7
```

2、 OSPF

① OSPF 状态

```
# config vdom
# edit NAT ( 进入需要查看路由的 VDOM )
# get router info ospf status
 Routing Process "ospf 0" with ID 192.168.77.1
 Process uptime is 2 hours 47 minutes
 Process bound to VRF default
 Conforms to RFC2328, and RFC1583Compatibility flag is disabled
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Do not support Restarting
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Refresh timer 10 secs
 Number of incomming current DD exchange neighbors 0/5
 Number of outgoing current DD exchange neighbors 0/5
 Number of external LSA 2. Checksum 0x0061BB
 Number of opaque AS LSA 0. Checksum 0x000000
 Number of non-default external LSA 1
 External LSA database is unlimited.
 Number of LSA originated 1
 Number of LSA received 19
 Number of areas attached to this router: 1
    Area 0.0.0.0 (BACKBONE)
        Number of interfaces in this area is 2(2)
        Number of fully adjacent neighbors in this area is 2
        Area has no authentication
        SPF algorithm last executed 00:13:48.950 ago
        SPF algorithm executed 10 times
        Number of LSA 4. Checksum 0x018d2b
```

② OSPF 邻居

```
# config vdom
# edit NAT ( 进入需要查看路由的 VDOM )
# get router info ospf neighbor
OSPF process 0, VRF 0:
Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.35.2      1   Full/ -         00:00:33    192.168.15.2    vlan15
192.168.16.2      1   Full/ -         00:00:36    192.168.16.2    vlan16
```

3、 BGP

① BGP 状态

```
# config vdom
# edit NAT ( 进入需要查看路由的 VDOM )
# get router info bgp summary
BGP router identifier 192.168.77.3, local AS number 65500
BGP table version is 1
1 BGP AS-PATH entries
0 BGP community entries
Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.15.1    4      65500       0       0        0    0    0     never Active
Total number of neighbors 1
```

② BGP 邻居

```
# config vdom
# edit NAT ( 进入需要查看路由的 VDOM )
# get router info bgp neighbors
BGP neighbor is 192.168.15.1, remote AS 65500, local AS 65500, internal link
  BGP version 4, remote router ID 0.0.0.0
  BGP state = Active
  Last read           , hold time is 180, keepalive interval is 60 seconds
  Configured hold time is 180, keepalive interval is 60 seconds
  Received 0 messages, 0 notifications, 0 in queue
  Sent 1 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 0
  Index 1, Offset 0, Mask 0x2
```

```
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes
 For address family: IPv6 Unicast
  BGP table version 1, neighbor version 0
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes
 Connections established 0; dropped 0
Next connect timer due in 88 seconds
```

七、日志相关

1、 命令行查看日志

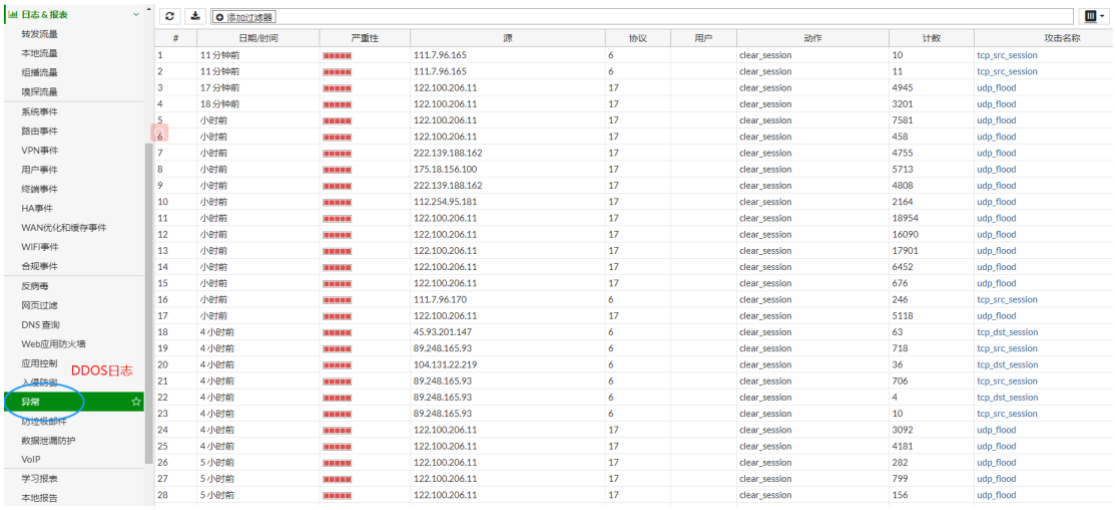
```
# config vdom
# edit root
# execute log filter xxxx（过滤想要查看到的日志内容）
# execute log display （查看日志内容）
```

21: date=2021-03-03 time=14:57:19 logid="0000000013" type="traffic" subtype="forward" level="notice" vd="root" eventtime=1614754639 srcip=101:101:: srcport=34474 srcintf="To_FW" srcintfrole="undefined" dstip=202:202:: dstport=20 dstintf="ipv4_external" dstintfrole="lan" sessionid=100000 proto=6 vrf=32 action="accept" policyid=1 policytype="policy6" service="tcp/20" dstcountry="Reserved" srccountry="Reserved" trandisp="noop" duration=10 sentbyte=2000 rcvdbyte=1000 sentpkt=0 rcvdpkt=0 appid=6 app="BitTorrent" appcat="P2P" apprisk="high" utmaction="allow" countapp=1 crscore=5 craction=1048576 utmref=100000

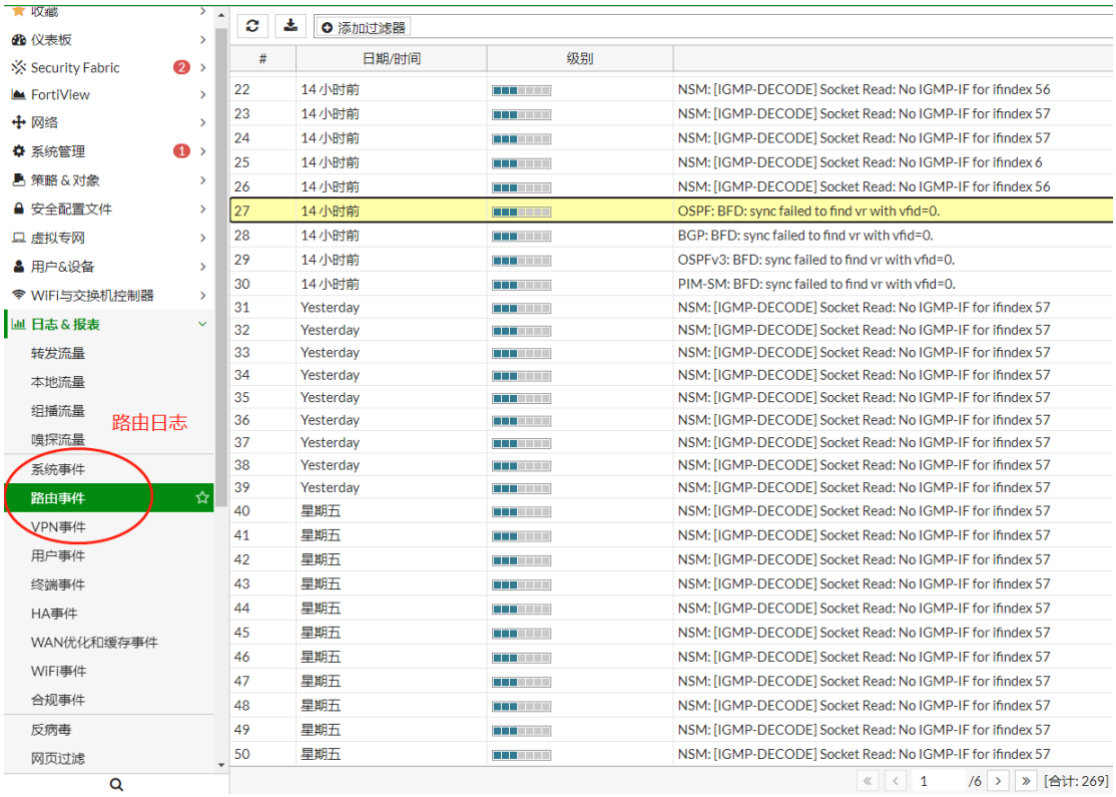
22: date=2021-03-03 time=14:57:19 logid="0000000013" type="traffic" subtype="forward" level="notice" vd="root" eventtime=1614754639 srcip=1.1.1.1 srcport=60000 srcintf="To_FW" srcintfrole="undefined" dstip=2.2.2.2 dstport=20 dstintf="ipv4_external" dstintfrole="lan" sessionid=60000 proto=6 vrf=32 action="accept" policyid=1 policytype="policy" service="tcp/20" dstcountry="France" srccountry="Australia" trandisp="noop" duration=10 sentbyte=2000 rcvdbyte=1000 sentpkt=0 rcvdpkt=0 appcat="unscanned" utmaction="allow" countapp=1 devtype="iPad" devcategory="None" osname="Apple" osversion="ver" mastersrcmac="01:01:01:01:01:01" srcmac="01:01:01:01:01:01" srcserver=0 dstdevtype="Android Phone" dstdevcategory="None" dstosname="Android" dstosversion="ver" masterdstmac="02:02:02:02:02:02" dstmac="02:02:02:02:02:02" dstserver=0 utmref=60000

23: date=2021-03-03 time=14:57:19 logid="0000000013" type="traffic" subtype="forward" level="notice" vd="root" eventtime=1614754639 srcip=1.1.1.1 srcport=50000 srcintf="To_FW" srcintfrole="undefined" dstip=2.2.2.2 dstport=20 dstintf="ipv4_external" dstintfrole="lan" sessionid=50000 proto=6 vrf=32 action="accept" policyid=1 policytype="policy" service="tcp/20" dstcountry="France" srccountry="Australia" trandisp="noop" duration=10 sentbyte=2000 rcvdbyte=1000 sentpkt=0 rcvdpkt=0 appcat="unscanned" utmaction="allow" countips=1 crscore=30 craction=8192 devtype="iPad" devcategory="None" osname="Apple" osversion="ver" mastersrcmac="01:01:01:01:01:01" srcmac="01:01:01:01:01:01" srcserver=0 dstdevtype="Android Phone" dstdevcategory="None" dstosname="Android" dstosversion="ver" masterdstmac="02:02:02:02:02:02" dstmac="02:02:02:02:02:02" dstserver=0 utmref=50000

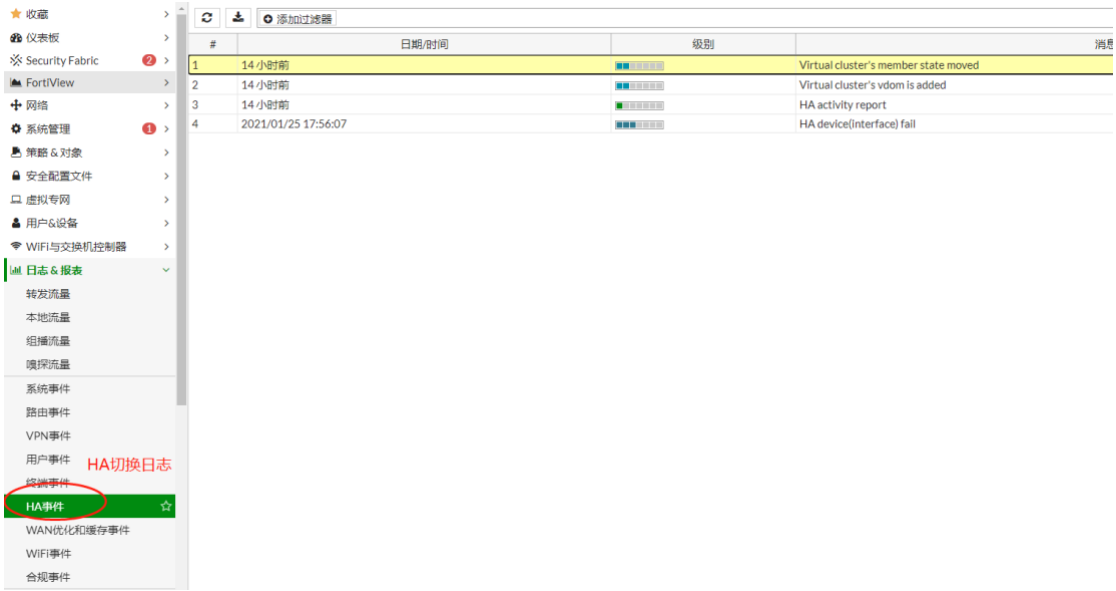
2、 DoS 日志



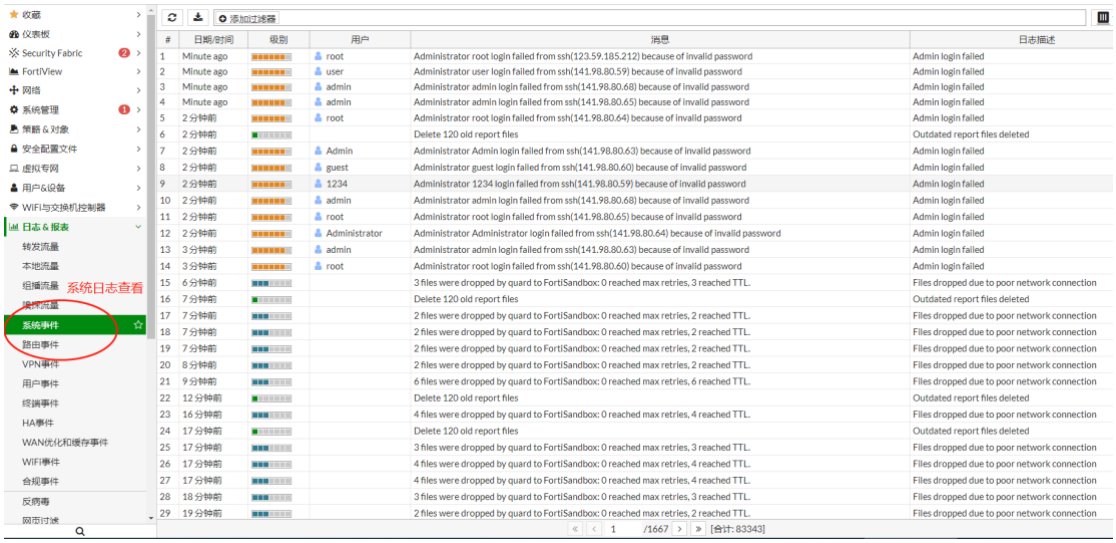
3、 路由日志



4、 HA 切换日志



5、 系统日志


收藏
仪表板
Security Fabric
FortiView
网络
系统管理
策略 & 对象
安全配置文件
虚拟专网
用户&设备
WiFi与交换机控制器
日志 & 报表
转发流量
本地流量
组播流量
应用流量
系统事件
路由事件
VPN事件
用户事件
终端事件
HA事件
WAN优化和缓存事件
WiFi事件
合规事件
反病毒
网页过滤
系统日志查看
添加过滤器
日期/时间 级别 用户 消息 日志描述
1 Minute ago root Administrator root login failed from ssh(123.59.185.212) because of invalid password Admin login failed
2 Minute ago user Administrator user login failed from ssh(141.98.80.59) because of invalid password Admin login failed
3 Minute ago admin Administrator admin login failed from ssh(141.98.80.68) because of invalid password Admin login failed
4 Minute ago admin Administrator admin login failed from ssh(141.98.80.65) because of invalid password Admin login failed
5 2 分钟前 root Administrator root login failed from ssh(141.98.80.64) because of invalid password Admin login failed
6 2 分钟前 Delete 120 old report files Outdated report files deleted
7 2 分钟前 Admin Administrator Admin login failed from ssh(141.98.80.63) because of invalid password Admin login failed
8 2 分钟前 guest Administrator guest login failed from ssh(141.98.80.60) because of invalid password Admin login failed
9 2 分钟前 1234 Administrator 1234 login failed from ssh(141.98.80.59) because of invalid password Admin login failed
10 2 分钟前 admin Administrator admin login failed from ssh(141.98.80.68) because of invalid password Admin login failed
11 2 分钟前 root Administrator root login failed from ssh(141.98.80.65) because of invalid password Admin login failed
12 2 分钟前 Administrator Administrator Administrator login failed from ssh(141.98.80.64) because of invalid password Admin login failed
13 3 分钟前 admin Administrator admin login failed from ssh(141.98.80.63) because of invalid password Admin login failed
14 3 分钟前 root Administrator root login failed from ssh(141.98.80.60) because of invalid password Admin login failed
15 6 分钟前 3 files were dropped by quard to FortiSandbox: 0 reached max retries, 3 reached TTL. Files dropped due to poor network connection
16 7 分钟前 Delete 120 old report files Outdated report files deleted
17 7 分钟前 2 files were dropped by quard to FortiSandbox: 0 reached max retries, 2 reached TTL. Files dropped due to poor network connection
18 7 分钟前 2 files were dropped by quard to FortiSandbox: 0 reached max retries, 2 reached TTL. Files dropped due to poor network connection
19 7 分钟前 2 files were dropped by quard to FortiSandbox: 0 reached max retries, 2 reached TTL. Files dropped due to poor network connection
20 8 分钟前 2 files were dropped by quard to FortiSandbox: 0 reached max retries, 2 reached TTL. Files dropped due to poor network connection
21 9 分钟前 6 files were dropped by quard to FortiSandbox: 0 reached max retries, 6 reached TTL. Files dropped due to poor network connection
22 12 分钟前 Delete 120 old report files Outdated report files deleted
23 16 分钟前 4 files were dropped by quard to FortiSandbox: 0 reached max retries, 4 reached TTL. Files dropped due to poor network connection
24 17 分钟前 Delete 120 old report files Outdated report files deleted
25 17 分钟前 3 files were dropped by quard to FortiSandbox: 0 reached max retries, 3 reached TTL. Files dropped due to poor network connection
26 17 分钟前 4 files were dropped by quard to FortiSandbox: 0 reached max retries, 4 reached TTL. Files dropped due to poor network connection
27 17 分钟前 4 files were dropped by quard to FortiSandbox: 0 reached max retries, 4 reached TTL. Files dropped due to poor network connection
28 18 分钟前 3 files were dropped by quard to FortiSandbox: 0 reached max retries, 3 reached TTL. Files dropped due to poor network connection
29 19 分钟前 2 files were dropped by quard to FortiSandbox: 0 reached max retries, 2 reached TTL. Files dropped due to poor network connection
1 /1667 [合计: 83343]

八、基本排障

1、 Ping 测试

```
# config vdom
# edit NAT ( 进入需要 ping 测试的 VDOM )
# execute ping 114.114.114.119

携带 ping-options，比如设置 ping 包的大小，ping 包个数，ping 包的源 IP 等等信息
FGT#    execute ping-options ?
execute ping-options adaptive-ping <enable|disable>
execute ping-options data-size <bytes>
execute ping-options df-bit {yes | no}
execute ping-options pattern <2-byte_hex>
execute ping-options repeat-count <repeats>
execute ping-options source {auto | <source-intf_ip>}
execute ping-options timeout <seconds>
execute ping-options tos <service_type>
execute ping-options ttl <hops>
execute ping-options validate-reply {yes | no}
execute ping-options view-settings

# execute ping-options    source 192.168.112.2

# execute ping 114.114.114.114
PING 114.114.114.114 (114.114.114.114): 56 data bytes
64 bytes from 114.114.114.114: icmp_seq=0 ttl=67 time=281.6 ms
64 bytes from 114.114.114.114: icmp_seq=1 ttl=64 time=282.1 ms
64 bytes from 114.114.114.114: icmp_seq=2 ttl=65 time=273.9 ms
64 bytes from 114.114.114.114: icmp_seq=3 ttl=57 time=277.7 ms
64 bytes from 114.114.114.114: icmp_seq=4 ttl=81 time=281.3 ms

--- 114.114.114.114 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 273.9/279.3/282.1 ms

# execute ping-options    reset
```

2、 Traceroute 测试

```
# config vdom
# edit NAT ( 进入需要 traceroute 测试的 VDOM )
# execute traceroute 114.114.114.114

携带 ping-options，比如设置 ping 包的大小，ping 包个数，ping 包的源 IP 等等信息

FGT# execute traceroute-options source 192.168.112.2

# execute traceroute 114.114.114.114
traceroute to 114.114.114.114 (114.114.114.114), 32 hops max, 3 probe packets per hop, 84 byte packets
 1   122.100.206.11   63.567 ms   62.221 ms   59.206 ms
 2   122.100.200.1   54.582 ms   45.155 ms   50.825 ms
 3   182.93.63.225   53.424 ms   76.430 ms   71.445 ms
 4   202.175.54.157   63.079 ms   61.107 ms   57.033 ms
 5   202.175.0.54   60.885 ms *   67.641 ms
 6   154.18.4.121   77.068 ms   60.769 ms   65.329 ms
 7   154.54.87.121   217.492 ms   217.488 ms   211.743 ms
 8   154.54.42.149   195.754 ms   197.387 ms   217.347 ms
 9   154.54.86.109   230.846 ms   229.508 ms   210.235 ms
10   154.54.42.98   221.108 ms   249.138 ms   237.969 ms
11   154.54.31.90   230.480 ms   233.100 ms   242.183 ms
12   154.54.44.170   271.583 ms   241.412 ms   257.967 ms
13   154.54.89.2   268.326 ms   254.575 ms   273.416 ms
14   38.142.58.114   275.943 ms   271.183 ms   253.467 ms
15   23.237.126.230   267.321 ms   265.119 ms   254.339 ms
16   * 23.237.136.242   271.085 ms   264.557 ms
17   114.114.114.114   265.090 ms   246.551 ms   262.582 ms
```

3、 Session List 会话查看

查看设备会话：

```
# config vdom
# edit NAT ( 进入需要查看会话的 VDOM )
# diagnose sys session filter dst 114.114.114.114
# diagnose sys session filter dport 53
# diagnose sys session filter
session filter:
        vd: any
        sintf: any
        dintf: any
        proto: any
        proto-state: any
        source ip: any
        NAT'd source ip: any
        dest ip: 114.114.114.114-114.114.114.114
        source port: any
        NAT'd source port: any
        dest port: 53-53
        policy id: any
        expire: any
        duration: any
        state1: any
        state2: any
# diagnose sys session list

session info: proto=17 proto_state=00 duration=348 expire=40 timeout=0 flags=00000000 sockflag=00000000 sockport=0 av_idx=0
use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=To_Macau/ helper=dns-udp vlan_cos=255/255
state=log local nds
statistic(bytes/packets/allow_err): org=31649/461/1 reply=0/0/0 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org out->post, reply pre->in dev=0->64/64->0 gwy=0.0.0.0/0.0.0.0
hook=out dir=org act=noop 111.204.123.114:1109->114.114.114.114:53(0.0.0.0:0)
hook=in dir=reply act=noop 114.114.114.114:53->111.204.123.114:1109(0.0.0.0:0)
misc=0 policy_id=0 auth_info=0 chk_client_info=0 vd=0
serial=000a4dc3 tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id = 00000000
dd_type=0 dd_mode=0
npu_state=00000000
no_ofld_reason:    local

清除设备会话：

# config vdom
# edit NAT ( 进入需要查看会话的 VDOM )
# diagnose sys session filter clear
# diagnose sys session filter dst 114.114.114.114
# diagnose sys session filter dport 53
# diagnose sys session filter
session filter:
        vd: any
        sintf: any
        dintf: any
        proto: any
        proto-state: any
        source ip: any
        NAT'd source ip: any
        dest ip: 114.114.114.114-114.114.114.114
        source port: any
        NAT'd source port: any
        dest port: 53-53
        policy id: any
        expire: any
        duration: any
        state1: any
        state2: any
# diagnose sys session clear
# diagnose sys session filter clear
```

4、 Sniffer 抓包

```
抓包命令：
# config vdom
# edit NAT（进入需要抓包的 VDOM）
# diagnose sniffer packet any "host 172.16.1.100 and icmp" 4                    //抓 172.16.1.100 的 ICMP 包
# diagnose sniffer packet any "host 172.16.1.100 and tcp" 4                     //抓 172.16.1.100 的 TCP 包
# diagnose sniffer packet any "host 172.16.1.100 and udp" 4                     //抓 172.16.1.100 的 UDP 包
# diagnose sniffer packet any "host 172.16.1.100 and tcp port 443" 4          //抓 172.16.1.100 且 https 的包
# diagnose sniffer packet any "host 172.16.1.100 and !tcp port 22" 4          //抓 172.16.1.100 且非 ssh 的包
# diagnose sniffer packet any "host 172.16.1.100 and port 10000" 4          //抓 172.16.1.100 且 TCP/UDP-Port=10000 的包
# diagnose sniffer packet any "host 114.114.119.119 and icmp" 4 0 a      // 携带 0 表示不限制抓包个数，携带 a 表示携带抓包的时间戳，a 表示不携带是时区的绝对时间

# diagnose sniffer packet any "host 114.114.119.119 and icmp" 4 0 l     // 携带 0 表示不限制抓包个数，携带 l 表示携带抓包的时间戳，l 表示携带是时区的绝对时间，通常我们使用这个参数，和设备保持一致

# diagnose sniffer packet any "host 114.114.119.119 and icmp" 4 0 l
interfaces=[any]
filters=[host 114.114.119.119 and icmp]
 2021-03-03 16:45:09.242113 p1v21 in 192.168.112.119 -> 114.114.119.119: icmp: echo request
2021-03-03 16:45:09.242154 wan1 out 111.204.123.114 -> 114.114.119.119: icmp: echo request
2021-03-03 16:45:09.255510 wan1 in 114.114.119.119 -> 111.204.123.114: icmp: echo reply
2021-03-03 16:45:09.255522 p1v21 out 114.114.119.119 -> 192.168.112.119: icmp: echo reply
2021-03-03 16:45:09.255523 port1 out 114.114.119.119 -> 192.168.112.119: icmp: echo reply
2021-03-03 16:45:10.247347 p1v21 in 192.168.112.119 -> 114.114.119.119: icmp: echo request
2021-03-03 16:45:10.247357 wan1 out 111.204.123.114 -> 114.114.119.119: icmp: echo request
2021-03-03 16:45:10.258293 wan1 in 114.114.119.119 -> 111.204.123.114: icmp: echo reply
2021-03-03 16:45:10.258300 p1v21 out 114.114.119.119 -> 192.168.112.119: icmp: echo reply
2021-03-03 16:45:10.258302 port1 out 114.114.119.119 -> 192.168.112.119: icmp: echo reply
2021-03-03 16:45:11.252070 p1v21 in 192.168.112.119 -> 114.114.119.119: icmp: echo request
2021-03-03 16:45:11.252078 wan1 out 111.204.123.114 -> 114.114.119.119: icmp: echo request
2021-03-03 16:45:11.263058 wan1 in 114.114.119.119 -> 111.204.123.114: icmp: echo reply
2021-03-03 16:45:11.263063 p1v21 out 114.114.119.119 -> 192.168.112.119: icmp: echo reply
2021-03-03 16:45:11.263065 port1 out 114.114.119.119 -> 192.168.112.119: icmp: echo reply
2021-03-03 16:45:12.254988 p1v21 in 192.168.112.119 -> 114.114.119.119: icmp: echo request
2021-03-03 16:45:12.254997 wan1 out 111.204.123.114 -> 114.114.119.119: icmp: echo request
2021-03-03 16:45:12.266359 wan1 in 114.114.119.119 -> 111.204.123.114: icmp: echo reply
2021-03-03 16:45:12.266364 p1v21 out 114.114.119.119 -> 192.168.112.119: icmp: echo reply
2021-03-03 16:45:12.266366 port1 out 114.114.119.119 -> 192.168.112.119: icmp: echo reply
```

5、 Debug flow 追踪流

```
追踪流命令：
Debug Flow 命令解析：diagnose debug flow filter addr x.x.x.x   //过滤某个 IP
diagnose debug flow show function-name enable          //显示功能模块名称
diagnose debug flow trace start 999                    //开启 debug flow trace 并显示 999 条 debug 信息
diagnose debug enable                                  //开启 debug 命令

diagnose debug flow trace stop                  //关闭 debug flow trace
diagnose debug flow filter clear                //清除过滤条件
diagnose debug disable                          //关闭 debug 命令
iagnose debug reset                             //重置所有的 debug 命令

常用 debug flow 举例 1：抓取 10.10.10.100 且 ICMP 的流量 debug flow 脚本
diagnose debug reset
diagnose debug console timestamp enable

diagnose debug flow filter addr 10.10.10.100
diagnose debug flow filter proto 1
diagnose debug flow show function-name enable
diagnose debug flow trace start 100
diagnose debug enable


常用 debug flow 举例 2：抓取 10.10.10.100 且 TCP 端口为 10443 的流量 debug flow 脚本
diagnose debug reset
diagnose debug console timestamp enable

diagnose debug flow filter addr 10.10.10.100
diagnose debug flow filter proto 6
diagnose debug flow filter port 10443
diagnose debug flow show function-name enable
diagnose debug flow trace start 100
```

diagnose debug enable

常用 debug flow 举例 3：抓取 10.10.10.100 且 UDP 端口为 500 的流量 debug flow 脚本
diagnose debug reset
diagnose debug console timestamp enable

diagnose debug flow filter addr 10.10.10.100
diagnose debug flow filter proto 17
diagnose debug flow filter port 500
diagnose debug flow show function-name enable
diagnose debug flow trace start 100
diagnose debug enable
Debug Flow 结束后关闭 debug flow 的脚本：关闭 debug flow 脚本
diagnose debug disable
diagnose debug reset

举例：
config vdom
edit NAT（进入需要查看流的 VDOM）
diagnose sys session filter dst 202.106.1.100
diagnose sys session clear

diagnose debug reset
diagnose debug console timestamp enable

diagnose debug flow filter addr 202.106.1.100
diagnose debug flow filter proto 1
diagnose debug flow show function-name enable
diagnose debug flow trace start 10
diagnose debug enable

正常通信时 Debug Flow 信息：
2016-11-04 02:37:25 id=20085 trace_id=31 func=print_pkt_detail line=4478 msg="vd-root received a packet(proto=1, 172.16.1.100:768->202.106.1.100:8) from port9. code=8, type=0, id=768, seq=768."
2016-11-04 02:37:25 id=20085 trace_id=31 func=init_ip_session_common line=4629 msg="allocate a new session-00082e36"
2016-11-04 02:37:25 id=20085 trace_id=31 func=vf_ip4_route_input line=1596 msg="find a route: flags=00000000 gw-202.106.1.100 via port10"
2016-11-04 02:37:25 id=20085 trace_id=31 func=fw_forward_handler line=675 msg="Allowed by Policy-6: SNAT"
2016-11-04 02:37:25 id=20085 trace_id=31 func=__ip_session_run_tuple line=2606 msg="SNAT 172.16.1.100->202.106.1.1:62464 "

2016-11-04 02:37:25 id=20085 trace_id=32 func=print_pkt_detail line=4478 msg="vd-root received a packet(proto=1, 202.106.1.100:62464->202.106.1.1:0) from port10. code=0, type=0, id=62464, seq=768."
2016-11-04 02:37:25 id=20085 trace_id=32 func=resolve_ip_tuple_fast line=4539 msg="Find an existing session, id-00082e36, reply direction"
2016-11-04 02:37:25 id=20085 trace_id=32 func=__ip_session_run_tuple line=2620 msg="DNAT 202.106.1.1:0->172.16.1.100:768"
2016-11-04 02:37:25 id=20085 trace_id=32 func=vf_ip4_route_input line=1596 msg="find a route: flags=00000000 gw-172.16.1.100 via port9 "

关闭 debug flow：
diagnose debug disable
diagnose debug reset

九、备份恢复

1、 备份配置

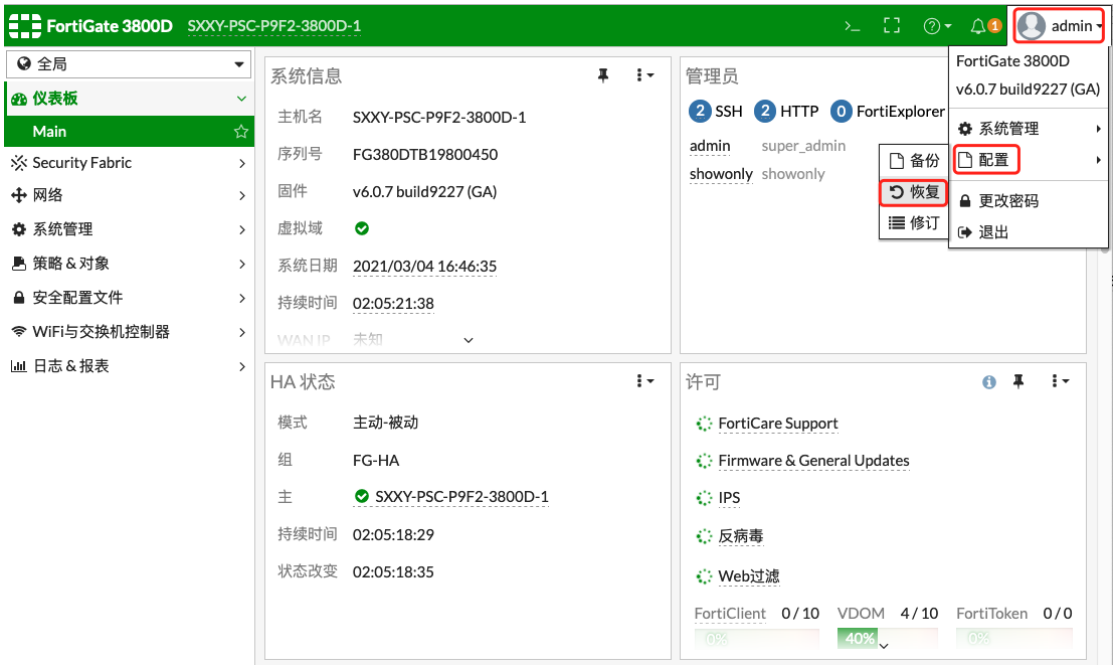
① 登陆设备的 Web 界面，点击右上方登录账号 admin，找到配置，点击“备份”按钮，对配置进行保存。

② 范围选择全局，本分到本地 PC，根据需求选择是否加密，点击确认按钮。

③ 选择要保存的路径，以及配置文件名称。

2、 恢复配置

① 登陆设备的 Web 界面，点击右上方登录账号 admin，找到配置，点击“恢复”按钮，对配置进行保存。

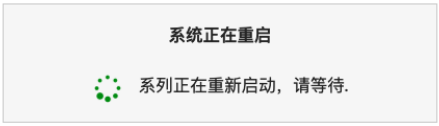


② 范围选择“全局”，恢复自选择“本地 PC”，点击上传按钮，选择配置文件，如果配置文件在保存时加密，则需要填入密码。

③ 范围选择“全局”，恢复自选择“本地 PC”，点击上传按钮，选择配置文件，如果配置文件在保存时加密，则需要填入密码。

④ 点击“确认”按钮上传配置，提示需要重启设备，确认无误后，点击 OK。

⑤ 等待设备重启完成，恢复配置成功。



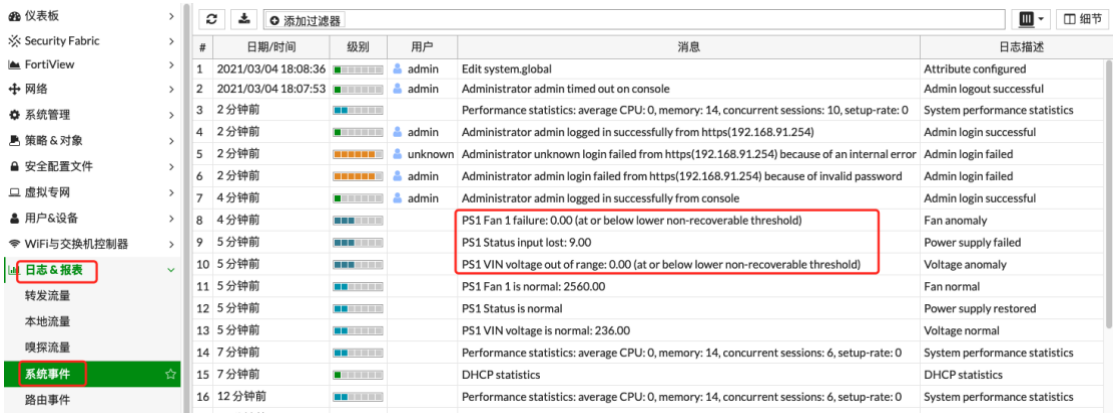
十、硬件故障

1、 电源

① 命令行方式查看电源状态。

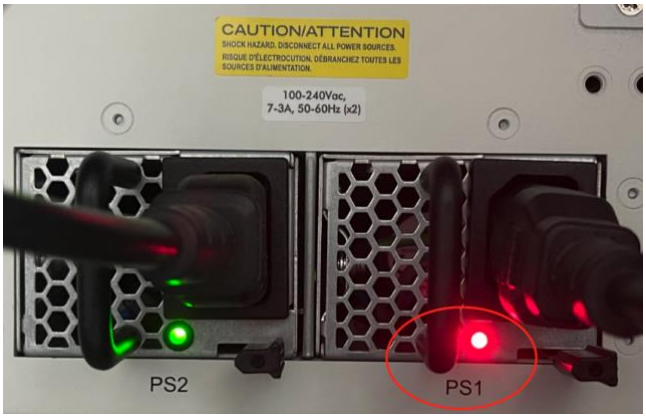
```
config global
exe sensor list
.....
        72 PS1 VIN              alarm=1   value=0   threshold_status=0x7
        73 PS1 VOUT_12V         alarm=1   value=-0.064   threshold_status=0x7
        74 PS1 IIN              alarm=0   value=0   threshold_status=0
        75 PS1 IOUT_12V         alarm=0   value=0   threshold_status=0
        76 PS1 POUT             alarm=0   (not detected)
        77 PS1 Temp 1           alarm=0   value=18   threshold_status=0
        78 PS1 Temp 2           alarm=0   (scanning disabled)
        79 PS1 Temp 3           alarm=0   value=20   threshold_status=0
        80 PS1 Fan 1            alarm=1   value=0   threshold_status=0x7
        81 PS1 Status           alarm=1
        82 PS2 VIN              alarm=0   value=236   threshold_status=0
        83 PS2 VOUT_12V         alarm=0   value=12.221   threshold_status=0
        84 PS2 IIN              alarm=0   value=1   threshold_status=0
        85 PS2 IOUT_12V         alarm=0   value=17.5   threshold_status=0
        86 PS2 POUT             alarm=0   (not detected)
        87 PS2 Temp 1           alarm=0   value=26   threshold_status=0
        88 PS2 Temp 2           alarm=0   value=32   threshold_status=0
        89 PS2 Temp 3           alarm=0   value=52   threshold_status=0
        90 PS2 Fan 1            alarm=0   value=4224   threshold_status=0
        91 PS2 Status           alarm=0
.....
```

② 设备管理页面查看系统日志中的电源日志。



#	日期/时间	级别	用户	消息	日志描述
1	2021/03/04 18:08:36		admin	Edit system.global	Attribute configured
2	2021/03/04 18:07:53		admin	Administrator admin timed out on console	Admin logout successful
3	2 分钟前			Performance statistics: average CPU: 0, memory: 14, concurrent sessions: 10, setup-rate: 0	System performance statistics
4	2 分钟前		admin	Administrator admin logged in successfully from https(192.168.91.254)	Admin login successful
5	2 分钟前		unknown	Administrator unknown login failed from https(192.168.91.254) because of an internal error	Admin login failed
6	2 分钟前		admin	Administrator admin login failed from https(192.168.91.254) because of invalid password	Admin login failed
7	4 分钟前		admin	Administrator admin logged in successfully from console	Admin login successful
8	4 分钟前			PS1 Fan 1 failure: 0.00 (at or below lower non-recoverable threshold)	Fan anomaly
9	5 分钟前			PS1 Status input lost: 9.00	Power supply failed
10	5 分钟前			PS1 VIN voltage out of range: 0.00 (at or below lower non-recoverable threshold)	Voltage anomaly
11	5 分钟前			PS1 Fan 1 is normal: 2560.00	Fan normal
12	5 分钟前			PS1 Status is normal	Power supply restored
13	5 分钟前			PS1 VIN voltage is normal: 236.00	Voltage normal
14	7 分钟前			Performance statistics: average CPU: 0, memory: 14, concurrent sessions: 6, setup-rate: 0	System performance statistics
15	7 分钟前			DHCP statistics	DHCP statistics
16	12 分钟前			Performance statistics: average CPU: 0, memory: 14, concurrent sessions: 6, setup-rate: 0	System performance statistics

③ 设备电源接口亮红灯持续闪烁。



④ 设备电源出现问题时，首先进行 HA 切换，确认将主设备切换到电源没有出现问题的设备，保留以上命令执行结果及日志，再联系原厂进行硬件检测。

2、 光模块

① 查看光模块状态参数。

```
# config global
# get sys interface transceiver <port id>
Interface port11 - SFP/SFP+
  Vendor Name   :                FINISAR CORP.
  Part No.      :                FTLX8574D3BCL
  Serial No.    :                A2MB1T5
  Measurement   Unit             Value          High Alarm    High Warning Low Warning   Low Alarm
  ------------ ------------ ------------ ------------ ------------ ------------ ------------
  Temperature   (Celsius)      34.5           78.0          73.0          -8.0          -13.0
  Voltage       (Volts)        3.37           3.70          3.60          3.00          2.90
  Tx Bias       (mA)           9.00           13.00         12.50         5.00          4.00
  Tx Power      (dBm)          -2.6           0.0           -1.0          -5.0          -6.0
  Rx Power      (dBm)          -3.3           0.0           -1.0          -18.0         -20.0
    ++ : high alarm, + : high warning, - : low warning, -- : low alarm, ? : suspect.
```

② 如果光模块状态出现问题，首先进行 HA 切换，恢复业务，再由现场更换光模块会线缆。